Rat der
Europäischen Union

Brüssel, den 4. August 2021
(OR. en)

11155/21
ADD 1

CYBER 218
JAI 904
TELECOM 307
CSC 300
CIS 99
RELEX 702
ENFOPOL 299
COPS 298
COSI 155
HYBRID 52
CSCI 115
POLGEN 151
DATAPROTECT 200

ÜBERMITTLUNGSVERMERK

Absender:	Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	2. August 2021
Empfänger:	Herr Jeppe TRANHOLM-MIKKELSEN, Generalsekretär des Rates der Europäischen Union
Nr. Komm.dok.:	C(2021) 4520 final
Betr.:	ANHANG der EMPFEHLUNG DER KOMMISSION zum Aufbau einer Gemeinsamen Cyber-Einheit

Die Delegationen erhalten in der Anlage das Dokument C(2021) 4520 final.

Anl.: C(2021) 4520 final Annex

EUROPÄISCHE
KOMMISSION

Brüssel, den 23.6.2021
C(2021) 4520 final

ANNEX

ANHANG

der

EMPFEHLUNG DER KOMMISSION

zum Aufbau einer Gemeinsamen Cyber-Einheit

ANHANG – STUFEN FÜR DEN AUFBAU DER GEMEINSAMEN CYBER-EINHEIT

In diesem Anhang werden die Kern- und Unterstützungsmaßnahmen für die Einrichtung und den Betrieb der Gemeinsamen Cyber-Einheit erläutert.

1. *Stufe 1 – Bewertung der organisatorischen Aspekte der Gemeinsamen Cyber-Einheit und Ermittlung der in der EU verfügbaren operativen Fähigkeiten*

KERNMAßNAHMEN

Die operativen Teilnehmer der Gemeinsamen Cyber-Einheit sollten in der von der Kommission eingesetzten Arbeitsgruppe und mit Unterstützung der ENISA Informationen über bereits vorhandene operative Fähigkeiten zusammenstellen – beispielsweise eine Liste der verfügbaren Experten unter Angabe ihrer jeweiligen Fachkenntnisse, eine Aufstellung der verfügbaren Instrumente zur Bewältigung von Sicherheitsvorfällen, ihrer Funktionen und Leistung, des Spektrums verfügbarer Schulungs- und Übungsangebote sowie bereits vorhandener Produkte für die Auswertung von Informationen und nachrichtendienstlichen Erkenntnissen. Auf der Grundlage dieser Beiträge sollten die operativen Teilnehmer eine Liste der **in der EU verfügbaren operativen Fähigkeiten** erstellen, die im Falle von Cybersicherheitsvorfällen oder -krisen, insbesondere unter Rückgriff auf die schnellen EU-Einsatzteams für Cybersicherheit, eingesetzt werden können.

Die Arbeitsgruppe sollte eine Bewertung der **organisatorischen Aspekte** der Gemeinsamen Cyber-Einheit **sowie der Aufgaben und Zuständigkeiten der operativen Teilnehmer innerhalb dieser Plattform** in die Wege leiten.

Um einen Überblick über die Fähigkeiten zu erhalten und eine Einigung über die Verfahren zu erzielen, sollten die für Stufe 1 festgelegten Kernmaßnahmen und möglichst auch die Unterstützungsmaßnahmen bis zum **31. Dezember 2021 [6 Monate nach der Annahme]** abgeschlossen sein.

2. *Stufe 2 – Ausarbeitung von Plänen für die Reaktion auf Cybersicherheitsvorfälle und -krisen sowie Umsetzung gemeinsamer Maßnahmen für die Abwehrbereitschaft*

KERNMAßNAHMEN

Die operativen Teilnehmer in der Arbeitsgruppe sollten in Absprache mit den unterstützenden Teilnehmern den **EU-Plan für die Reaktion auf Cybersicherheitsvorfälle und -krisen** auf der Grundlage der nationalen Pläne für die Reaktion auf Cybersicherheitsvorfälle und -krisen ausarbeiten. Der EU-Plan für die Reaktion auf Cybersicherheitsvorfälle und -krisen sollte Ziele

der Abwehrbereitschaft der EU, festgelegte Verfahren und sichere Kanäle für den Informationsaustausch vorsehen, darunter auch Methoden für den Umgang mit Informationen sowie Kriterien für die Aktivierung des Mechanismus für gegenseitige Unterstützung auf der Grundlage einer vereinbarten Klassifikationstaxonomie für Sicherheitsvorfälle und einer Liste der in der EU verfügbaren Fähigkeiten.

