EUROPÄISCHES PARLAMENT 2009 – 2014

Ausschuss für Industrie, Forschung und Energie

2013/0027(COD)

19.12.2013

STELLUNGNAHME

des Ausschusses für Industrie, Forschung und Energie

für den Ausschuss für Binnenmarkt und Verbraucherschutz

zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union
(COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

Verfasserin der Stellungnahme(*): del Pilar del Castillo Vera

(*) Assoziierter Ausschuss – Artikel 50 der Geschäftsordnung

PA_Legam

KURZE BEGRÜNDUNG

Im Februar 2013 legte die Kommission, wie vom Europäischen Parlament im Initiativbericht über eine Digitale Agenda für Europa gefordert, einen Vorschlag für eine Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union zusammen mit einer ersten Cybersicherheitsstrategie der EU vor. Laut Analyse der verfügbaren Daten könnten allein den kleinen und mittleren Unternehmen durch Vorfälle im Zusammenhang mit der IKT, die durch böswillige Absichten verursacht werden, schätzungsweise unmittelbare Kosten von mehr als 560 Millionen Euro pro Jahr entstehen. Alle Arten von Vorfällen zusammengenommen (einschließlich vorgelagerter Umwelt- oder physischer Probleme, wie Naturkatastrophen) könnten Kosten von mehr als 2,3 Milliarden verursachen. Unter Berücksichtigung dieser Fakten begrüßt die Verfasserin der Stellungnahme den Vorschlag ausdrücklich.

Hinsichtlich seiner Struktur stimmt die Verfasserin der Stellungnahme einigen der vorgeschlagenen Maßnahmen zu, wie der Ausweitung der Bestimmungen zur Berichterstattung über Sicherheitsvorfälle, die zurzeit gemäß Artikel 13a der Rahmenrichtlinie von 2009 auf Anbieter öffentlicher Kommunikationsnetze beschränkt sind, auf weitere wichtige Infrastrukturbereiche. Dementsprechend finden Vorschläge wie die Forderung, dass alle Mitgliedstaaten über ordnungsgemäß funktionierende IT-Notfallteams (Computer Emergency Response Teams, CERTs) verfügen und eine zuständige Behörde als Teil eines sicheren europaweiten Netzes zum elektronischen Datenaustausch benennen müssen, um für die sichere gemeinsame Nutzung und den sicheren Austausch von Informationen zur Cybersicherheit zu sorgen, großen Anklang. Diese Vorschläge haben das Potenzial, erheblich zum Ziel der vorgeschlagenen Richtlinie beizutragen, nämlich der Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union.

Die Verfasserin der Stellungnahme ist jedoch der Ansicht, dass der Vorschlag noch verbessert werden kann, indem zwei Hauptgrundsätze angewendet werden: Effizienz und Vertrauen.

Der erste Grundsatz - Effizienz

Hinsichtlich der Verpflichtung der Mitgliedstaaten, eine zuständige Behörde zu benennen, welche die Anwendung der Richtlinie für alle in Anhang II des Vorschlags aufgeführten Sektoren überwachen soll, ist die Verfasserin der Stellungnahme der Ansicht, dass es jedem Mitgliedstaat freistehen muss, den seiner Meinung nach am besten geeigneten Steuerungsrahmen für Cybersicherheit zu wählen, und dass es zudem zwingend geboten ist, eine Dopplung institutioneller Strukturen zu vermeiden, die potenziell zu Kompetenzstreitigkeiten und dem Abbruch der Kommunikation führen kann. Dementsprechend ist die Verfasserin der Stellungnahme der Ansicht, dass vorhandene einzelstaatliche Strukturen, die bereits Wirksamkeit zeigen und die Anforderungen und verfassungsrechtlichen Vorschriften des Mitgliedstaats erfüllen, nicht zerstört werden sollten. Sie ist jedoch der Auffassung, dass jeder Mitgliedstaat eine **zentrale Anlaufstelle** benennen muss, um den Austausch von Informationen auf Unionsebene, Benachrichtigungen über

frühzeitige Warnungen vor Gefahren und die Teilnahme am Kooperationsnetz auf effiziente Weise sicherzustellen.

Um die Effizienz der vorgeschlagenen Richtlinie noch weiter zu erhöhen, ist die Einrichtung eines nationalen **CERT** (**Computer Emergency Response Team)** nach Ansicht der Verfasserin der Stellungnahme möglicherweise nicht die am besten geeignete Maßnahme, angesichts der Tatsache, dass diese Maßnahme die unterschiedlichen Arten und Zusammensetzungen der vorhandenen CERTs außer Acht lässt. Die meisten Mitgliedstaaten verfügen nicht nur über mehrere CERTs, diese sind auch noch für verschiedene Arten von Vorfällen zuständig. Die Quantität und Qualität der Tätigkeiten unterscheidet sich auch je nachdem, ob Hochschul- oder Forschungseinrichtungen, Behörden oder private Unternehmen diese Teams betreiben. Zudem würden durch den vorliegenden Vorschlag die vorhandenen internationalen und europäischen Kooperationsnetze zerschlagen, zu denen bereits vorhandene CERTs gehören, die sich bei der Koordinierung internationaler und europäischer Reaktionen auf Vorfälle bewährt haben. Folglich ist die Verfasserin der Stellungnahme der Ansicht, dass die Richtlinie, statt sich auf ein einziges nationales CERT zu beziehen, auf die CERTs ausgerichtet sein sollte, die den in Anhang II genannten Sektoren ihre Dienstleistungen bereitstellen und somit ermöglichen, dass beispielsweise ein CERT Dienstleistungen für alle in Anhang II genannten Sektoren erbringt oder dass verschiedene CERTs für ein und denselben Sektor Dienstleistungen erbringen. Die Verfasserin der Stellungnahme vertritt jedoch die Auffassung, dass Mitgliedsstaaten jederzeit die volle Funktionsfähigkeit ihrer CERTs sicherstellen und dafür sorgen müssen, dass diese mit ausreichenden technischen, finanziellen und personellen Mitteln ausgestattet sind, um angemessen handeln und an Kooperationsnetzen auf internationaler und gemeinschaftlicher Ebene teilnehmen zu können.

Das Wirtschaftlichkeitsgebot erfordert darüber hinaus Änderungen an der vorgeschlagenen Richtlinie hinsichtlich **des Geltungsbereichs**. Die Verfasserin der Stellungnahme teilt zwar die Ansicht, dass eine Ausweitung des Berichterstattungspflichten auf den Energie-, Verkehrs-, Gesundheits- und Finanzsektor notwendig ist, hält den Vorschlag für eine Ausweitung der in Kapitel IV ausgeführten Zwangsmaßnahmen auf alle Marktteilnehmer in der „Internetwirtschaft“ jedoch für unverhältnismäßig und unkontrollierbar. Unverhältnismäßig, weil die willkürliche Auferlegung neuer Verpflichtungen auf eine offene und nicht definierte Kategorie wie „Anbieter von Diensten der Informationsgesellschaft, die die Bereitstellung anderer Dienste der Informationsgesellschaft ermöglichen“ mit Blick auf etwaige, durch einen Sicherheitsvorfall verursachte Schäden nicht nur unverständlich sondern auch nicht hinreichend begründet ist und potenziell eine weitere Bürokratieebene für unsere Industriesektoren und insbesondere für KMU nach sich ziehen kann. Unkontrollierbar, weil ernste Zweifel bestehen, ob die zuständigen Behörden in der Lage sein würden, sich mit allen potenziellen Meldungen auf eine proaktive Weise auseinanderzusetzen, die einen Dialog mit Marktteilnehmern fördern würde, um die Sicherheitsbedrohung zu beseitigen.

In Bezug auf die **öffentlichen Verwaltungen** sollte die Richtlinie ein Gleichgewicht zwischen dem Bedarf für eine Weiterentwicklung der E-Government-Dienste und den bereits bestehenden Sorgfaltspflichten der öffentlichen Verwaltungen hinsichtlich der Verwaltung und des Schutzes ihrer Netze und Informationssysteme anstreben. Folglich ist die Verfasserin

der Stellungnahme der Auffassung, dass die in Artikel 14 festgelegten Anforderungen an den Informationsaustausch für öffentliche Verwaltungen uneingeschränkt gelten sollten, die in Artikel 15 aufgeführten Verpflichtungen jedoch nicht.

Der zweite Grundsatz - Vertrauen

Nach Ansicht der Verfasserin der Stellungnahme liegt der Erfolg der Richtlinie zum großen Teil in ihrer Fähigkeit, die Marktteilnehmer zu einer Mitwirkung zu bewegen, wodurch ein vertrauenswürdiges Umfeld für die Netz- und Informationssicherheit geschaffen werden könnte, in dem diejenigen vor Ort bereit sind, sich proaktiv zu beteiligen. Wenn die Richtlinie dies nicht erreicht, wird sie scheitern. In diesem Zusammenhang schlägt die Verfasserin der Stellungnahme vor zu garantieren, dass die Mitwirkung und Meldungen der Marktteilnehmer keine negativen Folgen durch unnötige Veröffentlichungen der von ihnen gemeldeten Sicherheitsvorfälle nach sich ziehen oder dass sie von den zuständigen Behörden oder zentralen Anlaufstellen für den Datenverlust zur Verantwortung gezogen werden. Darüber hinaus muss der Dialog zwischen Marktteilnehmern und zuständigen Behörden offen sein, und die Mitwirkung der Marktteilnehmer muss in allen Foren, einschließlich des Kooperationsnetzes, gefördert werden.

Die Verfasserin der Stellungnahme steht zudem auf dem Standpunkt, dass Vertrauen die Grundlage für die Mitwirkung der zuständigen Behörden bzw. der zentralen Anlaufstellen bilden sollte, insbesondere hinsichtlich des Informationsaustausches. Um dies sicherzustellen, sollten Bestimmungen zu den Anforderungen an Vertraulichkeit und Sicherheit des Netzes in der Richtlinie festgehalten werden.

ÄNDERUNGSANTRÄGE

Der Ausschuss für Industrie, Forschung und Energie ersucht den federführenden Ausschuss für Binnenmarkt und Verbraucherschutz, folgende Änderungsanträge in seinen Bericht zu übernehmen:

Änderungsantrag 1

Vorschlag für eine Richtlinie
Erwägung 1

Vorschlag der Kommission	*Geänderter Text*
(1) Netze und Informationssysteme mit den zugehörigen Diensten spielen eine zentrale Rolle in der Gesellschaft. Für die Wirtschaft und das Gemeinwohl und insbesondere für das Funktionieren des Binnenmarkts ist es von entscheidender	(1) Netze und Informationssysteme mit den zugehörigen Diensten spielen eine zentrale Rolle in der Gesellschaft. Für die ***Freiheit und die allgemeine Sicherheit der Bürgerinnen und Bürger der EU sowie für die*** Wirtschaft und das Gemeinwohl

Bedeutung, dass sie verlässlich und sicher sind.	und insbesondere für das Funktionieren des Binnenmarkts ist es von entscheidender Bedeutung, dass sie verlässlich und sicher sind.

Änderungsantrag 2

Vorschlag für eine Richtlinie
Erwägung 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die Tragweite und ***Häufigkeit vorsätzlicher wie unbeabsichtigter Sicherheitsvorfälle*** nehmen zu und stellen eine erhebliche Bedrohung für den störungsfreien Betrieb von Netzen und Informationssystemen dar. Solche Sicherheitsvorfälle können die Ausübung wirtschaftlicher Tätigkeiten beeinträchtigen, finanzielle Verluste verursachen, das Vertrauen ***der Nutzer*** untergraben und der Wirtschaft der Union großen Schaden zufügen.	(2) Die Tragweite***, Häufigkeit*** und ***Auswirkungen von Sicherheitsvorfällen*** nehmen zu und stellen eine erhebliche Bedrohung für den störungsfreien Betrieb von Netzen und Informationssystemen dar. ***Diese Systeme können auch zu einem leichten Angriffsziel vorsätzlich schädigender Handlungen werden, die auf die Schädigung oder den Ausfall des Betriebs der Systeme gerichtet sind.*** Solche Sicherheitsvorfälle können die ***Sicherheit und Gesundheit der Einwohner gefährden, die*** Ausübung wirtschaftlicher Tätigkeiten beeinträchtigen, finanzielle Verluste verursachen, das Vertrauen ***von Nutzern und Investoren*** untergraben und der Wirtschaft der Union großen Schaden zufügen.

Begründung

Cyberangriffe auf börsennotierte Gesellschaften sind weit verbreitet und dienen dem Diebstahl finanzieller Vermögenswerte bzw. geistigen Eigentums oder führen zu Betriebsstörungen bei ihren Kunden oder Geschäftspartnern und könnten somit Einfluss auf die Beziehungen zu Aktionären oder auf die Entscheidungen potenzieller Investoren haben.

Änderungsantrag 3

Vorschlag für eine Richtlinie
Erwägung 3

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

Begründung

Die Robustheit und Stabilität der Netze und Informationssysteme des Binnenmarkts sind auch für die Interaktion mit globalen und regionalen Märkten wie Nordamerika, Asien usw. von entscheidender Bedeutung.

Änderungsantrag 4

Vorschlag für eine Richtlinie
Erwägung 4

Vorschlag der Kommission	*Geänderter Text*
(4) Auf Unionsebene sollte ein Kooperationsmechanismus eingerichtet werden, der den Informationsaustausch sowie eine koordinierte Erkennungs- und Reaktionsfähigkeit im Bereich der Netz- und Informationssicherheit (im Folgenden „NIS“) ermöglicht. Damit ein solcher Mechanismus wirksam sein kann und alle	(4) Auf Unionsebene sollte ein Kooperationsmechanismus eingerichtet werden, der den Informationsaustausch sowie eine koordinierte ***Präventions-,*** Erkennungs- und Reaktionsfähigkeit im Bereich der Netz- und Informationssicherheit (im Folgenden „NIS“) ermöglicht. Damit ein solcher

Beteiligten einbezogen werden, muss jeder Mitgliedstaat über Mindestkapazitäten und eine Strategie verfügen, die in seinem Hoheitsgebiet eine hohe NIS gewährleisten. Zur Förderung einer Risikomanagementkultur und um sicherzustellen, dass die gravierendsten Sicherheitsvorfälle gemeldet werden, sollten Mindestsicherheitsanforderungen auch für öffentliche ***Verwaltungen*** und Betreiber ***kritischer*** Informationsinfrastrukturen gelten.	Mechanismus wirksam sein kann und alle Beteiligten einbezogen werden, muss jeder Mitgliedstaat über Mindestkapazitäten und eine Strategie verfügen, die in seinem Hoheitsgebiet eine hohe NIS gewährleisten. Zur Förderung einer Risikomanagementkultur und um sicherzustellen, dass die gravierendsten Sicherheitsvorfälle gemeldet werden, sollten Mindestsicherheitsanforderungen auch für öffentliche und ***private*** Betreiber ***von*** Informationsinfrastrukturen ***und börsennotierten Unternehmen*** gelten. ***Der Rechtsrahmen sollte auf der Notwendigkeit beruhen, die Privatsphäre und Integrität der Bürgerinnen und Bürger zu schützen. Das Warn- und Informationsnetz für kritische Infrastrukturen (WINKI) sollte auf diese speziellen Betreiber ausgeweitet werden.***

Begründung

Sicherheitsverletzungen bei börsennotierten Gesellschaften könnten deren Produkte, Dienstleistungen, Kunden- und Lieferantenbeziehungen sowie die allgemeinen Wettbewerbsbedingungen wesentlich beeinträchtigen und daher mit erheblichen Folgen für das Funktionieren des Binnenmarkts (und des außereuropäischen Markts) verbunden sein. Daher sollten börsennotierte Gesellschaften ebenfalls unter die Richtlinie fallen.

Änderungsantrag 5

Vorschlag für eine Richtlinie
Erwägung 4 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(4a) Der Schwerpunkt dieser Richtlinie sollte auf kritischen Infrastrukturen liegen, die für die Aufrechterhaltung zentraler wirtschaftlicher und gesellschaftlicher Tätigkeiten in den Bereichen Energie, Verkehr, Banken, Finanzmarktinfrastrukturen und

Gesundheit unbedingt erforderlich sind.

