Rat der
Europäischen Union

Brüssel, den 7. September 2023
(OR. en)

12485/23
ADD 1

Interinstitutionelles Dossier:
2023/0318(NLE)

PROCIV 57	**ATO 48**
ENV 925	**CSC 408**
JAI 1084	**ECOFIN 839**
SAN 494	**CSCI 149**
COSI 140	**DATAPROTECT 216**
CHIMIE 85	**MI 698**
ENFOPOL 356	**CODEC 1500**
RECH 380	**COPS 418**
CT 133	**JAIEX 46**
DENLEG 38	**COPEN 292**
COTER 153	**IND 441**
RELEX 987	**POLMIL 221**
ENER 467	**IPCR 55**
HYBRID 53	**DIGIT 160**
TRANS 329	**DISINFO 62**
CYBER 203	**CSDP/PSDC 608**
TELECOM 251	**MARE 18**
ESPACE 45	**POLMAR 47**

ÜBERMITTLUNGSVERMERK

Absender:	Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	6. September 2023
Empfänger:	Frau Thérèse BLANCHET, Generalsekretärin des Rates der Europäischen Union
Nr. Komm.dok.:	COM(2023) 526 final
Betr.:	ANHANG des Vorschlags für eine Empfehlung des Rates für einen Konzeptentwurf zur Koordinierung der Reaktion – auf Unionsebene – auf Störungen kritischer Infrastrukturen von erheblicher grenzüberschreitender Bedeutung

Die Delegationen erhalten in der Anlage das Dokument COM(2023) 526 final.

Anl.: COM(2023) 526 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 6.9.2023
COM(2023) 526 final

ANNEX

ANHANG

des

Vorschlags für eine Empfehlung des Rates

für einen Konzeptentwurf zur Koordinierung der Reaktion – auf Unionsebene – auf Störungen kritischer Infrastrukturen von erheblicher grenzüberschreitender Bedeutung

ANHANG

In diesem Anhang werden die Grundsätze, Ziele, die zentralen Akteure, das Zusammenspiel mit bestehenden Krisenreaktionsmechanismen und die Funktionsweise eines Konzeptentwurfs für eine koordinierte Reaktion auf Störungen kritischer Infrastrukturen („Konzeptentwurf für kritische Infrastrukturen“) und eine bessere Zusammenarbeit zwischen den Mitgliedstaaten und den einschlägigen Organen, Einrichtungen und sonstigen Stellen der Union in Bezug auf solche Vorfälle im Einklang mit den geltenden Vorschriften und Verfahren beschrieben. Dieser Konzeptentwurf lässt die Rolle und Funktionsweise anderer Regelungen unberührt.

TEIL I: ZIELE, GRUNDSÄTZE, AKTEURE UND ANDERE INSTRUMENTE

1. Ziele

Mit dem Konzeptentwurf für kritische Infrastrukturen sollen die folgenden drei wichtigsten Ziele bei einer Reaktion auf einen erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen erreicht werden:

a) **eine gemeinsame Lageerfassung**, da ein fundiertes Verständnis des erheblichen Sicherheitsvorfalls bei kritischen Infrastrukturen in den Mitgliedstaaten, seines Ursprungs und seiner möglichen Folgen für alle relevanten Akteure auf operativer und strategischer/politischer Ebene für eine angemessene koordinierte Reaktion unabdingbar ist;

b) **eine koordinierte Unterrichtung der Öffentlichkeit**, da sie dazu beiträgt, negative Auswirkungen eines erheblichen Sicherheitsvorfalls bei kritischen Infrastrukturen abzumildern und Diskrepanzen bei den Informationen, die der Öffentlichkeit in den Mitgliedstaaten und zwischen den Mitgliedstaaten vermittelt werden, so gering wie möglich zu halten. Eine klare Unterrichtung der Öffentlichkeit ist auch wichtig, um die Folgen von Desinformation einzudämmen;

c) **eine wirksame Reaktion**, da eine verbesserte Reaktionsfähigkeit der Mitgliedstaaten und eine verstärkte Zusammenarbeit der Mitgliedstaaten und einschlägigen Organe, Einrichtungen und sonstigen Stellen der Union dazu beiträgt, die Auswirkungen eines erheblichen Sicherheitsvorfalls bei kritischen Infrastrukturen abzufedern und eine rasche Wiederherstellung wesentlicher Dienste ermöglicht, sodass die Anfälligkeit für weitere erhebliche Sicherheitsvorfälle reduziert wird.

2. Grundsätze

Verhältnismäßigkeit

Sicherheitsvorfälle, die kritische Infrastrukturen und/oder die Erbringung wesentlicher Dienste beeinträchtigen, liegen häufig unterhalb der Schwelle eines erheblichen Sicherheitsvorfalls bei kritischen Infrastrukturen wie in Abschnitt 2 dieser Empfehlung dargelegt. Daher können sie grundsätzlich auf nationaler Ebene wirksam angegangen werden. So beschränkt sich die Anwendung des Konzeptentwurfs für kritische Infrastrukturen auf erhebliche Sicherheitsvorfälle bei kritischen Infrastrukturen.

Subsidiarität

Im Einklang mit dem Unionsrecht sind vorrangig die Mitgliedstaaten dafür verantwortlich, auf Störungen bei kritischen Infrastrukturen oder bei den von kritischen Einrichtungen erbrachten wesentlichen Dienste zu reagieren. Den einschlägigen Organen, Einrichtungen und sonstigen Stellen der Union und dem Europäischen Auswärtigen Dienst (EAD) fällt eine

wichtige ergänzende Rolle im Falle eines erheblichen Sicherheitsvorfalls bei kritischen Infrastrukturen von erheblicher grenzüberschreitender Bedeutung zu, da ein solcher Vorfall mehrere oder sogar alle Bereiche des Wirtschaftslebens innerhalb des Binnenmarkts, das Leben der in der Union lebenden Bürgerinnen und Bürger, die Sicherheit und die internationalen Beziehungen der Union beeinträchtigen kann.

