Rat der
Europäischen Union

Brüssel, den 31. Mai 2016
(OR. en)

9690/16

Interinstitutionelles Dossier:
2013/0027 (COD)

TELECOM 107
DATAPROTECT 58
CYBER 61
MI 401
CSC 166
CODEC 789

ÜBERMITTLUNGSVERMERK

Absender:	Herr Jordi AYET PUIGARNAU, Direktor, im Auftrag des Generalsekretärs der Europäischen Kommission
Eingangsdatum:	30. Mai 2016
Empfänger:	Herr Jeppe TRANHOLM-MIKKELSEN, Generalsekretär des Rates der Europäischen Union
Nr. Komm.dok.:	COM(2016) 363 final
Betr.:	MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT gemäß Artikel 294 Absatz 6 des Vertrags über die Arbeitsweise der Europäischen Union betreffend den Standpunkt des Rates im Hinblick auf den Erlass einer Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Niveaus der Sicherheit von Netz- und Informationssystemen in der Union

Die Delegationen erhalten in der Anlage das Dokument COM(2016) 363 final.

Anl.: COM(2016) 363 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 30.5.2016
COM(2016) 363 final

2013/0027 (COD)

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT

gemäß Artikel 294 Absatz 6 des Vertrags über die Arbeitsweise der Europäischen Union

betreffend den

Standpunkt des Rates im Hinblick auf den Erlass einer Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Niveaus der Sicherheit von Netz- und Informationssystemen in der Union

(Text von Bedeutung für den EWR)

2013/0027 (COD)

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT

gemäß Artikel 294 Absatz 6 des Vertrags über die Arbeitsweise der Europäischen Union

betreffend den

Standpunkt des Rates im Hinblick auf den Erlass einer Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Niveaus der Sicherheit von Netz- und Informationssystemen in der Union

(Text von Bedeutung für den EWR)

1. HINTERGRUND

Übermittlung des Vorschlags an das Europäische Parlament und den Rat (COM(2013) 48 – 2013/0027/COD):	7.2.2013
Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses:	22.5.2013
Standpunkt des Europäischen Parlaments in erster Lesung:	13.3.2014
Festlegung des Standpunkts des Rates:	17.5.2016

2. GEGENSTAND DES VORSCHLAGS DER KOMMISSION

Erstens sieht der Vorschlag für alle Mitgliedstaaten die Verpflichtung vor, ein Mindestniveau nationaler Kapazitäten zu schaffen, indem sie:

- zuständige nationale Behörden für die Sicherheit von Netz- und Informationssystemen (NIS) einrichten;
- IT-Noteinsatzteams (CSIRTs) einrichten;
- nationale NIS-Strategien und nationale NIS-Kooperationspläne aufstellen.

Zweitens sollten die zuständigen nationalen Behörden in einem Netz zusammenarbeiten, das eine sichere und wirksame Koordinierung ermöglicht, wozu auch ein koordinierter Informationsaustausch sowie eine Erkennungs- und Reaktionsfähigkeit auf EU-Ebene gehören. Über dieses Netz sollten die Mitgliedstaaten Informationen austauschen und zusammenarbeiten, um NIS-Bedrohungen und NIS-Vorfällen auf der Grundlage eines europäischen NIS-Kooperationsplans zu begegnen. Damit alle betreffenden Behörden gebührend und rechtzeitig einbezogen werden, sieht der Vorschlag außerdem vor, dass den Strafverfolgungsbehörden Sicherheitsvorfälle mit kriminellem Hintergrund gemeldet werden müssen und dass Europol in den EU-weiten Koordinierungsmechanismus eingebunden wird.

Drittens soll der Vorschlag nach dem Muster der Rahmenrichtlinie für die elektronische Kommunikation dafür sorgen, dass sich eine Kultur des Risikomanagements entwickelt und dass ein Informationsaustausch zwischen privatem und öffentlichem Sektor stattfindet. Unternehmen in besonders betroffenen Sektoren und öffentliche Verwaltungen sollen verpflichtet werden, die Risiken, denen sie unterliegen, zu bewerten und geeignete und angemessene Maßnahmen zur Gewährleistung der NIS zu ergreifen. Sie werden verpflichtet sein, den zuständigen Behörden alle Sicherheitsvorfälle zu melden, welche ihre Netze und Informationssysteme wie auch die Kontinuität kritischer Dienste und die Lieferung von Waren ernsthaft beeinträchtigen.

3. BEMERKUNGEN ZUM STANDPUNKT DES RATES

Insgesamt unterstützt der Standpunkt des Rates die Kernziele des Kommissionsvorschlags, nämlich die Sicherung eines hohen gemeinsamen Niveaus der Sicherheit von Netz- und Informationssystemen. Der Rat nimmt jedoch eine Reihe von Änderungen in Bezug darauf vor, wie dieses Ziel erreicht werden soll.

Nationale Cybersicherheitskapazitäten

Nach dem Standpunkt des Rates werden die Mitgliedstaaten verpflichtet sein, eine nationale NIS-Strategie festzulegen, in der die strategischen Ziele und angemessene Politik- und Regulierungsmaßnahmen für die Cybersicherheit bestimmt werden. Sie werden ferner eine für die Anwendung und Durchsetzung der Richtlinie zuständige nationale Behörde und Noteinsatzteams für IT-Sicherheitsvorfälle benennen müssen.

Wenngleich die Mitgliedstaaten dem Standpunkt des Rates zufolge nicht verpflichtet sein sollen, einen nationalen NIS-Kooperationsplan aufzustellen, wie im ursprünglichen Vorschlag vorgesehen, kann der Standpunkt dennoch unterstützt werden, da einige Aspekte des Kooperationsplans in die Bestimmung über die NIS-Strategie übernommen werden.

