RAT DER EUROPÄISCHEN UNION

Brüssel, den 4. April 2014 (OR. en)

Interinstitutionelles Dossier: 2013/0027 (COD)

7451/14

CODEC 712
TELECOM 77
DATAPROTECT 42
CYBER 15
MI 253
PE 168

INFORMATORISCHER VERMERK

des	Generalsekretariats
für den	Ausschuss der Ständigen Vertreter/Rat
Betr.:	Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union – Ergebnis der ersten Lesung des Europäischen Parlaments (Straßburg, 10.-13. März 2014)

I. EINLEITUNG

Der Berichterstatter, Herr Andreas SCHWAB (PPE – DE), hat im Namen des Ausschusses für Binnenmarkt und Verbraucherschutz einen Bericht mit 138 Abänderungen (Abänderungen 1-138) an dem Richtlinienvorschlag vorgelegt. Außerdem brachte die Fraktion Verts/EFA drei weitere Änderungsanträge (Änderungsanträge 140-142) ein.

II. AUSSPRACHE

Der Berichterstatter eröffnete die Aussprache am 12. März 2014 und

- wies darauf hin, dass der Ausschuss für Binnenmarkt und Verbraucherschutz und die anderen beteiligten Ausschüsse sehr intensiv gearbeitet hätten, um die erste Lesung dieses Dossiers vor den Wahlen zum Europäischen Parlament abzuschließen; Ziel sei es, ein hohes Maß an Netz- und Informationssicherheit sowie die sichere Speicherung und den Schutz von Kundendaten zu gewährleisten;
- stellte fest, dass der Bericht über den Richtlinienvorschlag drei Ziele verfolge, und zwar erstens: Konzentration auf die Gewährleistung der IT-Sicherheit kritischer Infrastrukturen; zweitens: mehr Transparenz für Bürgerinnen und Bürger in Bezug auf Cyberangriffe und auf die Frage, wie personenbezogene Daten von Unternehmen, die solche Daten speichern, besser geschützt werden können; drittens: Einführung von Sicherheitsaudits durch externe Experten als notwendiger Kontrollmechanismus;
- verteidigte die Einschränkung des Geltungsbereichs und die Ausklammerung der öffentlichen Verwaltung aus der vorgeschlagenen Richtlinie. Die Mitgliedstaaten und ihre öffentlichen Verwaltungen hätten ihre eigenen Resilienzprogramme und es sei daher nicht notwendig, sie in den Geltungsbereich einzubeziehen. Sollte sich diese Annahme als falsch herausstellen, so sei er bereit, eine Einbeziehung zu akzeptieren;
- stellte fest, dass das Kooperationsnetzwerk der Mitgliedstaaten für Cybersicherheit gut funktioniere und dass sich die Europäische Union auf dem Weg zu einem digitalen Binnenmarkt befinde.

Die Vizepräsidentin der Europäischen Kommission Neelie KROES führte Folgendes aus:

- die vorgeschlagene Richtlinie beruhe auf drei zentralen Säulen: zum einen müssten die Mitgliedstaaten dafür gerüstet sein, die Netz- und Informationssicherheit technisch und organisatorisch umzusetzen; die Mitgliedstaaten müssten die in der Richtlinie festgelegten spezifischen Funktionen und Aufgaben wahrnehmen, aber die vorgeschlagenen Abänderungen böten mehr Flexibilität, um sicherzustellen, dass die Mitgliedstaaten vorbereitet seien. Zum anderen werde die Richtlinie für mehr Zusammenarbeit zwischen den Mitgliedstaaten sorgen; sie müssten Informationen über Cyberangriffe austauschen, sich gegenseitig vorwarnen und erforderlichenfalls Unterstützung anbieten. Drittens führe die Richtlinie zu einer besseren Abwehrbereitschaft und mehr Transparenz in wichtigen Bereichen, sowohl im öffentlichen als auch im privaten Sektor;
- es sei bedauerlich, dass öffentliche Verwaltungen und Internetunternehmen aus dem Anwendungsbereich ausgeklammert seien. Der öffentliche Sektor sollte mit gutem Beispiel vorangehen und Cyber-Gefahren minimieren;

- die Kommission müsse flexibel auf die rasche Veränderung der digitalen Welt reagieren können; daher müsse eine geeignete Befugnisübertragung vorgesehen werden. Außerdem sollte die Pflicht zur Meldung vermuteter schwerer krimineller Vorfälle an die Strafverfolgungsbehörden in den Geltungsbereich der Richtlinie aufgenommen werden.

Herr Carl SCHLYTER (Verts/EFA – SE) wies im Namen des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres darauf hin, dass es wichtig sei, Daten, die an Drittländer übermittelt werden, besonders zu schützen.

Frau Ana GOMES (S&D – PT) ergriff im Namen des Ausschusses für auswärtige Fragen das Wort und

- erklärte, dass der Unterausschuss für Sicherheit und Verteidigung auf Lücken in der vorgeschlagenen Richtlinie hingewiesen habe, durch die die Sicherheit der Europäischen Union bedroht sein könnte;
- hob hervor, dass in der Richtlinie ein Koordinierungsmechanismus unter Berücksichtigung der außen- und sicherheitspolitischen Interessen der Union vorgesehen werden müsse. Eine Koordinierung auf Ebene des Binnenmarktes reiche nicht aus; der externe und der internationale Datenaustausch müssten ebenfalls geschützt werden, insbesondere wenn Dritte beteiligt seien.

Frau Pilar DEL CASTILLO VERA (PPE – ES), die im Namen des Ausschusses für Industrie, Forschung und Energie sprach,

- erklärte, dass es unbedingt erforderlich sei, die Konzepte der Mitgliedstaaten in diesem Bereich aufeinander abzustimmen;
- hob hervor, dass die Unterschiede der in den Mitgliedstaaten vorhandenen Infrastrukturen Flexibilität erforderten. Für eine gute Koordinierung sei es erforderlich, dass es in jedem Mitgliedstaat eine zentrale Ansprechstelle gebe.

Herr Vincent Miguel GARCES RAMON (S&D – ES) ergriff im Namen seiner Fraktion das Wort und

- hob hervor, wie wichtig die vorgeschlagene Richtlinie für ein hohes Maß an Netz- und Informationssicherheit sei. Ziel der Richtlinie sollte es sein, die Grundrechte der Information und der Kommunikation zu wahren, die Netzneutralität sicherzustellen und Ungleichheiten zwischen Mitgliedstaaten zu vermeiden;
- wies auf die Bedeutung für die Wirtschaft, insbesondere die KMU, und die Gesellschaft insgesamt hin. Mitgliedstaaten müssten nationale Cybersicherheitspläne und nationale Notfallpläne erarbeiten, soweit sie noch nicht darüber verfügten;

- stellte fest, dass der Datenschutz gewährleistet sein müsse und dass er Bestandteil der Verhandlungen über die transatlantische Handels- und Investitionspartnerschaft (TTIP) sein müsse.

Frau Norica NICOLAI (ALDE – RO) äußerte sich im Namen ihrer Fraktion und

- betonte, dass die vorgeschlagene Richtlinie notwendig sei, um Risiken für Nutzer zu bekämpfen. Rechtsvorschriften und die Einrichtung einer Behörde seien jedoch nicht die einzige Lösung, da sich die Dinge in diesem Bereich sehr rasch entwickelten;
- sprach sich für klare Regeln für die Zusammenarbeit zwischen den Mitgliedstaaten und auch für die Zusammenarbeit mit Drittländern aus;
- stellte fest, dass der Kenntnisstand der Nutzer berücksichtigt werden müsse und dass allen Internetnutzern Schulungen angeboten werden sollten, damit sie unbeabsichtigte Fehler vermeiden könnten, durch die Nutzerdaten gefährdet würden.

Herr Christian ENGSTRÖM (Verts/ALE – SE) äußerte sich im Namen seiner Fraktion wie folgt:

- Er würdigte Herrn Schwabs hervorragenden Bericht, da er den ursprünglichen Kommissionsvorschlag in die richtige Richtung ändere und primär auf kritische Infrastrukturen abstelle. Der Kommissionsvorschlag sei zu detailliert gewesen und die Strukturen seien für diesen Bereich, in dem sich die Dinge sehr schnell änderten, zu starr gewesen. Das Europäische Parlament habe für die notwendige Flexibilität gesorgt.
- Er betonte, dass die Wahl der Rechtsgrundlage für die Harmonisierung im Binnenmarkt (Artikel 114 AEUV) eine hervorragende Entscheidung sei; dies sei der wichtigste Punkt der vorgeschlagenen Richtlinie.

Herr Adam BIELAN (ECR – PL) äußerte sich im Namen seiner Fraktion und

- betonte, dass die Privatsphäre im Cyberspace geschützt werden müsse, insbesondere im Hinblick auf junge Nutzer, die den größten Gefahren ausgesetzt seien;
- stellte fest, dass bestimmte Online-Dienste wie Online-Banking und gesundheitsbezogene Dienste besonders behandelt werden müssten; diese Dienste müssten spezielle Regeln für die Internetsicherheit einhalten;
- sprach sich im Sinne eines Frühwarn- und Risikobewertungssystems für einen wirksamen Informationsaustausch und eine wirksame Zusammenarbeit zwischen den Mitgliedstaaten sowie zwischen den spezialisierten Agenturen aus. Internetsicherheit und Online-Dienste würden dadurch besser.

III. ABSTIMMUNG

Bei der Abstimmung am 13. März 2014 nahm das Parlament 138 Abänderungen (Abänderungen 1-138) an. Weitere Abänderungen wurden nicht angenommen.

Der auf diese Weise geänderte Kommissionsvorschlag und die legislative Entschließung stellen den Standpunkt des Europäischen Parlaments in erster Lesung dar. Der Wortlaut der angenommenen Abänderungen und der legislativen Entschließung des Europäischen Parlaments ist in der Anlage wiedergegeben.