Komplementarität

Der Konzeptentwurf für kritische Infrastrukturen berücksichtigt und spiegelt die Funktionsweise der bestehenden Krisenbewältigungsmechanismen auf Unionsebene wider, darunter die Integrierte Regelung für die politische Reaktion auf Krisen (IPCR) des Rates, den internen Krisenkoordinierungsprozess der Kommission ARGUS, das Katastrophenschutzverfahren der Union (UCPM), das vom Zentrum für die Koordination von Notfallmaßnahmen (ERCC) unterstützt wird, und das Krisenreaktionsverfahren des EAD. Er stützt sich ferner auf sektorbezogene Vereinbarungen, einschließlich der Bestimmungen für das koordinierte Management von Cybersicherheitsvorfällen großen Ausmaßes gemäß der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates[1] und des Rahmens, der im Konzeptentwurf zur koordinierten Reaktion auf grenzüberschreitende Cybersicherheitsvorfälle und -krisen großen Ausmaßes („Cyber Blueprint“)[2] festgelegt ist, sowie auf das Netz der nationalen Anlaufstellen für den Verkehr[3] und das Krisenkoordinierungsgremium für die Europäische Luftfahrt[4].

Darüber hinaus baut der Konzeptentwurf für kritische Infrastrukturen auf den gemäß der Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates[5] eingerichteten Strukturen und Mechanismen auf und ist im Einklang damit anzuwenden, insbesondere was die Zusammenarbeit zwischen den zuständigen Behörden und mit der Kommission und innerhalb der Gruppe für die Resilienz kritischer Einrichtungen anbelangt. Er trägt auch den Zuständigkeiten der einschlägigen Organe, Einrichtungen und sonstigen Stellen der Union gemäß dem für diese geltenden Rechtsrahmen Rechnung. Die Krisenreaktionsmaßnahmen für kritische Infrastrukturen ergänzen andere Krisenmanagementmechanismen auf Unionsebene sowie auf nationaler und sektoraler Ebene, die die sektorübergreifende Koordinierung unterstützen.

Vertraulichkeit von Informationen

Der Konzeptentwurf für kritische Infrastrukturen berücksichtigt, wie wichtig es ist, dass die Vertraulichkeit von als Verschlusssache eingestuften und nicht als Verschlusssache eingestuften sensiblen Informationen in Bezug auf kritische Infrastrukturen und kritische Einrichtungen gewahrt bleibt.

---

1 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (ABl. L 333 vom 27.12.2022, S. 80).

2 Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen (ABl. L 239 vom 19.9.2017, S. 36).

3 Mitteilung der Kommission „Ein Notfallplan für den Verkehr“ (COM(2022) 211 final).

4 Eingerichtet nach Artikel 19 der Durchführungsverordnung (EU) 2019/123 der Kommission vom 24. Januar 2019 zur Festlegung detaillierter Durchführungsbestimmungen für die Netzfunktionen des Flugverkehrsmanagements.

5 Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates (ABl. L 333 vom 27.12.2022, S. 164).

3. Einschlägige Akteure

Jeder Mitgliedstaat und die unter den Buchstaben a bis e genannten einschlägigen Organe, Einrichtungen und sonstigen Stellen der Union entscheiden im Einklang mit den jeweils geltenden Vorschriften und Verfahren je nach betroffenem Sektor und Art des Vorfalls über die einschlägigen Akteure für jeden erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen.

a) Mitgliedstaaten

- zuständige Behörden (z. B. für kritische Infrastrukturen zuständige Behörden, einschlägige sektorale Behörden, gemäß Artikel 9 Absatz 2 der Richtlinie (EU) 2022/2557 benannte oder errichtete zentrale Anlaufstellen, gemäß Artikel 9 Absatz 1 der Richtlinie (EU) 2022/2557 benannte oder eingerichtete Behörden);

- gegebenenfalls das Europäische Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe) gemäß Artikel 16 der Richtlinie (EU) 2022/2555;

- die in Artikel 14 der Richtlinie (EU) 2022/2555 genannte Kooperationsgruppe;

- gegebenenfalls andere Interessenträger einschließlich Einrichtungen oder Personen des Privatsektors, z. B. Betreiber kritischer Infrastrukturen, einschließlich der als kritisch eingestuften Einrichtungen;

- für die Resilienz kritischer Infrastrukturen zuständige Minister und/oder Minister, die für die Sektoren zuständig sind, die am stärksten von dem betreffenden erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen betroffen sind.

b) der Rat

- der turnusmäßig wechselnde Vorsitz;

- die einschlägigen Arbeitsgruppen wie die Gruppe „Katastrophenschutz“ einschließlich der Untergruppe „Resilienz kritischer Einrichtungen“ (PROCIV-CER) und des Vorsitzes der einschlägigen Arbeitsgruppe(n) je nach betroffenem Sektor und Art des Vorfalls, wie die Horizontale Gruppe „Fragen des Cyberraums“ und die Horizontale Gruppe „Stärkung der Resilienz und Abwehr hybrider Bedrohungen“;

- AStV, das Politische und Sicherheitspolitische Komitee und die IPCR-Regelung, die alle vom Generalsekretariat des Rates unterstützt werden.

c) die Kommission, einschließlich Expertengruppen der Kommission

- benannte federführende Dienststelle (je nach betroffenem Sektor), die vom ERCC als rund um die Uhr operierendes Zentrum für die Krisenbewältigung und von der Generaldirektion Migration und Inneres als der in diesem Bereich zuständigen Dienststelle unterstützt wird, und bei einem sektorübergreifenden Vorfall die Generaldirektion Migration und Inneres sowie andere einschlägige Dienststellen der Kommission;

- die Generaldirektion Kommunikation und der Sprecherdienst;

- die Generaldirektion HERA, Europäische Behörde für die Krisenvorsorge und -reaktion bei gesundheitlichen Notlagen;

- die durch die Richtlinie (EU) 2022/2557 eingesetzte Gruppe für die Resilienz kritischer Einrichtungen unter dem Vorsitz eines Vertreters der Kommission (Generaldirektion

Migration und Inneres) und gegebenenfalls anderer einschlägiger Expertengruppen und -ausschüsse;