Änderungsantrag 6

Vorschlag für eine Richtlinie
Erwägung 4 b (neu)

Vorschlag der Kommission	*Geänderter Text*
	(4b) Um sicherzustellen, dass die Regierungen ihre Befugnisse nicht überschreiten oder missbrauchen, ist es von entscheidender Bedeutung, dass die Informations- und Sicherheitssysteme der öffentlichen Behörden transparent, rechtmäßig und eindeutig sind und im Rahmen eines demokratischen Prozesses in transparenter Weise angenommen werden.

Änderungsantrag 7

Vorschlag für eine Richtlinie
Erwägung 6

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

umfassender, wirksamer Mechanismus für die Zusammenarbeit auf Unionsebene geschaffen werden.

umfassender, wirksamer Mechanismus für die Zusammenarbeit auf Unionsebene geschaffen werden***, wodurch zudem die Wirksamkeit der internationalen Zusammenarbeit und infolgedessen die Bekämpfung globaler Sicherheitsprobleme beeinträchtigt wird und die international führende Position der Union bei der Beibehaltung und Förderung eines offenen, effizienten und sicheren Internets***.

Änderungsantrag 8

Vorschlag für eine Richtlinie
Erwägung 7

Vorschlag der Kommission	*Geänderter Text*
(7) Um wirksam auf die Herausforderungen im Bereich der Sicherheit von Netzen und Informationssystemen reagieren zu können, ist deshalb ein umfassender Ansatz auf Unionsebene erforderlich, der gemeinsame Mindestanforderungen für Kapazitätsaufbau und -planung, Informationsaustausch, Maßnahmenkoordinierung sowie gemeinsame Mindestsicherheitsanforderungen ***für alle betroffenen Marktteilnehmer und öffentlichen Verwaltungen*** beinhaltet.	(7) Um wirksam auf die Herausforderungen im Bereich der Sicherheit von Netzen und Informationssystemen reagieren zu können, ist deshalb ein umfassender Ansatz auf Unionsebene erforderlich, der gemeinsame Mindestanforderungen für Kapazitätsaufbau und -planung***, die Entwicklung ausreichender Kompetenzen auf dem Gebiet der Cybersicherheit,*** Informationsaustausch, Maßnahmenkoordinierung sowie gemeinsame Mindestsicherheitsanforderungen beinhaltet. ***In Übereinstimmung mit geeigneten Empfehlungen der Koordinierungsgruppe für die Cybersicherheit (CSGC) sollten gemeinsame Mindestnormen angewendet werden.***

Änderungsantrag 9

Vorschlag für eine Richtlinie
Erwägung 9

Vorschlag der Kommission	*Geänderter Text*
(9) Um eine hohe gemeinsame Netz- und Informationssicherheit zu erreichen und aufrechtzuerhalten sollte jeder Mitgliedstaat über eine nationale NIS-Strategie verfügen, in der die strategischen Ziele sowie konkrete politische Maßnahmen vorgesehen sind. Auf nationaler Ebene müssen NIS-Kooperationspläne aufgestellt werden, die gewisse Grundanforderungen erfüllen, so dass ein Kapazitätsniveau erreicht werden kann, das bei Sicherheitsvorfällen eine wirksame und effiziente Zusammenarbeit auf nationaler und auf Unionsebene ermöglicht.	(9) Um eine hohe gemeinsame Netz- und Informationssicherheit zu erreichen und aufrechtzuerhalten sollte jeder Mitgliedstaat über eine nationale NIS-Strategie verfügen, in der die strategischen Ziele sowie konkrete politische Maßnahmen vorgesehen sind. Auf nationaler Ebene müssen auf der Grundlage der in dieser Richtlinie festgelegten Mindestanforderungen NIS-Kooperationspläne aufgestellt werden, die gewisse Grundanforderungen erfüllen, so dass ein Kapazitätsniveau erreicht werden kann, das bei Sicherheitsvorfällen eine wirksame und effiziente Zusammenarbeit auf nationaler und auf Unionsebene ermöglicht. ***Jeder Mitgliedstaat sollte daher zur Einhaltung gemeinsamer Normen im Hinblick auf das Datenformat und die Austauschbarkeit der gemeinsam genutzten und zu bewertenden Daten verpflichtet werden. Die Mitgliedstaaten können die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) um Unterstützung bei der Entwicklung ihrer nationalen NIS-Strategien auf der Grundlage eines gemeinsamen Entwurfs für eine Mindeststrategie zur NIS ersuchen.***

Begründung

Die ENISA wird von den maßgeblichen Beteiligten bereits als höchst kompetentes Exzellenzzentrum und verlässliches Instrument zur Förderung der Cybersicherheit in der EU anerkannt. Daher sollte die EU Doppelarbeit und -strukturen vermeiden, indem auf dem Know-How der ENISA aufgebaut und die ENISA verpflichtet wird, für Mitgliedstaaten, die nicht über NIS-Einrichtungen und die notwendigen Kenntnisse verfügen und um Unterstützung dieser Art ersuchen, Beratungsdienste anzubieten.

Änderungsantrag 10

Vorschlag für eine Richtlinie
Erwägung 10

Vorschlag der Kommission	*Geänderter Text*
(10) Zur effektiven Umsetzung der Bestimmungen dieser Richtlinie sollte in jedem Mitgliedstaat eine für die Koordinierung in Sachen NIS zuständige Stelle geschaffen oder auf Unionsebene benannt werden, die für die Zwecke der grenzübergreifenden Zusammenarbeit als Anlaufstelle dient. Diese Stellen sollten mit angemessenen 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.	(10) Zur effektiven Umsetzung der Bestimmungen dieser Richtlinie sollte in jedem Mitgliedstaat eine für die Koordinierung in Sachen NIS zuständige Stelle geschaffen oder auf Unionsebene benannt werden, die für die Zwecke der ***internen Koordinierung und der*** grenzübergreifenden Zusammenarbeit als ***zentrale*** Anlaufstelle dient. ***Die Benennung dieser zentralen nationalen Anlaufstellen sollte die Möglichkeit der Mitgliedstaaten unberührt lassen, gemäß ihren jeweiligen verfassungsrechtlichen, gerichtlichen oder verwaltungsrechtlichen Bestimmungen mehr als eine nationale Behörde mit Zuständigkeit für die Netz- und Informationssicherheit zu bestimmen. Gleichwohl sollten die Anlaufstellen mit einer koordinierenden Aufgabe auf einzelstaatlicher und Unionsebene betraut werden.*** Diese Stellen sollten mit angemessenen technischen, finanziellen und personellen Ressourcen ausgestattet sein, um die ihnen übertragenen Aufgaben ***dauerhaft,*** wirksam und effizient erfüllen und somit die Ziele dieser Richtlinie erreichen zu können.

Änderungsantrag 11

Vorschlag für eine Richtlinie
Erwägung 10 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(10a) Da Unterschiede zwischen den Verwaltungsstrukturen der einzelnen Mitgliedstaaten bestehen, bereits geltende sektorbezogene Vereinbarungen beibehalten werden sollten und damit keine Dopplungen entstehen, sollten die Mitgliedstaaten mehrere nationale zuständige Behörden benennen können, die im Rahmen dieser Richtlinie die Aufgaben im Zusammenhang mit der Netz- und Informationssicherheit von Marktteilnehmern wahrnehmen. Allerdings ist es im Interesse einer reibungslosen länderübergreifenden Zusammenarbeit und Kommunikation notwendig, dass jeder Mitgliedstaat eine einzige zentrale Anlaufstelle für die länderübergreifende Zusammenarbeit auf Unionsebene benennt. Ein Mitgliedstaat sollte auch – sofern dies verfassungsmäßig oder aufgrund anderer Vereinbarungen erforderlich ist – befugt sein, nur eine Behörde zu benennen, die die Aufgaben der zuständigen Behörde und der zentralen Anlaufstelle wahrnimmt.

Änderungsantrag 12

Vorschlag für eine Richtlinie
Erwägung 11

Vorschlag der Kommission	*Geänderter Text*
(11) Alle Mitgliedstaaten sollten über angemessene technische und organisatorische Kapazitäten verfügen, um die Prävention, Erkennung, Reaktion und Folgenminderung bei NIS-Vorfällen und -Risiken gewährleisten zu können. Dafür sollten im Einklang mit den grundlegenden	(11) Alle Mitgliedstaaten ***sowie Marktteilnehmer*** sollten über angemessene technische und organisatorische Kapazitäten verfügen, um die Prävention, Erkennung, Reaktion und Folgenminderung bei NIS-Vorfällen und -Risiken ***jederzeit*** gewährleisten zu können.

Anforderungen in allen Mitgliedstaaten gut funktionierende IT-Notfallteams (Computer Emergency Response Teams) eingerichtet werden, damit wirksame und geeignete Kapazitäten geschaffen werden, die in der Lage sind, Sicherheitsvorfälle und -risiken zu bewältigen und eine effiziente Zusammenarbeit auf Unionsebene zu gewährleisten.	***Die Sicherheitssysteme in der öffentlichen Verwaltung müssen sicher sein und der demokratischen Kontrolle und Prüfung unterliegen. Die gebräuchlichen Ausstattungen und Kapazitäten sollten den gemeinsam vereinbarten technischen Normen sowie Standardvorgehensweisen entsprechen.*** Dafür sollten im Einklang mit den grundlegenden Anforderungen in allen Mitgliedstaaten gut funktionierende IT-Notfallteams (Computer Emergency Response Teams***, CERT***) eingerichtet werden, damit wirksame und geeignete Kapazitäten geschaffen werden, die in der Lage sind, Sicherheitsvorfälle und -risiken zu bewältigen und eine effiziente Zusammenarbeit auf Unionsebene zu gewährleisten. ***Diese IT-Notfallteams sollten in die Lage versetzt werden, auf der Grundlage gemeinsamer technischer Normen und Standardvorgehensweisen zu interagieren. Angesichts der unterschiedlichen Beschaffenheit der bestehenden CERT, welche für die unterschiedlichen subjektiven Bedürfnisse und Akteure zuständig sind, sollten die Mitgliedstaaten sicherstellen, dass jedem der im Anhang II genannten Sektoren Dienstleistungen von mindestens einem CERT geboten werden. In Bezug auf die grenzüberschreitende CERT-Kooperation sollten die Mitgliedstaaten sicherstellen, dass CERTs über hinreichende Mittel verfügen, um an den vorhandenen internationalen und europäischen Kooperationsnetzen mitzuwirken.***

Begründung

Die Interoperabilität muss sichergestellt werden.

Änderungsantrag 13

Vorschlag für eine Richtlinie
Erwägung 12

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

Änderungsantrag 14

Vorschlag für eine Richtlinie
Erwägung 13

Vorschlag der Kommission	*Geänderter Text*
(13) Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) sollte die Mitgliedstaaten und die Kommission mit Fachkompetenz, als Berater und als Mittler für den Austausch bewährter Verfahren unterstützen. Insbesondere ***sollte*** die Kommission die ENISA bei der Anwendung dieser Richtlinie zu Rate ziehen. Damit sichergestellt ist, dass die	(13) Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) sollte die Mitgliedstaaten und die Kommission mit Fachkompetenz, als Berater und als Mittler für den Austausch bewährter Verfahren unterstützen. Insbesondere ***sollten*** die Kommission ***und*** die ***Mitgliedstaaten die*** ENISA bei der Anwendung dieser Richtlinie zu Rate

Mitgliedstaaten und die Kommission tatsächlich und rechtzeitig informiert werden, sollten Frühwarnungen vor Sicherheitsvorfällen und -risiken über das Kooperationsnetz ausgegeben werden. Um Kapazitäten und Fachwissen unter den Mitgliedstaaten aufbauen zu können, sollte das Kooperationsnetz auch als Mittel für den Austausch bewährter Verfahren dienen und damit seinen Mitgliedern beim Kapazitätsaufbau helfen sowie die Organisation von gegenseitigen Überprüfungen und NIS-Übungen leiten.

ziehen. Damit sichergestellt ist, dass die Mitgliedstaaten und die Kommission tatsächlich und rechtzeitig informiert werden, sollten Frühwarnungen vor Sicherheitsvorfällen und -risiken über das Kooperationsnetz ausgegeben werden. Um Kapazitäten und Fachwissen unter den Mitgliedstaaten aufbauen zu können, sollte das Kooperationsnetz auch als Mittel für den Austausch bewährter Verfahren dienen und damit seinen Mitgliedern beim Kapazitätsaufbau helfen sowie die Organisation von gegenseitigen Überprüfungen und NIS-Übungen leiten.

Änderungsantrag 15

Vorschlag für eine Richtlinie
Erwägung 14

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

Netz festlegen.

Änderungsantrag 16

Vorschlag für eine Richtlinie
Erwägung 14 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(14a) Marktteilnehmer können, falls erforderlich, auch zur Mitwirkung bei der Tätigkeit des Kooperationsnetzes aufgefordert werden.

Änderungsantrag 17

Vorschlag für eine Richtlinie
Erwägung 15

Vorschlag der Kommission	*Geänderter Text*
(15) Da die meisten Netze und Informationssysteme privat betrieben werden, ist die Zusammenarbeit zwischen dem privaten und dem öffentlichen Sektor von zentraler Bedeutung. Die Marktteilnehmer sollten angehalten werden, sich eines eigenen informellen Kooperationsmechanismus zur Gewährleistung der NIS zu bedienen. Sie sollten ferner mit dem öffentlichen Sektor zusammenarbeiten und Informationen und bewährte Verfahren austauschen und ***im Gegenzug operative*** Unterstützung im Falle von Sicherheitsvorfällen ***erhalten***.	(15) Da die meisten Netze und Informationssysteme privat betrieben werden, ist die Zusammenarbeit zwischen dem privaten und dem öffentlichen Sektor von zentraler Bedeutung. Die Marktteilnehmer sollten angehalten werden, sich eines eigenen informellen Kooperationsmechanismus zur Gewährleistung der NIS zu bedienen. Sie sollten ferner mit dem öffentlichen Sektor zusammenarbeiten und ***untereinander*** Informationen und bewährte Verfahren austauschen***, einschließlich des gegenseitigen Austauschs relevanter Informationen*** und ***operativer*** Unterstützung ***sowie strategisch analysierte Informationen*** im Falle von Sicherheitsvorfällen. ***Zur wirksamen Unterstützung des Austauschs von Informationen und bewährten Verfahren muss unbedingt sichergestellt werden, dass Marktteilnehmer, die an einem***

	solchen Austausch beteiligt sind, keine Benachteiligung aufgrund ihrer Zusammenarbeit erfahren. Durch angemessene Sicherheitsvorkehrungen muss gewährleistet werden, dass eine solche Zusammenarbeit für diese Betreiber nicht mit einem erhöhten Risiko der Nichteinhaltung oder neuen Verbindlichkeiten gemäß den Rechtsvorschriften unter anderem zu Wettbewerb, geistigem Eigentum, Datenschutz oder Cyberkriminalität einhergeht und auch nicht mit höheren operativen oder sicherheitstechnischen Risiken verbunden ist.

Änderungsantrag 18

Vorschlag für eine Richtlinie
Erwägung 16

Vorschlag der Kommission	*Geänderter Text*
(16) Um Transparenz zu gewährleisten und die Bürger und Marktteilnehmer der EU angemessen zu informieren, sollten die ***zuständigen Behörden*** eine gemeinsame Website zur Veröffentlichung nichtvertraulicher Informationen über Sicherheitsvorfälle und -risiken einrichten.	(16) Um Transparenz zu gewährleisten und die Bürger und Marktteilnehmer der EU angemessen zu informieren, sollten die ***zentralen Anlaufstellen*** eine gemeinsame ***unionsweite*** Website zur Veröffentlichung nichtvertraulicher Informationen über ***über*** Sicherheitsvorfälle und -risiken ***und letztlich zur Bereitstellung von Empfehlungen zu geeigneten Wartungsmaßnahmen*** einrichten.

