Europäisches Parlament
2019-2024

Ausschuss für Verkehr und Tourismus

2023/0109(COD)

25.10.2023

STELLUNGNAHME

des Ausschusses für Verkehr und Tourismus

für den Ausschuss für Industrie, Forschung und Energie

zu dem Vorschlag für eine 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
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Verfasser der Stellungnahme: Gheorghe Falcă

PA_Legam

KURZE BEGRÜNDUNG

Organisationen, die von Cyberangriffen betroffen sind, auch im Verkehrssektor, melden diese selten, insbesondere Unternehmen des Privatsektors, da sie in ihren Augen eher „schlechte Werbung“ sind. Die meisten Organisationen ziehen es vor, intern mit ihnen umzugehen, und oft sind es die Angreifer, die sie öffentlich machen. Die gute Nachricht für die EU ist, dass mit dem Inkrafttreten der Richtlinie 2022/2555 über Netzsicherheit (bekannt als „NIS-2-Richtlinie“), die die Mitgliedstaaten bis Oktober 2024 umsetzen müssen, die Verpflichtungen zur Meldung von Sicherheitsvorfällen in allen Mitgliedstaaten harmonisiert werden. Daher dürfte sich in den kommenden Jahren ein besseres Verständnis von Art und Ausmaß des Problems herausbilden.

Die Agentur der Europäischen Union für Cybersicherheit (ENISA) veröffentlichte kürzlich einen Bericht[1] mit Informationen über Cybersicherheitsbedrohungen im Verkehrssektor, in dem sie betont, dass Cyberkriminelle für mehr als die Hälfte der im Berichtszeitraum 2022 beobachteten Vorfälle (55 %) verantwortlich waren und dass die Hauptmotivation für diese Angriffe ein finanzieller Gewinn war. Sie stellt ferner fest, dass die meisten Cyberangriffe im Verkehrssektor auf IT-Systeme abzielen, wodurch Betriebsstörungen verursacht werden.

Im Hinblick auf die Abwehrbereitschaft und Reaktion auf Cybersicherheitsvorfälle gibt es derzeit nur wenig Unterstützung auf Unionsebene und eine begrenzte Solidarität zwischen den Mitgliedstaaten. In den Schlussfolgerungen des Rates vom Mai 2022 wurde hervorgehoben, dass diese Lücken angegangen werden müssen, und hierzu die Kommission aufgefordert, einen Vorschlag für einen neuen **Cybersicherheits-Notfallfonds**[2] vorzulegen.

Mit dieser Verordnung wird die im Dezember 2020 angenommene **EU-Cybersicherheitsstrategie** umgesetzt, in der die Schaffung eines **europäischen Cyberschutzschilds** angekündigt wurde, mit dem die Fähigkeiten zur Erkennung von Cyberbedrohungen und zum Informationsaustausch in der Europäischen Union durch einen Zusammenschluss nationaler und grenzübergreifender Sicherheitseinsatzzentren (Security Operations Centres, SOCs) gestärkt werden sollen. Die Maßnahmen dieser Verordnung werden **im Rahmen des strategischen Ziels „Cybersicherheit“ des Programms Digitales Europa unterstützt**.

Die Gesamtmittelausstattung enthält eine Aufstockung um 100 Mio. EUR, indem – wie in dieser Verordnung vorgeschlagen – Mittel aus anderen strategischen Zielen des Programms Digitales Europa umgeschichtet werden. Damit erhöht sich der neue Gesamtbetrag, der für Cybersicherheitsmaßnahmen im Rahmen des Programms Digitales Europa zur Verfügung steht, auf 842,8 Mio. EUR.

Ein Teil der zusätzlichen 100 Mio. EUR wird in das vom Europäischen Kompetenzzentrum für Cybersicherheit (European Cybersecurity Competence Centre, ECCC) verwaltete Budget für die Durchführung von Maßnahmen in Bezug auf SOCs und auf die Abwehrbereitschaft im Rahmen des bzw. der Arbeitsprogramme einfließen. Darüber hinaus werden die zusätzlichen

[1] „Understanding Cyber Threats in Transport“ (Cyberbedrohungen im Verkehr verstehen), ENISA, veröffentlicht am 21. März 2023.
[2] Schlussfolgerungen des Rates zur Entwicklung der Cyberabwehr der Europäischen Union vom 23. Mai 2022 (Dok. 9364/22).

Mittel dazu dienen, die Einrichtung der EU-Cybersicherheitsreserve zu unterstützen. Sie ergänzen die bereits für ähnliche Maßnahmen im Arbeitsprogramm für das Hauptprogramm Digitales Europa und das strategische Ziel „Cybersicherheit“ für den Zeitraum 2023-2027 vorgesehenen Mittel, wodurch sich der Gesamtbetrag für den Zeitraum 2023-2027 auf 551 Mio. EUR erhöhen könnte, während 115 Mio. EUR bereits für Pilotprojekte im Zeitraum 2021-2022 eingesetzt wurden. Einschließlich der Beiträge der Mitgliedstaaten könnte sich das Gesamtbudget auf bis zu 1,109 Mrd. EUR belaufen.

Standpunkt des Verfassers

Der neue Vorschlag wird begrüßt, und es wird die Ansicht vertreten, dass er den verschiedenen Interessenträgern erhebliche Vorteile bringen wird. Betont wird, dass ein tieferes Verständnis der Cybersicherheitsbedürfnisse und -anforderungen im Verkehrssektor erforderlich ist und dass kritische Verkehrseinheiten Zugang zu angemessenen Finanzmitteln für die Abwehrbereitschaft, die Reaktion auf und die Bewältigung von Sicherheitsvorfällen erhalten müssen.

Das „Instrumentarium für die Cybersicherheit im Verkehrssektor“, mit dem ein Beitrag zu einem höheren Maß an Cybersicherheitsbewusstsein und Cyberhygiene geleistet werden soll, wird unterstützt, wobei ein besonderer Schwerpunkt auf dem Verkehrssektor liegt. Es richtet sich an Verkehrsorganisationen, unabhängig von ihrer Größe und ihrem Tätigkeitsbereich, und umfasst kritische Verkehrsinfrastrukturen und militärische Mobilität, insbesondere vor dem Hintergrund des Krieges in der Ukraine, vor allem, aber nicht beschränkt auf:

- Luftfahrtunternehmen, Flughafenleitungsorgane, Flughäfen des Kernnetzes, Flugverkehrsmanagement- und Flugverkehrskontrollzentren, die Agentur der Europäischen Union für Flugsicherheit und Eurocontrol;
- Infrastrukturbetreiber, Eisenbahnunternehmen und das Europäische Eisenbahnverkehrsleitsystem (ERTMS);
- Personen- und Frachtbeförderungsunternehmen der Binnen-, See- und Küstenschifffahrt, Leitungsorgane von Häfen einschließlich ihrer Hafenanlagen, Einrichtungen, die innerhalb von Häfen befindliche Anlagen und Ausrüstung betreiben, Betreiber von Schiffsverkehrsdiensten;
- Straßenverkehrsbehörden, die für die Kontrolle des Verkehrsmanagements zuständig sind, Betreiber intelligenter Verkehrssysteme;
- Post- und Kurierdienste.