- das im Rahmen des Katastrophenschutzverfahrens der Union (UCPM) durch den Beschluss Nr. 1313/2013/EU des Europäischen Parlaments und des Rates[6] eingerichtete ERCC (rund um die Uhr operierende Plattform für das Management von Notsituationen im Rahmen des Katastrophenschutzverfahrens der Union in der Generaldirektion Europäischer Katastrophenschutz und humanitäre Hilfe);

- die in Artikel 14 der Richtlinie (EU) 2022/2555 genannte Kooperationsgruppe;

- das Zentrum für Cyberlageerfassung und -analyse;

- der in Artikel 4 der Richtlinie (EU) 2022/2371 genannte Gesundheitssicherheitsausschuss[7];

- das Generalsekretariat der Kommission (ARGUS-Sekretariat) und der (stellvertretende) Generalsekretär (ARGUS-Verfahren), Generaldirektion Humanressourcen (Direktion Sicherheit);

- andere einschlägige Expertengruppen der Kommission, die die Kommission bei der Koordinierung von Maßnahmen in Not- oder Krisensituationen unterstützen;

- andere Krisenmanagementnetze, einschließlich sektoraler Netze (z. B. Netz der von der Generaldirektion Mobilität und Verkehr verwalteten nationaler Verkehrskontaktstellen, der interinstitutionelle Krisenstab für Cybersicherheit[8], das Krisenkoordinierungsgremium für die Europäische Luftfahrt);

- die Präsidentin und/oder der/die zuständige Vizepräsident/in bzw. das bevollmächtigte Kommissionsmitglied.

d) EAD

- Single Intelligence Analysis Capability (Einheitliches Analyseverfahren, SIAC), bestehend aus dem Zentrum der Europäischen Union für Informationsgewinnung und Lageerfassung (IntCen) und die Abteilung Aufklärung des Militärstabs der EU (EUMS Int);

- das Krisenreaktionszentrum (CRC);

- der Hohe Vertreter der Union für Außen- und Sicherheitspolitik/Vizepräsident der Europäischen Kommission.

e) relevante Einrichtungen und Stellen der Union sowie einschlägige Agenturen der Union wie Europol, je nach betroffenem Bereich[9].

---

6 Beschluss Nr. 1313/2013/EU des Europäischen Parlaments und des Rates vom 17. Dezember 2013 über ein Katastrophenschutzverfahren der Union (ABl. L 347 vom 20.12.2013, S. 924).

7 Verordnung (EU) 2022/2371 des Europäischen Parlaments und des Rates vom 23. November 2022 zu schwerwiegenden grenzüberschreitenden Gesundheitsgefahren und zur Aufhebung des Beschlusses Nr. 1082/2013/EU (ABl. L 314 vom 6.12.2022, S. 26).

8 Eine informelle Gruppe, in der die zuständigen Kommissionsdienststellen, der EAD, die Agentur der Europäischen Union für Cybersicherheit (ENISA), das CERT-EU und Europol unter dem gemeinsamen Vorsitz der Generaldirektion Kommunikationsnetze, Inhalte und Technologien und des EAD vertreten sind.

9 Wie Europol; Bereich Verkehr: die Agentur der Europäischen Union für Flugsicherheit (EASA), die Europäische Agentur für die Sicherheit des Seeverkehrs (EMSA), die Europäische Eisenbahnagentur (ERA); Bereich Gesundheit: das Europäisches Zentrum für die Prävention und die Kontrolle von

4. Zusammenspiel mit anderen einschlägigen Krisenbewältigungsmechanismen und -instrumenten

Der Konzeptentwurf für kritische Infrastrukturen ist ein flexibles Instrument, mit dem verschiedene Maßnahmen erfasst werden, die teilweise oder vollständig unter Rückgriff auf unterschiedliche bestehende Regelungen erfolgen könnten, je nach Art und Schwere des erheblichen Sicherheitsvorfalls bei kritischen Infrastrukturen und der Notwendigkeit einer operativen, strategischen/politischen Koordinierung.

a) das Protokoll der EU für das operative Vorgehen bei der Abwehr hybrider Bedrohungen[10] (im Folgenden „EU-Protokoll“)

Das EU-Protokoll gilt im Falle hybrider Bedrohungen[11] und enthält eine Übersicht über die Verfahren und Instrumente, die im Falle solcher Bedrohungen oder Kampagnen Anwendung finden.

Im Falle eines erheblichen Sicherheitsvorfalls bei kritischen Infrastrukturen mit hybrider Dimension gilt das EU-Protokoll gegebenenfalls ergänzend zum Konzeptentwurf für kritische Infrastrukturen, z. B. für spezifische Informationen, Analysen oder die Kommunikation über hybride Aspekte des erheblichen Sicherheitsvorfalls bei kritischen Infrastrukturen und in Bezug auf die Zusammenarbeit mit externen Partnern.

b) Konzeptentwurf zur koordinierten Reaktion auf grenzüberschreitende Cybersicherheitsvorfälle und -krisen großen Ausmaßes

Dieser Konzeptentwurf beschäftigt sich mit Sicherheitsvorfällen großen Ausmaßes, die so große Störungen hervorrufen, dass der betroffene Mitgliedstaat sie allein nicht bewältigen kann, oder die so weitreichende und beträchtliche Auswirkungen von technischer oder politischer Tragweite auf zwei oder mehr Mitgliedstaaten oder EU-Organe haben, dass rasch koordinierte Maßnahmen zu treffen sind und auf Unionsebene politisch reagiert werden muss.

Im Falle eines erheblichen Sicherheitsvorfalls bei kritischen Infrastrukturen, der mit einem Cybersicherheitsvorfall großen Ausmaßes zusammenfällt oder damit in Zusammenhang zu stehen scheint, legen die zuständigen Arbeitsgruppen des Rates eine angemessene Koordinierung auf operativer Ebene fest, beispielsweise mit EU-CyCLONe oder durch eine gemeinsame Sitzung der Gruppe für die Resilienz kritischer Einrichtungen mit der Kooperationsgruppe. Zweck der Koordinierung ist festzustellen, welche Akteure, Instrumente oder Mechanismen am wirksamsten dazu beitragen könnten, auf erhebliche Sicherheitsvorfälle bei kritischen Infrastrukturen zu reagieren, wobei Doppelarbeit und parallele Arbeit zu vermeiden sind.

