EUROPÄISCHE
KOMMISSION

Brüssel, den 7.2.2013
COM(2013) 48 final

2013/0027 (COD)

Vorschlag für eine

RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union

{SWD(2013) 31 final}
{SWD(2013) 32 final}

BEGRÜNDUNG

Ziel der vorgeschlagenen Richtlinie ist die Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit (NIS). Hierbei geht es um die Erhöhung der Sicherheit des Internets und der privaten Netze und Informationssysteme, die für das Funktionieren unserer Gesellschaften und Volkswirtschaften unverzichtbar sind. Dies soll erreicht werden, indem die Mitgliedstaaten verpflichtet werden, ihre Abwehrbereitschaft zu erhöhen und ihre Zusammenarbeit untereinander zu verbessern, und indem die Betreiber kritischer Infrastrukturen wie Energieversorger, Verkehrsunternehmen und wichtige Anbieter von Diensten der Informationsgesellschaft (Plattformen für den elektronischen Geschäftsverkehr, soziale Netze usw.) und die öffentlichen Verwaltungen verpflichtet werden, geeignete Schritte zur Beherrschung von Sicherheitsrisiken zu unternehmen und den zuständigen nationalen Behörden gravierende Sicherheitsvorfälle zu melden.

Dieser Vorschlag wird in Verbindung mit der gemeinsamen Mitteilung der Kommission und der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik über eine europäische Cybersicherheitsstrategie vorgelegt. Ziel der Strategie ist die Gewährleistung eines sicheren und vertrauenswürdigen digitalen Umfelds, während gleichzeitig die Grundrechte und die anderen Grundwerte der EU gefördert und gewahrt werden. Dieser Vorschlag ist die wichtigste Maßnahme der genannten Strategie. Weitere Maßnahmen der Strategie in diesem Bereich betreffen die Sensibilisierung, den Aufbau eines Binnenmarkts für Cybersicherheitsprodukte und -dienste sowie die Förderung von Investitionen in die Forschung und Entwicklung. Sie werden ergänzt durch weitere Maßnahmen zur Verstärkung des Kampfes gegen die Cyberkriminalität und zur Schaffung einer internationalen Cybersicherheitspolitik für die EU.

1.1. Gründe und Ziele des Vorschlags

Die Netz- und Informationssicherheit (NIS) hat eine wachsende Bedeutung in unserer Wirtschaft und Gesellschaft. Sie ist auch eine wichtige Voraussetzung für die Schaffung eines verlässlichen Umfelds für den weltweiten Dienstleistungsverkehr. Informationssysteme können aber aufgrund von Sicherheitsvorfällen wie menschlichem Versagen, Naturereignissen, technischen Fehlern oder böswilligen Angriffen gestört werden. Derartige Vorfälle werden immer größer, häufiger und komplexer. Die von der Kommission durchgeführte Online-Konsultation zur „Verbesserung der Netz- und Informationssicherheit in der EU“[1] ergab, dass 57 % der Konsultationsteilnehmer im vorangegangenen Jahr NIS-Vorfälle mit ernsten Auswirkungen auf ihre Tätigkeiten zu verzeichnen hatten. Unerlässliche Dienste, die von der Integrität der Netze und Informationssysteme abhängen, können durch eine mangelnde NIS beeinträchtigt werden. Dies kann dazu führen, dass Unternehmen nicht mehr arbeiten können, dass der EU-Wirtschaft große finanzielle Verluste entstehen und dass das gesellschaftliche Wohl leidet.

Darüber hinaus sind digitale Informationssysteme, allen voran das Internet, als Kommunikationsmittel, die keine Ländergrenzen kennen, in allen Mitgliedstaaten miteinander vernetzt und spielen im grenzüberschreitenden Waren-, Dienstleistungs- und Personenverkehr eine wesentliche Rolle. Eine schwere Störung dieser Systeme in einem Mitgliedstaat kann daher auch andere Mitgliedstaaten und die EU insgesamt in Mitleidenschaft ziehen. Deshalb ist die Robustheit und Stabilität der Netze und Informationssysteme eine Voraussetzung für die Vollendung des digitalen Binnenmarkts und für das reibungslose Funktionieren des Binnenmarkts überhaupt. Die Wahrscheinlichkeit und Häufigkeit von Sicherheitsvorfällen sowie die Unfähigkeit, einen wirksamen Schutz zu gewährleisten, untergraben auch das

[1] Die öffentliche Online-Konsultation zur „Verbesserung der Netz- und Informationssicherheit in der EU“ lief vom 23. Juli bis zum 15. Oktober 2012.

Vertrauen der Öffentlichkeit in Netze und Informationssysteme. So ergab beispielsweise die 2012 durchgeführte Eurobarometer-Erhebung zur Cybersicherheit, dass 38 % der Internetznutzer in der EU Bedenken in Bezug auf die Sicherheit von Online-Zahlungen haben und dass sie infolge der Sicherheitsbedenken ihr Verhalten geändert haben, denn 18 % sind weniger geneigt, Waren online zu kaufen und 15 % sind weniger geneigt, Bankgeschäfte online abzuwickeln[2].

Die gegenwärtige Situation in der EU ist das Ergebnis des bislang rein freiwilligen Vorgehens und bietet keinen ausreichenden EU-weiten Schutz vor NIS-Vorfällen und NIS-Risiken. Bestehende NIS-Kapazitäten und -Mechanismen reichen einfach nicht aus, um mit den schnellen Veränderungen der Bedrohungen Schritt zu halten und in allen Mitgliedstaaten ein gleich hohes Schutzniveau zu gewährleisten.

Trotz der bereits ergriffenen Initiativen gibt es große Unterschiede in Bezug auf die Kapazitäten und die Abwehrbereitschaft der einzelnen Mitgliedstaaten, was zu einem fragmentierten Vorgehen in der EU führt. Angesichts der Tatsache, dass Netze und Systeme eng miteinander verflochten sind, wird die Netz- und Informationssicherheit der EU durch Mitgliedstaaten mit unzureichendem Schutzniveau insgesamt geschwächt. Diese Situation behindert auch die Schaffung von Vertrauen zwischen den Partnern als Voraussetzung für die Zusammenarbeit und den Informationsaustausch. In der Folge findet eine Zusammenarbeit nur zwischen jenen wenigen Mitgliedstaaten statt, die bereits über hohe Kapazitäten verfügen.

Deshalb gibt es auf EU-Ebene gegenwärtig keinen wirksamen Mechanismus für eine effektive Zusammenarbeit und für einen vertrauensvollen Informationsaustausch über NIS-Vorfälle und NIS-Risiken zwischen den Mitgliedstaaten. Dadurch kann es zu einer unkoordinierten Regulierung, uneinheitlichen Strategien und abweichenden Normen kommen, was einen unzureichenden Schutz vor NIS-Vorfällen in der gesamten EU nach sich zieht. Außerdem können so Marktschranken entstehen, aus denen sich Befolgungskosten für jene Unternehmen ergeben, die in mehr als einem Mitgliedstaat tätig sind.

Schließlich unterliegen die Marktteilnehmer, die kritische Infrastrukturen betreiben oder die Dienste erbringen, welche für das Funktionieren unserer Gesellschaften unverzichtbar sind, keiner angemessenen Verpflichtung, entsprechende Risikomanagementmaßnahmen zu treffen und einen Informationsaustausch mit den zuständigen Behörden zu pflegen. Einerseits haben die Unternehmen so keine wirksamen Anreize für die Einführung eines ernsthaften Risikomanagements, das eine Risikobewertung und geeignete Schritte zur Gewährleistung der NIS umfasst. Anderseits wird ein großer Teil der Sicherheitsvorfälle den zuständigen Behörden gar nicht zur Kenntnis gebracht und bleibt von diesen unbemerkt. Informationen über solche Sicherheitsvorfälle sind jedoch die Voraussetzung dafür, dass die Behörden hierauf reagieren, geeignete Gegenmaßnahmen treffen und angemessene strategische Prioritäten für die NIS setzen können.

Nach dem derzeit geltenden Rechtsrahmen sind nur Telekommunikationsunternehmen dazu verpflichtet, Risikomanagementmaßnahmen zu ergreifen und gravierende NIS-Vorfälle zu melden. Aber auch viele andere Sektoren hängen wesentlich von den IKT als Tätigkeitsgrundlage ab und sollten sich daher ebenfalls mit Fragen der NIS befassen. Bestimmte Infrastrukturbetreiber und Diensteanbieter sind wegen ihrer hohen Abhängigkeit von korrekt funktionierenden Netzen und Informationssystemen besonders anfällig. Diese Sektoren spielen eine wesentliche Rolle bei der Erbringung wichtiger Unterstützungsdienste für unsere Wirtschaft und Gesellschaft, und die Sicherheit ihrer Systeme ist von besonderer Bedeutung für das Funktionieren des Binnenmarkts. Dazu gehören Banken und Börsen, die

[2] Eurobarometer 390 (2012).

Energieerzeugung, -übertragung und -verteilung, der Verkehr (Luft-, Schienen- und Seeverkehr), das Gesundheitswesen, Internetdienste und öffentliche Verwaltungen.

Beim Umgang mit Fragen der NIS ist deshalb in der EU ein neues Herangehen erforderlich. Es werden rechtliche Verpflichtungen benötigt, um gleiche Wettbewerbsbedingungen zu schaffen und bestehende Gesetzeslücken zu schließen. Um diese Probleme zu lösen und die Netz- und Informationssicherheit innerhalb der Europäischen Union zu erhöhen, werden mit der vorgeschlagenen Richtlinie die folgenden Ziele verfolgt.

Erstens sieht der Vorschlag für alle Mitgliedstaaten die Verpflichtung vor, ein Mindestniveau nationaler Kapazitäten zu schaffen, indem sie für die NIS zuständige Behörden einrichten, IT-Notfallteams (*Computer Emergency Response Teams*, CERTs) bilden und nationale NIS-Strategien und nationale NIS-Kooperationspläne aufstellen.

Zweitens sollten die zuständigen nationalen Behörden in einem Netz zusammenarbeiten, das eine sichere und wirksame Koordinierung ermöglicht, wozu auch ein koordinierter Informationsaustausch sowie eine Erkennungs- und Reaktionsfähigkeit auf EU-Ebene gehören. Über dieses Netz sollten die Mitgliedstaaten Informationen austauschen und zusammenarbeiten, um NIS-Bedrohungen und NIS-Vorfällen auf der Grundlage eines europäischen NIS-Kooperationsplans zu begegnen.

Drittens soll der Vorschlag nach dem Muster der Rahmenrichtlinie für die elektronische Kommunikation dafür sorgen, dass sich eine Kultur des Risikomanagements entwickelt und dass ein Informationsaustausch zwischen privatem und öffentlichem Sektor stattfindet. Unternehmen in den oben erwähnten besonders betroffenen Sektoren und öffentliche Verwaltungen sollen verpflichtet werden, die Risiken, denen sie unterliegen, zu bewerten und geeignete und angemessene Maßnahmen zur Gewährleistung der NIS zu ergreifen. Sie werden verpflichtet sein, den zuständigen Behörden alle Sicherheitsvorfälle zu melden, welche ihre Netze und Informationssysteme wie auch die Kontinuität kritischer Dienste und die Lieferung von Waren ernsthaft beeinträchtigen.

1.2. Allgemeiner Kontext

Schon im Jahr 2001 hob die Kommission in ihrer Mitteilung „Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz“[3] die wachsende Bedeutung der Netz- und Informationssicherheit hervor. Darauf folgte 2006 die Annahme einer Strategie für eine sichere Informationsgesellschaft[4], die auf die Entwicklung einer Kultur der Netz- und Informationssicherheit in Europa abzielte. Die Hauptelemente dieser Strategie wurden in einer Entschließung des Rates[5] gebilligt.

Darüber hinaus nahm die Kommission am 30. März 2009 eine Mitteilung über den Schutz kritischer Informationsinfrastrukturen (CIIP)[6] an, in deren Mittelpunkt der Schutz Europas vor Cyberstörungen durch eine Erhöhung der Sicherheitsvorkehrungen steht. Mit der Mitteilung wurde auch ein Aktionsplan in Angriff genommen, um die Mitgliedstaaten bei der Prävention und Reaktion zu unterstützen. Der Aktionsplan wurde in den Schlussfolgerungen des Ratsvorsitzes zum Schutz kritischer Informationsinfrastrukturen anlässlich der Ministerkonferenz 2009 in Tallinn gebilligt. Am 18. Dezember 2009 nahm der Rat eine Entschließung über ein kooperatives europäisches Vorgehen im Bereich der Netz- und Informationssicherheit[7] an.

---

3 KOM(2001) 298.
4 KOM(2006) 251, http://eur-lex.europa.eu/LexUriServ/site/de/com/2006/com2006_0251de01.pdf.
5 2007/068/01.
6 KOM(2009) 149.
7 2009/C 321/01.

In der im Mai 2010 verabschiedeten Digitalen Agenda für Europa[8] (DAE) und den diesbezüglichen Schlussfolgerungen des Rates[9] wurde das Einvernehmen darüber hervorgehoben, dass Vertrauen und Sicherheit grundlegende Voraussetzungen für eine breite Nutzung der IKT und damit für das Erreichen der Ziele des „intelligenten Wachstums“ im Rahmen der Strategie Europa 2020[10] sind. In der DAE wird im Kapitel zu Vertrauen und Sicherheit betont, dass alle Akteure sich mit vereinten Kräften in einem ganzheitlichen Ansatz um die Sicherheit und Robustheit der IKT-Infrastrukturen mit den Schwerpunkten Prävention, Abwehrbereitschaft und Sensibilisierung sowie um die Entwicklung wirksamer und koordinierter Sicherheitsmechanismen bemühen müssen. Die Schlüsselaktion 6 der Digitalen Agenda für Europa sieht so insbesondere Maßnahmen für eine Politik zur Stärkung der Netz- und Informationssicherheit auf hohem Niveau vor.

In ihrer Mitteilung zum Schutz kritischer Informationsinfrastrukturen (CIIP) vom März 2011 „Ergebnisse und nächste Schritte: der Weg zur globalen Netzsicherheit“[11] zog die Kommission eine Bilanz der seit der Verabschiedung des CIIP-Aktionsplans 2009 erreichten Ergebnisse und gelangte angesichts der Durchführung des Aktionsplans zu dem Schluss, dass ein rein nationales Vorgehen zur Bewältigung der Probleme in Bezug auf die Sicherheit und Robustheit nicht ausreicht und dass Europa seine Anstrengungen um eine kohärente und kooperative Vorgehensweise fortsetzen sollte. In der CIIP-Mitteilung von 2011 kündigte die Kommission eine Reihe von Maßnahmen an und rief die Mitgliedstaaten zur Erhöhung ihrer NIS-Kapazitäten und zur grenzübergreifenden Zusammenarbeit auf. Die meisten dieser Maßnahmen sollten im Jahr 2012 abgeschlossen werden, sind bislang aber noch nicht umgesetzt worden.

In seinen Schlussfolgerungen vom 27. Mai 2011 zum Schutz kritischer Informationsinfrastrukturen betonte der Rat der Europäischen Union die dringende Notwendigkeit, die Informatiksysteme und -netze gegen unbeabsichtigte wie beabsichtigte Störungen aller Art widerstandsfähig zu machen und abzusichern, in der gesamten EU eine hohe Abwehrbereitschaft, Sicherheit und Robustheit zu entwickeln, die fachlichen Kompetenzen zu erhöhen, damit sich Europa der Herausforderung des Schutzes der Netze und Informationsinfrastrukturen stellen kann, und die Zusammenarbeit zwischen den Mitgliedstaaten durch Einrichtung von Kooperationsmechanismen für Sicherheitsvorfälle zu verbessern.