Änderungsantrag 19

Vorschlag für eine Richtlinie
Erwägung 17

Vorschlag der Kommission	*Geänderter Text*
(17) Werden die betreffenden Informationen nach Vorschriften der EU und der Mitgliedstaaten über das Geschäftsgeheimnis als vertraulich eingestuft, ist deren Vertraulichkeit bei den in dieser Richtlinie vorgesehenen Tätigkeiten und bei der Erreichung der darin gesetzten Ziele sicherzustellen.	(17) ***Die in Erwägung 14 genannte Strategie zur Klassifizierung von Informationen sollte sich an dem von der ENISA empfohlenen Ampelprotokoll für den Informationsaustausch (Information Sharing Traffic Light Protocol) orientieren. Jede ausgetauschte Information wird entsprechend dem Grad ihrer Sensibilität nach den Angaben der Informationsquelle klassifiziert und behandelt.*** Werden die betreffenden Informationen nach Vorschriften der EU und der Mitgliedstaaten über das Geschäftsgeheimnis als vertraulich eingestuft, ist deren Vertraulichkeit bei den in dieser Richtlinie vorgesehenen Tätigkeiten und bei der Erreichung der darin gesetzten Ziele sicherzustellen.

Änderungsantrag 20

Vorschlag für eine Richtlinie
Erwägung 18

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

Änderungsantrag 21

Vorschlag für eine Richtlinie
Erwägung 19

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

Änderungsantrag 22

Vorschlag für eine Richtlinie
Erwägung 20

Vorschlag der Kommission	*Geänderter Text*
(20) Bei Eingang einer Frühwarnung und bei deren Bewertung sollten sich die ***zuständigen Behörden*** auf eine koordinierte Reaktion nach dem NIS-Kooperationsplan der EU einigen. Die ***zuständigen Behörden*** und die Kommission sollten über die im Zuge der	(20) Bei Eingang einer Frühwarnung und bei deren Bewertung sollten sich die ***zentralen Anlaufstellen*** auf eine koordinierte Reaktion nach dem NIS-Kooperationsplan der EU einigen. Die ***zentralen Anlaufstellen, die ENISA*** und die Kommission sollten über die im Zuge

koordinierten Reaktion auf nationaler Ebene ergriffenen Maßnahmen informiert werden.

der koordinierten Reaktion auf nationaler Ebene ergriffenen Maßnahmen informiert werden.

Änderungsantrag 23

Vorschlag für eine Richtlinie
Erwägung 22

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

Änderungsantrag 24

Vorschlag für eine Richtlinie
Erwägung 24

Vorschlag der Kommission	*Geänderter Text*
(24) Diese Verpflichtungen sollten ***über den elektronischen Kommunikationssektor hinaus ausgeweitet werden auf wichtige Anbieter von Diensten der***	(24) Diese Verpflichtungen sollten ***auf Betreiber von*** Infrastrukturen ausgeweitet werden, die stark von der Informations- und Kommunikationstechnik abhängen und für die Aufrechterhaltung wichtiger

Informationsgesellschaft im Sinne der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft[27], auf die sich nachgelagerte Dienste der Informationsgesellschaft oder Online-Tätigkeiten wie Plattformen des elektronischen Geschäftsverkehrs, Internet-Zahlungs-Gateways, soziale Netze, Suchmaschinen, Cloud-Computing-Dienste und Application Stores stützen. Störungen dieser grundlegenden Dienste der Informationsgesellschaft verhindern die Erbringung anderer, darauf aufbauender Dienste der Informationsgesellschaft. Softwareentwickler und Hardwarehersteller sind keine Anbieter von Diensten der Informationsgesellschaft und sind deshalb ausgenommen. Die Verpflichtungen sollten auch auf öffentliche Verwaltungen und Betreiber kritischer Infrastrukturen ausgeweitet werden, die stark von der Informations- und Kommunikationstechnik abhängen und für die Aufrechterhaltung wichtiger wirtschaftlicher und gesellschaftlicher Bereiche (Strom- und Gasversorgung, Verkehr, ***Finanzinstitutionen***, ***Börsen,*** Gesundheitswesen usw.) unerlässlich sind. Eine Störung dieser Netze und Informationssysteme würde den Binnenmarkt beeinträchtigen.

---

[27] ABl. L 204, 21.7.1998, S. 37.

wirtschaftlicher und gesellschaftlicher Bereiche (Strom- und Gasversorgung, Verkehr, ***Kreditinstitute***, ***Finanzmarktinfrastrukturen,*** Gesundheitswesen usw.) unerlässlich sind. Eine Störung dieser Netze und Informationssysteme würde den Binnenmarkt beeinträchtigen. ***Die in dieser Richtlinie festgelegten Verpflichtungen gelten zwar nicht für wichtige Anbieter von Diensten der Informationsgesellschaft im Sinne der Richtlinie 98/34/EG des europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften für die Dienste[27] der Informationsgesellschaft, auf die sich nachgelagerte Dienste der Informationsgesellschaft oder Online-Tätigkeiten wie Plattformen des elektronischen Geschäftsverkehrs, Internet-Zahlungs-Gateways, soziale Netze, Suchmaschinen, Cloud-Computing-Dienste und Application Stores stützen, diese können jedoch auf freiwilliger Basis die zuständige Behörde oder die zentrale Anlaufstelle über die die Netzsicherheit betreffenden Vorfälle informieren, die sie für relevant halten. Die zuständige Behörde oder die zentrale Anlaufstelle sollte, falls im angemessenen Rahmen möglich, die Marktteilnehmer, die den Vorfall gemeldet haben, mit strategisch analysierten Informationen versorgen, mit denen die Sicherheitsbedrohung beseitigt wird.***

---

[27] ABl. L 204, 21.7.1998, S. 37.

Änderungsantrag 25

Vorschlag für eine Richtlinie

Erwägung 25

Vorschlag der Kommission	*Geänderter Text*
(25) Zu den von öffentlichen Verwaltungen und Marktteilnehmern zu ergreifenden technischen und organisatorischen Maßnahmen sollte nicht die Verpflichtung gehören, bestimmte geschäftliche Informationen und Produkte der Kommunikationstechnik in bestimmter Weise zu konzipieren, zu entwickeln oder herzustellen.	(25) Zu den von den Marktteilnehmern zu ergreifenden technischen und organisatorischen Maßnahmen sollte nicht die Verpflichtung gehören, bestimmte geschäftliche Informationen und Produkte der Kommunikationstechnik in bestimmter Weise zu konzipieren, zu entwickeln oder herzustellen. ***Allerdings sollte die Anwendung internationaler Normen zur Cybersicherheit vorgeschrieben sein.***

Änderungsantrag 26

Vorschlag für eine Richtlinie
Erwägung 28

Vorschlag der Kommission	*Geänderter Text*
(28) Die zuständigen Behörden sollten dafür Sorge tragen, dass informelle, vertrauenswürdige Kanäle für den Informationsaustausch zwischen Marktteilnehmern sowie zwischen dem öffentlichen und dem privaten Sektor erhalten bleiben. Bei der Bekanntmachung von Sicherheitsvorfällen, die den zuständigen Behörden gemeldet werden, sollte das Interesse der Öffentlichkeit, über Bedrohungen informiert zu werden, sorgfältig gegen einen möglichen wirtschaftlichen Schaden bzw. einen Imageschaden abgewogen werden, der den öffentlichen Verwaltungen bzw. den Marktteilnehmern, die solche Vorfälle melden, entstehen kann. Bei der Erfüllung der Meldepflichten sollten die zuständigen Behörden besonders darauf achten, dass Informationen über die Anfälligkeit von Produkten bis zur Veröffentlichung der entsprechenden Sicherheitsfixes streng	(28) Die zuständigen Behörden und die zentralen Anlaufstellen sollten dafür Sorge tragen, dass informelle, vertrauenswürdige Kanäle für den Informationsaustausch zwischen Marktteilnehmern sowie zwischen dem öffentlichen und dem privaten Sektor erhalten bleiben. ***Werden den zuständigen Behörden zuvor unbekannte Anfälligkeiten oder Sicherheitsvorfälle gemeldet, sollten sie die Hersteller betroffener IKT-Produkte und die Anbieter betroffener IKT-Dienste benachrichtigen.*** Bei der Bekanntmachung von Sicherheitsvorfällen, die den zuständigen Behörden und den zentralen Anlaufstellen 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 Marktteilnehmern, die solche

vertraulich bleiben.	Sicherheitsvorfälle melden, entstehen kann. Um Vertrauen und Wirksamkeit sicherzustellen, findet eine Veröffentlichung der Vorfälle nur nach Rücksprache mit den Teilnehmern statt, die den Vorfall gemeldet haben, und nur dann, wenn es für das Erreichen der Ziele dieser Richtlinie unbedingt erforderlich ist. Bei der Erfüllung der Meldepflichten sollten die zuständigen Behörden und die zentrale Anlaufstelle besonders darauf achten, dass Informationen über die Anfälligkeit von Produkten bis zur Veröffentlichung der entsprechenden Sicherheitsfixes streng vertraulich bleiben, ohne jedoch entsprechende Meldungen länger als unbedingt erforderlich hinauszuzögern. ***Generell sollten die zentralen Anlaufstellen keine personenbezogenen Daten von natürlichen Personen offenlegen, die an Sicherheitsvorfällen beteiligt sind. Die zentralen Anlaufstellen sollten personenbezogene Daten nur dann offenlegen, wenn dies im Hinblick auf den damit verfolgten Zweck notwendig und verhältnismäßig ist.***

Begründung

Wenn den Behörden Informationen zur Anfälligkeit bestimmter IKT-Produkte oder -Dienste vorliegen, sollten sie die Hersteller und Diensteanbieter benachrichtigen, damit diese die Möglichkeit einer zeitnahen Anpassung ihrer Produkte und Dienste haben.

Änderungsantrag 27

Vorschlag für eine Richtlinie
Erwägung 29

Vorschlag der Kommission	*Geänderter Text*
(29) Die zuständigen Behörden sollten mit den für die Erfüllung ihrer Aufgaben erforderlichen Mitteln ausgestattet sein; sie sollten auch befugt sein, hinreichende	(29) Die zuständigen Behörden ***und die zentralen Anlaufstellen*** sollten mit den für die Erfüllung ihrer Aufgaben erforderlichen Mitteln ausgestattet sein; sie

Auskünfte von Marktteilnehmern ***und öffentlichen Verwaltungen*** einzuholen, damit sie die Sicherheit von Netzen und Informationssystemen beurteilen können und über verlässliche, umfassende Daten über tatsächliche Sicherheitsvorfälle verfügen, die den Betrieb von Netzen und Informationssystemen beeinträchtigt haben.

sollten auch befugt sein, hinreichende Auskünfte von Marktteilnehmern einzuholen, damit sie die Sicherheit von Netzen und Informationssystemen ***sowie Anzahl, Tragweite und Ausmaß von Zwischenfällen*** beurteilen können und über verlässliche, umfassende Daten über tatsächliche Sicherheitsvorfälle verfügen, die den Betrieb von Netzen und Informationssystemen beeinträchtigt haben.

Änderungsantrag 28

Vorschlag für eine Richtlinie
Erwägung 30

Vorschlag der Kommission	*Geänderter Text*
(30) Häufig gehen Sicherheitsvorfälle auf kriminelle Handlungen zurück. Selbst wenn zunächst keine hinreichenden Beweise vorliegen, kann bei Sicherheitsvorfällen ein krimineller Hintergrund vermutet werden. In diesem Zusammenhang sollte eine sachgerechte Zusammenarbeit zwischen den zuständigen Behörden und den Strafverfolgungsbehörden Bestandteil einer wirksamen, umfassenden Reaktion auf die Bedrohung durch Sicherheitsvorfälle sein. Die Förderung einer sicheren, robusteren Umgebung setzt insbesondere voraus, dass die Strafverfolgungsbehörden systematisch über Sicherheitsvorfälle mit mutmaßlich kriminellem Hintergrund Bericht informiert werden. Ob es sich um Sicherheitsvorfälle aufgrund schwerer Straftaten handelt, sollte nach den EU-Vorschriften über Cyberkriminalität beurteilt werden.	(30) Häufig gehen Sicherheitsvorfälle auf kriminelle Handlungen ***oder Cyberkriegsaktivitäten*** zurück. Selbst wenn zunächst keine hinreichenden Beweise vorliegen, kann bei Sicherheitsvorfällen ein krimineller Hintergrund vermutet werden. In diesem Zusammenhang sollte eine sachgerechte Zusammenarbeit zwischen den zuständigen Behörden***, den zentralen Anlaufstellen*** und den Strafverfolgungsbehörden ***sowie eine Zusammenarbeit mit dem EC3 (Europäisches Zentrum zur Bekämpfung der Cyberkriminalität) und der ENISA*** Bestandteil einer wirksamen, umfassenden Reaktion auf die Bedrohung durch Sicherheitsvorfälle sein. Die Förderung einer sicheren, robusteren Umgebung setzt insbesondere voraus, dass die Strafverfolgungsbehörden systematisch über Sicherheitsvorfälle mit mutmaßlich kriminellem Hintergrund Bericht informiert werden. Ob es sich um Sicherheitsvorfälle aufgrund schwerer Straftaten handelt, sollte nach den EU-

Vorschriften über Cyberkriminalität beurteilt werden.

Änderungsantrag 29

Vorschlag für eine Richtlinie
Erwägung 31

Vorschlag der Kommission	*Geänderter Text*
(31) Häufig ist bei Sicherheitsvorfällen der Schutz personenbezogener Daten nicht mehr gewährleistet. Deshalb sollten die zuständigen Behörden und die Datenschutzbehörden zusammenarbeiten und Informationen zu allen einschlägigen Fragen austauschen, um derartigen Verletzungen des Schutzes personenbezogener Daten zu begegnen. Die Mitgliedstaaten sollten die Meldepflicht bei Sicherheitsvorfällen so umsetzen, dass der Verwaltungsaufwand bei Sicherheitsvorfällen, die gleichzeitig eine Verletzung des Schutzes personenbezogener Daten im Sinne der Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr darstellen, so gering wie möglich gehalten wird28. Über Kontakte mit den zuständigen Behörden und den Datenschutzbehörden könnte die ENISA Unterstützung bieten, indem sie Mechanismen für den Informationsaustausch sowie Muster entwickelt, mit denen die Verwendung zweier verschiedener Muster für die Meldung von NIS-Vorfällen vermieden werden kann. Die Meldung anhand eines einzigen Musters wäre bei Sicherheitsvorfällen, bei denen der Schutz personenbezogener Daten beeinträchtigt wurde, eine Vereinfachung und würde	(31) Häufig ist bei Sicherheitsvorfällen der Schutz personenbezogener Daten nicht mehr gewährleistet. ***Mitgliedstaaten und Marktteilnehmer sollten gespeicherte, verarbeitete oder übermittelte Daten gegen zufällige oder rechtswidrige Zerstörung, zufälligen Verlust oder zufällige Änderung sowie gegen unbefugte oder rechtswidrige Speicherung, Preisgabe, Verbreitung oder Zugriff schützen; sie sollten darüber hinaus die Umsetzung eines Sicherheitskonzepts für die Verarbeitung personenbezogener Daten sicherstellen.*** Deshalb sollten die zuständigen Behörden, die zentralen Anlaufstellen und die Datenschutzbehörden zusammenarbeiten und Informationen zu allen einschlägigen Fragen austauschen, um derartigen Verletzungen des Schutzes personenbezogener Daten zu begegnen. Die Meldepflicht bei Sicherheitsvorfällen sollte so umgesetzt werden, dass der Verwaltungsaufwand bei Sicherheitsvorfällen, die gleichzeitig eine Verletzung des Schutzes personenbezogener Daten darstellen und gemäß der geltenden Gesetze gemeldet werden müssen, so gering wie möglich gehalten wird. Die ENISA sollte Unterstützung bieten, indem sie Mechanismen für den Informationsaustausch und ein einziges Muster entwickelt, mit dem die Meldung

damit den Verwaltungsaufwand für Unternehmen und öffentliche Verwaltungen verringern.

von Sicherheitsvorfällen, bei denen der Schutz personenbezogener Daten beeinträchtigt wurde, vereinfacht und damit der Verwaltungsaufwand für Unternehmen und öffentliche Verwaltungen verringert würde.

