Rat der
Europäischen Union

Brüssel, den 15. November 2016
(OR. en)

14540/16

CYBER 130
COMPET 597
IND 245
RECH 320
TELECOM 241

BERATUNGSERGEBNISSE

Absender:	Generalsekretariat des Rates
vom	15. November 2016
Empfänger:	Delegationen
Nr. Vordok.:	13967/1/16 REV 1
Betr.:	Schlussfolgerungen des Rates zur Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit und Förderung einer wettbewerbsfähigen und innovativen Cybersicherheitsbranche – Schlussfolgerungen des Rates (15. November 2016)

Die Delegationen erhalten in der Anlage die Schlussfolgerungen des Rates zur Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit und Förderung einer wettbewerbsfähigen und innovativen Cybersicherheitsbranche, die der Rat (Allgemeine Angelegenheiten) auf seiner 3499. Tagung vom 15./16. November 2016 in Brüssel angenommen hat.

ANLAGE

Schlussfolgerungen des Rates zur Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit und Förderung einer wettbewerbsfähigen und innovativen Cybersicherheitsbranche

DER RAT DER EUROPÄISCHEN UNION –

UNTER HINWEIS AUF

- seine Schlussfolgerungen zur gemeinsamen Mitteilung der Kommission und der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik "Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum"[1];
- den EU-Politikrahmen für die Cyberabwehr[2];
- seine Schlussfolgerungen zur Cyberdiplomatie[3];
- die Mitteilung der Kommission "Strategie für einen digitalen Binnenmarkt für Europa"[4];
- seine Schlussfolgerungen zur Bewältigung hybrider Bedrohungen[5];
- seine Schlussfolgerungen zum eGovernment-Aktionsplan 2016-2020[6];
- die Mitteilung der Kommission über die Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit und Förderung einer wettbewerbsfähigen und innovativen Cybersicherheitsbranche[7];
- seine Schlussfolgerungen zur Globalen Strategie für die Außen- und Sicherheitspolitik der Europäischen Union[8];

---

1 Dok. 12109/13.
2 Dok. 15585/14.
3 Dok. 6122/15.
4 COM(2015) 192 final vom 6. Mai 2015.
5 Dok. 7857/16.
6 Dok.12080/16.
7 COM(2016) 410 final vom 5. Juli 2016.
8 Dok. 13202/16.

IN ANBETRACHT

- der Ergebnisse der hochrangigen Konferenz über Cybersicherheit vom Mai 2016 in Amsterdam;

- der Ergebnisse der globalen Konferenzen über den Cyberraum von 2011 (London), 2012 (Budapest), 2013 (Seoul) und 2015 (Den Haag) –

STELLT FEST, DASS

1. die Mitgliedstaaten, die Kommission und die anderen EU-Institutionen gemäß dem Subsidiaritätsgrundsatz insbesondere seit der Annahme der Cybersicherheitsstrategie der EU eng zusammengearbeitet haben, um die Cybersicherheit und die diesbezügliche Abwehrfähigkeit auf EU- und nationaler Ebene zu steigern, und eine weitere intensive Zusammenarbeit unerlässlich ist, um die EU vor Cyber-Bedrohungen zu schützen und zugleich ein umfassendes und in sich geschlossenes Konzept für die Cybersicherheit beizubehalten;

2. Cyberbedrohungen und Angriffsflächen für Cyberattacken sich weiterentwickeln und zunehmen, weshalb insbesondere zur Bewältigung schwerwiegender grenzüberschreitender Cybervorfälle eine ständige und noch engere Zusammenarbeit erforderlich ist;

3. die Cybersicherheit eine wesentliche Voraussetzung für das reibungslose Funktionieren des digitalen Binnenmarkts ist, da Cybervorfälle nicht nur zu schweren Störungen der modernen Gesellschaft und zu erheblichem wirtschaftlichem Schaden für europäische Unternehmen führen können, sondern als solche auch das Vertrauen der Bürgerinnen und Bürger sowie der Unternehmen in die digitale Gesellschaft erschüttern und eine Zurückhaltung bei der Nutzung digitaler Technologien bewirken können;