Zusammenarbeit zwischen den Mitgliedstaaten

Dem Standpunkt des Rates zufolge soll durch die Richtlinie eine „Kooperationsgruppe“ aus Vertretern der Mitgliedstaaten, der Kommission und der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) eingesetzt werden, um die strategische Zusammenarbeit und den Informationsaustausch zwischen den Mitgliedstaaten zu unterstützen und zu erleichtern. Außerdem wird durch die Richtlinie ein Netz der IT-Noteinsatzteams (das sog. CSIRTs-Netz) eingerichtet, um eine schnelle und wirksame operative Zusammenarbeit bei konkreten Cybersicherheitvorfällen und den Austausch von Informationen über Risiken zu fördern.

Obwohl der Standpunkt des Rates wesentlich von dem im ursprünglichen Vorschlag verfolgten Ansatz abweicht, kann er dennoch unterstützt werden, da er dem übergeordneten Ziel der Verbesserung der Zusammenarbeit zwischen den Mitgliedstaaten dient.

Sicherheitsanforderungen und Meldepflichten für die Betreiber wesentlicher Dienste

Dem Standpunkt des Rates zufolge werden „Betreiber wesentlicher Dienste“ (was „Betreibern kritischer Infrastrukturen“ im ursprünglichen Vorschlag entspricht) verpflichtet sein, geeignete Sicherheitsmaßnahmen zu treffen und den zuständigen nationalen Behörden relevante Sicherheitsvorfälle zu melden. Die Einführung einer Verpflichtung der zuständigen

nationalen Behörden, den Strafverfolgungsbehörden Sicherheitsvorfälle mit kriminellem Hintergrund zu melden, wurde vom Rat jedoch nicht unterstützt.

Wie der ursprüngliche Vorschlag erfasst auch der Standpunkt des Rates Betreiber in den Bereichen Energie-, Verkehrs-, Banken- und Finanzmarktinfrastrukturen und im Gesundheitswesen. Der Standpunkt des Rates bezieht außerdem noch die Bereiche Wasserversorgung und digitale Infrastrukturen mit ein.

Die Mitgliedstaaten werden verpflichtet sein, diese Betreiber anhand bestimmter Kriterien zu ermitteln, wie z. B. der Frage, ob der Dienst für die Aufrechterhaltung grundlegender gesellschaftlicher oder wirtschaftlicher Tätigkeiten unerlässlich ist. Dieses Verfahren der Ermittlung war zwar im ursprünglichen Vorschlag nicht vorgesehen, kann aber akzeptiert werden, da die Mitgliedstaaten verpflichtet sein werden, der Kommission die Informationen zu übermitteln, die sie benötigt um zu prüfen, ob die Mitgliedstaaten einen einheitlichen Ansatz im Hinblick auf die Ermittlung der Betreiber wesentlicher Dienste verfolgen.

Öffentliche Verwaltungen als solche werden vom Standpunkt des Rates nicht mit einbezogen. Sollten diese jedoch die in Artikel 5 festgelegten Kriterien erfüllen, werden auch sie von den Mitgliedstaaten als Betreiber wesentlicher Dienste zu benennen sein, denn sowohl öffentliche als auch private Einrichtungen können Betreiber wesentlicher Dienste sein.

Sicherheitsanforderungen und Meldepflichten für die Anbieter digitaler Dienste

Dem Standpunkt des Rates zufolge werden die Mitgliedstaaten dafür zu sorgen haben, dass Anbieter digitaler Dienste geeignete Sicherheitsmaßnahmen treffen und den zuständigen nationalen Behörden relevante Sicherheitsvorfälle melden. Der Standpunkt des Rates erfasst Online-Marktplätze (was „Plattformen für den elektronischen Geschäftsverkehr“ im ursprünglichen Vorschlag entspricht), Cloud-Computing-Dienste und Suchmaschinen. Im Vergleich zum ursprünglichen Vorschlag erfasst der Standpunkt des Rates keine

- Internet-Zahlungs-Gateways – diese werden nun von der überarbeiteten Zahlungsdiensterichtlinie erfasst;
- *Application Stores* – diese sind als eine Art Online-Marktplatz einzuordnen;
- sozialen Netze – entsprechend der zwischen dem Europäischen Parlament und dem Rat erzielten politischen Einigung.

Dem Standpunkt des Rates zufolge werden der Kommission Durchführungsbefugnisse für die Festlegung der für das Funktionieren der Kooperationsgruppe erforderlichen Verfahrensmodalitäten sowie für die genauere Bestimmung gewisser Elemente in Bezug auf Anbieter digitaler Dienste, einschließlich der Formate und Verfahren der für diese Anbieter geltenden Meldepflichten, übertragen.

Die Kommission unterstützt dieses Ergebnis.

Infolge der informellen Dreiergespräche am 14. Oktober 2014, 11. November 2014, 30. April 2015, 29. Juni 2015, 17. November 2015 und 7. Dezember 2015 haben das Parlament und der Rat eine vorläufige politische Einigung über den Text erzielt.

Diese politische Einigung wurde vom Rat am 18. Dezember 2015 bestätigt. Am 17. Mai 2016 legte der Rat seinen Standpunkt in erster Lesung fest.

4. SCHLUSSFOLGERUNG

Die Kommission unterstützt die Ergebnisse der Verhandlungen zwischen den Organen und akzeptiert daher den vom Rat in erster Lesung festgelegten Standpunkt.