1.3. Derzeitige einschlägige Vorschriften auf EU- und internationaler Ebene

Durch die Verordnung (EG) Nr. 460/2004 errichtete die Europäische Union im Jahr 2004 die Europäische Agentur für Netz- und Informationssicherheit (ENISA)[12], um zur Gewährleistung einer hohen Netz- und Informationssicherheit und zur Entwicklung einer NIS-Kultur in der EU beizutragen. Ein Vorschlag zur Modernisierung des Auftrags der ENISA wurde am 30. September 2010 angenommen und liegt derzeit dem Rat und dem Europäischen Parlament zur Beratung vor[13]. Der neugefasste Rechtsrahmen für die elektronische Kommunikation[14], der seit November 2009 in Kraft ist, erlegt den Anbietern

---

8 KOM(2010) 245.

9 Schlussfolgerungen des Rates vom 31. Mai 2010 zur Mitteilung „Eine digitale Agenda für Europa“ (10130/10).

10 KOM(2010) 2020 und Schlussfolgerungen des Europäischen Rates vom 25./26. März 2010 (EUCO 7/10).

11 KOM(2011) 163.

12 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:DE:HTML.

13 KOM(2010) 521.

14 Siehe http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf.

elektronischer Kommunikationsnetze und -dienste bestimmte Sicherheitspflichten auf[15]. Diese Verpflichtungen mussten bis Mai 2011 auf nationaler Ebene umgesetzt werden.

Alle für die Datenverarbeitung Verantwortlichen (z. B. Banken oder Krankenhäuser) sind nach dem Datenschutzrechtsrahmen[16] verpflichtet, Sicherheitsvorkehrungen zum Schutz personenbezogener Daten zu treffen. Außerdem sollen nach dem Vorschlag der Kommission von 2012 für eine Datenschutz-Grundverordnung[17] alle für die Datenverarbeitung Verantwortlichen dazu verpflichtet werden, Verletzungen des Schutzes personenbezogener Daten den nationalen Aufsichtsbehörden zu melden. Das bedeutet, dass beispielsweise ein NIS-Vorfall, der zwar die Bereitstellung eines Dienstes stört, ohne aber den Schutz personenbezogener Daten zu beeinträchtigen (z. B. eine IKT-Störung bei einem Energieversorger, die zu einem Stromausfall führt) nicht gemeldet zu werden bräuchten.

Im Rahmen der Richtlinie 2008/114/EG des Rates über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern, enthält das „Europäische Programm für den Schutz kritischer Infrastrukturen“[18] (EPCIP) ein übergreifendes Gesamtkonzept für den Schutz kritischer Infrastrukturen in der EU. Die Ziele des EPCIP stehen in vollem Einklang mit dem vorliegenden Vorschlag, und die Richtlinie sollte unbeschadet der Richtlinie 2008/114/EG gelten. Das EPCIP sieht weder für Betreiber Meldepflichten bei schweren Sicherheitsverletzungen noch für die Mitgliedstaaten Kooperations- und Reaktionsmechanismen bei Sicherheitsvorfällen vor.

Die Gesetzgeber beraten derzeit über den Vorschlag der Kommission für eine Richtlinie über Angriffe auf Informationssysteme[19], mit dem die Strafbarkeit bestimmter Verhaltensweisen vereinheitlicht werden soll. Der Vorschlag regelt lediglich die Strafbarkeit bestimmter Verhaltensweisen, nicht aber die Prävention von NIS-Risiken und NIS-Vorfällen, die Reaktion auf NIS-Vorfälle oder die Minderung ihrer Folgen. Die vorliegende Richtlinie sollte unbeschadet der Richtlinie über Angriffe auf Informationssysteme gelten.

Am 28. März 2012 nahm die Kommission eine Mitteilung über die Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität (EC3) an[20]. Dieses Zentrum besteht seit dem 11. Januar 2013 als Teil des Europäischen Polizeiamts (EUROPOL) und dient als zentrale Anlaufstelle für die Bekämpfung der Cyberkriminalität in der EU. Das EC3 soll cyberkriminalistische Fachkompetenzen bündeln, um die Mitgliedstaaten beim Aufbau geeigneter Kapazitäten zu unterstützen, die Ermittlungsarbeiten der Mitgliedstaaten bei Cyberstraftaten unterstützen sowie in enger Zusammenarbeit mit Eurojust zum gemeinsamen Sprachrohr aller mit der Untersuchung von Cyberstraftaten befassten Ermittler der Strafverfolgungs- und Justizbehörden in der EU werden.

Die Organe, Einrichtungen und sonstigen Stellen der Europäischen Union haben mit dem „CERT-EU“ ihr eigenes IT-Notfallteam eingerichtet.

Auf internationaler Ebene ist die EU im Bereich der Cybersicherheit sowohl auf bilateraler als auch multilateraler Ebene tätig. Auf dem Gipfeltreffen EU-USA[21] wurde die Arbeitsgruppe EU-USA zur Cybersicherheit und Cyberkriminalität eingesetzt. Darüber hinaus ist die EU

---

15 Artikel 13a und 13b der Rahmenrichtlinie.

16 Richtlinie 2002/58/EG vom 12. Juli 2002.

17 KOM(2012) 11.

18 KOM(2006) 786, http://eur-lex.europa.eu/LexUriServ/site/de/com/2006/com2006_0786de01.pdf.

19 KOM(2010) 517, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:DE:PDF.

20 KOM(2012) 140, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:DE:PDF.

21 http://europa.eu/rapid/press-release_MEMO-10-597_en.htm.

auch in anderen einschlägigen multilateralen Gremien aktiv tätig, z. B. der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD), der Generalversammlung der Vereinten Nationen (UNGA), der Internationalen Fernmeldeunion (ITU), der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE), dem Weltgipfel über die Informationsgesellschaft (WSIS) und dem Internet-Verwaltungs-Forum (IGF).

2. ERGEBNISSE DER KONSULTATIONEN DER INTERESSIERTEN KREISE UND DER FOLGENABSCHÄTZUNGEN

2.1. Anhörung interessierter Kreise und Nutzung von Sachverstand

Eine öffentliche Online-Konsultation zur „Verbesserung der NIS in der EU“ wurde vom 23. Juli bis zum 15. Oktober 2012 durchgeführt. Die Kommission erhielt 160 Antworten auf den Online-Fragebogen.

Als wichtigstes Ergebnis ist festzuhalten, dass die Interessenträger ihre allgemeine Unterstützung für eine notwendige Verbesserung der Netz- und Informationssicherheit in der EU bekundet haben. Im Einzelnen äußerten 82,8 % der Konsultationsteilnehmer die Ansicht, dass die Regierungen in der EU mehr tun sollten, um eine hohe Netz- und Informationssicherheit zu gewährleisten, 82,8 % waren der Meinung, dass den Benutzern von Informationen und Systemen die bestehenden NIS-Bedrohungen und NIS-Vorfälle nicht bewusst sind, 66,3 % würden grundsätzlich die Einführung von rechtlichen Vorgaben für ein Management der NIS-Risiken befürworten und 84,8 % meinten, dass solche Anforderungen auf EU-Ebene festgesetzt werden sollten. Eine hohe Zahl der Antwortenden meinte, dass die Einführung von NIS-Anforderungen besonders in den folgenden Sektoren wichtig wäre: Banken und Finanzen (91,1 %), Energie (89,4 %), Verkehr (81,7 %), Gesundheit (89,4 %), Internetdienste (89,1 %) und öffentliche Verwaltungen (87,5 %). Ferner meinten die Konsultationsteilnehmer, dass im Fall der Einführung einer Pflicht zur Meldung von NIS-Sicherheitsverletzungen bei der zuständigen nationalen Behörde eine solche Vorgabe auf EU-Ebene festgelegt werden sollte (65,1 %), und dass eine solche Pflicht auch für öffentliche Verwaltungen gelten sollte (93,5 %). Schließlich erklärten die Teilnehmer, dass eine Anforderung zur Einführung eines NIS-Risikomanagements entsprechend dem Stand der Technik für sie keine erheblichen Mehrkosten verursachen würde (63,4 %) und dass eine Meldepflicht für Sicherheitsverletzungen ebenfalls keine erheblichen Mehrkosten verursachen würde (72,3 %).

Die Konsultation der Mitgliedstaaten erfolgte in mehreren einschlägigen Ratsformationen, im Rahmen des Europäischen Forums der Mitgliedstaaten (EFMS), auf der von der Kommission und dem Europäischen Auswärtigen Dienst organisierten Konferenz zum Thema Cybersicherheit am 6. Juli 2012 wie auch und in besonderen bilateralen Treffen, die auf Wunsch einzelner Mitgliedstaaten stattfanden.

Gespräche mit dem Privatsektor wurden auch im Rahmen der Europäischen öffentlich-privaten Partnerschaft für Robustheit (EP3R)[22] und auf bilateralen Treffen geführt. Im Hinblick auf den öffentlichen Sektor führte die Kommission Gespräche mit der ENISA und dem CERT für die EU-Organe.

2.2. Folgenabschätzung

Die Kommission führte eine Folgenabschätzung für drei Politikoptionen durch:

Option 1: „Business as usual“ (Ausgangsszenario): Beibehaltung des derzeitigen Ansatzes;

[22] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r.

Option 2: ein Regulierungsansatz, bestehend aus einem Legislativvorschlag zur Schaffung eines gemeinsamen EU-Rechtsrahmens für die NIS im Hinblick auf die Kapazitäten der Mitgliedstaaten, Mechanismen für die Zusammenarbeit auf EU-Ebene und Anforderungen an wichtige private Akteure und öffentliche Verwaltungen;

Option 3: ein gemischter Ansatz, der freiwillige Initiativen in Bezug auf die NIS-Kapazitäten der Mitgliedstaaten und Mechanismen für die Zusammenarbeit auf EU-Ebene mit Regulierungsvorgaben für wichtige private Akteure und öffentliche Verwaltungen verbindet.

Die Kommission kam zu dem Schluss, dass mit der Option 2 die größte positive Wirkung erzielt werden könnte, weil dadurch der Schutz der Verbraucher, Unternehmen und Behörden in der EU vor NIS-Vorfällen beträchtlich erhöht würde. Insbesondere würde durch die für die Mitgliedstaaten geltenden Verpflichtungen eine angemessene Abwehrbereitschaft auf nationaler Ebene sichergestellt; dies würde ein Klima gegenseitigen Vertrauens schaffen, das eine Voraussetzung für eine wirksame Zusammenarbeit auf EU-Ebene ist. Die Einrichtung von Mechanismen für eine Zusammenarbeit auf EU-Ebene über das genannte Netz würde eine kohärente und koordinierte Prävention und Reaktion auf grenzübergreifende NIS-Vorfälle und -Risiken ermöglichen. Mit der Einführung verbindlicher NIS-Risikomanagement-Anforderungen für öffentliche Verwaltungen und wichtige private Wirtschaftsteilnehmer würde ein starker Anreiz geschaffen, Sicherheitsrisiken wirksam zu managen. Die Meldepflicht für NIS-Vorfälle mit beträchtlichen Auswirkungen würde eine bessere Reaktion auf Sicherheitsvorfälle ermöglichen und die Transparenz erhöhen. Die Bewältigung der internen Herausforderungen würde sich ferner positiv auf die internationale Ausstrahlung der EU auswirken, so dass sie zu einem noch glaubwürdigeren Partner für die Zusammenarbeit auf bilateraler und multilateraler Ebene würde. Auch wäre sie so in einer besseren Position, um die Grundrechte und die Grundwerte der EU jenseits ihrer Grenzen zu fördern.

Die quantitative Bewertung ergab, dass durch die Option 2 den Mitgliedstaaten keine unverhältnismäßig großen Belastungen auferlegt werden. Die Kosten für den Privatsektor wären ebenfalls begrenzt, denn viele der betroffenen Stellen müssen ohnehin bereits bestehende Sicherheitsanforderungen erfüllen (so sind die für die Datenverarbeitung Verantwortlichen verpflichtet, technische und organisatorische Vorkehrungen zum Schutz personenbezogener Daten zu treffen, was auch NIS-Vorkehrungen einschließt). Die bereits bestehenden Sicherheitsausgaben im Privatsektor wurden ebenfalls berücksichtigt.

Dieser Vorschlag steht im Einklang mit den in der Charta der Grundrechte der Europäischen Union anerkannten Grundsätzen, d. h. dem Recht auf Achtung des Privatlebens und der Kommunikation, dem Schutz personenbezogener Daten, der unternehmerischen Freiheit, dem Eigentumsrecht, dem Recht auf einen wirksamen Rechtsbehelf und dem Recht auf Anhörung. Diese Richtlinie ist im Einklang mit diesen Rechten und Grundsätzen umzusetzen.

3. RECHTLICHE ASPEKTE DES VORSCHLAGS

3.1. Rechtsgrundlage

Im Einklang mit den einschlägigen Bestimmungen der Verträge (Artikel 26 des Vertrags über die Arbeitsweise der Europäischen Union, AEUV) kann die Europäische Union Maßnahmen ergreifen, um den Binnenmarkt zu verwirklichen bzw. dessen Funktionieren zu gewährleisten. Laut Artikel 114 AEUV kann die EU „Maßnahmen zur *Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten*, welche die Errichtung und das Funktionieren des Binnenmarktes zum Gegenstand haben“ erlassen.

Wie bereits erwähnt kommt Netzen und Informationssystemen bei der Erleichterung des grenzüberschreitenden Waren-, Dienstleistungs- und Personenverkehrs eine wesentliche Rolle zu. Häufig sind sie auch miteinander verbunden, und das Internet ist seinem Wesen nach ohnehin ein globales Netz. Wegen dieser transnationalen Dimension kann eine Störung in einem Mitgliedstaat auch andere Mitgliedstaaten und die EU insgesamt in Mitleidenschaft ziehen. Die Robustheit und Stabilität der Netze und Informationssysteme ist daher eine Voraussetzung für das reibungslose Funktionieren des Binnenmarkts.

Der EU-Gesetzgeber hat bereits anerkannt, dass es im Hinblick auf die Entwicklung des Binnenmarkts notwendig ist, die NIS-Vorschriften zu harmonisieren. Dies gilt insbesondere für die Verordnung (EG) Nr. 460/2004 zur Errichtung der ENISA[23], die auf Artikel 114 AEUV beruht.

Die großen Unterschiede zwischen den Mitgliedstaaten, die sich aus ungleichen nationalen Kapazitäten, Strategien und Schutzniveaus im Bereich der NIS ergeben, führen zu Hindernissen im Binnenmarkt und rechtfertigen daher ein Tätigwerden der EU.

3.2. Subsidiarität

Ein Handeln der EU im Bereich der Netz- und Informationssicherheit ist nach dem Subsidiaritätsprinzip gerechtfertigt.

Erstens würde aufgrund der grenzüberschreitenden Natur der NIS ein Nichthandeln auf EU-Ebene zu einer Situation führen, in der jeder Mitgliedstaat allein handelt, ohne die gegenseitigen Abhängigkeiten zwischen Netzen und Informationssystemen in der EU zu beachten. Eine angemessene Koordinierung zwischen den Mitgliedstaaten würde ein gutes Management der NIS-Risiken im grenzübergreifenden Umfeld, in dem sie auftreten, ermöglichen. Abweichende NIS-Vorgaben sind ein Hindernis für Unternehmen, die in mehreren Ländern tätig werden wollen, und verhindern die Erzielung globaler Größenvorteile.

Zweitens werden rechtliche Verpflichtungen auf EU-Ebene benötigt, um gleiche Wettbewerbsbedingungen zu schaffen und Gesetzeslücken zu schließen. Ein rein freiwilliges Vorgehen hat bislang zu einer Zusammenarbeit nur zwischen jenen wenigen Mitgliedstaaten geführt, die ohnehin bereits über hohe Kapazitäten verfügen. Um aber alle Mitgliedstaaten einzubeziehen, muss sichergestellt werden, dass sie alle über die erforderlichen Mindestkapazitäten verfügen. Die von den Regierungen beschlossenen NIS-Maßnahmen müssen so aufeinander abgestimmt und koordiniert werden, dass sie die Folgen von NIS-Vorfällen eindämmen und minimieren können. Die zuständigen Behörden und die Kommission werden innerhalb des Netzes, durch Austausch bewährter Verfahren und unter ständiger Einbindung der ENISA zusammenarbeiten, um eine abgestimmte Umsetzung und Anwendung der Richtlinie in der gesamten EU zu erleichtern. Zudem kann sich eine abgestimmte NIS-Politik äußerst positiv auf den wirksamen Schutz der Grundrechte auswirken, insbesondere des Rechts auf Schutz personenbezogener Daten und der Privatsphäre. Maßnahmen auf EU-Ebene würden deshalb die Wirksamkeit bestehender nationaler Strategien erhöhen und die Entwicklung solcher Strategien erleichtern.

