Rat der
Europäischen Union

Brüssel, den 10. Februar 2016
(OR. en)

5894/16

Interinstitutionelles Dossier:
2013/0027 (COD)

TELECOM 14
DATAPROTECT 10
CYBER 10
MI 65
CSC 24
CODEC 134

VERMERK

Absender:	Generalsekretariat des Rates
Empfänger:	Ausschuss der Ständigen Vertreter/Rat
Nr. Komm.dok.:	6342/13 TELECOM 24 DATAPRTOECT 14 CYBER 2 MI 104 CODEC 313
Betr.:	Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union – Politische Einigung

Im Hinblick auf die Erzielung einer politischen Einigung erhalten die Delegationen in der Anlage den Text des obengenannten Vorschlags, über den beim informellen Trilog vom 7. Dezember 2015 eine inhaltliche Einigung erzielt worden ist. Die inhaltliche Einigung ist anschließend vom Ausschuss der Ständigen Vertreter[1] und vom Ausschuss für Binnenmarkt und Verbraucherschutz (IMCO) des Europäischen Parlaments am 18. Dezember 2015 bzw. 14. Januar 2016 gebilligt worden.

[1] Dok. 15229/2/15 REV 2.

Damit den für Ratsdokumente geltenden Formvorschriften entsprochen wird, haben die Rechts- und Sprachsachverständigen des Rates und des Europäischen Parlaments erste technische Anpassungen an dem Kompromisstext vorgenommen, was jedoch keine inhaltlichen Änderungen zur Folge hatte. Die technischen Änderungen bestehen darin, dass die Erwägungsgründe in die übliche Reihenfolge gebracht wurden, dass die Bezugnahmen auf Rechtsakte der EU gemäß dem Gemeinsamen Leitfaden für die Abfassung von Rechtstexten der Europäischen Union überarbeitet wurden und dass hinsichtlich der Verwendung von Abkürzungen im gesamten Text eine kurze Übereinstimmungskontrolle durchgeführt wurde. Die Änderungen sind natürlich kein Vorgriff auf die weitere Überarbeitung durch die Rechts- und Sprachsachverständigen, die nach der Bestätigung der politischen Einigung durch den Rat beginnen wird.

RICHTLINIE (EU) 2016/... DES EUROPÄISCHEN PARLAMENTS UND DES RATES
vom ...
über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netzen und Informationssystemen in der Union

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION –

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

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses[2],

gemäß dem ordentlichen Gesetzgebungsverfahren[3],

in Erwägung nachstehender Gründe:

[2] ABl. C […] vom […], S. […].

[3] Standpunkt des Europäischen Parlaments vom … [(ABl. …)/(noch nicht im Amtsblatt veröffentlicht)] und Standpunkt des Rates in erster Lesung vom … [(ABl. …)/(noch nicht im Amtsblatt veröffentlicht)]. Standpunkt des Europäischen Parlaments vom ... [(ABl. ...)/(noch nicht im Amtsblatt veröffentlicht)].

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

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

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

(4) Auf der Grundlage der beträchtlichen Fortschritte, die im Rahmen des Europäischen Forums der Mitgliedstaaten (EFMS) zur Förderung von Gesprächen und des Austauschs bewährter Vorgehensweisen, unter anderem zur Entwicklung von Grundsätzen für die europäische Zusammenarbeit bei Cyberkrisen, erzielt worden sind, sollte eine Kooperationsgruppe eingesetzt werden, der Vertreter der Mitgliedstaaten, der Kommission und der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) angehören, um die strategische Zusammenarbeit zwischen den Mitgliedstaaten im Bereich der Netz-und Informationssicherheit (im Folgenden "NIS") zu unterstützen und zu erleichtern. Damit eine solche Gruppe wirksam sein kann und alle Beteiligten einbezogen werden, muss jeder Mitgliedstaat über Minimalfähigkeiten und eine Strategie verfügen, die in seinem Hoheitsgebiet ein hohes Niveau an NIS gewährleisten. Außerdem sollten für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste Anforderungen in Bezug auf die Sicherheit und die Meldung von Sicherheitsvorfällen gelten, damit eine Kultur des Risikomanagements gefördert wird und sichergestellt ist, dass die gravierendsten Sicherheitsvorfälle gemeldet werden.

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

(6) 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, Zusammenarbeit sowie gemeinsame Sicherheits-anforderungen für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste beinhaltet.

(6a) Betreiber wesentlicher Dienste und Anbieter digitaler Dienste sollten nicht daran gehindert werden, strengere Sicherheitsmaßnahmen anzuwenden, als sie in dieser Richtlinie vorgesehen sind.

(7) Um alle einschlägigen Sicherheitsvorfälle und Sicherheitsrisiken abdecken zu können, sollte diese Richtlinie sowohl für Betreiber wesentlicher Dienste als auch für Anbieter digitaler Dienste gelten. Die den Betreibern wesentlicher Dienste und den Anbietern digitaler Dienste auferlegten Verpflichtungen sollten hingegen nicht für Unternehmen gelten, die öffentliche Kommunikationsnetze oder öffentlich zugängliche elektronische Kommunikationsdienste im Sinne der Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002[4] bereitstellen und die den besonderen Sicherheits- und Integritäts-anforderungen des Artikels 13a jener Richtlinie unterliegen; die Verpflichtungen sollten auch nicht für Vertrauensdiensteanbieter im Sinne der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates[5] gelten, die den Anforderungen des Artikels 19 jener Verordnung unterliegen.

---

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

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

(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, sollte von den Bestimmungen dieser Richtlinie unberührt bleiben. Nach Artikel 346 AEUV ist kein Mitgliedstaat verpflichtet, Auskünfte zu erteilen, deren Preisgabe seines Erachtens seinen wesentlichen Sicherheitsinteressen widerspricht. In diesem Zusammenhang sind der Beschluss 2011/292/EU des Rates[6] sowie Geheimhaltungsvereinbarungen oder informelle Geheimhaltungsvereinbarungen wie das sogenannte Traffic Light Protocol (TLP) von Bedeutung.

(9) Für bestimmte Wirtschaftssektoren gelten bereits sektorspezifische Rechtsakte der Union, die Vorschriften im Zusammenhang mit der Sicherheit von Netzen und Informationssystemen beinhalten; für weitere Wirtschaftssektoren kann dies künftig der Fall sein. Wann immer solche Unionsrechtsakte Bestimmungen enthalten, mit denen Anforderungen in Bezug auf die Sicherheit von Netzen und Informationssystemen oder die Meldung von Sicherheitsvorfällen auferlegt werden, sollten diese Bestimmungen anstelle der entsprechenden Bestimmungen dieser Richtlinie gelten, wenn sie Anforderungen vorsehen, die hinsichtlich ihrer Wirkung den in dieser Richtlinie enthaltenen Verpflichtungen mindestens gleichwertig sind.

(10) Die Mitgliedstaaten sollten dann die Bestimmungen des betreffenden sektorspezifischen Unionsrechtsakts anwenden, einschließlich der Bestimmungen über die gerichtliche Zuständigkeit, und nicht das in dieser Richtlinie festgelegte Verfahren zur Ermittlung der Betreiber wesentlicher Dienste durchführen. In diesem Zusammenhang sollten die Mitgliedstaaten die Kommission über die Anwendung der "lex specialis"-Bestimmung unterrichten.

(11) Bei der Feststellung, ob die in sektorspezifischen Unionsrechtsakten enthaltenen Anforderungen in Bezug auf die Sicherheit von Netzen und Informationssystemen und/oder die Meldung von Sicherheitsvorfällen den in den Artikeln 14 und 15a dieser Richtlinie enthaltenen Anforderungen gleichwertig sind, sollten ausschließlich die Bestimmungen der einschlägigen Unionsrechtsakte und ihre Anwendung in den Mitgliedstaaten berücksichtigt werden.

---

[6] Beschluss 2011/292/EU des Rates vom 31. März 2011 über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen (ABl. L 141 vom 27.5.2011, S. 17).

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

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

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

(15) Cloud-Computing-Dienste umfassen eine breite Palette von Tätigkeiten, die auf unterschiedliche Weise erbracht werden können. Für die Zwecke dieser Richtlinie sind unter "Cloud-Computing-Diensten" Dienste zu verstehen, die den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglichen. Unter den Begriff "Rechenressourcen" fallen Ressourcen wie Netze, Server oder sonstige Infrastruktur, Speicher, Anwendungen und Dienste. "Skalierbar" bedeutet, dass Rechenressourcen unabhängig von ihrem geografischen Standort vom Anbieter des Cloud-Dienstes flexibel zugeteilt werden, damit Nachfrageschwankungen bewältigt werden können. "Elastischer Pool" bedeutet, dass diese Rechenressourcen entsprechend der Nachfrage bereitgestellt und freigegeben werden, damit die verfügbaren Ressourcen je nach Arbeitsaufkommen rasch auf- bzw. abgebaut werden können. "Gemeinsam nutzbar" bedeutet, dass diese Rechenressourcen einer Vielzahl von Nutzern bereitgestellt werden, die über einen gemeinsamen Zugang auf den Dienst zugreifen, wobei jedoch die Verarbeitung für jeden Nutzer separat erfolgt, obwohl der Dienst von ein und derselben elektronischen Einrichtung erbracht wird.

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

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

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

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

(20) Einrichtungen in den in Anhang II aufgeführten Sektoren und Teilsektoren können wesentliche und nicht wesentliche Dienste erbringen. Beispielsweise können im Luftverkehrssektor die Flughäfen Dienste erbringen, die von einem Mitgliedstaat als wesentlich betrachtet werden, wie etwa das Start-und Landebahn-Management, jedoch auch eine Reihe von Diensten, die als nicht wesentlich betrachtet werden könnten, wie die Bereitstellung von Einkaufsbereichen. Betreiber wesentlicher Dienste sollten den spezifischen Sicherheitspflichten nur in Bezug auf die als wesentlich geltenden Dienste unterworfen sein. Zum Zwecke der Ermittlung von Betreibern sollten die Mitgliedstaaten deshalb ein Verzeichnis der Dienste erstellen, die als wesentlich betrachtet werden.