ANLAGE
(13.3.2014)

P7_TA-PROV(2014)0244

Hohe gemeinsame Netz- und Informationssicherheit in der Union ***I

Legislative Entschließung des Europäischen Parlaments vom 13. März 2014 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))

(Ordentliches Gesetzgebungsverfahren: erste Lesung)

Das Europäische Parlament,

– in Kenntnis des Vorschlags der Kommission an das Europäische Parlament und den Rat (COM(2013)0048),

– gestützt auf Artikel 294 Absatz 2 und Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union, auf deren Grundlage ihm der Vorschlag der Kommission unterbreitet wurde (C7-0035/2013),

– gestützt auf Artikel 294 Absatz 3 des Vertrags über die Arbeitsweise der Europäischen Union,

– in Kenntnis der vom schwedischen Reichstag im Rahmen des Protokolls Nr. 2 über die Anwendung der Grundsätze der Subsidiarität und der Verhältnismäßigkeit vorgelegten begründeten Stellungnahme, in der geltend gemacht wird, dass der Entwurf eines Gesetzgebungsakts nicht mit dem Subsidiaritätsprinzip vereinbar ist,

– gestützt auf Artikel 55 seiner Geschäftsordnung,

– in Kenntnis der Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses vom 22. Mai 2013[1],

– unter Hinweis auf seine Entschließung vom 12. September 2013 mit dem Titel „Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum“[2],

– in Kenntnis des Berichts des Ausschusses für Binnenmarkt und Verbraucherschutz sowie der Stellungnahmen des Ausschusses für Industrie, Forschung und Energie, des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres und des Ausschusses für auswärtige Angelegenheiten (A7-0103/2014),

1. legt den folgenden Standpunkt in erster Lesung fest;

2. fordert die Kommission auf, es erneut zu befassen, falls sie beabsichtigt, ihren Vorschlag entscheidend zu ändern oder durch einen anderen Text zu ersetzen;

---

1 ABl. C 271 vom 19.9.2013, S. 133.

2 Angenommene Texte, P7_TA(2013)0376.

3. beauftragt seinen Präsidenten, den Standpunkt des Parlaments dem Rat und der Kommission sowie den nationalen Parlamenten zu übermitteln.

Abänderung 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 Bedeutung, dass sie verlässlich und sicher sind.	(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 Union,*** für die Wirtschaft und das Gemeinwohl und insbesondere für das Funktionieren des Binnenmarkts ist es von entscheidender Bedeutung, dass sie verlässlich und sicher sind.

Abänderung 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 Störung oder den Ausfall des Betriebs der Systeme gerichtet sind.*** Solche Sicherheitsvorfälle können die Ausübung von Wirtschaftstätigkeiten beeinträchtigen, finanzielle Verluste verursachen, das Vertrauen der Nutzer ***und Investoren*** untergraben und der Wirtschaft der Union großen Schaden zufügen ***und letztendlich das Wohlergehen der Bürger der Union sowie die Fähigkeit der Mitgliedstaaten, sich selbst zu schützen und für den Schutz der kritischen Infrastruktur zu sorgen, gefährden***.

Abänderung 3

Vorschlag für eine Richtlinie
Erwägung 3 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(3a) Da Systemausfällen nach wie vor in der Regel keine Absicht zugrunde liegt und sie beispielsweise auf natürliche Ursachen oder menschliches Versagen zurückzuführen sind, sollte die Infrastruktur sowohl vorsätzlichen als auch unbeabsichtigten Störungen standhalten, und die Betreiber kritischer Infrastrukturen sollten robuste Systeme konstruieren.

Abänderung 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 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	(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 Mechanismus wirksam sein kann und alle Beteiligten einbezogen werden, muss jeder Mitgliedstaat über Mindestkapazitäten und eine Strategie verfügen, ***durch*** die in seinem Hoheitsgebiet für eine hohe NIS ***gesorgt ist***. ***Damit das Risikomanagement stärker in die Denk- und Verhaltensweisen integriert wird*** und die gravierendsten Sicherheitsvorfälle ***tatsächlich*** gemeldet werden, sollten

Betreiber kritischer Informationsinfrastrukturen gelten.	Mindestsicherheitsanforderungen ***zumindest*** auch für ***bestimmte Marktteilnehmer im Bereich*** Informationsinfrastrukturen gelten. ***Börsennotierten Unternehmen sollte nahegelegt werden, Sicherheitsvorfälle freiwillig in ihren Finanzberichten zu veröffentlichen. Der Rechtsrahmen sollte darauf beruhen, dass die Privatsphäre und Integrität der Bürger geschützt werden müssen. Das Warn- und Informationsnetz für kritische Infrastrukturen (WINKI) sollte auf Marktteilnehmer, die unter diese Richtlinie fallen, ausgeweitet werden.***

Abänderung 5

Vorschlag für eine Richtlinie
Erwägung 4 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(4a) Während die öffentlichen Verwaltungen aufgrund ihres öffentlichen Auftrags gebührende Sorgfalt beim Betrieb und Schutz ihrer Netze und Informationssysteme walten lassen sollten, sollte der Schwerpunkt dieser Richtlinie 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. Diese Richtlinie sollte nicht für Softwareentwickler und Hardwarehersteller gelten.

Abänderung 6

Vorschlag für eine Richtlinie
Erwägung 4 b (neu)

Vorschlag der Kommission	*Geänderter Text*
	(4b) Die Zusammenarbeit und Abstimmung der einschlägigen Stellen der Union mit der Hohen Vertreterin und Vizepräsidentin mit Zuständigkeit für die Gemeinsame Außen- und Sicherheitspolitik und die Gemeinsame Sicherheits- und Verteidigungspolitik sowie mit dem EU-Koordinator für die Terrorismusbekämpfung sollten in den Fällen sichergestellt werden, in denen Sicherheitsvorfälle mit erheblichen Auswirkungen als äußere Gefährdung oder Terrorgefahr eingestuft werden.

Abänderung 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 umfassender, wirksamer Mechanismus für die Zusammenarbeit auf Unionsebene geschaffen werden.	(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 Marktteilnehmer kann wiederum kein umfassender, wirksamer Mechanismus für die Zusammenarbeit auf Unionsebene geschaffen werden. ***Universitäten und Forschungszentren spielen eine zentrale Rolle, wenn es darum geht, Forschung, Entwicklung und Innovationen in diesen Bereichen voranzutreiben, und sollten mit***

angemessenen Finanzmitteln ausgestattet werden.

Abänderung 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 ***enthält***. ***In Übereinstimmung mit den einschlägigen Empfehlungen der Koordinierungsgruppe für die Cybersicherheit (CSGC) sollten gemeinsame Mindestnormen angewendet werden.***

Abänderung 9

Vorschlag für eine Richtlinie
Erwägung 8

Vorschlag der Kommission	*Geänderter Text*
(8) Die Möglichkeit der Mitgliedstaaten, die für die Wahrung ihrer wesentlichen Sicherheitsinteressen und den Schutz der öffentlichen Ordnung und der öffentlichen Sicherheit erforderlichen Maßnahmen zu ergreifen und die Ermittlung, Feststellung und Verfolgung von Straftaten zuzulassen, bleibt von den Bestimmungen dieser Richtlinie unberührt. Nach Artikel 346	(8) Die Möglichkeit der Mitgliedstaaten, die für die Wahrung ihrer wesentlichen Sicherheitsinteressen und den Schutz der öffentlichen Ordnung und der öffentlichen Sicherheit erforderlichen Maßnahmen zu ergreifen und die Ermittlung, Feststellung und Verfolgung von Straftaten zuzulassen, bleibt von den Bestimmungen dieser Richtlinie unberührt. Nach Artikel 346

AEUV ist kein Mitgliedstaat verpflichtet, Auskünfte zu erteilen, deren Preisgabe seines Erachtens seinen wesentlichen Sicherheitsinteressen widerspricht.	AEUV ist kein Mitgliedstaat verpflichtet, Auskünfte zu erteilen, deren Preisgabe seines Erachtens seinen wesentlichen Sicherheitsinteressen widerspricht. ***Kein Mitgliedstaat ist verpflichtet, Informationen offenzulegen, die nach dem Beschluss des Rates vom 31. März 2011 über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen (2011/292/EU) als EU-Verschlusssachen eingestuft sind bzw. unter Geheimhaltungsvereinbarungen oder informelle Geheimhaltungsvereinbarungen wie das sogenannte Traffic Light Protocol fallen.***

Abänderung 10

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, ***sodass*** ein Kapazitätsniveau erreicht werden kann, das bei Sicherheitsvorfällen eine wirksame und effiziente Zusammenarbeit auf nationaler und auf Unionsebene ermöglicht***, wobei die Privatsphäre und personenbezogene Daten geachtet und geschützt werden***. ***Die Mitgliedstaaten sollten daher zur Einhaltung gemeinsamer Normen im Hinblick auf das Datenformat und die Austauschbarkeit der gemeinsam zu nutzenden und zu bewertenden Daten***

	verpflichtet werden. Die Mitgliedstaaten sollten 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 von Mindestanforderungen an NIS-Strategien ersuchen können.

