RAT DER EUROPÄISCHEN UNION

Brüssel, den 22. November 2013

16630/13

Interinstitutionelles Dossier: 2013/0027 (COD)

TELECOM 322
DATAPROTECT 178
CYBER 33
MI 1064
CODEC 2676

VERMERK

des	Vorsitzes
für die	Delegationen
Nr. Komm.dok.:	6342/13 TELECOM 24 DATAPROTECT 14 CYBER 2 MI 104 CODEC 313 + ADD1 +ADD2
Nr. Vordok.:	16333/13 TELECOM 313 DATAPROTECT 170 CYBER 30 MI 1039 CODEC 2717
Betr.:	Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union – *Fortschrittsbericht*

Dieser Bericht wurde unter der Verantwortung des litauischen Vorsitzes erstellt. In dem Bericht wird dargelegt, welche Arbeit in den Vorbereitungsgremien des Rates bereits geleistet worden ist und wie weit die Beratungen über den eingangs genannten Vorschlag gediehen sind.

VERFAHRENSTECHNISCHE ASPEKTE

1. Am 12. Februar 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*[1] (im Folgenden "NIS-Richtlinie"), die Artikel 114 AEUV als Rechtsgrundlage hat, übermittelt. Der Vorschlag ist Bestandteil der "Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum"[2], zu der der Rat am 25. Juni 2013 Schlussfolgerungen[3] angenommen hat. Der Rat "Verkehr, Telekommunikation und Energie" hat am 6. Juni 2013 die Fortschritte zur Kenntnis genommen, die bei der Prüfung des Vorschlags für eine NIS-Richtlinie erzielt worden sind.[4]

2. Der Europäische Wirtschafts- und Sozialausschuss[5] und der Ausschuss der Regionen[6] haben am 22. Mai bzw. 3./4. Juli zu dem Vorschlag Stellung genommen. Im Europäischen Parlament ist der Ausschuss für Binnenmarkt (IMCO) federführend, und die Ausschüsse für Industrie (ITRE) und bürgerliche Freiheiten (LIBE) fungieren als assoziierte Ausschüsse. Was die Zeitplanung anbelangt, so wird voraussichtlich der LIBE-Ausschuss im November und der ITRE-Ausschuss im Dezember eine Abstimmung durchführen und der IMCO-Ausschuss beabsichtigt, in seiner Sitzung am 22./23. Januar 2014 einen Bericht und eine Reihe von Änderungsanträgen anzunehmen.

3. Während des litauischen Vorsitzes hat die Gruppe "Telekommunikation und Informationsgesellschaft" (WP TELE) den Vorschlag in fünf Sitzungen[7] erörtert. Da viele Delegationen lediglich erste Überlegungen äußern konnten und zu dem Text oder zu Teilen des Textes Prüfungsvorbehalte haben, war es dem litauischen Vorsitz nicht möglich, diesem Fortschrittsbericht eine überarbeitete Fassung des Textes beizufügen. Dennoch haben die Delegationen bei den Beratungen eine Reihe von Schlüsselfragen und Anliegen zur Sprache gebracht, die im Folgenden dargelegt werden und bei der Überarbeitung des Wortlauts des Vorschlags zu berücksichtigen sind.

---

1 Dok. 6342/13.
2 Dok. 6225/13.
3 Dok. 11357/13.
4 Dok. 10076/13 und 10457/13.
5 TEN/513.
6 2013/C 280/05.
7 Am 18.7., 26.9., 8.10, 5.11 und 19.11.2013.

SACHFRAGEN

4. Eine allgemeine Beschreibung der wichtigsten Aspekte der vorgeschlagenen NIS-Richtlinie ist im Fortschrittsbericht für die Juni-Tagung des Rates "Verkehr, Telekommunikation und Energie"[8] enthalten. Alle Delegationen sind sich zwar voll und ganz bewusst, dass Maßnahmen gegen NIS-Vorfälle und Cyberangriffe erforderlich sind, aber es bestehen unterschiedliche Auffassungen darüber, wie die Netzsicherheit in der gesamten Union am besten gewährleistet werden kann. Bei der Prüfung der einzelnen Artikel haben einige Delegationen erklärt, dass sie eine flexible Vorgehensweise bevorzugen würden, bei der EU-weit bindende Vorschriften nur für kritische Infrastrukturen und grundlegende Anforderungen, die durch fakultative und freiwillige Maßnahmen zu ergänzen wären, gelten würden, während andere Delegationen und die Kommission der Auffassung waren, dass das in der Union erforderliche Sicherheitsniveau nur mit rechtlich bindenden Maßnahmen erreicht werden kann. Aufgrund dieser unterschiedlichen Konzepte werden die konträren Standpunkte verständlich, die zu den einzelnen Bestimmungen des Vorschlags eingenommen wurden und im Folgenden erläutert werden.

5. *NIS-Strategie und die für NIS zuständige Stelle*: Im Hinblick auf das Ziel, über eine Mindestkapazität zu verfügen, um bei Sicherheitsrisiken und -vorfällen, die Netze und Informationssysteme beeinträchtigen, Prävention, Bewältigung und Reaktion zu gewährleisten, sollen die Mitgliedstaaten nationale NIS-Strategien annehmen, die für NIS zuständigen nationalen Stellen benennen und IT-Notfallteams für NIS aufstellen.