Es wird die Ansicht vertreten, dass der Umfang der Mittel für die Funktionsweise des **Notfallfonds für Cybersicherheit** (ERFC) den Erfolg des Fonds bestimmen wird; daher sollten die Mittel ausreichend hoch sein, um die Mitgliedstaaten bei der **Vorsorge für, der Bewältigung von und der sofortigen Wiederherstellung nach** schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes zu unterstützen. Auch die Organe, Einrichtungen und sonstigen Stellen der Union werden Unterstützung für die Bewältigung von Vorfällen erhalten.

Der **Europäische Cyberschutzschild** wird die Fähigkeiten der Mitgliedstaaten zur Erkennung von Cyberbedrohungen verbessern. Der **Cybernotfallmechanismus** wird die Maßnahmen der

Mitgliedstaaten durch eine Soforthilfe bei der Abwehrbereitschaft, Reaktion und sofortigen Wiederherstellung bzw. Wiederaufnahme des Betriebs wesentlicher Dienste ergänzen.

ÄNDERUNGSANTRÄGE

Der Ausschuss für Verkehr und Tourismus ersucht den federführenden Ausschuss für Industrie, Forschung und Energie, folgende Änderungsanträge zu berücksichtigen:

Änderungsantrag 1

Vorschlag für eine Verordnung
Erwägung 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die Tragweite, die Häufigkeit und die Auswirkungen von Cybersicherheitsvorfällen nehmen zu, was auch Cyberangriffe im Zusammenhang mit Cyberspionage, Ransomware oder Störungen einschließt. Sie stellen eine große Bedrohung für das Funktionieren von Netz- und Informationssystemen dar. Angesichts der sich wandelnden Bedrohungslandschaft ist wegen der Gefahr von Vorfällen großen Ausmaßes, die erhebliche Störungen oder Schäden an kritischen Infrastrukturen verursachen, eine erhöhte Abwehrbereitschaft auf allen Ebenen des Cybersicherheitsrahmens der Union erforderlich. Diese Bedrohung geht über die militärische Aggression Russlands gegen die Ukraine hinaus und wird angesichts der Vielzahl staatsnaher, krimineller und hacktivistischer Akteure, die an den derzeitigen geopolitischen Spannungen beteiligt sind, wahrscheinlich andauern. Solche Vorfälle können – auch in kritischen oder hochkritischen Sektoren – die Erbringung öffentlicher Dienstleistungen und die Ausübung wirtschaftlicher Tätigkeiten beeinträchtigen, erhebliche finanzielle Verluste verursachen, das Vertrauen der Nutzer untergraben und der Wirtschaft der Union schweren Schaden zufügen und sogar gesundheitliche oder lebensbedrohliche Folgen haben. Darüber hinaus sind Cybersicherheitsvorfälle unvorhersehbar, da sie oft innerhalb sehr kurzer Zeiträume auftreten und sich	(2) Die Tragweite, die Häufigkeit und die Auswirkungen von Cybersicherheitsvorfällen nehmen zu, was auch Cyberangriffe im Zusammenhang mit Cyberspionage, Ransomware oder Störungen einschließt. Sie stellen eine große Bedrohung für das Funktionieren von Netz- und Informationssystemen ***sowie für kritische IT und physische Infrastrukturen*** dar. Angesichts der sich wandelnden Bedrohungslandschaft ist wegen der Gefahr von Vorfällen großen Ausmaßes, die erhebliche Störungen oder Schäden an kritischen Infrastrukturen verursachen, eine erhöhte Abwehrbereitschaft auf allen Ebenen des Cybersicherheitsrahmens der Union erforderlich. Diese Bedrohung geht über die militärische Aggression Russlands gegen die Ukraine hinaus und wird angesichts der Vielzahl staatsnaher, krimineller und hacktivistischer Akteure, die an den derzeitigen geopolitischen Spannungen beteiligt sind, wahrscheinlich andauern. Solche Vorfälle können – auch in kritischen oder hochkritischen Sektoren – die Erbringung öffentlicher Dienstleistungen***, den öffentlichen und privaten Verkehr,*** und die Ausübung wirtschaftlicher Tätigkeiten beeinträchtigen, erhebliche finanzielle Verluste verursachen, das Vertrauen der Nutzer untergraben und der Wirtschaft ***der Union sowie der Mobilität innerhalb*** der Union schweren Schaden zufügen und sogar gesundheitliche oder

fortentwickeln, nicht auf ein bestimmtes geografisches Gebiet beschränkt sind, sondern sich gleichzeitig in vielen Ländern ereignen oder sich rasch in andere Länder ausbreiten können.	lebensbedrohliche Folgen haben. Darüber hinaus sind Cybersicherheitsvorfälle unvorhersehbar, da sie oft innerhalb sehr kurzer Zeiträume auftreten und sich fortentwickeln, nicht auf ein bestimmtes geografisches Gebiet beschränkt sind, sondern sich gleichzeitig in vielen Ländern ereignen oder sich rasch in andere Länder ausbreiten können.

Änderungsantrag 2

Vorschlag für eine Verordnung
Erwägung 2 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(2a) Eine zunehmend ernste Bedrohung für den Verkehrssektor geht von staatlich unterstützten Akteuren, Cyberkriminellen und Hacktivisten aus, die sich gegen Behörden, Betreiber, Hersteller, Lieferanten und Dienstleister im Luft-, See-, Schienen- und Straßenverkehr richten. Die Agentur der Europäischen Union für Cybersicherheit (ENISA) hat im Jahr 2022 einen Anstieg der monatlichen durchschnittlichen Zahl der gemeldeten Vorfälle mit Auswirkungen auf den Verkehrssektor um 25 % gegenüber 2021 festgestellt. Ein Großteil der Angriffe auf den Verkehrssektor richtet sich gegen IT-Systeme und kann Betriebsstörungen zur Folge haben.[14a]
	[14b] ENISA (2023), ENISA Threat Landscape: Transport Sector (ENISA-Bericht zur Bedrohungslage: Verkehrssektor), S. 7 und 17.

Änderungsantrag 3

Vorschlag für eine Verordnung
Erwägung 2 b (neu)

Vorschlag der Kommission	*Geänderter Text*
	(2b) Die unprovozierte Invasion Russlands in die Ukraine führte zu einem erheblichen Anstieg der Cybersicherheitsvorfälle, einschließlich verteilter Denial-of-Service-Angriffe (DDoS-Angriffe), die auf den Verkehrssektor in der EU und in EU-nahen Gebieten, vor allem auf Flughäfen, Eisenbahnnetze und Verkehrsbehörden, abzielen[14b]. Diese Zunahme der Angriffe wird sich höchstwahrscheinlich fortsetzen.
	[14b] ENISA (2023), ENISA Threat Landscape: Transport Sector (ENISA-Bericht zur Bedrohungslage: Verkehrssektor), S. 9.

