Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses 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) 48 final — 2013/0027 (COD)

(2013/C 271/25)

Berichterstatter: **Thomas McDONOGH**

Der Rat und das Europäische Parlament beschlossen am 21. Februar bzw. 15. April 2013, den Europäischen Wirtschafts- und Sozialausschuss gemäß Artikel 114 AEUV um Stellungnahme zu folgender Vorlage zu ersuchen:

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) 48 final – 2013/0027 (COD).

Die mit den Vorarbeiten beauftragte Fachgruppe Verkehr, Energie, Infrastrukturen, Informationsgesellschaft nahm ihre Stellungnahme am 30. April 2013 an.

Der Ausschuss verabschiedete auf seiner 490. Plenartagung am 22./23. Mai 2013 (Sitzung vom 22. Mai) mit 163 Stimmen gegen 1 Stimme bei 5 Enthaltungen folgende Stellungnahme:

1. Schlussfolgerungen und Empfehlungen

1.1 Der Ausschuss stellt fest, dass in der vorgeschlagenen Richtlinie, die in den übergeordneten Zusammenhang der jüngst veröffentlichten Cybersicherheitsstrategie einzureihen ist ([1]), ein umfassender Ansatz für Netz- und Informationssicherheit (NIS) entworfen wird, um ein sicheres Wachstum der digitalen Wirtschaft zu gewährleisten, während gleichzeitig die europäischen Werte Freiheit und Demokratie gefördert werden.

1.2 Der Ausschuss begrüßt diesen Vorschlag für eine Richtlinie zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der gesamten EU. Harmonisierung und Management von NIS auf europäischer Ebene ist wesentliche Voraussetzung für die Vollendung des digitalen Binnenmarkts und für das reibungslose Funktionieren des Binnenmarkts insgesamt. Der Ausschuss teilt die Bedenken der Europäischen Kommission in Bezug auf die mögliche, enorme Schädigung der Wirtschaft und Beeinträchtigung des Wohlergehens der Unionsbürger bei NIS-Versagen. Allerdings erfüllt die vorgeschlagene Richtlinie nicht die Erwartungen, die der Ausschuss an starke Rechtsvorschriften in diesem kritischen Bereich stellt.

1.3 Der Ausschuss ist ausgesprochen enttäuscht über den Mangel an Fortschritten in zahlreichen Mitgliedstaaten bei der Einführung einer wirksamen NIS auf nationaler Ebene. Er bedauert die damit verbundenen zunehmenden Risiken für die Bürger und negativen Auswirkungen auf die Vollendung des digitalen Binnenmarkts. Sämtliche Mitgliedstaaten sollten schleunigst ihren noch ausstehenden NIS-Verpflichtungen nachkommen.

1.4 Durch diesen Mangel an Fortschritt tut sich eine neue digitale Kluft zwischen der Elite unter den Mitgliedstaaten, die über fortschrittlichste NIS verfügen, und den rückständigeren Mitgliedstaaten auf. Diese Kluft beeinträchtigt Vertrauen und Zusammenarbeit im NIS-Bereich auf EU-Ebene, und wenn nicht schleunigst etwas dagegen getan wird, wird das Kompetenzgefälle zwischen den Mitgliedstaaten aller Voraussicht nach zu Binnenmarktversagen führen.

1.5 Wie in früheren Stellungnahmen ([2]) schon betont der Ausschuss erneut, dass zögerliche, freiwillige Maßnahmen seines Erachtens nicht zum Erfolg führen und strenge rechtliche Verpflichtungen der Mitgliedstaaten erforderlich sind, um Governance und Durchsetzung einer harmonisierten europäischen NIS zu ermöglichen. Leider wartet dieser Richtlinienvorschlag nicht mit den notwendigen klaren und entschiedenen Vorschriften auf. Um das erforderliche hohe gemeinsame NIS-Niveau zu erreichen, hält der Ausschuss eine Verordnung mit klar definierten zwingenden Auflagen für die Mitgliedstaaten für besser geeignet als eine Richtlinie.