4. die kürzlich angenommene NIS-Richtlinie[9] mit ihren neuen Mechanismen für die Zusammenarbeit, die zu gegebener Zeit zu erneuernde Cybersicherheitsstrategie der EU und die demnächst zu überarbeitende ENISA-Verordnung das Herzstück des EU-Rahmens für die Cyber-Abwehrfähigkeit bilden, in dem die Frage der Cybersicherheit der Mitgliedstaaten und der EU-Institutionen wirksam angegangen werden sollte;

5. durch allgemeine und berufliche Bildung vermittelte angemessene Kenntnisse über Cybersicherheit zur Verhinderung von Cybervorfällen und zur Bewältigung und Abmilderung ihrer Folgen zu den wichtigsten Aspekten bei der Verwirklichung der Cyber-Abwehrfähigkeit gehören, wobei zugleich gegebenenfalls die Zusammenarbeit zwischen den Mitgliedstaaten, der Kommission, dem EAD, der ENISA, Europol, Eurojust, der EDA sowie der NATO weiter gefördert werden muss;

6. für die Aufrechterhaltung der Cybersicherheit und die Verhinderung von Cybervorfällen sowie die Abmilderung ihrer Auswirkungen die Zusammenarbeit und der Informationsaustausch in strategischer und operativer Hinsicht ausschlaggebend sind, und zwar sektorenübergreifend in den Mitgliedstaaten und grenzüberschreitend innerhalb der EU. Diese Zusammenarbeit trägt nicht nur zur Erhöhung der Bereitschaft und Abwehrfähigkeit, sondern auch zu einem besseren Verständnis der Interdependenzen bei, z.B. durch die Durchführung des Europäischen Programms für den Schutz kritischer Infrastrukturen;

7. für die Bewertung des Umfangs der gemeinsamen Risiken und der Auswirkungen schwerwiegender Cybervorfällen sowohl im öffentlichen als auch im privaten Sektor der Umfang der grenz- und sektorenüberschreitenden Interdependenz maßgeblich ist;

8. es wichtig ist, angemessene Finanzmittel zur Unterstützung von KMU und Start-up-Unternehmen im Bereich der Cybersicherheit, insbesondere deren Zugang zu Finanzmitteln und Investitionen vor allem in ihrer Aufbauphase, sicherzustellen;

9. die Errichtung einer vertraglichen öffentlich-privaten Partnerschaft für Cybersicherheit im Rahmen von "*Horizont 2020*" einen Mehrwert mit sich bringt, der die Wettbewerbs- und Innovationsfähigkeit der europäischen Cybersicherheitsbranche stimulieren kann;

---

9 Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

10. dynamische technologische Entwicklungen im digitalen Bereich, die in ein breites Spektrum unterschiedlicher IKT-Produkte, -Dienstleistungen und -Lösungen umgesetzt werden und im digitalen Binnenmarkt stärker berücksichtigt und gefördert werden sollten, nicht nur neue gesellschaftliche und wirtschaftliche Herausforderungen, sondern auch neue Herausforderungen für die Sicherheit insbesondere in Bezug auf Daten hervorrufen;

11. der Cyberdiebstahl von Geschäftsgeheimnissen die Innovations- und Wettbewerbsfähigkeit der europäischen Wirtschaft schädigen kann und seine Auswirkungen weiter geprüft werden müssen;

12. die Mitgliedstaaten auch in Bezug auf den Cyberraum das gemeinsame Ziel verfolgen, einen Beitrag zur strategischen Autonomie Europas zu leisten, wie in den Schlussfolgerungen des Rates zur Globalen Strategie für die Außen- und Sicherheitspolitik der Europäischen Union dargelegt;

BETONT, DASS

13. jeder Mitgliedstaat nach wie vor für die erforderlichen Maßnahmen zum Schutz seiner wesentlichen Sicherheitsinteressen unter vollständiger Achtung der Verträge verantwortlich ist;

14. die Mitgliedstaaten vorrangig die NIS-Richtlinie in nationales Recht umsetzen sollten, sodass die Zusammenarbeit in der neu eingesetzten Kooperationsgruppe und dem CSIRT-Netz, die sich positiv auf die Stärkung der Cyber-Abwehrfähigkeit und die Cybersicherheit sowie die Bewältigung schwerwiegender Vorfällen auswirken würde, tatsächlich zum Tragen kommt;