Abänderung 11

Vorschlag für eine Richtlinie
Erwägung 10 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(10a) Die Mitgliedstaaten sollten wegen der Unterschiede zwischen ihren Verwaltungsstrukturen und mit dem Ziel, dass bereits geltende sektorbezogene Vereinbarungen beibehalten werden bzw. bereits eingerichtete Aufsichts- und Regulierungsstellen der Union fortbestehen können und dass keine Doppelungen entstehen, mehrere nationale zuständige Behörden benennen können, die im Rahmen dieser Richtlinie Aufgaben im Zusammenhang mit der Netz- und Informationssicherheit von Marktteilnehmern wahrnehmen. Im Interesse der reibungslosen länderübergreifenden Zusammenarbeit und Kommunikation ist es allerdings notwendig, dass jeder Mitgliedstaat unbeschadet der sektorbezogenen Vereinbarungen nur eine nationale zentrale Anlaufstelle mit Zuständigkeit für die länderübergreifende Zusammenarbeit auf Unionsebene benennt. Ein Mitgliedstaat sollte auch – sofern es 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. Die zuständigen Behörden und die zentralen Anlaufstellen sollten zivile Stellen sein,

	die der vollständigen demokratischen Kontrolle unterliegen, und sie sollten weder Aufgaben in den Bereichen Geheimdienst, Strafverfolgung oder Verteidigung wahrnehmen noch organisatorisch in irgendeiner Form mit in diesen Bereichen tätigen Stellen verbunden sein.

Abänderung 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 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***.	(11) Alle Mitgliedstaaten ***und Marktteilnehmer*** sollten über angemessene technische und organisatorische Kapazitäten verfügen, um die Prävention, Erkennung, Reaktion und Folgenminderung bei NIS-Vorfällen und -Risiken ***jederzeit durchführen*** zu können. ***Die Sicherheitssysteme in der öffentlichen Verwaltung sollten sicher sein und der demokratischen Kontrolle und Prüfung unterliegen. Die allgemein erforderlichen Geräte und Kapazitäten sollten den gemeinsam vereinbarten technischen Normen sowie Standardverfahren entsprechen.*** Dafür sollten im Einklang mit den grundlegenden Anforderungen in allen Mitgliedstaaten gut funktionierende IT-Notfallteams (Computer Emergency Response Teams***, CERTs***) eingerichtet werden, damit wirksame und geeignete Kapazitäten geschaffen werden, die in der Lage sind, Sicherheitsvorfälle und -risiken zu bewältigen und ***für*** eine effiziente Zusammenarbeit auf Unionsebene zu ***sorgen***. ***Diese CERTs sollten in die Lage versetzt werden, auf der Grundlage gemeinsamer technischer Normen und Standardverfahren zu interagieren. Da die bestehenden CERTs, die für die einzelnen subjektiven Bedürfnisse und Akteure zuständig sind, unterschiedliche***

	Merkmale aufweisen, sollten die Mitgliedstaaten sicherstellen, dass jedem der in dieser Richtlinie genannten Sektoren von mindestens einem CERT Dienstleistungen angeboten werden. In Bezug auf die länderübergreifende CERT-Zusammenarbeit sollten die Mitgliedstaaten sicherstellen, dass die CERTs über hinreichende Mittel verfügen, um an den auf internationaler Ebene und in der Union vorhandenen Kooperationsnetzen mitzuwirken.

Abänderung 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 ***Verfahren***, 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. ***Über diesen sicheren*** und ***wirksamen*** Kooperationsmechanismus***, an dem, falls angezeigt, auch die Marktteilnehmer mitwirken, sollten Informationen ausgetauscht sowie Sicherheitsvorfälle*** in strukturierter, abgestimmter Weise auf Unionsebene ***erkannt und bewältigt werden***.

Abänderung 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 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.	(13) Die 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 ziehen. Damit 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.

Abänderung 15

Vorschlag für eine Richtlinie
Erwägung 13 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(13a) Bei der Umsetzung dieser Richtlinie sollten die Mitgliedstaaten bestehende Organisationsstrukturen, falls vorhanden, nutzen oder anpassen können.

Abänderung 16

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 errichtet werden, damit sensible und vertrauliche Informationen über das Kooperationsnetz übermittelt werden können. ***In der Union bestehende Strukturen sollten in vollem Umfang zu diesem Zweck genutzt werden.*** 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 ***und dabei transparente Verfahren anwenden***.

Abänderung 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 ***Fall*** 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 sollte sichergestellt werden, dass eine solche Zusammenarbeit für diese Betreiber gemäß den Rechtsvorschriften, beispielsweise über den Wettbewerb, das geistige Eigentum, den Datenschutz oder die Cyberkriminalität, nicht mit einem erhöhten Risiko von Verstößen einhergeht oder dass ihnen daraus keine neue Haftung erwächst und dass diese Zusammenarbeit für sie auch nicht mit höheren operativen oder sicherheitstechnischen Risiken verbunden ist.***

Abänderung 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 ***für*** Transparenz zu ***sorgen*** und die Bürger und Marktteilnehmer der ***Union*** angemessen zu informieren, sollten die ***zentralen Anlaufstellen*** eine gemeinsame ***unionsweite*** Website zur Veröffentlichung nichtvertraulicher Informationen über Sicherheitsvorfälle und -risiken***, Möglichkeiten der Risikobegrenzung und, falls notwendig, zur Bereitstellung von Empfehlungen zu geeigneten Wartungsmaßnahmen*** einrichten. ***Die Informationen auf dieser Website sollten geräteunabhängig zugänglich sein. Die auf dieser Website veröffentlichten personenbezogenen Daten sollten auf das Notwendige beschränkt und so anonym wie möglich sein.***

Abänderung 19

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 ***Prävention, Entdeckung, Meldung und*** Bewältigung von Sicherheitsrisiken und -vorfällen festgelegt werden. Diesem Plan sollte bei Frühwarnungen über das Kooperationsnetz angemessen Rechnung getragen werden.

Abänderung 20

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	(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.	werden.

Abänderung 21

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 koordinierten Reaktion auf nationaler Ebene ergriffenen Maßnahmen informiert werden.	(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 der koordinierten Reaktion auf nationaler Ebene ergriffenen Maßnahmen informiert werden.

Abänderung 22

Vorschlag für eine Richtlinie
Erwägung 21

Vorschlag der Kommission	*Geänderter Text*
(21) Angesichts des globalen Charakters von NIS-Problemen bedarf es einer engeren internationalen Zusammenarbeit, damit die Sicherheitsstandards und der Informationsaustausch verbessert werden können und ein gemeinsames globales Konzept für NIS-Fragen gefördert werden kann.	(21) Angesichts des globalen Charakters von NIS-Problemen bedarf es einer engeren internationalen Zusammenarbeit, damit die Sicherheitsstandards und der Informationsaustausch verbessert werden können und ein gemeinsames globales Konzept für NIS-Fragen gefördert werden kann. ***Der Rahmen für eine derartige internationale Zusammenarbeit sollte den Bestimmungen der Richtlinie 95/46/EG und der Verordnung (EG) Nr. 45/2001 unterliegen.***

Abänderung 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 Marktteilnehmern. Durch geeignete Vorschriften und freiwillige Branchenpraxis ***sollten die Integration des Risikomanagements in die Denk- und Verhaltensweisen, enge Zusammenarbeit und Vertrauen*** gefördert und ***weiterentwickelt*** werden, die u. a. die Risikobewertung und die Anwendung von Sicherheitsmaßnahmen umfassen ***sollten***, die den jeweiligen Risiken ***und vorsätzlichen wie unbeabsichtigten Sicherheitsvorfällen*** 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.

Abänderung 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 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, auf die sich	(24) ***Diese Verpflichtungen sollten auf Betreiber von Infrastrukturen ausgeweitet werden, die stark von der Informations- und Kommunikationstechnik abhängen und für die Aufrechterhaltung wichtiger wirtschaftlicher und gesellschaftlicher Bereiche (Strom- und Gasversorgung, Verkehr, Kreditinstitute, Finanzmarktinfrastrukturen, Gesundheitswesen usw.) unbedingt notwendig sind. Durch eine Störung dieser Netze und Informationssysteme***

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***.

würde der Binnenmarkt beeinträchtigt. Während die in dieser Richtlinie festgelegten Verpflichtungen ***nicht*** über Anbieter von Diensten der Informationsgesellschaft im Sinne der Richtlinie 98/34/EG des ***Europäischen*** Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft ***hinaus ausgeweitet werden sollte***, auf die sich nachgelagerte Dienste der Informationsgesellschaft oder Online-Tätigkeiten wie Plattformen des elektronischen Geschäftsverkehrs, Internet-Zahlungs-Gateways, soziale Netze, Suchmaschinen, Cloud-Computing-Dienste ***im Allgemeinen oder*** Application Stores stützen, ***könnten diese Anbieter auf freiwilliger Grundlage 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, wenn möglich, den Marktteilnehmern, die den Sicherheitsvorfall gemeldet haben, strategische, analysierte Informationen übermitteln, mit denen dazu beigetragen wird, die sicherheitsrelevante Bedrohung zu überwinden***.

Abänderung 25

Vorschlag für eine Richtlinie
Erwägung 24 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(24a) Zwar sind Hardware- und Softwareanbieter keine Marktteilnehmer, die mit denen vergleichbar sind, die unter diese Richtlinie fallen, doch begünstigen ihre Produkte die Sicherheit von Netzen und Informationssystemen. Ihnen kommt deshalb eine wichtige Aufgabe zu, wenn es darum geht, die Marktteilnehmer in die Lage zu versetzen, ihre Netz- und

	Informationsinfrastrukturen zu sichern. Da Hardware- und Softwareprodukte bereits den geltenden Produkthaftungsvorschriften unterliegen, sollten die Mitgliedstaaten Vorkehrungen dafür treffen, dass diese Vorschriften auch durchgesetzt werden.

Abänderung 26

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.

Abänderung 27

Vorschlag für eine Richtlinie
Erwägung 26

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

diese Aufgabe ausgliedern.