Änderungsantrag 4

Vorschlag für eine Verordnung
Erwägung 2 c (neu)

Vorschlag der Kommission	*Geänderter Text*
	(2c) Cyberangriffe richten sich gegen Behörden und Einrichtungen in allen Teilsektoren des Verkehrssektors, wobei unter anderem Eisenbahnunternehmen und Infrastrukturbetreiber sowie Hafenbetreiber betroffen sind. Im Straßensektor wurden die Erstausrüster, Zulieferer und Dienstleister sowie öffentliche Verkehrsunternehmen ins Visier genommen. Im Luftfahrtsektor waren die wichtigsten Ziele Fluggesellschaften und Flughafenbetreiber, gefolgt von Dienstleistern, Bodenbeförderungsanbietern und der Lieferkette.[14c]
	[14c] ENISA (2023), ENISA Threat Landscape: Transport Sector (ENISA-

	Bericht zur Bedrohungslage: Verkehrssektor), S. 17.

Änderungsantrag 5

Vorschlag für eine Verordnung
Erwägung 3

Vorschlag der Kommission	*Geänderter Text*
(3) Es ist notwendig, die Wettbewerbsposition der Industrie- und Dienstleistungssektoren in der Union in der gesamten digitalisierten Wirtschaft zu stärken und ihren digitalen Wandel zu unterstützen, indem das Cybersicherheitsniveau im digitalen Binnenmarkt erhöht wird. Wie in drei verschiedenen Vorschlägen der Konferenz zur Zukunft Europas[16] empfohlen, muss die Resilienz der Bürgerinnen und Bürger ***und*** der Unternehmen und Einrichtungen, die kritische Infrastrukturen betreiben, gegenüber den zunehmenden Cybersicherheitsbedrohungen, die verheerende gesellschaftliche und wirtschaftliche Auswirkungen haben können, erhöht werden. Daher sind Investitionen in Infrastrukturen und Dienste erforderlich, die eine schnellere Erkennung von Cybersicherheitsbedrohungen und -vorfällen und eine schnellere Reaktion darauf unterstützen, und die Mitgliedstaaten benötigen Unterstützung zur Verbesserung der Vorsorgemaßnahmen und der Reaktion auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes. Auch die Union sollte ihre Kapazitäten in diesen Bereichen ausbauen, insbesondere in Bezug auf die Erhebung und Analyse von Daten über Cybersicherheitsbedrohungen und ***-vorfälle***.	(3) Es ist notwendig, die Wettbewerbsposition der Industrie- und Dienstleistungssektoren in der Union in der gesamten digitalisierten Wirtschaft zu stärken und ihren digitalen Wandel zu unterstützen, indem das Cybersicherheitsniveau im digitalen Binnenmarkt erhöht wird. Wie in drei verschiedenen Vorschlägen der Konferenz zur Zukunft Europas[16] empfohlen, muss die Resilienz der Bürgerinnen und Bürger***,*** der Unternehmen***, der Verkehrsunternehmen*** und ***der*** Einrichtungen, die kritische Infrastrukturen betreiben, gegenüber den zunehmenden Cybersicherheitsbedrohungen, die verheerende gesellschaftliche und wirtschaftliche Auswirkungen haben können, erhöht werden. Daher sind Investitionen in Infrastrukturen und Dienste erforderlich, die eine schnellere Erkennung von Cybersicherheitsbedrohungen und -vorfällen und eine schnellere Reaktion darauf unterstützen, und die Mitgliedstaaten benötigen Unterstützung zur Verbesserung der Vorsorgemaßnahmen und der Reaktion auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes. Auch die Union sollte ihre Kapazitäten in diesen Bereichen ausbauen, insbesondere in Bezug auf die Erhebung und Analyse von Daten über Cybersicherheitsbedrohungen und ***-vorfälle sowie über den Zustand und die Entwicklung des Arbeitsmarkts im Bereich der Cybersicherheit, da dieser***

eine entscheidende Rolle bei der Bereitstellung der erforderlichen Erkennungs- und Reaktionsdienste spielt.

[16] https://futureu.europa.eu/de/

[16] https://futureu.europa.eu/de/

Änderungsantrag 6

Vorschlag für eine Verordnung
Erwägung 4

Vorschlag der Kommission	*Geänderter Text*
(4) Die Union hat bereits eine Reihe von Rechtsakten erlassen, um Sicherheitslücken zu verringern und die Resilienz kritischer Infrastrukturen und Einrichtungen gegenüber Cybersicherheitsrisiken zu erhöhen, darunter insbesondere die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates[17], die Empfehlung (EU) 2017/1584 der Kommission[18], die Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates[19] und die Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates[20]. Ferner wurden die Mitgliedstaaten in der Empfehlung des Rates für eine unionsweite koordinierte Vorgehensweise zur Stärkung der Resilienz kritischer Infrastruktur aufgefordert, unverzüglich wirksame Maßnahmen zu ergreifen und loyal, effizient, solidarisch und in koordinierter Weise mit der Kommission und anderen einschlägigen Behörden sowie den betreffenden Einrichtungen zusammenzuarbeiten, um die Resilienz kritischer Infrastrukturen, die für die Erbringung wesentlicher Dienste im Binnenmarkt genutzt werden, zu erhöhen.	(4) Die Union hat bereits eine Reihe von Rechtsakten erlassen, um Sicherheitslücken zu verringern und die Resilienz kritischer Infrastrukturen und Einrichtungen gegenüber Cybersicherheitsrisiken zu erhöhen, darunter insbesondere die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates[17], die Empfehlung (EU) 2017/1584 der Kommission[18], die Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates[19] und die Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates[20] ***sowie der Vorschlag für eine Verordnung über Leitlinien für den Aufbau eines transeuropäischen Verkehrsnetzes und der Vorschlag für eine Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (Cyberresilienzgesetz)***. Ferner wurden die Mitgliedstaaten in der Empfehlung des Rates für eine unionsweite koordinierte Vorgehensweise zur Stärkung der Resilienz kritischer Infrastruktur aufgefordert, unverzüglich wirksame Maßnahmen zu ergreifen und loyal, effizient, solidarisch und in koordinierter Weise mit der Kommission und anderen einschlägigen Behörden sowie den betreffenden Einrichtungen zusammenzuarbeiten, um die Resilienz kritischer Infrastrukturen, die für die

Erbringung wesentlicher Dienste im Binnenmarkt genutzt werden, zu erhöhen.

[17] 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).

[18] 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).

[19] Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates (ABl. L 218 vom 14.8.2013, S. 8).

[20] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15).

[17] 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).

[18] 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).

[19] Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates (ABl. L 218 vom 14.8.2013, S. 8).

[20] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15).