Krankheiten (ECDC) und die Europäische Arzneimittel-Agentur (EMA); Bereich Energie: die Agentur für die Zusammenarbeit der Energieregulierungsbehörden (ACER) Bereich Weltraum: die Agentur der Europäischen Union für das Weltraumprogramm (EUSPA), Lebensmittelsektor: Europäische Behörde für Lebensmittelsicherheit (EFSA) Auf See: Europäische Fischereiaufsichtsagentur (EFCA) Bereich Cybervorfälle: die Agentur der Europäischen Union für Cybersicherheit (ENISA), Computer Security Incident Response Teams (Reaktionsteam für Computersicherheitsverletzungen, CSIRT), das IT-Notfallteam für die Organe, Einrichtungen und sonstigen Stellen der EU (CERT-EU).

10 Joint Staff Working Document – EU Protocol for countering hybrid threats (SWD(2023) 116 final).

11 Hybride Bedrohungen können als Mischung von Zwang und Unterwanderung und von konventionellen und unkonventionellen Methoden beschrieben werden, auf die staatliche oder nichtstaatliche Akteure in koordinierter Weise zurückgreifen können, um bestimmte Ziele zu verfolgen, ohne dabei die Schwelle eines offiziell erklärten Kriegs zu erreichen, siehe EU-Protokoll über hybride Bedrohungen.

c) Katastrophenschutzverfahren der Union und Zentrum für die Koordination von Notfallmaßnahmen

Im Einklang mit dem Beschluss Nr. 1313/2013/EU über ein Katastrophenschutzverfahren der Union werden operative Reaktionen im Rahmen des Katastrophenschutzverfahrens der Union auf eingetretene oder unmittelbar bevorstehende Naturkatastrophen und vom Menschen verursachte Katastrophen innerhalb und außerhalb der Union (einschließlich die kritische Infrastruktur betreffende) vom ERCC, dem Zentrum für die Koordination von Notfallmaßnahmen, geleitet, der einzigen rund um die Uhr einsatzbereiten operativen Plattform der Kommission zur Krisenbewältigung. In solchen Fällen kann das ERCC Frühwarnungen, Meldungen, Analysen erstellen und den Informationsaustausch sowie im Falle einer Aktivierung des Katastrophenschutzverfahrens der Union durch einen Mitgliedstaat die Entsendung von operativer Hilfe und Experten in die betroffenen Gebiete unterstützen. Das ERCC kann darüber hinaus die sektorale und sektorübergreifende Koordinierung sowohl auf Unionsebene als auch zwischen der Union und den zuständigen nationalen Behörden, einschließlich der für den Katastrophenschutz und die Resilienz kritischer Infrastrukturen zuständigen Behörden, erleichtern.

d) andere sektorale oder sektorübergreifende Mechanismen und Instrumente

Der Konzeptentwurf für kritische Infrastrukturen überschneidet sich nicht mit anderen sektoralen oder sektorübergreifenden Krisenbewältigungsinstrumenten oder Koordinierungsmechanismen. Sind solche Instrumente oder Mechanismen in dem betroffenen Sektor bereits vorhanden, kann dieser Konzeptentwurf für kritische Infrastrukturen innerhalb seines Anwendungsbereichs als ergänzendes Instrument zu den sektoralen oder sektorübergreifenden Instrumenten oder Mechanismen verwendet werden, ersetzt diese jedoch nicht. Es gilt, die notwendige Koordinierung zwischen den verschiedenen Akteuren sicherzustellen, um solche Überschneidungen zu vermeiden. Dies könnte beispielsweise im Rahmen des internen Krisenkoordinierungsprozesses der Kommission ARGUS, unterstützt durch das ERCC, und/oder IPCR-Koordinierungssitzungen erreicht werden.

TEIL II: INFORMATIONSAUSTAUSCH UND KOORDINIERTE REAKTION

Die nachstehend beschriebenen Maßnahmen umfassen Formen der Zusammenarbeit, d. h. den Informationsaustausch, die koordinierte Kommunikation und Reaktion. Diese Struktur entspricht den Modalitäten der Integrierten EU-Regelung für die politische Reaktion auf Krisen (IPCR) und berücksichtigt im weiteren Sinne den potenziellen Einsatz der auf EU-Ebene bereits bestehenden Krisenkoordinierungsmechanismen. Diese Struktur zeigt, wie sich diese Formen der Zusammenarbeit integrieren würden, sofern sie genutzt werden. Die meisten dieser Maßnahmen können jedoch auch eigenständig ergriffen werden: Sie hängen nicht von der Anwendung dieser Regelung ab, sondern ergänzen sie. Die Maßnahmen werden in chronologischer Reihenfolge dargestellt, wobei zu berücksichtigen ist, dass in einem Krisenfall großen Ausmaßes, die einen erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen darstellt, mehrere Maßnahmen gleichzeitig und durchgängig durchgeführt werden können.

1. INFORMATIONSAUSTAUSCH

a) Operative Ebene

Die von einem erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen betroffenen Mitgliedstaaten wenden ihre eigenen Notfallmaßnahmen an, sorgen für die Koordinierung mit

den einschlägigen nationalen Krisenmanagementmechanismen und beziehen gegebenenfalls alle einschlägigen nationalen, regionalen und lokalen Akteure ein.

