Rat der
Europäischen Union

Brüssel, den 19. Juni 2018
(OR. en)

10085/18

CYBER 138
COPEN 208
COPS 209
COSI 147
DATAPROTECT 127
JAI 636
JAIEX 65
POLMIL 81
TELECOM 187
DAPIX 186

I/A-PUNKT-VERMERK

Absender:	Generalsekretariat des Rates
Empfänger:	Ausschuss der Ständigen Vertreter/Rat
Nr. Vordok.:	9240/4/18
Betr.:	Entwurf von Schlussfolgerungen des Rates zu einer koordinierten Reaktion der EU auf große Cybersicherheitsvorfälle und -krisen

1. In der Sitzung der Horizontalen Gruppe "Fragen des Cyberraums" vom 2. Mai 2018 informierte der Vorsitz die Delegationen über seine Absicht, Schlussfolgerungen des Rates zu dem Thema einer koordinierten Reaktion der EU auf große Cybersicherheitsvorfälle und -krisen auszuarbeiten.

2. In der Sitzung der Horizontalen Gruppe "Fragen des Cyberraums" vom 30. Mai 2018 wurde der Entwurf von Schlussfolgerungen des Rates zu einer koordinierten Reaktion der EU auf große Cybersicherheitsvorfälle und -krisen von den Delegationen geprüft[1].

3. Im Anschluss an die Sitzung und auf der Grundlage der schriftlichen Bemerkungen der Delegationen wurde eine neue Fassung[2] ausgearbeitet und in der Sitzung der Horizontalen Gruppe "Fragen des Cyberraums" vom 11. Juni 2018 erörtert.

4. In dieser Sitzung forderten die Delegationen einige weitere Anpassungen, und der Text der Schlussfolgerungen des Rates wurde entsprechend geändert[3]. Anschließend unterliefen die Schlussfolgerungen des Rates das Verfahren der stillschweigenden Zustimmung, das am 15. Juni 2018 um 12.00 Uhr endete. Im Zuge dieses Verfahrens brachten mehrere Mitgliedstaaten Bemerkungen vor, denen entsprechend zwei überarbeitete Fassungen des Textes erstellt wurden[4]. Die Frist für das Verfahren der stillschweigenden Zustimmung wurde bis zum 15. Juni 2018 (Dienstschluss) bzw. 18. Juni 2018 (Dienstschluss) verlängert. Bis zum Ende der verlängerten Frist für das Verfahren der stillschweigenden Zustimmung (18. Juni 2018, Dienstschluss) erhoben die Mitgliedstaaten keine Einwände, sodass der Vorsitz die Verhandlungen über den Entwurf der Schlussfolgerungen des Rates erfolgreich abschließen konnte (siehe Anlage).

5. Vor diesem Hintergrund wird der AStV gebeten, den Rat zu ersuchen, den in der Anlage enthaltenen Entwurf von Schlussfolgerungen des Rates zu einer koordinierten Reaktion der EU auf große Cybersicherheitsvorfälle und -krisen anzunehmen.

---

1 Dok. 9240/18.
2 Dok. 9240/1/18 REV 1.
3 Dok. 9240/2/18 REV 2.
4 Dok. 9240/3/18 REV 3 und 9240/4/18 REV 4.

ANLAGE

ENTWURF VON SCHLUSSFOLGERUNGEN DES RATES ZU EINER KOORDINIERTEN REAKTION DER EU AUF GROßE CYBERSICHERHEITSVORFÄLLE UND -KRISEN

Der Rat der Europäischen Union –

1. IN DEM BEWUSSTSEIN, dass große Cybersicherheitsvorfälle und -krisen einer effizienten Reaktion auf EU-Ebene bedürfen, wie in seinen Schlussfolgerungen vom 20. November 2017 zur Gemeinsamen Mitteilung an das Europäische Parlament und den Rat: "Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen" hervorgehoben[5];

2. UNTER HINWEIS AUF seine Schlussfolgerungen vom 19. Juni 2017 über einen Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten ("Cyber Diplomacy Toolbox")[6] und die entsprechenden Durchführungsleitlinien vom 11. Oktober 2017 sowie die 2013 angenommenen Vorkehrungen für eine integrierte Reaktion auf politische Krisen[7];

3. UNTER BERÜCKSICHTIGUNG der Empfehlung der Kommission vom 13. September 2017[8] für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen und der darin festgelegten Kernziele und Leitprinzipien;

4. UNTER KENNTNISNAHME von den Beratungen auf der Konferenz über die Herausforderungen für die Cybersicherheit vom 26. März 2018 in Sofia;

