Rat der
Europäischen Union

Brüssel, den 21. April 2016
(OR. en)

5581/16
ADD 1

Interinstitutionelles Dossier:
2013/0027 (COD)

TELECOM 7
DATAPROTECT 6
CYBER 4
MI 37
CSC 15
CODEC 84

ENTWURF DER BEGRÜNDUNG DES RATES

Betr.:	Standpunkt des Rates in erster Lesung im Hinblick auf den Erlass der RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union – Entwurf der Begründung des Rates

I. EINLEITUNG

1. Am 12. Februar 2013 hat die Kommission ihren Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über *Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union* (im Folgenden "NIS-Richtlinie") mit Artikel 114 AEUV als Rechtsgrundlage übermittelt.

2. Der Europäische Wirtschafts- und Sozialausschuss hat seine Stellungnahme am 22. Mai 2013 abgegeben, der Ausschuss der Regionen hat am 3./4. Juli 2013 Stellung genommen.

3. Das Europäische Parlament hat am 13. März 2014 im Rahmen seiner legislativen Entschließung seinen Standpunkt in erster Lesung festgelegt[1] und dabei 138 Abänderungen angenommen.

4. Der Rat und das Europäische Parlament haben im Oktober 2014 Verhandlungen aufgenommen, um eine frühzeitige Einigung in zweiter Lesung zu erzielen. Die Verhandlungen wurden am 7. Dezember 2015 mit einer vorläufigen Einigung zwischen Europäischem Parlament und Rat über einen Kompromisstext erfolgreich abgeschlossen.

5. Am 18. Dezember 2015 hat der Ausschuss der Ständigen Vertreter den Kompromisstext der Richtlinie in der von den beiden Organen vereinbarten Fassung bestätigt.

6. Am 28. Januar 2016 hat die Vorsitzende des Ausschusses für Industrie, Forschung und Energie (IMCO) des Europäischen Parlaments dem Vorsitz des Ausschusses der Ständigen Vertreter in einem Schreiben mitgeteilt, dass sie – sollte der Rat dem Europäischen Parlament seinen Standpunkt in der vereinbarten Fassung vorbehaltlich der Überarbeitung durch die Rechts- und Sprachsachverständigen förmlich übermitteln – dem Plenum empfehlen würde, den Standpunkt des Rates ohne Abänderungen in zweiter Lesung des Parlaments zu billigen.

7. Am 29. Februar 2016 hat der Rat seine politische Einigung über den Kompromisstext der Richtlinie bestätigt.

---

[1] 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 (NIS) in der Union.

II. ZIEL

8. Aus dem Verhandlungsergebnis geht hervor, dass in der Richtlinie Maßnahmen festgelegt werden, mit denen ein hohes gemeinsames Sicherheitsniveau von Netzen und Informationssystemen in der Europäischen Union erreicht werden soll, um so das Funktionieren des Binnenmarkts zu verbessern.

III. ANALYSE DES STANDPUNKTS DES RATES IN ERSTER LESUNG

A. Allgemeines

9. Im Anschluss an die Abstimmung im Plenum haben das Europäische Parlament und der Rat Verhandlungen geführt, um in zweiter Lesung auf der Grundlage eines Standpunkts des Rates in erster Lesung, den das Parlament unverändert billigen könnte, eine Einigung zu erreichen. Der Wortlaut des Standpunkts des Rates in erster Lesung spiegelt den zwischen den Gesetzgebern erzielten Kompromiss voll und ganz wider.

B. Grundlegende Erwägungen

10. Die wichtigsten Bestandteile des mit dem Europäischen Parlament erzielten Kompromisses sind im Folgenden beschrieben:

a. *Nationale Fähigkeiten*

11. Gemäß dem Kompromiss haben die Mitgliedsstaaten bestimmte Verpflichtungen hinsichtlich ihrer nationalen Fähigkeiten im Bereich der Cybersicherheit. Zunächst müssen die Mitgliedsstaaten eine nationale Strategie festlegen, in der die strategischen Ziele und geeignete Politik- und Regulierungsmaßnahmen bestimmt werden, mit denen ein hohes Sicherheitsniveau von Netzen und Informationssystemen erreicht werden kann.

12. Zweitens sollen die Mitgliedsstaaten eine oder mehrere für die Sicherheit von Netzen und Informationssystemen zuständige nationale Behörden benennen, um die Umsetzung der Richtlinie auf nationaler Ebene zu überwachen.

13. Drittens müssen die Mitgliedstaaten auch eine nationale zentrale Anlaufstelle für die Sicherheit von Netzen und Informationssystemen benennen, die als Verbindungsstelle zur Gewährleistung der Zusammenarbeit der Behörden der Mitgliedstaaten untereinander und der grenzüberschreitenden Zusammenarbeit mit den entsprechenden Behörden in anderen Mitgliedsaaten sowie mit der Kooperationsgruppe und dem Netz von CSIRT (Computer Security Incident Response Teams - Computer-Notfallteams) dienen soll. Die zentrale Anlaufstelle wird der Kooperationsgruppe auch einen jährlichen Bericht über die eingegangenen Meldungen vorlegen.