1.6 Ungeachtet der Absicht der Europäischen Kommission, mittels delegierter Rechtsakte einheitliche Voraussetzungen für die Umsetzung von Teilen dieser Richtlinie zu gewährleisten, mangelt es in dem Richtlinienvorschlag nach Ansicht des Ausschusses an Normen, klaren Definitionen und kategorischen Verpflichtungen, so dass den Mitgliedstaaten zu viel Spielraum bei der Auslegung und Umsetzung kritischer Elemente bleibt. Der Ausschuss plädiert für eine genauere Ausformulierung der Normen, Anforderungen und Verfahren, die für die Mitgliedstaaten, Behörden, Marktteilnehmer und Infrastrukturbetreiber für wichtige Internetdienste gelten sollen.

([1]) Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum JOIN (2013) 1.

([2]) EWSA-Stellungnahmen zu den Themen „Schutz kritischer Informationsinfrastrukturen“ ABl. C 255 vom 22.9.2010, S. 98 und „Angriffe auf Informationssysteme“ ABl. C 218 vom 23.7.2011, S. 130.

1.7 Der Ausschuss würde die Schaffung einer NIS-Behörde auf EU-Ebene nach dem Vorbild der Europäischen Agentur für Flugsicherheit (EASA) ([3]) befürworten, um für die Durchsetzung einer robusten NIS-Politik in der EU zu sorgen. Eine solche Behörde würde Standards aufstellen und alle Elemente der NIS in der ganzen EU überwachen, von der Zertifizierung sicherer Endgeräte und ihrer Nutzung über die Netzsicherheit bis hin zur Datensicherheit.

1.8 Der Ausschuss ist sich deutlich der wachsenden Gefährdung von Cybersicherheit und Datenschutz bewusst, die von der zunehmenden Nutzung von Cloud Computing ([4]) in Europa ausgehen. Der Richtlinienvorschlag sollte explizit spezifische zusätzliche Sicherheitsanforderungen und Auflagen im Zusammenhang mit der Bereitstellung und Nutzung von Cloud-Diensten enthalten.

1.9 Im Interesse einer echten Rechenschaftspflicht für NIS sollte in dem letztendlichen Rechtsakt klargestellt werden, dass Einrichtungen, die im Rahmen der vorgeschlagenen Richtlinie Verpflichtungen unterliegen, berechtigt wären, Software- und Hardware-Anbieter für Mängel ihrer Produkte oder Dienste haftbar zu machen, die unmittelbar zu NIS-Vorfällen beitragen.

1.10 Der Ausschuss fordert die Mitgliedstaaten auf, der Verbesserung von NIS-Wissen und Cybersicherheitskompetenz der KMU besondere Aufmerksamkeit zu widmen. Er weist die Kommission auf den Erfolg von „Hacker-Wettbewerben" in den USA ([5]) und einigen Mitgliedstaaten ([6]) hin, durch die das Bewusstsein für Cybersicherheitsbelange gefördert und die nächste Generation von NIS-Spezialisten herangezogen werden kann.

1.11 Da es für die Netz- und Informationssicherheit der gesamten EU wichtig ist, dass alle Mitgliedstaaten die Vorschriften einhalten, sollte die Kommission prüfen, welche Mittel im Rahmen des mehrjährigen Finanzrahmens für NIS-Compliance genutzt werden könnten, um den Mitgliedstaaten zu helfen, die finanzielle Unterstützung benötigen.

1.12 Ausgaben für Forschung, Entwicklung und Innovation (FuDuI) im Bereich NIS-Technologien sollte im Rahmenprogramm für Forschung und Innovation „Horizont 2020" hohe Priorität zukommen, damit Europa mit der dynamischen Entwicklung von Cyber-Bedrohungen Schritt halten kann.

([3]) Europäische Agentur für Flugsicherheit (EASA) http://www.easa.europa.eu/language/de/home.php

([4]) EWSA-Stellungnahmen zu den Themen „Cloud Computing in Europa" ABl. C 24 vom 28.1.2012, S. 40 und „Eine Cloud-Computing-Strategie für die EU" ABl. C 76 vom 14.3.2013, S. 59.

([5]) http://www.nytimes.com/2013/03/25/technology/united-states-wants-to-attract-hackers-to-public-sector.html?pagewanted=all&_r=0

([6]) http://www.bbc.co.uk/news/technology-17333601

1.13 Um für Klarheit darüber zu sorgen, welche Einrichtungen im Rahmen der vorgeschlagenen Richtlinie rechtliche Verantwortlichkeiten haben, plädiert der Ausschuss für eine Verpflichtung aller Mitgliedstaaten zur Veröffentlichung eines Online-Verzeichnisses all derjenigen Einrichtungen, für die die Risikomanagement- und Meldepflichten gemäß der Richtlinie gelten. Die damit einhergehende Transparenz und öffentliche Rechenschaftspflicht würde die Vertrauensbildung und die Einhaltung der Vorschriften unterstützen.