   Den Delegationen ist bewusst, dass eine schwere Störung in einem Mitgliedstaat auch andere Mitgliedstaaten in Mitleidenschaft ziehen kann, weshalb sie einer nationalen Koordinierungsstelle grundsätzlich zustimmen könnten. Allerdings scheinen insbesondere diejenigen Mitgliedstaaten, die bereits NIS-Strategien angenommen, zuständige Stellen benannt und ein nationales IT-Notfallteam aufgestellt haben, Kapitel II des Vorschlags, das den *nationalen Rahmen für die Netz- und Informationssicherheit* betrifft, kritisch zu bewerten: Sie möchten sicherstellen, dass die von den Mitgliedstaaten zu erfüllenden Anforderungen mit den derzeitigen nationalen Gepflogenheiten vereinbar sind und nicht darüber hinausgehen. Nach Auffassung einiger Delegationen sollte es sich bei der zuständigen Stelle lediglich um eine Kontaktstelle handeln, die Aufgaben an die nationalen Regulierungsbehörden delegiert, da diese über die erforderlichen sektorspezifischen Fachkenntnisse verfügen. Dies würde auch sicherstellen, dass die vorgeschriebenen Anforderungen mit den nationalen Sicherheitsbestimmungen im Einklang stehen. Einige Delegationen betonen, dass mehr vertrauensbildende Maßnahmen notwendig sind und der Schwerpunkt weniger auf administrativen und bürokratischen Regelungen liegen sollte.

---

[8] Dok. 10076/13.

Andere Delegationen wünschen sich näheren Aufschluss über die in diesem Kapitel verwendete Terminologie, etwa über die Begriffe "Risiken" und "Bedrohungen", würden gerne wissen, welche genauen Anforderungen bestehen, und fragen sich, ob diese Anforderungen nur den privaten Sektor oder auch den öffentlichen Sektor betreffen sollten. Im Zusammenhang mit der zuständigen Behörde und ihrer Aufgabenbeschreibung müssen noch zahlreiche Punkte geklärt werden, so die Fragen, ob diese Behörde operative Aufgaben wahrnehmen soll, was viele Mitgliedstaaten ablehnen, und wie die Aufteilung der Zuständigkeiten mit den nationalen IT-Notfallteams aussehen soll.

6. *Risikomanagement und Meldung von Sicherheitsvorfällen:* Marktteilnehmer und öffentliche Verwaltungen sollten die Risiken für ihre Informationssysteme angemessen bewerten, geeignete Maßnahmen ergreifen, um Sicherheitsvorfälle zu vermeiden oder zu bewältigen, und alle gravierenden Sicherheitsvorfälle melden, die erhebliche Auswirkungen auf die den zuständigen Behörden bereitgestellten Kerndienste haben.

   Bei Kapitel IV des Vorschlags über die *Sicherheit der Netze und Informationssysteme der öffentlichen Verwaltungen und der Marktteilnehmer* fragen sich mehrere Delegationen, ob sich der Vorschlag neben den "Betreibern kritischer Infrastrukturen" auch auf "Anbieter von Diensten der Informationsgesellschaft" erstrecken soll. Diese Bedenken in Bezug auf den Geltungsbereich hängen eng zusammen mit der Definition des Begriffs "Marktteilnehmer" in Kapitel I und mit der nicht erschöpfenden Liste in Anhang II. Viele Delegationen fordern eine genauere Definition und mehr Flexibilität für die Mitgliedstaaten, wenn es darum geht, zu bestimmen, welche Sektoren zu den nationalen kritischen Infrastrukturen zählen. Einige Delegationen möchten, dass die vorgeschlagenen Anforderungen nur für den privaten Sektor gelten, während andere wiederum dafür sind, dass die Meldung von Sicherheitsverletzungen entsprechend den derzeitigen nationalen Gepflogenheiten freiwillig sein sollte. Auch wurde die Frage aufgeworfen, warum Hardware-/Software-Hersteller und Kleinstunternehmen nicht einbezogen werden; zudem haben die Mitgliedstaaten Bedenken hinsichtlich der Vereinbarkeit der vorgeschlagenen Pflicht zur Meldung von Sicherheitsverletzungen mit den Anforderungen in anderen Rechtsvorschriften der Union wie dem Rechtsrahmen für die elektronische Kommunikation, weil die Anforderungen gemäß dem Vorschlag nicht für Betreiber von elektronischen Kommunikationsnetzen oder -diensten oder Vertrauensdiensteanbieter gelten. Allgemein fragen sich viele Delegationen, ob und wie die Mitgliedstaaten konkret "gewährleisten" können, dass die Akteure ihre Netze sichern und Sicherheitsvorfälle melden; in diesem Zusammenhang wurde auch vorgebracht, dass geklärt werden muss, ob Artikel 114 AEUV als Rechtsgrundlage angemessen ist. Darüber hinaus bestehen Bedenken hinsichtlich der Auswirkungen der Meldungen auf den Schutz der Privatsphäre oder der Vertraulichkeit von Informationen.