Änderungsantrag 7

Vorschlag für eine Verordnung
Erwägung 4 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(4a) Das von der Kommission vorgelegte Instrumentarium für die Cybersicherheit im Verkehrssektor[2a], das

grundlegende Informationen über Bedrohungen enthält, die sich auf Verkehrsorganisationen auswirken können (Verbreitung von Schadsoftware, Denial of Service, unbefugter Zugriff und Diebstahl sowie Softwaremanipulation), und in dem bewährte Abwehrverfahren aufgeführt sind, wird zwar begrüßt, dennoch sollten die Verkehrsunternehmen mit entsprechenden Schulungen zum Thema Cybersicherheit und mit geeigneten Instrumenten zur Verhinderung von Cyberbedrohungen ausgestattet werden. Aus dem Unionshaushalt sollte außerdem die Unterstützung finanziert werden, die von der ENISA z. B. in Form von Schulungen bereitgestellt wird, um die wirksame Umsetzung der im Instrumentarium enthaltenen bewährten Abwehrmaßnahmen durch die Verkehrsunternehmen zu ermöglichen.

[1a] ENISA Threat Landscape: Transport Sector (ENISA-Bericht zur Bedrohungslage: Verkehrssektor), März 2023.

[2a] Europäische Kommission (2021). Instrumentarium für die Cybersicherheit im Verkehrssektor, abrufbar unter https://transport.ec.europa.eu/transport-themes/security-safety/cybersecurity_de.

Änderungsantrag 8

Vorschlag für eine Verordnung
Erwägung 4 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(4a) Grundlage für einen unionsweit koordinierten Ansatz zur Stärkung der Vorsorge und der Widerstandsfähigkeit von kritischer Infrastruktur, wie z. B. der Verkehrsinfrastruktur, bildet der Kapazitätsaufbau der Mitgliedstaaten.

Wie in der jüngsten Mitteilung der Kommission an das Europäische Parlament und den Rat zur Schließung der Fachkräftelücke im Cybersicherheitsbereich zur Förderung der Wettbewerbsfähigkeit, des Wachstums und der Resilienz in der EU[19a] anerkannt, kann die Sicherheit der EU nur mithilfe des wertvollsten Guts der EU sichergestellt werden: mithilfe der Menschen.

[19a] Mitteilung der Kommission an das Europäische Parlament und den Rat: Schließung der Fachkräftelücke im Cybersicherheitsbereich zur Förderung der Wettbewerbsfähigkeit, des Wachstums und der Resilienz in der EU („Akademie für Cybersicherheitskompetenzen"), COM(2023)207.

Änderungsantrag 9

Vorschlag für eine Verordnung
Erwägung 12

Vorschlag der Kommission	*Geänderter Text*
(12) Um Cyberbedrohungen und -vorfälle wirksamer zu verhüten, zu bewerten und zu bewältigen, ist es notwendig, umfassendere Kenntnisse über die bestehenden Bedrohungen für kritische Anlagen und Infrastrukturen im Gebiet der Union zu erlangen, einschließlich ihrer geografischen Verteilung, ihres Zusammenwirkens und ihrer potenziellen Auswirkungen im Falle von Cyberangriffen, die diese Infrastrukturen betreffen. Es sollte eine große Unionsinfrastruktur für SOCs (im Folgenden „europäischer Cyberschutzschild") eingerichtet werden, die aus mehreren interoperativen grenzübergreifenden Plattformen besteht, die jeweils mehrere nationale SOCs zusammenführen. Diese Infrastruktur sollte	(12) Um Cyberbedrohungen und -vorfälle wirksamer zu verhüten, zu bewerten und zu bewältigen, ist es notwendig, umfassendere Kenntnisse über die bestehenden Bedrohungen für kritische Anlagen und Infrastrukturen im Gebiet der Union zu erlangen, einschließlich ihrer geografischen Verteilung, ihres Zusammenwirkens und ihrer potenziellen Auswirkungen im Falle von Cyberangriffen, die diese Infrastrukturen betreffen. ***Zu diesen kritischen Anlagen und Infrastrukturen gehören intelligente Verkehrssysteme, die zwar für die automatisierte und multimodale Mobilität von wesentlicher Bedeutung sind, aber auf der Grundlage eines kritischen Austauschs sensibler Daten betrieben werden.*** Es sollte eine große

den Interessen und Bedürfnissen der Mitgliedstaaten und der Union im Bereich der Cybersicherheit dienen, indem sie den neuesten Stand der Technik für fortgeschrittene Instrumente der Datenerhebung und -analyse nutzt, die Fähigkeiten zur Erkennung und Bewältigung von Cyberangriffen verbessert und eine Echtzeit-Lageerfassung ermöglicht. Sie sollte auch dazu dienen, die Erkennung von Cybersicherheitsbedrohungen und -vorfällen zu verbessern und somit die für das Krisenmanagement in der Union zuständigen Einrichtungen und Netze der Union, insbesondere das EU-Netz der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe) im Sinne der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates[24], zu ergänzen und zu unterstützen.	Unionsinfrastruktur für SOCs (im Folgenden „europäischer Cyberschutzschild“) eingerichtet werden, die aus mehreren interoperativen grenzübergreifenden Plattformen besteht, die jeweils mehrere nationale SOCs zusammenführen. Diese Infrastruktur sollte den Interessen und Bedürfnissen der Mitgliedstaaten und der Union im Bereich der Cybersicherheit dienen, indem sie den neuesten Stand der Technik für fortgeschrittene Instrumente der Datenerhebung und -analyse nutzt, die Fähigkeiten zur Erkennung und Bewältigung von Cyberangriffen verbessert und eine Echtzeit-Lageerfassung ermöglicht. Sie sollte auch dazu dienen, die Erkennung von Cybersicherheitsbedrohungen und -vorfällen zu verbessern und somit die für das Krisenmanagement in der Union zuständigen Einrichtungen und Netze der Union, insbesondere das EU-Netz der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe) im Sinne der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates[24], zu ergänzen und zu unterstützen.
[24] 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 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80).	[24] 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 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80).

Änderungsantrag 10

Vorschlag für eine Verordnung
Erwägung 14 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(14a) Der Verkehrssektor wird zunehmend zu einem der lukrativsten Geschäftsfelder für Cyberkriminelle, wobei Kundendaten als sehr wertvolle Ware gelten und die Transportlieferkette zunehmend ins Visier gerät. Aus diesem Grund sollte die Verkehrsinfrastruktur, die durch einen grenzüberschreitenden Charakter bzw. durch den Datenaustausch über drahtlose Technologien gekennzeichnet ist, sowohl von nationalen als auch insbesondere von grenzüberschreitenden SOCs als zentraler Gegenstand der Analyse und Überwachung betrachtet werden. So erfordert beispielsweise der jüngste Vorschlag zur Überarbeitung der TEN-V-Verordnung mehr Solidarität und Zusammenarbeit beim Austausch von Informationen über grenzüberschreitende Cyberbedrohungen, denen dieses transnationale Netz ausgesetzt sein könnte. In ähnlicher Weise sind intelligente Verkehrssysteme (IVS) von entscheidender Bedeutung, um den Verkehr sicherer, effizienter und nachhaltiger zu machen. Allerdings machen sie die Verkehrssysteme anfälliger für Cyberangriffe, die Unfälle, Staus oder wirtschaftliche Verluste für private und öffentliche Betreiber verursachen können. Um die Sicherheit der Fahrgäste und den Schutz der Daten von Nutzern und Anbietern sicherzustellen und finanzielle Schäden zu vermeiden, ist es von wesentlicher Bedeutung, dass das Durchführungsprogramm zu der überarbeiteten Richtlinie über intelligente Verkehrssysteme Bestimmungen und Instrumente enthält, um die Zusammenarbeit zwischen den Mitgliedstaaten bei der Erkennung, Vorsorge und Bewältigung von Cybersicherheitsbedrohungen und -vorfällen zu stärken.