Soweit dies für die Katastrophenschutzhilfe erforderlich ist, wird die Koordinierung zwischen den Mitgliedstaaten und der Kommission über das ERCC im Rahmen des Katastrophenschutzverfahrens der Union sichergestellt.

i) Informationsaustausch und Meldung durch die zuständigen nationalen Behörden

Zusätzlich zu den Melde- und Informationspflichten gemäß Artikel 15 der Richtlinie (EU) 2022/2557 teilen die für kritische Infrastrukturen zuständigen nationalen Behörden in den von dem erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen betroffenen Mitgliedstaaten den turnusmäßig wechselnden Vorsitz des Rates und der Kommission über ihre zentralen Anlaufstellen unverzüglich die einschlägigen Informationen mit, die sie von Betreibern kritischer Infrastrukturen, von kritischen Einrichtungen oder aus anderen Quellen erhalten haben, und unterrichten sie über aktivierte Krisenmanagementmechanismen. Das ERCC gewährleistet für die Kommission rund um die Uhr eine operierende Kontaktstelle und Kapazitäten und koordiniert, überwacht und unterstützt in Echtzeit die Reaktion auf Notfälle auf Unionsebene und dient den Mitgliedstaaten und der Kommission als operierende Plattform zur Krisenbewältigung und fördert einen sektorübergreifenden Ansatz für das Katastrophenmanagement.

Ein solcher Informationsaustausch betrifft die Art des erheblichen Sicherheitsvorfalls bei kritischen Infrastrukturen, seine Ursache, die festgestellten oder geschätzten Auswirkungen der Störung auf kritische Infrastrukturen und die Erbringung wesentlicher Dienste, die Folgen des Sicherheitsvorfalls über Sektoren und Grenzen hinweg und die Abhilfemaßnahmen, die auf nationaler Ebene oder mit den jeweiligen Mitgliedstaaten und der Kommission im Rahmen bestehender Vereinbarungen, z. B. die Vereinbarungen über den Informationsaustausch gemäß den Artikeln 9 und 15 der Richtlinie (EU) 2022/2557 geplant sind oder bereits getroffen wurden. Diese Meldung sollte nicht dazu führen, dass Ressourcen kritischer Infrastrukturen oder in einigen Fällen die eines Mitgliedstaats durch Maßnahmen im Zusammenhang mit dem Umgang mit Sicherheitsvorfällen, denen Vorrang einzuräumen ist, abgezweigt werden.

Zur Gewährleistung von Folgemaßnahmen unterrichten das ERCC oder die benachrichtigten Kommissionsdienststellen, die für den jeweiligen Sektor bzw. die Sektoren zuständig sind, in dem/denen der erhebliche Sicherheitsvorfall bei kritischen Infrastrukturen eintrat, die Kontaktstelle in der Generaldirektion Migration und Inneres und das Generalsekretariat der Kommission. Falls nicht bereits geschehen, beginnt das ERCC zwischenzeitlich Beobachtungsmaßnahmen, insbesondere falls das Katastrophenschutzverfahren der Union durch einen oder mehrere der betroffenen Mitgliedstaaten aktiviert wurde.

Wenn die Informationen Cybersicherheitsaspekte betreffen oder sich auf einen Cybersicherheitsvorfall beziehen könnten, tauscht die Kommission einschlägige Informationen mit EU-CyCLONe aus.

Die gemäß der Richtlinie (EU) 2022/2557 zuständigen nationalen Behörden sollten im Zusammenhang mit Cybersicherheitsvorfällen und Sicherheitsvorfällen, die kritische Einrichtungen betreffen, nach Maßgabe der Richtlinie (EU) 2022/2555 mit den zuständigen Behörden unverzüglich zusammenarbeiten und Informationen austauschen, unter anderem auch zu den von kritischen Einrichtungen ergriffenen Cybersicherheitsmaßnahmen und physischen Maßnahmen.

Im maritimen Bereich sollten die zuständigen nationalen Behörden die Möglichkeit prüfen, den gemeinsamen Informationsraum (CISE) zu nutzen, um unverzüglich Informationen auszutauschen.

ii) Organisation von Sachverständigensitzungen

Die Kommission beruft so bald als möglich die Gruppe für die Resilienz kritischer Einrichtungen ein, um den Austausch einschlägiger Informationen zwischen den für kritische Infrastrukturen zuständigen nationalen Behörden und den einschlägigen Organen, Einrichtungen und sonstigen Stellen der Union über den Vorfall (Art, Ursache, Auswirkungen und Folgen über Sektoren und Grenzen hinweg) und über Reaktionsmaßnahmen, einschließlich Abhilfemaßnahmen und technischer Unterstützung für die betroffenen Mitgliedstaaten, zu erleichtern. Je nach Schwere des Sicherheitsvorfalls werden die zuständigen Kommissionsdienststellen eng in die Sitzung der Gruppe für die Resilienz kritischer Einrichtungen einbezogen, um die im Rahmen bestehender sektoraler Instrumente erfassten Informationen auszutauschen. Bei Sicherheitsvorfällen mit einer Kombination sowohl cyberbezogener als auch physischer, nicht cyberbezogener Aspekte unterrichten und konsultieren und unterrichten sich die zuständigen Kommissionsdienststellen, das CERT-EU und erforderlichenfalls der EAD so bald als möglich im Rahmen des Krisenstabs für Cybersicherheit, ebenso werden die jeweiligen Vorsitzenden der in Artikel 14 der Richtlinie (EU) 2022/2555 genannten Kooperationsgruppe und gegebenenfalls EU-CyCLONe bezüglich der Notwendigkeit von Koordinierungsmaßnahmen informiert. Im Einvernehmen mit den jeweiligen Vorsitzenden kann die Kommission (Generaldirektion Migration und Inneres und Generaldirektion Kommunikationsnetz, Inhalte und Technologien) eine gemeinsame Sitzung der Gruppe für die Resilienz kritischer Einrichtungen mit der Kooperationsgruppe vorschlagen, um eine gemeinsame Lageerfassung und entsprechende Reaktionen zu koordinieren.

Bei einem erheblichen sektorübergreifenden Sicherheitsvorfall bei kritischen Infrastrukturen, der eine Folgenbewältigung auf Unionsebene erfordert oder voraussichtlich erfordern wird, kann die Kommission sektorübergreifende Koordinierungssitzungen mit allen einschlägigen Interessenträgern einberufen.