14. Schließlich sollen die Mitgliedsstaaten ein oder mehrere Computer-Notfallteams (im Folgenden "CSIRT") benennen, die für die Bewältigung von Sicherheitsvorfällen und Sicherheitsrisiken zuständig sind. In Anhang I des Kompromisstextes sind die Anforderungen an die CSIRT sowie deren Aufgaben enthalten.

b. *Zusammenarbeit*

15. Zur Unterstützung und Erleichterung der strategischen Zusammenarbeit zwischen den Mitgliedstaaten, zur Vertrauensbildung und im Hinblick auf ein hohes gemeinsames Sicherheitsniveau von Netzen und Informationssystemen in der Union wird mit dem Kompromisstext eine Kooperationsgruppe eingesetzt. Die Gruppe wird aus Vertretern der Mitgliedsstaaten, der Kommission und der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) bestehen und spezifische Aufgaben haben, die im Text aufgelistet werden, z.B. Austausch bewährter Verfahren und Informationen über bestimmte Aspekte oder Beratung über Fähigkeiten und die Abwehrbereitschaft der Mitgliedsstaaten.

16. Außerdem wird mit dem Kompromiss ein Netz der nationalen CSIRT errichtet, um zur Vertrauensbildung zwischen den Mitgliedstaaten beizutragen und eine rasche und wirksame operative Zusammenarbeit zu fördern. Das Netz wird sich aus Vertretern der CSIRT der Mitgliedstaaten und des CERT-EU zusammensetzen und die Kommission wird als Beobachter am CSIRT-Netz teilnehmen. Die ENISA führt die Sekretariatsgeschäfte und unterstützt aktiv die Zusammenarbeit zwischen den CSIRT. Im Text werden eine Reihe von Aufgaben genannt, die vom Netz erfüllt werden sollen, so z.B. der Informationsaustausch zu den Diensten, Tätigkeiten und Kooperationsfähigkeiten der CSIRT, die Unterstützung der Mitgliedstaaten bei der Bewältigung grenzüberschreitender Sicherheitsvorfälle oder – unter bestimmten Voraussetzungen – der Austausch sowie die Erörterung von Informationen im Zusammenhang mit Sicherheitsvorfällen und damit verbundenen Sicherheitsrisiken.

c. *Sicherheits- und Meldeanforderungen*

17. Die Richtlinie legt bestimmte Verpflichtungen für zwei Arten von Marktteilnehmern, nämlich die Betreiber wesentlicher Dienste und die Anbieter digitaler Dienste, fest.

18. In Anhang II der Richtlinie werden eine Reihe von Sektoren aufgelistet, die für Gesellschaft und Wirtschaft von Bedeutung sind, nämlich Energie, Transport, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserlieferung und -versorgung sowie digitale Infrastruktur. Anhand eindeutiger, in der Richtlinie festgelegter Kriterien sollen die Mitgliedstaaten ermitteln, welche Betreiber in diesen Sektoren wesentliche Dienste erbringen.

19. In Anhang III der Richtlinie sind drei Arten digitaler Dienste aufgelistet, deren Anbieter die Anforderungen der Richtlinie erfüllen müssen: Online-Marktplätze, Online-Suchmaschinen und Cloud-Computing-Dienste. Alle Anbieter der aufgelisteten digitalen Dienste, ausgenommen Klein- und Kleinstunternehmen, müssen die Anforderungen der Richtlinie erfüllen.

20. Beide Arten von Marktteilnehmern müssen organisatorische und technische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netze und Informationssysteme zu managen und den Auswirkungen von Sicherheitsvorfällen, die die Sicherheit dieser Systeme beeinträchtigen, vorzubeugen bzw. diese so gering wie möglich zu halten. Sicherheitsvorfälle, die sich in bestimmtem Maße auf die betreffenden Dienste auswirken, müssen außerdem den zuständigen nationalen Behörden oder den CSIRT gemeldet werden. In der Richtlinie sind die Kriterien enthalten, anhand derer bestimmt wird, in welchem Maße sich derartige Sicherheitsvorfälle auswirken.

21. In der Richtlinie wurde ein differenzierter Ansatz im Hinblick auf die zwei Kategorien von Marktteilnehmern gewählt. Die Sicherheitsanforderungen und Meldepflichten sind für Anbieter digitaler Dienste geringer als für Betreiber wesentlicher Dienste, womit das Ausmaß des Risikos, das eine Störung ihrer Dienste für Gesellschaft und Wirtschaft hat, zum Ausdruck gebracht werden soll. Unter Berücksichtigung der Tatsache, dass Anbieter digitaler Dienste häufig in mehreren Mitgliedstaaten aktiv sind und zur Sicherstellung eines hohen Maßes an Harmonisierung wird es den Mitgliedsstaaten in der Richtlinie untersagt, diesen Anbietern weitere Sicherheitsanforderungen und Meldepflichten aufzuerlegen.

22. Im Kompromisstext wird außerdem besagt, dass Einrichtungen, die weder als Betreiber wesentlicher Dienste ermittelt wurden noch Anbieter digitaler Dienste sind, bestimmte Sicherheitsvorfälle auf freiwilliger Basis melden können.

d. *Umsetzung*

23. Die Mitgliedsstaaten müssen diese Richtlinie spätestens 21 Monate nach ihrem Inkrafttreten umsetzen und haben weitere 6 Monate Zeit, um die Betreiber wesentlicher Dienste zu ermitteln.

IV. FAZIT

24. Der Standpunkt des Rates spiegelt den im Rahmen der Verhandlungen zwischen dem Europäischen Parlament und dem Rat mit Einverständnis der Kommission erzielten Kompromiss voll und ganz wider. Der Kompromiss wird mit dem Schreiben des Vorsitzenden des IMCO-Ausschusses vom 28. Januar 2016 an den Präsidenten des Ausschusses der Ständigen Vertreter bestätigt.