Änderungsantrag 11

Vorschlag für eine Verordnung
Erwägung 15

Vorschlag der Kommission	*Geänderter Text*
(15) Auf nationaler Ebene wird die Überwachung, Erkennung und Analyse von Cyberbedrohungen in der Regel durch SOCs öffentlicher und privater Einrichtungen in Kombination mit CSIRTs sichergestellt. Darüber hinaus tauschen die CSIRTs im Rahmen des CSIRT-Netzes Informationen gemäß der Richtlinie (EU) 2022/2555 aus. Die grenzübergreifenden SOCs-Plattformen sollten eine neue Kapazität bilden, die das CSIRTs-Netz ergänzt, indem sie Daten über Bedrohungen der Cybersicherheit von öffentlichen und privaten Einrichtungen zusammenführen und weitergeben, den Wert solcher Daten durch Expertenanalysen, gemeinsam beschaffte Infrastrukturen und modernste Instrumente steigern und zur Entwicklung der Fähigkeiten und technologischen Souveränität der Union beitragen.	(15) Auf nationaler Ebene wird die Überwachung, Erkennung und Analyse von Cyberbedrohungen in der Regel durch SOCs öffentlicher und privater Einrichtungen in Kombination mit CSIRTs sichergestellt. Darüber hinaus tauschen die CSIRTs im Rahmen des CSIRT-Netzes Informationen gemäß der Richtlinie (EU) 2022/2555 aus. Die grenzübergreifenden SOCs-Plattformen sollten eine neue Kapazität bilden, die das CSIRTs-Netz ergänzt, indem sie Daten über Bedrohungen der Cybersicherheit von öffentlichen und privaten Einrichtungen zusammenführen und weitergeben, den Wert solcher Daten durch Expertenanalysen, gemeinsam beschaffte Infrastrukturen und modernste Instrumente steigern und zur Entwicklung der Fähigkeiten und technologischen Souveränität der Union beitragen. ***In diesem Zusammenhang ist es zur Stärkung der Autonomie der Union im Cyberbereich unter Bezugnahme auf Artikel 47 Absatz 4 der vorgeschlagenen Verordnung über Leitlinien für den Aufbau eines transeuropäischen Verkehrsnetzes (COM(2021)0812) auch erforderlich, den Zugang zu Daten, die zu Cyberbedrohungen führen, zu verhindern, indem ein solider Rechtsrahmen durchgesetzt wird, der ausländische Beteiligungen an und Investitionen in kritische Infrastruktur wie den Verkehrssektor regelt.***

Änderungsantrag 12

Vorschlag für eine Verordnung

Erwägung 21

Vorschlag der Kommission	*Geänderter Text*
(21) Obwohl der europäische Cyberschutzschild ein ziviles Projekt ist, könnten die Cyberabwehrkreise von besseren zivilen Fähigkeiten zur Erkennung und Lageerfassung profitieren, die für den Schutz kritischer Infrastrukturen entwickelt werden. Grenzübergreifende SOCs sollten mit Unterstützung der Kommission und des Europäischen Kompetenzzentrums für Cybersicherheit (ECCC) und in Zusammenarbeit mit dem Hohen Vertreter der Union für Außen- und Sicherheitspolitik (im Folgenden „Hoher Vertreter“) schrittweise spezielle Protokolle und Standards entwickeln, um die Zusammenarbeit mit den Cyberabwehrkreisen, auch in Bezug auf Sicherheitsüberprüfungen und -bedingungen, zu ermöglichen. Die Entwicklung des europäischen Cyberschutzschilds sollte von Überlegungen begleitet werden, die eine künftige Zusammenarbeit mit Netzen und Plattformen, die dem Informationsaustausch in der Cyberabwehrgemeinschaft dienen, in enger Abstimmung mit dem Hohen Vertreter ermöglichen sollen.	(21) Obwohl der europäische Cyberschutzschild ein ziviles Projekt ist, könnten die Cyberabwehrkreise von besseren zivilen Fähigkeiten zur Erkennung und Lageerfassung profitieren, die für den Schutz kritischer Infrastrukturen entwickelt werden. Grenzübergreifende SOCs sollten mit Unterstützung der Kommission und des Europäischen Kompetenzzentrums für Cybersicherheit (ECCC) und in Zusammenarbeit mit dem Hohen Vertreter der Union für Außen- und Sicherheitspolitik (im Folgenden „Hoher Vertreter“) schrittweise spezielle Protokolle und Standards entwickeln, um die Zusammenarbeit mit den Cyberabwehrkreisen, auch in Bezug auf Sicherheitsüberprüfungen und -bedingungen, zu ermöglichen. Die Entwicklung des europäischen Cyberschutzschilds sollte von Überlegungen begleitet werden, die eine künftige Zusammenarbeit mit Netzen und Plattformen, die dem Informationsaustausch in der Cyberabwehrgemeinschaft dienen, in enger Abstimmung mit dem Hohen Vertreter ermöglichen sollen. ***Er sollte auch Synergien mit dem Aktionsplan zur militärischen Mobilität 2.0 ermöglichen. Ein gut funktionierendes militärisches Mobilitätsnetz muss widerstandsfähig sein, auch im Zusammenhang mit Cyberbedrohungen und anderen hybriden Bedrohungen, die kritische Knotenpunkte des Verkehrssystems mit doppeltem Verwendungszweck beeinträchtigen könnten. So könnte beispielsweise ein Cyberangriff auf Systeme, die in Flughäfen, Häfen oder im Schienennetz eingesetzt werden, oder ein Cyberangriff auf militärische Anlagen erhebliche Folgen haben. Die Digitalisierung von Prozessen und Verfahren, auch für die***

	notwendige zivile und militärische Zusammenarbeit, erfordert daher die Stärkung der Computerinformationssysteme gegen Cyberbedrohungen.

Änderungsantrag 13

Vorschlag für eine Verordnung
Erwägung 21 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(21a) Im Falle einer Cybersicherheitskrise ist ein wirksamer Informationsaustausch von entscheidender Bedeutung, um die Lagerfassung des militärischen und zivilen Verkehrssektors sicherzustellen. Dieser Informationsaustausch sollte auch die Zusammenarbeit zwischen den einschlägigen sektoralen Behörden, die für den Verkehr zuständig sind, den für Cybersicherheit zuständigen Behörden, den SOCs und den CSIRTs fördern.