(21) Das Verzeichnis der Dienste sollte den zuständigen nationalen Behörden als Bezugspunkt für die Ermittlung von Betreibern wesentlicher Dienste dienen. In dem Verzeichnis sollen die in einem bestimmten in Anhang II aufgeführten Sektor als wesentlich geltenden Arten von Diensten ausgewiesen und damit von den nicht wesentlichen Tätigkeiten abgegrenzt werden, für die eine in einem bestimmten Sektor tätige Einrichtung zuständig sein kann. Das Verzeichnis der Dienste sollte alle im Hoheitsgebiet eines Mitgliedstaats erbrachten Dienste enthalten, die die Anforderungen nach dieser Richtlinie erfüllen. Der betreffende Mitgliedstaat sollte die Möglichkeit haben, in das bestehende Verzeichnis neue Dienste aufzunehmen, die möglicherweise künftig entwickelt werden. Das von jedem Mitgliedstaat erstellte Verzeichnis der Dienste wäre ein weiterer Beitrag zur Beurteilung der Regelungspraxis der einzelnen Mitgliedstaaten im Hinblick auf das Ziel, ein insgesamt kohärentes Verfahren der Ermittlung auf der Ebene der Mitgliedstaaten zu gewährleisten.

(22) Bietet ein potenzieller Betreiber die wesentlichen Dienste in zwei oder mehr Mitgliedstaaten an, sollten diese Mitgliedstaaten zur Ermittlung des Betreibers bilaterale oder multilaterale Beratungen aufnehmen. Dieser Konsultationsprozess soll den Mitgliedstaaten dabei helfen, die Kritikalität des Betreibers im Hinblick auf grenzüberschreitende Auswirkungen zu beurteilen, und ermöglicht es jedem beteiligten Mitgliedstaat, sich zu den Risiken zu äußern, die seiner Ansicht nach mit den von dem Betreiber angebotenen Diensten verbunden sind. Hierbei sollten die betroffenen Mitgliedstaaten den Ansichten der jeweils anderen Mitgliedstaaten Rechnung tragen. Die betroffenen Mitgliedstaaten können diesbezüglich die Unterstützung der Kooperationsgruppe anfordern.

(23) Aufgrund des Prozesses der Ermittlung sollten die Mitgliedstaaten nationale Maßnahmen erlassen, in denen bestimmt wird, welche Einrichtungen den NIS-Verpflichtungen unterliegen. Dies könnte durch die Festlegung eines Verzeichnisses sämtlicher Betreiber wesentlicher Dienste oder durch die Annahme nationaler Maßnahmen einschließlich objektiv quantifizierbarer Kriterien (z.B. Leistung des Betreibers oder Anzahl der Nutzer) zur Bestimmung der Einrichtungen, die den NIS-Verpflichtungen unterliegen, erfolgen. Die nationalen Maßnahmen sollten sämtliche rechtlichen und verwaltungsrechtlichen Maßnahmen sowie alle Strategien umfassen, die die Ermittlung von Betreibern wesentlicher Dienste im Sinne dieser Richtlinie ermöglichen, gleich, ob sie bereits gelten oder im Rahmen dieser Richtlinie angenommen werden.

(24) Zur Angabe der Bedeutung der ermittelten Betreiber in Bezug auf den jeweiligen Sektor sollten die Mitgliedstaaten der Anzahl und der Größe der ermittelten Betreiber Rechnung tragen, beispielsweise im Hinblick auf deren Marktanteil oder die produzierte oder beförderte Datenmenge, ohne dabei verpflichtet zu sein, Informationen preiszugeben, aus denen hervorgeht, welche Betreiber ermittelt wurden.

(25) Bei der Feststellung, in welchem Maße ein Sicherheitsvorfall sich störend auf einen wesentlichen Dienst auswirkt, sollten die Mitgliedstaaten berücksichtigen, wie viele natürliche und juristische Personen diesen Dienst zu privaten oder beruflichen Zwecken nutzen. Die Nutzung dieses Dienstes kann unmittelbar, mittelbar oder durch Vermittlung erfolgen.

(26) Um zu bestimmen, ob ein Sicherheitsvorfall zu erheblichen Störungen bei der Bereitstellung eines Dienstes führen würde, sollten die Mitgliedstaaten eine Reihe unterschiedlicher Faktoren berücksichtigen. Bei der Beurteilung, in welchem Ausmaß und wie lange sich ein Sicherheitsvorfall auf wirtschaftliche und gesellschaftliche Tätigkeiten oder die öffentliche Sicherheit auswirken könnte, sollten die Mitgliedstaaten außerdem die Zeitspanne abschätzen, die voraussichtlich vergeht, bevor die Unterbrechung nachteilige Auswirkungen hätte.

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

(28) Um ein hohes gemeinsames Niveau der Sicherheit von Netzen und Informationssystemen zu erreichen und aufrechtzuerhalten, sollte jeder Mitgliedstaat über eine nationale NIS-Strategie verfügen, in der die strategischen Ziele sowie konkrete politische Maßnahmen vorgesehen sind.

(29) Um die effektive Umsetzung der aufgrund dieser Richtlinie erlassenen Bestimmungen zu ermöglichen, sollte in jedem Mitgliedstaat eine für die Koordinierung von Fragen der NIS zuständige Stelle geschaffen oder benannt werden, die auf Unionsebene für die Zwecke der grenzüberschreitenden Zusammenarbeit als zentrale Anlaufstelle dient. Die zuständigen Behörden und die zentrale Anlaufstelle sollten mit angemessenen technischen, finanziellen und personellen Ressourcen ausgestattet sein, um die ihnen übertragenen Aufgaben wirksam und effizient erfüllen und somit die Ziele dieser Richtlinie erreichen zu können. Da mit dieser Richtlinie durch den Aufbau von Vertrauen ein besseres Funktionieren des Binnenmarkts bezweckt wird, müssen die Stellen der Mitgliedstaaten wirksam mit den Wirtschaftsteilnehmern zusammenarbeiten können und über entsprechende Strukturen verfügen.

(30) Angesichts der unterschiedlichen nationalen Verwaltungsstrukturen und zur Beibehaltung bereits bestehender sektorbezogener Vereinbarungen bzw. bereits eingerichteter Aufsichts- und Regulierungsstellen der Union und zur Vermeidung von Doppelungen sollten die Mitgliedstaaten mehrere nationale zuständige Behörden benennen können, die für die Erfüllung von Aufgaben im Zusammenhang mit der Sicherheit von Netzen und Informationssystemen von Betreibern wesentlicher Dienste und Anbietern digitaler Dienste im Rahmen dieser Richtlinie zuständig sind. Zur Erleichterung der grenzüberschreitenden Zusammenarbeit und Kommunikation ist es allerdings notwendig, dass jeder Mitgliedstaat unbeschadet der sektorbezogenen regulatorischen Vereinbarungen eine nationale zentrale Anlaufstelle mit Zuständigkeit für die grenzüberschreitende Zusammenarbeit auf Unionsebene benennt.

(31) Sicherheitsvorfälle sollten den zuständigen Behörden oder den Computer-Notfallteams (CSIRT – Computer Security Incident Response Team) gemeldet werden. Sicherheitsvorfälle sollten nicht unmittelbar den zentralen Anlaufstellen gemeldet werden, es sei denn, diese üben außerdem die Funktion einer zuständigen Behörde oder eines CSIRT aus. Eine zuständige Behörde oder ein CSIRT könnte allerdings die zentrale Anlaufstelle beauftragen, Meldungen über Sicherheitsvorfälle an die zentralen Anlaufstellen anderer betroffener Mitgliedstaaten weiterzuleiten.

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

(33) Alle Mitgliedstaaten sollten über angemessene technische und organisatorische Fähigkeiten verfügen, um die Prävention, Erkennung, Reaktion und Folgenminderung bei NIS-Vorfällen und -Risiken gewährleisten zu können. Alle Mitgliedstaaten sollten daher gewährleisten, dass sie über gut funktionierende CSIRT – auch IT-Notfallteams (CERT – Computer Emergency Response Teams) genannt – verfügen, die die grundlegenden Anforderungen im Hinblick auf die Gewährleistung wirksamer und kompatibler Fähigkeiten zur Bewältigung von Sicherheitsvorfällen und Sicherheitsrisiken und einer effizienten Zusammenarbeit auf Unionsebene erfüllen. Damit alle Arten von Betreibern wesentlicher Dienste und Anbietern digitaler Dienste diese Fähigkeiten und diese Zusammenarbeit nutzen können, sollten die Mitgliedstaaten sicherstellen, dass für jede Art eine benannte CSIRT zuständig ist. Wegen der Bedeutung der internationalen Zusammenarbeit zur Cybersicherheit sollten die CSIRT die Möglichkeit erhalten, sich zusätzlich zum durch diese Richtlinie geschaffenen CSIRT-Netz an internationalen Kooperationsnetzen zu beteiligen.

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

(35) Die ENISA sollte die Mitgliedstaaten und die Kommission mit Fachkompetenz, als Berater und als Mittler für den Austausch bewährter Verfahren unterstützen. Insbesondere sollte die Kommission und könnten die Mitgliedstaaten die ENISA bei der Anwendung dieser Richtlinie zu Rate ziehen. Damit sichergestellt ist, dass die Mitgliedstaaten und die Kommission wirksam informiert werden, sollte der Kooperationsgruppe ein zusammenfassender Bericht über die Meldungen vorgelegt werden. Um Kapazitäten und Fachwissen unter den Mitgliedstaaten aufbauen zu können, sollte die Kooperationsgruppe auch als Mittel für den Austausch bewährter Verfahren, für die Beratung über Fähigkeiten und die Abwehrbereitschaft der Mitgliedstaaten dienen und damit ihren Mitgliedern – auf freiwilliger Basis – bei der Evaluierung der nationalen NIS-Strategien, beim Kapazitätsaufbau und bei NIS-Übungen helfen.

(36) Bei der Anwendung der Bestimmungen dieser Richtlinie sollten die Mitgliedstaaten bestehende Organisationsstrukturen oder bestehende Strategien nutzen oder anpassen können.

(37) Die jeweiligen Aufgaben der Kooperationsgruppe und der ENISA bedingen einander und ergänzen sich. Im Einklang mit ihrem in Artikel 2 der Verordnung (EU) Nr. 526/2013 des Europäischen Parlaments und des Rates[7] festgelegten Ziel, "[...] die Organe, Einrichtungen und sonstigen Stellen der Union und die Mitgliedstaaten dabei [zu unterstützen], die politischen Maßnahmen durchzuführen, die erforderlich sind, um die rechtlichen und regulatorischen Anforderungen in Bezug auf Netz- und Informationssicherheit in geltenden und künftigen Rechtsakten der Union zu erfüllen [...]", sollte die ENISA die nach Artikel 8a eingesetzte Kooperationsgruppe bei der Ausführung ihrer Aufgaben unterstützen. Die ENISA sollte insbesondere in den Bereichen Unterstützung leisten, die ihren eigenen, in Artikel 3 der Verordnung 526/2013 festgelegten Aufgaben entsprechen, nämlich Strategien zur Netz- und Informationssicherheit zu analysieren, die Organisation und Durchführung von Übungen zur Netz- und Informationssicherheit auf Unionsebene zu unterstützen und Informationen und bewährte Verfahren in den Bereichen Öffentlichkeitsarbeit und Fortbildung auszutauschen. Die ENISA sollte außerdem an der Entwicklung von Leitlinien für sektorspezifische Kriterien zur Bestimmung der Bedeutung der Auswirkungen eines Sicherheitsvorfalls beteiligt sein.

