Rat der
Europäischen Union

Brüssel, den 21. Juni 2022
(OR. en)

10504/22

CYBER 232
TELECOM 288
CSC 286
CSCI 96
FIN 689

BERATUNGSERGEBNISSE

Absender:	Generalsekretariat des Rates
vom	21. Juni 2022
Empfänger:	Delegationen
Nr. Vordok.:	9716/22
Betr.:	Schlussfolgerungen des Rates zum Sonderbericht Nr. 5/2022 des Europäischen Rechnungshofs mit dem Titel „Cybersicherheit: Organe, Einrichtungen und sonstige Stellen der EU sind insgesamt nicht ausreichend gegen Bedrohungen gewappnet“ – Schlussfolgerungen des Rates, die der Rat auf seiner Tagung vom 21. Juni 2022 gebilligt hat

Die Delegationen erhalten in der Anlage die oben genannten Schlussfolgerungen, die der Rat auf seiner Tagung vom 21. Juni 2022 gebilligt hat.

ANLAGE

SCHLUSSFOLGERUNGEN DES RATES

zum Sonderbericht Nr. 5/2022 des Europäischen Rechnungshofs mit dem Titel „Cybersicherheit: Organe, Einrichtungen und sonstige Stellen der EU sind insgesamt nicht ausreichend gegen Bedrohungen gewappnet“

DER RAT DER EUROPÄISCHEN UNION —

UNTER HINWEIS auf seine Schlussfolgerungen betreffend die Verbesserung des Verfahrens zur Prüfung der im Rahmen des Entlastungsverfahrens erstellten Sonderberichte des Rechnungshofs[1] —

1. NIMMT KENNTNIS von dem Sonderbericht Nr. 5/2022 des Europäischen Rechnungshofs mit dem Titel „Cybersicherheit: Organe, Einrichtungen und sonstige Stellen der EU sind insgesamt nicht ausreichend gegen Bedrohungen gewappnet“[2];

2. HEBT HERVOR, wie wichtig und dringend es ist, das Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der EU angesichts der jüngsten Intensivierung des digitalen Wandels innerhalb der Organe, der von ihnen verarbeiteten sensiblen Informationen, der ständig zunehmenden Zahl und Schwere der Angriffe auf die Organe, Einrichtungen und sonstigen Stellen der EU und des Ausmaßes der Bedrohung, von der sie betroffen sind, zu stärken;

3. WEIST auf die Schlussfolgerungen des Europäischen Rates vom 20. Juni 2019[3] HIN, in denen dieser die EU-Institutionen ersucht hat, zusammen mit den Mitgliedstaaten Maßnahmen auszuarbeiten, um die Resilienz zu stärken und die Sicherheitskultur der EU hinsichtlich Cyberbedrohungen und hybrider Bedrohungen von außerhalb der EU zu verbessern und die Kommunikations- und Informationsnetze der EU sowie ihre Entscheidungsprozesse besser vor böswilligen Handlungen aller Art zu schützen;

---

1 Dok. 7515/00 + COR 1.
2 Dok. 8040/22.
3 Dok. EUCO 9/19.

4. WEIST auf seine Schlussfolgerungen vom 10. Dezember 2019 zu zusätzlichen Anstrengungen zur Stärkung der Resilienz und zur Abwehr hybrider Bedrohungen[4] HIN, in denen er alle Organe, Agenturen und Einrichtungen der EU ersucht hat, mit der Unterstützung der Mitgliedstaaten auf der Grundlage einer umfassenden Einschätzung der Bedrohungslage dafür zu sorgen, dass die Union in der Lage ist, ihre Integrität zu schützen, und sicherzustellen, dass die Kommunikations- und Informationsnetze und die Beschlussfassungsverfahren der EU vor böswilligen Aktivitäten aller Art geschützt sind. Wie es in den Schlussfolgerungen heißt, sollten daher die Organe, Einrichtungen und Agenturen der EU im Einklang mit dem vom Europäischen Rat auf seiner Tagung im Juni 2019 erteilten Mandat[5] mit der Unterstützung der Mitgliedstaaten ein umfassendes Bündel von Maßnahmen ausarbeiten und umsetzen, um für ihre Sicherheit zu sorgen;

5. WEIST auf seine Schlussfolgerungen vom 22. März 2021 zur Cybersicherheitsstrategie der EU für die digitale Dekade[6] HIN, in denen betont wird, dass Cybersicherheit für das Funktionieren der öffentlichen Verwaltung und der öffentlichen Institutionen sowohl auf nationaler als auch auf EU-Ebene sowie für unsere Gesellschaft und die Wirtschaft insgesamt von entscheidender Bedeutung ist;

6. WEIST auf seine Schlussfolgerungen vom 23. Mai 2022 zur Entwicklung der Cyberabwehr der Europäischen Union[7] HIN, in denen die Organe, Einrichtungen und Agenturen der EU ermutigt wurden, sich an der Bestandsaufnahme der bestehenden Instrumente für eine sichere Kommunikation im Cyberbereich zu beteiligen, die in den einschlägigen Ratsgremien und mit einschlägigen Kooperationsgruppen wie dem CSIRTs network und EU CyCLONe erörtert werden soll;

7. HEBT HERVOR, dass das systemische Risiko angegangen werden muss, das trotz ihrer institutionellen Unabhängigkeit und Verwaltungsautonomie in der Verflechtung zwischen den Organen, Einrichtungen und sonstigen Stellen der EU sowie zwischen ihnen und den Organen der Mitgliedstaaten besteht;