Änderungsantrag 14

Vorschlag für eine Verordnung
Erwägung 29

Vorschlag der Kommission	*Geänderter Text*
(29) Im Rahmen der Vorsorgemaßnahmen sollten koordinierte Tests und eine entsprechende Bewertung der Cybersicherheit von in hochkritischen Sektoren tätigen Einrichtungen gemäß der Richtlinie (EU) 2022/2555 unterstützt werden, um einen kohärenten Ansatz zu fördern und die Sicherheit in der gesamten Union und ihrem Binnenmarkt zu erhöhen. Dazu sollte die Kommission mit Unterstützung der ENISA und in Zusammenarbeit mit der durch die Richtlinie (EU) 2022/2555 eingesetzten NIS-Kooperationsgruppe regelmäßig	(29) Im Rahmen der Vorsorgemaßnahmen sollten koordinierte Tests und eine entsprechende Bewertung der Cybersicherheit von in hochkritischen Sektoren tätigen Einrichtungen gemäß der Richtlinie (EU) 2022/2555 unterstützt werden, um einen kohärenten Ansatz zu fördern und die Sicherheit in der gesamten Union und ihrem Binnenmarkt zu erhöhen. Dazu sollte die Kommission mit Unterstützung der ENISA und in Zusammenarbeit mit der durch die Richtlinie (EU) 2022/2555 eingesetzten NIS-Kooperationsgruppe regelmäßig

einschlägige Sektoren oder Teilsektoren festlegen, die für eine finanzielle Unterstützung für koordinierte Tests auf Unionsebene in Betracht kommen sollen. Die Sektoren oder Teilsektoren sollten aus Anhang I der Richtlinie (EU) 2022/2555 („Sektoren der hohen Kritikalität“) ausgewählt werden. Die koordinierten Tests sollten auf gemeinsamen Risikoszenarien und -methoden beruhen. Auch angesichts der Notwendigkeit, Doppelarbeit zu vermeiden, sollten bei der Auswahl der Sektoren und der Entwicklung von Risikoszenarien einschlägige unionsweite Risikobewertungen und –szenarien berücksichtigt werden, darunter etwa die Risikobewertung und szenarien, zu deren Durchführung die Kommission, der Hohe Vertreter und die NIS-Kooperationsgruppe in Abstimmung mit den einschlägigen zivilen und militärischen Einrichtungen und Agenturen sowie bestehenden Netzwerken wie dem EU-CyCLONe in den Schlussfolgerungen des Rates zur Entwicklung der Cyberabwehr der Europäischen Union aufgefordert werden; dazu zählen auch die Risikobewertung von Kommunikationsnetzen und infrastrukturen, die im gemeinsamen Ministeraufruf von Nevers gefordert und von der NIS-Kooperationsgruppe mit Unterstützung der Kommission und der ENISA und in Zusammenarbeit mit dem Gremium Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) durchgeführt wird, die gemäß Artikel 22 der Richtlinie (EU) 2022/2555 durchzuführenden koordinierten Risikobewertungen und das Testen der digitalen operationalen Resilienz gemäß der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates[29]. Bei der Auswahl der Sektoren sollte auch der Empfehlung des Rates für eine unionsweite koordinierte Vorgehensweise zur Stärkung der Resilienz kritischer Infrastrukturen

einschlägige Sektoren oder Teilsektoren festlegen, die für eine finanzielle Unterstützung für koordinierte Tests auf Unionsebene in Betracht kommen sollen. Die Sektoren oder Teilsektoren sollten aus Anhang I der Richtlinie (EU) 2022/2555 („Sektoren der hohen Kritikalität“) ausgewählt werden. ***Besondere Aufmerksamkeit sollte dem Verkehrssektor und seinen Teilsektoren (Luft, Schiene, Wasser, Straße) gewidmet werden, da sie kritische Infrastrukturen umfassen, in denen Cybervorfälle und -angriffe die Sicherheit von Fahrgästen und Betreibern ernsthaft gefährden könnten.*** Die koordinierten Tests sollten auf gemeinsamen Risikoszenarien und -methoden beruhen. Auch angesichts der Notwendigkeit, Doppelarbeit zu vermeiden, sollten bei der Auswahl der Sektoren und der Entwicklung von Risikoszenarien einschlägige unionsweite Risikobewertungen und –szenarien berücksichtigt werden, darunter etwa die Risikobewertung und szenarien, zu deren Durchführung die Kommission, der Hohe Vertreter und die NIS-Kooperationsgruppe in Abstimmung mit den einschlägigen zivilen und militärischen Einrichtungen und Agenturen sowie bestehenden Netzwerken wie dem EU-CyCLONe in den Schlussfolgerungen des Rates zur Entwicklung der Cyberabwehr der Europäischen Union aufgefordert werden; dazu zählen auch die Risikobewertung von Kommunikationsnetzen und -infrastrukturen, die im gemeinsamen Ministeraufruf von Nevers gefordert und von der NIS-Kooperationsgruppe mit Unterstützung der Kommission und der ENISA und in Zusammenarbeit mit dem Gremium Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) durchgeführt wird, die gemäß Artikel 22 der Richtlinie (EU) 2022/2555 durchzuführenden koordinierten Risikobewertungen und das Testen der digitalen operationalen Resilienz gemäß der Verordnung (EU)

Rechnung getragen werden.	2022/2554 des Europäischen Parlaments und des Rates[29]. Bei der Auswahl der Sektoren sollte auch der Empfehlung des Rates für eine unionsweite koordinierte Vorgehensweise zur Stärkung der Resilienz kritischer Infrastrukturen Rechnung getragen werden.
[29] Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011.	[29] Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011.

Änderungsantrag 15

Vorschlag für eine Verordnung
Erwägung 30 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(30a) Angesichts der Kritikalität des Sektors und der Auswirkungen von Cyberbedrohungen auf die Mobilität und damit auf das menschliche Leben von Fahrgästen und Fußgängern sollte der Verkehrssektor im Hinblick auf die koordinierten Tests der Abwehrbereitschaft von Einrichtungen Vorrang haben.

Änderungsantrag 16

Vorschlag für eine Verordnung
Erwägung 35 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(35a) Angesichts der erweiterten Aufgaben und Zuständigkeiten, die der ENISA durch diesen Vorschlag und den Vorschlag zum Cyberresilienzgesetz übertragen werden, ist die Annahme des

Berichtigungshaushaltsplans Nr. 1/2022 der ENISA für die Pilotphase der Umsetzung einer Maßnahme zur Unterstützung der Cybersicherheit erforderlich. Darüber hinaus sollten der ENISA angesichts der auf dem Spiel stehenden Unionsinteressen zusätzliche finanzielle und personelle Ressourcen zugewiesen werden.