Die vorgeschlagenen Maßnahmen sind auch nach dem Grundsatz der Verhältnismäßigkeit gerechtfertigt. Die von den Mitgliedstaaten zu erfüllenden Anforderungen werden auf dem Mindestniveau festgesetzt, das erforderlich ist, um eine ausreichende Abwehrbereitschaft zu erzielen und eine vertrauensvolle Zusammenarbeit zu ermöglichen. Dadurch sind auch die

[23] 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).

Mitgliedstaaten in der Lage, nationale Besonderheiten hinreichend zu berücksichtigen, und es ist gewährleistet, dass die gemeinsamen EU-Grundsätze in verhältnismäßiger Weise angewandt werden. Der weite Anwendungsbereich erlaubt es den Mitgliedstaaten, die Richtlinie im Hinblick auf die tatsächlich auf nationaler Ebene bestehenden Risiken umzusetzen, wie in der nationalen NIS-Strategie angegeben. Die Vorgaben bezüglich der Einführung eines Risikomanagements betreffen nur kritische Einrichtungen und sehen nur Maßnahmen vor, die angesichts der Risiken angemessen sind. Die öffentliche Konsultation hat verdeutlicht, wie wichtig die Gewährleistung der Sicherheit dieser kritischen Einrichtungen ist. Die Meldepflichten würden nur für Sicherheitsvorfälle mit beträchtlichen Auswirkungen gelten. Die Maßnahmen würden – wie bereits erwähnt – keine unverhältnismäßigen Kosten verursachen, denn bei vielen dieser Einrichtungen handelt es sich um für die Datenverarbeitung Verantwortliche, die nach geltendem Datenschutzrecht ohnehin den Schutz personenbezogener Daten gewährleisten müssen.

Damit keine unverhältnismäßige Belastung für kleine Betreiber und insbesondere für KMU entsteht, sollten die Anforderungen in einem angemessenen Verhältnis zu den Risiken stehen, denen das betreffende Netz oder Informationssystem ausgesetzt ist, und nicht für Kleinstunternehmen gelten. Die Feststellung der Risiken ist in erster Linie Sache der Stellen, die diesen Verpflichtungen unterliegen und auch entscheiden müssen, welche Maßnahmen zur Minderung der Risiken zu ergreifen sind.

Angesichts der grenzübergreifenden Aspekte der NIS-Vorfälle und NIS-Risiken können die genannten Ziele besser auf EU-Ebene als durch die Mitgliedstaaten allein erreicht werden. Die EU kann deshalb im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union niedergelegten Subsidiaritätsprinzip tätig werden. Entsprechend dem Grundsatz der Verhältnismäßigkeit geht die vorgeschlagene Richtlinie nicht über das zum Erreichen dieses Ziels erforderliche Maß hinaus.

Im Hinblick auf die Erreichung der Ziele sollte der Kommission die Befugnis übertragen werden, delegierte Rechtsakte gemäß Artikel 290 des Vertrags über die Arbeitsweise der Europäischen Union zur Ergänzung oder Änderung bestimmter nicht wesentlicher Bestimmungen des zugrundeliegenden Rechtsakts zu erlassen. Der Vorschlag der Kommission soll auch einen Prozess der Verhältnismäßigkeit bei der Umsetzung und Anwendung der den privaten und öffentlichen Akteuren auferlegten Verpflichtungen fördern.

Im Hinblick auf die Gewährleistung einheitlicher Bedingungen für die Durchführung des zugrundeliegenden Rechtsakts sollte der Kommission die Befugnis übertragen werden, delegierte Rechtsakte gemäß Artikel 291 des Vertrags über die Arbeitsweise der Europäischen Union zu erlassen.

Insbesondere angesichts des weiten Anwendungsbereichs der vorgeschlagenen Richtlinie, des vorgesehenen Eingriffs in stark regulierte Bereiche und der aus ihrem Kapitel IV erwachsenden Rechtspflichten sollte die Mitteilung der Umsetzungsmaßnahmen durch erläuternde Dokumente ergänzt werden. Gemäß der Gemeinsamen Politischen Erklärung der Mitgliedstaaten und der Kommission vom 28. September 2011 zu erläuternden Dokumenten haben sich die Mitgliedstaaten verpflichtet, in begründeten Fällen zusätzlich zur Mitteilung ihrer Umsetzungsmaßnahmen ein oder mehrere Dokumente zu übermitteln, in dem bzw. denen der Zusammenhang zwischen den Bestandteilen einer Richtlinie und den entsprechenden Teilen innerstaatlicher Umsetzungsinstrumente erläutert wird. In Bezug auf diese Richtlinie hält der Gesetzgeber die Übermittlung derartiger Dokumente für gerechtfertigt.

4. AUSWIRKUNGEN AUF DEN HAUSHALT

Die Zusammenarbeit und der Informationsaustausch zwischen den Mitgliedstaaten sollten über eine sichere Infrastruktur erfolgen. Der Vorschlag wird sich nur dann auf den EU-Haushalt auswirken, wenn die Mitgliedstaaten beschließen, eine bestehende Infrastruktur (z. B. sTESTA) anzupassen, und die Kommission innerhalb des MFF 2014–2020 mit der Durchführung beauftragen. Die einmaligen Anpassungskosten werden mit 1 250 000 EUR veranschlagt und würden zulasten des EU-Haushalts, Haushaltslinie 09 03 02 (für die Förderung des Zusammenschlusses und der Interoperabilität nationaler öffentlicher Dienstleistungen online sowie Zugang zu solchen Netzen – Kapitel 09 03, Fazilität „Connecting Europe“ – Telekommunikationsnetze) gehen, unter der Voraussetzung, dass im Rahmen der Fazilität „Connecting Europe“ ausreichende Mittel zur Verfügung stehen. Alternativ hierzu können die Mitgliedstaaten auch entweder die einmaligen Kosten der Anpassung einer bestehenden Infrastruktur gemeinsam übernehmen oder aber auf ihre Kosten die Einrichtung einer neuen Infrastruktur beschließen, deren Kosten auf ungefähr 10 Millionen EUR pro Jahr geschätzt werden.

2013/0027 (COD)

Vorschlag für eine

RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION –

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

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

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

nach Anhörung des Europäischen Datenschutzbeauftragten,

gemäß dem ordentlichen Gesetzgebungsverfahren,

in Erwägung nachstehender Gründe:

(1) Netze und Informationssysteme mit den zugehörigen Diensten spielen eine zentrale Rolle in der Gesellschaft. Für die Wirtschaft und das Gemeinwohl und insbesondere für das Funktionieren des Binnenmarkts ist es von entscheidender Bedeutung, dass sie verlässlich und sicher sind.

(2) Die Tragweite und Häufigkeit vorsätzlicher wie unbeabsichtigter Sicherheitsvorfälle nehmen zu und stellen eine erhebliche Bedrohung für den störungsfreien Betrieb von Netzen und Informationssystemen dar. Solche Sicherheitsvorfälle können die Ausübung wirtschaftlicher Tätigkeiten beeinträchtigen, finanzielle Verluste verursachen, das Vertrauen der Nutzer untergraben und der Wirtschaft der Union großen Schaden zufügen.

(3) Digitale Informationssysteme, allen voran das Internet, spielen als Kommunikationsmittel, das keine Landesgrenzen kennt, eine tragende Rolle bei der Erleichterung des grenzüberschreitenden Waren-, Dienstleistungs- und Personenverkehrs. Aufgrund dieses transnationalen Charakters kann eine schwere Störung solcher Systeme in einem Mitgliedstaat auch andere Mitgliedstaaten und die EU insgesamt in Mitleidenschaft ziehen. Robuste, stabile Netze und Informationssysteme sind daher unerlässlich für das reibungslose Funktionieren des Binnenmarkts.

(4) Auf Unionsebene sollte ein Kooperationsmechanismus eingerichtet werden, der den Informationsaustausch sowie eine koordinierte Erkennungs- und Reaktionsfähigkeit im Bereich der Netz- und Informationssicherheit (im Folgenden „NIS“) ermöglicht. Damit ein solcher Mechanismus wirksam sein kann und alle Beteiligten einbezogen werden, muss jeder Mitgliedstaat über Mindestkapazitäten und eine Strategie verfügen, die in seinem Hoheitsgebiet eine hohe NIS gewährleisten. Zur Förderung

[1] ABl. C […], […], S. […].

einer Risikomanagementkultur und um sicherzustellen, dass die gravierendsten Sicherheitsvorfälle gemeldet werden, sollten Mindestsicherheitsanforderungen auch für öffentliche Verwaltungen und Betreiber kritischer Informationsinfrastrukturen gelten.

(5) Um alle einschlägigen Sicherheitsvorfälle und -risiken abdecken zu können, sollte diese Richtlinie für alle Netze und Informationssysteme gelten. Die den öffentlichen Verwaltungen und den Marktteilnehmern auferlegten Verpflichtungen sollten hingegen nicht für Unternehmen gelten, die öffentliche Kommunikationsnetze oder öffentlich zugängliche elektronische Kommunikationsdienste im Sinne der Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie)[2] bereitstellen und die den besonderen Sicherheits- und Integritätsanforderungen des Artikels 13a der Richtlinie unterliegen; die Verpflichtungen sollten auch nicht für Vertrauensdiensteanbieter gelten.

(6) Die bestehenden Kapazitäten reichen nicht aus, um eine hohe NIS in der EU zu gewährleisten. Aufgrund des sehr unterschiedlichen Niveaus der Abwehrbereitschaft verfolgen die Mitgliedstaaten uneinheitliche Ansätze innerhalb der Union. Dies führt dazu, dass Verbraucher und Unternehmen ein unterschiedliches Schutzniveau genießen und die NIS in der Union generell untergraben wird. Wegen fehlender gemeinsamer Mindestanforderungen für öffentliche Verwaltungen und Marktteilnehmer kann wiederum kein umfassender, wirksamer Mechanismus für die Zusammenarbeit auf Unionsebene geschaffen werden.

(7) Um wirksam auf die Herausforderungen im Bereich der Sicherheit von Netzen und Informationssystemen reagieren zu können, ist deshalb ein umfassender Ansatz auf Unionsebene erforderlich, der gemeinsame Mindestanforderungen für Kapazitätsaufbau und -planung, Informationsaustausch, Maßnahmenkoordinierung sowie gemeinsame Mindestsicherheitsanforderungen für alle betroffenen Marktteilnehmer und öffentlichen Verwaltungen beinhaltet.

(8) Die Möglichkeit der Mitgliedstaaten, die für die Wahrung ihrer wesentlichen Sicherheitsinteressen und den Schutz der öffentlichen Ordnung und der öffentlichen Sicherheit erforderlichen Maßnahmen zu ergreifen und die Ermittlung, Feststellung und Verfolgung von Straftaten zuzulassen, bleibt von den Bestimmungen dieser Richtlinie unberührt. Nach Artikel 346 AEUV ist kein Mitgliedstaat verpflichtet, Auskünfte zu erteilen, deren Preisgabe seines Erachtens seinen wesentlichen Sicherheitsinteressen widerspricht.

(9) Um eine hohe gemeinsame Netz- und Informationssicherheit zu erreichen und aufrechtzuerhalten sollte jeder Mitgliedstaat über eine nationale NIS-Strategie verfügen, in der die strategischen Ziele sowie konkrete politische Maßnahmen vorgesehen sind. Auf nationaler Ebene müssen NIS-Kooperationspläne aufgestellt werden, die gewisse Grundanforderungen erfüllen, so dass ein Kapazitätsniveau erreicht werden kann, das bei Sicherheitsvorfällen eine wirksame und effiziente Zusammenarbeit auf nationaler und auf Unionsebene ermöglicht.

(10) Zur effektiven Umsetzung der Bestimmungen dieser Richtlinie sollte in jedem Mitgliedstaat eine für die Koordinierung in Sachen NIS zuständige Stelle geschaffen oder auf Unionsebene benannt werden, die für die Zwecke der grenzübergreifenden Zusammenarbeit als Anlaufstelle dient. Diese Stellen sollten mit angemessenen

[2] ABl. L 108 vom 24.4.2002, S. 33.

technischen, finanziellen und personellen Ressourcen ausgestattet sein, um die ihnen übertragenen Aufgaben wirksam und effizient erfüllen und somit die Ziele dieser Richtlinie erreichen zu können.

(11) Alle Mitgliedstaaten sollten über angemessene technische und organisatorische Kapazitäten verfügen, um die Prävention, Erkennung, Reaktion und Folgenminderung bei NIS-Vorfällen und -Risiken gewährleisten zu können. Dafür sollten im Einklang mit den grundlegenden Anforderungen in allen Mitgliedstaaten gut funktionierende IT-Notfallteams (Computer Emergency Response Teams) eingerichtet werden, damit wirksame und geeignete Kapazitäten geschaffen werden, die in der Lage sind, Sicherheitsvorfälle und -risiken zu bewältigen und eine effiziente Zusammenarbeit auf Unionsebene zu gewährleisten.

(12) Auf der Grundlage der beträchtlichen Fortschritte, die im Rahmen des Europäischen Forums der Mitgliedstaaten (EFMS) zur Förderung von Gesprächen und des Austauschs bewährter Vorgehensweisen, u. a. zur Entwicklung von Grundsätzen für die europäische Zusammenarbeit bei Cyberkrisen, erzielt worden sind, sollten die Mitgliedstaaten und die Kommission ein Netz bilden, um eine kontinuierliche Kommunikation herzustellen und ihre Zusammenarbeit auszubauen. Dieser sichere und wirksame Kooperationsmechanismus sollte den Austausch von Informationen sowie die Erkennung und Bewältigung von Sicherheitsvorfällen in strukturierter, abgestimmter Weise auf Unionsebene ermöglichen.

(13) Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) sollte die Mitgliedstaaten und die Kommission mit Fachkompetenz, als Berater und als Mittler für den Austausch bewährter Verfahren unterstützen. Insbesondere sollte die Kommission die ENISA bei der Anwendung dieser Richtlinie zu Rate ziehen. Damit sichergestellt ist, dass die Mitgliedstaaten und die Kommission tatsächlich und rechtzeitig informiert werden, sollten Frühwarnungen vor Sicherheitsvorfällen und -risiken über das Kooperationsnetz ausgegeben werden. Um Kapazitäten und Fachwissen unter den Mitgliedstaaten aufbauen zu können, sollte das Kooperationsnetz auch als Mittel für den Austausch bewährter Verfahren dienen und damit seinen Mitgliedern beim Kapazitätsaufbau helfen sowie die Organisation von gegenseitigen Überprüfungen und NIS-Übungen leiten.

(14) Es sollte eine sichere Infrastruktur für den Informationsaustausch errichtet werden, damit sensible und vertrauliche Informationen über das Kooperationsnetz übermittelt werden können. Unbeschadet der Verpflichtung der Mitgliedstaaten, dem Kooperationsnetz Sicherheitsvorfälle und -risiken von unionsweiter Bedeutung zu melden, sollte der Zugang zu vertraulichen Informationen anderer Mitgliedstaaten nur gewährt werden, wenn diese nachweisen können, dass durch ihre technischen, finanziellen und personellen Ressourcen und Verfahren sowie ihre Kommunikationsinfrastruktur sichergestellt ist, dass sie in wirksamer, effizienter und sicherer Weise an der Arbeit des Netzes teilnehmen können.