---

[28] SEC(2012) 72 final

Begründung

Anpassung an den Entwurf der Datenschutzrichtlinie.

Änderungsantrag 30

Vorschlag für eine Richtlinie
Erwägung 32

Vorschlag der Kommission	*Geänderter Text*
(32) Die Normung von Sicherheitsanforderungen ist ein vom Markt ausgehender Vorgang. Um die Sicherheitsstandards einander anzunähern, sollten die Mitgliedstaaten die Anwendung oder Einhaltung konkreter Normen fördern, damit ein hohes Sicherheitsniveau auf Unionsebene gewährleistet wird. dies sollte nach der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 zur europäischen Normung, zur Änderung der ***Richtlinien 89/686/EWG*** und 93/15/EWG des Rates sowie der ***Richtlinien 94/9/EG***, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG und 2009/105/EG des Europäischen Parlaments und des Rates und zur Aufhebung des ***Beschlusses 87/95/EWG*** des Rates und des Beschlusses Nr. 1673/2006/EG des Europäischen Parlaments und des Rates29 geschehen.	(32) Die Normung von Sicherheitsanforderungen ist ein vom Markt ausgehender Vorgang ***auf freiwilliger Basis, der es Marktteilnehmern ermöglichen sollte, alternative Mittel einzusetzen, um mindestens ähnliche Ergebnisse zu erzielen***. Um die Sicherheitsstandards einander anzunähern, sollten die Mitgliedstaaten die Anwendung oder Einhaltung konkreter ***interoperabler*** Normen fördern, damit ein hohes Sicherheitsniveau auf Unionsebene gewährleistet wird. ***Zu diesem Zweck sollte die Anwendung offener internationaler Normen für Netzinformationssicherheit oder die Konzipierung entsprechender Tools in Erwägung gezogen werden. Ein weiterer Schritt könnte erforderlich sein, um harmonisierte Normen auszuarbeiten; Ein weiterer Schritt nach vorne könnte darin bestehen, harmonisierte Normen***

auszuarbeiten; dies sollte nach der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 zur europäischen Normung, zur Änderung der ***Richtlinien 89/686/EWG*** und 93/15/EWG des Rates sowie der ***Richtlinien 94/9/EG***, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG und 2009/105/EG des Europäischen Parlaments und des Rates und zur Aufhebung des ***Beschlusses 87/95/EWG*** des Rates und des Beschlusses Nr. 1673/2006/EG des Europäischen Parlaments und des Rates[29] geschehen. ***Insbesondere sollten das ETSI, das CEN und das CENELEC ermächtigt werden, effektive und effiziente offene EU-Sicherheitsstandards zu empfehlen, bei denen technische Voreinstellungen so weit wie möglich vermieden werden und die für kleine und mittlere Marktteilnehmer praktikabel sind. Internationale Normen bezüglich Cybersicherheit sollten sehr sorgfältig geprüft werden, um sicherzustellen, dass bei ihnen keine Abstriche gemacht wurden und dass sie ein ausreichend hohes Sicherheitsniveau bieten und somit sicherstellen, dass die gebotene Einhaltung der Cybersicherheitsstandards das Gesamtniveau der Cybersicherheit in der Union erhöht und nicht herabsetzt.***

[29] ABl. L 316, 14.11.2012, S. 12.

[29] ABl. L 316, 14.11.2012, S. 12.

Änderungsantrag 31

Vorschlag für eine Richtlinie
Erwägung 33

Vorschlag der Kommission	*Geänderter Text*
(33) Die Kommission sollte diese	(33) Die Kommission sollte diese

Richtlinie regelmäßig überprüfen, insbesondere um festzustellen, ob sie veränderten technischen oder Marktbedingungen anzupassen ist.	Richtlinie regelmäßig ***in Abstimmung mit allen betroffenen Akteuren*** überprüfen, insbesondere um festzustellen, ob sie veränderten ***gesellschaftlichen, politischen,*** technischen oder Marktbedingungen anzupassen ist.

Änderungsantrag 32

Vorschlag für eine Richtlinie
Erwägung 34

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

Änderungsantrag 33

Vorschlag für eine Richtlinie
Erwägung 35

Vorschlag der Kommission	*Geänderter Text*
(35) Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer ***Vorbereitungsarbeiten*** angemessene ***Konsultationen –*** auch auf der Ebene von ***Sachverständigen –*** durchführt. ***Bei der Vorbereitung und Ausarbeitung***	(35) Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer ***Vorbereitungsarbeit*** angemessene ***Konsultationen –*** auch ***mit allen Interessenträgern und*** auf der Ebene von ***Sachverständigen –*** durchführt. Die

delegierter Rechtsakte sollte die Kommission ***sicherstellen, dass die*** einschlägigen Dokumente ***dem Europäischen*** Parlament und ***dem Rat gleichzeitig, rechtzeitig und ordnungsgemäß übermittelt werden***.

Kommission ***sollte eine gleichzeitige und frühzeitige Übermittlung der*** einschlägigen Dokumente ***an das Europäische*** Parlament und ***an den Rat in geeigneter Weise gewährleisten***.

Änderungsantrag 34

Vorschlag für eine Richtlinie
Erwägung 36

Vorschlag der Kommission	*Geänderter Text*
(36) Zur Gewährleistung einheitlicher Voraussetzungen für die Umsetzung dieser Richtlinie sollten der Kommission Durchführungsbefugnisse in Bezug auf die Zusammenarbeit zwischen den ***zuständigen Behörden*** und der Kommission im Rahmen des Kooperationsnetzes, ***den Zugang zur sicheren*** Infrastruktur für den Informationsaustausch, den NIS-Kooperationsplan***,*** die Formen und Verfahren ***zur Information der Öffentlichkeit über Sicherheitsvorfälle und NIS-bezogene Normen und/oder technische Spezifikationen*** übertragen werden. Diese Befugnisse sollten gemäß der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren30, ausgeübt werden.	(36) Zur Gewährleistung einheitlicher Voraussetzungen für die Umsetzung dieser Richtlinie sollten der Kommission***, unbeschadet der Mechanismen der Zusammenarbeit auf nationaler Ebene,*** Durchführungsbefugnisse in Bezug auf die Zusammenarbeit zwischen den ***zentralen Anlaufstellen*** und der Kommission im Rahmen des Kooperationsnetzes, ***die Reihe gemeinsamer Standards hinsichtlich Zusammenschaltung und Sicherheit für die sichere*** Infrastruktur für den Informationsaustausch, den NIS-Kooperationsplan ***und*** die Formen und Verfahren ***für die Meldung von schwerwiegenden Vorfällen*** übertragen werden. Diese Befugnisse sollten gemäß der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren30, ausgeübt werden.
[30] ABl. L 55, 28.2.2011, S.13.	[30] ABl. L 55, 28.2.2011, S. 13.

Änderungsantrag 35

Vorschlag für eine Richtlinie
Erwägung 37

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

Änderungsantrag 36

Vorschlag für eine Richtlinie
Erwägung 38

Vorschlag der Kommission	*Geänderter Text*
(38) Informationen, die nach den Vorschriften der Union und der Mitgliedstaaten über das Geschäftsgeheimnis von einer ***zuständigen Behörde*** als vertraulich eingestuft werden, sollten mit der Kommission ***und anderen*** zuständigen Behörden nur ausgetauscht werden, wenn sich dies für die Zwecke dieser Richtlinie als unbedingt erforderlich erweist. Der Informationsaustausch sollte im Umfang so begrenzt bleiben, dass er im Hinblick auf das verfolgte Ziel relevant und angemessen ist.	(38) Informationen, die nach den Vorschriften der Union und der Mitgliedstaaten über das Geschäftsgeheimnis von einer ***zentralen Anlaufstelle*** als vertraulich eingestuft werden, sollten mit der Kommission***, deren einschlägigen Agenturen, zentralen Anlaufstellen und/oder weiteren*** zuständigen ***nationalen*** Behörden nur ***dann*** ausgetauscht werden, wenn sich dies für die Zwecke dieser Richtlinie als unbedingt erforderlich erweist. Der Informationsaustausch sollte im Umfang so begrenzt bleiben, dass er im Hinblick auf das verfolgte Ziel relevant***, notwendig*** und angemessen ist ***und dass zuvor festgelegte Vertraulichkeits- und Sicherheitskriterien und Klassifizierungsprotokolle zur Regelung des Informationsaustauschprozesses beachtet***

werden.

Änderungsantrag 37

Vorschlag für eine Richtlinie
Erwägung 39

Vorschlag der Kommission	*Geänderter Text*
(39) Der Austausch von Informationen über Sicherheitsrisiken und -vorfälle über das Kooperationsnetz und die Einhaltung der Verpflichtung zur Meldung von Sicherheitsvorfällen bei den zuständigen nationalen Behörden kann die Verarbeitung personenbezogener Daten erfordern. Diese Verarbeitung personenbezogener Daten ist notwendig, um die mit dieser Richtlinie verfolgten Ziele des öffentlichen Interesses zu erreichen, und somit nach Artikel 7 der Richtlinie 95/46/EG zulässig. Im Hinblick auf diesen legitimen Zweck ist sie weder unverhältnismäßig noch handelt es sich um einen nicht tragbaren Eingriff, der das in Artikel 8 der Charta der Grundrechte verbriefte Recht auf den Schutz personenbezogener Daten in ihrem Wesensgehalt antastet. Bei der Anwendung dieser Richtlinie sollte die Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission[31] entsprechend gelten. Die Datenverarbeitung durch die Organe und Einrichtungen der Union für die Zwecke dieser Richtlinie sollte nach der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der	(39) Der Austausch von Informationen über Sicherheitsrisiken und -vorfälle über das Kooperationsnetz und die Einhaltung der Verpflichtung zur Meldung von Sicherheitsvorfällen bei den zuständigen nationalen Behörden ***oder zentralen Anlaufstellen*** kann die Verarbeitung personenbezogener Daten erfordern. Diese Verarbeitung personenbezogener Daten ist notwendig, um die mit dieser Richtlinie verfolgten Ziele des öffentlichen Interesses zu erreichen, und somit nach Artikel 7 der Richtlinie 95/46/EG zulässig. Im Hinblick auf diesen legitimen Zweck ist sie weder unverhältnismäßig noch handelt es sich um einen nicht tragbaren Eingriff, der das in Artikel 8 der Charta der Grundrechte verbriefte Recht auf den Schutz personenbezogener Daten in ihrem Wesensgehalt antastet. Bei der Anwendung dieser Richtlinie sollte die Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission[31] entsprechend gelten. Die Datenverarbeitung durch die Organe und Einrichtungen der Union für die Zwecke dieser Richtlinie sollte nach der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der

Gemeinschaft und zum freien Datenverkehr erfolgen.

_____

[31] ABl. L 145, 31.5.2001, S. 43.

Gemeinschaft und zum freien Datenverkehr erfolgen.

_____

[31] ABl. L 145, 31.5.2001, S. 43.

Änderungsantrag 38

Vorschlag für eine Richtlinie
Erwägung 41 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(41a) Gemäß der Gemeinsamen Politischen Erklärung der Mitgliedstaaten und der Kommission vom 28. September 2011 zu erläuternden Dokumenten haben sich die Mitgliedstaaten verpflichtet, in begründeten Fällen zusätzlich zur Mitteilung ihrer Umsetzungsmaßnahmen ein oder mehrere Dokumente zu übermitteln, in denen der Zusammenhang zwischen den Bestandteilen einer Richtlinie und den entsprechenden Teilen der nationalen Umsetzungsinstrumente erläutert wird. In Bezug auf diese Richtlinie hält der Gesetzgeber die Übermittlung derartiger Dokumente für gerechtfertigt.

Änderungsantrag 39

Vorschlag für eine Richtlinie
Artikel 1 – Absatz 2 – point b

Vorschlag der Kommission	*Geänderter Text*
b) die Schaffung eines Kooperationsmechanismus zwischen den Mitgliedstaaten zur Gewährleistung einer einheitlichen Anwendung dieser Richtlinie in der Union, damit erforderlichenfalls in koordinierter, effizienter Weise mit Sicherheitsrisiken und -vorfällen, die Netze	b) die Schaffung eines Kooperationsmechanismus zwischen den Mitgliedstaaten zur Gewährleistung einer einheitlichen Anwendung dieser Richtlinie in der Union, damit erforderlichenfalls in koordinierter, effizienter Weise mit Sicherheitsrisiken und -vorfällen, die Netze

und Informationssysteme beeinträchtigen, umgegangen bzw. darauf reagiert werden kann;	und Informationssysteme beeinträchtigen, ***unter Mitwirkung der Betroffenen*** umgegangen bzw. darauf reagiert werden kann;

Änderungsantrag 40

Vorschlag für eine Richtlinie
Artikel 1 – Absatz 6

Vorschlag der Kommission	*Geänderter Text*
6. Der Austausch von Informationen über das Kooperationsnetz nach Kapitel III und die Meldung von NIS-Vorfällen nach Artikel 14 können die Verarbeitung von personenbezogenen Daten erforderlich machen. Eine solche Verarbeitung personenbezogener Daten, die notwendig ist, um die mit dieser Richtlinie verfolgten Ziele des öffentlichen Interesses zu erreichen, wird von den Mitgliedstaaten nach Artikel 7 der Richtlinie 95/46/EG und der Richtlinie 2002/58/EG in ihrer in einzelstaatliches Recht umgesetzten Form genehmigt.	6. Der Austausch von Informationen über das Kooperationsnetz nach Kapitel III und die Meldung von NIS-Vorfällen nach Artikel 14 können eine Mitteilung an vertrauenswürdige Dritte sowie die Verarbeitung von personenbezogenen Daten erforderlich machen. Eine solche Verarbeitung personenbezogener Daten, die notwendig ist, um die mit dieser Richtlinie verfolgten Ziele des öffentlichen Interesses zu erreichen, wird von den Mitgliedstaaten nach Artikel 7 der Richtlinie 95/46/EG und der Richtlinie 2002/58/EG in ihrer in einzelstaatliches Recht umgesetzten Form genehmigt. ***Die Mitgliedstaaten erlassen Rechtsvorschriften gemäß Artikel 13 der Richtlinie 95/46/EG, um sicherzustellen, dass öffentliche Verwaltungen, Marktteilnehmer und zuständige Behörden nicht haftbar gemacht werden, wenn sie personenbezogene Daten verarbeiten, die für den Informationsaustausch im Rahmen des Kooperationsnetzes und der Meldung von Sicherheitsvorfällen benötigt werden.***

Änderungsantrag 41

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
Unbeschadet ihrer Verpflichtungen nach dem Unionsrecht werden die Mitgliedstaaten nicht daran gehindert, Bestimmungen zur Gewährleistung eines höheren Sicherheitsniveaus zu erlassen oder aufrechtzuerhalten.	Unbeschadet ihrer Verpflichtungen nach dem Unionsrecht werden die Mitgliedstaaten nicht daran gehindert, Bestimmungen zur Gewährleistung eines höheren Sicherheitsniveaus zu erlassen oder aufrechtzuerhalten***, die sich im Einklang mit der Charta der Grundrechte der EU befinden***.

Begründung

Der Ermessenspielraum, der den Mitgliedstaaten in Bezug auf Sicherheitsfragen eingeräumt wird, sollte von der Einhaltung der in der Charta der Grundrechte der EU anerkannten Rechte abhängig gemacht werden, sprich unter anderem von der Einhaltung des Rechts auf Achtung des Privatlebens und der Kommunikation, des Rechts auf Schutz personenbezogener Daten, des Rechts auf unternehmerische Freiheit und des Rechts auf einen wirksamen Rechtsbehelf.