Änderungsantrag 17

Vorschlag für eine Verordnung
Erwägung 38 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(38a) Die Entwicklung von Fähigkeiten und Kompetenzen sollte daher in allen Sektoren im Mittelpunkt stehen, nicht zuletzt für diejenigen, die anfällig für Cybersicherheitsbedrohungen sind, wie z. B. Personal, das im Bereich des Massentransits oder kritischer Infrastrukturen tätig ist, einschließlich Zugsteuerungssystemen und digitaler Verkehrsplanungsinstrumente für alle Verkehrsträger. Die Einführung und Weiterentwicklung der Cybersicherheitskultur ist daher von entscheidender Bedeutung für den Erfolg der Umsetzung dieser Verordnung sowohl im Hinblick auf das Bewusstsein der Bürgerinnen und Bürger als auch auf das Wissen der Fachleute in allen Sektoren der kritischen Infrastruktur.

Änderungsantrag 18

Vorschlag für eine Verordnung
Artikel 1 – Absatz 2 – Buchstabe a

Vorschlag der Kommission	*Geänderter Text*
a) Stärkung der gemeinsamen Fähigkeiten der Union zur Erkennung und Lageerfassung im Bereich der	a) Stärkung der gemeinsamen Fähigkeiten der Union zur Erkennung und Lageerfassung im Bereich der

Cyberbedrohungen und -vorfälle, um so in der gesamten digitalen Wirtschaft der Union eine Stärkung der Wettbewerbsfähigkeit der ***Industrie-*** und Dienstleistungszweige zu ermöglichen und zur technologischen Souveränität der Union im Bereich der Cybersicherheit beizutragen;	Cyberbedrohungen und -vorfälle, um so in der gesamten digitalen Wirtschaft der Union eine Stärkung der Wettbewerbsfähigkeit der ***Industrie, der Verkehrsinfrastruktur*** und ***der*** Dienstleistungszweige zu ermöglichen und zur technologischen Souveränität der Union im Bereich der Cybersicherheit beizutragen;

Änderungsantrag 19

Vorschlag für eine Verordnung
Artikel 1 – Absatz 2 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
b) Stärkung der Abwehrbereitschaft der in kritischen und hochkritischen Sektoren tätigen Einrichtungen in der gesamten Union und Stärkung der Solidarität durch den Aufbau gemeinsamer Kapazitäten für die Reaktion auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes, indem u. a. die Unionsunterstützung für die Bewältigung von Cybersicherheitsvorfällen auch Drittländern, die mit dem Programm Digitales Europa (DEP) assoziiert sind, zur Verfügung gestellt wird;	b) Stärkung der Abwehrbereitschaft der in kritischen und hochkritischen Sektoren tätigen Einrichtungen in der gesamten Union und Stärkung der Solidarität durch den Aufbau gemeinsamer Kapazitäten für die Reaktion auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes ***unter besonderer Berücksichtigung kritischer IT und physischer Infrastrukturen***, indem u. a. die Unionsunterstützung für die Bewältigung von Cybersicherheitsvorfällen auch Drittländern, die mit dem Programm Digitales Europa (DEP) assoziiert sind, zur Verfügung gestellt wird;

Änderungsantrag 20

Vorschlag für eine Verordnung
Artikel 1 – Absatz 2 – Buchstabe c a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ca) Stärkung der Abwehrbereitschaft, Zusammenarbeit und Wirksamkeit der Union beim Schutz der Verkehrsinfrastruktur und -dienste in den Mitgliedstaaten vor Cybersicherheitsvorfällen, um das

	kontinuierliche Funktionieren des Verkehrssektors, die Integrität der Lieferketten und die unionsweite Mobilität zu gewährleisten.

Änderungsantrag 21

Vorschlag für eine Verordnung
Artikel 3 – Absatz 2 – Unterabsatz 1 – Buchstabe c

Vorschlag der Kommission	*Geänderter Text*
c) Leisten eines Beitrags zu einem besseren Schutz vor Cyberbedrohungen und einer besseren Reaktion darauf***;***	c) Leisten eines Beitrags zu einem besseren Schutz vor Cyberbedrohungen und einer besseren Reaktion darauf***, auch bei Verkehrsinfrastrukturen, die durch grenzüberschreitenden Charakter gekennzeichnet sind (z. B. das TEN-V) oder sich durch den Datenaustausch über drahtlose Technologien auszeichnen (z. B. intelligente Verkehrssysteme).***

Änderungsantrag 22

Vorschlag für eine Verordnung
Artikel 3 – Absatz 2 – Unterabsatz 2

Vorschlag der Kommission	*Geänderter Text*
Sein Aufbau erfolgt in Zusammenarbeit mit der europaweiten Hochleistungsrecheninfrastruktur, die gemäß der Verordnung (EU) 2021/1173 eingerichtet worden ist.	Sein Aufbau erfolgt in Zusammenarbeit mit der europaweiten Hochleistungsrecheninfrastruktur, die gemäß der Verordnung (EU) 2021/1173 eingerichtet worden ist. ***Er ermöglicht die Zusammenarbeit mit der Cyberabwehrgemeinschaft mittels spezieller Protokolle und Standards, um die Entwicklung besserer ziviler Fähigkeiten zur Erkennung und Lageerfassung für den Schutz kritischer Infrastrukturen sicherzustellen. In diesem Zusammenhang werden auch Synergien mit dem Aktionsplan zur militärischen Mobilität 2.0 entwickelt, und es wird für einen wirksamen Informationsaustausch gesorgt, um die Lageerfassung des militärischen und zivilen Verkehrssektors***

sicherzustellen.

Änderungsantrag 23

Vorschlag für eine Verordnung
Artikel 8 – Absatz 2 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(2a) Die Kommission bezieht den europäischen Cyberschutzschild, insbesondere die grenzübergreifenden SOCs, überall dort in ihre Stellungnahme an die Mitgliedstaaten im Rahmen des Vorschlags für eine Verordnung über das transeuropäische Verkehrsnetz (COM(2021)0812) ein, wo die Beteiligung oder der Beitrag einer natürlichen Person aus einem Drittland oder eines Unternehmens aus einem Drittland die Cybersicherheit grenzüberschreitender kritischer Infrastrukturen wie des TEN-V beeinträchtigen dürfte.