---

4 Dok. 14972/19.
5 Dok. EUCO 9/19.
6 Dok. 6722/21.
7 Dok. 9364/22.

8. NIMMT KENNTNIS von den Bemerkungen des Sonderberichts, wonach die Organe, Einrichtungen und sonstigen Stellen der EU nicht ausreichend gegen Cyberbedrohungen gewappnet sind und bei der Cybersicherheit unterschiedliche Reifegrade aufweisen; IST SICH BEWUSST, dass das Niveau der Cybersicherheitsvorkehrungen der Organe, Einrichtungen und sonstigen Stellen der EU sowie die Synergien zwischen ihnen verbessert werden sollten;

9. ERMUTIGT daher die Organe, Einrichtungen und sonstigen Stellen der EU nachdrücklich, die Umsetzung von Maßnahmen für das Cyberrisikomanagement fortzusetzen, mit denen ein angemessenes Cybersicherheitsniveau sichergestellt wird, wie es in der vorgeschlagenen Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148 vorgesehen ist, um besser gegen Bedrohungen gewappnet zu sein;

10. ERSUCHT die Organe, Einrichtungen und sonstigen Stellen der EU, sowohl ihre Anstrengungen zu ihrem Schutz vor Cyberbedrohungen als auch ihre Zusammenarbeit bei der Festlegung einheitlicher Normen und Spezifikationen, insbesondere für die Vergabe öffentlicher Aufträge, Projekte und Dienste im Zusammenhang mit der Cybersicherheit, zu intensivieren und die Interoperabilität ihrer IT-Systeme zu verbessern, auch um die sichere Kommunikation von nicht als Verschlusssache eingestuften Inhalten sicherzustellen;

11. ERSUCHT die Agentur der Europäischen Union für Cybersicherheit (ENISA) und das IT-Notfallteam für die Organe, Einrichtungen und sonstigen Stellen der EU (CERT-EU), im Rahmen ihrer Zuständigkeiten ihre Zusammenarbeit bei der Unterstützung der Organe, Einrichtungen und sonstigen Stellen der EU bei ihren Bemühungen im Bereich der Cybersicherheit zu intensivieren, insbesondere im Hinblick auf den Aufbau von Kapazitäten für diejenigen Organe, Einrichtungen und sonstigen Stellen der EU, die bei der Cybersicherheit einen geringeren Reifegrad aufweisen;

12. NIMMT KENNTNIS von den Schlussfolgerungen und Empfehlungen im Sonderbericht und IST SICH BEWUSST, dass das Niveau der Cybersicherheitsvorkehrungen der Organe, Einrichtungen und sonstigen Stellen der EU sowie die Synergien zwischen ihnen erheblich verbessert werden sollten. Die Organe, Einrichtungen und sonstigen Stellen der EU sollten über einen umfassenden Rahmen für das Risikomanagement im Bereich der Cybersicherheit verfügen, regelmäßige Risikobewertungen und Audits auf der Grundlage einer gemeinsamen oder bekannten Methodik und internationaler Standards durchführen und Programme zur Sensibilisierung und Schulung des Personals im Bereich der Cybersicherheit systematisieren;

13. BETONT ferner, dass die Organe, Einrichtungen und sonstigen Stellen der EU ausreichende Haushaltsmittel bereitstellen sollten, um die Umsetzung von Schutzmaßnahmen gegen Cyberbedrohungen unter Einhaltung des mehrjährigen Finanzrahmens sicherzustellen, und NIMMT KENNTNIS von der Empfehlung im Sonderbericht, eine Stelle zu benennen, die alle Organe, Einrichtungen und sonstigen Stellen der EU vertritt und über das entsprechende Mandat und ausreichende Mittel verfügt, um die Einhaltung der gemeinsamen Cybersicherheitsvorschriften überprüfen zu können;

14. IST SICH BEWUSST, dass das CERT-EU unverzüglich über bedeutende Sicherheitsvorfälle in den Organen, Einrichtungen und sonstigen Stellen der EU informiert und zu diesem Zweck mit angemessenen Ressourcen ausgestattet werden sollte, die vorhersehbar sind und an das derzeitige Bedrohungsniveau und die Bedürfnisse der Organe, Einrichtungen und sonstigen Stellen der EU angepasst sind, insbesondere in Bezug auf Personal, technische Ausrüstung und Infrastruktur;

15. STELLT FEST, dass die Zusammenarbeit und der Informationsaustausch im Bereich der Cybersicherheit sowie die Interoperabilität sicherer Kommunikationskanäle zwischen den Organen, Einrichtungen und sonstigen Stellen der EU gestärkt und systematisiert werden sollte; FORDERT, dass eine solche Zusammenarbeit und ein solcher Informationsaustausch auch die für Cybersicherheit zuständigen Behörden in den Mitgliedstaaten einbeziehen;

16. NIMMT KENNTNIS von den Antworten der Kommission, des CERT-EU und der ENISA, die dem Sonderbericht beigefügt sind;

17. ERSUCHT die Kommission, die Empfehlungen des Sonderberichts zu berücksichtigen, sich bei der Gestaltung der Cybersicherheitsstrategien der Organe, Einrichtungen und sonstigen Stellen der EU ehrgeizige Ziele zu setzen und sich für mehr Synergien zwischen ihnen einzusetzen.