Änderungsantrag 42

Vorschlag für eine Richtlinie
Artikel 3 – Absatz 1 – Nummer 1 – point b

Vorschlag der Kommission	*Geänderter Text*
b) Vorrichtungen oder Gruppen miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung ***von Computerdaten*** durchführen sowie	b) Vorrichtungen oder Gruppen miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung ***digitaler Daten*** durchführen**,** sowie

Änderungsantrag 43

Vorschlag für eine Richtlinie

Artikel 3 – Absatz 1 – Nummer 1 – point c

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

Änderungsantrag 44

Vorschlag für eine Richtlinie
Artikel 3 – Absatz 1 – Nummer 2

Vorschlag der Kommission	*Geänderter Text*
(2) „Sicherheit“ die Fähigkeit von Netzen und Informationssystemen, bei einem bestimmten Vertrauensniveau Störungen und böswillige Angriffe abzuwehren, die die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit gespeicherter oder übermittelter Daten oder entsprechender Dienste beeinträchtigen, die über dieses Netz und Informationssystem angeboten werden beziehungsweise zugänglich sind;	(2) „Sicherheit“ die Fähigkeit von Netzen und Informationssystemen, bei einem bestimmten Vertrauensniveau Störungen und böswillige Angriffe abzuwehren, die die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit gespeicherter oder übermittelter Daten oder entsprechender Dienste beeinträchtigen, die über dieses Netz und Informationssystem angeboten werden beziehungsweise zugänglich sind; ***nach dieser Definition umfasst „Sicherheit“ technische Geräte, Lösungen und Betriebsabläufe, die es ermöglichen, die in der vorliegenden Richtlinie vorgesehenen Sicherheitsanforderungen zu erfüllen;***

Änderungsantrag 45

Vorschlag für eine Richtlinie
Artikel 3 – Absatz 1 – Nummer 4

Vorschlag der Kommission	*Geänderter Text*
(4) „Sicherheitsvorfälle“ alle Umstände oder Ereignisse, die tatsächlich negative Auswirkungen auf die Sicherheit haben;	(4) „Sicherheitsvorfälle“ alle ***nach vernünftigem Ermessen ermittelten*** Umstände oder Ereignisse, die tatsächlich negative Auswirkungen auf die Sicherheit haben;

Begründung

Der ursprüngliche Wortlaut war zu allgemein und hätte die Anwendung der Definition erschwert.

Änderungsantrag 46

Vorschlag für eine Richtlinie
Artikel 3 – Absatz 1 – Nummer 5

Vorschlag der Kommission	*Geänderter Text*
(5) „Dienst der Informationsgesellschaft“ einen Dienst im Sinne der Nummer 2 des Artikels 1 der Richtlinie 98/34/EG;	***entfällt***

Änderungsantrag 47

Vorschlag für eine Richtlinie
Artikel 3 – Absatz 1 – Nummer 8 – Buchstabe a

Vorschlag der Kommission	*Geänderter Text*
a) Anbieter von Diensten der Informationsgesellschaft, die die Bereitstellung anderer Dienste der Informationsgesellschaft ermöglichen; Anhang II enthält eine nicht erschöpfende Liste solcher Anbieter;	***entfällt***

Änderungsantrag 48

Vorschlag für eine Richtlinie
Artikel 3 – Absatz 1 – Nummer 7

Vorschlag der Kommission	*Geänderter Text*
(7) „Bewältigung von Sicherheitsvorfällen“ alle Verfahren zur Unterstützung der Analyse, Eindämmung und Reaktion im Falle von Sicherheitsvorfällen;	(7) „Bewältigung von Sicherheitsvorfällen“ alle Verfahren zur Unterstützung der ***Erkennung, Vorbeugung,*** Analyse, Eindämmung und Reaktion im Falle von Sicherheitsvorfällen;

Änderungsantrag 49

Vorschlag für eine Richtlinie
Artikel 3 – Absatz 1 – Nummer 8

Vorschlag der Kommission	*Geänderter Text*
a) Anbieter von Diensten der Informationsgesellschaft, die die Bereitstellung anderer Dienste der Informationsgesellschaft ermöglichen; Anhang II enthält eine nicht erschöpfende Liste solcher Anbieter;	
b) Betreiber ***kritischer*** Infrastrukturen, die für die Aufrechterhaltung zentraler wirtschaftlicher und gesellschaftlicher Tätigkeiten in den Bereichen Energie, Verkehr, Banken, ***Börsen*** und Gesundheit unerlässlich sind; Anhang II enthält eine ***nicht erschöpfende*** Liste dieser Betreiber;	b) ***öffentliche oder private*** Betreiber ***von*** Infrastrukturen, die für die Aufrechterhaltung zentraler wirtschaftlicher und gesellschaftlicher Tätigkeiten in den Bereichen Energie, Verkehr, Banken, ***Finanzmarkt*** und Gesundheit unerlässlich sind ***und deren Unterbrechung oder Zerstörung in einem Mitgliedstaat erhebliche Folgen hätte, weil deren Funktionsfähigkeit nicht aufrechterhalten werden könnte***; Anhang II enthält eine Liste dieser Betreiber;

Änderungsantrag 50

Vorschlag für eine Richtlinie
Artikel 3 – Absatz 1 – Nummer 8 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(8a) „Sicherheitsvorfall mit beträchtlichen Auswirkungen“ einen Sicherheitsvorfall, der die Sicherheit und Kontinuität eines Informationsnetzes oder –systems so stark beeinträchtigt, dass es zu erheblichen Störungen zentraler wirtschaftlicher und gesellschaftlicher Funktionen kommt;

Änderungsantrag 51

Vorschlag für eine Richtlinie
Artikel 3 – Absatz 1 – Nummer 8 b (neu)

Vorschlag der Kommission	*Geänderter Text*
	(8b) „Dienst“ eine von einem Marktteilnehmer erbrachte Dienstleistung, unter Ausschluss aller anderen Dienstleistungen dieser öffentlichen Verwaltung oder dieses Marktteilnehmers;

Änderungsantrag 52

Vorschlag für eine Richtlinie
Artikel 3 – Absatz 1 – Nummer 11 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(11a) „geregelter Markt“ einen Markt im Sinne von Absatz 4 Nummer 14 der Richtlinie 2004/39/EG des Europäischen Parlaments und des Rates[28a];

[28a] Richtlinie 2004/39/EG des Europäischen Parlaments und des Rates vom 21. April 2004 über Märkte für Finanzinstrumente (ABl. L 45 vom 16.2.2005, S. 18).

Änderungsantrag 53

Vorschlag für eine Richtlinie
Artikel 3 – Absatz 1 – Nummer 11 b (neu)

Vorschlag der Kommission	*Geänderter Text*
	(11b) „multilaterales Handelssystem (MTF)“ ein multilaterales Handelssystem im Sinne von Artikel 4 Nummer 15 der Richtlinie 2004/39/EG;

Änderungsantrag 54

Vorschlag für eine Richtlinie
Artikel 3 – Absatz 1 – Nummer 11 c (neu)

Vorschlag der Kommission	*Geänderter Text*
	(11c) „organisiertes Handelssystem“ (OTF) ein/eine von einer Wertpapierfirma oder einem Marktbetreiber betriebenes multilaterales System oder betriebene multilaterale Fazilität, bei dem/der es sich nicht um einen geregelten Markt oder ein multilaterales Handelssystem oder eine zentrale Gegenpartei handelt und das/die die Interessen einer Vielzahl Dritter am Kauf und Verkauf von Schuldverschreibungen, strukturierten Finanzprodukten, Emissionszertifikaten oder Derivaten innerhalb des Systems in einer Weise zusammenführt, die zu einem Vertrag gemäß den Bestimmungen des Titels II der Richtlinie 2004/39/EG führt;

Änderungsantrag 55

Vorschlag für eine Richtlinie
Artikel 4 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
Die Mitgliedstaaten gewährleisten in Übereinstimmung mit dieser Richtlinie eine hohe Netz- und Informationssicherheit in ihren Hoheitsgebieten.	Die Mitgliedstaaten gewährleisten in Übereinstimmung mit ***der Charta der Grundrechte der EU und mit*** dieser Richtlinie eine ***nachhaltige, kontinuierlich*** hohe Netz- und Informationssicherheit in ihren Hoheitsgebieten.

Begründung

Der Ermessenspielraum, der den Mitgliedstaaten in Bezug auf Sicherheitsfragen eingeräumt wird, sollte von der Einhaltung der in der Charta der Grundrechte der EU anerkannten Rechte abhängig gemacht werden, sprich unter anderem von der Einhaltung des Rechts auf Achtung des Privatlebens und der Kommunikation, des Rechts auf Schutz personenbezogener Daten, des Rechts auf unternehmerische Freiheit und des Rechts auf einen wirksamen Rechtsbehelf.

Änderungsantrag 56

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 1 – Buchstabe e a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(ea) Die Mitgliedstaaten können die Europäische Agentur für Netz- und Informationssicherheit (ENISA) um Unterstützung bei der Entwicklung ihrer nationalen NIS-Strategien und ihrer nationalen NIS-Kooperationspläne auf der Basis eines gemeinsamen Konzepts für Mindestanforderungen an NIS-Strategien und -Kooperationspläne ersuchen.

Änderungsantrag 57

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe a

Vorschlag der Kommission	*Geänderter Text*
a) einen ***Risikobewertungsplan zur*** Bestimmung ***der*** Risiken ***und zur*** Bewertung der Auswirkungen potenzieller Sicherheitsvorfälle;	a) einen ***Rahmen für das Risikomanagement, der die*** Bestimmung***, Priorisierung, Evaluierung und Behandlung von*** Risiken***, die*** Bewertung der Auswirkungen potenzieller Sicherheitsvorfälle***, Präventions- und Kontrollmöglichkeiten und Kriterien für die Auswahl möglicher Gegenmaßnahmen umfasst***;

Änderungsantrag 58

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
b) Festlegung der Aufgaben und Zuständigkeiten der verschiedenen an der Umsetzung des ***Plans Beteiligten***;	b) Festlegung der Aufgaben und Zuständigkeiten der verschiedenen ***Behörden und anderen Akteure, die*** an der Umsetzung des ***Rahmens beteiligt sind***;

Änderungsantrag 59

Vorschlag für eine Richtlinie
Artikel 6 – title

Vorschlag der Kommission	*Geänderter Text*
Für die Netz- und Informationssicherheit zuständige nationale ***Behörde***	Für die Netz- und Informationssicherheit zuständige nationale ***Behörden und zentrale Anlaufstellen***

Änderungsantrag 60

Vorschlag für eine Richtlinie
Artikel 6 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
1. Jeder Mitgliedstaat benennt eine für die Netz- und Informationssicherheit zuständige nationale ***Behörde*** (im Folgenden „zuständige Behörde“).	1. Jeder Mitgliedstaat benennt eine ***oder mehrere*** für die Netz- und Informationssicherheit zuständige nationale ***Behörden*** (im Folgenden „zuständige Behörde“).

Änderungsantrag 61

Vorschlag für eine Richtlinie
Artikel 6 – Absatz 2 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	2a. Benennt ein Mitgliedstaat mehr als eine zuständige Behörde, benennt er eine nationale Behörde, beispielsweise eine zuständige Behörde, als nationale zentrale Anlaufstelle für die Netz- und Informationssicherheit (im Folgenden „zentrale Anlaufstelle“). Benennt ein Mitgliedstaat nur eine zuständige Behörde, ist diese zuständige Behörde auch die zentrale Anlaufstelle.

Änderungsantrag 62

Vorschlag für eine Richtlinie
Artikel 6 – Absatz 2 b (neu)

Vorschlag der Kommission	*Geänderter Text*
	2b. Die zuständigen Behörden und die zentrale Anlaufstelle eines Mitgliedstaats arbeiten im Hinblick auf die Verpflichtungen gemäß dieser Richtlinie eng zusammen.

Änderungsantrag 63

Vorschlag für eine Richtlinie
Artikel 6 – Absatz 2 c (neu)

Vorschlag der Kommission	*Geänderter Text*
	2c. Die zentrale Anlaufstelle sorgt für die länderübergreifende Zusammenarbeit mit anderen zentralen Anlaufstellen.

Änderungsantrag 64

Vorschlag für eine Richtlinie
Artikel 6 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
3. Die Mitgliedstaaten gewährleisten, dass die zuständigen Behörden mit angemessenen technischen, finanziellen und personellen Ressourcen ausgestattet sind, damit sie die ihnen übertragenen Aufgaben wirksam und effizient wahrnehmen und die Ziele dieser Richtlinie erreicht werden. Die Mitgliedstaaten stellen eine wirksame, effiziente und sichere Zusammenarbeit der ***zuständigen Behörden*** über das in Artikel 8 genannte Netz sicher.	3. Die Mitgliedstaaten gewährleisten, dass die zuständigen Behörden ***und die zentralen Anlaufstellen*** mit angemessenen technischen, finanziellen und personellen Ressourcen ausgestattet sind, damit sie die ihnen übertragenen Aufgaben wirksam und effizient wahrnehmen und die Ziele dieser Richtlinie erreicht werden. Die Mitgliedstaaten stellen eine wirksame, effiziente und sichere Zusammenarbeit der ***zentralen Anlaufstellen*** über das in Artikel 8 genannte Netz sicher.

Änderungsantrag 65

Vorschlag für eine Richtlinie
Artikel 6 – Absatz 4

Vorschlag der Kommission	*Geänderter Text*
4. Die Mitgliedstaaten gewährleisten, dass die zuständigen Behörden von ***öffentlichen Verwaltungen und*** Marktteilnehmern die Meldungen der Sicherheitsvorfälle nach Artikel 14 Absatz 2 erhalten und ihnen die in Artikel 15 genannten Durchführungs-	4. Die Mitgliedstaaten gewährleisten, dass die zuständigen Behörden ***und die zentralen Anlaufstellen*** von ***den*** Marktteilnehmern die Meldungen der Sicherheitsvorfälle nach Artikel 14 Absatz 2 erhalten und ihnen die in

und Durchsetzungsbefugnisse eingeräumt werden.	Artikel 15 genannten Durchführungs- und Durchsetzungsbefugnisse eingeräumt werden.

Änderungsantrag 66

Vorschlag für eine Richtlinie
Artikel 6 – Absatz 5

Vorschlag der Kommission	*Geänderter Text*
5. Die zuständigen Behörden ***konsultieren gegebenenfalls*** die einschlägigen ***nationalen Strafverfolgungs- und*** Datenschutzbehörden***,*** und arbeiten mit ***ihnen*** zusammen.	5. Die zuständigen Behörden ***sind verpflichtet,*** die einschlägigen Datenschutzbehörden ***zu konsultieren*** und arbeiten ***gegebenenfalls*** mit ***den nationalen Strafverfolgungsbehörden und den Behörden*** zusammen.

Begründung

Gibt es nur eine Behörde, die für die Kontrolle auf nationaler Ebene zuständig ist, ohne dabei mit einer anderen, einen Ausgleich schaffenden Stelle zusammenzuarbeiten, ist dies dem Gleichgewicht zwischen dem Schutz der Sicherheit und der Freiheit abträglich.

Änderungsantrag 67

Vorschlag für eine Richtlinie
Artikel 6 – Absatz 5

Vorschlag der Kommission	*Geänderter Text*
5. Die zuständigen Behörden konsultieren gegebenenfalls die einschlägigen nationalen Strafverfolgungs- und Datenschutzbehörden, und arbeiten mit ihnen zusammen.	5. Die zuständigen Behörden ***und die zentralen Anlaufstellen*** konsultieren gegebenenfalls die einschlägigen nationalen Strafverfolgungs- und Datenschutzbehörden, und arbeiten mit ihnen zusammen.