---

[7] Verordnung (EU) Nr. 526/2013 des Europäischen Parlaments und des Rates vom 21. Mai 2013 über die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) und zur Aufhebung der Verordnung (EG) Nr. 460/2004 (ABl. L 165 vom 18.6.2013, S. 4).

(38) Zur Förderung einer verbesserten Netz- und Informationssicherheit sollte die Kooperationsgruppe gegebenenfalls mit den einschlägigen Organen, Einrichtungen und sonstigen Stellen der Union zusammenarbeiten, um Know-how und bewährte Verfahren mit ihnen auszutauschen und sie bezüglich Aspekten der Netz- und Informationssicherheit, die Auswirkungen auf ihre Arbeit haben könnten, zu beraten, wobei die geltenden Vereinbarungen für den Austausch von einem eingeschränkten Zugang unterliegenden Informationen einzuhalten sind. Bei ihrer Zusammenarbeit mit Rechtsdurchsetzungsbehörden in Bezug auf Netz- und Informationssicherheitsaspekte, die sich möglicherweise auf ihre Arbeit auswirken, sollte die Kooperationsgruppe vorhandene Informationskanäle und bestehende Netze beachten.

(39) Informationen über NIS-Vorfälle sind für die allgemeine Öffentlichkeit und Unternehmen, insbesondere für kleine und mittlere Unternehmen, zunehmend von Bedeutung. In manchen Fällen werden derartige Informationen bereits über das Internet auf nationaler Ebene in der jeweiligen Landessprache und mit besonderem Schwerpunkt auf Sicherheitsvorfälle und Sicherheitsereignisse mit nationalem Bezug bereitgestellt. Da Unternehmen immer stärker grenzüberschreitend tätig sind und die Bürger Online-Dienste nutzen, sollten die Informationen über Sicherheitsvorfälle auf EU-Ebene in aggregierter Form bereitgestellt werden. Das Sekretariat des CSIRT-Netzes wird ermutigt, eine Website zu unterhalten oder eine entsprechende Seite auf einer bestehenden Website einzustellen, auf der allgemeine Informationen über größere NIS-Vorfälle, die in der Union auftreten, mit einem besonderen Schwerpunkt auf die Interessen und den Bedarf von Unternehmen der allgemeinen Öffentlichkeit zur Verfügung gestellt werden. CSIRT, die sich am CSIRT-Netz beteiligen, werden ermutigt, die auf dieser Website zu veröffentlichenden Informationen auf freiwilliger Basis bereitzustellen. Diese Websites sollen keine vertraulichen oder sensiblen Informationen enthalten.

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

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

(42) 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 umfassendes Konzept für NIS-Fragen gefördert werden kann.

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

(44) Diese Richtlinie gilt nur für die Arten von öffentlichen Verwaltungen, die im Anhang II aufgeführt sind und als Betreiber wesentlicher Dienste ermittelt wurden. Die Mitgliedstaaten sind für die Gewährleistung der Sicherheit von Netzen und Informationssystemen der öffentlichen Verwaltungen verantwortlich, die nicht in den Geltungsbereich dieser Richtlinie fallen.

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

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

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

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

(49) Zwar sind Hersteller von Hardware und Softwareentwickler keine Betreiber wesentlicher Dienste oder Anbieter digitaler Dienste, die mit denen vergleichbar sind, die unter diese Richtlinie fallen, doch begünstigen ihre Produkte die Sicherheit von Netzen und Informationssystemen. Daher spielen sie eine wichtige Rolle dabei, die Betreiber wesentlicher Dienste und die Anbieter digitaler Dienste in die Lage zu versetzen, ihre Netz- und Informationsinfrastukturen sichern zu können. Derartige Hardware- und Softwareprodukte unterliegen bereits geltenden Produkthaftungsvorschriften.

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

(51) Die Betreiber wesentlicher Dienste und die Anbieter digitaler Dienste sollten die Sicherheit der von ihnen verwendeten 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 Sicherheitsanforderungen und die Meldepflicht sollten für die einschlägigen Betreiber wesentlicher Dienste und Anbieter digitaler Dienste unabhängig davon gelten, ob sie ihre Netze und Informationssysteme intern warten oder diese Aufgabe ausgliedern.

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

(53) Nehmen öffentliche Verwaltungen in den Mitgliedstaaten die Dienste von Anbietern digitaler Dienste in Anspruch, insbesondere Cloud-Computing-Dienste, ist es möglich, dass sie vom Anbieter derartiger Dienste zusätzliche Sicherheitsmaßnahmen über das üblicherweise von Anbietern digitaler Dienste im Einklang mit dieser Richtlinie Angebotene hinaus wünschen. Sie können dies über vertragliche Verpflichtungen regeln.

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

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

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

(57) Mit dieser Richtlinie sollte den Mitgliedstaaten nicht untersagt werden, Einrichtungen, die keine Anbieter digitaler Dienste innerhalb des Geltungsbereichs dieser Richtlinie sind, unbeschadet der den Mitgliedstaaten nach Unionsrecht auferlegten Pflichten Sicherheitsanforderungen und Meldepflichten aufzuerlegen.

(58) Die Kommission wird ermutigt, den folgenden Beispielen Rechnung zu tragen, wenn sie Durchführungsrechtsakte über Sicherheitsanforderungen für Anbieter digitaler Dienste erlässt: im Zusammenhang mit der Sicherheit der Systeme und Anlagen: physische Sicherheit und Sicherheit des Umfelds, Sicherheit des Materials, Kontrolle des Zugangs zum Netz und zu Informationssystemen sowie Integrität des Netzes und der Informationssysteme; im Hinblick auf die Bewältigung von Sicherheitsvorfällen: Verfahren für die Bewältigung von Sicherheitsvorfällen, Kapazitäten zum Aufspüren von Sicherheitsvorfällen, Meldung und Mitteilung von Sicherheitsvorfällen; in Bezug auf Betriebskontinuitätsmanagement: Strategie für die Kontinuität der Dienste sowie Notfallpläne, Kapazitäten zur Wiederherstellung im Falle eines Systemabsturzes; und in Bezug auf Überwachung, Überprüfung und Erprobung: Strategien für die Überwachung und Protokollierung, Beübung von Notfallplänen, Erprobung des Netzes und der Informationssysteme, Sicherheitsbewertungen und Überwachung der Einhaltung der Anforderungen.

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

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

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

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

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

(64) Ein Anbieter digitaler Dienste sollte der gerichtlichen Zuständigkeit nur eines Mitgliedstaats unterliegen, und zwar des Mitgliedstaats, in dem er seine Hauptniederlassung in der Union hat; dies ist im Allgemeinen der Ort, an dem er seinen Hauptsitz in der Union hat. Eine Niederlassung setzt die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus. Die Rechtsform einer solchen Einrichtung, gleich, ob es sich um eine Zweigstelle oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handelt, ist dabei unerheblich. Dieses Kriterium sollte nicht davon abhängen, ob sich der physische Standort des Netzes und der Informationssysteme an diesem Ort befindet; das Vorhandensein und die Nutzung derartiger Systeme stellen an sich keine derartige Hauptniederlassung dar und sind daher kein Kriterium für die Bestimmung der Hauptniederlassung.

(65) Bietet ein Anbieter digitaler Dienste, der keine Niederlassung in der Union hat, Dienste in der Union an, so sollte er einen Vertreter benennen. Um festzustellen, ob ein solcher Anbieter digitaler Dienste in der Union Dienste anbietet, sollte geprüft werden, ob er offensichtlich beabsichtigt, Personen in einem oder mehreren Mitgliedstaaten der Union Dienste anzubieten. Während die bloße Zugänglichkeit der Website eines Anbieters digitaler Dienste oder eines Vermittlers in der Union oder einer E-Mail-Adresse oder anderer Kontaktdaten oder die Verwendung einer Sprache, die in dem Drittland, in dem der Anbieter digitaler Dienste niedergelassen ist, allgemein gebräuchlich ist, hierfür kein ausreichender Anhaltspunkt sind, können andere Faktoren wie die Verwendung einer Sprache oder Währung, die in einem oder mehreren Mitgliedstaaten gebräuchlich ist, in Verbindung mit der Möglichkeit, Dienste in dieser anderen Sprache zu bestellen, und/oder die Erwähnung von Kunden oder Nutzern in der Union darauf hindeuten, dass der Anbieter digitaler Dienste beabsichtigt, in der Union Dienste anzubieten. Der Vertreter sollte im Auftrag des Anbieters digitaler Dienste handeln, und die zuständigen Behörden oder die CSIRT können mit ihm Kontakt aufnehmen. Der Anbieter digitaler Dienste sollte den Vertreter ausdrücklich schriftlich beauftragen, hinsichtlich seiner Pflichten in seinem Auftrag zu handeln; hierzu zählt auch das Melden von Sicherheitsvorfällen im Sinne dieser Richtlinie.

(66) Die Normung von Sicherheitsanforderungen ist ein vom Markt ausgehender Vorgang. Um die Sicherheitsstandards einander anzunähern, sollten die Mitgliedstaaten die Anwendung oder Einhaltung konkreter Normen fördern, damit ein hohes Sicherheitsniveau auf Unionsebene gewährleistet wird. Die ENISA sollte den Mitgliedstaaten mit Leitlinien beratend zur Seite stehen. Zu diesem Zweck könnte es hilfreich sein, harmonisierte Normen auszuarbeiten; dies sollte nach der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates[8] geschehen.

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

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

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

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

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

(71) Wie die Europäische Zentralbank in ihrer Stellungnahme vom 25. Juli 2014 zum Vorschlag zur Netz- und Informationssicherheit[9] festgestellt hat, berührt die Richtlinie nicht die bestehenden unionsrechtlichen Bestimmungen zur Überwachung von Zahlungsverkehrs- und Abwicklungssystemen durch das Eurosystem. Die für eine derartige Überwachung verantwortlichen Behörden sollten ihre Erfahrungen zu NIS-bezogenen Angelegenheiten mit den nach dieser Richtlinie zuständigen Behörden austauschen. Gleiches gilt für die Mitgliedstaaten, die zwar nicht Mitglied des Eurosystems, wohl aber des Europäischen Systems der Zentralbanken sind, und die eine Überwachung der Zahlungsverkehrs- und Abwicklungssysteme auf der Grundlage einzelstaatlicher Gesetze und Vorschriften vornehmen.