15. die Erhöhung der Netz- und Informationssicherheit der EU-Institutionen als Teil der Priorität für die Verstärkung der Cybersicherheit in der ganzen EU betrachtet werden sollte;

16. zur Verhinderung von Cybervorfällen und zur Begrenzung der damit verbundenen Risiken sowie zur Schaffung von Vertrauen und Zuversicht hinsichtlich des digitalen Binnenmarkts Maßnahmen zum Kapazitätsaufbau für Cyberangelegenheiten und zur Vertrauensbildung erforderlich sind;

17. es des Einsatzes diplomatischer, rechtlicher und technischer Instrumente und einer intensiveren Zusammenarbeit auf EU- und nationaler Ebene bedarf, um erfolgreich auf Cybervorfälle einschließlich Cyberangriffe zu reagieren und die Cyberkriminalität zu bekämpfen;

18. die EU die Konzepte der eingebauten Sicherheit und des eingebauten Datenschutzes in vollem Umfang anwenden muss, um wirksame, hochwertige, erschwingliche und interoperable Cybersicherheitsprodukte und -dienste zu entwickeln, bereitzustellen und einzusetzen, und dass sie auf die Verwirklichung eines stärker integrierten und globalen Marktes für sie hinarbeiten muss;

19. die Förderung des Dialogs mit der Wirtschaft über Cybersicherheit dazu beitragen könnte, Lücken bei den diesbezüglichen Zertifizierungs- und Validierungsverfahren sowie in den einschlägigen Kennzeichnungssystemen zu schließen, bei denen die international anerkannten Standards und Grundsätze eingehalten werden sollten;

20. im Hinblick auf eine effektive Verwirklichung der europäischen Cyberabwehrsysteme die jeweiligen Maßnahmen im Einklang mit den Strategien, Finanzinstrumenten und Programmen der EU stehen müssen;

21. die vertragliche öffentlich-private Partnerschaft für Cybersicherheit neuen Interessenten offen stehen sollten und dass die Bedingungen für die Teilnahme transparent und Informationen über die Bedingungen weiterhin leicht zugänglich sein sollten;

FORDERT DIE KOMMISSION AUF,

22. die in der Mitteilung über die Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit angegebenen Ziele dadurch zu erreichen, dass sie insbesondere

a) in der ersten Jahreshälfte 2017 einen Konzeptentwurf zur Zusammenarbeit bei der Reaktion auf schwerwiegende Cybervorfälle auf EU-Ebene zur Prüfung durch die NIS-Leitungsgremien und andere einschlägige Akteure – insbesondere die ENISA – vorzulegen, wobei der Ergänzungsfunktion des Konzeptentwurfs Rechnung zu tragen ist;

b) die Evaluierung der ENISA bis spätestens Ende 2017 abzuschließen und so bald wie möglich alle für eine Verlängerung des Mandats der ENISA relevanten Aspekte (einschließlich einer Erweiterung der Agentur zur Übernahme der in der NIS-Richtlinie vorgesehenen Aufgaben) vorzulegen;

c) in enger Zusammenarbeit mit den Mitgliedstaaten, dem EAD, Europol, Eurojust, der ENISA, der EDA und anderen einschlägigen EU-Einrichtungen eine Ausbildungsplattform zur Cybersicherheit einzurichten;

d) zu prüfen, welche rechtlichen und organisatorischen Voraussetzungen erfüllt sein müssen, damit die Mitgliedstaaten die öffentlich zugängliche Netzinfrastruktur regelmäßig auf Schwachstellen kontrollieren können;

e) zu prüfen, ob gegebenenfalls ein Cybersicherheitszertifizierungs- und -kennzeichnungssystem geschaffen werden sollte, das jedoch den bereits funktionierenden Sicherheitssystemen Rechnung trägt, und zwar im Hinblick darauf, dass bis 2017 Maßnahmen – auch legislativer Art – zur Bewältigung der betreffenden Herausforderungen vorgeschlagen werden;

f) Cybersicherheitskreise verstärkt auf die bestehenden Finanzierungsmechanismen aufmerksam zu machen und die Inanspruchnahme von EU-Werkzeugen und -Instrumenten zur Unterstützung innovativer KMU zu fördern;

g) Mittel und Wege zur Erleichterung des Zugangs zu Finanzmitteln und Investitionen (etwa durch eine spezielle Investitionsplattform für die Cybersicherheit) für KMU und Start-up-Unternehmen vor allem in ihrer Aufbauphase auszuloten;