5. IN ANERKENNUNG der Zuständigkeiten der Mitgliedstaaten und ihrer Verantwortung für die nationale Sicherheit im Bereich der Cybersicherheit;

---

5 Dok. 14435/17.
6 Dok. 9916/17.
7 Dok. 10708/13.
8 C(2017) 6100 final.

6. UNTER WÜRDIGUNG der Annahme der Standardverfahren (Standard Operating Procedures – SOP) des CSIRTs-Netzwerks und der laufenden Arbeiten in der NIS-Kooperationsgruppe in Bezug auf die gemeinsame Systematik für Cybersicherheitsvorfälle;

7. IN ANERKENNUNG der laufenden Arbeiten in Bezug auf das Notfallprotokoll für die Strafverfolgungsbehörden, in dem ein Mechanismus für die frühzeitige Erkennung und Identifizierung von Cybersicherheitsvorfällen und -krisen beschrieben wird, der letztlich zu einer Untersuchung im Rahmen der normalen Arbeitsverfahren führt und eine Reaktion der Strafverfolgungsbehörden ergänzt und an die bestehenden Krisenreaktionsmechanismen der EU angleicht;

8. UNTER BERÜCKSICHTIGUNG der Vereinbarung zur Schaffung eines Kooperationsrahmens zwischen der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA), dem Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (EC3), dem IT-Notfallteam für die Organe, Einrichtungen und sonstigen Stellen der EU (CERT-EU) und der Europäischen Verteidigungsagentur (EDA), der ihre Zusammenarbeit im Rahmen ihrer jeweiligen Mandate, insbesondere in Fragen des Informationsaustauschs, der Cyber-Übungen und der technischen Zusammenarbeit, weiter verstärken wird;

9. UNTER HERVORHEBUNG der Notwendigkeit, die bestehenden Krisenbewältigungsmechanismen, -prozesse und -verfahren auf nationaler und europäischer Ebene zu nutzen;

10. UNTER HINWEIS DARAUF, wie wichtig es ist, die Richtlinie über die Sicherheit von Netz- und Informationssystemen[9] wirksam umzusetzen und die Fähigkeiten der zuständigen Behörden der nationalen CSIRTs und der zentralen Anlaufstellen in Bezug auf die Reaktion auf Cybersicherheitsvorfälle und deren Bewältigung auszubauen;

11. UNTER HINWEIS DARAUF, dass Maßnahmen auf EU-Ebene in Bezug auf große Cybersicherheitsvorfälle und -krisen nach den Grundsätzen der Subsidiarität und der Verhältnismäßigkeit durchgeführt werden;

---

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).

12. IN ANERKENNUNG der Bedeutung eines abgestimmten Lagebewusstseins – auf der Grundlage nationaler Schlussfolgerungen der Mitgliedstaaten –, einer koordinierten Unterrichtung der Öffentlichkeit und einer wirksamen Reaktion im Falle großer Cybersicherheitsvorfälle und -krisen auf EU-Ebene durch bestehende Mechanismen;

13. IN ANERKENNUNG der Zusammenarbeit zwischen der EU und der NATO im Bereich Cybersicherheit und Cyberabwehr unter uneingeschränkter Achtung der Grundsätze der Inklusivität, der Gegenseitigkeit und der Beschlussfassungsautonomie der EU, einschließlich des Informationsaustauschs zwischen dem CERT-EU und der NCIRC ("Computer Incident Response Capability" der NATO) –

Förderung der Abwehrbereitschaft und der Krisenprävention

14. BEKRÄFTIGT die Notwendigkeit, Cybersicherheitsvorfälle und -krisen zu verhindern, indem die Fähigkeit der EU und ihrer Mitgliedstaaten zur Bekämpfung von Cyber-Bedrohungen weiter gestärkt wird;

15. FORDERT die Mitgliedstaaten AUF, dafür zu sorgen, dass ihre nationalen Krisenbewältigungsmechanismen angemessen auf Cybersicherheitsvorfälle und -krisen reagieren können und geeignete Verfahren für die technische, operative und politische Zusammenarbeit auf EU-Ebene nutzen und, sofern erforderlich, einrichten;

16. BETONT, wie wichtig es ist, dass die EU und ihre Mitgliedstaaten regelmäßige Übungen hinsichtlich ihrer Reaktion auf große Cybersicherheitsvorfälle und -krisen durchführen, auch im Rahmen der von der ENISA organisierten CyberEurope-Übungen;

