Rat der
Europäischen Union

Brüssel, den 22. März 2022
(OR. en)

7474/22
ADD 3

Interinstitutionelles Dossier:
2022/0085(COD)

CYBER 93
TELECOM 116
JAI 383
INST 89
INF 32
CSC 119
CSCI 39
DATAPROTECT 81
FIN 353
BUDGET 2
CODEC 349
IA 30

ÜBERMITTLUNGSVERMERK

Absender:	Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	22. März 2022
Empfänger:	Herr Jeppe TRANHOLM-MIKKELSEN, Generalsekretär des Rates der Europäischen Union
Nr. Komm.dok.:	SWD(2022) 68 final
Betr.:	ARBEITSUNTERLAGE DER KOMMISSIONSDIENSTSTELLEN ZUSAMMENFASSUNG DER FOLGENDENABSCHÄTZUNG Begleitunterlage zum Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zur Festlegung von Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union

Die Delegationen erhalten in der Anlage das Dokument SWD(2022) 68 final.

Anl.: SWD(2022) 68 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 22.3.2022
SWD(2022) 68 final

ARBEITSUNTERLAGE DER KOMMISSIONSDIENSTSTELLEN

ZUSAMMENFASSUNG DER FOLGENDENABSCHÄTZUNG

Begleitunterlage zum

Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

zur Festlegung von Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union

{COM(2022) 122 final} - {SWD(2022) 67 final}

1. Einführung

Im Jahr 2020 stieg bei den Organen, Einrichtungen und sonstigen Stellen der Union die Zahl der erheblichen Sicherheitsvorfälle, die von Akteuren ausgingen, die als „fortgeschrittene andauernde Bedrohung“ (*Advanced Persistent Threat*, APT) zu betrachten sind. Dies spiegelt sich auch in der Zahl der 2020 vom CERT-EU analysierten forensischen Abbilder wider, die sich im Vergleich zu 2019 mehr als verdreifacht hat, während die Zahl der erheblichen Sicherheitsvorfälle seit 2018 sogar um mehr als das Zehnfache gestiegen ist.

Bei den Cybersicherheitskapazitäten und den Ausgaben für IT-Sicherheit in den Organen, Einrichtungen und sonstigen Stellen der Union bestehen jedoch zum Teil enorme Unterschiede, was zu einem breiten Spektrum an Reifegraden im Bereich der Cybersicherheit zwischen den Organen, Einrichtungen und sonstigen Stellen der Union führt. Darüber hinaus zeigen die Analysen der Bedrohungslandschaft und die Statistiken über IT-Sicherheitsvorfälle, dass die Organe, Einrichtungen und sonstigen Stellen der Union immer häufiger noch größeren Cyberbedrohungen ausgesetzt sein werden.

2. Ziele

Die festgestellten Mängel führen letztlich zur Feststellung einer unzureichenden Cyberresilienz in allen Organen, Einrichtungen und sonstigen Stellen der Union, einer fragmentierten Mittelausstattung für die IT-Sicherheit und einer Unausgewogenheit der IT-Sicherheitslagen.

Ziel eines Rechtsakts wäre es, Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union vorzusehen. Damit soll dazu beigetragen und dafür gesorgt werden, dass der Cybersicherheitsreifegrad mit der beschleunigten Digitalisierung der Organe, Einrichtungen und sonstigen Stellen der Union Schritt halten kann.

3. Ein Interinstitutioneller Cybersicherheitsbeirat und ein Cybersicherheitsrahmen

Der Vorschlag für einen Interinstitutionellen Cybersicherheitsbeirat und einen Cybersicherheitsrahmen sieht Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union vor, die eine Angleichung innerhalb eines Rahmens ermöglichen, mit dem Bedrohungen für die Cybersicherheit aller Organe, Einrichtungen und sonstigen Stellen der Union bewältigt werden sollen. Außerdem wird darin eine Überwachung und Berichterstattung an einen Interinstitutionellen Cybersicherheitsbeirat festgelegt.

Mit dem Vorschlag werden der Auftrag und die Aufgaben des CERT-EU unter Berücksichtigung der neuen und zunehmenden Digitalisierung der Organe, Einrichtungen und sonstigen Stellen der Union in den letzten Jahren und der sich wandelnden Bedrohungslandschaft im Bereich der Cybersicherheit modernisiert.

Daraus ergeben sich keine direkten Folgen oder Haushaltsauswirkungen für die Mitgliedstaaten oder die Bürgerinnen und Bürger der EU.

Die Rechtsgrundlage für die vorgeschlagene Verordnung ist Artikel 298 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), der vorsieht, dass sich die Organe, Einrichtungen und sonstigen Stellen der Union zur Ausübung ihrer Aufgaben auf eine offene, effiziente und unabhängige europäische Verwaltung stützen.

Dieser Vorschlag beruht auf der EU-Strategie für eine Sicherheitsunion (COM(2020) 605 final) und auf der Cybersicherheitsstrategie der EU für die digitale Dekade (JOIN(2020) 18 final).

4. Schlussfolgerung

Mit einem Interinstitutionellen Cybersicherheitsbeirat und einem Cybersicherheitsrahmen werden die meisten der angestrebten Ziele auf eine verhältnismäßig wirksame, effiziente und mit anderen Bereichen der Unionspolitik kohärente Weise und mit breitestmöglicher Unterstützung der Interessenträger erreicht. Angesichts der geltenden rechtlichen Schranken, innerhalb deren wir handeln, stellt die gewählte Lösung die am besten durchführbare Option dar, denn ein Pauschalansatz würde den heute unterschiedlichen Reifegraden in den Organen, Einrichtungen und sonstigen Stellen der Union und den vielfältigen technologischen Risiken und der Komplexität, mit denen sie konfrontiert sind, nicht gerecht.