Rat der
Europäischen Union

Brüssel, den 22. März 2022
(OR. en)

7474/22
ADD 1

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

VORSCHLAG

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.:	COM(2022) 122 final - Annexes
Betr.:	ANHÄNGE des Vorschlags 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 COM(2022) 122 final - Annexes.

Anl.: COM(2022) 122 final - Annexes

EUROPÄISCHE
KOMMISSION

Brüssel, den 22.3.2022
COM(2022) 122 final

ANNEXES 1 to 2

ANHÄNGE

des

Vorschlags 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

{SWD(2022) 67 final} - {SWD(2022) 68 final}

ANHANG I

Die Cybersicherheitsgrundregeln betreffen folgende Bereiche:

(1) Cybersicherheitspolitik, einschließlich der Ziele und Prioritäten für die Sicherheit von Netz- und Informationssystemen, insbesondere hinsichtlich der Nutzung von Cloud-Computing-Diensten (im Sinne des Artikels 4 Nummer 19 der Richtlinie [NIS-2-Vorschlag]) und technischer Vorkehrungen zur Ermöglichung der Telearbeit;

(2) Organisation der Cybersicherheit, einschließlich Festlegung der Aufgaben und Zuständigkeiten;

(3) Verwaltung der Vermögenswerte, einschließlich IT-Bestandsverzeichnis und IT-Netzkartografie;

(4) Zugangskontrolle;

(5) Betriebssicherheit;

(6) Kommunikationssicherheit;

(7) Beschaffung, Entwicklung und Wartung von Systemen;

(8) Lieferantenbeziehungen;

(9) Management von Sicherheitsvorfällen, einschließlich der Konzepte zur Verbesserung der Abwehrbereitschaft, Reaktion und Folgenbewältigung bei Sicherheitsvorfällen und der Zusammenarbeit mit dem CERT-EU, z. B. bei der Aufrechterhaltung der Sicherheitsüberwachung und -protokollierung;

(10) Betriebskontinuitätsmanagement und Krisenmanagement;

(11) Ausbildungs-, Aufklärungs- und Schulungsprogramme im Bereich der Cybersicherheit.

ANHANG II

Im Einklang mit den Leitlinien und Empfehlungen des IICB berücksichtigen die Organe, Einrichtungen und sonstigen Stellen der Union bei der Umsetzung der Cybersicherheitsgrundregeln und in ihren Cybersicherheitsplänen zumindest die folgenden besonderen Cybersicherheitsmaßnahmen:

(1) konkrete Schritte für den Übergang zu einer „Zero-Trust-Architektur“ (d. h. zu einem Sicherheitsmodell mit einer Reihe von Grundsätzen für die Systemgestaltung und eine koordinierte Cybersicherheits- und Systemmanagementstrategie, die auf der Anerkennung beruhen, dass sowohl innerhalb als auch außerhalb der herkömmlichen Netzgrenzen Bedrohungen bestehen);

(2) Einführung der Multifaktor-Authentifizierung als Norm in allen Netz- und Informationssystemen;

(3) Schaffung von Sicherheit in der Software-Lieferkette durch Kriterien für die sichere Softwareentwicklung und -bewertung;

(4) Erweiterung der Vorschriften für die Auftragsvergabe, um ein hohes gemeinsames Cybersicherheitsniveau zu erleichtern, und zwar durch

   (a) die Beseitigung vertraglicher Hindernisse, die den Informationsaustausch der IT-Dienstleister über Sicherheitsvorfälle, Schwachstellen und Cyberbedrohungen mit dem CERT-EU einschränken;

   (b) die vertragliche Pflicht zur Meldung von Sicherheitsvorfällen, Sicherheitslücken und Cyberbedrohungen sowie zur angemessenen Bewältigung und Überwachung von Sicherheitsvorfällen.