Am Ende von Stufe 2 sollte die Arbeitsgruppe ihre Bewertung der organisatorischen Aspekte der Gemeinsamen Cyber-Einheit sowie der Aufgaben und Zuständigkeiten der operativen Teilnehmer innerhalb dieser Plattform abgeschlossen haben. Die Arbeitsgruppe sollte die Ergebnisse dieser Bewertung der Kommission und dem Hohen Vertreter vorlegen, die diese Bewertung dem Rat übermitteln sollten. Die Kommission und der Hohe Vertreter sollten im Rahmen ihrer jeweiligen Zuständigkeiten auf der Grundlage dieser Bewertung in Zusammenarbeit einen gemeinsamen Bericht erstellen und den Rat ersuchen, diesen Bericht im Wege von Schlussfolgerungen des Rates zu billigen.

UNTERSTÜZUNGSMAßNAHMEN

Der EU-Plan für die Reaktion auf Cybersicherheitsvorfälle und -krisen sollte auf den Hauptelementen der nationalen Pläne für die Reaktion auf Cybersicherheitsvorfälle und -krisen aufbauen. Im Einklang mit dem Vorschlag der Kommission für eine Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148[1] sollten die Mitgliedstaaten nationale Pläne für die Reaktion auf Cybersicherheitsvorfälle und -krisen annehmen. In den nationalen Plänen, die einer gegenseitigen Begutachtung unterzogen werden könnten, sollten Ziele und Modalitäten für die Bewältigung von Cybersicherheitsvorfällen und -krisen großen Ausmaßes festgelegt werden. In den nationalen Plänen sollte insbesondere auf Folgendes eingegangen werden:

a. Ziele der Maßnahmen und Tätigkeiten für die nationale Abwehrbereitschaft,
b. Aufgaben und Verantwortlichkeiten der zuständigen nationalen Behörden,
c. nationale Krisenmanagementverfahren und Kanäle für den Informationsaustausch,
d. Festlegung der Maßnahmen für die Abwehrbereitschaft, einschließlich Übungen und Schulungen,
e. Identifizierung der einschlägigen öffentlichen und privaten Interessenträger und der betroffenen Infrastruktur,
f. die zwischen den einschlägigen nationalen Behörden und Stellen festgelegten nationalen Verfahren und Vereinbarungen, beispielsweise zwischen den Stellen, die für alle Cybergemeinschaften zuständig sind, damit die Mitgliedstaaten in der Lage sind, an der koordinierten Bewältigung von Cybersicherheitsvorfällen und -krisen großen Ausmaßes auf EU-Ebene effektiv mitzuwirken und diese zu unterstützen.

Auf der Grundlage der Beiträge der Mitgliedstaaten und der Organe, Einrichtungen und sonstigen Stellen der EU sollten die operativen Teilnehmer die folgenden Unterstützungsmaßnahmen im Rahmen der Gemeinsamen Cyber-Einheit wahrnehmen:

[1] COM(2020) 823 final 2020/0359 (COD), Brüssel, 16.12.2020.

a. Erstellung eines ersten integrierten Lageberichts der EU auf der Grundlage der nationalen Pläne für die Reaktion auf Cybersicherheitsvorfälle und -krisen,
b. Aufbau von Kommunikationsfähigkeiten und Instrumenten für den sicheren Informationsaustausch,
c. Moderierung der Annahme von Protokollen für die gegenseitige Unterstützung zwischen den Teilnehmern,
d. Organisation gemeinschaftsübergreifender Übungen und Schulungen für die in der EU-Liste über die verfügbaren operativen Fähigkeiten genannten Experten,
e. Entwicklung eines Mehrjahresplans zur Koordinierung von Übungen.

Bei Bedarf sollten die operativen Teilnehmer die unterstützenden Teilnehmer konsultieren. Die ENISA sollte mit Unterstützung der Kommission, von Europol und dem CERT-EU Kommunikationsfähigkeiten und Instrumente für den sicheren Informationsaustausch aufbauen und diesen so ermöglichen.

Damit die notwendigen Pläne fertiggestellt sind und die gemeinsamen Tätigkeiten aufgenommen werden können, sollten die für Stufe 2 festgelegten Kernmaßnahmen und möglichst auch die Unterstützungsmaßnahmen bis zum **30. Juni 2022 [6 Monate nach Abschluss von Stufe 1]** abgeschlossen sein.