Abänderung 28

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 vertraulich bleiben.	(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. ***Die zuständigen Behörden und die zentralen Anlaufstellen sollten die Hersteller betroffener IKT-Produkte und die Anbieter betroffener IKT-Dienste über ihnen gemeldete Sicherheitsvorfälle mit erheblichen Auswirkungen 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 ***Sicherheitsvorfälle*** melden, entstehen kann. Bei der Erfüllung der Meldepflichten sollten die zuständigen Behörden ***und die zentralen Anlaufstellen*** besonders darauf achten, dass Informationen über die Anfälligkeit von Produkten bis zur ***Bereitstellung*** der entsprechenden Sicherheitsfixes streng vertraulich bleiben. ***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 es im Hinblick auf den damit verfolgten Zweck notwendig und verhältnismäßig ist.***

Abänderung 29

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

Abänderung 30

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	(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***, 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

Sicherheitsvorfälle aufgrund schwerer Straftaten handelt, sollte nach den EU-Vorschriften über Cyberkriminalität beurteilt werden.	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.

Abänderung 31

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 wird. ***Über Kontakte mit den zuständigen Behörden und den Datenschutzbehörden könnte die ENISA Unterstützung bieten, indem sie Mechanismen für den Informationsaustausch sowie Muster entwickelt, mit denen die Verwendung zweier verschiedener Muster für die Meldung von NIS-Vorfällen vermieden werden kann.*** Die Meldung ***anhand eines einzigen Musters wäre bei*** Sicherheitsvorfällen, bei denen der Schutz personenbezogener Daten beeinträchtigt	(31) Häufig ist bei Sicherheitsvorfällen der Schutz personenbezogener Daten nicht mehr gewährleistet. ***Die 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, Offenlegung oder Verbreitung schützen; sie sollten darüber hinaus für die Umsetzung eines Sicherheitskonzepts für die Verarbeitung personenbezogener Daten sorgen.*** Deshalb sollten die zuständigen Behörden ***die zentralen Anlaufstellen*** und die Datenschutzbehörden zusammenarbeiten und Informationen austauschen, ***falls angezeigt, auch mit den Marktteilnehmern,*** um derartigen Verletzungen des Schutzes personenbezogener Daten ***im Einklang mit den geltenden Datenschutzvorschriften*** 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 den geltenden Datenschutzvorschriften der Union gemeldet werden müssen***, so gering wie möglich gehalten wird. Die ***ENISA sollte***

wurde, ***eine Vereinfachung*** und ***würde*** damit ***den*** Verwaltungsaufwand für Unternehmen und öffentliche Verwaltungen ***verringern***.	***Unterstützung bieten, indem sie Mechanismen für den Informationsaustausch und ein einziges Muster entwickelt, mit denen bzw. dem die*** Meldung ***von*** Sicherheitsvorfällen, bei denen der Schutz personenbezogener Daten beeinträchtigt wurde, ***vereinfacht*** und damit ***der*** Verwaltungsaufwand für Unternehmen und öffentliche Verwaltungen ***verringert würde***.

Abänderung 32

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***. Zu diesem Zweck könnte ***es erforderlich sein***, harmonisierte Normen auszuarbeiten; dies sollte nach der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 zur europäischen Normung, zur Änderung der Richtlinien 89/686/EWG und 93/15/EWG des Rates sowie der Richtlinien 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG und 2009/105/EG des Europäischen Parlaments und des Rates und zur Aufhebung des Beschlusses 87/95/EWG des Rates und des Beschlusses Nr. 1673/2006/EG des Europäischen Parlaments und des Rates[29] geschehen.	(32) Die Normung von Sicherheitsanforderungen ist ein vom Markt ausgehender Vorgang ***auf freiwilliger Grundlage, 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 ***für*** ein hohes Sicherheitsniveau auf Unionsebene ***gesorgt ist***. Zu diesem Zweck ***sollte die Anwendung offener internationaler Normen für Netzinformationssicherheit oder die Konzipierung entsprechender Instrumente in Erwägung gezogen werden. Ein weiterer Schritt*** 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, wirkungsvolle und effiziente offene Sicherheitsstandards der Union zu empfehlen, bei denen so weit wie möglich keine technischen Voreinstellungen vorgenommen werden und die für kleine und mittelgroße Marktteilnehmer praktikabel sind. Internationale Standards über die Cybersicherheit sollten sehr sorgfältig geprüft werden, um sicherzustellen, dass bei ihnen keine Abstriche gemacht wurden und dass sie ein ausreichend hohes Sicherheitsniveau bieten und folglich dafür gesorgt ist, dass durch die gebotene Einhaltung der Cybersicherheitsstandards das Gesamtniveau der Cybersicherheit in der Union erhöht und nicht herabgesetzt wird.***
[29] ABl. L 316 vom 14.11.2012, S. 12.	[29] ABl. L 316 vom 14.11.2012, S. 12.

Abänderung 33

Vorschlag für eine Richtlinie
Erwägung 33

Vorschlag der Kommission	*Geänderter Text*
(33) Die Kommission sollte diese Richtlinie regelmäßig überprüfen, insbesondere um festzustellen, ob sie veränderten technischen oder Marktbedingungen anzupassen ist.	(33) Die Kommission sollte diese Richtlinie regelmäßig ***in Abstimmung mit allen betroffenen Interessenträgern*** überprüfen, insbesondere**,** um festzustellen, ob sie veränderten ***gesellschaftlichen, politischen,*** technischen oder Marktbedingungen anzupassen ist.

Abänderung 34

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.	(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 ***in Bezug auf das Paket der gemeinsamen Verbindungs- und Sicherheitsstandards für die sichere Infrastruktur*** für den Informationsaustausch ***und zur*** weiteren Spezifikation für Auslöser von Frühwarnungen zu erlassen.

Abänderung 35

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 ***nach*** der	(36) Zur Gewährleistung einheitlicher ***Bedingungen*** 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, ***den Zugang zur sicheren Infrastruktur für den Informationsaustausch,*** den NIS-Kooperationsplan ***der Union und*** die Formen und Verfahren ***für die Meldung von Sicherheitsvorfällen mit erheblichen Auswirkungen*** übertragen werden. Diese Befugnisse sollten ***im Einklang mit*** der

Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren, ausgeübt werden.	Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren, ausgeübt werden.

.

Abänderung 36

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 ***elektronische Verwaltung***, Energie, Verkehr***,*** Gesundheit ***und Verteidigung***, in Kontakt stehen.

Abänderung 37

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	(38) Informationen, die nach den Vorschriften der Union und der Mitgliedstaaten über das Geschäftsgeheimnis von einer zuständigen Behörde ***oder einer zentralen Anlaufstelle*** als vertraulich eingestuft werden, sollten mit der Kommission***, ihren einschlägigen Stellen, zentralen Anlaufstellen und/oder weiteren*** zuständigen ***nationalen*** Behörden nur dann ausgetauscht werden, wenn ***es*** sich für die Zwecke dieser Richtlinie als

Hinblick auf das verfolgte Ziel relevant und angemessen ist.	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 im Einklang mit dem Beschluss des Rates vom 31. März 2011 über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen (2011/292/EU), Geheimhaltungsvereinbarungen und informellen Geheimhaltungsvereinbarungen wie dem sogenannten Traffic Light Protocol beachtet werden***.

Abänderung 38

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	(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 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.	der Kommission 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.

Abänderung 39

Vorschlag für eine Richtlinie
Erwägung 41 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(41a) Gemäß der gemeinsamen politischen Erklärung der Mitgliedstaaten und der Kommission zu erläuternden Dokumenten vom 28. September 2011 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 innerstaatlicher Umsetzungsinstrumente erläutert wird. In Bezug auf diese Richtlinie hält der Gesetzgeber die Übermittlung derartiger Dokumente für gerechtfertigt.

Abänderung 40

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

Vorschlag der Kommission	*Geänderter Text*
b) die Schaffung eines	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;	Kooperationsmechanismus zwischen den Mitgliedstaaten zur Gewährleistung einer einheitlichen Anwendung dieser Richtlinie in der Union, damit erforderlichenfalls in koordinierter, effizienter ***und wirkungsvoller*** Weise mit Sicherheitsrisiken und -vorfällen, ***durch*** die Netze und Informationssysteme ***beeinträchtigt werden***, ***unter Mitwirkung der Betroffenen*** umgegangen bzw. darauf reagiert werden kann;

Abänderung 41

Vorschlag für eine Richtlinie
Artikel 1 – Absatz 2 – Buchstabe c

Vorschlag der Kommission	*Geänderter Text*
c) die Festlegung von Sicherheitsvorschriften für Marktteilnehmer ***und öffentliche Verwaltungen***.	c) die Festlegung von Sicherheitsvorschriften für Marktteilnehmer.

Abänderung 42

Vorschlag für eine Richtlinie
Artikel 1 – Absatz 5

Vorschlag der Kommission	*Geänderter Text*
5) Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und die Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher	5) Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und die Verordnung ***(EG) Nr. 45/2001*** des Europäischen Parlaments und des Rates

Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr bleiben von dieser Richtlinie ebenfalls unberührt.	***vom 18. Dezember 2000*** zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ***durch die Organe und Einrichtungen der Gemeinschaft*** und zum freien Datenverkehr bleiben von dieser Richtlinie ebenfalls unberührt. ***Die Nutzung personenbezogener Daten muss auf das für die Zwecke dieser Richtlinie absolut notwendige Mindestmaß beschränkt sein, und die Daten müssen so anonym wie möglich, wenn nicht gar vollständig anonym sein.***

Abänderung 43

Vorschlag für eine Richtlinie
Artikel 1 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	Artikel 1a
	Schutz und Verarbeitung personenbezogener Daten
	1) Die Verarbeitung personenbezogener Daten in den Mitgliedstaaten gemäß dieser Richtlinie erfolgt im Einklang mit den Richtlinien 95/46/EG und 2002/58/EG.
	2) Die Verarbeitung personenbezogener Daten durch die Kommission und die ENISA gemäß dieser Richtlinie erfolgt im Einklang mit der Verordnung (EG) Nr. 45/2001.
	3) Die Verarbeitung personenbezogener Daten durch das bei Europol angesiedelte Europäische Zentrum zur Bekämpfung der Cyberkriminalität gemäß dieser Richtlinie erfolgt im Einklang mit dem Beschluss 2009/371/JI.
	4) Die Verarbeitung personenbezogener Daten erfolgt auf redliche und rechtmäßige Weise und wird auf das für die Zwecke der Datenverarbeitung absolut notwendige Mindestmaß beschränkt. Die personenbezogenen Daten werden in einer Form gespeichert, die die

	Identifizierung der betroffenen Personen höchstens so lange ermöglicht, wie es für die Realisierung des Verarbeitungszwecks erforderlich ist.
	5) Die Meldung von Sicherheitsvorfällen gemäß Artikel 14 lässt die Bestimmungen über die Meldepflicht bei Verstößen gegen den Schutz personenbezogener Daten nach Artikel 4 der Richtlinie 2002/58/EG und der Verordnung (EU) Nr. 611/2013 unberührt.

