Rat der
Europäischen Union

Brüssel, den 20. April 2023
(OR. en)

8512/23
ADD 1

Interinstitutionelles Dossier:
2023/0109(COD)

CYBER 92
TELECOM 108
CADREFIN 51
FIN 448
BUDGET 6
IND 181
JAI 471
MI 314
DATAPROTECT 110
RELEX 481
CODEC 662

ÜBERMITTLUNGSVERMERK

Absender:	Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	19. April 2023
Empfänger:	Frau Thérèse BLANCHET, Generalsekretärin des Rates der Europäischen Union
Nr. Komm.dok.:	COM(2023) 209 final - Annex
Betr.:	ANHANG der VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über Maßnahmen zur Stärkung der Solidarität und der Kapazitäten in der Union für die Erkennung, Vorsorge und Bewältigung von Cybersicherheitsbedrohungen und -vorfällen

Die Delegationen erhalten in der Anlage das Dokument COM(2023) 209 final - Annex.

Anl.: COM(2023) 209 final - Annex

EUROPÄISCHE
KOMMISSION

Straßburg, den 18.4.2023
COM(2023) 209 final

ANNEX

ANHANG

der

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über Maßnahmen zur Stärkung der Solidarität und der Kapazitäten in der Union für die Erkennung, Vorsorge und Bewältigung von Cybersicherheitsbedrohungen und -vorfällen

ANHANG

Die Verordnung (EU) 2021/694 wird wie folgt geändert:

1. In Anhang I erhält der Abschnitt/das Kapitel „Spezifisches Ziel 3 – Cybersicherheit und Vertrauen“ folgende Fassung:

„Spezifisches Ziel 3 – Cybersicherheit und Vertrauen

Das Programm regt die Verstärkung, den Aufbau und den Erwerb grundlegender Kapazitäten zur Sicherung der digitalen Wirtschaft, Gesellschaft und Demokratie in der Union an, indem es das industrielle Potenzial und die Wettbewerbsfähigkeit der Union im Bereich der Cybersicherheit stärkt und die Kapazitäten der Privatwirtschaft und des öffentlichen Sektors zum Schutz der Bürger und Unternehmen vor Cyberbedrohungen verbessert, einschließlich durch Unterstützung bei der Umsetzung der Richtlinie (EU) 2016/1148.

Die anfänglichen und gegebenenfalls nachfolgenden Maßnahmen im Rahmen dieses Ziels umfassen Folgendes:

1. Koinvestitionen mit Mitgliedstaaten in fortgeschrittene Cybersicherheitsausrüstung und -infrastrukturen sowie Know-how im Bereich der Cybersicherheit, die für den Schutz kritischer Infrastrukturen und des digitalen Binnenmarkts insgesamt von wesentlicher Bedeutung sind. Solche Koinvestitionen könnten Investitionen in Quantencomputeranlagen und Datenressourcen für Cybersicherheit, die Lageerfassung im Cyberraum, ***einschließlich der nationalen SOCs und der grenzübergreifenden SOCs, die den europäischen Cyberschutzschild bilden***, sowie weitere Instrumente umfassen, die dem öffentlichen Sektor und der Privatwirtschaft in ganz Europa zugänglich zu machen sind;

2. Ausweitung der vorhandenen technologischen Kapazitäten und Vernetzung der Kompetenzzentren in den Mitgliedstaaten sowie Sicherstellung, dass diese Kapazitäten dem Bedarf des öffentlichen Sektors und der Industrie entsprechen, einschließlich durch Produkte und Dienstleistungen zur Stärkung der Cybersicherheit und des Vertrauens in den digitalen Binnenmarkt;

3. Sicherstellung einer breiten Einführung wirksamer moderner cybersicherheits- und vertrauensfördernder Lösungen in allen Mitgliedstaaten. Zu einer solchen Einführung gehört auch die Stärkung der Produktsicherheit vom Design bis zur Kommerzialisierung der Produkte;

4. Unterstützung bei der Schließung der Kompetenzlücke im Bereich der Cybersicherheit, z. B. durch die Angleichung der entsprechenden Qualifikationsprogramme, ihre Anpassung an die sektorspezifischen Bedürfnisse und die Erleichterung des Zugangs zu gezielten spezialisierten Schulungen.

5. ***Förderung der Solidarität zwischen den Mitgliedstaaten bei der Vorbereitung und Reaktion auf schwerwiegende Cybersicherheitsvorfälle durch eine grenzüberschreitende Einführung von Cybersicherheitsdiensten, einschließlich der Unterstützung der Amtshilfe zwischen Behörden und der Einrichtung einer Reserve vertrauenswürdiger Cybersicherheitsanbieter auf Unionsebene.***“

2. In Anhang II erhält der Abschnitt/das Kapitel „Spezifisches Ziel 3 – Cybersicherheit und Vertrauen“ folgende Fassung:

„Spezifisches Ziel 3 – Cybersicherheit und Vertrauen

3.1. Anzahl der gemeinsam beschafften Cybersicherheitsinfrastrukturen oder -werkzeuge oder beider[1]

3.2. Anzahl der Nutzer und Nutzergemeinschaften, die Zugang zu europäischen Cybersicherheitseinrichtungen erhalten

3.3. Anzahl der Maßnahmen zur Unterstützung der Abwehrbereitschaft und der Reaktion auf Cybersicherheitsvorfälle im Rahmen des Cybernotfallmechanismus“.