Änderungsantrag 68

Vorschlag für eine Richtlinie
Artikel 6 – Absatz 6

Vorschlag der Kommission	*Geänderter Text*
6. Die Mitgliedstaaten teilen der Kommission unverzüglich die Benennung der zuständigen ***Behörde***, deren Aufgaben sowie etwaige spätere Änderungen mit. Die Mitgliedstaaten machen die Benennung der zuständigen ***Behörde*** öffentlich bekannt.	6. Die Mitgliedstaaten teilen der Kommission unverzüglich die Benennung der zuständigen ***Behörden und der zentralen Anlaufstelle***, deren Aufgaben sowie etwaige spätere Änderungen mit. Die Mitgliedstaaten machen die Benennung der zuständigen ***Behörden*** öffentlich bekannt.

Änderungsantrag 69

Vorschlag für eine Richtlinie
Artikel 7 – Absatz 1

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

Änderungsantrag 70

Vorschlag für eine Richtlinie
Artikel 7 – Absatz 5

Vorschlag der Kommission	*Geänderter Text*
5. ***Das CERT untersteht*** der Aufsicht der zuständigen Behörde, die die Angemessenheit der ***ihm*** zur Verfügung gestellten Ressourcen, ***sein Mandat*** und die Wirksamkeit ***seines Verfahrens*** zur	5. ***Die CERTs unterstehen*** der Aufsicht der zuständigen Behörde ***oder der zentralen Anlaufstelle***, die die Angemessenheit der ***ihnen*** zur Verfügung gestellten Ressourcen, ***ihre Mandate*** und

Bewältigung von Sicherheitsvorfällen regelmäßig überprüft.	die Wirksamkeit ***ihrer Verfahren*** zur Bewältigung von Sicherheitsvorfällen regelmäßig überprüft.

Änderungsantrag 71

Vorschlag für eine Richtlinie
Artikel 7 – Absatz 5 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	5a. Die Mitgliedstaaten stellen sicher, dass die CERTs mit angemessenen personellen und finanziellen Ressourcen ausgestattet sind, damit sie sich aktiv an internationalen Kooperationsnetzen und insbesondere Kooperationsnetzen der Union beteiligen können.

Änderungsantrag 72

Vorschlag für eine Richtlinie
Artikel 7 – Absatz 5 – Unterabsatz 1 (neu)

Vorschlag der Kommission	*Geänderter Text*
	(1) Das CERT wird in die Lage versetzt und aufgefordert, gemeinsame Übungen mit bestimmten CERTs, mit den CERTs aller Mitgliedstaaten und mit entsprechenden Einrichtungen in Nicht-Mitgliedstaaten sowie mit CERTs von multinationalen und internationalen Institutionen wie NATO und VN zu initiieren und sich daran zu beteiligen.

Änderungsantrag 73

Vorschlag für eine Richtlinie
Artikel 7 – Absatz 5 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	5a. Die Mitgliedstaaten können die Europäische Agentur für Netz- und Informationssicherheit (ENISA) oder andere Mitgliedstaaten um Unterstützung bei der Entwicklung ihrer nationalen CERTs ersuchen.

Änderungsantrag 74

Vorschlag für eine Richtlinie
Artikel 8

Vorschlag der Kommission	*Geänderter Text*
1. Die ***zuständigen Behörden*** und die Kommission bilden ein Netz (im Folgenden „Kooperationsnetz“) ***für die Zusammenarbeit*** bei der Bewältigung von Sicherheitsrisiken und -vorfällen, die Netze und Informationssysteme betreffen.	1. Die ***zentralen Anlaufstellen, die die Europäische Agentur für Netz-*** und ***Informationssicherheit (ENISA) und*** die Kommission bilden ein Netz (im Folgenden „Kooperationsnetz“)***, in dem sie*** bei der Bewältigung von Sicherheitsrisiken und -vorfällen, die Netze und Informationssysteme betreffen***, zusammenarbeiten***.
2. Die Kommission und die ***zuständigen Behörden*** stehen über das Kooperationsnetz in ständigem Kontakt. ***Auf Anfrage kann*** die Europäische Agentur für Netz- und Informationssicherheit (ENISA) das Kooperationsnetz mit Know-how und Beratung ***unterstützen***.	2. Die Kommission und die ***zentralen Anlaufstellen*** stehen über das Kooperationsnetz in ständigem Kontakt. Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) ***unterstützt*** das Kooperationsnetz mit Know-how und Beratung. ***Das Kooperationsnetz arbeitet falls notwendig mit den Datenschutzbehörden zusammen.***
3. Die ***zuständigen Behörden*** haben innerhalb des Netzes folgende Aufgaben:	3. Die ***zentralen Anlaufstellen*** haben innerhalb des Netzes folgende Aufgaben:
a) Verbreitung von Frühwarnungen vor Sicherheitsrisiken und -vorfällen nach Artikel 10;	a) Verbreitung von Frühwarnungen vor Sicherheitsrisiken und -vorfällen nach Artikel 10;
b) Gewährleistung einer koordinierten Reaktion nach Artikel 11;	b) Gewährleistung einer koordinierten Reaktion nach Artikel 11;

c) regelmäßige Veröffentlichung nichtvertraulicher Informationen über laufende Frühwarnungen und koordinierte Reaktionen auf einer gemeinsamen Website;	c) regelmäßige Veröffentlichung nichtvertraulicher Informationen über laufende Frühwarnungen und koordinierte Reaktionen auf einer gemeinsamen Website;
	(ca) gemeinsame Erörterung, Vereinbarung einer gemeinsamen Auslegung, einheitliche Anwendung und Koordinierung ihrer Maßnahmen in Bezug auf Sicherheitsanforderungen und Meldung von Sicherheitsvorfällen laut Artikel 14 und auf Umsetzung und Durchsetzung laut Artikel 15;
(d) ***auf Anfrage eines Mitgliedstaats oder der Kommission*** die gemeinsame Erörterung und Bewertung einer oder mehrerer der in Artikel 5 genannten nationalen NIS-Strategien und NIS-Kooperationspläne innerhalb des Geltungsbereichs der Richtlinie;	(d) die gemeinsame Erörterung und Bewertung einer oder mehrerer der in Artikel 5 genannten nationalen NIS-Strategien und NIS-Kooperationspläne innerhalb des Geltungsbereichs der Richtlinie;
e) auf Anfrage eines Mitgliedstaats oder der Kommission die gemeinsame Erörterung und Bewertung der Wirksamkeit der CERTs, insbesondere bei der Durchführung von NIS-Übungen auf Unionsebene;	e) auf Anfrage eines Mitgliedstaats oder der Kommission die gemeinsame Erörterung und Bewertung der Wirksamkeit der CERTs ***unverzüglich***, insbesondere bei der Durchführung von NIS-Übungen auf Unionsebene***, und Umsetzung von Maßnahmen zur Behebung erkannter Schwachstellen***;
f) Zusammenarbeit und Informationsaustausch in Bezug auf alle einschlägigen Angelegenheiten mit ***dem bei Europol angesiedelten Europäischen Zentrum zur Bekämpfung der Cyberkriminalität*** und anderen einschlägigen europäischen Einrichtungen in den Bereichen Datenschutz, Energie, Verkehr, Banken, Börsen und Gesundheit;	f) Zusammenarbeit und Informationsaustausch in Bezug auf alle einschlägigen Angelegenheiten ***im Zusammenhang*** mit ***der Netz-*** und ***Informationssicherheit mit*** anderen einschlägigen europäischen Einrichtungen in den Bereichen Datenschutz, Energie, Verkehr, Banken, Börsen und Gesundheit;
	(fa) Diskussion und Einigung über die gemeinsame Auslegung, konsequente Anwendung und harmonisierte Umsetzung der Bestimmungen aus Kapitel IV innerhalb der Union;
(g) Austausch von Informationen und	(g) Austausch von Informationen und

bewährten Verfahren untereinander und mit der Kommission sowie gegenseitige Unterstützung beim Kapazitätsaufbau im Bereich der NIS;

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

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

bewährten Verfahren untereinander und mit der Kommission sowie gegenseitige Unterstützung beim Kapazitätsaufbau im Bereich der NIS;

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

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

(ia) aktive Förderung der Beteiligung sowie Konsultation und Informationsaustausch mit Marktteilnehmern.

Die Kommission informiert das Kooperationsnetz regelmäßig über Sicherheitsforschung und andere entsprechende Programme von Horizont 2020.

3a. Marktteilnehmer und die zuständigen öffentlichen Verwaltungsbehörden werden, falls notwendig, auch zur Mitwirkung an den Aufgaben des Kooperationsnetzes gemäß Absatz 3 Buchstaben c, g, h und i aufgefordert.

3b. Sofern Informationen, Frühwarnungen oder bewährte Verfahren, die von Marktteilnehmern oder öffentlichen Verwaltungen stammen, innerhalb des Kooperationsnetzes ausgetauscht oder von diesem preisgegeben werden, erfolgt dieser Austausch bzw. diese Preisgabe im Einklang mit der in der ursprünglichen Quelle festgelegten Klassifizierung der Informationen gemäß Artikel 9 Absatz 1.

3c. Die Kommission veröffentlicht einmal jährlich einen Bericht über die vorangegangenen zwölf Monate, der sich auf seine Aufgaben bezieht und auf dem gemäß Artikel 14 Absatz 4 dieser Richtlinie vorgelegten

	zusammenfassenden Berichts beruht. Bei der Bekanntmachung jeglicher, einzelner Sicherheitsvorfälle, die den zuständigen Behörden und den zentralen Anlaufstellen 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 Marktteilnehmern, die solche Sicherheitsvorfälle gemeldet haben, entstehen kann. Eine solche Bekanntmachung darf nur nach vorheriger Konsultation durchgeführt werden.
4. Die Kommission legt mittels Durchführungsrechtsakten die erforderlichen Modalitäten für eine Erleichterung der in den Absätzen 2 und 3 genannten Zusammenarbeit zwischen den ***zuständigen Behörden*** und der Kommission fest. Diese Durchführungsrechtsakte werden nach dem in Artikel 19 Absatz 2 genannten Konsultationsverfahren angenommen.	4. Die Kommission legt mittels Durchführungsrechtsakten die erforderlichen Modalitäten für eine Erleichterung der in den Absätzen 2 und 3 genannten Zusammenarbeit zwischen den ***zentralen Anlaufstellen, der ENISA*** und der Kommission fest. Diese Durchführungsrechtsakte werden nach dem in Artikel 19 Absatz 2 genannten Konsultationsverfahren angenommen.

Änderungsantrag 75

Vorschlag für eine Richtlinie
Artikel 9 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
1. Der Austausch sensibler und vertraulicher Informationen über das Kooperationsnetz erfolgt über eine sichere Infrastruktur.	Der Austausch sensibler und vertraulicher Informationen über das Kooperationsnetz erfolgt über eine sichere Infrastruktur, die unter Aufsicht der ENISA betrieben wird. ***Die Mitgliedsstaaten sichern zu, dass von anderen Staaten oder der Kommission geteilte sensible oder geheime Informationen nicht mit Drittstaaten geteilt oder zweckfremd, beispielsweise für***

	Geheimdiensttätigkeiten oder Wirtschaftsentscheidungen, genutzt werden;

Änderungsantrag 76

Vorschlag für eine Richtlinie
Artikel 9 – Absatz 2 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
2. Die Kommission wird nach ***Artikel 18*** ermächtigt, ***delegierte Rechtsakte*** zu erlassen, die die Festlegung von Kriterien im Hinblick auf nachstehende Aspekte betreffen, die ***ein Mitgliedstaat*** zu erfüllen hat, um für die Teilnahme am sicheren System für den Informationsaustausch zugelassen zu werden:	2. Die Kommission wird nach ***Artikel 19*** ermächtigt, ***Durchführungsrechtsakte*** zu erlassen, die die Festlegung von Kriterien im Hinblick auf nachstehende Aspekte betreffen, die ***eine zentrale Anlaufstelle*** zu erfüllen hat, um für die Teilnahme am sicheren System für den Informationsaustausch zugelassen zu werden:

Änderungsantrag 77

Vorschlag für eine Richtlinie
Artikel 9 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
3. Die Kommission erlässt ***nach den in den Absätzen 2 und 3 genannten Kriterien*** mittels Durchführungsrechtsakten ***Beschlüsse über den Zugang der Mitgliedstaaten zu dieser sicheren Infrastruktur***. Diese Durchführungsrechtsakte werden nach dem in Artikel 19 Absatz 3 genannten Prüfverfahren angenommen.	3. Die Kommission erlässt mittels Durchführungsrechtsakten ***ein einheitliches Paket von Zusammenschlüssen und Sicherheitsstandards, die zentrale Anlaufstellen für einen Informationsaustausch erfüllen müssen***. Diese Durchführungsrechtsakte werden nach dem in Artikel 19 Absatz 3 genannten Prüfverfahren angenommen.

Änderungsantrag 78

Vorschlag für eine Richtlinie
Artikel 10

Vorschlag der Kommission	*Geänderter Text*
1. Die ***zuständigen Behörden*** oder die Kommission geben im Kooperationsnetz Frühwarnungen zu solchen Sicherheitsrisiken und -vorfällen aus, die mindestens eine der folgenden Voraussetzungen erfüllen:	1. Die ***zentralen Anlaufstellen*** oder die Kommission geben im Kooperationsnetz Frühwarnungen zu solchen Sicherheitsrisiken und -vorfällen aus, die mindestens eine der folgenden Voraussetzungen erfüllen:
a) sie weiten sich rasch aus oder können sich rasch ausweiten;	
b) ***sie übersteigen*** die nationale Reaktionskapazität ***oder können diese übersteigen***;	b) die ***zentrale Anlaufstelle beurteilt, ob das Sicherheitsrisiko oder der Sicherheitsvorfall rasch wächst oder rasch wachsen könnte und die*** nationale Reaktionskapazität ***möglicherweise übersteigt***;
c) ***sie betreffen*** oder ***können*** mehr als einen Mitgliedstaat ***betreffen***.	c) ***die zentrale Anlaufstelle gelangt zu der Einschätzung, dass das Sicherheitsrisiko*** oder ***der Sicherheitsvorfall*** mehr als einen Mitgliedstaat ***betrifft***.
2. Bei Frühwarnungen stellen die ***zuständigen Behörden*** und die Kommission alle in ihrem Besitz befindlichen relevanten Informationen zur Verfügung, die für die Beurteilung der Sicherheitsrisiken oder -vorfälle von Nutzen sein können.	2. Bei Frühwarnungen stellen die ***zentralen Anlaufstellen*** und die Kommission ***unverzüglich*** alle in ihrem Besitz befindlichen relevanten Informationen zur Verfügung, die für die Beurteilung der Sicherheitsrisiken oder -vorfälle von Nutzen sein können. ***Informationen, die von dem betroffenen Marktteilnehmer als klassifiziert oder vertraulich eingestuft werden, sowie die Identität dieses Marktteilnehmers werden nur in dem Umfang offengelegt, wie dies zur Beurteilung des Risikos oder des Sicherheitsvorfalls erforderlich ist.***
3. Die Kommission kann auf Anfrage eines Mitgliedstaats oder von Amts wegen einen anderen Mitgliedstaat ersuchen, relevante Informationen zu einem bestimmten	3. Die Kommission kann auf Anfrage eines Mitgliedstaats oder von Amts wegen einen anderen Mitgliedstaat ersuchen, relevante***, nicht als Verschlusssache eingestufte*** Informationen zu einem bestimmten

Sicherheitsrisiko oder -vorfall vorzulegen.	Sicherheitsrisiko oder -vorfall vorzulegen.
4. Hat das der Frühwarnung zugrundeliegende Sicherheitsrisiko bzw. der Sicherheitsvorfall einen mutmaßlich kriminellen Hintergrund, ***informieren*** die ***zuständigen Behörden oder die*** Kommission ***das bei Europol angesiedelte Europäische*** Zentrum zur Bekämpfung der Cyberkriminalität.	4. Hat das der Frühwarnung zugrundeliegende Sicherheitsrisiko bzw. der Sicherheitsvorfall einen mutmaßlich ***schwerwiegenden*** kriminellen Hintergrund, ***setzen sich*** die ***zentralen Anlaufstellen und die*** Kommission ***falls erforderlich mit den Behörden zur Bekämpfung von Cyberkriminalität in Verbindung und versetzen sie in die Lage, unverzüglich mit dem Europäischen*** Zentrum zur Bekämpfung der Cyberkriminalität ***zusammenzuarbeiten und Informationen mit diesem auszutauschen***.
	4 a. Mitglieder des Kooperationsnetzes veröffentlichen gemäß Absatz 1 keinerlei erhaltene Informationen bezüglich Sicherheitsrisiken oder -vorfälle, ohne die vorherige Genehmigung der meldenden zentralen Anlaufstelle erhalten zu haben.
	4b. Hat das der Frühwarnung zugrundeliegende Sicherheitsrisiko bzw. der Sicherheitsvorfall einen mutmaßlich schwerwiegenden grenzüberschreitenden technischen Hintergrund, informieren die zuständigen Behörden oder die zentralen Anlaufstellen oder die Kommission Kommission die ENISA.
5. Die Kommission wird ermächtigt, ***delegierte Rechtsakte*** nach ***Artikel 18*** zur Präzisierung der Sicherheitsrisiken und -vorfälle zu erlassen, die die in Absatz 1 genannten Frühwarnungen auslösen.	5. Die Kommission wird ermächtigt, ***Durchführungsrechtsakte*** nach ***Artikel 19*** zur Präzisierung der Sicherheitsrisiken und -vorfälle zu erlassen, die die in Absatz 1 genannten Frühwarnungen ***sowie die Verfahren zur Weitergabe sensibler Informationen für Marktteilnehmer*** auslösen.

