Rat der
Europäischen Union

Brüssel, den 20. März 2019
(OR. en)

7737/19

CYBER 101	**RELEX 287**
COPEN 118	**TELECOM 141**
COPS 92	**DAPIX 109**
COSI 52	**CATS 43**
DATAPROTECT 98	**CSC 111**
IND 102	**CSCI 47**
JAI 313	**IA 106**
JAIEX 44	**EJUSTICE 44**
POLMIL 31	

BERATUNGSERGEBNISSE

Absender:	Generalsekretariat des Rates
vom	19. März 2019
Empfänger:	Delegationen
Nr. Vordok.:	6866/19
Betr.:	Schlussfolgerungen des Rates über Cybersicherheitskapazitäten und deren Aufbau in der EU

Die Delegationen erhalten in der Anlage die Schlussfolgerungen des Rates über Cybersicherheitskapazitäten und deren Aufbau in der EU, die der Rat (Allgemeine Angelegenheiten) am 19. März 2019 angenommen hat.

ANLAGE

Schlussfolgerungen des Rates über Cybersicherheitskapazitäten und deren Aufbau in der EU

Der Rat der Europäischen Union –

1. UNTER HINWEIS auf seine Schlussfolgerungen zu "Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen"[1];

2. UNTER HINWEIS auf seine Schlussfolgerungen zu einer koordinierten Reaktion der EU auf große Cybersicherheitsvorfälle und -krisen[2];

3. UNTER HINWEIS auf seine Schlussfolgerungen zum Aufbau externer Cyberkapazitäten[3];

4. IN BEKRÄFTIGUNG dessen, dass durch den Ausbau der Cybersicherheitskapazitäten der Mitgliedstaaten und der Organe, Einrichtungen und sonstigen Stellen der EU sowie die daraus folgende Stärkung ihrer Cyberabwehrfähigkeit ein hohes Sicherheitsniveau für Netz- und Informationssysteme erreicht werden kann;

5. ERFREUT über die Fortschritte der Mitgliedstaaten beim Ausbau der Reaktionsteams für Computersicherheitsverletzungen (CSIRT);

6. IN WÜRDIGUNG der Errichtung des CSIRT-Netzes, bei der die Mitgliedstaaten von der Kommission und der ENISA aktiv unterstützt werden, sowie der verstärkten strategischen Zusammenarbeit in der Kooperationsgruppe für Netz- und Informationssicherheit, in der die Mitgliedstaaten, die Kommission und die ENISA vertreten sind;

---

1 Dok. 14435/17 (Schlussfolgerungen des Rates zur Gemeinsamen Mitteilung an das Europäische Parlament und den Rat: "Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen" vom 20. November 2017).

2 Dok. 10086/18 (Schlussfolgerungen zu einer koordinierten Reaktion der EU auf große Cybersicherheitsvorfälle und -krisen vom 26. Juni 2018).

3 Dok. 10496/18 (Schlussfolgerungen des Rates zu den EU-Leitlinien für den Aufbau externer Cyberkapazitäten vom 26. Juni 2018).

7. UNTER BETONUNG der Schlüsselrolle der Kooperationsgruppe für Netz- und Informationssicherheit bei der Erteilung der erforderlichen Vorgaben für ein möglichst einheitliches Vorgehen in der gesamten EU bei der Umsetzung der Richtlinie zur Netz- und Informationssicherheit[4] und bei der Auseinandersetzung mit wichtigen Fragen der Cybersicherheit;

8. IN ANERKENNUNG der Unterstützung, die die Kommission den Mitgliedstaaten beim Kapazitätsaufbau der CSIRT durch die Fazilität "Connecting Europe" bereits leistet;

9. IN ANERKENNUNG der Unterstützung, die den Strafverfolgungsbehörden beim Kapazitätsaufbau zur Bekämpfung der Cyberkriminalität durch den Fonds für die innere Sicherheit und die CEPOL zuteilwird;

10. ERFREUT darüber, dass der EU-Politikrahmen für die Cyberabwehr dahingehend aktualisiert wurde, dass der Ausbau der Cyberabwehrkapazitäten der Mitgliedstaaten weiter unterstützt wird;

11. IN WÜRDIGUNG der Fortschritte bei der Umsetzung der Richtlinie zur Netz- und Informationssicherheit durch die Mitgliedstaaten;

12. IN DEM BEWUSSTSEIN, dass die Cybersicherheit ein komplexer und sich ständig wandelnder Bereich ist, der mit anderen Bereichen verflochten ist und die Anpassung des politischen und rechtlichen Rahmens an neue technologische Trends und neu entstehende Technologien wie künstliche Intelligenz, Blockchain und Quanteninformatik erfordert;

---

[4] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016).

13. UNTER HERVORHEBUNG dessen, dass Schulungs- und Ausbildungsprogramme im Zusammenhang mit Cybersicherheit sowie die Information und Sensibilisierung von Endnutzern über Sicherheitsbedrohungen für die Verringerung der Cybersicherheitsrisiken von wesentlicher Bedeutung sind;

14. UNTER BETONUNG dessen, dass Cyberübungen effiziente Instrumente zur Bewertung und weiteren Verbesserung des Niveaus der Abwehrbereitschaft der EU und ihrer Mitgliedstaaten gegen große Cybersicherheitsvorfälle und -krisen darstellen;

15. UNTER ERNEUTEM HINWEIS darauf, dass der Cyberraum keine Grenzen hat, weshalb eine grenzüberschreitende und bereichsübergreifende Sichtweise und Zusammenarbeit ein unumstößlicher Grundsatz für die Tätigkeiten und Initiativen zum Aufbau von Cyberkapazitäten sind;