Abänderung 44

Vorschlag für eine Richtlinie
Artikel 3 – Nummer 1 – Buchstabe 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

Abänderung 45

Vorschlag für eine Richtlinie
Artikel 3 – Nummer 1 – Buchstabe 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;

Abänderung 46

Vorschlag für eine Richtlinie
Artikel 3 – 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; ***der Ausdruck „Sicherheit“ bezeichnet auch technische Geräte, Lösungen und Betriebsabläufe, mit denen sichergestellt wird, dass die in dieser Richtlinie festgelegten Sicherheitsanforderungen erfüllt werden;***

Abänderung 47

Vorschlag für eine Richtlinie
Artikel 3 – Nummer 3

Vorschlag der Kommission	*Geänderter Text*
3) „Sicherheitsrisiko“ alle Umstände oder Ereignisse, die potenziell negative Auswirkungen auf die Sicherheit haben;	3) „Sicherheitsrisiko“ alle ***mit vernünftigem Aufwand feststellbaren*** Umstände oder Ereignisse, die potenziell negative Auswirkungen auf die Sicherheit haben;

Abänderung 48

Vorschlag für eine Richtlinie
Artikel 3 – Nummer 4

Vorschlag der Kommission	*Geänderter Text*
4) „Sicherheitsvorfälle“ alle ***Umstände oder*** Ereignisse, die tatsächlich negative	4) „Sicherheitsvorfälle“ alle Ereignisse, die tatsächlich negative Auswirkungen auf die

Auswirkungen auf die Sicherheit haben;	Sicherheit haben;

Abänderung 49

Vorschlag für eine Richtlinie
Artikel 3 – 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***

Abänderung 50

Vorschlag für eine Richtlinie
Artikel 3 – 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, Prävention,*** Analyse, Eindämmung und Reaktion im ***Fall*** von Sicherheitsvorfällen;

Abänderung 51

Vorschlag für eine Richtlinie
Artikel 3 – 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***

Abänderung 52

Vorschlag für eine Richtlinie
Artikel 3 – Nummer 8 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
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) Betreiber von Infrastrukturen, die für die Aufrechterhaltung zentraler wirtschaftlicher und gesellschaftlicher Tätigkeiten in den Bereichen Energie, Verkehr, Banken, ***Finanzmarktinfrastrukturen, Internet-Knoten, Lebensmittelversorgungskette*** und Gesundheit unerlässlich sind ***und deren Unterbrechung oder Zerstörung mit dem Ergebnis, dass ihre Funktionsfähigkeit nicht aufrechterhalten werden kann, in einem Mitgliedstaat erhebliche Folgen hätte***; ***soweit die betroffenen Netze und Informationssysteme mit den Kerndiensten im Zusammenhang stehen, enthält*** Anhang II eine nicht erschöpfende Liste dieser Betreiber;

Abänderung 53

Vorschlag für eine Richtlinie
Artikel 3 – 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;

Abänderung 54

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

Vorschlag der Kommission	*Geänderter Text*
	11a) „geregelter Markt“ einen Markt im Sinne von Artikel 4 Absatz 1 Nummer 14 der Richtlinie 2004/39/EG des Europäischen Parlaments und des Rates[1a];
	[1a] 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).

Abänderung 55

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

Vorschlag der Kommission	*Geänderter Text*
	11b) „multilaterales Handelssystem (MTF)“ ein multilaterales Handelssystem im Sinne von Artikel 4 Absatz 1 Nummer 15 der Richtlinie 2004/39/EG;

Abänderung 56

Vorschlag für eine Richtlinie
Artikel 3 – 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 Titel II der Richtlinie 2004/39/EG führt;

Abänderung 57

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

Vorschlag der Kommission	*Geänderter Text*
	ea) Die Mitgliedstaaten können die ENISA um Unterstützung bei der Entwicklung ihrer nationalen NIS-Strategien und ihrer nationalen NIS-Kooperationspläne auf der Grundlage gemeinsamer Mindestanforderungen an NIS-Strategien ersuchen.

Abänderung 58

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 im Hinblick auf die Ausarbeitung von Methoden*** zur ***Ermittlung, Priorisierung, Evaluierung*** und ***Behandlung von Risiken, die*** Bewertung der Auswirkungen potenzieller Sicherheitsvorfälle***, Präventions- und Kontrollmöglichkeiten sowie auf die Festlegung von Kriterien für die Auswahl***

	möglicher Gegenmaßnahmen;

Abänderung 59

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***;

Abänderung 60

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
3) Die nationale NIS-Strategie und der nationale NIS-Kooperationsplan werden der Kommission innerhalb ***eines Monats*** nach ihrer Annahme mitgeteilt.	3) Die nationale NIS-Strategie und der nationale NIS-Kooperationsplan werden der Kommission innerhalb ***von drei Monaten*** nach ihrer Annahme mitgeteilt.

Abänderung 61

Vorschlag für eine Richtlinie
Artikel 6 – Überschrift

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

Abänderung 62

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 zivile,*** für die Netz- und Informationssicherheit zuständige nationale ***Behörden*** (im Folgenden „zuständige ***Behörden***“).

Abänderung 63

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

Vorschlag der Kommission	*Geänderter Text*
	2a) Benennt ein Mitgliedstaat mehr als eine zuständige Behörde, so benennt er eine zivile 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, so ist diese zuständige Behörde auch die zentrale Anlaufstelle.

Abänderung 64

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.

Abänderung 65

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.

Abänderung 66

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.

Abänderung 67

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- und Durchsetzungsbefugnisse eingeräumt werden.	4) Die Mitgliedstaaten gewährleisten, dass die zuständigen Behörden und ***die zentralen Anlaufstellen, falls im Sinne von Artikel 2a vorhanden, von den*** Marktteilnehmern die Meldungen der Sicherheitsvorfälle nach Artikel 14 Absatz 2 erhalten und ihnen die in Artikel 15 genannten Durchführungs- und Durchsetzungsbefugnisse eingeräumt werden.

Abänderung 68

Vorschlag für eine Richtlinie
Artikel 6 – Absatz 4 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	4a) Sehen die Unionsrechtsvorschriften eine sektorbezogene Aufsichts- oder Regulierungsstelle der Union vor, beispielsweise zur Netz- und Informationssicherheit, so werden dieser Stelle Sicherheitsvorfälle im Sinne von Artikel 14 Absatz 2 von den betroffenen Marktteilnehmern des jeweiligen Sektors gemeldet und Umsetzungs- und Durchsetzungsbefugnisse nach Artikel 15 eingeräumt. Diese Stelle der Union arbeitet im Hinblick auf diese Verpflichtungen eng mit den zuständigen Behörden und der zentralen Anlaufstelle des Aufnahmestaats zusammen. Die zentrale Anlaufstelle des Aufnahmestaats vertritt die Stelle der Union im Zusammenhang mit den Verpflichtungen gemäß Kapitel III.

Abänderung 69

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.

Abänderung 70

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.

Abänderung 71

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	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.	eingerichtet werden.

Abänderung 72

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

Abänderung 73

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.

Abänderung 74

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

Vorschlag der Kommission	*Geänderter Text*
	5b) Die CERTs werden in die Lage versetzt und aufgefordert, gemeinsame Übungen mit bestimmten CERTs, mit den CERTs aller Mitgliedstaaten und mit entsprechenden Einrichtungen Staaten außerhalb der EU sowie mit CERTs von multinationalen und internationalen Institutionen wie NATO und VN zu initiieren und sich daran zu beteiligen.

Abänderung 75

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

Vorschlag der Kommission	*Geänderter Text*
	5c) Die Mitgliedstaaten können die ENISA oder andere Mitgliedstaaten um Unterstützung bei der Entwicklung ihrer nationalen CERTs ersuchen.

Abänderung 76

Vorschlag für eine Richtlinie
Artikel 8 – Absatz 1

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

Abänderung77

Vorschlag für eine Richtlinie
Artikel 8 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
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. Auf Anfrage kann die ENISA das Kooperationsnetz mit Know-how und Beratung unterstützen. ***Die Marktteilnehmer und Anbieter von Cybersicherheitslösungen können, falls notwendig, auch aufgefordert werden, an den Aufgaben des Kooperationsnetzes nach Absatz 3 Buchstaben g und i***

mitzuwirken.

Das Kooperationsnetz arbeitet, falls notwendig, mit den Datenschutzbehörden zusammen.