Ist ein Drittstaat ebenfalls von einem erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen betroffen, so konsultiert die Kommission die zuständige Behörde des betroffenen Drittstaats und kann sie zu einer Sitzung der Gruppe für die Resilienz kritischer Einrichtungen einladen.

iii) Unterstützung durch die Kommission und die Agenturen der Union

Gegebenenfalls legt Europol im Einklang mit seinem Mandat einen Lagebericht über Sicherheitsvorfälle auf Unionsebene vor. Andere Agenturen der Union übermitteln ihrer jeweiligen „Mutter“-Generaldirektion gegebenenfalls und im Einklang mit ihren jeweiligen Mandaten einschlägige Informationen, die zur Lageerfassung in Bezug auf den erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen oder zur koordinierten Reaktion darauf beitragen, die ihrerseits wiederum der Kommission Bericht erstattet (Generaldirektion Migration und Inneres als Vorsitz der Gruppe für die Resilienz kritischer Einrichtungen).

Die Kommission kann gegebenenfalls und im Einklang mit dem geltenden Rechtsrahmen einen Beitrag zur Lageerfassung unter Nutzung der Ressourcen des Weltraumprogramms der Union[12] wie Copernicus, Galileo und EGNOS leisten.

b) Strategische Ebene

i) Erstellung von Berichten zur Lageerfassung

Auf der Grundlage von Informationen, die von den zuständigen nationalen Behörden in einer Sitzung der Gruppe für die Resilienz kritischer Einrichtungen oder gemeinsamen Sitzungen mit einschlägigen Dienststellen, Expertengruppen oder Netzen ausgetauscht werden, erstellt die Kommission auf Basis der Beiträge der zuständigen nationalen Behörden und anderer verfügbarer Informationen einen Bericht zur Lageerfassung.

Dieser Bericht sollten gegebenenfalls den Ergebnissen der einschlägigen Risikobewertungen, -evaluierungen und -szenarien auf EU-Ebene unter dem Gesichtspunkt der Cybersicherheit Rechnung tragen, darunter jenen, die von der Kommission, dem Hohen Vertreter der Union für Außen- und Sicherheitspolitik und der Kooperationsgruppe durchgeführt wurden.

Im Falle der Aktivierung der IPCR-Regelung kann dieser Bericht zur Integrierten Lageerfassungsanalyse (ISAA) beitragen, die von den Kommissionsdienststellen und dem EAD erstellt wird.

Mithilfe des SIAC wird gegebenenfalls eine aktuelle erkenntnisgestützte Bewertung des Sicherheitsvorfalls vorgelegt.

ii) Aktivierung der Krisenkoordinierungsmechanismen der Union und Nutzung von Unionsinstrumenten

Das ERCC beginnt mit der Unterstützung der Lageerfassung im Zusammenhang mit dem Sicherheitsvorfall, sofern dies relevant ist, insbesondere wenn mit dem Ereignis das Katastrophenschutzverfahren der Union ausgelöst wird.[13] Darüber hinaus können die betroffenen Mitgliedstaaten Satellitenbilder ihres Hoheitsgebiets über den Copernicus-Katastrophen- und Krisenmanagementdienst anfordern.

Wenn es für den Informationsaustausch zwischen der Kommission und dem EAD sowie den einschlägigen Agenturen der Union zweckmäßig erscheint, leitet die federführende Generaldirektion oder die Generaldirektion Migration und Inneres in Abstimmung mit dem Generalsekretariat den internen Krisenkoordinierungsprozess der Kommission ARGUS Phase I ein, indem sie ein Ereignis im Argus-IT-Instrument öffnet.

Der turnusmäßig wechselnde Vorsitz des Rates der Union kann die IPCR-Regelung im Informationsaustausch-Modus aktivieren, was dazu führt, dass die Kommission und der EAD ISAA-Berichte mit Beiträgen der zuständigen nationalen Behörden und gegebenenfalls anderer Quellen ausarbeiten. Auch ohne Aktivierung der IPCR-Regelung kann unter bestimmten Bedingungen eine Beobachtungswebsite auf der IPCR-Internet-Plattform vom turnusmäßig wechselnden Ratsvorsitz oder von der Kommission eingerichtet werden.

---

[12] Verordnung (EU) 2021/696 des Europäischen Parlaments und des Rates vom 28. April 2021 zur Einrichtung des Weltraumprogramms der Union und der Agentur der Europäischen Union für das Weltraumprogramm und zur Aufhebung der Verordnungen (EU) Nr. 912/2010, (EU) Nr. 1285/2013 und (EU) Nr. 377/2014 sowie des Beschlusses Nr. 541/2014/EU (ABl. L 170 vom 12.5.2021, S. 69).

[13] Wie die Veröffentlichung von Medienbeobachtungsprodukten, Katastrophenschutzmitteilungen, Kurzanalysen, ECHO Daily Maps, ECHO Daily Flashes und anderen maßgeschneiderten Produkten.

Andere (sektorale) Krisenbewältigungsmechanismen und -instrumente der Union können gegebenenfalls nach Maßgabe der jeweiligen Verfahren aktiviert werden. Die Kommission gewährleistet die Koordinierung zwischen diesen Mechanismen und Instrumenten.

Fällt der physische Sicherheitsvorfall mit einem Cybersicherheitsvorfall großen Ausmaßes im Sinne von Artikel 6 Nummer 7 der Richtlinie (EU) 2022/2555 zusammen bzw. scheint damit in Zusammenhang zu stehen, so kann der turnusmäßig wechselnde Ratsvorsitz den Cyber Blueprint dazu nutzen, eine angemessene Koordinierung auf operativer Ebene festzulegen, an der unter anderem EU-CyCLONe und die Gruppe für die Resilienz kritischer Einrichtungen beteiligt sind.

iii) Koordinierung der Unterrichtung der Öffentlichkeit

Die von einem erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen betroffenen Mitgliedstaaten stimmen ihre Unterrichtung der Öffentlichkeit über die Krise so weit wie möglich ab, wobei sie nationale Zuständigkeiten achten. Gegebenenfalls kann das im Rahmen der IPCR-Regelung eingerichtete informelle Krisenkommunikationsnetz einbezogen werden.