1.14 Der Ausschuss verweist die Europäische Kommission auf seine zahlreichen früheren Stellungnahmen, in denen er sich zur Netz- und Informationssicherheit sowie zur Notwendigkeit einer sicheren Informationsgesellschaft und des Schutzes kritischer Informationsinfrastrukturen geäußert hat ([7]).

2. **Wesentlicher Inhalt des Kommissionsvorschlags**

2.1 Der Vorschlag für eine NIS-Richtlinie wurde in Verbindung mit der EU-Cybersicherheitsstrategie veröffentlicht, die zum Ziel hat, die Robustheit der Informationssysteme zu verstärken, die Cyberkriminalität zurückzudrängen, eine internationale Cybersicherheitspolitik für die EU und die Cyberverteidigung der EU zu fördern, die industriellen und technischen Ressourcen für die Cybersicherheit zu entwickeln und gleichzeitig die Grundrechte und die anderen Grundwerte der EU zu fördern.

2.2 Bei der NIS geht es um die Erhöhung der Sicherheit des Internets und anderer Netze, Informationssysteme und darauf beruhender Dienste, die für das Funktionieren unserer Gesellschaften unverzichtbar sind. NIS ist wesentliche Voraussetzung für ein reibungsloses Funktionieren des Binnenmarkts.

2.3 Das bisherige, rein auf Freiwilligkeit beruhende NIS-Konzept der EU bietet keinen ausreichenden Schutz gegen NIS-Bedrohungen. Die bestehenden NIS-Kapazitäten reichen nicht aus, um mit den sich schnell verändernden Bedrohungen Schritt zu halten und in allen Mitgliedstaaten ein gleich hohes Schutzniveau zu gewährleisten.

([7]) EWSA-Stellungnahme zum Thema „Eine Strategie für eine sichere Informationsgesellschaft", ABl. C 97 vom 28.4.2007, S. 21.
EWSA-Stellungnahme zum Thema „Schutz kritischer Informationsinfrastrukturen", ABl. C 255 vom 22.9.2010, S. 98.
EWSA-Stellungnahme zum Thema „Neue ENISA-Verordnung", ABl. C 107 vom 6.4.2011, S. 58.
EWSA-Stellungnahme zum Thema „Datenschutz-Grundverordnung", ABl. C 229 vom 31.7.2012, S. 90.
EWSA-Stellungnahme zum Thema „Angriffe auf Informationssysteme", ABl. C 218 vom 23.7.2011, S. 130.
EWSA-Stellungnahme zum Thema „Elektronische Transaktionen im Binnenmarkt", ABl. C 351 vom 15.11.2012, S. 73.
EWSA-Stellungnahme zum Thema „Eine Cloud-Computing-Strategie für die EU", ABl. C 76 vom 14.3.2013, S. 59.

2.4 Es gibt große Unterschiede in Bezug auf die Kapazitäten und die Abwehrbereitschaft der einzelnen Mitgliedstaaten, was zu einem fragmentierten Vorgehen im NIS-Bereich in der EU führt. Da die Netze und Systeme miteinander verbunden sind, mindern die Mitgliedstaaten mit einem unzureichenden Schutzniveau die Gesamt-NIS in der EU. Diese Situation behindert auch die Schaffung von Vertrauen zwischen den Partnern als Voraussetzung für Zusammenarbeit und Informationsaustausch. In der Folge findet eine Zusammenarbeit nur zwischen jenen wenigen Mitgliedstaaten statt, die bereits über hohe Kapazitäten verfügen.

2.5 Ziel der im Einklang mit Artikel 114 AEUV vorgeschlagenen Richtlinie ist es, die Vollendung und das reibungslose Funktionieren des digitalen Binnenmarkts zu fördern und dazu

— ein gemeinsames NIS-Mindestniveau in den Mitgliedstaaten einzuführen, um die Abwehrbereitschaft und Reaktionsfähigkeit insgesamt zu erhöhen;

— die Zusammenarbeit im Bereich NIS auf EU-Ebene zu verbessern, um grenzübergreifende Sicherheitsvorfälle und Bedrohungen zu bewältigen;

— eine Risikomanagementkultur zu schaffen und den Informationsaustausch zwischen dem privaten und dem öffentlichen Sektor zu verbessern.