Änderungsantrag 79

Vorschlag für eine Richtlinie
Artikel 11 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
1. Im Anschluss an eine Frühwarnung nach Artikel 10 einigen sich die ***zuständigen Behörden*** nach einer Bewertung der einschlägigen Informationen auf eine koordinierte Reaktion gemäß dem in Artikel 12 genannten NIS-Kooperationsplan der Union.	1. Im Anschluss an eine Frühwarnung nach Artikel 10 einigen sich die ***zentralen Anlaufstellen unverzüglich*** nach einer Bewertung der einschlägigen Informationen auf eine koordinierte Reaktion gemäß dem in Artikel 12 genannten NIS-Kooperationsplan der Union.

Änderungsantrag 80

Vorschlag für eine Richtlinie
Artikel 12 – Absatz 2 – point a – indent 1

Vorschlag der Kommission	*Geänderter Text*
– die Festlegung der Form und der Verfahren für die Einholung und den Austausch geeigneter und vergleichbarer Informationen über Sicherheitsrisiken und -vorfälle durch die ***zuständigen Behörden***,	– die Festlegung der Form und der Verfahren für die Einholung und den Austausch geeigneter und vergleichbarer Informationen über Sicherheitsrisiken und -vorfälle durch die ***zentralen Anlaufstellen***,

Änderungsantrag 81

Vorschlag für eine Richtlinie
Artikel 12 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
3. Der NIS-Kooperationsplan wird spätestens ein Jahr nach dem Inkrafttreten dieser Richtlinie angenommen und regelmäßig überarbeitet.	3. Der NIS-Kooperationsplan wird spätestens ein Jahr nach dem Inkrafttreten dieser Richtlinie angenommen und regelmäßig überarbeitet. ***Über die Ergebnisse jeder Überarbeitung wird dem Europäischen Parlament Bericht erstattet.***

Änderungsantrag 82

Vorschlag für eine Richtlinie
Artikel 12 – Absatz 3 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	3a. Die Kommission legt einen Haushaltsplan für die Entwicklung des NIS-Kooperationsplans der Union vor.

Änderungsantrag 83

Vorschlag für eine Richtlinie
Artikel 13 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
Unbeschadet der Möglichkeiten des Kooperationsnetzes, auf internationaler Ebene informell zusammenzuarbeiten, kann die Union internationale Vereinbarungen mit Drittländern oder internationalen Organisationen schließen, in denen deren Beteiligung an bestimmten Aktivitäten des Kooperationsnetzes ermöglicht und geregelt wird. In solchen Vereinbarungen wird der Notwendigkeit eines angemessenen Schutzes der im Kooperationsnetz zirkulierenden personenbezogenen Daten Rechnung getragen.	Unbeschadet der Möglichkeiten des Kooperationsnetzes, auf internationaler Ebene informell zusammenzuarbeiten, kann die Union internationale Vereinbarungen mit Drittländern oder internationalen Organisationen schließen, in denen deren Beteiligung an bestimmten Aktivitäten des Kooperationsnetzes ermöglicht und geregelt wird. In den Vereinbarungen werden die zur Sicherstellung des Schutzes der im Kooperationsnetz zirkulierenden personenbezogenen Daten umzusetzenden Kontrollverfahren angegeben. ***Das Europäische Parlament wird über die Verhandlungen in Bezug auf die Vereinbarung in Kenntnis gesetzt und die Transparenz des Inhalts der Vereinbarung wird sichergestellt. Die Übermittlung personenbezogener Daten an Empfänger in Ländern außerhalb der Union erfolgt nach Maßgabe der Artikel 25 und 26 der Richtlinie 95/46/EG und des Artikels 9 der Verordnung (EG) Nr. 45/2001.***

Begründung

Die mit anderen Ländern oder Sicherheitsbehörden geschlossenen internationalen Vereinbarungen müssen zwingend einen Mechanismus zur Kontrolle der Achtung der bürgerlichen Rechte enthalten. Zudem sollte eine wirksame demokratische Kontrolle der Vereinbarungen vonseiten des Europäischen Parlaments ausgeübt werden, welches rechtzeitig über die Inhalte der Verhandlungen über die Vereinbarung in Kenntnis zu setzen ist.

Änderungsantrag 84

Vorschlag für eine Richtlinie
Artikel 14

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

2. Die Mitgliedstaaten gewährleisten, dass ***öffentliche Verwaltungen und*** Marktteilnehmer den zuständigen Behörden Sicherheitsvorfälle melden, die erhebliche Auswirkungen auf die Sicherheit der von ihnen bereitgestellten Kerndienste haben.	2. Die Mitgliedstaaten ***ergreifen Maßnahmen, die*** gewährleisten, dass ***die*** Marktteilnehmer den zuständigen Behörden Sicherheitsvorfälle ***unverzüglich*** melden, die erhebliche Auswirkungen auf die Sicherheit ***oder Kontinuität*** der von ihnen bereitgestellten Kerndienste haben. ***Die Benachrichtigung führt nicht zu einer größeren Haftung der benachrichtigenden Seite. Zur Feststellung des Ausmaßes der Auswirkungen eines Sicherheitsvorfalls werden unter anderem folgende Parameter herangezogen:*** ***a) die Anzahl der Nutzer, deren Kerndienst betroffen ist;*** ***b) die Dauer des Sicherheitsvorfalls;*** ***c) die geografische Ausbreitung im Sinne des von dem Sicherheitsvorfall betroffenen Gebiets.*** ***Diese Kriterien werden gemäß Artikel 8 Absatz 3 Buchstabe c a (neu) näher bestimmt.*** ***2a. Die nicht unter Anhang II fallenden Einrichtungen können die Vorfälle gemäß Artikel 14 Absatz 2 freiwillig melden.*** ***2b. Der Empfänger eines Sicherheitsberichts unterrichtet die Einrichtung, die den Vorfall gemeldet hat, unverzüglich von den ergriffenen Maßnahmen sowie über sämtliche informierte Dritte und die Sicherheits und Verschlussprotokolle, die für die ausgetauschten Informationen gelten.***
3. Die Anforderungen der Absätze 1 und 2 gelten für alle Marktteilnehmer, die Dienste in der Europäischen Union bereitstellen.	3. Die Anforderungen der Absätze 1 und 2 gelten für alle Marktteilnehmer, die Dienste in der Europäischen Union bereitstellen. ***Marktteilnehmer, die keine Dienste in der Europäischen Union anbieten, können auf freiwilliger Basis über Vorfälle berichten.***

	3a. Die Mitgliedstaaten stellen sicher, dass die Marktteilnehmer den zuständigen Behörden oder der zentralen Anlaufstelle des Mitgliedstaats, in dem ein Kerndienst betroffen ist, die in den Absätzen 1 und 2 genannten Sicherheitsvorfälle melden. Sind Kerndienste in mehreren Mitgliedstaaten betroffen, warnt die zentrale Anlaufstelle, bei der die Meldung eingegangen ist, die anderen betroffenen zentralen Anlaufstellen und stützt sich dabei auf die vom Marktteilnehmer übermittelten Angaben. Der Marktteilnehmer wird unverzüglich davon in Kenntnis gesetzt, welche weiteren zentralen Anlaufstellen von dem Vorfall unterrichtet und welche Maßnahmen eingeleitet wurden. Er erhält ferner sämtliche Informationen, die für den Vorfall relevant sind.
4. ***Die zuständige Behörde kann die Öffentlichkeit unterrichten oder die öffentliche Verwaltung und die Marktteilnehmer zur Unterrichtung verpflichten, wenn sie zu dem Schluss gelangt, dass die Bekanntmachung des Sicherheitsvorfalls im öffentlichen Interesse liegt. Die zuständige Behörde legt dem Kooperationsnetz jährlich einen zusammenfassenden Bericht über die eingegangenen Meldungen und die nach diesem Absatz ergriffenen Maßnahmen vor.***	4. ***Nach Konsultation der zuständigen Behörde und des betroffenen Marktteilnehmers unterrichtet die zentrale Anlaufstelle die Öffentlichkeit über einzelne Sicherheitsvorfälle, wenn sie zu dem Ergebnis gelangt, dass der Öffentlichkeit der Sachverhalt bekannt sein muss, damit weiteren Sicherheitsvorfällen vorgebeugt werden kann oder noch andauernde Sicherheitsvorfälle behandelt werden können, die Vertreter der Öffentlichkeit in die Lage versetzt werden müssen, Folgen aus dem Vorfall für sie selbst abzumildern oder wenn ein von einem Sicherheitsvorfall betroffener Marktteilnehmer es abgelehnt hat, unverzüglich auf eine im Zusammenhang mit diesem Sicherheitsvorfall gravierende strukturelle Schwachstelle zu reagieren. Die zentrale Anlaufstelle muss eine solche Entscheidung angemessen begründen. Wenn dies für möglich gehalten wird, übermittelt die zuständige Behörde oder die zentrale Anlaufstelle den***

	Marktteilnehmern, die den Vorfall gemeldet haben, strategische, analysierte Informationen, die dazu beitragen, die sicherheitsrelevante Bedrohung zu überwinden. Die zentrale Anlaufstelle legt dem Kooperationsnetz zweimal jährlich einen zusammenfassenden Bericht über die eingegangenen Meldungen und die nach diesem Absatz ergriffenen Maßnahmen vor. Bei der Bekanntmachung jeglicher, einzelner Sicherheitsvorfälle, die den zuständigen Behörden und den zentralen Anlaufstellen 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 Marktteilnehmern, die solche Sicherheitsvorfälle gemeldet haben, entstehen kann. Eine solche Bekanntmachung darf nur nach vorheriger Konsultation durchgeführt werden.
	Werden dem Kooperationsnetz im Sinne des Artikels 8 Sicherheitsvorfälle gemeldet, veröffentlichen andere nationale zuständige Behörden keine bezüglich der Risiken oder Sicherheitsvorfälle erhaltenen Informationen, ohne die Genehmigung der unterrichtenden zuständigen Behörde erhalten zu haben.
5. Die Kommission wird nach Artikel 18 ermächtigt, delegierte Rechtsakte zu erlassen, in denen festgelegt wird, unter welchen Umständen bei Sicherheitsvorfällen für öffentliche Verwaltungen und Marktteilnehmer die Meldepflicht gilt.	
6. ***Vorbehaltlich etwaiger nach Absatz 5 erlassener delegierter Rechtsakte können die zuständigen Behörden Leitlinien annehmen und erforderlichenfalls***	6. ***Die zuständigen Behörden oder die zentrale Anlaufstelle nehmen Leitlinien zu den Umständen an, in denen für***

Anweisungen zu den Umständen herausgeben, in denen für öffentliche Verwaltungen und Marktteilnehmer die Meldepflicht gilt.	***Marktteilnehmer die Meldepflicht gilt.***
7. Die Kommission wird ermächtigt, mittels Durchführungsrechtsakten die für die Zwecke des Absatzes 2 geltenden Formen und Verfahren festzulegen. Diese Durchführungsrechtsakte werden nach dem in Artikel 19 Absatz 3 genannten Prüfverfahren angenommen.	7. Die Kommission wird ermächtigt, mittels Durchführungsrechtsakten die für die Zwecke des Absatzes 2 geltenden Formen und Verfahren festzulegen. Diese Durchführungsrechtsakte werden nach dem in Artikel 19 Absatz 3 genannten Prüfverfahren angenommen.
8. Die Absätze 1 und 2 gelten nicht für Kleinstunternehmen im Sinne der Definition der Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen[35].	8. Die Absätze 1 und 2 gelten nicht für Kleinstunternehmen im Sinne der Definition der Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen[35].
[35] ABl. L 124, 20.5.2003, S. 36.	[35] ABl. L 124, 20.5.2003, S. 36.

Änderungsantrag 85

Vorschlag für eine Richtlinie
Artikel 14 – Absatz 4 – Unterabsatz 1 (neu)

Vorschlag der Kommission	*Geänderter Text*
	Zusätzlich zur Meldung an die zuständigen Behörden werden die Marktteilnehmer ermutigt, Sicherheitsvorfälle, an denen ihre Unternehmen beteiligt sind, freiwillig in ihren Finanzberichten bekannt zu geben.

Begründung

Sicherheitsvorfälle im IT-Bereich können hohe finanzielle Verluste und erhebliche Kosten verursachen. Aktionäre und Investoren sollten über die Folgen solcher Sicherheitsvorfälle unterrichtet werden. Indem Unternehmen dazu ermutigt werden, freiwillig Sicherheitsvorfälle im IT-Bereich zu veröffentlichen, könnte die sektorübergreifende Diskussion über die Wahrscheinlichkeit künftiger Sicherheitsvorfälle, die Dimension dieser Risiken und die

Angemessenheit der ergriffenen Vorbeugungsmaßnahmen zur Verringerung von Sicherheitslücken im IT-Bereich angeregt werden.

Änderungsantrag 86

Vorschlag für eine Richtlinie
Artikel 15

Vorschlag der Kommission	*Geänderter Text*
1. Die Mitgliedstaaten gewährleisten, dass den zuständigen Behörden ***alle*** Befugnisse eingeräumt werden, die ***für die Untersuchung von Verstößen der öffentlichen Verwaltungen oder der Marktteilnehmer gegen die*** Verpflichtungen des Artikels 14 sowie deren Auswirkungen auf die Netz- und Informationssicherheit ***erforderlich sind***.	1. Die Mitgliedstaaten gewährleisten, dass den zuständigen Behörden ***und den zentralen Anlaufstellen die*** Befugnisse eingeräumt werden, ***um sicherzustellen, dass*** die Verpflichtungen des Artikels 14 sowie deren Auswirkungen auf die Netz- und Informationssicherheit ***beachtet werden***.
2. Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden befugt sind, von den Marktteilnehmern ***und den öffentlichen Verwaltungen*** zu verlangen, dass sie	2. Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden ***und die zentralen Anlaufstellen*** befugt sind, von den Marktteilnehmern zu verlangen, dass sie
a) die zur Beurteilung der Sicherheit ihrer Netze und Informationssysteme erforderlichen Informationen, einschließlich der Unterlagen über ihre Sicherheitsmaßnahmen, übermitteln;	a) die zur Beurteilung der Sicherheit ihrer Netze und Informationssysteme erforderlichen Informationen, einschließlich der Unterlagen über ihre Sicherheitsmaßnahmen, übermitteln;
b) ***sich*** einer Sicherheitsüberprüfung ***unterziehen***, die von einer qualifizierten unabhängigen Stelle oder einer ***zuständigen*** nationalen Behörde durchgeführt ***wird***, und ***deren Ergebnisse der zuständigen*** Behörde übermitteln.	b) ***Belege über die tatsächliche Umsetzung der Sicherheitsmaßnahmen vorlegen, beispielsweise die Ergebnisse*** einer Sicherheitsüberprüfung, die von ***internen Prüfern,*** einer qualifizierten unabhängigen Stelle oder einer nationalen Behörde durchgeführt ***wurde***, und ***die Belege an die zuständige*** Behörde ***oder die zentrale Anlaufstelle*** übermitteln***; dabei kann die zuständige Behörde oder die zentrale Anlaufstelle, falls notwendig, zusätzliche Belege verlangen oder ausnahmsweise und mit Abgabe einer Begründung eine zusätzliche***

Überprüfung durchführen.