3. *Stufe 3 – Aufnahme der Tätigkeit der Gemeinsamen Cyber-Einheit*

KERNMAßNAHMEN

Nachdem der Rat die Schlussfolgerungen der Kommission zu dem Bericht in Stufe 2 gebilligt hat, sollten die operativen Teilnehmer den Einsatz **schneller EU-Einsatzteams für Cybersicherheit** innerhalb der Gemeinsamen Cyber-Einheit koordinieren und eine **physische Plattform** einrichten, die es den Teams ermöglicht, technische und operative Tätigkeiten durchzuführen. Auf der Grundlage der Vorbereitungsarbeiten in Stufe 2 sollten die Teilnehmer den EU-Plan für die Reaktion auf Cybersicherheitsvorfälle und -krisen fertigstellen. Die operativen Teilnehmer sollten sicherstellen, dass die in der Liste der in der EU verfügbaren operativen Fähigkeiten aufgeführten Experten und Fähigkeiten auch zur Verfügung stehen und bereit sind, einen Beitrag zur Tätigkeit der schnellen EU-Einsatzteams für Cybersicherheit zu leisten.

Für die Umsetzung des EU-Plans für Cybersicherheitsvorfälle und -krisen sollten die Teilnehmer ein jährliches Arbeitsprogramm festlegen.

UNTERSTÜZUNGSMAßNAHMEN

Die gemeinsame Cyber-Einheit kann von der Cyberdiplomatiegemeinschaft in Anspruch genommen werden, um die öffentliche Kommunikation abzustimmen. Die Plattform kann es den Teilnehmern gestatten, an der politischen Zuweisung und der Zuweisung innerhalb des auf polizeilicher und justizieller Ebene eingesetzten strafrechtlichen Rahmens mitzuwirken. Darüber hinaus kann sie die Folgenbewältigung erleichtern und strukturierte Synergien mit nationalen und grenzüberschreitenden Monitoring- und Detektionsfähigkeiten ermöglichen.

Für die Einsatzfähigkeit der Gemeinsamen Cyber-Einheit sollten die für Stufe 3 festgelegten Kernmaßnahmen und möglichst auch die Unterstützungsmaßnahmen bis zum **31. Dezember 2022 [6 Monate nach Abschluss von Stufe 2]** abgeschlossen sein.

4. *Stufe 4 – Ausweitung der Zusammenarbeit innerhalb der Gemeinsamen Cyber-Einheit auf private Einrichtungen und Berichterstattung über die Fortschritte.*

KERNMAßNAHMEN

Die Teilnehmer der Gemeinsamen Cyber-Einheit sollten einen **Tätigkeitsbericht über die Fortschritte bei der Umsetzung der vier in der Empfehlung dargelegten Stufen erstellen, in dem die erzielten Fortschritte und Herausforderungen beschrieben werden**. Dieser Bericht sollte statistische Informationen über die in den vier Stufen durchgeführten Tätigkeiten der operativen Zusammenarbeit enthalten. Der Bericht sollte der Kommission und dem Hohen Vertreter vorgelegt werden.

UNTERSTÜZUNGSMAßNAHMEN

Damit den schnellen EU-Einsatzteams für Cybersicherheit noch mehr Fähigkeiten und Informationen zur Verfügung stehen, sollten die Teilnehmer sicherstellen, dass die Gemeinsame Cyber-Einheit beim Abschluss von **Vereinbarungen über den Informationsaustausch und die operative Zusammenarbeit zwischen Teilnehmern und Stellen des privaten Sektors**, die beispielsweise Bedrohungsanalysen und Sicherheitsvorfall-Notdienste bereitstellen, Unterstützung leistet. Sie sollten unter anderem auch sicherstellen, dass die Gemeinsame Cyber-Einheit in ihrem regelmäßigen Dialog und Informationsaustausch über Bedrohungen und Schwachstellen mit Nutzern von Cybersicherheitslösungen vor allem diejenigen Nutzer unterstützt, die in den Anwendungsbereich der NIS-Richtlinie fallen oder in den **Informationsaustausch- und -analysezentren (ISAC) auf EU-Ebene** erfasst werden.

Die Mitgliedstaaten sollten insbesondere diejenigen in ihrem Hoheitsgebiet tätigen Einrichtungen, die in den Anwendungsbereich der NIS-Richtlinie fallen, darin unterstützen, Zugang zu öffentlich-privaten Dialogen mit den ISAC auf EU-Ebene zu erhalten und selbst an diesen Dialogen mitzuwirken.

Im Interesse einer angemessenen Einbeziehung des Privatsektors sollten die für Stufe 4 festgelegten Kernmaßnahmen und möglichst auch die Unterstützungsmaßnahmen bis zum **30. Juni 2023 [6 Monate nach Abschluss von Stufe 3]** abgeschlossen sein.