(15) Da die meisten Netze und Informationssysteme privat betrieben werden, ist die Zusammenarbeit zwischen dem privaten und dem öffentlichen Sektor von zentraler Bedeutung. Die Marktteilnehmer sollten angehalten werden, sich eines eigenen informellen Kooperationsmechanismus zur Gewährleistung der NIS zu bedienen. Sie sollten ferner mit dem öffentlichen Sektor zusammenarbeiten und Informationen und bewährte Verfahren austauschen und im Gegenzug operative Unterstützung im Falle von Sicherheitsvorfällen erhalten.

(16) Um Transparenz zu gewährleisten und die Bürger und Marktteilnehmer der EU angemessen zu informieren, sollten die zuständigen Behörden eine gemeinsame Website zur Veröffentlichung nichtvertraulicher Informationen über Sicherheitsvorfälle und -risiken einrichten.

(17) Werden die betreffenden Informationen nach Vorschriften der EU und der Mitgliedstaaten über das Geschäftsgeheimnis als vertraulich eingestuft, ist deren Vertraulichkeit bei den in dieser Richtlinie vorgesehenen Tätigkeiten und bei der Erreichung der darin gesetzten Ziele sicherzustellen.

(18) Die Kommission und die Mitgliedstaaten sollten auf der Grundlage nationaler Erfahrungen im Krisenmanagement in Zusammenarbeit mit der ENISA einen NIS-Kooperationsplan der EU ausarbeiten, in dem Kooperationsmechanismen zur Bewältigung von Sicherheitsrisiken und -vorfällen festgelegt werden. Diesem Plan sollte bei Frühwarnungen über das Kooperationsnetz angemessen Rechnung getragen werden.

(19) Eine Verpflichtung zur Herausgabe einer Frühwarnung über das Netz sollte nur bestehen, wenn Tragweite und Schwere des Sicherheitsvorfalls oder betreffenden -risikos so erheblich sind oder werden können, dass ein Informationsaustausch oder eine Koordinierung der Reaktion auf EU-Ebene erforderlich ist. Frühwarnungen sollten deshalb auf diejenigen tatsächlichen oder potenziellen Sicherheitsvorfälle und -risiken beschränkt bleiben, die sich rasch ausweiten, nationale Reaktionskapazitäten überschreiten oder mehr als einen Mitgliedstaat betreffen. Um eine angemessene Bewertung zu ermöglichen, sollten dem Kooperationsnetz alle für die Beurteilung des Sicherheitsrisikos oder -vorfalls erheblichen Informationen mitgeteilt werden.

(20) Bei Eingang einer Frühwarnung und bei deren Bewertung sollten sich die zuständigen Behörden auf eine koordinierte Reaktion nach dem NIS-Kooperationsplan der EU einigen. Die zuständigen Behörden und die Kommission sollten über die im Zuge der koordinierten Reaktion auf nationaler Ebene ergriffenen Maßnahmen informiert werden.

(21) Angesichts des globalen Charakters von NIS-Problemen bedarf es einer engeren internationalen Zusammenarbeit, damit die Sicherheitsstandards und der Informationsaustausch verbessert werden können und ein gemeinsames globales Konzept für NIS-Fragen gefördert werden kann.

(22) Die Verantwortung für die Gewährleistung der NIS liegt in erheblichem Maße bei den öffentlichen Verwaltungen und den Marktteilnehmern. Durch geeignete Vorschriften und freiwillige Branchenpraxis sollte eine Risikomanagementkultur gefördert und entwickelt werden, die u. a. die Risikobewertung und die Anwendung von Sicherheitsmaßnahmen umfassen sollte, die den jeweiligen Risiken angemessen sind. Ferner ist es für ein ordnungsgemäßes Funktionieren des Kooperationsnetzes von großer Bedeutung, gleiche Ausgangsbedingungen zu schaffen, damit eine wirksame Zusammenarbeit aller Mitgliedstaaten sichergestellt ist.

(23) Die Richtlinie 2002/21/EG sieht vor, dass Unternehmen, die öffentliche Kommunikationsnetze oder öffentlich zugängliche elektronische Kommunikationsdienste bereitstellen, angemessene Maßnahmen zum Schutz der Integrität und Sicherheit dieser Netze ergreifen müssen, und enthält eine Meldepflicht im Falle von Sicherheitsverletzungen und Integritätsverlust. Nach der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in

der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)[3] müssen Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes geeignete technische und organisatorische Maßnahmen ergreifen, um die Sicherheit ihrer Dienste zu gewährleisten.

(24) Diese Verpflichtungen sollten über den elektronischen Kommunikationssektor hinaus ausgeweitet werden auf wichtige Anbieter von Diensten der Informationsgesellschaft im Sinne der Richtlinie 98/34/EG des europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft[4], auf die sich nachgelagerte Dienste der Informationsgesellschaft oder Online-Tätigkeiten wie Plattformen des elektronischen Geschäftsverkehrs, Internet-Zahlungs-Gateways, soziale Netze, Suchmaschinen, Cloud-Computing-Dienste und Application Stores stützen. Störungen dieser grundlegenden Dienste der Informationsgesellschaft verhindern die Erbringung anderer, darauf aufbauender Dienste der Informationsgesellschaft. Softwareentwickler und Hardwarehersteller sind keine Anbieter von Diensten der Informationsgesellschaft und sind deshalb ausgenommen. Die Verpflichtungen sollten auch auf öffentliche Verwaltungen und Betreiber kritischer Infrastrukturen ausgeweitet werden, die stark von der Informations- und Kommunikationstechnik abhängen und für die Aufrechterhaltung wichtiger wirtschaftlicher und gesellschaftlicher Bereiche (Strom- und Gasversorgung, Verkehr, Finanzinstitutionen, Börsen, Gesundheitswesen usw.) unerlässlich sind. Eine Störung dieser Netze und Informationssysteme würde den Binnenmarkt beeinträchtigen.

(25) Zu den von öffentlichen Verwaltungen und Marktteilnehmern zu ergreifenden technischen und organisatorischen Maßnahmen sollte nicht die Verpflichtung gehören, bestimmte geschäftliche Informationen und Produkte der Kommunikationstechnik in bestimmter Weise zu konzipieren, zu entwickeln oder herzustellen.

(26) Öffentliche Verwaltungen und Marktteilnehmer sollten die Sicherheit der ihnen unterstehenden Netze und Systeme gewährleisten. Dabei handelt es sich hauptsächlich um private Netze und Systeme, die entweder von internem IT-Personal verwaltet werden oder deren Sicherheit Dritten anvertraut wurde. Die Verpflichtung zur Gewährleistung der Sicherheit und die Meldepflicht sollten für die einschlägigen Marktteilnehmer und öffentlichen Verwaltungen unabhängig davon gelten, ob sie ihre Netze und Informationssysteme intern warten oder diese Aufgabe ausgliedern.

(27) Damit keine unverhältnismäßige finanzielle und administrative Belastung für kleine Betreiber und Nutzer entsteht, sollten die Verpflichtungen in einem angemessenen Verhältnis zu den Risiken stehen, denen das betreffende Netz oder Informationssystem ausgesetzt ist; dabei wird dem bei solchen Maßnahmen geltenden neuesten Stand Rechnung getragen. Diese Bestimmungen sollten nicht für Kleinstunternehmen gelten.

(28) Die zuständigen Behörden sollten dafür Sorge tragen, dass informelle, vertrauenswürdige Kanäle für den Informationsaustausch zwischen Marktteilnehmern sowie zwischen dem öffentlichen und dem privaten Sektor erhalten bleiben. Bei der Bekanntmachung von Sicherheitsvorfällen, die den zuständigen Behörden gemeldet werden, sollte das Interesse der Öffentlichkeit, über Bedrohungen informiert zu werden, sorgfältig gegen einen möglichen wirtschaftlichen Schaden bzw. einen Imageschaden abgewogen werden, der den öffentlichen Verwaltungen bzw. den

[3] ABl. L 201 vom 31.7.2002, S. 37.
[4] ABl. L 204 vom 21.7.1998, S. 37.

Marktteilnehmern, die solche Vorfälle melden, entstehen kann. Bei der Erfüllung der Meldepflichten sollten die zuständigen Behörden besonders darauf achten, dass Informationen über die Anfälligkeit von Produkten bis zur Veröffentlichung der entsprechenden Sicherheitsfixes streng vertraulich bleiben.

(29) Die zuständigen Behörden sollten mit den für die Erfüllung ihrer Aufgaben erforderlichen Mitteln ausgestattet sein; sie sollten auch befugt sein, hinreichende Auskünfte von Marktteilnehmern und öffentlichen Verwaltungen einzuholen, damit sie die Sicherheit von Netzen und Informationssystemen beurteilen können und über verlässliche, umfassende Daten über tatsächliche Sicherheitsvorfälle verfügen, die den Betrieb von Netzen und Informationssystemen beeinträchtigt haben.

(30) Häufig gehen Sicherheitsvorfälle auf kriminelle Handlungen zurück. Selbst wenn zunächst keine hinreichenden Beweise vorliegen, kann bei Sicherheitsvorfällen ein krimineller Hintergrund vermutet werden. In diesem Zusammenhang sollte eine sachgerechte Zusammenarbeit zwischen den zuständigen Behörden und den Strafverfolgungsbehörden Bestandteil einer wirksamen, umfassenden Reaktion auf die Bedrohung durch Sicherheitsvorfälle sein. Die Förderung einer sicheren, robusteren Umgebung setzt insbesondere voraus, dass die Strafverfolgungsbehörden systematisch über Sicherheitsvorfälle mit mutmaßlich kriminellem Hintergrund Bericht informiert werden. Ob es sich um Sicherheitsvorfälle aufgrund schwerer Straftaten handelt, sollte nach den EU-Vorschriften über Cyberkriminalität beurteilt werden.

(31) Häufig ist bei Sicherheitsvorfällen der Schutz personenbezogener Daten nicht mehr gewährleistet. Deshalb sollten die zuständigen Behörden und die Datenschutzbehörden zusammenarbeiten und Informationen zu allen einschlägigen Fragen austauschen, um derartigen Verletzungen des Schutzes personenbezogener Daten zu begegnen. Die Mitgliedstaaten sollten die Meldepflicht bei Sicherheitsvorfällen so umsetzen, dass der Verwaltungsaufwand bei Sicherheitsvorfällen, die gleichzeitig eine Verletzung des Schutzes personenbezogener Daten im Sinne der Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[5] darstellen, so gering wie möglich gehalten wird. Über Kontakte mit den zuständigen Behörden und den Datenschutzbehörden könnte die ENISA Unterstützung bieten, indem sie Mechanismen für den Informationsaustausch sowie Muster entwickelt, mit denen die Verwendung zweier verschiedener Muster für die Meldung von NIS-Vorfällen vermieden werden kann. Die Meldung anhand eines einzigen Musters wäre bei Sicherheitsvorfällen, bei denen der Schutz personenbezogener Daten beeinträchtigt wurde, eine Vereinfachung und würde damit den Verwaltungsaufwand für Unternehmen und öffentliche Verwaltungen verringern.

(32) Die Normung von Sicherheitsanforderungen ist ein vom Markt ausgehender Vorgang. Um die Sicherheitsstandards einander anzunähern, sollten die Mitgliedstaaten die Anwendung oder Einhaltung konkreter Normen fördern, damit ein hohes Sicherheitsniveau auf Unionsebene gewährleistet wird. Zu diesem Zweck könnte es erforderlich sein, harmonisierte Normen auszuarbeiten; dies sollte nach der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 zur europäischen Normung, zur Änderung der Richtlinien 89/686/EWG und 93/15/EWG des Rates sowie der Richtlinien 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG und 2009/105/EG des Europäischen Parlaments und des Rates und zur Aufhebung des Beschlusses

[5] SEK(2012) 72 endg.

87/95/EWG des Rates und des Beschlusses Nr. 1673/2006/EG des Europäischen Parlaments und des Rates[6] geschehen.

(33) Die Kommission sollte diese Richtlinie regelmäßig überprüfen, insbesondere um festzustellen, ob sie veränderten technischen oder Marktbedingungen anzupassen ist.

(34) Damit das Kooperationsnetz ungehindert arbeiten kann, sollte der Kommission nach Artikel 290 des Vertrags über die Arbeitsweise der Europäischen Union die Befugnis übertragen werden, Rechtsakte zur Festlegung der Kriterien, die ein Mitgliedstaat erfüllen muss, um zur Teilnahme am sicheren System für den Informationsaustausch zugelassen zu werden, sowie der weiteren Spezifikation für Auslöser von Frühwarnungen und der Festlegung der Umstände, in denen für Marktteilnehmer und öffentliche Verwaltungen die Meldepflicht gilt, zu erlassen.

(35) Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeiten angemessene Konsultationen – auch auf der Ebene von Sachverständigen – durchführt. Bei der Vorbereitung und Ausarbeitung delegierter Rechtsakte sollte die Kommission sicherstellen, dass die einschlägigen Dokumente dem Europäischen Parlament und dem Rat gleichzeitig, rechtzeitig und ordnungsgemäß übermittelt werden.

(36) Zur Gewährleistung einheitlicher Voraussetzungen für die Umsetzung dieser Richtlinie sollten der Kommission Durchführungsbefugnisse in Bezug auf die Zusammenarbeit zwischen den zuständigen Behörden und der Kommission im Rahmen des Kooperationsnetzes, den Zugang zur sicheren Infrastruktur für den Informationsaustausch, den NIS-Kooperationsplan, die Formen und Verfahren zur Information der Öffentlichkeit über Sicherheitsvorfälle und NIS-bezogene Normen und/oder technische Spezifikationen übertragen werden. Diese Befugnisse sollten nach der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren[7], ausgeübt werden.

(37) Bei der Anwendung dieser Richtlinie sollte die Kommission gegebenenfalls mit den einschlägigen Ausschüssen und Einrichtungen auf EU-Ebene, insbesondere denen der Bereiche Energie, Verkehr und Gesundheit, in Kontakt stehen.

(38) Informationen, die nach den Vorschriften der Union und der Mitgliedstaaten über das Geschäftsgeheimnis von einer zuständigen Behörde als vertraulich eingestuft werden, sollten mit der Kommission und anderen zuständigen Behörden nur ausgetauscht werden, wenn sich dies für die Zwecke dieser Richtlinie als unbedingt erforderlich erweist. Der Informationsaustausch sollte im Umfang so begrenzt bleiben, dass er im Hinblick auf das verfolgte Ziel relevant und angemessen ist.

(39) Der Austausch von Informationen über Sicherheitsrisiken und -vorfälle über das Kooperationsnetz und die Einhaltung der Verpflichtung zur Meldung von Sicherheitsvorfällen bei den zuständigen nationalen Behörden kann die Verarbeitung personenbezogener Daten erfordern. Diese Verarbeitung personenbezogener Daten ist notwendig, um die mit dieser Richtlinie verfolgten Ziele des öffentlichen Interesses zu erreichen, und somit nach Artikel 7 der Richtlinie 95/46/EG zulässig. Im Hinblick auf diesen legitimen Zweck ist sie weder unverhältnismäßig noch handelt es sich um einen nicht tragbaren Eingriff, der das in Artikel 8 der Charta der Grundrechte verbriefte

[6] ABl. L 316 vom 14.11.2012, S. 12.
[7] ABl. L 55 vom 28.2.2011, S. 13.

Recht auf den Schutz personenbezogener Daten in ihrem Wesensgehalt antastet. Bei der Anwendung dieser Richtlinie sollte die 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[8] entsprechend gelten. Die Datenverarbeitung durch die Organe und Einrichtungen der Union für die Zwecke dieser Richtlinie 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 erfolgen.

(40) Da das Ziel dieser Richtlinie, nämlich die Gewährleistung einer hohen Netz- und Informationssicherheit in der Union, auf der Ebene der Mitgliedstaaten allein nicht ausreichend verwirklicht werden kann und daher wegen der Wirkung der Maßnahme auf Unionsebene besser zu verwirklichen ist, kann die Union in Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union niedergelegten Subsidiaritätsprinzip Maßnahmen erlassen. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Richtlinie nicht über das zur Erreichung dieser Ziele erforderliche Maß hinaus.