Auf der Grundlage der gemeinsamen Lageerfassung stimmen die Gruppe für die Resilienz kritischer Einrichtungen und die betroffenen Mitgliedstaaten gegebenenfalls die Ausarbeitung von Informationen zur Unterrichtung der Öffentlichkeit miteinander ab.

Europol und andere einschlägige Agenturen der Union koordinieren ihre Öffentlichkeitsarbeit auf der Grundlage einer gemeinsamen Lageerfassung mit dem Sprecherdienst der Kommission.

Wenn der erhebliche Sicherheitsvorfall bei kritischen Infrastrukturen externe oder hybride Aspekte oder Aspekte der Gemeinsamen Sicherheits- und Verteidigungspolitik umfasst, wird die Unterrichtung der Öffentlichkeit mit dem EAD und dem Sprecherdienst der Kommission im Einklang mit dem Protokoll der EU für das operative Vorgehen bei der Abwehr hybrider Bedrohungen[14] koordiniert.

2. REAKTION (UNTER EINBEZIEHUNG DER IM ABSCHNITT INFORMATIONSAUSTAUSCH BESCHRIEBENEN DURCHGÄNGIGEN MAßNAHMEN UND DER ZUSÄTZLICHEN MAßNAHMEN AUF STRATEGISCHER/POLITISCHER EBENE)

a) Strategische Ebene

i) Fortlaufende Erstellung von Lageberichten

Die Ratsgruppe „Katastrophenschutz – Resilienz kritischer Einrichtungen“ (PROCIV-CER) wird über die Erstellung eines politisch-strategischen Lageberichts (z. B. die ISAA im Falle einer Aktivierung der IPCR-Regelung oder den von der Kommission erstellten gemeinsamen Lagebericht) unterrichtet und bereitet die Sitzung des AStV, falls dieser noch nicht einberufen wurde, oder gegebenenfalls die Sitzung des Politischen und Sicherheitspolitischen Komitees vor.

Im Rahmen des SIAC werden die Kontakte zu den Nachrichtendiensten der Mitgliedstaaten intensiviert, die Informationen aus allen Quellen zusammengefasst und eine Analyse und eine Bewertung des Sicherheitsvorfalls sowie erforderlichenfalls regelmäßige Aktualisierungen erstellt.

ii) Vollständige Aktivierung der Krisenkoordinierungsmechanismen der Union und Nutzung von Unionsinstrumenten

[14] Joint Staff Working Document – EU Protocol for countering hybrid threats (SWD(2023) 116 final).

Falls die Präsidentin der Kommission den internen Krisenkoordinierungsprozess der Kommission ARGUS Phase II in Gang setzt, werden kurzfristig Sitzungen des Krisenkoordinierungsausschusses, an denen die zuständigen Dienststellen, Agenturen und gegebenenfalls der EAD beteiligt sind, einberufen, um die Koordinierung in Bezug auf alle Aspekte des erheblichen Sicherheitsvorfalls bei kritischen Infrastrukturen zu gewährleisten.

Sollte die IPCR-Regelung vom Ratsvorsitz vollständig aktiviert werden:

- beruft der turnusmäßig wechselnde Ratsvorsitz ein zeitnahes informelles Rundtischgespräch ein, an dem die einschlägigen nationalen, europäischen und internationalen Akteure teilnehmen, wobei der Vertreter der Kommission, der als Vorsitzender der Gruppe für die Resilienz kritischer Einrichtungen (Generaldirektion Migration und Inneres) fungiert, über die zuvor einberufene(n) Sitzung(en) der Gruppe berichten kann; gegebenenfalls kommen andere Kommissionsdienststellen und der EAD ergänzend hinzu;

- das SIAC und die einschlägigen Agenturen der Union können ersucht werden, im Rahmen der Gespräche aktuelle Informationen über die Lage in Bezug auf den erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen vorzulegen.

Die federführende Dienststelle der ISAA (federführende Dienststelle der Kommission oder der EAD) erstellt den ISAA-Bericht mit Beiträgen der zuständigen Kommissionsdienststellen, der einschlägigen Ämter, Einrichtungen und sonstigen Stellen der Union und der zuständigen nationalen Behörden. Die Mitgliedstaaten werden ersucht, über die IPCR-Internet-Plattform Beiträge zu den ISAA-Berichten zu leisten.

Bei einem erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen mit internationaler Sicherheitsrelevanz können die Kommissionsdienststellen und der EAD einen strukturierten Dialog zwischen der EU und der NATO über Resilienz einberufen, um zur gemeinsamen Lageerfassung und zum Informationsaustausch über die von der Union bzw. der NATO ergriffenen Maßnahmen beizutragen.

iii) Unterrichtung der Öffentlichkeit

Der Rat arbeitet gemeinsame Botschaften für die Unterrichtung der Öffentlichkeit aus. Dabei kann er von dem im Rahmen der IPCR eingerichteten informellen Krisenkommunikationsnetz unterstützt werden. Der Sprecherdienst der Kommission bereitet gegebenenfalls auch Botschaften für die Unterrichtung der Öffentlichkeit aus.

Wenn der erhebliche Sicherheitsvorfall bei kritischen Infrastrukturen externe oder hybride Aspekte oder Aspekte der Gemeinsamen Sicherheits- und Verteidigungspolitik umfasst, wird die Unterrichtung der Öffentlichkeit mit dem EAD und dem Sprecherdienst der Kommission abgestimmt.

iv) Unterstützung der Mitgliedstaaten und wirksame Reaktion

Der turnusmäßig wechselnde Vorsitz kann eine Sitzung des PROCIV-CER einberufen, um die Tätigkeiten im Rahmen der IPCR-Regelung zu unterstützen, sofern diese Regelung aktiviert ist.

Die von dem erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen betroffenen Mitgliedstaaten können über die Gruppe für die Resilienz kritischer Einrichtungen die technische Unterstützung anderer Mitgliedstaaten oder der einschlägigen Organe, Einrichtungen und sonstigen Stellen der Union anfordern, z. B. spezifisches Fachwissen zur Eindämmung nachteiliger Auswirkungen des erheblichen Sicherheitsvorfalls.