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

(72) Zur Gewährleistung einheitlicher Voraussetzungen für die Umsetzung dieser Richtlinie sollten der Kommission Durchführungsbefugnisse in Bezug auf die Festlegung der Verfahrensmodalitäten, die für das Funktionieren der Kooperationsgruppe erforderlich sind, und der Sicherheitsanforderungen und Meldepflichten für Anbieter digitaler Dienste übertragen werden. Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates[10] ausgeübt werden. Wenn die Kommission Durchführungsrechtsakte zu Sicherheitsanforderungen und Meldepflichten für Anbieter digitaler Dienste erlässt, sollte sie der Stellungnahme der ENISA weitestgehend Rechnung tragen und sich mit interessierten Kreisen abstimmen. Wenn sie Durchführungsrechtsakte zu Verfahrensmodalitäten, die für das Funktionieren der Kooperationsgruppe erforderlich sind, erlässt, sollte sie der Stellungnahme der ENISA weitestgehend Rechnung tragen.

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

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

---

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

(75) Der Austausch von Informationen über Sicherheitsrisiken und -vorfälle in der Kooperationsgruppe und im CSIRT-Netz und die Einhaltung der Verpflichtung zur Meldung von Sicherheitsvorfällen bei den zuständigen nationalen Behörden oder den CSIRT kann die Verarbeitung personenbezogener Daten erfordern. Diese Verarbeitung von personenbezogenen Daten sollte mit der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates[11] und der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates[12] vereinbar sein. 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[13] entsprechend gelten.

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

---

11 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31).

12 Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (ABl. L 8 vom 12.1.2001, S. 1).

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

14 ABl. C 32 vom 4.2.2014, S. 19.

(77) Da das Ziel dieser Richtlinie, eine hohe Netz- und Informationssicherheit in der Union zu erreichen, 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.

(78) 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, dem Schutz personenbezogener Daten, der unternehmerischen Freiheit, dem Eigentumsrecht, dem Recht auf einen wirksamen Rechtsbehelf und dem Recht, gehört zu werden, im Einklang. Diese Richtlinie ist im Einklang 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 festgelegt, mit denen ein hohes gemeinsames Sicherheitsniveau von Netzen und Informationssystemen (im Folgenden "NIS") in der Union erreicht werden soll, um so das Funktionieren des Binnenmarkts zu verbessern.

2. Zu diesem Zweck sieht diese Richtlinie Folgendes vor:

(a) die Pflicht für alle Mitgliedstaaten, eine nationale NIS-Strategie festzulegen;

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

(ba) die Schaffung eines Netzes von Computer-Notfallteams (CSIRT – Computer Security Incident Response Teams), um zum Aufbau von Vertrauen zwischen den Mitgliedstaaten beizutragen und eine rasche und wirksame operative Zusammenarbeit zu fördern;

(c) Sicherheitsanforderungen und Meldepflichten für die Betreiber wesentlicher Dienste;

(ca) Sicherheitsanforderungen und Meldepflichten für die Anbieter digitaler Dienste;

(d) die Pflicht für die Mitgliedstaaten, nationale zuständige Behörden, zentrale Anlaufstellen und CSIRT zu benennen, die Aufgaben im Zusammenhang mit der Sicherheit von Netzen und Informationssystemen zu erfüllen haben.

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

4. Die Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates[15], die Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates[16] und die Richtlinie 2008/114/EG des Rates[17] bleiben von der vorliegenden Richtlinie unberührt.

5. Die Richtlinie 95/46/EG bleibt von der vorliegenden Richtlinie unberührt.

---

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

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

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

6a. Unbeschadet des Artikels 346 AEUV werden Informationen, die gemäß den Vorschriften der Union und der Mitgliedstaaten vertraulich sind, wie z.B. Vorschriften über das Geschäftsgeheimnis, mit der Kommission und anderen zuständigen Behörden nur ausgetauscht, wenn dies für die Anwendung dieser Richtlinie erforderlich ist. Der Informationsaustausch bleibt im Umfang so begrenzt, dass er im Hinblick auf das verfolgte Ziel relevant und angemessen ist. Bei diesem Informationsaustausch müssen die Vertraulichkeit der Informationen sowie die Sicherheit und die geschäftlichen Interessen der Betreiber wesentlicher Dienste und der Anbieter digitaler Dienste gewahrt bleiben.

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

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

Artikel 1a

Schutz und Verarbeitung personenbezogener Daten

1. Die Verarbeitung personenbezogener Daten gemäß dieser Richtlinie erfolgt im Einklang mit der Richtlinie 95/46/EG.

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

Artikel 1b

Freiwillige Meldung

1. Unbeschadet des Artikels 2 können Einrichtungen, die nicht als Betreiber wesentlicher Dienste ermittelt wurden und die keine Anbieter digitaler Dienste sind, auf freiwilliger Basis Sicherheitsvorfälle melden, die erhebliche Auswirkungen auf die Kontinuität der von ihnen angebotenen Dienste haben.

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

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

Artikel 2

Mindestharmonisierung

Unbeschadet des Artikels 15a Absatz 1b und ihrer Verpflichtungen nach dem Unionsrecht werden die Mitgliedstaaten nicht daran gehindert, Bestimmungen zu erlassen oder aufrechtzuerhalten, mit denen ein höheres Sicherheitsniveau von Netzen und Informationssystemen erreicht werden soll.

Artikel 3

Begriffsbestimmungen

Im Sinne dieser Richtlinie bezeichnet der Ausdruck

(1) "Netz und Informationssystem"

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

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

(c) die von den unter den Buchstaben a und b genannten Elementen zum Zwecke des Betriebs, der Nutzung, des Schutzes und der Pflege gespeicherten, verarbeiteten, abgerufenen oder übertragenen digitalen Daten;

(2) "Sicherheit von Netzen und Informationssystemen" die Fähigkeit von Netzen und Informationssystemen, bei einem bestimmten Vertrauensniveau alle Angriffe abzuwehren, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten oder entsprechender Dienste, die über diese Netze und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen;

(3) "Sicherheitsrisiko" alle mit vernünftigem Aufwand feststellbaren Umstände oder Ereignisse, die potenziell nachteilige Auswirkungen auf die Sicherheit von Netzen und Informationssystemen haben;

(4) "Sicherheitsvorfall" alle Ereignisse, die tatsächlich nachteilige Auswirkungen auf die Sicherheit von Netzen und Informationssystemen haben;

(6a) "nationale Strategie für die Sicherheit von Netzen und Informationssystemen" ("NIS-Strategie") ein Rahmenwerk mit strategischen Zielen und Prioritäten betreffend NIS auf nationaler Ebene;

(7) "Bewältigung von Sicherheitsvorfällen" alle Verfahren zur Unterstützung der Erkennung, Analyse, Eindämmung und Reaktion im Falle von Sicherheitsvorfällen;

(8) "Betreiber wesentlicher Dienste" eine öffentliche oder private Einrichtung einer in Anhang II genannten Art, die den Kriterien des Artikels 3a Absatz 1a entspricht;

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

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

(11d) "digitaler Dienst" einen Dienst im Sinne des Artikels 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates[18] einer in Anhang III genannten Art;

(11 da) "Anbieter digitaler Dienste" eine juristische Person, die einen digitalen Dienst anbietet;

(11e) "Online-Marktplatz" einen digitalen Dienst, der es Verbrauchern und/oder Unternehmern im Sinne des Artikels 4 Absatz 1 Buchstabe a bzw. Buchstabe b der Richtlinie 2013/11/EU des Europäischen Parlaments und des Rates[19] ermöglicht, entweder auf der Website des Online-Marktplatzes oder auf der Website eines Unternehmers, die von dem Online-Marktplatz bereitgestellte Rechendienste verwendet, Online-Kaufverträge und Online-Dienstleistungsverträge mit Unternehmern abzuschließen;

(11g) "Online-Suchmaschine" einen digitalen Dienst, der es Nutzern ermöglicht, Suchen grundsätzlich auf allen Websites oder auf Websites in einer bestimmten Sprache anhand einer Abfrage zu einem beliebigen Thema in Form eines Stichworts, einer Wortgruppe oder einer anderen Eingabe vorzunehmen, und der daraufhin Links anzeigt, über die Informationen im Zusammenhang mit dem angeforderten Inhalt gefunden werden können;

---

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

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

(11j) "Cloud-Computing-Dienst" einen digitalen Dienst, der den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglicht;

(11k) "Vertreter" eine in der Union niedergelassene natürliche oder juristische Person, die ausdrücklich benannt wurde, um im Auftrag eines nicht in der Union niedergelassenen Anbieters digitaler Dienste zu handeln, und an die sich die zuständige Behörde oder das CSIRT – statt an den Anbieter digitaler Dienste – hinsichtlich der Pflichten des Anbieters digitaler Dienste gemäß dieser Richtlinie wenden kann;

(11l) "Internet-Knoten" ("IXP" – Internet Exchange Point) eine Netzeinrichtung, die die Zusammenschaltung von mehr als zwei unabhängigen autonomen Systemen ermöglicht, in erster Linie zur Erleichterung des Austauschs von Internet-Datenverkehr. Ein IXP dient ausschließlich der Zusammenschaltung autonomer Systeme. Bei einem IXP ist es nicht erforderlich, dass der Internet-Datenverkehr zwischen zwei beliebigen teilnehmenden autonomen Systemen über ein drittes autonomes System läuft; der betreffende Datenverkehr wird auch weder verändert noch anderweitig beeinträchtigt;

(11m) "Domain-Namen-System-Diensteanbieter" eine Einrichtung, die DNS-Dienste im Internet anbietet (DNS ist ein hierarchisch unterteiltes Bezeichnungssystem in einem Netz zur Beantwortung von Anfragen zu Domain-Namen);

(11n) "Top-Level-Domain-Name-Registry" eine Einrichtung, die die Registrierung von Internet-Domain-Namen innerhalb einer spezifischen Top-Level-Domain (TLD) verwaltet und betreibt.

Artikel 3a

Ermittlung der Betreiber wesentlicher Dienste

1. Die Mitgliedstaaten ermitteln bis zum ... [6 Monate nach dem Datum in Artikel 21 Absatz 1] für jeden in Anhang II genannten Teilsektor die Betreiber wesentlicher Dienste mit einer Niederlassung in ihrem Hoheitsgebiet.