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

Abänderung 78

Vorschlag für eine Richtlinie
Artikel 8 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
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;
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) die gemeinsame Erörterung und Bewertung der Wirksamkeit der ***CERTs***, insbesondere bei der Durchführung von NIS-Übungen auf Unionsebene;
f) Zusammenarbeit und ***Informationsaustausch*** in Bezug auf ***alle einschlägigen*** Angelegenheiten mit dem	f) Zusammenarbeit und ***Austausch von Fachwissen*** in Bezug auf ***einschlägige*** Angelegenheiten ***der Netz- und***

bei Europol angesiedelten Europäischen Zentrum zur Bekämpfung der Cyberkriminalität und anderen einschlägigen ***europäischen Einrichtungen in den Bereichen Datenschutz, Energie, Verkehr, Banken, Börsen und Gesundheit***;	***Informationssicherheit, vor allem in den Bereichen Datenschutz, Energie, Verkehr, Banken, Finanzmärkte und Gesundheit,*** mit dem bei Europol angesiedelten Europäischen Zentrum zur Bekämpfung der Cyberkriminalität und anderen einschlägigen ***EU-Einrichtungen***;
	fa) falls angezeigt, Übermittlung von Informationen an den EU-Koordinator für die Terrorismusbekämpfung in Form eines Berichts; sie können auch um Unterstützung bei Analysen, Vorbereitungstätigkeiten und Maßnahmen des Kooperationsnetzes ersuchen;
g) Austausch von Informationen und bewährten Verfahren untereinander und mit der Kommission sowie gegenseitige Unterstützung beim Kapazitätsaufbau im Bereich der NIS;	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.	i) Durchführung von NIS-Übungen auf Unionsebene und gegebenenfalls Teilnahme an internationalen NIS-Übungen.
	ia) Einbeziehung, Konsultation und, falls notwendig, Informationsaustausch mit Marktteilnehmern, über Sicherheitsrisiken und -vorfälle, durch die deren Netze und Informationssysteme beeinträchtigt werden;
	ib) in Zusammenarbeit mit der ENISA die Ausarbeitung von Leitlinien für sektorbezogene Kriterien im Hinblick auf die Meldung von Sicherheitsvorfällen mit beträchtlichen Auswirkungen, zusätzlich zu den Parametern nach Artikel 14 Absatz 2, zur gemeinsamen Auslegung, konsequenten Anwendung und harmonisierten Umsetzung innerhalb der Union.

Abänderung 79

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

Vorschlag der Kommission	*Geänderter Text*
	3a) Das Kooperationsnetz veröffentlicht einmal jährlich einen Bericht über die vorangegangenen 12 Monate, der sich auf seine Aufgaben bezieht und auf dem gemäß Artikel 14 Absatz 4 dieser Richtlinie vorgelegten zusammenfassenden Berichts beruht.

Abänderung 80

Vorschlag für eine Richtlinie
Artikel 8 – Absatz 4

Vorschlag der Kommission	*Geänderter Text*
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 Kommission ***und der ENISA*** fest. Diese Durchführungsrechtsakte werden ***gemäß*** dem in Artikel 19 Absatz 3 genannten ***Prüfverfahren erlassen***.

Abänderung 81

Vorschlag für eine Richtlinie
Artikel 9 – Absatz 1 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	1a) In allen Verarbeitungsphasen werden bei der Mitwirkung an der sicheren Infrastruktur unter anderem geeignete Vertraulichkeits- und Sicherheitsmaßnahmen gemäß der Richtlinie 95/46/EG und der Verordnung (EG) Nr. 45/2001 getroffen.

Abänderung 82

Vorschlag für eine Richtlinie
Artikel 9 – Absatz 2

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:	***entfällt***
a) die Verfügbarkeit einer sicheren, robusten Kommunikations- und Informationsinfrastruktur auf nationaler Ebene, die mit der sicheren Infrastruktur des Kooperationsnetzes nach Artikel 7 Absatz 3 kompatibel und interoperabel ist;	
b) die Verfügbarkeit adäquater technischer, finanzieller und personeller Ressourcen und Verfahren für die zuständigen Behörde und das CERT, durch die eine wirksame, effiziente und sichere Teilnahme am sicheren System für den Informationsaustausch nach Artikel 6 Absatz 3, Artikel 7 Absatz 2 und Artikel 7 Absatz 3 ermöglicht wird.	

Abänderung 83

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***	3) Die Kommission erlässt mittels ***delegierter Rechtsakte ein Paket mit gemeinsamen Verbindungs- und Sicherheitsstandards, die zentrale Anlaufstellen erfüllen müssen, bevor sensible und vertrauliche Informationen über das Kooperationsnetz ausgetauscht werden***.

Prüfverfahren angenommen.

Abänderung 84

Vorschlag für eine Richtlinie
Artikel 10 – Absatz 1

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 gelangt zu der Einschätzung, dass das Sicherheitsrisiko oder der Sicherheitsvorfall*** 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***.

Abänderung 85

Vorschlag für eine Richtlinie
Artikel 10 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
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.

Abänderung 86

Vorschlag für eine Richtlinie
Artikel 10 – Absatz 3

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

Abänderung 87

Vorschlag für eine Richtlinie
Artikel 10 – Absatz 4

Vorschlag der Kommission	*Geänderter Text*
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 Sicherheitsrisiko ***oder*** der Sicherheitsvorfall***, für das bzw. den eine Frühwarnung ausgegeben werden muss, mutmaßlich*** einen kriminellen Hintergrund ***und hat der betroffene Marktteilnehmer Sicherheitsvorfälle mit mutmaßlich schwerwiegendem kriminellem Hintergrund nach Artikel 15 Absatz 4 gemeldet, sorgen die Mitgliedstaaten dafür, dass gegebenenfalls*** das bei Europol angesiedelte Europäische Zentrum zur Bekämpfung der Cyberkriminalität ***informiert wird***.

Abänderung 88

Vorschlag für eine Richtlinie
Artikel 10 – Absatz 4 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	4a) Die Mitglieder des Kooperationsnetzes dürfen Informationen über Sicherheitsrisiken und -vorfälle im Sinne von Absatz 1 ohne vorherige

	Genehmigung der zentralen Anlaufstelle, die die Meldung übermittelt hat, nicht veröffentlichen.
	Darüber hinaus informiert die zentrale Anlaufstelle, die die Meldung übermittelt, vor der Weitergabe von Informationen über das Kooperationsnetz den Marktteilnehmer, auf den sich die Maßnahme bezieht, und anonymisiert die entsprechenden Informationen, sofern sie es für notwendig erachtet.

Abänderung 89

Vorschlag für eine Richtlinie
Artikel 10 – Absatz 4 b (neu)

Vorschlag der Kommission	*Geänderter Text*
	4b) Hat das Sicherheitsrisiko oder der Sicherheitsvorfall, für das bzw. den eine Frühwarnung ausgegeben werden muss, mutmaßlich einen schwerwiegenden länderübergreifenden technischen Hintergrund, informieren die zentralen Anlaufstellen oder die Kommission die ENISA.

Abänderung 90

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.

Abänderung 91

Vorschlag für eine Richtlinie
Artikel 12 – Absatz 2 – Buchstabe a – Spiegelstrich 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***,

Abänderung 92

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.***

Abänderung 93

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

Vorschlag der Kommission	*Geänderter Text*
	3a) Es wird dafür gesorgt, dass der NIS-Kooperationsplan der Union mit den nationalen NIS-Strategien und den nationalen NIS-Kooperationsplänen gemäß Absatz 5 dieser Richtlinie im Einklang steht.

Abänderung 94

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 solchen Vereinbarungen wird der ***Tatsache Rechnung getragen, dass die im Kooperationsnetz zirkulierenden personenbezogenen Daten angemessen geschützt werden müssen, und das Kontrollverfahren angegeben, das anzuwenden ist, um für den Schutz*** der im Kooperationsnetz zirkulierenden personenbezogenen Daten ***Sorge zu tragen***. ***Das Europäische Parlament wird über die Aushandlung der Vereinbarungen unterrichtet. 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.***

Abänderung 95

Vorschlag für eine Richtlinie
Artikel 13 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	Artikel 13a
	Kritikalitätsstufe von Marktteilnehmern
	Die Mitgliedstaaten können die

	Kritikalitätsstufe von Marktteilnehmern festlegen und berücksichtigen dabei die Besonderheiten der Sektoren, Parameter wie die Bedeutung des jeweiligen Marktteilnehmers für die Aufrechterhaltung des sektorbezogenen Diensts in ausreichendem Umfang, die Anzahl der Dienstempfänger des Marktteilnehmers und die Zeitspanne, ab deren Ablauf die Unterbrechung der Kerndienste des Marktteilnehmers negative Auswirkungen auf die Aufrechterhaltung zentraler wirtschaftlicher und gesellschaftlicher Tätigkeiten hat.

Abänderung 96

Vorschlag für eine Richtlinie
Artikel 14 – Absatz 1

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 ***und verhältnismäßige*** 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 konkret*** zu ***bewältigen***. ***Mit diesen*** Maßnahmen ***muss*** unter Berücksichtigung des Standes der Technik ***für*** ein Maß an Sicherheit ***gesorgt werden***, das angesichts des bestehenden Risikos angemessen ist. Insbesondere müssen Maßnahmen ergriffen werden, um Folgen von Sicherheitsvorfällen, die ***die Sicherheit ihrer*** 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,

	sichergestellt ist.

Abänderung 97

Vorschlag für eine Richtlinie
Artikel 14 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
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 ***sorgen dafür***, dass ***die*** Marktteilnehmer ***der*** zuständigen ***Behörde oder der zentralen Anlaufstelle*** Sicherheitsvorfälle ***unverzüglich*** melden, die erhebliche Auswirkungen auf die ***Kontinuität*** der von ihnen bereitgestellten Kerndienste haben. ***Durch die Meldung entsteht der meldenden Partei keine höhere Haftung.***
	Zur Feststellung des Ausmaßes der Auswirkungen eines Sicherheitsvorfalls werden unter anderem folgende Parameter herangezogen:

Abänderung 98

Vorschlag für eine Richtlinie
Artikel 14 – Absatz 2 – Buchstabe a (neu)

Vorschlag der Kommission	*Geänderter Text*
	a) die Anzahl der Nutzer, deren Kerndienst betroffen ist;

Abänderung 99

Vorschlag für eine Richtlinie
Artikel 14 – Absatz 2 – Buchstabe b (neu)

Vorschlag der Kommission	*Geänderter Text*
	b) die Dauer des Sicherheitsvorfalls;

Abänderung 100

Vorschlag für eine Richtlinie
Artikel 14 – Absatz 2 – Buchstabe c (neu)

Vorschlag der Kommission	*Geänderter Text*
	c) die geografische Ausbreitung im Sinne des von dem Sicherheitsvorfall betroffenen Gebiets.