16. UNTER BETONUNG der Bedeutung der Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor sowie der Wissenschaft, insbesondere durch kooperative Projekte;

17. UNTER HERVORHEBUNG der Bedeutung der zivil-militärischen Zusammenarbeit im Hinblick auf gemeinsame Ziele im Cyberbereich, mit der kohärente und wirksame Reaktionen auf Cyberbedrohungen gewährleistet werden sollen –

18. NIMMT die Fortschritte einer Gruppe von Mitgliedstaaten beim Aufbau von Teams für die rasche Reaktion auf Cybervorfälle ZUR KENNTNIS, mit denen die freiwillige Zusammenarbeit im Cyberbereich durch gegenseitige Hilfe verstärkt werden soll;

19. BEGRÜSST die laufenden Beratungen im Rat über den Vorschlag der Kommission für eine Verordnung des Europäischen Parlaments und des Rates zur Einrichtung des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und des Netzes nationaler Koordinierungszentren;

20. ERMUNTERT zur aktiven Beteiligung an der laufenden Arbeit der Kooperationsgruppe für Netz- und Informationssicherheit, insbesondere hinsichtlich des Aufbaus von Cyberkapazitäten;

21. BEFÜRWORTET die derzeitigen Arbeiten der Kooperationsgruppe für Netz- und Informationssicherheit an einer koordinierten Reaktion der EU auf große Cybersicherheitsvorfälle und -krisen;

22. ERSUCHT die Mitgliedstaaten, ihre nationalen Cybersicherheitsstrategien weiterzuentwickeln und die Cybersicherheit durchgängig zu berücksichtigen, wobei sektorspezifischen Anforderungen Rechnung zu tragen ist;

23. FORDERT die Mitgliedstaaten AUF, ständig zu beobachten und zu evaluieren/zu bewerten, wie sich die auf nationaler Ebene getroffenen Maßnahmen zur Stärkung der Cyberabwehrfähigkeit und zum Ausbau der Cyberkapazitäten auswirken;

24. ERSUCHT die Mitgliedstaaten, die Cybersicherheit und digitale Kompetenzen durchgängig in die Lehrpläne für alle Bildungsebenen (Grund- und Sekundarschulen, Hochschulen, lebenslanges Lernen) einzubeziehen, gegebenenfalls auf der Grundlage bereits bestehender und künftiger Stellenprofile;

25. FORDERT die Mitgliedstaaten AUF, für die Öffentlichkeit und die Endnutzer Initiativen zur Sensibilisierung für Cybersicherheit und zur Cyberhygiene durchzuführen, mit besonderer Ausrichtung auf Angestellte des öffentlichen Dienstes;

26. LEGT den Mitgliedstaaten NAHE, auf nationaler Ebene Cybersicherheitsübungen durchzuführen sowie auf EU-Ebene entsprechende Übungen durchzuführen und/oder daran teilzunehmen, um strategische und technologische Aspekte zu testen und einzuüben und die erforderlichen Fähigkeiten in der Praxis effektiv zu entwickeln;

27. ERSUCHT die Mitgliedstaaten, die technischen und operativen Cybersicherheitskapazitäten ihrer CSIRT zur Prävention und Eindämmung von Vorfällen sowie zu einer entsprechenden Reaktion weiterzuentwickeln;

28. RUFT die Kommission und die ENISA AUF, die Mitgliedstaaten weiter beim Ausbau der Kapazitäten und Fähigkeiten des CSIRT-Netzes zu unterstützen, damit sie besser zusammenarbeiten, Informationen über Vorfälle austauschen und auf große grenzüberschreitende Vorfälle wirksam reagieren können;

29. ERSUCHT die Mitgliedstaaten, die Strafverfolgungsbehörden weiter dabei zu unterstützen, in Koordination mit den zuständigen europäischen Behörden spezifische Kompetenzen zu entwickeln, um die Cyberkriminalität auf EU-Ebene wirksam zu bekämpfen;

30. FORDERT die Mitgliedstaaten zu größeren Investitionen in den Aufbau von Cyberkapazitäten AUF;

31. RUFT die Kommission und die ENISA AUF, Sensibilisierungsprogramme und Schulungen über Cybersicherheit durchzuführen, die auf die Beschäftigten der Organe, Einrichtungen und sonstigen Stellen der EU ausgerichtet sind;

32. APPELLIERT an die EU und ihre Mitgliedstaaten, freiwillig Informationen und bewährte Verfahren auszutauschen, um dazu beizutragen, dass auf nationaler und auf EU-Ebene die wichtigsten Erfordernisse beim Aufbau von Cyberkapazitäten ermittelt und angegangen werden;

33. ERSUCHT die EU und ihre Mitgliedstaaten, die Forschung im Bereich der Cybersicherheit zu unterstützen und in anderen Studienrichtungen für die Thematisierung der Cybersicherheit zu werben, indem verschiedene Bereiche der Forschung und Entwicklung im Zusammenhang mit der Cybersicherheit zu einem einheitlichen Ganzen zusammengeführt werden, sowie die Exzellenz in der Cybersicherheitsforschung zu fördern;

34. FORDERT die EU und ihre Mitgliedstaaten AUF, eine Cybersicherheitsforschung zu entwickeln, die den gesellschaftlichen Bedürfnissen entspricht und die Forschungsergebnisse in den Markt einbringt;

35. RUFT die EU und ihre Mitgliedstaaten AUF, gegebenenfalls bei ihren Beschaffungsverfahren für IKT die Cybersicherheit zu berücksichtigen.