1a. Die in Artikel 3 Nummer 8 genannten Kriterien sind folgende:

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

(b) die Bereitstellung dieses Dienstes ist abhängig von Netzen und Informationssystemen;

(c) ein Sicherheitsvorfall im Zusammenhang mit den Netzen und Informationssystemen dieses Dienstes würde eine erhebliche Störung seiner Bereitstellung bewirken.

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

3. Stellt eine Einrichtung einen in Absatz 1a Buchstabe a genannten Dienst in zwei oder mehr Mitgliedstaaten bereit, so konsultieren diese Mitgliedstaaten einander für die Zwecke des Absatzes 1. Diese Konsultation erfolgt, bevor eine Entscheidung über die Ermittlung getroffen wird.

4. Die Mitgliedstaaten überprüfen das Verzeichnis der ermittelten Betreiber wesentlicher Dienste regelmäßig, mindestens jedoch alle zwei Jahre nach dem in Artikel 21 Absatz 1 genannten Zeitpunkt, und aktualisieren dieses gegebenenfalls.

5. Im Einklang mit den in Artikel 8a genannten Aufgaben obliegt es der Kooperationsgruppe, die Mitgliedstaaten dabei zu unterstützen, einen einheitlichen Ansatz im Hinblick auf die Ermittlung der Betreiber wesentlicher Dienste zu verfolgen.

6. Für die Zwecke der Überprüfung gemäß Artikel 20 übermitteln die Mitgliedstaaten spätestens sechs Monate nach dem Tag der Umsetzung, und danach alle zwei Jahre, der Kommission die Informationen, die sie benötigt, um die Durchführung dieser Richtlinie zu bewerten, insbesondere ob die Mitgliedstaaten bei der Ermittlung der Betreiber wesentlicher Dienste einen einheitlichen Ansatz verfolgen. Diese Informationen müssen mindestens Folgendes umfassen:

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

(b) die Liste der Dienste gemäß Absatz 2;

(c) die Zahl der in jedem der in Anhang II genannten Sektoren ermittelten Betreiber wesentlicher Dienste und einen Hinweis auf ihre Bedeutung in Bezug auf den jeweiligen Sektor;

(d) gegebenenfalls Schwellenwerte zur Bestimmung des einschlägigen Angebotsumfangs entsprechend der Zahl der Nutzer, die den jeweiligen Dienst in Anspruch nehmen, gemäß Artikel 3b Absatz 1 Buchstabe a oder entsprechend der Bedeutung des betreffenden Betreibers wesentlicher Dienste gemäß Artikel 3b Absatz 1 Buchstabe f.

Um zur Bereitstellung vergleichbarer Informationen beizutragen, kann die Kommission – unter größtmöglicher Berücksichtigung der Stellungnahme der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) – geeignete technische Leitlinien zu den Parametern für die in diesem Absatz genannten Informationen festlegen.

Artikel 3b

Erhebliche Störung

1. Bei der Bestimmung des Ausmaßes einer Störung gemäß Artikel 3a Absatz 1a Buchstabe c tragen die Mitgliedstaaten mindestens den folgenden sektorübergreifenden Faktoren Rechnung:

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

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

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

(d) Marktanteil der Einrichtung;

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

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

2. Bei der Bestimmung, ob ein Sicherheitsvorfall eine erhebliche Störung bewirken würde, tragen die Mitgliedstaaten gegebenenfalls auch sektorspezifischen Faktoren Rechnung.

KAPITEL II

NATIONALE RAHMEN FÜR DIE NETZ- UND INFORMATIONSSICHERHEIT

Artikel 5

Nationale NIS-Strategie

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

   (a) Die Ziele und Prioritäten der nationalen NIS-Strategie;

   (b) ein Steuerungsrahmen zur Erreichung der Ziele und Prioritäten der nationalen NIS-Strategie, wozu auch die Aufgaben und Zuständigkeiten der staatlichen Stellen und der anderen einschlägigen Akteure gehören;

   (c) die Bestimmung von Maßnahmen zur Abwehrbereitschaft, Reaktion und Wiederherstellung, wozu auch die Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor gehört;

   (d) eine Aufstellung der Ausbildungs-, Aufklärungs- und Schulungsprogramme im Zusammenhang mit der NIS-Strategie;

(e) eine Aufstellung der Forschungs- und Entwicklungspläne im Zusammenhang mit der NIS-Strategie;

(f) ein Risikobewertungsplan zur Bestimmung möglicher Sicherheitsrisiken;

(g) eine Auflistung der verschiedenen Akteure, die an der Umsetzung der NIS-Strategie beteiligt sind.

2a. Die Mitgliedstaaten können die ENISA um Unterstützung bei der Ausarbeitung der nationalen NIS-Strategien ersuchen.

3. Die nationale NIS-Strategie wird der Kommission innerhalb von drei Monaten nach ihrer Festlegung mitgeteilt. Dabei können die Mitgliedstaaten die Elemente der Strategie, die die nationale Sicherheit berühren, ausklammern.

Artikel 6

Nationale zuständige Behörden und zentrale Anlaufstelle

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

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

2a. Jeder Mitgliedstaat benennt eine für die Sicherheit von Netzen und Informationssystemen zuständige nationale zentrale Anlaufstelle (im Folgenden "zentrale Anlaufstelle"). Die Mitgliedstaaten können diese Funktion einer bestehenden Behörde zuweisen. Benennt ein Mitgliedstaat nur eine zuständige Behörde, so ist diese zuständige Behörde auch die zentrale Anlaufstelle.

2c. Die zentrale Anlaufstelle dient als Verbindungsstelle zur Gewährleistung der Zusammenarbeit der Behörden der Mitgliedstaaten untereinander und der grenzüberschreitenden Zusammenarbeit mit den entsprechenden Behörden in anderen Mitgliedsaaten sowie mit der Kooperationsgruppe und dem CSIRT-Netz.

3. Die Mitgliedstaaten gewährleisten, dass die benannten zuständigen Behörden und zentralen Anlaufstellen mit angemessenen Ressourcen ausgestattet sind, damit sie die ihnen übertragenen Aufgaben wirksam und effizient wahrnehmen können und die Ziele dieser Richtlinie somit erreicht werden. Die Mitgliedstaaten stellen eine wirksame, effiziente und sichere Zusammenarbeit der benannten Vertreter in der Kooperationsgruppe gemäß Artikel 8a sicher.

4. Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden oder die CSIRT die gemäß dieser Richtlinie übermittelten Meldungen von Sicherheitsvorfällen erhalten.

4a. Damit die zentralen Anlaufstellen der Kooperationsgruppe einen zusammenfassenden Bericht über die Meldungen vorlegen können, stellen die Mitgliedstaaten sicher, dass die zuständigen Behörden oder die CSIRT die zentralen Anlaufstellen über die gemäß dieser Richtlinie übermittelten Meldungen von Sicherheitsvorfällen unterrichten.

4b. Die zentrale Anlaufstelle legt der Kooperationsgruppe einmal jährlich einen zusammenfassenden Bericht über die eingegangenen Meldungen, einschließlich der Zahl der Meldungen und der Art der gemeldeten Sicherheitsvorfälle, und über die ergriffenen Maßnahmen gemäß Artikel 14 Absatz 2, Artikel 14 Absatz 2ac und Artikel 15a Absatz 2 vor.

5. Die zuständigen Behörden und die zentrale Anlaufstelle konsultieren gegebenenfalls und im Einklang mit dem nationalen Recht die einschlägigen nationalen Strafverfolgungsbehörden und die nationalen Datenschutzbehörden und arbeiten mit ihnen zusammen.

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

Artikel 7

Computer-Notfallteams

1. Jeder Mitgliedstaat benennt ein oder mehrere Computer-Notfallteams (Computer Security Incident Response Teams, im Folgenden "CSIRT"), die mindestens die in Anhang II genannten Sektoren und die in Anhang III genannten digitalen Dienste abdecken und die für die Bewältigung von Sicherheitsvorfällen und Sicherheitsrisiken nach einem genau festgelegten Ablauf zuständig sind und die Anforderungen des Anhangs I Nummer 1 erfüllen. Ein CSIRT kann innerhalb einer zuständigen Behörde eingerichtet werden.

1a. Handelt es sich bei der zuständigen Behörde, der zentralen Anlaufstelle und den CSIRT desselben Mitgliedstaats um getrennte Einrichtungen, so arbeiten sie in Bezug auf die in dieser Richtlinie festgelegten Pflichten zusammen. Entscheidet ein Mitgliedstaat, dass die CSIRT keine Meldungen erhalten, so wird den CSIRT in dem zur Erfüllung ihrer Aufgaben erforderlich Umfang Zugang zu den Daten über Sicherheitsvorfälle gewährt, die von Betreibern wesentlicher Dienste gemäß Artikel 14 Absätze 2 und 2ac oder von Anbietern digitaler Dienste gemäß Artikel 15a Absatz 2 gemeldet werden.

2. Die Mitgliedstaaten gewährleisten, dass die benannten CSIRT mit angemessenen Ressourcen ausgestattet sind, damit sie ihre in Anhang I Nummer 2 aufgeführten Aufgaben wirksam wahrnehmen können.

   Die Mitgliedstaaten stellen sicher, dass ihre CSIRT im CSIRT-Netz gemäß Artikel 8b wirksam, effizient und sicher zusammenarbeiten.

3. Die Mitgliedstaaten stellen sicher, dass die benannten CSIRT Zugang zu einer angemessenen, sicheren und robusten Kommunikations- und Informationsinfrastruktur auf nationaler Ebene haben.

4. Die Mitgliedstaaten unterrichten die Kommission über den Auftrag der CSIRT sowie über die wichtigsten Elemente ihrer Verfahren zur Bewältigung von Sicherheitsvorfällen.

5c. Die Mitgliedstaaten können die ENISA um Unterstützung bei der Einsetzung nationaler CSIRT ersuchen.

KAPITEL III

ZUSAMMENARBEIT ZWISCHEN DEN ZUSTÄNDIGEN BEHÖRDEN

Artikel 8a

Kooperationsgruppe

1. Zur Unterstützung und Erleichterung der strategischen Zusammenarbeit zwischen den Mitgliedstaaten, zum Aufbau von Vertrauen und im Hinblick auf die Erreichung eines hohen gemeinsamen Sicherheitsniveaus von Netzen und Informationssystemen in der Union wird eine Kooperationsgruppe eingesetzt.

   Die Kooperationsgruppe nimmt ihre Aufgaben auf der Grundlage von zweijährlichen Arbeitsprogrammen gemäß Artikel 8a Absatz 3 Buchstabe a wahr.

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

   Die Sekretariatsgeschäfte werden von der Kommission geführt.