2.6 In der vorgeschlagenen Richtlinie werden u.a. folgende rechtlichen Anforderungen vorgesehen:

(a) Jeder Mitgliedstaat nimmt eine nationale NIS-Strategie an und benennt eine für die NIS zuständige nationale Behörde, die mit angemessenen finanziellen und personellen Ressourcen ausgestattet wird, um die Prävention von, den Umgang mit und die Reaktion auf NIS-Vorfälle und -Risiken gewährleisten zu können;

(b) Einrichtung von Kooperationsmechanismen zwischen den Mitgliedstaaten und der Kommission zur Verbreitung von Frühwarnungen vor Sicherheitsrisiken und –vorfällen, zur Zusammenarbeit und Durchführung regelmäßiger gegenseitiger Überprüfungen;

(c) Bestimmte Arten von Einrichtungen in der ganzen EU müssen eine Risikomanagementkultur entwickeln und ihrer zuständigen nationalen Behörde Sicherheitsvorfälle mit erheblichen Auswirkungen auf die von ihnen bereitgestellten Kerndienste melden. Davon betroffen sind Betreiber kritischer Informationsinfrastrukturen in einer Reihe von Sektoren (Finanzdienstleistungen, Verkehr, Energie, Gesundheitswesen), wichtige Anbieter von Diensten der Informationsgesellschaft (Cloud Computing, Plattformen für den elektronischen Geschäftsverkehr, Internet-Zahlungs-Gateways, Suchmaschinen, Application Stores und soziale Netze) und öffentliche Verwaltungen.

2.7 Die Mitgliedstaaten müssen die Richtlinie binnen 18 Monaten nach ihrer Annahme durch den Rat und das Europäische Parlament (voraussichtlich 2014) umsetzen.

3. **Allgemeine Bemerkungen**

3.1 Das Internet und die digitale Gesellschaft breiten sich immer mehr im Alltag aus. Je mehr wir jedoch auf das Internet angewiesen sind, desto mehr hängen unsere Freiheit, unser Wohlstand und unsere Lebensqualität von einer zuverlässigen Netz- und Informationssicherheit (NIS) ab: Eine unterbrochene Internet-Verbindung und eine im medizinischen Notfall unzugängliche elektronische Patientenakte kann ein Todesurteil sein. Die Sicherheit der kritischen Informationsinfrastrukturen ist aber zunehmenden Bedrohungen ausgesetzt und unser NIS-Niveau ist unzureichend.

3.2 Europol-Direktor Rob Wainwright äußerte vergangenes Jahr seine große Besorgnis angesichts des großen unangebrachten Vertrauens in die Robustheit des Internet ([8]). Immer wieder wird über neue Cyberangriffe auf wesentliche Infrastrukturen berichtet, die von Kriminellen, Terroristen oder fremden Regierungen ausgehen. Cyber-Opfer melden Angriffe meist nicht, um Imageschäden zu vermeiden; indes haben in den vergangenen Wochen Angriffe auf die europäische Internetinfrastuktur ([9]) und Bankensysteme ([10]) stattgefunden, deren Ausmaß nicht vertuscht werden konnte. Einem Bericht ([11]) zufolge wurden in den Niederlanden im Jahr 2011 92 Mio. Cyberangriffe verzeichnet und in Deutschland 82 Mio. Schätzungen der britischen Regierung zufolge fanden im Vereinigten Königreich 2011 44 Mio. Cyberangriffe statt, die wirtschaftliche Kosten in Höhe von 30 Mrd. EUR verursachten ([12]).

3.3 2007 befasste sich der Rat der EU mit der NIS-Problematik in Europa ([13]). Die seitherige Strategie ([14]) beruhte jedoch zumeist auf freiwilligen Maßnahmen der Mitgliedstaaten, von denen nur wenige auf wirksame Weise tätig wurden. Der Ausschuss stellt fest, dass viele Mitgliedstaaten bislang weder eine nationale Cybersicherheitsstrategie veröffentlicht noch nationale Notfallpläne für Cybervorfälle aufgestellt und zum Teil auch noch kein IT-Notfallteam (Computer Emergency Response Team, CERT) eingerichtet haben. Verschiedene Mitgliedstaaten haben auch noch nicht das Übereinkommen des Europarats über Computerkriminalität ratifiziert ([15]).