Abänderung 101

Vorschlag für eine Richtlinie
Artikel 14 – Absatz 2 – Unterabsatz 1 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	Diese Parameter werden im Einklang mit Artikel 8 Absatz 3 Buchstabe ib genauer festgelegt.

Abänderung 102

Vorschlag für eine Richtlinie
Artikel 14 – Absatz 2 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	2a) Die Marktteilnehmer melden den zuständigen Behörden oder der zentralen Anlaufstelle des Mitgliedstaats, in dem ein Kerndienst betroffen ist, die in den Absätzen 1 und 2 genannten Sicherheitsvorfälle. Sind Kerndienste in mehreren Mitgliedstaaten betroffen, so 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 Sicherheitsvorfall unterrichtet wurden, welche Maßnahmen eingeleitet wurden

	und zu welchen Ergebnissen dies geführt hat; darüber hinaus erhält er sämtliche Informationen, die für den Sicherheitsvorfall relevant sind.

Abänderung 103

Vorschlag für eine Richtlinie
Artikel 14 – Absatz 2 b (neu)

Vorschlag der Kommission	*Geänderter Text*
	2b) Enthält die Meldung personenbezogene Daten, so dürfen sie nur Empfängern in der zuständigen Behörde oder zentralen Anlaufstelle offengelegt werden, bei der die Meldung eingegangen ist und die diese Daten verarbeiten müssen, um ihre Aufgaben im Einklang mit den Datenschutzvorschriften zu erfüllen. Offengelegt werden dürfen nur Daten, deren Offenlegung notwendig ist, damit die Aufgaben erfüllt werden können.

Abänderung 104

Vorschlag für eine Richtlinie
Artikel 14 – Absatz 2 c (neu)

Vorschlag der Kommission	*Geänderter Text*
	2c) Marktteilnehmer, die in Anhang II nicht aufgeführt sind, können Sicherheitsvorfälle gemäß Artikel 14 Absatz 2 freiwillig melden.

Abänderung 105

Vorschlag für eine Richtlinie
Artikel 14 – Absatz 4

Vorschlag der Kommission	*Geänderter Text*
4) ***Die zuständige*** Behörde kann die	4) ***Nach Konsultation der zuständigen***

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.***	Behörde***, bei der eine Meldung eingegangen ist, und des betroffenen Marktteilnehmers*** kann die ***zentrale Anlaufstelle*** die ***Öffentlichkeit über einzelne Sicherheitsvorfälle unterrichten***, wenn sie ***festlegt***, dass ***der Öffentlichkeit der Sachverhalt bekannt sein muss***, ***damit weiteren Sicherheitsvorfällen vorgebeugt werden kann oder noch andauernde Sicherheitsvorfälle behandelt werden können, oder wenn ein von einem Sicherheitsvorfall betroffener Marktteilnehmer es abgelehnt hat, unverzüglich auf eine im Zusammenhang mit diesem Sicherheitsvorfall gravierende strukturelle Schwachstelle zu reagieren***. ***Vor der Bekanntmachung in der Öffentlichkeit muss die zuständige Behörde, bei der die Meldung eingegangen ist, dafür sorgen, dass der betroffene Marktteilnehmer angehört werden kann und dass der Beschluss über die Bekanntmachung in der Öffentlichkeit sorgsam gegen das Interesse der Öffentlichkeit abgewogen wurde.*** ***Werden Informationen über einzelne Sicherheitsvorfälle in der Öffentlichkeit bekannt gemacht, so muss die zuständige Behörde oder zentrale Anlaufstelle, bei der die Meldung eingegangen ist, dafür sorgen, dass die Bekanntmachung so anonym wie möglich erfolgt.*** ***Wenn es nach vernünftigem Ermessen möglich ist, übermittelt die zuständige Behörde oder die zentrale Anlaufstelle dem betroffenen Marktteilnehmer Informationen, die der konkreten Behandlung des gemeldeten Sicherheitsvorfalls zuträglich sind.***
Die ***zuständige Behörde*** legt dem Kooperationsnetz jährlich einen zusammenfassenden Bericht über die eingegangenen Meldungen und die nach diesem Absatz ergriffenen Maßnahmen vor.	Die ***zentrale Anlaufstelle*** legt dem Kooperationsnetz jährlich einen zusammenfassenden Bericht über die eingegangenen Meldungen ***mit der Anzahl der Meldungen und unter Nennung der in Absatz 2 aufgeführten Parameter eines Sicherheitsvorfalls*** und die nach diesem Absatz ergriffenen Maßnahmen vor.

Abänderung 106

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

Vorschlag der Kommission	*Geänderter Text*
	4a) Die Mitgliedstaaten legen den Marktteilnehmern nahe, Sicherheitsvorfälle, an denen ihre Unternehmen beteiligt sind, freiwillig in ihren Finanzberichten zu veröffentlichen.

Abänderung 107

Vorschlag für eine Richtlinie
Artikel 14 – Absatz 5

Vorschlag der Kommission	*Geänderter Text*
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.	***entfällt***

Abänderung 108

Vorschlag für eine Richtlinie
Artikel 14 – Absatz 6

Vorschlag der Kommission	*Geänderter Text*
6) ***Vorbehaltlich etwaiger nach Absatz 5 erlassener delegierter Rechtsakte können*** die zuständigen Behörden Leitlinien ***annehmen und erforderlichenfalls Anweisungen*** zu den Umständen ***herausgeben***, in denen für ***öffentliche Verwaltungen und*** Marktteilnehmer die Meldepflicht gilt.	6) Die zuständigen Behörden ***oder die zentralen Anlaufstellen können*** Leitlinien zu den Umständen ***erlassen***, in denen für Marktteilnehmer die Meldepflicht gilt.

Abänderung 109

Vorschlag für eine Richtlinie
Artikel 14 – Absatz 8

Vorschlag der Kommission	*Geänderter Text*
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]***, es sei denn, das Kleinstunternehmen ist als Tochterunternehmen eines Marktteilnehmers im Sinne von Artikel 3 Nummer 8 Buchstabe b tätig***.
[35] ABl. L 124 vom 20.5.2003, S. 36.	[35] ABl. L 124 vom 20.5.2003, S. 36.

Abänderung 110

Vorschlag für eine Richtlinie
Artikel 14 – Absatz 8 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	8a) Die Mitgliedstaaten können beschließen, diesen Artikel und Artikel 15 entsprechend auf öffentliche Verwaltungen anzuwenden.

Abänderung 111

Vorschlag für eine Richtlinie
Artikel 15 – Absatz 1

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***	1) Die Mitgliedstaaten ***sorgen dafür***, dass den zuständigen Behörden ***und den zentralen Anlaufstellen die*** Befugnisse eingeräumt werden, die ***diese benötigen, um sicherzustellen, dass*** die

Marktteilnehmer ***gegen die*** Verpflichtungen ***des Artikels*** 14 sowie deren Auswirkungen auf die Netz- und Informationssicherheit ***erforderlich sind***.	Marktteilnehmer ***ihren*** Verpflichtungen ***gemäß Artikel*** 14 sowie deren Auswirkungen auf die Netz- und Informationssicherheit ***nachkommen***.

Abänderung 112

Vorschlag für eine Richtlinie
Artikel 15 – Absatz 2 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
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

Abänderung 113

Vorschlag für eine Richtlinie
Artikel 15 – Absatz 2 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
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 einer qualifizierten unabhängigen Stelle oder einer zuständigen nationalen Behörde durchgeführt wird, und der zuständigen Behörde ***oder der zentralen Anlaufstelle die Belege*** übermitteln***;***

Abänderung 114

Vorschlag für eine Richtlinie
Artikel 15 – Absatz 2 – Unterabsatz 1 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	Die zuständigen Behörden und die zentralen Anlaufstellen nennen bei Übermittlung ihres Ersuchens dessen

	Zweck und geben hinreichend genau an, welche Angaben verlangt werden.

Abänderung 115

Vorschlag für eine Richtlinie
Artikel 15 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
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, Marktteilnehmern verbindliche Anweisungen zu erteilen.

Abänderung 116

Vorschlag für eine Richtlinie
Artikel 15 – Absätze 3 a und 3 b (neu)

Vorschlag der Kommission	*Geänderter Text*
	3a) Abweichend von Absatz 2 Buchstabe b können die Mitgliedstaaten beschließen, dass die zuständigen Behörden oder die zentralen Anlaufstellen auf der Grundlage der nach Artikel 13a festgelegten jeweiligen Kritikalitätsstufe auf bestimmte Marktteilnehmer ein anderes Verfahren anwenden. In diesem Fall
	a) sind die zuständigen Behörden bzw. zentralen Anlaufstellen befugt, den Marktteilnehmern eine hinreichend spezifische Aufforderung zu übermitteln, mit der Auflage, Belege über die tatsächliche Umsetzung der Sicherheitsmaßnahmen vorzulegen, beispielsweise die Ergebnisse einer Sicherheitsüberprüfung, die von einem qualifizierten internen Prüfer durchgeführt wurde, und die Belege an die zuständige Behörde oder die zentrale Anlaufstelle zu übermitteln;

	b) kann die zuständige Behörde oder die zentrale Anlaufstelle nach Übermittlung der Auskünfte durch den Marktteilnehmer gemäß Buchstabe a bei Bedarf zusätzliche Belege oder eine zusätzliche Überprüfung durch eine qualifizierte unabhängige Stelle oder eine nationale Behörde anfordern.
	3b) Die Mitgliedstaaten können die Häufigkeit und Intensität der Überprüfungen eines Marktteilnehmers verringern, wenn aus der Sicherheitsüberprüfung hervorgeht, dass er seinen Verpflichtungen nach Kapitel IV durchgehend nachgekommen ist.