   Gegebenenfalls kann die Kooperationsgruppe Vertreter der einschlägigen Interessenträger einladen, an ihren Arbeiten teilzunehmen.

3. Die Kooperationsgruppe hat folgende Aufgaben:

a. Bis spätestens ... [18 Monate nach Inkrafttreten dieser Richtlinie] und danach alle zwei Jahre Erstellung eines Arbeitsprogramms bezüglich der Maßnahmen, die zur Umsetzung der Ziele und Aufgaben zu ergreifen sind, im Einklang mit den Zielen dieser Richtlinie;

b. Bereitstellung strategischer Leitlinien für die Tätigkeiten des gemäß Artikel 8b errichteten CSIRT-Netzes;

c. Austausch von bewährten Verfahren und Informationen im Zusammenhang mit der Meldung von Sicherheitsvorfällen gemäß Artikel 14 Absatz 2ac und Artikel 15a Absatz 2;

d. Austausch bewährter Verfahren zwischen den Mitgliedstaaten und – in Zusammenarbeit mit der ENISA – Unterstützung der Mitgliedstaaten beim Kapazitätenaufbau im Bereich NIS;

e. Erörterung der Fähigkeiten und der Abwehrbereitschaft der Mitgliedstaaten und Bewertung – auf freiwilliger Basis – der nationalen NIS-Strategien und der Wirksamkeit der CSIRT, sowie Bestimmung bewährter Verfahren;

f. Austausch von Informationen und bewährten Verfahren zu Sensibilisierung und Schulung;

g. Austausch von Informationen und bewährten Verfahren zu Forschung und Entwicklung bezüglich der Netz- und Informationssicherheit;

h. gegebenenfalls Erfahrungsaustausch zu NIS-bezogenen Angelegenheiten mit den einschlägigen Organen, Einrichtungen und sonstigen Stellen der Union;

i. Erörterung der in Artikel 16 genannten Normen mit Vertretern der einschlägigen europäischen Normungsorganisationen;

j. Erhebung bewährter Verfahren zu Sicherheitsrisiken und Sicherheitsvorfällen in Verbindung mit Netzen und Informationssystemen;

k. jährliche Prüfung der zusammenfassenden Berichte gemäß Artikel 6 Absatz 4b;

l. Erörterung der durchgeführten Arbeiten in Bezug auf NIS-Übungen, Ausbildungsprogramme und Schulung, einschließlich der Arbeit der ENISA;

m. Austausch bewährter Verfahren – mit Unterstützung der ENISA – bezüglich der Ermittlung der Betreiber wesentlicher Dienste durch die Mitgliedstaaten, auch im Zusammenhang mit grenzüberschreitenden Abhängigkeiten hinsichtlich NIS-Sicherheitsrisiken und Sicherheitsvorfällen;

n. Erörterung der Modalitäten für die Berichterstattung über die Meldung von Sicherheitsvorfällen gemäß den Artikeln 14 und 15a.

4. Als Beitrag zur regelmäßigen Überprüfung des Funktionierens dieser Richtlinie durch die Kommission erstellt die Kooperationsgruppe alle 18 Monate einen Bericht, in dem die im Rahmen der strategischen Zusammenarbeit nach diesem Artikel gewonnenen Erfahrungen bewertet werden.

5. Die Kommission legt im Wege von Durchführungsrechtsakten die für das Funktionieren der Kooperationsgruppe erforderlichen Verfahrensmodalitäten fest. Diese Durchführungsrechtsakte werden nach dem in Artikel 19 Absatz 3 genannten Prüfverfahren erlassen. Für die Zwecke des Unterabsatzes 1 legt die Kommission dem Ausschuss den ersten Entwurf eines Durchführungsrechtsakts spätestens am ... [6 Monate nach Inkrafttreten dieser Richtlinie] vor.

Artikel 8b

CSIRT-Netz

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

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

3. Das CSIRT-Netz hat folgende Aufgaben:

   a. Informationsaustausch zu den Diensten, Tätigkeiten und Kooperationsfähigkeiten der CSIRT;

   b. auf Antrag des Vertreters eines von einem Sicherheitsvorfall potenziell betroffenen Mitgliedstaats Austausch und Erörterung von wirtschaftlich nicht sensiblen Informationen im Zusammenhang mit diesem Sicherheitsvorfall und damit verbundenen Sicherheitsrisiken. Ein Mitgliedstaat kann die Beteiligung an diesen Erörterungen ablehnen, wenn die Gefahr einer Beeinträchtigung der Untersuchung des Sicherheitsvorfalls besteht;

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

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

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

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

(i) Kategorien von Sicherheitsrisiken und Sicherheitsvorfällen,

(ii) Frühwarnungen,

(iii) gegenseitiger Amtshilfe,

(iv) Grundsätzen und Modalitäten der Koordinierung hinsichtlich der Reaktion der Mitgliedstaaten auf grenzüberschreitende NIS-Sicherheitsrisiken und Sicherheitsvorfälle;

g. Unterrichtung der Kooperationsgruppe über seine Tätigkeiten und über die gemäß Absatz 3 Buchstabe f erörterten weiteren Formen der operativen Zusammenarbeit, und Ersuchen um entsprechende Leitlinien;

h. Erörterung der aus den NIS-Übungen, auch den von der ENISA organisierten derartigen Übungen – gezogenen Lehren;

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

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

4. Als Beitrag zur regelmäßigen Überprüfung des Funktionierens dieser Richtlinie durch die Kommission erstellt das CSIRT-Netz alle 18 Monate einen Bericht, in dem die im Rahmen der operativen Zusammenarbeit nach diesem Artikel gewonnenen Erfahrungen, wozu auch Schlussfolgerungen und Empfehlungen gehören, bewertet werden. Dieser Bericht wird auch der Kooperationsgruppe übermittelt.

5. Das CSIRT-Netz gibt sich eine Geschäftsordnung.

Artikel 13

Internationale Zusammenarbeit

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

KAPITEL IV

SICHERHEIT DER NETZE UND INFORMATIONSSYSTEME DER BETREIBER WESENTLICHER DIENSTE

Artikel 14

Sicherheitsanforderungen und Meldung von Sicherheitsvorfällen

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

1a. Die Mitgliedstaaten stellen sicher, dass die Betreiber wesentlicher Dienste geeignete Maßnahmen ergreifen, um den Auswirkungen von Sicherheitsvorfällen, die die Sicherheit der von ihnen für die Bereitstellung dieser wesentlichen Dienste genutzten Netze und Informationssysteme beeinträchtigen, vorzubeugen beziehungsweise diese so gering wie möglich zu halten, damit die Kontinuität dieser Dienste gewährleistet wird.

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

2a. Zur Feststellung des Ausmaßes der Auswirkungen eines Sicherheitsvorfalls werden insbesondere folgende Parameter berücksichtigt:

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

(b) Dauer des Sicherheitsvorfalls;

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

2ac. Auf der Grundlage der von dem Betreiber wesentlicher Dienste bereitgestellten Informationen unterrichtet die zuständige Behörde oder das CSIRT, der bzw. dem die Meldung erstattet wurde, etwaige andere betroffene Mitgliedstaaten, sofern der Sicherheitsvorfall erhebliche Auswirkungen auf die Kontinuität wesentlicher Dienste in den betreffenden Mitgliedstaaten hat. Dabei wahrt die zuständige Behörde oder das CSIRT im Einklang mit dem Unionsrecht oder mit den dem Unionsrecht entsprechenden nationalen Rechtsvorschriften die Sicherheit und das wirtschaftliche Interesse des Betreibers sowie die Vertraulichkeit der von diesem bereitgestellten Informationen.

Wenn es nach den Umständen möglich ist, stellt die zuständige Behörde oder das CSIRT dem die Meldung erstattenden Betreiber wesentlicher Dienste alle einschlägigen Informationen in Bezug auf die Weiterverfolgung der Meldung eines Sicherheitsvorfalls, wie etwa Informationen, die für die wirksame Bewältigung des Sicherheitsvorfalls von Nutzen sein könnten, zur Verfügung.

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

4. Nach Anhörung des betreffenden Betreibers wesentlicher Dienste können die zuständige Behörde oder das CSIRT, der bzw. dem die Meldung erstattet wurde, die Öffentlichkeit über einzelne Sicherheitsvorfälle unterrichten, sofern die Sensibilisierung der Öffentlichkeit zur Verhütung von Sicherheitsvorfällen oder zur Bewältigung aktueller Sicherheitsvorfälle erforderlich ist.

6. Die im Rahmen der Kooperationsgruppe gemeinsam handelnden zuständigen Behörden können Leitlinien zu den Umständen, unter denen die Betreiber wesentlicher Dienste Sicherheitsvorfälle melden müssen, ausarbeiten und annehmen; dies gilt auch für die Parameter zur Feststellung des Ausmaßes der Auswirkungen eines Sicherheitsvorfalls gemäß Absatz 2a.

Artikel 15

Umsetzung und Durchsetzung

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

2. Die Mitgliedstaaten gewährleisten, dass die zuständigen Behörden über die Befugnisse und Mittel verfügen, um von den Betreibern wesentlicher Dienste verlangen zu können, dass sie

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

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

   Die zuständigen Behörden nennen bei Übermittlung ihres Ersuchens dessen Zweck und geben an, welche Informationen verlangt werden.

3. Im Anschluss an die Bewertung der Informationen oder der Ergebnisse der in Absatz 2 genannten Sicherheitsüberprüfungen kann die zuständige Behörde den Betreibern wesentlicher Dienste verbindliche Anweisungen für Abhilfemaßnahmen im Interesse des Betriebs erteilen.

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

KAPITEL IVa

SICHERHEIT DER NETZE UND INFORMATIONSSYSTEME DER ANBIETER DIGITALER DIENSTE

Artikel 15a

Sicherheitsanforderungen und Meldung von Sicherheitsvorfällen

1. Die Mitgliedstaaten stellen sicher, dass die Anbieter digitaler Dienste geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netze und Informationssysteme, die sie im Rahmen der Erbringung der in Anhang III aufgeführten Dienste innerhalb der Union für ihre Tätigkeiten nutzen, zu bewältigen. Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik ein Niveau der Sicherheit der Netze und Informationssysteme gewährleisten, das dem bestehenden Sicherheitsrisiko angemessen ist, wobei folgenden Elementen Rechnung getragen wird:

   - Sicherheit der Systeme und Anlagen,

   - Bewältigung von Sicherheitsvorfällen,

   - Betriebskontinuitätsmanagement,

   - Überwachung, Überprüfung und Erprobung,

   - Einhaltung der internationalen Normen.