([8]) http://forumblog.org/2012/05/what-if-the-internet-collapsed/
([9]) http://www.nytimes.com/2013/03/27/technology/internet/online-dispute-becomes-internet-snarling-attack.html?pagewanted=all&_r=0
([10]) http://www.dutchnews.nl/news/archives/2013/04/online_retailers_demand_banks.php
([11]) http://www.securelist.com/en/analysis/204792216/Kaspersky_Security_Bulletin_Statistics_2011
([12]) UK Cyber Security Strategy – Landscape Review: http://media.nao.org.uk/uploads/2013/03/Cyber-security-Full-report.pdf
([13]) Entschließung des Rates 2007/C 68/01: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:068:0001:0004:DE:PDF
([14]) COM(2006) 251 und COM(2009) 149.
([15]) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?CL=GER&CM=&NT=185&DF=&VL

3.4 Zehn Mitgliedstaaten mit einem sehr hohen NIS-Niveau haben die europäische EGC-Gruppe (European Governmental CERTs Group – EGC) gegründet, um wirksam zusammenzuarbeiten für den Fall, dass gemeinschaftlich auf IT-Sicherheitsvorfälle reagiert werden muss. Die EGC ist eine geschlossene Elite-Gruppe, von der die rückständigeren übrigen 17 Mitgliedstaaten sowie das neu gegründete CERT-EU ([16]) derzeit ausgeschlossen sind. Eine neue digitale Kluft zwischen den Mitgliedstaaten, die über fortschrittlichste NIS verfügen, und den übrigen Mitgliedstaaten tut sich auf. Wenn diese Kluft nicht geschlossen wird, wird das NIS-Gefälle den digitalen Binnenmarkt im Kern gefährden und die Vertrauensentwicklung, Harmonisierung und Interoperabilität hemmen. Ohne konsequente Maßnahmen dürfte die Schere zwischen den fortschrittlichsten und den rückständigeren Mitgliedstaaten immer weiter aufgehen und Binnenmarktversagen, das auf das Kompetenzgefälle zwischen den Mitgliedstaaten zurückzuführen ist, zunehmen.

3.5 Voraussetzung für den Erfolg der Cybersicherheitsstrategie und die Wirksamkeit der vorgeschlagenen NIS-Richtlinie sind eine starke NIS-Industrie in Europa und genügend ausgebildete NIS-Fachkräfte. Der Ausschuss begrüßt, dass in dem Richtlinienvorschlag berücksichtigt wird, dass die Mitgliedstaaten in Ausbildungs-, Aufklärungs- und Schulungsprogramme für NIS investieren müssen. Dazu sollte jeder Mitgliedstaat gezielt auf die KMU zugeschnittene Informations-, Bildungs- und Fördermaßnahmen im Bereich Cybersicherheit vorsehen. Große Unternehmen können das erforderliche Wissen leicht beschaffen, KMU hingegen müssen hierbei unterstützt werden.

3.6 Der Ausschuss freut sich auf die Zusammenarbeit mit der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) im Rahmen der Sensibilisierung für NIS anlässlich des Europäischen Monats der Cybersicherheit im Spätjahr 2013. Mit Blick auf das Ziel der Cybersicherheitsstrategie und der NIS-Richtlinie, eine Sicherheitskultur in Europa zu fördern, sowie auf eine Verbesserung der NIS-Kompetenzen verweist der Ausschuss die Kommission auf die „Hacker-Wettbewerbe" für Teenager, die in einigen Mitgliedstaaten und in den USA so erfolgreich zur Sensibilisierung beigetragen haben.

3.7 Der Ausschuss nimmt zufrieden zur Kenntnis, dass die Cybersicherheitsstrategie Ausgaben für Forschung, Entwicklung und Innovation im Bereich NIS-Technologien vorsieht.

3.8 Durch die Ausweitung von Cloud Computing entstehen viele neue Cybersicherheits-Bedrohungen. Beispielsweise können Cyberkriminelle nun zu geringen Kosten auf enorme Computerkapazitäten zugreifen, und Daten von Tausenden Unternehmen werden auf zentralen Servern gehostet, die gezielt attackiert werden können. Der Ausschuss hat höhere IT-Widerstandsfähigkeit bei Cloud Computing gefordert ([17]).