(41) Diese Richtlinie steht mit den in der Charta der Grundrechte der Europäischen Union anerkannten Grundrechten und Grundsätzen, d. h. der Achtung des Privatlebens und der Kommunikation, der unternehmerischen Freiheit, dem Eigentumsrecht, dem Recht auf einen wirksamen Rechtsbehelf und dem Recht auf Anhörung im Einklang. Diese Richtlinie ist in Übereinstimmung mit diesen Rechten und Grundsätzen umzusetzen –

HABEN FOLGENDE RICHTLINIE ERLASSEN:

KAPITEL I

ALLGEMEINE BESTIMMUNGEN

Artikel 1

Gegenstand und Geltungsbereich

1) Mit dieser Richtlinie werden Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit (im Folgenden „NIS“) in der Union festgelegt.

2) Für diese Zwecke wird in der Richtlinie Folgendes festgelegt:

a) für alle Mitgliedstaaten geltende Verpflichtungen hinsichtlich der Prävention, des Umgangs und der Reaktion in Bezug auf Sicherheitsrisiken und -vorfälle, die Netze und Informationssysteme beeinträchtigen;

b) die Schaffung eines Kooperationsmechanismus zwischen den Mitgliedstaaten zur Gewährleistung einer einheitlichen Anwendung dieser Richtlinie in der Union, damit erforderlichenfalls in koordinierter, effizienter Weise mit Sicherheitsrisiken und -vorfällen, die Netze und Informationssysteme beeinträchtigen, umgegangen bzw. darauf reagiert werden kann;

c) die Festlegung von Sicherheitsvorschriften für Marktteilnehmer und öffentliche Verwaltungen.

[8] ABl. L 145 vom 31.5.2001, S. 43.

3) Die in Artikel 14 vorgesehenen Sicherheitsanforderungen gelten weder für Unternehmen, die öffentliche Kommunikationsnetze oder öffentlich zugängliche elektronische Kommunikationsdienste im Sinne der Richtlinie 2002/21/EG bereitstellen und die die besonderen Sicherheits- und Integritätsanforderungen der Artikel 13a und 13b der genannten Richtlinie erfüllen müssen, noch für Vertrauensdiensteanbieter.

4) Die EU-Vorschriften über Cyberkriminalität sowie die Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern[9] bleiben von dieser Richtlinie unberührt.

5) Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[10], die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und die Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[11] bleiben von dieser Richtlinie ebenfalls unberührt.

6) Der Austausch von Informationen über das Kooperationsnetz nach Kapitel III und die Meldung von NIS-Vorfällen nach Artikel 14 können die Verarbeitung von personenbezogenen Daten erforderlich machen. Eine solche Verarbeitung personenbezogener Daten, die notwendig ist, um die mit dieser Richtlinie verfolgten Ziele des öffentlichen Interesses zu erreichen, wird von den Mitgliedstaaten nach Artikel 7 der Richtlinie 95/46/EG und der Richtlinie 2002/58/EG in ihrer in einzelstaatliches Recht umgesetzten Form genehmigt.

Artikel 2

Mindestharmonisierung

Unbeschadet ihrer Verpflichtungen nach dem Unionsrecht werden die Mitgliedstaaten nicht daran gehindert, Bestimmungen zur Gewährleistung eines höheren Sicherheitsniveaus zu erlassen oder aufrechtzuerhalten.

Artikel 3

Begriffsbestimmungen

Im Sinne dieser Richtlinie bezeichnet der Ausdruck

1) „Netze und Informationssysteme“

a) elektronische Kommunikationsnetze im Sinne der Richtlinie 2002/21/EG,

b) Vorrichtungen oder Gruppen miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung von Computerdaten durchführen sowie

[9] ABl. L 345 vom 23.12.2008, S. 75.
[10] ABl. L 281 vom 23.11.1995, S. 31.
[11] SEK(2012) 72 endg.

c) Computerdaten, die von den in Buchstaben a und b genannten Elementen zum Zwecke des Betriebs, der Nutzung, des Schutzes und der Pflege gespeichert, verarbeitet, abgerufen oder übertragen werden;

2) „Sicherheit“ die Fähigkeit von Netzen und Informationssystemen, bei einem bestimmten Vertrauensniveau Störungen und böswillige Angriffe abzuwehren, die die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit gespeicherter oder übermittelter Daten oder entsprechender Dienste beeinträchtigen, die über dieses Netz und Informationssystem angeboten werden beziehungsweise zugänglich sind;

3) „Sicherheitsrisiko“ alle Umstände oder Ereignisse, die potenziell negative Auswirkungen auf die Sicherheit haben;

4) „Sicherheitsvorfälle“ alle Umstände oder Ereignisse, die tatsächlich negative Auswirkungen auf die Sicherheit haben;

5) „Dienst der Informationsgesellschaft“ einen Dienst im Sinne der Nummer 2 des Artikels 1 der Richtlinie 98/34/EG;

6) „NIS-Kooperationsplan“ einen Plan zur Einrichtung eines Rahmens für organisatorische Aufgaben, Zuständigkeiten und Verfahren, die der Aufrechterhaltung oder Wiederherstellung des Betriebs von Netzen und Informationssystemen dienen, die durch Sicherheitsrisiken oder -vorfällen beeinträchtigt wurden;

7) „Bewältigung von Sicherheitsvorfällen“ alle Verfahren zur Unterstützung der Analyse, Eindämmung und Reaktion im Falle von Sicherheitsvorfällen;

8) „Marktteilnehmer“

a) Anbieter von Diensten der Informationsgesellschaft, die die Bereitstellung anderer Dienste der Informationsgesellschaft ermöglichen; Anhang II enthält eine nicht erschöpfende Liste solcher Anbieter;

b) Betreiber kritischer Infrastrukturen, die für die Aufrechterhaltung zentraler wirtschaftlicher und gesellschaftlicher Tätigkeiten in den Bereichen Energie, Verkehr, Banken, Börsen und Gesundheit unerlässlich sind; Anhang II enthält eine nicht erschöpfende Liste dieser Betreiber;

9) „Norm“ eine Norm nach der Verordnung (EU) Nr. 1025/2012;

10) „Spezifikation“ eine Spezifikation nach der Verordnung (EU) Nr. 1025/2012;

11) „Vertrauensdiensteanbieter“ eine natürliche oder juristische Person, die elektronische Dienste bereitstellt, die die Erstellung, Überprüfung, Validierung, Handhabung und Bewahrung elektronischer Signaturen, elektronischer Siegel, elektronischer Zeitstempel, elektronischer Dokumente, elektronischer Zustelldienste, der Website-Authentifizierung und elektronischer Zertifikate einschließlich der Zertifikate für elektronische Signaturen und elektronische Siegel beinhalten.

KAPITEL II

NATIONALER RAHMEN FÜR DIE NETZ- UND INFORMATIONSSICHERHEIT

Artikel 4

Grundsatz

Die Mitgliedstaaten gewährleisten in Übereinstimmung mit dieser Richtlinie eine hohe Netz- und Informationssicherheit in ihren Hoheitsgebieten.

Artikel 5

Nationale NIS-Strategie und nationaler NIS-Kooperationsplan

1) Jeder Mitgliedstaat nimmt eine nationale NIS-Strategie an, die die strategischen Ziele und konkreten politischen und Regulierungsmaßnahmen enthält, mit denen eine hohe Netz- und Informationssicherheit erreicht und aufrechterhalten werden soll. Gegenstand der nationalen NIS-Strategie sind insbesondere die folgenden Aspekte:

a) die Festlegung der Ziele und Prioritäten der Strategie auf der Grundlage einer aktuellen Analyse der Sicherheitsrisiken und -vorfälle;

b) ein Steuerungsrahmen zur Erreichung der strategischen Ziele und Prioritäten, einschließlich einer klaren Festlegung der Aufgaben und Zuständigkeiten der staatlichen Stellen und der anderen einschlägigen Akteure;

c) die Bestimmung allgemeiner Maßnahmen zur Abwehrbereitschaft, Reaktion und Wiederherstellung mit Mechanismen für die Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor;

d) die Aufstellung von Ausbildungs-, Aufklärungs- und Schulungsprogrammen;

e) Forschungs- und Entwicklungspläne und eine Darlegung, wie diese Pläne die Prioritäten widerspiegeln.

2) Die nationale NIS-Strategie umfasst einen nationalen NIS-Kooperationsplan, der mindestens die folgenden Elemente enthält:

a) einen Risikobewertungsplan zur Bestimmung der Risiken und zur Bewertung der Auswirkungen potenzieller Sicherheitsvorfälle;

b) Festlegung der Aufgaben und Zuständigkeiten der verschiedenen an der Umsetzung des Plans Beteiligten;

c) die Festlegung von Kooperations- und Kommunikationsabläufen zur Gewährleistung der Prävention, Erkennung, Reaktion, Reparatur und Wiederherstellung, die je nach Alarmstufe angepasst werden;

d) einen Fahrplan für NIS-Übungen und -Schulungen zur Verbesserung, Validierung und Erprobung des Plans. Neue Erkenntnisse werden dokumentiert und bei Aktualisierungen in den Plan aufgenommen.

3) Die nationale NIS-Strategie und der nationale NIS-Kooperationsplan werden der Kommission innerhalb eines Monats nach ihrer Annahme mitgeteilt.

Artikel 6

Für die Netz- und Informationssicherheit zuständige nationale Behörde

1) Jeder Mitgliedstaat benennt eine für die Netz- und Informationssicherheit zuständige nationale Behörde (im Folgenden „zuständige Behörde“).

2) Die zuständigen Behörden überwachen die Anwendung dieser Richtlinie auf nationaler Ebene und tragen zu ihrer einheitlichen Anwendung in der Union bei.

3) Die Mitgliedstaaten gewährleisten, dass die zuständigen Behörden mit angemessenen technischen, finanziellen und personellen Ressourcen ausgestattet sind, damit sie die

ihnen übertragenen Aufgaben wirksam und effizient wahrnehmen und die Ziele dieser Richtlinie erreicht werden. Die Mitgliedstaaten stellen eine wirksame, effiziente und sichere Zusammenarbeit der zuständigen Behörden über das in Artikel 8 genannte Netz sicher.

4) Die Mitgliedstaaten gewährleisten, dass die zuständigen Behörden von öffentlichen Verwaltungen und Marktteilnehmern die Meldungen der Sicherheitsvorfälle nach Artikel 14 Absatz 2 erhalten und ihnen die in Artikel 15 genannten Durchführungs- und Durchsetzungsbefugnisse eingeräumt werden.

5) Die zuständigen Behörden konsultieren gegebenenfalls die einschlägigen nationalen Strafverfolgungs- und Datenschutzbehörden, und arbeiten mit ihnen zusammen.

6) Die Mitgliedstaaten teilen der Kommission unverzüglich die Benennung der zuständigen Behörde, deren Aufgaben sowie etwaige spätere Änderungen mit. Die Mitgliedstaaten machen die Benennung der zuständigen Behörde öffentlich bekannt.

Artikel 7

IT-Notfallteam

1) Jeder Mitgliedstaat richtet ein IT-Notfallteam (Computer Emergency Response Team, im Folgenden „CERT“) ein, das für die Bewältigung von Sicherheitsvorfällen und -risiken nach einem genau festgelegten Ablauf zuständig ist und die Voraussetzungen von Anhang I Nummer 1 erfüllt. Ein CERT kann innerhalb einer zuständigen Behörde eingerichtet werden.

2) Die Mitgliedstaaten gewährleisten, dass die CERTs technisch, finanziell und personell angemessen ausgestattet sind, um ihre in Anhang I Nummer 2 aufgeführten Aufgaben wirksam wahrnehmen zu können.

3) Die Mitgliedstaaten gewährleisten, dass sich die CERTs auf nationaler Ebene auf eine sichere, robuste Kommunikations- und Informationsinfrastruktur stützen, die mit dem in Artikel 9 genannten sicheren System für den Informationsaustausch kompatibel und interoperabel ist.

4) Die Mitgliedstaaten informieren die Kommission über die Ressourcen und den Auftrag der CERTs sowie über deren Verfahren zur Bewältigung von Sicherheitsvorfällen.

5) Das CERT untersteht der Aufsicht der zuständigen Behörde, die die Angemessenheit der ihm zur Verfügung gestellten Ressourcen, sein Mandat und die Wirksamkeit seines Verfahrens zur Bewältigung von Sicherheitsvorfällen regelmäßig überprüft.

KAPITEL III

ZUSAMMENARBEIT ZWISCHEN DEN ZUSTÄNDIGEN BEHÖRDEN

Artikel 8

Kooperationsnetz

1) Die zuständigen Behörden und die Kommission bilden ein Netz (im Folgenden „Kooperationsnetz“) für die Zusammenarbeit bei der Bewältigung von Sicherheitsrisiken und -vorfällen, die Netze und Informationssysteme betreffen.

2) Die Kommission und die zuständigen Behörden stehen über das Kooperationsnetz in ständigem Kontakt. Auf Anfrage kann die Europäische Agentur für Netz- und

Informationssicherheit (ENISA) das Kooperationsnetz mit Know-how und Beratung unterstützen.

3) Die zuständigen Behörden haben innerhalb des Netzes folgende Aufgaben:

a) Verbreitung von Frühwarnungen vor Sicherheitsrisiken und -vorfällen nach Artikel 10;

b) Gewährleistung einer koordinierten Reaktion nach Artikel 11;

c) regelmäßige Veröffentlichung nichtvertraulicher Informationen über laufende Frühwarnungen und koordinierte Reaktionen auf einer gemeinsamen Website;

d) auf Anfrage eines Mitgliedstaats oder der Kommission die gemeinsame Erörterung und Bewertung einer oder mehrerer der in Artikel 5 genannten nationalen NIS-Strategien und NIS-Kooperationspläne innerhalb des Geltungsbereichs der Richtlinie;

e) auf Anfrage eines Mitgliedstaats oder der Kommission die gemeinsame Erörterung und Bewertung der Wirksamkeit der CERTs, insbesondere bei der Durchführung von NIS-Übungen auf Unionsebene;

f) Zusammenarbeit und Informationsaustausch in Bezug auf alle einschlägigen Angelegenheiten mit dem bei Europol angesiedelten Europäischen Zentrum zur Bekämpfung der Cyberkriminalität und anderen einschlägigen europäischen Einrichtungen in den Bereichen Datenschutz, Energie, Verkehr, Banken, Börsen und Gesundheit;

g) Austausch von Informationen und bewährten Verfahren untereinander und mit der Kommission sowie gegenseitige Unterstützung beim Kapazitätsaufbau im Bereich der NIS;

h) Durchführung regelmäßiger gegenseitiger Überprüfungen der Kapazitäten und der Abwehrbereitschaft;

i) Durchführung von NIS-Übungen auf Unionsebene und gegebenenfalls Teilnahme an internationalen NIS-Übungen.

4) Die Kommission legt mittels Durchführungsrechtsakten die erforderlichen Modalitäten für eine Erleichterung der in den Absätzen 2 und 3 genannten Zusammenarbeit zwischen den zuständigen Behörden und der Kommission fest. Diese Durchführungsrechtsakte werden nach dem in Artikel 19 Absatz 2 genannten Konsultationsverfahren angenommen.

Artikel 9

Sicheres System für den Informationsaustausch

1) Der Austausch sensibler und vertraulicher Informationen über das Kooperationsnetz erfolgt über eine sichere Infrastruktur.

2) Die Kommission wird nach Artikel 18 ermächtigt, delegierte Rechtsakte zu erlassen, die die Festlegung von Kriterien im Hinblick auf nachstehende Aspekte betreffen, die ein Mitgliedstaat zu erfüllen hat, um für die Teilnahme am sicheren System für den Informationsaustausch zugelassen zu werden:

a) die Verfügbarkeit einer sicheren, robusten Kommunikations- und Informationsinfrastruktur auf nationaler Ebene, die mit der sicheren Infrastruktur des Kooperationsnetzes nach Artikel 7 Absatz 3 kompatibel und interoperabel ist;

b) die Verfügbarkeit adäquater technischer, finanzieller und personeller Ressourcen und Verfahren für die zuständigen Behörde und das CERT, durch die eine wirksame, effiziente

und sichere Teilnahme am sicheren System für den Informationsaustausch nach Artikel 6 Absatz 3, Artikel 7 Absatz 2 und Artikel 7 Absatz 3 ermöglicht wird.