1a. Es werden insbesondere Maßnahmen getroffen, um den Auswirkungen von Sicherheitsvorfällen, die die Sicherheit der Netze und Informationssysteme des Anbieters digitaler Dienste bei den in Anhang III genannten, innerhalb der Union erbrachten Diensten beeinträchtigen, vorzubeugen beziehungsweise diese so gering wie möglich zu halten, um die Kontinuität dieser Dienste sicherzustellen.

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

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

2a. Zur Feststellung der Auswirkungen eines Sicherheitsvorfalls werden die folgenden Parameter zugrunde gelegt, und zwar insbesondere

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

(b) Dauer des Sicherheitsvorfalls;

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

(d) Ausmaß der Unterbrechung der Bereitstellung des Dienstes;

(e) Ausmaß der Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten.

Die Pflicht zur Meldung eines Sicherheitsvorfalls gilt nur, wenn der Anbieter digitaler Dienste Zugang zu den Informationen hat, die benötigt werden, um zu ermessen, ob die Kriterien erfüllt sind.

2b. Nimmt ein Betreiber wesentlicher Dienste für die Bereitstellung eines Dienstes, der für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten von wesentlicher Bedeutung ist, die Dienste eines Dritten als Anbieter digitaler Dienste in Anspruch, so hat der Betreiber wesentlicher Dienste jede erhebliche Auswirkung auf die Kontinuität der wesentlichen Dienste, die von einem den Anbieter digitaler Dienste beeinträchtigenden Sicherheitsvorfall verursacht wurde, zu melden.

3. Gegebenenfalls unterrichtet die zuständige Behörde oder das CSIRT, der bzw. dem die Meldung erstattet wurde, andere betroffene Mitgliedstaaten; dies gilt insbesondere, wenn der in Absatz 2 genannte Sicherheitsvorfall zwei oder mehr Mitgliedstaaten betrifft. Dabei wahren die zuständigen Behörden, CSIRT und zentralen Anlaufstellen im Einklang mit dem Unionsrecht oder mit den dem Unionsrecht entsprechenden nationalen Rechtsvorschriften die Sicherheit und das wirtschaftliche Interesse des Anbieters digitaler Dienste sowie die Vertraulichkeit der bereitgestellten Informationen.

Nach Anhörung des betreffenden Anbieters digitaler Dienste können die zuständige Behörde oder das CSIRT, der bzw. dem die Meldung erstattet wurde, und gegebenenfalls die Behörden oder CSIRT anderer betroffener Mitgliedstaaten die Öffentlichkeit über einzelne Sicherheitsvorfälle unterrichten oder verlangen, dass der Anbieter digitaler Dienste dies unternimmt, sofern die Sensibilisierung der Öffentlichkeit notwendig ist, um einem Sicherheitsvorfall vorzubeugen oder ihn zu bewältigen, oder wenn die Offenlegung des Sicherheitsvorfalls auf sonstige Weise im öffentlichen Interesse liegt.

4. Der Kommission wird die Befugnis übertragen, gemäß Artikel 19 Absatz 3 Durchführungsrechtsakte zu erlassen, um die in Absatz 1 aufgeführten Elemente genauer zu bestimmen. Diese Durchführungsrechtsakte werden bis zum ... [ein Jahr nach dem Inkrafttreten dieser Richtlinie] erlassen.

4a. Der Kommission wird die Befugnis übertragen, gemäß Artikel 19 Absatz 3 Durchführungsrechtsakte zu erlassen, um die in Absatz 2 aufgeführten Parameter zu bestimmen. Diese Durchführungsrechtsakte werden bis zum ... [ein Jahr nach dem Inkrafttreten dieser Richtlinie] erlassen.

4b. Die Kommission kann im Wege von Durchführungsrechtsakten Form und Verfahren der vorgeschriebenen Meldungen festlegen. Diese Durchführungsrechtsakte werden nach dem in Artikel 19 Absatz 3 genannten Prüfverfahren angenommen.

5. Dieses Kapitel gilt nicht für Kleinstunternehmen und kleine Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission[20].

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

Artikel 15b/c

Umsetzung und Durchsetzung

1. Die Mitgliedstaaten gewährleisten, dass die zuständigen Behörden erforderlichenfalls im Wege von Ex-post-Überwachungsmaßnahmen tätig werden, wenn ihnen Nachweise dafür vorlegt werden, dass ein Anbieter digitaler Dienste die in Artikel 15a niedergelegten Anforderungen nicht einhält. Derartige Nachweise können von der zuständigen Behörde eines anderen Mitgliedstaats, in dem der Dienst bereitgestellt wird, vorgelegt werden.

2. Für die Zwecke des Absatzes 1 müssen die zuständigen Behörden über die erforderlichen Befugnisse und Mittel verfügen, um

   (a) von den Anbietern digitaler Dienste zu verlangen, die zur Beurteilung der Sicherheit ihrer Netze und Informationssysteme erforderlichen Informationen, einschließlich der Unterlagen über ihre Sicherheitsmaßnahmen, zu übermitteln;

   (b) von den Anbietern digitaler Dienste zu verlangen, bei jedem Fall von Nichteinhaltung der in Artikel 15a niedergelegten Anforderungen Abhilfe zu schaffen.

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

Artikel 15c/d

Gerichtliche Zuständigkeit und Territorialität

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

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

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

KAPITEL IVb

NORMUNG

Artikel 16

Normung

1. Um eine einheitliche Anwendung des Artikels 14 Absätze 1 und 1a und des Artikels 15a Absätze 1 und 1a zu gewährleisten, fördern die Mitgliedstaaten ohne Auferlegung oder willkürliche Bevorzugung der Verwendung einer bestimmten Technologieart die Anwendung europäischer oder international anerkannter Normen und/oder Spezifikationen für die Sicherheit von Netzen und Informationssystemen.

1a. Die ENISA arbeitet in Zusammenarbeit mit den Mitgliedstaaten Beratung und Leitlinien zu den technischen Bereichen aus, die in Bezug auf Absatz 1 in Betracht gezogen werden sollten, sowie zu den bereits bestehenden Normen – einschließlich der nationalen Normen der Mitgliedstaaten –, von denen diese Bereiche erfasst werden könnten.

KAPITEL V

SCHLUSSBESTIMMUNGEN

Artikel 17

Sanktionen

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

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.

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

Artikel 20

Überprüfung

1. Die Kommission legt dem Europäischen Parlament und dem Rat ein Jahr nach dem Zeitpunkt der Umsetzung einen Bericht vor, in dem die Kohärenz der Ansätze der Mitgliedstaaten für die Ermittlung der Betreiber wesentlicher Dienste bewertet wird.

2. Die Kommission überprüft regelmäßig die Anwendung dieser Richtlinie und erstattet dem Europäischen Parlament und dem Rat Bericht. Zu diesem Zweck berücksichtigt die Kommission im Hinblick auf die weitere Förderung der strategischen und operativen Zusammenarbeit die Berichte der Kooperationsgruppe und des CSIRT-Netzes über die auf strategischer und operativer Ebene gemachten Erfahrungen. Bei ihrer Überprüfung bewertet die Kommission ferner die in den Anhängen II und III enthaltene Liste und die Kohärenz bei der Ermittlung der Betreiber wesentlicher Dienste und der Dienste in den in Anhang II genannten Sektoren. Der erste Bericht wird spätestens drei Jahre nach dem Tag vorgelegt, auf den in Artikel 21 Absatz 1 Bezug genommen wird.

Artikel 20a

Übergangsmaßnahmen

1. Unbeschadet des Artikels 21 beginnen die Kooperationsgruppe und das CSIRT-Netz mit der Erfüllung ihrer in Artikel 8a Absatz 3 beziehungsweise Artikel 8b Absatz 3 niedergelegten Aufgaben spätestens sechs Monate nach dem Tag des Inkrafttretens dieser Richtlinie mit dem Ziel, den Mitgliedstaaten weitere Optionen für eine angemessene Zusammenarbeit während des Übergangszeitraums zu ermöglichen.

1a. Im Zeitraum zwischen den in Absatz 1 und in Artikel 3a Absatz 1 genannten Zeitpunkten erörtert die Kooperationsgruppe im Hinblick auf die Unterstützung der Mitgliedstaaten bei einem kohärenten Ansatz für den Prozess der Ermittlung der Betreiber wesentlicher Dienste Verfahren, Inhalt und Art der nationalen Maßnahmen, die die Ermittlung der Betreiber wesentlicher Dienste in einem spezifischen Sektor gemäß den in den Artikeln 3a und 3b festgelegten Kriterien gestatten. Die Kooperationsgruppe erörtert ferner auf Ersuchen eines Mitgliedstaats einen Entwurf spezifischer Maßnahmen dieses Mitgliedstaats, die die Ermittlung von Betreibern wesentlicher Dienste in einem spezifischen Sektor gemäß den in den Artikeln 3a und 3b festgelegten Kriterien gestatten.

2. Innerhalb eines Zeitraums von sechs Monaten ab dem Tag des Inkrafttretens dieser Richtlinie sorgen die Mitgliedstaaten für die Zwecke dieses Artikels für ihre angemessene Vertretung in der Kooperationsgruppe und im CSIRT-Netz.

Artikel 21

Umsetzung

1. Die Mitgliedstaaten erlassen und veröffentlichen bis zum ... [21 Monate nach dem Tag des Inkrafttretens dieser Richtlinie] die Rechts- und Verwaltungsvorschriften, die erforderlich sind, um dieser Richtlinie nachzukommen. Sie teilen der Kommission unverzüglich den Wortlaut dieser Vorschriften mit.

2. Sie wenden diese Maßnahmen ab dem Tag an, der auf den Tag folgt, auf den in Absatz 1 Bezug genommen wird.

3. 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.

4. 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 … am ...

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

Computer Security Incident Response Team (CSIRT) – Anforderungen und Aufgaben

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

(1) Anforderungen an das CSIRT

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

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

(e) Betriebskontinuität:

- Das CSIRT muss über ein geeignetes System zur Verwaltung und Weiterleitung von Anfragen verfügen, um Übergaben zu erleichtern.

- Das CSIRT muss personell so ausgestattet sein, dass es eine ständige Verfügbarkeit gewährleisten kann.

- Das CSIRT muss auf eine Infrastruktur gestützt sein, deren Kontinuität sichergestellt ist. Zu diesem Zweck müssen Redundanzsysteme und Ausweicharbeitsräume zur Verfügung stehen.

(f) Die CSIRTs müssen die Möglichkeit haben, sich gegebenenfalls an internationalen Kooperationsnetzen zu beteiligen.