7. *Kooperationsnetz*: Um koordinierte Reaktionen auf Sicherheitsvorfälle sicherzustellen, sollte erforderlichenfalls ein Kooperationsnetz zu NIS-Risiken und -vorfällen eingerichtet werden, um eine ständige Kommunikation zwischen der Kommission und den 28 zuständigen Behörden zu ermöglichen.

   Kapitel III über die *Zusammenarbeit zwischen den zuständigen Behörden* bedarf einer weiteren Prüfung. Die Aufgaben des Kooperationsnetzes müssen weiter erörtert werden, obgleich zahlreiche Delegationen der Meinung sind, dass es keine operativen Aufgaben wahrnehmen sollte; einige Delegationen halten es in diesem Zusammenhang für besser, von einem *Mechanismus* anstatt einem *Netz* zu sprechen. Eine Reihe organisatorischer Aspekte bedürfen ebenfalls der weiteren Klärung, so z. B. die Frage, wer im Kooperationsnetz den Vorsitz führen wird, was das Netz kosten würde und wie die Beziehungen und die Aufteilung der Zuständigkeiten im Rahmen der Zusammenarbeit der nationalen IT-Notfallteams mit der ENISA und mit Europol aussehen sollen. Einige Delegationen vertreten die Auffassung, dass der Informationsaustausch im Kooperationsnetz auf Freiwilligkeit beruhen sollte, und bezweifeln, dass das vorgeschlagene "sichere System für den Informationsaustausch" notwendig ist. Der vorgeschlagene Frühwarnmechanismus wirft zahlreiche Fragen auf und sorgt für Bedenken, weil z. B. nicht klar ist, welche Informationen zu welchem Zeitpunkt ausgetauscht werden sollen und welche möglichen Folgen dies in Bezug auf Sicherheitsvorfälle oder Risiken hat. Zudem finden viele Mitgliedstaaten, dass der vorgeschlagene Mechanismus für koordinierte Reaktionen zu weit geht, und fordern einen NIS-Kooperationsrahmen anstatt eines operativen Plans für Reaktionen auf Sicherheitsvorfälle. Wann und unter welchen Bedingungen eine koordinierte Reaktion zu erfolgen hat, muss noch weiter erörtert werden.

8. Zu Kapitel I und V des Vorschlags, d. h. zu den *allgemeinen Bestimmungen* (die während des irischen Vorsitzes geprüft wurden) und den *Schlussbestimmungen*, fand zwar bereits ein erster allgemeiner Gedankenaustausch statt, aber einige Bestimmungen, die u. a. folgende Punkte betreffen, müssen erneut geprüft werden: die Anwendung der vorgeschlagenen Sicherheitsanforderungen in Bezug auf die entsprechenden Anforderungen in der Rahmenrichtlinie (2002/21/EG), die Definitionen der Begriffe "Sicherheitsrisiko", "Sicherheitsvorfall" und "Marktteilnehmer" (in Verbindung mit der *Liste der Marktteilnehmer* in Anhang II), die Durchsetzung (z. B. die Meldung von Sicherheitsvorfällen an die Polizei), die Normierung, die Durchführungsrechtsakte (alle Delegationen sind gegen den Rückgriff auf delegierte Rechtsakte in diesem Arbeitsbereich) und der Umsetzungszeitraum (für die Umsetzung in nationales Recht und für die Vorlage der nationalen NIS-Strategien).

AUSBLICK

9. Bei der Prüfung der einzelnen Artikel des Vorschlags hat sich gezeigt, dass die Delegationen von der Kommission näheren Aufschluss über die vorgeschlagenen Maßnahmen und eine Begründung für die Maßnahmen erhalten möchten, und zwar anhand eines Vergleichs mit der derzeitigen Situation in den Mitgliedstaaten und mit (nationalen und internationalen) Mechanismen der freiwilligen Meldung von Sicherheitsvorfällen und der Kooperation, wie es sie in europäischen und internationalen CERT-Gemeinschaften (beispielsweise in der Gruppe staatlicher europäischer IT-Notfallteams) bereits gibt, wobei diese auch die Mittlerrolle der ENISA einschließen könnten. Bei der weiteren Prüfung des Vorschlags in der WP TELE hat sich gezeigt, dass die größte Herausforderung darin bestehen wird, sich auf ein gemeinsames Konzept zu einigen, bei dem das richtige Gleichgewicht zwischen unionsweit bindenden Vorschriften und fakultativen und freiwilligen Maßnahmen besteht, was insgesamt zu einem ähnlich hohen Niveau der Abwehrbereitschaft der Mitgliedstaaten führen und die EU in die Lage versetzen soll, auf NIS-Herausforderungen wirksam zu reagieren.

10. Die Delegationen können dem Vorsitz zusätzliche Formulierungsvorschläge übermitteln, die bei der weiteren Prüfung des Vorschlags gebührend berücksichtigt werden.

*

* *

Der Vorsitz wird dem Rat diesen Fortschrittsbericht zur Kenntnisnahme vorlegen, nachdem ihn der AStV am 27. November geprüft hat.