Abänderung 117

Vorschlag für eine Richtlinie
Artikel 15 – Absatz 4

Vorschlag der Kommission	*Geänderter Text*
4) Die zuständigen Behörden ***melden*** den Strafverfolgungsbehörden Sicherheitsvorfälle***, bei denen ein schwerwiegender krimineller*** Hintergrund ***vermutet wird***.	4) Die zuständigen Behörden ***und die zentralen Anlaufstellen unterrichten die betroffenen Marktteilnehmer über die Möglichkeit,*** den Strafverfolgungsbehörden Sicherheitsvorfälle ***mit mutmaßlich schwerwiegendem kriminellem*** Hintergrund ***zu melden***.

Abänderung 118

Vorschlag für eine Richtlinie
Artikel 15 – Absatz 5

Vorschlag der Kommission	*Geänderter Text*
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 Datenschutzvorschriften 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 arbeiten gemeinsam mit der ENISA Mechanismen für den Informationsaustausch und ein einheitliches Muster aus, mit denen bzw. dem Meldungen gemäß Artikel 14 Absatz 2 dieser Richtlinie und weiteren Unionsrechtsvorschriften über den Datenschutz übermittelt werden.***

Abänderung 119

Vorschlag für eine Richtlinie
Artikel 15 – Absatz 6

Vorschlag der Kommission	*Geänderter Text*
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 ***sorgen dafür***, dass alle Verpflichtungen, die Marktteilnehmern nach diesem Kapitel auferlegt werden, einer gerichtlichen Nachprüfung unterzogen werden können.

Abänderung 120

Vorschlag für eine Richtlinie
Artikel 15 – Absatz 6 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	6a) Die Mitgliedstaaten können beschließen, Artikel 14 und diesen Artikel entsprechend auf öffentliche Verwaltungen anzuwenden.

Abänderung 121

Vorschlag für eine Richtlinie
Artikel 16 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
1) ***Um eine einheitliche Umsetzung des***	1) ***Damit Artikel*** 14 Absatz 1 ***einheitlich***

Artikels 14 Absatz 1 ***zu gewährleisten***, fördern die Mitgliedstaaten die Anwendung einschlägiger Normen und/oder Spezifikationen für die Netz- und Informationssicherheit.	***umgesetzt wird***, fördern die Mitgliedstaaten die Anwendung einschlägiger ***europäischer oder internationaler interoperabler*** Normen und/oder Spezifikationen für die Netz- und Informationssicherheit***, ohne jedoch die Anwendung einer bestimmten Technologie vorzuschreiben***.

Abänderung 122

Vorschlag für eine Richtlinie
Artikel 16 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
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 dem zuständigen europäischen Normungsgremium nach Rücksprache mit den maßgeblichen Interessenträgern 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.

Abänderung 123

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

Vorschlag der Kommission	*Geänderter Text*
	1a) Die Mitgliedstaaten sorgen dafür, dass die Sanktionen nach Absatz 1 nur greifen, wenn der Marktteilnehmer seinen Verpflichtungen nach Kapitel IV vorsätzlich oder grob fahrlässig nicht nachgekommen ist.

Abänderung 124

Vorschlag für eine Richtlinie
Artikel 18 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
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***.	3) Die ***Befugnisübertragung gemäß*** Artikel 9 Absatz 2 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 ***im Beschluss über den Widerruf*** angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit ***von delegierten Rechtsakten, die*** bereits in Kraft ***sind, wird von dem Beschluss über den Widerruf nicht berührt***.

Abänderung 125

Vorschlag für eine Richtlinie
Artikel 18 – Absatz 5

Vorschlag der Kommission	*Geänderter Text*
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.	5) Ein delegierter Rechtsakt, der ***gemäß*** Artikel 9 Absatz 2 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 ***haben*** oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Initiative des Europäischen Parlaments oder des Rates ***wird diese Frist*** um zwei Monate verlängert.

Abänderung 126

Vorschlag für eine Richtlinie
Artikel 20

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 ***und insbesondere die Liste in Anhang II*** 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.

Abänderung 127

Vorschlag für eine Richtlinie
Anhang I – Überschrift

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

Abänderung 128

Vorschlag für eine Richtlinie
Anhang I – 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	a) Die ***CERTs sorgen für die*** hohe Verfügbarkeit ***ihrer*** Kommunikationsdienste***, indem sie punktuellen Ausfällen vorbeugen*** und ***mehrere*** Kanäle ***bereitstellen***, damit ***die CERTs*** ständig erreichbar ***bleiben*** und selbst Kontakt ***untereinander*** aufnehmen ***können***. Die Kommunikationskanäle müssen genau spezifiziert sein und den CERT-Nutzern (Constituency) und

(Constituency) und Kooperationspartnern bekannt gegeben werden.	Kooperationspartnern bekannt gegeben werden.

Abänderung 129

Vorschlag für eine Richtlinie
Anhang I – – 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.

Abänderung 130

Vorschlag für eine Richtlinie
Anhang I – 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;

Abänderung 131

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

Vorschlag der Kommission	*Geänderter Text*
	– aktive Mitwirkung in internationalen CERT-Kooperationsnetzen sowie CERT-Kooperationsnetzen der Union;

Abänderung 132

Vorschlag für eine Richtlinie
Anhang II – Einleitung

Vorschlag der Kommission	*Geänderter Text*
Liste der Marktteilnehmer	Liste der Marktteilnehmer
nach Artikel 3 Absatz 8 Buchstabe a	
1. Plattformen des elektronischen Geschäftsverkehrs	
2. Internet-Zahlungs-Gateways	
3. Soziale Netze	
4. Suchmaschinen	
5. Cloud-Computing-Dienste	
6. Application Stores	
nach Artikel 3 Absatz 8 Buchstabe b	

Abänderung 133

Vorschlag für eine Richtlinie
Anhang II – Nummer 1

Vorschlag der Kommission	*Geänderter Text*
Liste der Marktteilnehmer	Liste der Marktteilnehmer
1. Energie	1. Energie
	a) Strom
– Strom- und Gasversorger	***– Lieferanten***
– Verteilernetzbetreiber und Endkundenlieferanten im Strom- und/oder Gassektor	***– Fernleitungsnetzbetreiber und Endkundenlieferanten***
– Erdgas-Fernleitungsnetzbetreiber, Erdgasspeicher- und LNG-Anlagenbetreiber	
– Übertragungsnetzbetreiber (Strom)	– Übertragungsnetzbetreiber (Strom)
	b) Erdöl
– Erdöl-Fernleitungen und Erdöllager	***– Erdölfernleitungen*** und Erdöllager
	– Betreiber von Anlagen zur Produktion, Raffination und Behandlung von Erdöl, Betreiber von Erdöllagern und -fernleitungen
	c) Erdgas

– Strom- und Gasmarktteilnehmer	***– Lieferanten***
	– Fernleitungsnetzbetreiber und Endkundenlieferanten
	– Erdgas-Fernleitungsnetzbetreiber, Erdgasspeicher- und LNG-Anlagenbetreiber
– Betreiber von ***Erdöl- und Erdgas-Produktions-, -Raffinations- und Behandlungsanlagen***	– Betreiber von ***Anlagen zur Produktion, Raffination und Behandlung von Erdgas, Betreiber von Erdgasspeichern und -fernleitungen***
	– Marktteilnehmer (Erdgas)

Abänderung 134

Vorschlag für eine Richtlinie
Anhang II – Nummer 2

Vorschlag der Kommission	*Geänderter Text*
2. Verkehr	2. Verkehr
– Luftfahrtunternehmen (Luftfrachtverkehr und Personenbeförderung)	***a) Straßenverkehr***
– Beförderungsunternehmen des Seeverkehrs (Personen- und Güterbeförderung in der See- und Küstenschifffahrt)	***i) Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen***
– Eisenbahnen (Infrastrukturbetreiber, integrierte Unternehmen und Eisenbahnunternehmen)	***ii) unterstützende Logistikdienste:***
– Flughäfen	***– Lagerhaltung und Lagerung***
– Häfen	***– Frachtumschlagsleistungen und***
– Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen	***– andere unterstützende Verkehrsleistungen***
– Unterstützende Logistikdienste: a) Lagerhaltung und Lagerung b) Frachtumschlagsleistungen und c) andere unterstützende Verkehrsleistungen	***b) Schienenverkehr***
	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)

Abänderung 135

Vorschlag für eine Richtlinie
Anhang II – Nummer 4

Vorschlag der Kommission	*Geänderter Text*
4. Finanzmarktinfrastrukturen: ***Börsen*** und Clearingstellen mit zentraler Gegenpartei	4. Finanzmarktinfrastrukturen: ***geregelte Märkte, multilaterale Handelssysteme, organisierte Handelssysteme*** und Clearingstellen mit zentraler Gegenpartei

Abänderung 136

Vorschlag für eine Richtlinie
Anhang II – Nummer 5 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	5a. Wassergewinnung und -versorgung

Abänderung 137

Vorschlag für eine Richtlinie
Anhang II – Nummer 5 b (neu)

Vorschlag der Kommission	*Geänderter Text*
	5b. Lebensmittelversorgungskette

Abänderung 138

Vorschlag für eine Richtlinie
Anhang II – Nummer 5 c (neu)

Vorschlag der Kommission	*Geänderter Text*
	5c. Internet-Knoten