(2) Aufgaben des CSIRT

(a) Die Aufgaben des CSIRT müssen mindestens Folgendes umfassen:

- Überwachung von Sicherheitsvorfällen auf nationaler Ebene;
- Ausgabe von Frühwarnungen und Alarmmeldungen sowie Bekanntmachung und Verbreitung von Informationen über Sicherheitsrisiken und -vorfälle unter den einschlägigen Akteuren;

- Reaktion auf Sicherheitsvorfälle;

- dynamische Analyse von Sicherheitsrisiken und -vorfällen und Lagebeurteilung;

- Beteiligung am CSIRT-Netz.

(b) Das CSIRT baut Kooperationsbeziehungen zum Privatsektor auf.

(c) Zur Erleichterung der Zusammenarbeit fördert das CSIRT die Annahme und Anwendung gemeinsamer oder standardisierter Verfahren für

- Abläufe zur Bewältigung von Sicherheitsvorfällen und -risiken;

- Systeme zur Klassifizierung von Sicherheitsvorfällen, Sicherheitsrisiken und Informationen.

Sektor	Teilsektor	Art der Einrichtung im Sinne des Artikels 3 Nummer 8
1. Energie	*a) Elektrizität*	Elektrizitätsunternehmen im Sinne des Artikels 2 Nummer 35 der Richtlinie 2009/72/EG des Europäischen Parlaments und des Rates[21], die die Funktion "Versorgung" im Sinne des Artikels 2 Nummer 19 jener Richtlinie wahrnehmen
		- Verteilernetzbetreiber im Sinne des Artikels 2 Nummer 6 der Richtlinie 2009/72/EG
		- Übertragungsnetzbetreiber im Sinne des Artikels 2 Nummer 4 der Richtlinie 2009/72/EG
	b) Erdöl	- Betreiber von Erdöl-Fernleitungen
		- Betreiber von Anlagen zur Produktion, Raffination und Aufbereitung von Erdöl sowie Betreiber von Erdöllagern und Erdöl-Fernleitungen

[21] Richtlinie 2009/72/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 über gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt und zur Aufhebung der Richtlinie 2003/54/EG (ABl. L 211 vom 14.8.2009, S. 55).

	c) Erdgas	- Versorgungsunternehmen im Sinne des Artikels 2 Nummer 8 der Richtlinie 2009/73/EG des Europäischen Parlaments und des Rates[22];
		- Verteilernetzbetreiber im Sinne des Artikels 2 Nummer 6 der Richtlinie 2009/73/EG
		- Fernleitungsnetzbetreiber im Sinne des Artikels 2 Nummer 4 der Richtlinie 2009/73/EG
		- Betreiber einer Speicheranlage im Sinne des Artikels 2 Nummer 10 der Richtlinie 2009/73/EG
		- Betreiber einer LNG-Anlage im Sinne des Artikels 2 Nummer 12 der Richtlinie 2009/73/EG
		- Erdgasunternehmen im Sinne des Artikels 2 Nummer 1 der Richtlinie 2009/73/EG
		- Betreiber von Anlagen zur Raffination und Aufbereitung von Erdgas

[22] Richtlinie 2009/73/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 über gemeinsame Vorschriften für den Erdgasbinnenmarkt und zur Aufhebung der Richtlinie 2003/55/EG (ABl. L 211 vom 14.8.2009, S. 94).

2. Verkehr	*(a) Luftverkehr*	- Luftfahrtunternehmen im Sinne des Artikels 3 Nummer 4 der Verordnung (EG) Nr. 300/2008 des Europäischen Parlaments und des Rates[23]
		- Flughafenleitungsorgane im Sinne des Artikels 2 Nummer 2 der Richtlinie 2009/12/EG des Europäischen Parlaments und des Rates[24], die Flughäfen im Sinne des Artikels 2 Nummer 1 jener Richtlinie – einschließlich der in Anhang II Abschnitt 2 der Verordnung (EU) Nr. 1315/2013 des Europäischen Parlaments und des Rates[25] aufgeführten Flughäfen des Kernnetzes – verwalten, und Einrichtungen, die innerhalb von Flughäfen befindliche zugehörige Einrichtungen betreiben.
		- Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen, die Flugverkehrskontrolldienste im Sinne des Artikels 2 Nummer 1 der Verordnung (EG) Nr. 549/2004 des Europäischen Parlaments und des Rates[26] bereitstellen
	(b) Schienenverkehr	- Infrastrukturbetreiber im Sinne des Artikels 3 Nummer 2 der Richtlinie 2012/34/EU des Europäischen Parlaments und des Rates[27]
		- Eisenbahnunternehmen im Sinne des Artikels 3 Nummer 1 der Richtlinie 2012/34/EU,

[23] Verordnung (EG) Nr. 300/2008 des Europäischen Parlaments und des Rates vom 11. März 2008 über gemeinsame Vorschriften für die Sicherheit in der Zivilluftfahrt und zur Aufhebung der Verordnung (EG) Nr. 2320/2002 (ABl. 97 vom 9.4.2008, S. 72).

[24] Richtlinie 2009/12/EG des Europäischen Parlaments und des Rates vom 11. März 2009 über Flughafenentgelte (ABl. L 70 vom 14.3.2009, S. 11).

[25] Verordnung (EU) Nr. 1315/2013 des Europäischen Parlaments und des Rates vom 11. Dezember 2013 über Leitlinien der Union für den Aufbau eines transeuropäischen Verkehrsnetzes und zur Aufhebung des Beschlusses Nr. 661/2010/EU (ABl. L 348 vom 20.12.2013, S. 1).

[26] Verordnung (EG) Nr. 549/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Festlegung des Rahmens für die Schaffung eines einheitlichen europäischen Luftraums ("Rahmenverordnung") (ABl. L 96 vom 31.3.2004, S. 1).

[27] Richtlinie 2012/34/EU des Europäischen Parlaments und des Rates vom 21. November 2012 zur Schaffung eines einheitlichen europäischen Eisenbahnraums (ABl. L 343 vom 14.12.2012, S. 32).

		einschließlich Betreiber einer Serviceeinrichtung im Sinne des Artikels 3 Nummer 12 jener Richtlinie
	(c) *Schifffahrt*	(i) Passagier- und Frachtbeförderungs-unternehmen der Binnen-, See- und Küstenschifffahrt, wie sie in Anhang I der Verordnung (EG) Nr. 725/2004 des Europäischen Parlaments und des Rates[28] für die Schifffahrt definiert sind, ausschließlich der einzelnen von diesen Unternehmen betriebenen Schiffe
		(ii) Leitungsorgane von Häfen im Sinne des Artikels 3 Nummer 1 der Richtlinie 2005/65/EG des Europäischen Parlaments und des Rates[29], einschließlich ihrer Hafenanlagen im Sinne des Artikels 2 Nummer 11 der Verordnung (EG) Nr. 725/2004, sowie Einrichtungen, die innerhalb von Häfen befindliche Anlagen und Ausrüstung betreiben.

[28] Verordnung (EG) Nr. 725/2004 des Europäischen Parlaments und des Rates vom 31. März 2004 zur Erhöhung der Gefahrenabwehr auf Schiffen und in Hafenanlagen (ABl. L 129 vom 29.4.2004, S. 6).

[29] Richtlinie 2005/65/EG des Europäischen Parlaments und des Rates vom 26. Oktober 2005 zur Erhöhung der Gefahrenabwehr in Häfen (ABl. L 310 vom 25.11.2005, S. 28).

		(iii) Betreiber von Schiffsverkehrsdiensten im Sinne des Artikels 3 Buchstabe o der Richtlinie 2002/59/EG des Europäischen Parlaments und des Rates[30]
	(d) Straßenverkehr	(i) Straßenverkehrsbehörden im Sinne des Artikels 2 Nummer 12 der Delegierten Verordnung (EU) 2015/962 der Kommission[31], die für Verkehrsmanagement- und Verkehrssteuerung verantwortlich sind.
		(ii) Betreiber intelligenter Verkehrssysteme im Sinne des Artikels 4 Nummer 1 der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates[32]

30 Richtlinie 2002/59/EG des Europäischen Parlaments und des Rates vom 27. Juni 2002 über die Einrichtung eines gemeinschaftlichen Überwachungs- und Informationssystems für den Schiffsverkehr und zur Aufhebung der Richtlinie 93/75/EWG des Rates (ABl. L 208 vom 5.8.2002, S. 10).

31 Delegierte Verordnung (EU) 2015/962 der Kommission vom 18. Dezember 2014 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates hinsichtlich der Bereitstellung EU-weiter Echtzeit-Verkehrsinformationsdienste (ABl. L 157 vom 23.6.2015, S. 21).

32 Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates vom 7. Juli 2010 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern (ABl. L 207 vom 6.8.2010, S. 1).

3. Bankwesen		- Kreditinstitute im Sinne des Artikels 4 Nummer 1 der Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates[33]
4. Finanzmarktinfrastrukturen		- Betreiber von Handelsplätzen im Sinne des Artikels 4 der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates[34]
		- zentrale Gegenparteien im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates[35]
5. Gesundheitswesen	Einrichtungen der medizinischen Versorgung (einschließlich Krankenhäuser und Privatkliniken)	- Gesundheitsdienstleister im Sinne des Artikels 3 Buchstabe g der Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates[36]

[33] Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen und zur Änderung der Verordnung (EU) Nr. 648/2012 (ABl. L 176 vom 27.6.2013, S. 1).

[34] Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU (ABl. L 173 vom 12.6.2014, S. 349).

[35] Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates vom 4. Juli 2012 über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister (ABl. L 201 vom 27.7.2012, S. 1).

[36] Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung (ABl. L 88 vom 4.4.2011, S. 45).

6. Trinkwasserlieferung und -versorgung		Lieferanten von und Unternehmen der Versorgung mit "Wasser für den menschlichen Gebrauch" im Sinne des Artikels 2 Nummer 1 Buchstabe a der Richtlinie 98/83/EG des Rates[37], jedoch unter Ausschluss der Lieferanten, für die die Lieferung von Wasser für den menschlichen Gebrauch nur ein Teil ihrer allgemeinen Tätigkeit der Lieferung von Rohstoffen und Gütern ist.
7. Digitale Infrastruktur		Internet-Knoten
		Domain-Namen-System-Diensteanbieter
		Top-Level-Domain-Name-Registries

[37] Richtlinie 98/83/EG des Rates vom 3. November 1998 über die Qualität von Wasser für den menschlichen Gebrauch (ABl. L 330 vom 5.12.1998, S. 32).

Arten digitaler Dienste im Sinne des Artikels 3 Nummer 11d

1. Online-Marktplatz

2. Online-Suchmaschine

3. Cloud-Computing-Dienst