Verbesserung des Lagebewusstseins

17. FORDERT die EU und ihre Mitgliedstaaten AUF, zusammenzuarbeiten und auf der Grundlage der nationalen Schlussfolgerungen der Mitgliedstaaten zum Lagebewusstsein der EU auf allen Ebenen (technisch, operativ und politisch) sowohl vor als auch während großer Cybersicherheitsvorfälle und -krisen durch einen raschen und wirksamen Austausch von Lageinformationen, gegebenenfalls auch mit wichtigen strategischen Partnern, beizutragen;

Gewährleistung einer wirksamen Reaktion

18. ERKENNT AN, dass eine Reaktion auf große Cybersicherheitsvorfälle und -krisen viele Formen annehmen und ein koordiniertes Vorgehen auf EU-Ebene erfordern könnte, das – je nach Art des Vorfalls oder der Krise – von der Ermittlung technischer Maßnahmen über operative Maßnahmen bis hin zu politischen Maßnahmen reicht;

19. FORDERT die Mitgliedstaaten AUF, rasch weitere Formen der operativen Zusammenarbeit bei der Reaktion der Mitgliedstaaten auf grenzüberschreitende Risiken und Vorfälle, einschließlich im Rahmen der SOP des CSIRTs-Netzwerks, im Zusammenhang mit Frühwarnungen, gegenseitiger Unterstützung sowie Grundsätzen und Modalitäten der Koordinierung zu ermitteln, zu entwickeln und umzusetzen und über die erzielten Fortschritte zu berichten;

20. NIMMT KENNTNIS von der Initiative einer Gruppe von Mitgliedstaaten im Rahmen der Ständigen Strukturierten Zusammenarbeit (SSZ), die freiwillige Zusammenarbeit im Bereich der Cybersicherheit durch einen besseren Austausch von Cyber-Informationen und die Schaffung von Teams für die rasche Reaktion auf Cybervorfälle, die bei der Reaktion auf schwerwiegende Cybervorfälle gegenseitige Unterstützung leisten, zu vertiefen;

21. ERKENNT AN, dass Cybersicherheitsvorfälle durchaus zu sektorübergreifenden oder grenzüberschreitenden Krisen führen können, die sich gleichzeitig auf das Funktionieren verschiedener Infrastrukturen oder Dienste auswirken, und FORDERT die Mitgliedstaaten AUF, geeignete Verfahren und konkrete Maßnahmen für den rechtzeitigen Informationsaustausch und ein Lagebewusstsein auf operativer Ebene unter den zuständigen Behörden, wie die nationale zentrale Anlaufstelle im Rahmen der NIS-Richtlinie, zu ermitteln und einzuführen;

Straffung der Unterrichtung der Öffentlichkeit

22. ERKENNT AN, dass die Unterrichtung der Öffentlichkeit die negativen Auswirkungen von großen Cybersicherheitsvorfällen und -krisen eindämmen und dazu dienen könnte, die zu erwartenden Folgen einer diplomatischen Reaktion klar zu signalisieren, um so Einfluss auf das Verhalten potenzieller Aggressoren zu nehmen;

23. FORDERT die Institutionen, Agenturen und Einrichtungen der EU und der Mitgliedstaaten AUF, eine wirksame und, soweit erforderlich und möglich, koordinierte Kommunikation mit der Öffentlichkeit über die bestehenden Mechanismen sicherzustellen;

Aufbauen auf bisherigen Erfahrungen und Analysen nach Vorfällen

24. FORDERT die EU und ihre Mitgliedstaaten AUF, die Analyse operativer und strategischer Aspekte der bisherigen Erfahrungen aus großen Cybersicherheitsvorfällen, -krisen und -übungen auf der Grundlage ihrer nationalen Schlussfolgerungen innerhalb der Gemeinschaft der einschlägigen beteiligten Akteure zu fördern und allen zugänglich zu machen;

Entwicklung eines europäischen Rahmens für die Zusammenarbeit bei Cybersicherheitskrisen

25. FORDERT die EU und ihre Mitgliedstaaten AUF, gemeinsam auf die Entwicklung einer europäischen Zusammenarbeit bei Cybersicherheitskrisen hinzuarbeiten und für die praktische Einsatzfähigkeit und Dokumentation aller relevanten Akteure, Prozesse und Verfahren im Rahmen der bestehenden Krisenbewältigungsmechanismen der EU, insbesondere der Vorkehrungen für eine integrierte Reaktion auf politische Krisen, zu sorgen;

26. FORDERT die EU und ihre Mitgliedstaaten AUF, die erforderlichen Schritte zu unternehmen, um die Hindernisse zu beseitigen und/oder gegebenenfalls die festgestellten Mängel sowohl im Hinblick auf den Informationsfluss als auch auf die Interoperabilität der bestehenden Verfahren, Prozesse und Mechanismen zu beheben.