3) Die Kommission erlässt nach den in den Absätzen 2 und 3 genannten Kriterien mittels Durchführungsrechtsakten Beschlüsse über den Zugang der Mitgliedstaaten zu dieser sicheren Infrastruktur. Diese Durchführungsrechtsakte werden nach dem in Artikel 19 Absatz 3 genannten Prüfverfahren erlassen.

Artikel 10

Frühwarnungen

1) Die zuständigen Behörden oder die Kommission geben im Kooperationsnetz Frühwarnungen zu solchen Sicherheitsrisiken und -vorfällen aus, die mindestens eine der folgenden Voraussetzungen erfüllen:

a) sie weiten sich rasch aus oder können sich rasch ausweiten;

b) sie übersteigen die nationale Reaktionskapazität oder können diese übersteigen;

c) sie betreffen oder können mehr als einen Mitgliedstaat betreffen.

2) Bei Frühwarnungen stellen die zuständigen Behörden und die Kommission alle in ihrem Besitz befindlichen relevanten Informationen zur Verfügung, die für die Beurteilung der Sicherheitsrisiken oder -vorfälle von Nutzen sein können.

3) Die Kommission kann auf Anfrage eines Mitgliedstaats oder von Amts wegen einen anderen Mitgliedstaat ersuchen, relevante Informationen zu einem bestimmten Sicherheitsrisiko oder -vorfall vorzulegen.

4) Hat das der Frühwarnung zugrundeliegende Sicherheitsrisiko bzw. der Sicherheitsvorfall einen mutmaßlich kriminellen Hintergrund, informieren die zuständigen Behörden oder die Kommission das bei Europol angesiedelte Europäische Zentrum zur Bekämpfung der Cyberkriminalität.

5) Die Kommission wird ermächtigt, delegierte Rechtsakte nach Artikel 18 zur Präzisierung der Sicherheitsrisiken und -vorfälle zu erlassen, die die in Absatz 1 genannten Frühwarnungen auslösen.

Artikel 11

Koordinierte Reaktion

1) Im Anschluss an eine Frühwarnung nach Artikel 10 einigen sich die zuständigen Behörden nach einer Bewertung der einschlägigen Informationen auf eine koordinierte Reaktion gemäß dem in Artikel 12 genannten NIS-Kooperationsplan der Union.

2) Die verschiedenen auf nationaler Ebene im Zuge der koordinierten Reaktion angenommenen Maßnahmen werden dem Kooperationsnetz mitgeteilt.

Artikel 12

NIS-Kooperationsplan der Union

1) Die Kommission wird ermächtigt, mittels Durchführungsrechtsakten einen NIS-Kooperationsplan der Union anzunehmen. Diese Durchführungsrechtsakte werden nach dem in Artikel 19 Absatz 3 genannten Prüfverfahren angenommen.

2) Der NIS-Kooperationsplan der Union sieht Folgendes vor:

a) für die Zwecke des Artikels 10:

- die Festlegung der Form und der Verfahren für die Einholung und den Austausch geeigneter und vergleichbarer Informationen über Sicherheitsrisiken und -vorfälle durch die zuständigen Behörden,
- die Festlegung der Verfahren und Kriterien zur Bewertung der Sicherheitsrisiken und -vorfälle durch das Kooperationsnetz.

b) die für die koordinierte Reaktion nach Artikel 11 einzuhaltenden Verfahren, einschließlich der Aufgaben und Zuständigkeiten und der Kooperationsverfahren;

c) einen Fahrplan für NIS-Übungen und -Schulungen zur Verbesserung, Validierung und Erprobung des Plans;

d) ein Programm für den Wissenstransfer zwischen den Mitgliedstaaten im Hinblick auf den Kapazitätsaufbau und das gegenseitige Lernen;

e) ein Programm zur Sensibilisierung und Schulung der Mitgliedstaaten untereinander.

3) Der NIS-Kooperationsplan wird spätestens ein Jahr nach dem Inkrafttreten dieser Richtlinie angenommen und regelmäßig überarbeitet.

Artikel 13

Internationale Zusammenarbeit

Unbeschadet der Möglichkeiten des Kooperationsnetzes, auf internationaler Ebene informell zusammenzuarbeiten, kann die Union internationale Vereinbarungen mit Drittländern oder internationalen Organisationen schließen, in denen deren Beteiligung an bestimmten Aktivitäten des Kooperationsnetzes ermöglicht und geregelt wird. In solchen Vereinbarungen wird der Notwendigkeit eines angemessenen Schutzes der im Kooperationsnetz zirkulierenden personenbezogenen Daten Rechnung getragen.

KAPITEL IV

SICHERHEIT DER NETZE UND INFORMATIONSSYSTEME DER ÖFFENTLICHEN VERWALTUNGEN UND DER MARKTTEILNEHMER

Artikel 14

Sicherheitsanforderungen und Meldung von Sicherheitsvorfällen

1) Die Mitgliedstaaten stellen sicher, dass öffentliche Verwaltungen und Marktteilnehmer geeignete technische und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netze und Informationssysteme, die ihnen unterstehen und die sie für ihre Tätigkeiten nutzen, zu managen. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik ein Maß an Sicherheit gewährleisten, das angesichts des bestehenden Risikos angemessen ist. Insbesondere müssen Maßnahmen ergriffen werden, um Folgen von Sicherheitsvorfällen, die ihre Netze und Informationssysteme betreffen, auf die von ihnen bereitgestellten Kerndienste zu verhindern beziehungsweise so gering wie möglich zu halten, damit die Kontinuität der Dienste, die auf diesen Netzen und Informationssystemen beruhen, gewährleistet wird.

2) Die Mitgliedstaaten gewährleisten, dass öffentliche Verwaltungen und Marktteilnehmer den zuständigen Behörden Sicherheitsvorfälle melden, die erhebliche Auswirkungen auf die Sicherheit der von ihnen bereitgestellten Kerndienste haben.

3) Die Anforderungen der Absätze 1 und 2 gelten für alle Marktteilnehmer, die Dienste in der Europäischen Union bereitstellen.

4) Die zuständige Behörde kann die Öffentlichkeit unterrichten oder die öffentliche Verwaltung und die Marktteilnehmer zur Unterrichtung verpflichten, wenn sie zu dem Schluss gelangt, dass die Bekanntmachung des Sicherheitsvorfalls im öffentlichen Interesse liegt. Die zuständige Behörde legt dem Kooperationsnetz jährlich einen zusammenfassenden Bericht über die eingegangenen Meldungen und die nach diesem Absatz ergriffenen Maßnahmen vor.

5) Die Kommission wird nach Artikel 18 ermächtigt, delegierte Rechtsakte zu erlassen, in denen festgelegt wird, unter welchen Umständen bei Sicherheitsvorfällen für öffentliche Verwaltungen und Marktteilnehmer die Meldepflicht gilt.

6) Vorbehaltlich etwaiger nach Absatz 5 erlassener delegierter Rechtsakte können die zuständigen Behörden Leitlinien annehmen und erforderlichenfalls Anweisungen zu den Umständen herausgeben, in denen für öffentliche Verwaltungen und Marktteilnehmer die Meldepflicht gilt.

7) Die Kommission wird ermächtigt, mittels Durchführungsrechtsakten die für die Zwecke des Absatzes 2 geltenden Formen und Verfahren festzulegen. Diese Durchführungsrechtsakte werden nach dem in Artikel 19 Absatz 3 genannten Prüfverfahren angenommen.

8) Die Absätze 1 und 2 gelten nicht für Kleinstunternehmen im Sinne der Definition der Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen[12].

Artikel 15

Umsetzung und Durchsetzung

1) Die Mitgliedstaaten gewährleisten, dass den zuständigen Behörden alle Befugnisse eingeräumt werden, die für die Untersuchung von Verstößen der öffentlichen Verwaltungen oder der Marktteilnehmer gegen die Verpflichtungen des Artikels 14 sowie deren Auswirkungen auf die Netz- und Informationssicherheit erforderlich sind.

2) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden befugt sind, von den Marktteilnehmern und den öffentlichen Verwaltungen zu verlangen, dass sie

a) die zur Beurteilung der Sicherheit ihrer Netze und Informationssysteme erforderlichen Informationen, einschließlich der Unterlagen über ihre Sicherheitsmaßnahmen, übermitteln;

b) sich einer Sicherheitsüberprüfung unterziehen, die von einer qualifizierten unabhängigen Stelle oder einer zuständigen nationalen Behörde durchgeführt wird, und deren Ergebnisse der zuständigen Behörde übermitteln.

[12] ABl. L 124 vom 20.5.2003, S. 36.

3) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden befugt sind, Marktteilnehmern und öffentlichen Verwaltungen verbindliche Anweisungen zu erteilen.

4) Die zuständigen Behörden melden den Strafverfolgungsbehörden Sicherheitsvorfälle, bei denen ein schwerwiegender krimineller Hintergrund vermutet wird.

5) Bei der Bearbeitung von Sicherheitsvorfällen, die zu Verletzungen des Schutzes personenbezogener Daten führen, arbeiten die zuständigen Behörden eng mit den Datenschutzbehörden zusammen.

6) Die Mitgliedstaaten gewährleisten, dass alle Verpflichtungen, die öffentlichen Verwaltungen oder Marktteilnehmern nach diesem Kapitel auferlegt werden, einer gerichtlichen Nachprüfung unterzogen werden können.

Artikel 16

Normung

1) Um eine einheitliche Umsetzung des Artikels 14 Absatz 1 zu gewährleisten, fördern die Mitgliedstaaten die Anwendung einschlägiger Normen und/oder Spezifikationen für die Netz- und Informationssicherheit.

2) Die Kommission stellt mittels Durchführungsrechtsakten eine Liste der in Absatz 1 genannten Normen auf. Diese Liste wird im *Amtsblatt der Europäischen Union* veröffentlicht.

KAPITEL V

SCHLUSSBESTIMMUNGEN

Artikel 17

Sanktionen

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

2) Die Mitgliedstaaten gewährleisten, dass die bei Sicherheitsvorfällen mit Folgen für den Schutz personenbezogener Daten vorgesehenen Sanktionen, mit den Sanktionen im Einklang stehen, die in der Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[13] vorgesehen sind.

Artikel 18

Ausübung der Befugnisübertragung

1) Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission nach Maßgabe dieses Artikels übertragen.

[13] SEK(2012) 72 endg.

2) Die in Artikel 9 Absatz 2, Artikel 10 Absatz 5 und Artikel 14 Absatz 5 genannte Befugnis zum Erlass delegierter Rechtsakte wird der Kommission übertragen. Die Kommission legt spätestens neun Monate vor Ablauf des Fünfjahreszeitraums einen Bericht über die übertragenen Befugnisse vor. Die Befugnisübertragung verlängert sich stillschweigend um Zeiträume gleicher Länge, es sei denn, das Europäische Parlament oder der Rat widerspricht einer solchen Verlängerung spätestens drei Monate vor Ablauf des jeweiligen Zeitraums.

3) Die in Artikel 9 Absatz 2, Artikel 10 Absatz 5 und Artikel 14 Absatz 5 genannte Befugnisübertragung kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* oder zu einem darin angegebenen späteren Zeitpunkt wirksam. Er berührt nicht die Gültigkeit der bereits in Kraft getretenen delegierten Rechtsakte.

4) Sobald die Kommission einen delegierten Rechtsakt erlassen hat, übermittelt sie ihn gleichzeitig dem Europäischen Parlament und dem Rat.

5) Ein delegierter Rechtsakt, der nach Artikel 9 Absatz 2, Artikel 10 Absatz 5 und Artikel 14 Absatz 5 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von zwei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben hat oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Diese Frist wird auf Initiative des Europäischen Parlaments oder des Rates um zwei Monate verlängert.

Artikel 19

Ausschussverfahren

1) Die Kommission wird von einem Ausschuss (Ausschuss für Netz- und Informationssicherheit) unterstützt. Bei diesem Ausschuss handelt es sich um einen Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.

2) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 4 der Verordnung (EU) Nr. 182/2011.

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

Artikel 20

Überprüfung

Die Kommission überprüft das Funktionieren dieser Richtlinie regelmäßig und erstattet dem Europäischen Parlament und dem Rat darüber Bericht. Der erste Bericht wird spätestens drei Jahre nach dem Datum der Umsetzung nach Artikel 21 vorgelegt. Für diese Zwecke kann die Kommission die Mitgliedstaaten ersuchen, ihr unverzüglich Auskünfte zu erteilen.

Artikel 21

Umsetzung

1) Die Mitgliedstaaten erlassen und veröffentlichen die erforderlichen Rechts- und Verwaltungsvorschriften spätestens [anderthalb Jahre nach deren Annahme], um dieser Richtlinie nachzukommen. Sie teilen der Kommission unverzüglich den Wortlaut dieser Vorschriften mit.

   Sie wenden diese Vorschriften [anderthalb Jahre nach ihrer Annahme] an.

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

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

Artikel 22

Inkrafttreten

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

Artikel 23

Adressaten

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.

Geschehen zu Brüssel am […]

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

ANHANG I

IT-Notfallteam (Computer Emergency Response Team, CERT) – Anforderungen und Aufgaben

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

1) Anforderungen an das CERT

a) Das CERT gewährleistet die hohe Verfügbarkeit seiner Kommunikationsdienste durch Vermeidung kritischer Ausfallverursacher und durch Bereitstellung verschiedener Kanäle, damit das CERT ständig erreichbar bleibt und selbst Kontakt aufnehmen kann. Die Kommunikationskanäle müssen genau spezifiziert sein und den CERT-Nutzern (Constituency) und Kooperationspartnern bekannt gegeben werden.

b) Das CERT ergreift und verwaltet Sicherheitsmaßnahmen, um die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der eingehenden und von ihm behandelten Informationen zu gewährleisten.

c) Die CERT-Dienststellen und die unterstützenden Informationssysteme werden an sicheren Standorten eingerichtet.

d) Es wird ein Managementsystem für die Dienstqualität eingerichtet, um die Arbeit des CERT nachzuverfolgen und eine kontinuierliche Verbesserung zu gewährleisten. Das System basiert auf genau definierten Metriken, die formale Dienstleistungsstufen und grundlegende Leistungsindikatoren umfassen.

e) Betriebskontinuität:

- Das CERT verfügt über ein geeignetes System zur Verwaltung und Weiterleitung von Anfragen, um Übergaben zu erleichtern.
- Das CERT ist personell so ausgestattet, dass es eine ständige Verfügbarkeit gewährleisten kann.
- Das CERT stützt sich auf eine Infrastruktur, deren Kontinuität sichergestellt ist. Zu diesem Zweck werden für die Arbeit des CERT Redundanzsysteme und Ausweicharbeitsräume geschaffen, damit der kontinuierliche Zugang zu den Kommunikationsmitteln gewährleistet ist.

2) Aufgaben des CERT

a) Die Aufgaben des CERT müssen mindestens Folgendes umfassen:

- Überwachung von Sicherheitsvorfällen auf nationaler Ebene;
- Ausgabe von Frühwarnungen, Alarmmeldungen sowie Bekanntmachung und Verbreitung von Informationen über Sicherheitsrisiken und -vorfälle unter den Betroffenen bzw. Beteiligten;
- Reaktion auf Sicherheitsvorfälle;
- dynamische Analyse von Sicherheitsrisiken und -vorfällen und Lagebeurteilung;
- Aufklärung der breiten Öffentlichkeit über die mit Online-Aktivitäten verbundenen Risiken;

– Durchführung von NIS-Kampagnen.

b) Das CERT unterhält zwecks Zusammenarbeit Verbindungen zum Privatsektor.

c) Zur Erleichterung der Zusammenarbeit fördert das CERT die Annahme und Anwendung gemeinsamer bzw. standardisierter Verfahren für:

– Abläufe zur Bewältigung von Sicherheitsvorfällen und -risiken;

– Systeme zur Klassifizierung von Sicherheitsvorfällen, Sicherheitsrisiken und Informationen;

– Klassifikationsschemata für Metriken;

– Formate für den Austausch von Informationen über Sicherheitsrisiken und -vorfälle sowie System-Namenskonventionen.

