I

(Gesetzgebungsakte)

RICHTLINIEN

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

vom 6. Juli 2016

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

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

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

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

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

gemäß dem ordentlichen Gesetzgebungsverfahren ([2]),

in Erwägung nachstehender Gründe:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

HABEN FOLGENDE RICHTLINIE ERLASSEN:

KAPITEL I

ALLGEMEINE BESTIMMUNGEN

Artikel 1

Gegenstand und Anwendungsbereich

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

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

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

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

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

---

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

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

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

[4] ABl. C 32 vom 4.2.2014, S. 19.

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

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

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

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

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

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

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

Artikel 2

Verarbeitung personenbezogener Daten

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

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

Artikel 3

Mindestharmonisierung

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

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

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

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

Artikel 4

Begriffsbestimmungen

Für die Zwecke dieser Richtlinie bezeichnet der Ausdruck

1. „Netz- und Informationssystem“

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Artikel 5

Ermittlung der Betreiber wesentlicher Dienste

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

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

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

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

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

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

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

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

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

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

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

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

b) die Liste der Dienste gemäß Absatz 3;

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

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

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

Artikel 6

Erhebliche Störung

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

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

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

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

d) Marktanteil dieser Einrichtung;

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

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

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

KAPITEL II

NATIONALE RAHMEN FÜR DIE SICHERHEIT VON NETZ- UND INFORMATIONSSYSTEMEN

Artikel 7

Nationale Strategie für die Sicherheit von Netz- und Informationssystemen

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

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

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

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

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

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

f) einen Risikobewertungsplan zur Bestimmung von Risiken;

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

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

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

Artikel 8

Nationale zuständige Behörden und zentrale Anlaufstelle

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

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

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

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

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

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

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

Artikel 9

Computer-Notfallteams (CSIRTs)

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

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

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

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

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

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

Artikel 10

Zusammenarbeit auf nationaler Ebene

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

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

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

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

KAPITEL III

ZUSAMMENARBEIT

Artikel 11

Kooperationsgruppe

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

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

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

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

Die Sekretariatsgeschäfte werden von der Kommission geführt.

(3) Die Kooperationsgruppe hat folgende Aufgaben:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Artikel 12

CSIRTs-Netzwerk

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

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

(3) Das CSIRTs-Netzwerk hat folgende Aufgaben:

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

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

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

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

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

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

   i) Kategorien von Risiken und Sicherheitsvorfällen,

   ii) Frühwarnungen,

   iii) gegenseitiger Unterstützung,

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

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

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

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

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

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

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

Artikel 13

Internationale Zusammenarbeit

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

KAPITEL IV

SICHERHEIT DER NETZ- UND INFORMATIONSSYSTEME DER BETREIBER WESENTLICHER DIENSTE

Artikel 14

Sicherheitsanforderungen und Meldung von Sicherheitsvorfällen

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

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

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

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

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

b) Dauer des Sicherheitsvorfalls;

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

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

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

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

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

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

Artikel 15

Umsetzung und Durchsetzung

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

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

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

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

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

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

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

KAPITEL V

SICHERHEIT DER NETZ- UND INFORMATIONSSYSTEME DER ANBIETER DIGITALER DIENSTE

Artikel 16

Sicherheitsanforderungen und Meldung von Sicherheitsvorfällen

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

a) Sicherheit der Systeme und Anlagen,

b) Bewältigung von Sicherheitsvorfällen,

c) Business continuity management,

d) Überwachung, Überprüfung und Erprobung,

e) Einhaltung der internationalen Normen.

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

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

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

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

b) Dauer des Sicherheitsvorfalls;

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

d) Ausmaß der Unterbrechung der Bereitstellung des Dienstes;

e) Ausmaß der Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten.

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

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

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

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

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

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

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

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

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

Artikel 17

Umsetzung und Durchsetzung

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

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

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

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

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

Artikel 18

Gerichtliche Zuständigkeit und Territorialität

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

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

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

KAPITEL VI

NORMUNG UND FREIWILLIGE MELDUNG

Artikel 19

Normung

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

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

Artikel 20

Freiwillige Meldung

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

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

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

KAPITEL VII

SCHLUSSBESTIMMUNGEN

Artikel 21

Sanktionen

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

Artikel 22

Ausschussverfahren

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

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

Artikel 23

Überprüfung

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

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

Artikel 24

Übergangsmaßnahmen

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

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

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

Artikel 25

Umsetzung

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

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

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

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

Artikel 26

Inkrafttreten

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

Artikel 27

Adressaten

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.

Geschehen zu Straßburg am 6. Juli 2016.

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

ANHANG I

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

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

1. Anforderungen an CSIRTs

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

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

   c) Betriebskontinuität:

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

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

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

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

2. Aufgaben der CSIRTs

   a) Die Aufgaben der CSIRTs umfassen mindestens Folgendes:

      i) Überwachung von Sicherheitsvorfällen auf nationaler Ebene;

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

      iii) Reaktion auf Sicherheitsvorfälle;

      iv) dynamische Analyse von Risiken und Vorfällen und Lagebeurteilung;

      v) Beteiligung am CSIRTs-Netzwerk.

   b) CSIRTs bauen Kooperationsbeziehungen zum Privatsektor auf.

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

      i) Abläufe zur Bewältigung von Sicherheitsvorfällen und Risiken;

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

ANHANG II

ARTEN VON EINRICHTUNGEN FÜR DIE ZWECKE DES ARTIKELS 4 NUMMER 4

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

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

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

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

ANHANG III

ARTEN DIGITALER DIENSTE IM SINNE DES ARTIKELS 4 NUMMER 5

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