Die von dem erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen betroffenen Mitgliedstaaten können auch die Kommission oder einschlägige Agenturen der Union um

technische und/oder finanzielle Unterstützung ersuchen. In Abstimmung mit den zuständigen Agenturen der Union bewertet die Kommission eine mögliche Unterstützung und aktiviert gegebenenfalls im Einklang mit ihren jeweiligen Verfahren technische Abhilfemaßnahmen auf Unionsebene und koordiniert die technischen Kapazitäten, die erforderlich sind, um die Auswirkungen des erheblichen Sicherheitsvorfalls bei kritischen Infrastrukturen zu beenden oder zu verringern.

Insbesondere im Rahmen des Katastrophenschutzverfahrens der Union könnten die betroffenen Länder Unterstützung über das Gemeinsame Kommunikations- und Informationssystem für Notfälle (CECIS) anfordern, woraufhin das ERCC die Bereitstellung von Unterstützung durch die Mitgliedstaaten und die Teilnehmerstaaten des Katastrophenschutzverfahrens der Union sowie über rescEU koordinieren würde.

Im Rahmen ihrer jeweiligen Mandate und auf Ersuchen unterstützen Europol und andere einschlägige Agenturen der Union die von einem erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen betroffenen Mitgliedstaaten bei der Untersuchung des Sicherheitsvorfalls.

b) Politische Ebene

Der Ratsvorsitz könnte prüfen, ob es notwendig ist, IPCR-Rundtischgespräche, Sitzungen von Ratsarbeitsgruppen, den AStV, den Ministerrat und/oder Gipfeltreffen einzuberufen, um sich über die mögliche Ursache und die erwarteten Folgen des schwerwiegenden Sicherheitsvorfalls bei kritischen Infrastrukturen für die Mitgliedstaaten und die Union auszutauschen, gemeinsame Leitlinien festzulegen und die erforderlichen Maßnahmen zu ergreifen, um die von dem erheblichen Sicherheitsvorfall bei kritischen Infrastrukturen betroffenen Mitgliedstaaten zu unterstützen und dessen Auswirkungen abzumildern.

Abbildung 1: Schematischer Überblick über den Konzeptentwurf für kritische Infrastrukturen

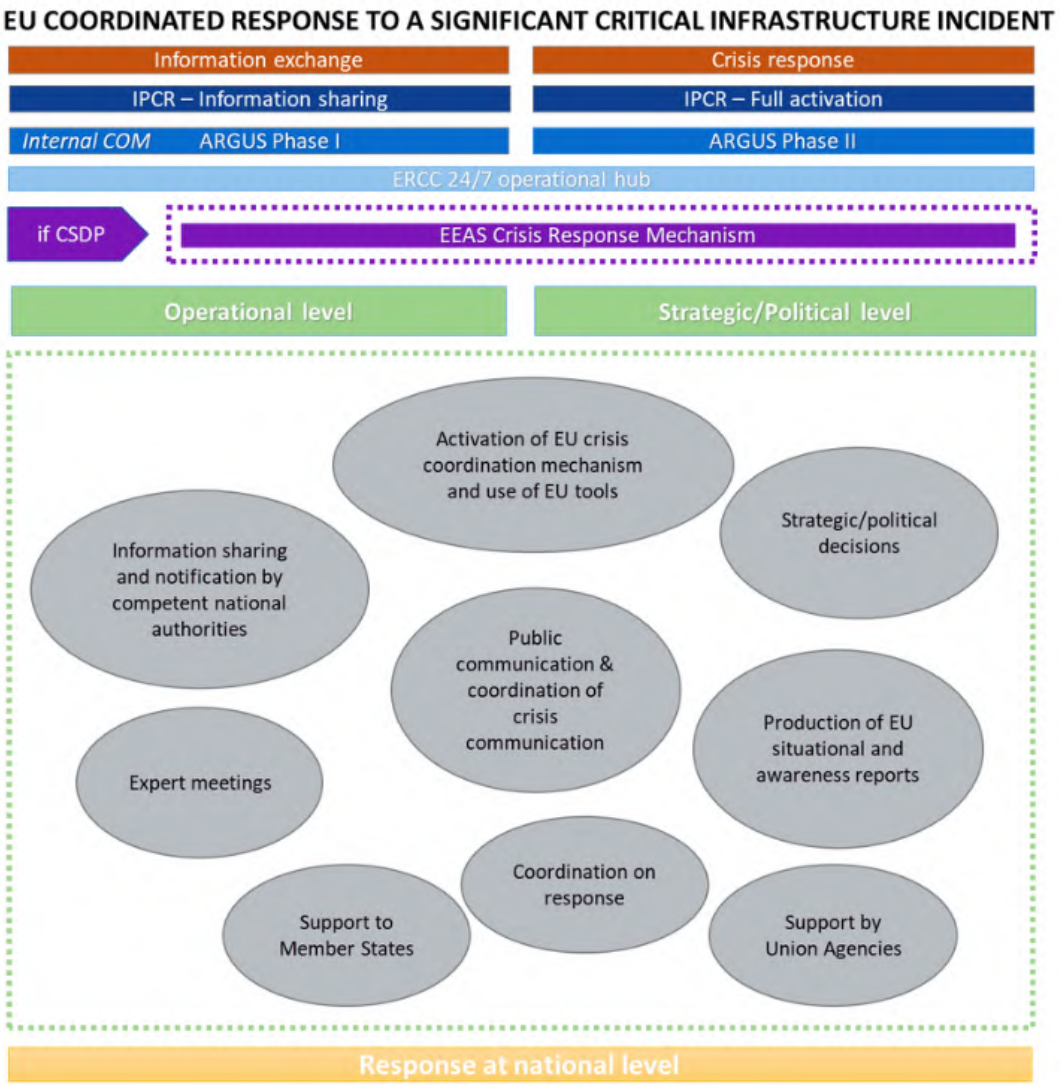

Abbildung 2: Beschluss über den Konzeptentwurf für kritische Infrastrukturen