ANHANG II

Liste der Marktteilnehmer

nach Artikel 3 Absatz 8 Buchstabe a

1. Plattformen des elektronischen Geschäftsverkehrs

2. Internet-Zahlungs-Gateways

3. Soziale Netze

4. Suchmaschinen

5. Cloud-Computing-Dienste

6. Application Stores

nach Artikel 3 Absatz 8 Buchstabe b

1. Energie

- Strom- und Gasversorger
- Verteilernetzbetreiber und Endkundenlieferanten im Strom- und/oder Gassektor
- Erdgas-Fernleitungsnetzbetreiber, Erdgasspeicher- und LNG-Anlagenbetreiber
- Übertragungsnetzbetreiber (Strom)
- Erdöl-Fernleitungen und Erdöllager
- Strom- und Gasmarktteilnehmer
- Betreiber von Erdöl- und Erdgas-Produktions-, -Raffinations- und Behandlungsanlagen

2. Verkehr

- Luftfahrtunternehmen (Luftfrachtverkehr und Personenbeförderung)
- Beförderungsunternehmen des Seeverkehrs (Personen- und Güterbeförderung in der See- und Küstenschifffahrt)
- Eisenbahnen (Infrastrukturbetreiber, integrierte Unternehmen und Eisenbahnunternehmen)
- Flughäfen
- Häfen
- Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen
- Unterstützende Logistikdienste: a) Lagerhaltung und Lagerung b) Frachtumschlagsleistungen und c) andere unterstützende Verkehrsleistungen

3. Bankwesen: Kreditinstitute nach Artikel 4 Absatz 1 der Richtlinie 2006/48/EG.

4. Finanzmarktinfrastrukturen: Börsen und Clearingstellen mit zentraler Gegenpartei

5. Gesundheitswesen: Einrichtungen der medizinischen Versorgung (einschließlich Krankenhäusern und Privatkliniken) sowie andere Einrichtungen der Gesundheitsfürsorge

FINANZBOGEN ZU RECHTSAKTEN

1. RAHMEN DES VORSCHLAGS/DER INITIATIVE

1.1. Bezeichnung des Vorschlags/der Initiative

1.2. Politikbereich(e) in der ABM/ABB-Struktur

1.3. Art des Vorschlags/der Initiative

1.4. Ziele

1.5. Begründung des Vorschlags/der Initiative

1.6. Dauer der Maßnahme und ihrer finanziellen Auswirkungen

1.7. Vorgeschlagene Methode(n) der Mittelverwaltung

2. VERWALTUNGSMASSNAHMEN

2.1. Monitoring und Berichterstattung

2.2. Verwaltungs- und Kontrollsystem

2.3. Prävention von Betrug und Unregelmäßigkeiten

3. GESCHÄTZTE FINANZIELLE AUSWIRKUNGEN DES VORSCHLAGS/DER INITIATIVE

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

3.2. Geschätzte Auswirkungen auf die Ausgaben

3.2.1. Übersicht

3.2.2. Geschätzte Auswirkungen auf die operativen Mittel

3.2.3. Geschätzte Auswirkungen auf die Verwaltungsmittel

3.2.4. Vereinbarkeit mit dem mehrjährigen Finanzrahmen

3.2.5. Finanzierungsbeteiligung Dritter

3.3. Geschätzte Auswirkungen auf die Einnahmen

FINANZBOGEN ZU RECHTSAKTEN

1. RAHMEN DES VORSCHLAGS/DER INITIATIVE

1.1. Bezeichnung des Vorschlags/der Initiative

Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union.

1.2. Politikbereich(e) in der ABM/ABB-Struktur[37]

- 09 – Kommunikationsnetze, Inhalte und Technologien

1.3. Art des Vorschlags/der Initiative

☒ Der Vorschlag/die Initiative betrifft **eine neue Maßnahme**.

☐ Der Vorschlag/die Initiative betrifft **eine neue Maßnahme im Anschluss an ein Pilotprojekt/eine vorbereitende Maßnahme**[38].

☐ Der Vorschlag/die Initiative betrifft **die Verlängerung einer bestehenden Maßnahme**.

☐ Der Vorschlag/die Initiative betrifft eine **neu ausgerichtete Maßnahme**.

1.4. Ziele

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

Mit der vorgeschlagenen Richtlinie wird das Ziel verfolgt, in der gesamten EU ein hohes gemeinsames Niveau der Netz- und Informationssicherheit (NIS) zu gewährleisten.

1.4.2. Einzelziele und ABM/ABB-Tätigkeiten

Der Vorschlag dient der Ergreifung von Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union.

Die besonderen Ziele sind:

1. Einführung eines NIS-Mindestniveaus in den Mitgliedstaaten, um die Abwehrbereitschaft und Reaktionsfähigkeit insgesamt zu erhöhen.

2. Verbesserte Zusammenarbeit im Bereich NIS auf EU-Ebene, damit grenzübergreifende Sicherheitsvorfälle und Bedrohungen wirksam bewältigt werden können. Es wird eine sichere Infrastruktur für den Informationsaustausch eingerichtet, um den Austausch sensibler und vertraulicher Informationen zwischen den zuständigen Behörden zu ermöglichen.

3. Schaffung einer Risikomanagementkultur und Verbesserung des Informationsaustauschs zwischen dem privaten und dem öffentlichen Sektor.

---

[37] ABM: *Activity Based Management* (maßnahmenbezogenes Management) – ABB: *Activity Based Budgeting* (maßnahmenbezogene Budgetierung).

[38] Im Sinne des Artikels 49 Absatz 6 Buchstabe a oder b der Haushaltsordnung.

Betroffene ABM/ABB-Tätigkeiten

Unter die Richtlinie fallen Einrichtungen (Unternehmen und Organisationen, einschließlich KMU) in einer Reihe von Sektoren (Energie, Verkehr, Kreditinstitute und Börsen, Gesundheitswesen und Infrastrukturbetreiber für wichtige Internetdienste) sowie öffentliche Verwaltungen. Sie regelt die Verbindungen mit der Strafverfolgung und dem Datenschutz wie auch die NIS-Aspekte der Außenbeziehungen.

09 – Kommunikationsnetze, Inhalte und Technologien

02 – Unternehmen

32 – Energie

06 – Mobilität und Verkehr

17 – Gesundheit und Verbraucherschutz

18 – Inneres

19 – Außenbeziehungen

33 – Justiz

12 – Binnenmarkt

1.4.3. Erwartete Ergebnisse und Auswirkungen

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

Der Schutz der Verbraucher, Unternehmen und Behörden der EU vor NIS-Vorfällen, -Bedrohungen und -Risiken würde erheblich verbessert werden.

Weitere Einzelheiten enthält Abschnitt 8.2 (Auswirkungen der Option 2 – Regulierungsansatz) der dem vorliegenden Legislativvorschlag beigefügten Arbeitsunterlage der Kommissionsdienststellen mit der Folgenabschätzung.

1.4.4. Leistungs- und Erfolgsindikatoren

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

Die Indikatoren für das Monitoring und die Evaluierung werden in Abschnitt 10 der Folgenabschätzung erläutert.

1.5. Begründung des Vorschlags/der Initiative

1.5.1. Kurz- oder längerfristig zu deckender Bedarf

Jeder Mitgliedstaat müsste Folgendes haben:

– eine nationale NIS-Strategie,

– einen NIS-Kooperationsplan,

– eine für die NIS zuständige nationale Behörde und

– ein IT-Notfallteam (*Computer Emergency Response Team*, CERT).

Auf EU-Ebene wären die Mitgliedstaaten verpflichtet, in einem Netz zusammenzuarbeiten.

Öffentliche Verwaltungen und wichtige private Wirtschaftsteilnehmer wären verpflichtet, ein NIS-Risikomanagement durchzuführen und den zuständigen Behörden NIS-Vorfälle mit beträchtlichen Auswirkungen zu melden.

1.5.2. Mehrwert durch die Intervention der EU

Aufgrund der grenzüberschreitenden Natur der NIS sind abweichende NIS-Vorschriften und Vorgaben ein Hindernis für Unternehmen, die in mehreren Ländern tätig werden wollen, und verhindern die Erzielung globaler Größenvorteile. Ein Nichthandeln auf EU-Ebene würde zu einer Situation führen, in der jeder Mitgliedstaat allein handelt, ohne die gegenseitigen Abhängigkeiten zwischen Netzen und Informationssystemen in der EU zu beachten.

Die genannten Ziele können daher besser auf EU-Ebene als durch die Mitgliedstaaten allein erreicht werden.

1.5.3. Aus früheren ähnlichen Maßnahmen gewonnene wesentliche Erkenntnisse

Der Vorschlag stützt sich auf die Erkenntnis, dass rechtliche Verpflichtungen benötigt werden, um gleiche Wettbewerbsbedingungen zu schaffen und bestehende Gesetzeslücken zu schließen. Auf diesem Gebiet hat ein rein freiwilliges Vorgehen bislang zu einer Zusammenarbeit nur zwischen jenen wenigen Mitgliedstaaten geführt, die bereits über hohe Kapazitäten verfügen.

1.5.4. Kohärenz mit anderen Finanzierungsinstrumenten sowie mögliche Synergieeffekte

Der Vorschlag ist vollständig mit der Digitalen Agenda für Europa und daher auch mit der Strategie Europa 2020 vereinbar. Er steht auch im Einklang mit dem EU-Rechtsrahmen für die elektronische Kommunikation, der EU-Richtlinie über den Schutz europäischer kritischer Infrastrukturen und der EU-Datenschutzrichtlinie, die er ergänzt.

Der Vorschlag ist ein wesentlicher Teil der gemeinsamen Mitteilung der Kommission und der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik über eine europäische Cybersicherheitsstrategie, der er beigefügt ist.

1.6. Dauer der Maßnahme und ihrer finanziellen Auswirkungen

– ☐ Vorschlag/Initiative mit befristeter Geltungsdauer

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

– ☐ Finanzielle Auswirkungen: JJJJ bis JJJJ

– ☒ Vorschlag/Initiative mit unbefristeter Geltungsdauer

– Der Umsetzungszeitraum beginnt unmittelbar nach der Annahme (voraussichtlich 2015) und erstreckt sich über 18 Monate. Die Durchführung der Richtlinie beginnt aber mit der Annahme und umfasst den Aufbau der sicheren Infrastruktur als Voraussetzung für die Zusammenarbeit der Mitgliedstaaten.

– anschließend reguläre Anwendung.

1.7. Vorgeschlagene Methoden der Mittelverwaltung[39]

– ☒ Direkte zentrale Verwaltung durch die Kommission

[39] Erläuterungen zu den Methoden der Mittelverwaltung und Verweise auf die Haushaltsordnung enthält die Website BudgWeb (in französischer und englischer Sprache): http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html.

– ☒ Indirekte zentrale Verwaltung durch Übertragung von Haushaltsvollzugsaufgaben an:

– ☐ Exekutivagenturen

– ☒ von der Europäischen Union geschaffene Einrichtungen[40]

– ☐ nationale öffentliche Einrichtungen bzw. privatrechtliche Einrichtungen, die im öffentlichen Auftrag tätig werden

– ☐ Personen, die mit der Durchführung bestimmter Maßnahmen im Rahmen des Titels V des Vertrags über die Europäische Union betraut und in dem maßgeblichen Basisrechtsakt nach Artikel 49 der Haushaltsordnung bezeichnet sind

– ☐ Geteilte Verwaltung mit Mitgliedstaaten

– ☐ Dezentrale Verwaltung mit Drittländern

– ☐ Gemeinsame Verwaltung mit internationalen Organisationen, u. a. der Europäischen Weltraumorganisation

Falls mehrere Methoden der Mittelverwaltung zum Einsatz kommen, ist dies unter „Bemerkungen" näher zu erläutern.

Bemerkungen:
Die ENISA ist eine von der Union geschaffene dezentrale Agentur und kann die Mitgliedstaaten und die Kommission bei der Anwendung der Richtlinie unterstützen, und zwar im Rahmen ihres bestehenden Auftrags und durch Umwidmung der im MFF 2014–2020 für diese Agentur vorgesehenen Mittel.

2. VERWALTUNGSMASSNAHMEN

2.1. Monitoring und Berichterstattung

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

Die Kommission wird das Funktionieren dieser Richtlinie regelmäßig überprüfen und dem Europäischen Parlament und dem Rat darüber Bericht erstatten. Darüber hinaus wird die Kommission die ordnungsgemäße Umsetzung der Richtlinie durch die Mitgliedstaaten bewerten. Der CEF-Vorschlag sieht auch die Möglichkeit vor, eine Evaluierung der Durchführungsmodalitäten der Maßnahmen sowie der Wirkung ihrer Durchführung vorzunehmen, um zu beurteilen, ob die Ziele, einschließlich der umweltbezogenen Ziele, erreicht worden sind.

2.2. Verwaltungs- und Kontrollsystem

2.2.1. Ermittelte Risiken

– Verzögerung der Projektdurchführung beim Aufbau der sicheren Infrastruktur

2.2.2. Vorgesehene Kontrollen

Die Vereinbarungen und Beschlüsse über die Durchführung der Maßnahmen im Rahmen der CEF sehen eine Überwachung und Finanzkontrolle durch die

[40] Einrichtungen im Sinne des Artikels 185 der Haushaltsordnung.

Kommission oder einen von ihr bevollmächtigten Vertreter sowie Prüfungen durch den Europäischen Rechnungshof und Überprüfungen vor Ort durch das Europäische Amt für Betrugsbekämpfung (OLAF) vor.

2.2.3. Kosten und Nutzen der Kontrollen und wahrscheinliche Verstoßquote

Dank risikobasierter Ex-ante- und Ex-post-Kontrollen sowie Vor-Ort-Prüfungen werden die Kontrollziele zu vertretbaren Kosten erreicht.

2.3. Prävention von Betrug und Unregelmäßigkeiten

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

Die Kommission gewährleistet bei der Durchführung der nach dieser Richtlinie finanzierten Maßnahmen den Schutz der finanziellen Interessen der Union durch geeignete Prävenntivmaßnahmen gegen Betrug, Korruption und sonstige rechtswidrige Handlungen, durch wirksame Kontrollen und – bei Feststellung von Unregelmäßigkeiten – durch Rückforderung zu Unrecht gezahlter Beträge sowie gegebenenfalls durch wirksame, verhältnismäßige und abschreckende Sanktionen.

Die Kommission oder ihre Vertreter und der Rechnungshof sind befugt, bei allen Empfängern, bei Auftragnehmern und Unterauftragnehmern, die Unionsmittel aus dem Programm erhalten haben, Rechnungsprüfungen anhand von Unterlagen und vor Ort durchzuführen.

Das Europäische Amt für Betrugsbekämpfung (OLAF) kann gemäß der Verordnung (Euratom, EG) Nr. 2185/96 bei allen direkt oder indirekt durch Finanzierungen aus Unionsmitteln betroffenen Wirtschaftsteilnehmern Kontrollen und Überprüfungen vor Ort durchführen, um festzustellen, ob im Zusammenhang mit einer Finanzhilfevereinbarung, einem Finanzhilfebeschluss oder einem Vertrag über eine Finanzierung aus Unionsmitteln ein Betrugs- oder Korruptionsdelikt oder eine sonstige rechtswidrige Handlung zum Nachteil der finanziellen Interessen der Union vorliegt.

Unbeschadet der vorstehenden Absätze ist der Kommission, dem Rechnungshof und dem OLAF in Kooperationsabkommen mit Drittstaaten und internationalen Organisationen, in Finanzhilfevereinbarungen, Finanzhilfebeschlüssen und Verträgen, sofern sich diese Abkommen, Vereinbarungen, Beschlüsse oder Verträge aus der Durchführung dieser Verordnung ergeben, ausdrücklich die Befugnis zu erteilen, derartige Rechnungsprüfungen sowie Kontrollen und Überprüfungen vor Ort durchzuführen.