([16]) CERT-EU ist das ständige IT-Notfallteam (Computer Emergency Response Team, CERT-EU) für die EU-Institutionen, -Agenturen und –Einrichtungen.

([17]) EWSA-Stellungnahmen zu den Themen „Cloud Computing in Europa" ABl. C 24 vom 28.1.2012, S. 40 und „Eine Cloud-Computing-Strategie für die EU" ABl. C 76 vom 14.3.2013, S. 59.

3.9 Der Ausschuss hat sich bereits für die Einführung eines freiwilligen europäischen Systems für elektronische Identifizierung bei Online-Transaktionen in Ergänzung bestehender nationaler Systeme ausgesprochen. Dadurch würden ein höherer Schutz vor Betrug, größeres Vertrauen zwischen den Wirtschaftsakteuren, geringere Kosten der Dienstleistungserbringung und höherwertige Dienste sowie ein besserer Schutz der Bürger erreicht werden.

4. **Besondere Bemerkungen**

4.1 Bedauerlicherweise ist der Kommissionsvorschlag für eine NIS-Richtlinie zu zögerlich und unscharf und baut zu stark auf Selbstregulierung der Mitgliedstaaten. Ein Mangel an Normen, klaren Definitionen und kategorischen Verpflichtungen, insbesondere in Kapitel IV der vorgeschlagenen Richtlinie, lässt den Mitgliedstaaten zu viel Spielraum bei der Auslegung und Umsetzung kritischer Elemente. Eine Verordnung mit klar definierten zwingenden Auflagen für die Mitgliedstaaten wäre wirksamer als eine Richtlinie.

4.2 Laut Artikel 6 der vorgeschlagenen Richtlinie benennt jeder Mitgliedstaat eine „zuständige Behörde", die die einheitliche Anwendung der Richtlinie in der Union überwacht und sicherstellt. Artikel 8 zufolge wird ein „Kooperationsnetz" gebildet, das gemeinsam mit der Kommission europaweit und bis hin zur Ebene der Mitgliedstaaten für Führung, verantwortliches Handeln und nötigenfalls für Durchsetzung sorgen wird. Aufbauend auf diesem Governance-Rahmen sollte die EU die Einrichtung einer NIS-Behörde auf EU-Ebene nach dem Vorbild der Europäischen Agentur für Flugsicherheit (EASA), die Standards festlegt und für die Überwachung der Durchsetzung von Sicherheitsvorschriften für Luftfahrzeuge, Flughäfen und Flugverkehr sorgt, in Betracht ziehen.

4.3 Diese NIS-Behörde auf EU-Ebene könnte sich auf die Arbeiten von ENISA (Europäische Agentur für Netz- und Informationssicherheit), CEN (Europäisches Komitee für Normung), IT-Notfallteams (Computer Emergency Response Teams, CERTs), der European Governmental CERT Group (EGC) u.a. stützen. Eine solche Behörde würde Standards aufstellen und alle Elemente der NIS überwachen, von der Zertifizierung sicherer Endgeräte und ihrer Nutzung über die Netzsicherheit bis hin zur Datensicherheit.

4.4 In Anbetracht der starken Verflechtungen zwischen den Mitgliedstaaten im Zusammenhang mit der EU-Netz- und Informationssicherheit sowie der potenziell sehr hohen Kosten für alle Betroffenen bei NIS-Versagen plädiert der Ausschuss für die Festlegung expliziter und verhältnismäßiger harmonisierter Strafen und Sanktionen für Verstöße gegen die Bestimmungen der Richtlinie, die der europäischen Dimension der Verantwortung und dem potenziellen Schadensausmaß nicht nur auf nationaler, sondern auch auf europäischer Ebene angemessen sind. Artikel 17 des Richtlinienvorschlags, in dem es um Sanktionen geht, ist zu allgemein gehalten, lässt den Mitgliedstaaten zu viel Spielraum bei der Festlegung von Sanktionen und bietet keine ausreichenden Vorgaben für die Berücksichtigung grenzüberschreitender und europaweiter Auswirkungen.