WIE KÖNNEN DIE OPERATIVEN FÄHIGKEITEN DER EU RASCH MOBILISIERT WERDEN?

WER STELLT FÄHIGKEITEN BEREIT: Operative Teilnehmer

WER VERWALTET DIE FÄHIGKEITEN: Teilnehmer innerhalb der Gemeinsamen Cyber-Einheit im Einklang mit den vereinbarten Aufgaben und Zuständigkeiten

Stufe	Ziel	Aufgabe	Kernmaßnahme	Unterstützungsmaßnahme
Stufe 1 – Definition Bis **31. Dezember 2021 [6 Monate nach Annahme]**	ABWEHR-BEREITSCHAFT	**Ermittlung von Fähigkeiten**	**Operative Teilnehmer erstellen eine Liste der in der EU verfügbaren operativen Fähigkeiten.**	
Stufe 2 – Vorbereitung Bis zum **30. Juni 2022 [6 Monate nach Abschluss von Stufe 1]**	ABWEHR-BEREITSCHAFT	**Festlegung einschlägiger Verfahren und Modalitäten zur Aktivierung von Fähigkeiten im Bedarfsfall**	**Operative Teilnehmer bereiten auf der Grundlage der verabschiedeten nationalen Pläne den EU-Plan für die Reaktion auf Cybersicherheitskrisen (EU-Rahmen für die Reaktion auf Cybersicherheitskrisen - „Konzeptentwurf“) vor**	**Operative Teilnehmer erstellen integrierte Lageberichte der EU auf der Grundlage des technischen EU-Cybersicherheitslageberichts**
	ABWEHR-BEREITSCHAFT	**Übungsfähigkeiten**		**Teilnehmer organisieren gemeinsame Übungen und Schulungen (gemeinschaftsübergreifend)** **Teilnehmer arbeiten zwecks Koordinierung der Übungen einen Mehrjahresplan aus**

	LAGE-BEWUSSTSEIN	**Festlegung von Instrumenten für den Austausch von Informationen und Unterstützungsersuchen**		**Teilnehmer entwickeln einen sicheren und schnellen Informationsaustausch**
GEMEINSAME CYBER-EINHEIT (JCU) IST BETRIEBSBEREIT **Grundlage sind die Vorbereitungsarbeiten der Teilnehmer im Rahmen einer von der Kommission eingesetzten Arbeitsgruppe**				
Stufe 3 – Einsatz Bis zum **31. Dezember 2022 [6 Monate nach Abschluss von Stufe 2]**	ABWEHR-BEREITSCHAFT	**Verabschiedung einschlägiger Verfahren, Modalitäten und Absichtserklärungen zur Aktivierung von Fähigkeiten im Bedarfsfall**	**Operative Teilnehmer stellen den EU-Plan für die Reaktion auf Cybersicherheitskrisen fertig und definieren seine Umsetzung im Rahmen jährlicher Arbeitsprogramme**	**Teilnehmer unterstützen die Einrichtung nationaler und grenzüberschreitender Monitoring- und Detektionsfähigkeiten, auch von SOC**
	KOORDINIERTE REAKTION	**Einsatz von Fähigkeiten im Bedarfsfall**	**Operative Teilnehmer koordinieren schnelle EU-Einsatzteams für Cybersicherheit über die virtuelle und physische JCU-Plattform in Brüssel**	**Teilnehmer koordinieren die öffentliche Kommunikation und tragen zur politischen Zuweisung sowie zur Zuweisung im Rahmen der Strafjustiz bei.**
Stufe 4 – Ausweitung und Bericht	LAGEBE-WUSSTSEIN	**Gewährleistung der Skalierbarkeit durch Einbeziehung des**	**Teilnehmer legen unter Rückgriff auf statistische Informationen einen Tätigkeitsbericht über die**	**Teilnehmer schließen Vereinbarungen mit Cybersicherheitsanbietern über den Informationsaustausch sowie über**

Bis zum **30. Juni 2023 [6 Monate nach Abschluss von Stufe 3]**	KOORDINIERTE REAKTION	**Privatsektors, um den sich abzeichnenden Bedarf zu decken**	**erzielten Fortschritte, die Ergebnisse und Herausforderungen vor**	**die operative Zusammenarbeit** **Teilnehmer schließen Vereinbarungen über den Informationsaustausch vor allem mit solchen Nutzern, die in den Anwendungsbereich der NIS-Richtlinie und der EU-ISAC fallen**

BEGLAUBIGTE AUSFERTIGUNG
Für die Generalsekretärin

Martine DEPREZ
Direktorin
Entscheidungsprozess & Kollegialität
EUROPÄISCHE KOMMISSION