Nach den Bestimmungen der CEF müssen Verträge über Finanzhilfen und Beschaffungsmaßnahmen auf Standardmustern basieren, in denen die allgemein anwendbaren Betrugsbekämpfungsmaßnahmen festgelegt sind.

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			
	Nummer [Bezeichnung……]	GM/NGM (41)	von EFTA-Ländern[42]	von Bewerberländern[43]	von Drittländern	nach Artikel 18 Absatz 1 Buchstabe aa der Haushaltsordnung
	09 03 02 Förderung des Zusammenschlusses und der Interoperabilität nationaler öffentlicher Dienstleistungen online sowie des Zugangs zu solchen Netzen	GM	Nein	Nein	Nein	Nein

- Neu zu schaffende Haushaltslinien (entfällt)

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

Rubrik des mehrjährigen Finanzrahmens	Haushaltslinie	Art der Ausgaben	Finanzierungsbeiträge			
	Nummer [Bezeichnung……]	GM/NGM	von EFTA-Ländern	von Bewerberländern	von Drittländern	nach Artikel 18 Absatz 1 Buchstabe aa der Haushaltsordnung
	[XX.YY.YY.YY]		JA/NEIN	JA/NEIN	JA/NEIN	JA/NEIN

41 GM = Getrennte Mittel / NGM = Nichtgetrennte Mittel.

42 EFTA: Europäische Freihandelsassoziation.

43 Bewerberländer sowie gegebenenfalls potenzielle Bewerberländer des Westbalkans.

3.2. Geschätzte Auswirkungen auf die Ausgaben

3.2.1. Übersicht

in Mio. EUR (3 Dezimalstellen)

Rubrik des mehrjährigen Finanzrahmens	1	Intelligentes und integratives Wachstum

GD: <…….>			2015* [44]	Jahr **2016**	Jahr **2017**	Jahr **2018**	Folgejahre (2019–2021) und danach			**INSGESAMT**
• Operative Mittel										
09 03 02	Verpflichtungen	(1)	1,250**	0,000						**1,250**
	Zahlungen	(2)	0,750	0,250	0,250					**1,250**
Aus der Dotation bestimmter operativer Programme finanzierte Verwaltungsausgaben[45]			**0,000**							**0,000**
Nummer der Haushaltslinie		(3)	**0,000**							**0,000**
Mittel INSGESAMT für GD <…>	Verpflichtungen	=1+1a +3	1,250	0,000						**1,250**
	Zahlungen	=2+2a +3	0,750	0,250	0,250					**1,250**

• Operative Mittel INSGESAMT	Verpflichtungen	(4)	1,250	0,000						**1,250**
	Zahlungen	(5)	0,750	0,250	0,250					**1,250**
• Aus der Dotation bestimmter operativer Programme finanzierte Verwaltungsausgaben INSGESAMT		(6)	**0.000**							

[44] Das Jahr N ist das Jahr, in dem mit der Umsetzung des Vorschlags/der Initiative begonnen wird.

[45] Ausgaben für technische und/oder administrative Unterstützung und Ausgaben zur Unterstützung der Umsetzung von Programmen bzw. Maßnahmen der EU (vormalige BA-Linien), indirekte Forschung, direkte Forschung.

Mittel INSGESAMT unter RUBRIK 1 des mehrjährigen Finanzrahmens	Verpflichtungen	=4+ 6	1,250	0,000						**1,250**
	Zahlungen	=5+ 6	0,750	0,250	0,250					**1,250**

* Die genaue zeitliche Planung hängt vom Datum der Annahme des Vorschlags durch den Gesetzgeber ab (d. h., wenn die Richtlinie im Laufe des Jahres 2014 erlassen wird, kann die Anpassung der bestehenden Infrastruktur im Jahr 2015 beginnen, ansonsten ein Jahr später).

** Sollten die Mitgliedstaaten beschließen, eine bestehende Infrastruktur zu nutzen und die einmaligen Kosten der Anpassung aus Mitteln des EU-Haushalts zu decken (wie in den Abschnitten 1.4.3 und 1.7 erläutert), so würden sich die Kosten der Anpassung eines bestehenden Netzes für die Unterstützung der Zusammenarbeit zwischen den Mitgliedstaaten gemäß Kapitel III der Richtlinie (Frühwarnung, koordinierte Reaktionsfähigkeit usw.) auf schätzungsweise 1 250 000 EUR belaufen. Dieser Betrag ist etwas höher als der in der Folgenabschätzung genannte Betrag („ungefähr 1 Mio. EUR“), weil er auf einer genaueren Schätzung der erforderlichen Komponenten einer solchen Infrastruktur beruht. Die erforderlichen Komponenten und die mit ihnen verbundenen Kosten beruhen auf einer Schätzung, die das JRC auf der Grundlage seiner Erfahrungen bei der Entwicklung ähnlicher Systeme für andere Gebiete wie das öffentliches Gesundheitswesen angefertigt hat, und umfassen: ein Schnellwarn- und Mitteilungssystem für NIS (275 000 EUR), eine Plattform für den Informationsaustausch (400 000 EUR), ein Frühwarn- und Reaktionssystem (275 000 EUR), ein Lagezentrum (300 000 EUR) mit Gesamtkosten von 1 250 000 EUR. Eine ausführlichere Durchführungsplanung wird voraussichtlich in der anstehenden Durchführbarkeitsstudie im Rahmen des Einzelvertrags SMART 2012/0010 enthalten sein: „Durchführbarkeitsstudie und vorbereitende Maßnahmen für die Umsetzung eines europäischen Frühwarn- und Abwehrsystems für Cyberangriffe und Störungen“.

Wenn der Vorschlag/die Initiative mehrere Rubriken betrifft:

• Operative Mittel INSGESAMT	Verpflichtungen	(4)	0,000	0,000						
	Zahlungen	(5)	0,000	0,000						
• Aus der Dotation bestimmter operativer Programme finanzierte Verwaltungsausgaben INSGESAMT		(6)	**0.000**	**0,000**						
Mittel INSGESAMT unter RUBRIKEN 1 bis 4 des mehrjährigen Finanzrahmens (Referenzbetrag)	Verpflichtungen	=4+ 6	1,250	0,000						1,250
	Zahlungen	=5+ 6	0,750	0,250	0,250					1,250

Rubrik des mehrjährigen Finanzrahmens	**5**	Verwaltungsausgaben

in Mio. EUR (3 Dezimalstellen)

		Jahr **2015**	Jahr **2016**	Jahr **2017**	Jahr **2018**	Folgejahre (2019–2021) und danach			**INSGESAMT**
GD: CNECT									
• Personalausgaben		0,572	0,572	0,572	0,572	0,572	0,572	**0,572**	**4,004**
• Sonstige Verwaltungsausgaben		0,318	0,118	0,318	0,118	0,318	0,118	**0,118**	**1,426**
GD CNECT INSGESAMT	Mittel	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

Mittel INSGESAMT unter RUBRIK 5 des mehrjährigen Finanzrahmens	(Verpflichtungen insges. = Zahlungen insges.)	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

in Mio. EUR (3 Dezimalstellen)

		Jahr **2015**[46]	Jahr **2016**	Jahr **2017**	Jahr **2018**	Folgejahre (2019–2021) und danach			**INSGESAMT**
Mittel INSGESAMT unter RUBRIKEN 1 bis 5 des mehrjährigen Finanzrahmens	Verpflichtungen	2,140	0,690	0,890	0,690	0,890	0,690	0,690	**6,680**
	Zahlungen	1,640	0,940	1,140	0,690	0,890	0,690	0,690	**6,680**

[46] Das Jahr N ist das Jahr, in dem mit der Umsetzung des Vorschlags/der Initiative begonnen wird.

3.2.2. Geschätzte Auswirkungen auf die operativen Mittel

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

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

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

Ziele und Ergebnisse ⇩			Jahr **2015***		Jahr **2016**		Jahr **2017**		Jahr **2018**		Folgejahre (2019–2021) und danach						**INSGESAMT**	
	ERGEBNISSE																	
	Art der Ergebnisse[47]	Durchschnittskosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Gesamtzahl	Gesamtkosten
EINZELZIEL Nr. 2[48] Sichere Infrastruktur für den Informationsaustausch																		
- Ergebnis	Anpassung der Infrastruktur																	
Zwischensumme für Einzelziel Nr. 2			1	1,250**													1	1,250
GESAMTKOSTEN				1,250														1,250

* Die genaue zeitliche Planung hängt vom Datum der Annahme des Vorschlags durch den Gesetzgeber ab (d. h., wenn die Richtlinie im Laufe des Jahres 2014 erlassen wird, kann die Anpassung der bestehenden Infrastruktur im Jahr 2015 beginnen, ansonsten ein Jahr später).

** Siehe Nummer 3.2.1.

47 Ergebnisse sind Produkte, die geliefert, und Dienstleistungen, die erbracht werden (z. B.: Austausch von Studenten, gebaute Straßenkilometer…).

48 Wie in Nummer 1.4.2. („Einzelziele…“) beschrieben.

3.2.3. Geschätzte Auswirkungen auf die Verwaltungsmittel

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)

	Jahr **2015**[49]	Jahr **2016**	Jahr **2017**	Jahr **2018**	Folgejahre (2019–2021) und danach			**INSGESAMT**
RUBRIK 5 des mehrjährigen Finanzrahmens								
Personalausgaben	0,572	0,572	0,572	0,572	0,572	0,572	0,572	**4,004**
Sonstige Verwaltungsausgaben	0,318	0,118	0,318	0,118	0,318	0,118	0,118	**1,426**
Zwischensumme RUBRIK 5 des mehrjährigen Finanzrahmens	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**
Außerhalb der RUBRIK 5[50] des mehrjährigen Finanzrahmens								
Personalausgaben	0,000	0,000						**0,000**
Sonstige Verwaltungsausgaben								
Zwischensumme der Mittel außerhalb der RUBRIK 5 des mehrjährigen Finanzrahmens	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**
INSGESAMT	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

Der Bedarf an Verwaltungsmitteln wird aus den Mitteln gedeckt, die der GD CNECT für die Verwaltung der Maßnahme bereits zugewiesen wurden bzw. durch Umschichtung innerhalb der GD verfügbar werden. Hinzu kommen etwaige zusätzliche Mittel, die der für die

49 Das Jahr N ist das Jahr, in dem mit der Umsetzung des Vorschlags/der Initiative begonnen wird.

50 Ausgaben für technische und administrative Unterstützung und Ausgaben zur Unterstützung der Umsetzung von Programmen oder Maßnahmen der EU (vormalige BA-Linien), indirekte Forschung, direkte Forschung.

Verwaltung der Maßnahme zuständigen GD nach Maßgabe der verfügbaren Mittel im Rahmen der jährlichen Mittelzuweisung zugeteilt werden.

Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) kann die Mitgliedstaaten und die Kommission bei der Anwendung der Richtlinie unterstützen, und zwar im Rahmen ihres bestehenden Auftrags und durch Umverteilung der im MFF 2014–2020 für diese Agentur vorgesehenen Mittel, d. h. ohne zusätzliche Haushaltsmittel oder Personalzuweisungen.

3.2.3.2. Geschätzte Auswirkungen auf die Humanressourcen

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

– ☑ Für den Vorschlag/die Initiative wird das folgende Kommissionspersonal benötigt:

Grundsätzlich wird kein zusätzliches Personal benötigt. Der Personalbedarf ist sehr begrenzt und wird durch bereits der Verwaltung der Maßnahme zugeordnetes Personal der GD gedeckt.

Schätzung in ganzzahligen Werten (oder mit höchstens einer Dezimalstelle)

		Jahr **2015**	Jahr **2016**	Jahr **2017**	Jahr **2018**	Folgejahre (2019–2021) und danach		
• Im Stellenplan vorgesehene Planstellen (Beamte und Bedienstete auf Zeit)								
09 01 01 01 (am Sitz und in den Vertretungen der Kommission)		4	4	4	4	4	4	4
XX 01 01 02 (in den Delegationen)								
XX 01 05 01 (indirekte Forschung)								
10 01 05 01 (direkte Forschung)								
• Externes Personal (in Vollzeitäquivalenten = VZÄ)[51]								
09 01 02 01 (AC, INT, ANS der Globaldotation)		1	1	1	1	1	1	1
XX 01 02 02 (AC, INT, JED, AL und ANS in den Delegationen)								
XX 01 04 ***yy***[52]	- am Sitz[53]							
	- in den Delegationen							
XX 01 05 02 (AC, INT, ANS der indirekten Forschung)								
10 01 05 02 (AC, INT, ANS der direkten Forschung)								

[51] AC = Vertragsbediensteter, INT = Leiharbeitskraft („Interimaire“), JED = Junger Sachverständiger in Delegationen, AL = örtlich Bediensteter, ANS = Abgeordneter Nationaler Sacherverständiger.

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

[53] Insbesondere für die Strukturfonds, den Europäischen Landwirtschaftsfonds für die Entwicklung des ländlichen Raums (ELER) und den Europäischer Fischereifonds (EFF).

Sonstige Haushaltslinien (bitte angeben)							
INSGESAMT	**5**	**5**	**5**	**5**	**5**	**5**	**5**

XX steht für den jeweiligen Haushaltstitel bzw. Politikbereich.

Der Personalbedarf wird durch der Maßnahme bereits zugeordnetes Personal der GD CNECT oder durch GD-interne Personalumsetzungen gedeckt. Hinzu kommen etwaige zusätzliche Mittel für Personal, die der für die Verwaltung der Maßnahme zuständigen GD nach Maßgabe der verfügbaren Mittel im Rahmen der jährlichen Mittelzuweisung zugeteilt werden können.

Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) kann die Mitgliedstaaten und die Kommission bei der Anwendung der Richtlinie unterstützen, und zwar im Rahmen ihres bestehenden Auftrags und durch Umwidmung der im MFF 2014–2020 für diese Agentur vorgesehenen Mittel, d. h. ohne zusätzliche Haushaltsmittel oder Personalzuweisungen.

Beschreibung der auszuführenden Aufgaben:

Beamte und Zeitbedienstete	– Ausarbeitung von delegierten Rechtsakten gemäß Artikel 14 Absatz 3 – Ausarbeitung von Durchführungsrechtsakten gemäß den Artikeln 8, 9 Absatz 2, 12, 14 Absatz 5 und 16. – Beitrag zur Zusammenarbeit sowohl auf strategischer wie auch operativer Ebene über das Netz. – Aufnahme internationaler Gespräche und möglicherweise Abschluss internationaler Vereinbarungen
Externes Personal	Unterstützung aller obigen Aufgaben, soweit notwendig

3.2.4. Vereinbarkeit mit dem mehrjährigen Finanzrahmen

– ☑ Der Vorschlag/die Initiative ist mit dem derzeitigen mehrjährigen Finanzrahmen vereinbar.

– ☐ Der Vorschlag/die Initiative erfordert eine Anpassung der betreffenden Rubrik des mehrjährigen Finanzrahmens.

Die geschätzten Auswirkungen auf die operativen Mittel werden eintreten, falls die Mitgliedstaaten beschließen, eine bestehende Infrastruktur anzupassen, und die Kommission innerhalb des MFF 2014–2020 mit der Durchführung der Anpassung beauftragen. Die damit verbundenen einmaligen Kosten würden aus CEF-Mittel gedeckt werden, unter der Voraussetzung, dass ausreichende Mittel zur Verfügung stehen. Alternativ hierzu können die Mitgliedstaaten entweder die Kosten der Anpassung der bestehenden Infrastruktur oder die Kosten der Einrichtung einer neuen Infrastruktur gemeinsam tragen.

– ☐ Der Vorschlag/die Initiative erfordert eine Inanspruchnahme des Flexibilitätsinstruments oder eine Änderung des mehrjährigen Finanzrahmens[54].

Entfällt.

3.2.5. Finanzierungsbeteiligung Dritter

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

[54] Siehe Nummern 19 und 24 der Interinstitutionellen Vereinbarung.

3.3. Geschätzte Auswirkungen auf die Einnahmen

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