4.5 Regierungen und Anbieter grundlegender Dienste machen heutzutage Sicherheits- und Stabilitätsprobleme nur publik, wenn dies unausweichlich ist. Diese mangelnde Offenlegung erfolgter Angriffe untergräbt die Fähigkeit Europas, rasch und wirksam auf Bedrohungen zu reagieren und die allgemeine NIS durch gemeinsame Lernerfahrungen zu verbessern. Der Ausschuss befürwortet den Beschluss der Kommission, in der Richtlinie eine Meldepflicht für NIS-Vorfälle mit beträchtlichen Auswirkungen vorzuschreiben. Seines Erachtens würde eine auf Freiwilligkeit beruhende Meldungsregelung nicht funktionieren, da die Versuchung zu groß wäre, NIS-Versagen zu vertuschen, um Rufschädigung und Haftungsansprüche zu vermeiden.

4.6 In Artikel 14 der vorgeschlagenen Richtlinie jedoch, in dem die Meldung von Sicherheitsvorfällen festgelegt wird, fehlt eine Definition von „Sicherheitsvorfälle[n] (…) die erhebliche Auswirkungen auf die Sicherheit (…) haben", und den betreffenden Einrichtungen und den Mitgliedstaaten wird ein zu großer Ermessensspielraum hinsichtlich der Meldung von NIS-Vorfällen eingeräumt. Wirksame Rechtsvorschriften setzen eindeutige Anforderungen voraus. Da wesentliche Anforderungen in der Richtlinie zu unscharf formuliert werden, können die betroffenen Parteien auch nicht für Verstöße gegen die Richtlinie, wie in Artikel 17 vorgesehen, zur Verantwortung gezogen werden.

4.7 Da NIS-Leistungen großteils vom privaten Sektor bereitgestellt werden, muss ein hohes Maß an Zuverlässigkeit und Zusammenarbeit aller für kritische Informationsinfrastrukturen und -dienste zuständigen Unternehmen gefördert werden. Die von der Europäischen Kommission 2009 auf den Weg gebrachte europäische öffentlich-private Partnerschaft für Robustheit (EP3R) ist zu befürworten und sollte unterstützt werden. Nach Meinung des Ausschusses muss diese Initiative jedoch durch eine rechtliche Verpflichtungen in der NIS-Richtlinie untermauert werden, um wichtige Interessenträger, die ihre Verantwortung nicht wahrnehmen, zur Zusammenarbeit zu verpflichten.

4.8 Jeder Mitgliedstaat sollte ein Online-Verzeichnis all derjenigen Einrichtungen veröffentlichen, die in seine Zuständigkeit fallen und für die die Sicherheitsanforderungen und Meldepflichten gemäß Artikel 14 der vorgeschlagenen Richtlinie gelten. Dies würde zum einen Klarheit darüber schaffen, wie die einzelnen Mitgliedstaaten die Begriffsbestimmungen in Artikel 3 auslegen, und zum anderen könnte durch die damit erreichte Transparenz bei den Bürgern ein Klima des Vertrauens geschaffen und eine Risikomanagementkultur gefördert werden.

4.9 Der Ausschuss nimmt zur Kenntnis, dass Softwareentwickler und Hardwarehersteller keine Anbieter von Diensten der Informationsgesellschaft und deshalb von den Richtlinienanforderungen ausgenommen sind. In dem vorgeschlagenen Rechtsakt sollte klargestellt werden, dass Einrichtungen, die im Rahmen der Richtlinie Verpflichtungen unterliegen, die Software- und Hardware-Anbieter für Mängel ihrer Produkte oder Dienste, die unmittelbar zu NIS-Vorfällen beitragen, haftbar machen würden.

4.10 Die Kommission veranschlagt die für den öffentlichen und privaten Sektor in Europa entstehenden Kosten für die Umsetzung der vorgeschlagenen NIS-Richtlinie auf ca. 2 Mrd. EUR jährlich; indes stellt der Ausschuss fest, dass es für einige Mitgliedstaaten aufgrund finanzieller Schwierigkeiten problematisch sein wird, die für die Einhaltung der Richtlinienvorschriften erforderlichen Investitionen zu tätigen. Es muss geprüft werden, inwieweit im Rahmen des mehrjährigen Finanzrahmens über verschiedene Instrumente, bspw. den Europäischen Fonds für regionale Entwicklung (EFRE) und womöglich den Fonds für die innere Sicherheit, Mittel für NIS-Compliance bereitgestellt werden könnten.

Brüssel, den 22. Mai 2013

Der Präsident
des Europäischen Wirtschafts- und Sozialausschusses
Henri MALOSSE