Die zuständigen Behörden und die zentralen Anlaufstellen nennen bei Übermittlung ihres Ersuchens dessen Zweck und geben hinreichend genau an, welche Angaben verlangt werden.

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

3. Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden ***und die zentralen Anlaufstellen*** befugt sind, ***allen in Anhang II aufgeführten*** Marktteilnehmern verbindliche Anweisungen zu erteilen.

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

4. Die zuständigen Behörden ***und die zentrale Anlaufstelle informieren die betroffenen Marktteilnehmer über die Möglichkeit***, bei ***Sicherheitsvorfällen, bei*** denen ein schwerwiegender krimineller Hintergrund vermutet wird***, bei den Strafverfolgungsbehörden Anklage zu erheben***.

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

5. ***Unbeschadet der geltenden rechtlichen Bestimmungen zum Datenschutz arbeiten die zuständigen behörden und zentralen Anlaufstellen*** bei der Bearbeitung von Sicherheitsvorfällen, die zu Verletzungen des Schutzes personenbezogener Daten führen, eng mit den Datenschutzbehörden zusammen. ***Die zentralen Anlaufstellen und die Datenschutzbehörden entwickeln in Zusammenarbeit mit der ENISA Mechanismen für den Informationsaustausch und ein einheitliches Muster für Meldungen nach Artikel 14 Absatz 2 dieser Richtlinie und der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.***

Die Kommission kann in Zusammenarbeit mit der ENISA durch die Annahme von Durchführungsrechtsakten und unter strenger Berücksichtigung sämtlicher

	Mechanismen zum Informationsaustausch und des von den zentralen Anlaufstellen und Datenschutzbehörden entwickelten einheitlichen Musters Verfahren für Mechanismen zum Informationsaustausch und das Format des einheitlichen Musters festlegen.
6. Die Mitgliedstaaten gewährleisten, dass alle Verpflichtungen, die ***öffentlichen Verwaltungen oder*** Marktteilnehmern nach diesem Kapitel auferlegt werden, einer gerichtlichen Nachprüfung unterzogen werden können.	6. Die Mitgliedstaaten gewährleisten, dass alle Verpflichtungen, die Marktteilnehmern nach diesem Kapitel auferlegt werden, einer gerichtlichen Nachprüfung unterzogen werden können.

Änderungsantrag 87

Vorschlag für eine Richtlinie
Artikel 16

Vorschlag der Kommission	*Geänderter Text*
1. Um eine einheitliche Umsetzung des Artikels 14 Absatz 1 zu gewährleisten, fördern die Mitgliedstaaten die Anwendung einschlägiger Normen und/oder Spezifikationen für die Netz- und Informationssicherheit.	1. Um eine einheitliche Umsetzung des Artikels 14 Absatz 1 zu gewährleisten, fördern die Mitgliedstaaten ***unter Einhaltung der Rechtsvorschriften der EU*** die Anwendung einschlägiger ***offener europäischer und internationaler interoperabler*** Normen und/oder Spezifikationen für die Netz- und Informationssicherheit***, ohne jedoch die Anwendung einer bestimmten Technologie vorzuschreiben***.
2. Die Kommission ***stellt mittels Durchführungsrechtsakten eine*** Liste ***der in Absatz 1*** genannten Normen ***auf***. Diese Liste wird im Amtsblatt der Europäischen Union veröffentlicht.	2. Die Kommission ***erteilt der zuständigen europäischen Standardisierungsstelle nach Rücksprache mit den maßgeblichen Akteuren das Mandat zur Erstellung einer*** Liste ***mit den in Absatz 1*** genannten Normen ***und/oder Spezifikationen***. Diese Liste wird im Amtsblatt der Europäischen Union veröffentlicht.

Änderungsantrag 88

Vorschlag für eine Richtlinie
Artikel 17 – Absatz 1

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

Begründung

Es sollte klargestellt werden, dass Sanktionen für Verstöße nur angewendet werden können, wenn Marktteilnehmer nicht alle erforderlichen Maßnahmen ergriffen haben, die nach vernünftigem Ermessen von ihnen erwartet werden konnten. Andernfalls könnten die Marktteilnehmer davon abgehalten werden, Sicherheitsvorfälle zu melden.

Änderungsantrag 89

Vorschlag für eine Richtlinie
Artikel 17 – Absatz 1 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	1a. Die Mitgliedstaaten stellen sicher, dass die in Absatz 1 dieses Artikels genannten Sanktionen nur dann Anwendung finden, wenn der Marktteilnehmer vorsätzlich oder grob fahrlässig gegen seine Verpflichtungen nach Kapitel IV verstoßen hat.

Änderungsantrag 90

Vorschlag für eine Richtlinie
Artikel 18

Vorschlag der Kommission	*Geänderter Text*
Artikel 18	***entfällt***
Ausübung der Befugnisübertragung	
1. Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission nach Maßgabe dieses Artikels übertragen.	
2. Die in Artikel 9 Absatz 2, Artikel 10 Absatz 5 und Artikel 14 Absatz 5 genannte Befugnis zum Erlass delegierter Rechtsakte wird der Kommission übertragen. Die Kommission legt spätestens neun Monate vor Ablauf des Fünfjahreszeitraums einen Bericht über die übertragenen Befugnisse vor. Die Befugnisübertragung verlängert sich stillschweigend um Zeiträume gleicher Länge, es sei denn, das Europäische Parlament oder der Rat widerspricht einer solchen Verlängerung spätestens drei Monate vor Ablauf des jeweiligen Zeitraums.	
3. Die in Artikel 9 Absatz 2, Artikel 10 Absatz 5 und Artikel 14 Absatz 5 genannte Befugnisübertragung kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im Amtsblatt der Europäischen Union oder zu einem darin angegebenen späteren Zeitpunkt wirksam. Er berührt nicht die Gültigkeit der bereits in Kraft getretenen delegierten Rechtsakte.	
4. Sobald die Kommission einen delegierten Rechtsakt erlassen hat, übermittelt sie ihn gleichzeitig dem	

Europäischen Parlament und dem Rat.

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

Änderungsantrag 91

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 1

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

Begründung

Um den sich ändernden Bedrohungen und Bedingungen im Bereich der Netzsicherheit Rechnung zu tragen, muss Anhang II regelmäßig überprüft und bearbeitet werden.

Änderungsantrag 92

Vorschlag für eine Richtlinie
Anhang 1 – Überschrift 1

Vorschlag der Kommission	*Geänderter Text*
IT-Notfallteam (Computer Emergency Response Team, CERT) – Anforderungen und Aufgaben	IT-Notfallteams (Computer Emergency Response Teams, CERTs) – Anforderungen und Aufgaben

Änderungsantrag 93

Vorschlag für eine Richtlinie
Anhang 1 – Absatz 1 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
Die Anforderungen an ***das CERT und seine*** Aufgaben werden angemessen und genau festgelegt und durch nationale Strategien und/oder Vorschriften gestützt. Sie müssen Folgendes umfassen:	Die Anforderungen an ***die CERTs und ihre*** Aufgaben werden angemessen und genau festgelegt und durch nationale Strategien und/oder Vorschriften gestützt. Sie müssen Folgendes umfassen: ***(Diese Änderung gilt im gesamten Text von Anhang I.)***

Änderungsantrag 94

Vorschlag für eine Richtlinie
Anhang 1 – Absatz 1 – Nummer 1 – Buchstabe a

Vorschlag der Kommission	*Geänderter Text*
a) ***Das CERT gewährleistet*** die hohe Verfügbarkeit ***seiner*** Kommunikationsdienste durch Vermeidung kritischer Ausfallverursacher und durch Bereitstellung verschiedener Kanäle, damit ***das CERT*** ständig erreichbar ***bleibt*** und selbst Kontakt aufnehmen ***kann***. Die Kommunikationskanäle müssen genau spezifiziert sein und den CERT-Nutzern (Constituency) und Kooperationspartnern	a) Die ***CERTs gewährleisten die*** hohe Verfügbarkeit ***ihrer*** Kommunikationsdienste durch Vermeidung kritischer Ausfallverursacher und durch Bereitstellung verschiedener Kanäle, damit ***die CERTs*** ständig erreichbar ***bleiben*** und selbst Kontakt aufnehmen ***können***. Die Kommunikationskanäle müssen genau spezifiziert sein und den CERT-Nutzern (Constituency) und Kooperationspartnern

bekannt gegeben werden.	bekannt gegeben werden.

Änderungsantrag 95

Vorschlag für eine Richtlinie
Anhang 1 – Absatz 1 – Nummer 1 – Buchstabe c

Vorschlag der Kommission	*Geänderter Text*
c) Die ***CERT-Dienststellen*** und die unterstützenden Informationssysteme werden an sicheren Standorten eingerichtet.	c) Die ***CERTs-Dienststellen*** und die unterstützenden Informationssysteme werden an sicheren Standorten ***und mit gesicherten Netzen und Informationssystemen*** eingerichtet.

Änderungsantrag 96

Vorschlag für eine Richtlinie
Anhang 1 – Absatz 1 – Nummer 2 – Buchstabe a – Spiegelstrich 1

Vorschlag der Kommission	*Geänderter Text*
– Überwachung von Sicherheitsvorfällen auf nationaler Ebene;	– ***Erkennung und*** Überwachung von Sicherheitsvorfällen auf nationaler Ebene;

Änderungsantrag 97

Vorschlag für eine Richtlinie
Anhang 1 – Absatz 1 – Nummer 2 – Buchstabe a – Spiegelstrich 5 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	– aktive Beteiligung an internationalen CERT-Kooperationsnetzen sowie CERT-Kooperationsnetzen der Union;

Änderungsantrag 98

Vorschlag für eine Richtlinie
Anhang II

Vorschlag der Kommission	*Geänderter Text*
Liste der Marktteilnehmer	Liste der Marktteilnehmer
1. Energie	1. Energie
	a) Strom
	- Zulieferer
	- Fernleitungsnetzbetreiber und Endkundenlieferanten
	- Übertragungsnetzbetreiber (Strom)
	- Marktteilnehmer (Strom)
	b) Erdöl
	- Erdöl-Fernleitungen und Erdöllager
	- Betreiber von Anlagen zur Produktion, Raffination und Behandlung von Erdöl, Erdöllagern und -fernleitungen
	c) Erdgas
	- Zulieferer
	- Fernleitungsnetzbetreiber und Endkundenlieferanten
	- Erdgas-Fernleitungsnetzbetreiber, Erdgasspeicher- und LNG-Anlagenbetreiber
	- Betreiber von Anlagen zur Produktion, Raffination und Behandlung von Erdgas, Erdgasspeichern und -fernleitungen
	- Marktteilnehmer (Erdgas)
2. Verkehr	2. Verkehr
	a) Straßenverkehr
	(i) Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen
	(ii) unterstützende Logistikdienste:
	- Lagerhaltung und Lagerung

- Frachtumschlagsleistungen und

- andere unterstützende Verkehrsleistungen

b) Eisenbahnverkehr

(i) Eisenbahnen (Infrastrukturbetreiber, integrierte Unternehmen und Eisenbahnunternehmen)

(ii) Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen

(iii) - unterstützende Logistikdienste:

- Lagerhaltung und Lagerung

- Frachtumschlagsleistungen und

- andere unterstützende Verkehrsleistungen

c) Luftverkehr

(i) Luftfahrtunternehmen (Luftfrachtverkehr und Personenbeförderung)

(ii) Flughäfen

(iii) Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen

(iv) unterstützende Logistikdienste:

- Lagerhaltung,

- Frachtumschlagsleistungen und

- andere unterstützende Verkehrsleistungen

(d) Seeverkehr

(i) Beförderungsunternehmen des Seeverkehrs (Personen- und Güterbeförderung in der Binnen-, See- und Küstenschifffahrt)

(ii) Häfen

(iii) Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen

(iv) unterstützende Logistikdienste:

- Lagerhaltung und Lagerung

	- Frachtumschlagsleistungen und
	- andere unterstützende Verkehrsleistungen
	2a. Wasserwirtschaft
3. Bankwesen: Kreditinstitute nach Artikel 4 Absatz 1 der Richtlinie 2006/48/EG.	3. Bankwesen: Kreditinstitute nach Artikel 4 Absatz 1 der Richtlinie 2006/48/EG.
4. Finanzmarktinfrastrukturen: ***Börsen*** und Clearingstellen mit zentraler Gegenpartei	4. Finanzmarktinfrastrukturen: ***geregelte Märkte, multilaterales Handelssysteme, organisierte Handelssysteme, Internet-Zahlungs-Gateways*** und Clearingstellen mit zentraler Gegenpartei
5. Gesundheitswesen: Einrichtungen der medizinischen Versorgung (einschließlich Krankenhäusern und Privatkliniken) sowie andere Einrichtungen der Gesundheitsfürsorge	5. Gesundheitswesen: Einrichtungen der medizinischen Versorgung (einschließlich Krankenhäusern und Privatkliniken) sowie andere Einrichtungen der Gesundheitsfürsorge
	6. IKT: Cloud-Computing-Dienste, die von einem Betreiber genutzt werden, um die in den Nummern 1 bis 5 genannten Dienste anzubieten
	Diese Liste wird alle zwei Jahre aktualisiert.

VERFAHREN

Titel	Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union
Bezugsdokumente - Verfahrensnummer	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)
Federführender Ausschuss Datum der Bekanntgabe im Plenum	IMCO 15.4.2013
Stellungnahme von Datum der Bekanntgabe im Plenum	ITRE 15.4.2013
Assoziierte(r) Ausschuss/Ausschüsse - datum der bekanntgabe im plenum	12.9.2013
Verfasser(in) der Stellungnahme Datum der Benennung	Pilar del Castillo Vera 23.5.2013
Prüfung im Ausschuss	14.10.2013 4.11.2013
Datum der Annahme	16.12.2013
Ergebnis der Schlussabstimmung	+: 36 –: 5 0: 0
Zum Zeitpunkt der Schlussabstimmung anwesende Mitglieder	Amelia Andersdotter, Josefa Andrés Barea, Bendt Bendtsen, Fabrizio Bertot, Reinhard Bütikofer, Maria Da Graça Carvalho, Giles Chichester, Pilar del Castillo Vera, Christian Ehler, Vicky Ford, Adam Gierek, Norbert Glante, Robert Goebbels, Fiona Hall, Romana Jordan, Philippe Lamberts, Marisa Matias, Judith A. Merkies, Angelika Niebler, Jaroslav Paška, Vittorio Prodi, Miloslav Ransdorf, Herbert Reul, Teresa Riera Madurell, Paul Rübig, Amalia Sartori, Salvador Sedó i Alabart, Evžen Tošenovský, Claude Turmes, Marita Ulvskog, Vladimir Urutchev
Zum Zeitpunkt der Schlussabstimmung anwesende Stellvertreter(innen)	Daniel Caspary, António Fernando Correia de Campos, Françoise Grossetête, Roger Helmer, Jolanta Emilia Hibner, Seán Kelly, Eija-Riitta Korhola, Holger Krahmer, Zofija Mazej Kukovič, Silvia-Adriana Ţicău, Lambert van Nistelrooij
Zum Zeitpunkt der Schlussabstimmung anwesende Stellv. (Art. 187 Abs. 2)	María Auxiliadora Correa Zamora