h) erforderlichenfalls die derzeitige Funktionsweise der europäischen Informationsaustausch- und -analysezentren (ISAC) zu evaluieren und zusammen mit den Mitgliedstaaten und gegebenenfalls den bestehenden nationalen ISAC auf Vorschläge zur weiteren Stärkung dieser Strukturen hinzuarbeiten;

i) das Konzept der eingebauten Sicherheit bei wichtigen Infrastrukturinvestitionen, die eine digitale Komponente haben und mit EU-Mitteln kofinanziert werden, zu fördern;

23. vor der Schaffung neuer Mechanismen und Strukturen (etwa eines Informationsknotenpunkts oder einer hochrangigen beratenden Gruppe) oder vor der Einführung neuer Instrumente (beispielsweise eines Konzeptentwurfs zur Zusammenarbeit) die Mitgliedstaaten zu konsultieren, und zwar jeweils was die Cybersicherheit, ihre Ergänzungsfunktion, ihre Ziele und ihre jeweiligen Aufgaben anbelangt;

24. dem Rat jährlich schriftlich über die Fortschritte zu berichten;

ERSUCHT DIE MITGLIEDSTAATEN,

25. die Mechanismen für die Zusammenarbeit bei der Cybersicherheit zur vollständigen Einsatzreife zu bringen und die grenzüberschreitende Zusammenarbeit in Bezug auf die Bereitschaft zur Prävention, Bewältigung und/oder Abmilderung der Auswirkungen schwerwiegender Cybervorfälle im Einklang mit den im Rahmen der NIS-Richtlinie vereinbarten Grundsätze und Bestimmungen zu verstärken;

26. sich zwecks Stärkung von Wettbewerbsfähigkeit, Forschungstätigkeit und Innovationsleistung der europäischen Wirtschaft aktiv an der vertraglichen öffentlich-privaten Partnerschaft für Cybersicherheit zu beteiligen;

27. mit der Kommission bei der Schaffung eines offenen europäischen Rahmens zusammenzuarbeiten und dabei im Einklang mit den internationalen Standards und auf der Grundlage der Mitwirkung von Experten der Entwicklung eines globalen Rahmens für die Zertifizierung von Cybersicherheitsprodukten und -diensten, der ein breites Spektrum von IKT-Systemen und -Lösungen jeder Sicherheitsstufe abdecken würde und in allen Mitgliedstaaten anwendbar wäre, Rechnung zu tragen, wobei das Ziel die Schaffung eines echten und sicheren digitalen Binnenmarkts ist, der Europa eine führende Rolle bei der weltweiten Standardisierung verschafft;

28. mit der Kommission und anderen einschlägigen Parteien im Hinblick auf die Verwirklichung der in diesen Schlussfolgerungen dargelegten Ziele zusammenzuarbeiten;

ERSUCHT DIE EINSCHLÄGIGEN AKTEURE,

29. die vorbildlichen Verfahren auf dem Gebiet der Cybersicherheit zu übernehmen, Sensibilisierung und Qualifikationsverbesserungen zu fördern und die Schulung auf dem Gebiet der Cybersicherheit zu verbessern;

30. eine Erhöhung der Investitionen in den Markt qualitativ hochwertiger Cybersicherheits-produkte und -dienste in Betracht zu ziehen, und gegebenenfalls die Zusammenarbeit mit den Behörden – einschließlich der nationalen CERT – zu vertiefen;

31. die vertragliche öffentlich-privaten Partnerschaft für Cybersicherheit und die europäischen ISAC bestmöglich zu nutzen, um die Zusammenarbeit der Branche insbesondere in den Bereichen Forschung und Innovation, Standardisierung, Zertifizierung, Kennzeichnung, gemeinsame Investitionen und Konsolidierung der Branche zu fördern;

32. proaktiv zur Verwirklichung der in diesen Schlussfolgerungen dargelegten Ziele beizutragen, um die Abwehrfähigkeit der europäischen Wirtschaft zu stärken;

33. den Schwerpunkt auf eine verstärkte Übernahme von Cybersicherheitslösungen in allen Sektoren und im gesamten Nutzerspektrum zu legen.