Änderungsantrag 24

Vorschlag für eine Verordnung
Artikel 10 – Absatz 1 – Buchstabe a

Vorschlag der Kommission	*Geänderter Text*
a) Vorsorgemaßnahmen, einschließlich koordinierter Tests der Abwehrbereitschaft der in hochkritischen Sektoren tätigen Einrichtungen in der gesamten Union;	a) Vorsorgemaßnahmen, einschließlich koordinierter Tests der Abwehrbereitschaft der in hochkritischen Sektoren tätigen Einrichtungen in der gesamten Union***, unter besonderer Berücksichtigung der Verkehrsinfrastruktur und ihrer Teilsektoren, die in Anhang I der Richtlinie (EU) 2022/2555 aufgeführt sind***;

Änderungsantrag 25

Vorschlag für eine Verordnung
Artikel 18 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Bei der Erstellung des in Absatz 1 genannten Berichts über die Überprüfung des Sicherheitsvorfalls arbeitet die ENISA mit allen einschlägigen Beteiligten zusammen, darunter mit Vertretern der Mitgliedstaaten, der Kommission, anderen einschlägigen Organen, Einrichtungen und sonstigen Stellen der EU, Anbietern verwalteter Sicherheitsdienste und Nutzern von Cybersicherheitsdiensten. Soweit dies zweckmäßig ist, arbeitet die ENISA auch mit Einrichtungen zusammen, die von schwerwiegenden Sicherheitsvorfällen oder Sicherheitsvorfällen großen Ausmaßes betroffen sind. Zur Unterstützung der Überprüfung kann die ENISA auch andere Arten von Interessenträgern befragen. Befragte Vertreter müssen etwaige Interessenkonflikte offenlegen.	(2) Bei der Erstellung des in Absatz 1 genannten Berichts über die Überprüfung des Sicherheitsvorfalls arbeitet die ENISA mit allen einschlägigen Beteiligten zusammen, darunter mit Vertretern der Mitgliedstaaten, der Kommission, anderen einschlägigen Organen, Einrichtungen und sonstigen Stellen der EU, Anbietern verwalteter Sicherheitsdienste und Nutzern von Cybersicherheitsdiensten. Soweit dies zweckmäßig ist, arbeitet die ENISA auch mit Einrichtungen zusammen, die von schwerwiegenden Sicherheitsvorfällen oder Sicherheitsvorfällen großen Ausmaßes betroffen sind***, einschließlich Verkehrsunternehmen***. Zur Unterstützung der Überprüfung kann die ENISA auch andere Arten von Interessenträgern befragen. Befragte Vertreter müssen etwaige Interessenkonflikte offenlegen.

Änderungsantrag 26

Vorschlag für eine Verordnung
Artikel 19 – Absatz 1 – Nummer 1 – Buchstabe b
Verordnung (EU) 2021/694
Artikel 6 – Absatz 2a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(2a) Angesichts der auf dem Spiel stehenden Interessen der Union, im Hinblick auf ihre Zuständigkeiten für die Ausarbeitung möglicher Schemata für die Zertifizierung gemäß der Verordnung (EU) 2019/881, ihre Zuständigkeiten für die Überprüfung und Bewertung von Cyberbedrohungen, Schwachstellen und Abwehrmaßnahmen, die Erstellung eines Berichts über die Überprüfung von Sicherheitsvorfällen für den Überprüfungsmechanismus für Cybersicherheitsvorfälle, sowie die Durchführung von Schulungen zu Cyberangriffen und Sicherheitsvorfällen

	für Betreiber kritischer Infrastrukturen und angesichts ihrer im Rahmen des Vorschlags für das Cyberresilienzgesetz neu zugewiesenen Zuständigkeiten werden der ENISA im Einklang mit den geltenden Rechtsvorschriften die erforderlichen Mittel aus dem Unionshaushalt zur Verfügung gestellt.

Änderungsantrag 27

Vorschlag für eine Verordnung
Artikel 19 – Absatz 1 – Nummer 1 a (neu)
Verordnung (EU) 2021/694
Artikel 7 – Absatz 1 – Buchstabe c a (neu)

Vorschlag der Kommission	*Geänderter Text*
	1a. Artikel 7 wird wie folgt geändert:
	a) Absatz 1 wird wie folgt geändert:
	1. folgender Buchstabe ca wird eingefügt:
	ca) Unterstützung hochwertiger Schulungen für Verkehrsunternehmen sowie für die Führungs- und Arbeitskräfte kritischer Verkehrsinfrastrukturen, auch mit dem Ziel, Abwehrmaßnahmen im Zusammenhang mit Cyberangriffen auf oder Sicherheitsvorfällen in kritische(n) Infrastrukturen wirksam auszutauschen und umzusetzen, wie etwa solche, die im Rahmen des Instrumentariums für die Cybersicherheit im Verkehrssektor bereitgestellt werden.

VERFAHREN DES MITBERATENDEN AUSSCHUSSES

Titel	Maßnahmen zur Stärkung der Solidarität und der Kapazitäten in der Union für die Erkennung, Vorsorge und Bewältigung von Cybersicherheitsbedrohungen und -vorfällen
Bezugsdokumente – Verfahrensnummer	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Federführender Ausschuss Datum der Bekanntgabe im Plenum	ITRE 1.6.2023
Stellungnahme von Datum der Bekanntgabe im Plenum	TRAN 1.6.2023
Verfasser(in) der Stellungnahme Datum der Benennung	Gheorghe Falcă 7.7.2023
Datum der Annahme	25.10.2023
Ergebnis der Schlussabstimmung	+: 38 –: 0 0: 0
Zum Zeitpunkt der Schlussabstimmung anwesende Mitglieder	Magdalena Adamowicz, Andris Ameriks, José Ramón Bauzá Díaz, Izaskun Bilbao Barandica, Karolin Braunsberger-Reinhold, Karima Delli, Anna Deparnay-Grunenberg, Gheorghe Falcă, Carlo Fidanza, Jens Gieseke, Elsi Katainen, Elena Kountoura, Bogusław Liberadzki, Peter Lundgren, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Tilly Metz, Cláudia Monteiro de Aguiar, Caroline Nagtegaal, Jan-Christoph Oetjen, Rovana Plumb, Thomas Rudner, Massimiliano Salini, Vera Tax, Barbara Thaler, István Ujhelyi, Achille Variati, Petar Vitanov, Elissavet Vozemberg-Vrionidi, Lucia Vuolo
Zum Zeitpunkt der Schlussabstimmung anwesende Stellvertreter	Sara Cerdas, Josianne Cutajar, Roman Haider, Pär Holmgren, Pierre Karleskind, Colm Markey, Ljudmila Novak, Dorien Rookmaker

NAMENTLICHE SCHLUSSABSTIMMUNG IM MITBERATENDEN AUSSCHUSS

38	+
ECR	Carlo Fidanza, Peter Lundgren, Dorien Rookmaker
ID	Roman Haider
PPE	Magdalena Adamowicz, Karolin Braunsberger-Reinhold, Gheorghe Falcă, Jens Gieseke, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Colm Markey, Cláudia Monteiro de Aguiar, Ljudmila Novak, Massimiliano Salini, Barbara Thaler, Elissavet Vozemberg-Vrionidi, Lucia Vuolo
Renew	José Ramón Bauzá Díaz, Izaskun Bilbao Barandica, Pierre Karleskind, Elsi Katainen, Caroline Nagtegaal, Jan-Christoph Oetjen
S&D	Andris Ameriks, Sara Cerdas, Josianne Cutajar, Bogusław Liberadzki, Rovana Plumb, Thomas Rudner, Vera Tax, István Ujhelyi, Achille Variati, Petar Vitanov
The Left	Elena Kountoura
Verts/ALE	Karima Delli, Anna Deparnay-Grunenberg, Pär Holmgren, Tilly Metz

0	-

0	0

Erklärung der benutzten Zeichen:
+ : dafür
- : dagegen
0 : Enthaltung