Európsky parlament
2019-2024

Výbor pre dopravu a cestovný ruch

2023/0109(COD)

25.10.2023

STANOVISKO

Výboru pre dopravu a cestovný ruch

pre Výbor pre priemysel, výskum a energetiku

k návrhu nariadenia Európskeho parlamentu a Rady, ktorým sa stanovujú opatrenia na posilnenie solidarity a kapacít v Únii na odhaľovanie kybernetických hrozieb a incidentov, prípravu a reakciu na ne
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Spravodajca výboru požiadaného o stanovisko: Gheorghe Falcă

PA_Legam

STRUČNÉ ODÔVODNENIE

Organizácie zasiahnuté kybernetickými útokmi, a to aj v odvetví dopravy, ich nahlasujú len zriedka, najmä spoločnosti zo súkromného sektora, pretože ich považujú za „zlú reklamu“. Väčšina organizácií ich radšej rieši interne a často sú to útočníci, ktorí ich zverejňujú. V EÚ je dobrou správou, že nadobudnutím účinnosti smernice 2022/2555 o bezpečnosti sietí (známej ako smernica NIS 2), ktorú musia členské štáty transponovať do októbra 2024, sa harmonizujú povinnosti týkajúce sa oznamovania incidentov vo všetkých členských štátoch. Preto je pravdepodobné, že v nadchádzajúcich rokoch dôjde k lepšiemu pochopeniu povahy a rozsahu problému.

Agentúra Európskej únie pre kybernetickú bezpečnosť (ENISA) nedávno uverejnila správu1, v ktorej sa uvádzajú informácie o kybernetickobezpečnostných hrozbách v odvetví dopravy, v ktorej zdôrazňuje, že páchatelia počítačovej kriminality boli zodpovední za viac ako polovicu incidentov zaznamenaných vo vykazovanom období roku 2022 (55 %) a že hlavnou motiváciou týchto útokov bol finančný zisk. Uvádza tiež, že väčšina kybernetických útokov v odvetví dopravy je zameraná na informačné systémy, čo spôsobuje narušenie prevádzky.

Pokiaľ ide o pripravenosť a reakciu na kybernetické incidenty, v súčasnosti existuje len nízka miera podpory na úrovni Únie a solidarity medzi členskými štátmi. Rada vo svojich záveroch z mája 2022 poukázala na potrebu riešiť tieto nedostatky, pričom vyzvala Komisiu, aby predložila návrh nového **Fondu pre reakcie na núdzové situácie v oblasti kybernetickej bezpečnosti**[2].

Týmto nariadením sa takisto vykonáva **stratégia kybernetickej bezpečnosti EÚ** prijatá v decembri 2020, ktorou sa oznámilo vytvorenie **európskeho kybernetického štítu**, ktorým sa posilňujú spôsobilosti Európskej únie týkajúce sa odhaľovania kybernetických hrozieb a výmeny informácií o nich prostredníctvom združenia vnútroštátnych a cezhraničných centier bezpečnostných operácií. Opatrenia tohto nariadenia sa podporia **finančnými prostriedkami strategického cieľa Kybernetická bezpečnosť programu Digitálna Európa.**

Celkový rozpočet obsahuje zvýšenie o 100 miliónov EUR, ktoré sa podľa návrhu v tomto nariadení majú prerozdeliť z iných strategických cieľov programu Digitálna Európa. Tým sa nová celková suma dostupná na opatrenia v oblasti kybernetickej bezpečnosti v rámci programu Digitálna Európa zvýši na 842,8 milióna EUR.

Časťou dodatočnej sumy 100 miliónov EUR sa podporí rozpočet spravovaný Európskym centrom priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti (ECCC) na vykonávanie opatrení týkajúcich sa centier bezpečnostných operácií a pripravenosti v rámci ich pracovných programov. Dodatočné finančné prostriedky okrem toho poslúžia na podporu vytvorenia rezervy EÚ na účely kybernetickej bezpečnosti. Tieto prostriedky doplňajú rozpočet, ktorý už bol stanovený na podobné opatrenia v rámci pracovného programu hlavného programu Digitálna Európa a cieľa Kybernetická bezpečnosť programu Digitálna Európa na roky 2023 – 2027, čím by sa celková suma na roky 2023 – 2027 mohla zvýšiť na 551 miliónov EUR, pričom 115 miliónov EUR už bolo vyčlenených vo forme

[1] Understanding Cyber Threats in Transport, ENISA, uverejnené 21. marca 2023.
[2] Závery Rady o vývoji prístupu Európskej únie ku kybernetickej bezpečnosti z 23. mája 2022 (9364/22).

pilotných projektov na roky 2021 – 2022. Spoločne s príspevkami členských štátov by celkový rozpočet mohol dosiahnuť až 1,109 miliardy EUR.

Stanovisko spravodajcu

Spravodajca víta nový návrh a domnieva sa, že bude veľkým prínosom pre rôzne zainteresované strany. Spravodajca zdôrazňuje, že je potrebné hlbšie pochopiť potreby a požiadavky kybernetickej bezpečnosti v doprave, ako aj poskytnúť kritickým subjektom v doprave prístup k riadnemu financovaniu určenému na pripravenosť, reakciu a riešenia incidentov.

Spravodajca podporuje súbor nástrojov pre kybernetickú bezpečnosť v oblasti dopravy, ktorého cieľom je prispieť k vyššej úrovni informovanosti o kybernetickej bezpečnosti a kybernetickej hygiene s osobitným zameraním na odvetvie dopravy. Zameriava sa na dopravné organizácie bez ohľadu na ich veľkosť a oblasť činnosti, ako aj na kritickú dopravnú infraštruktúru a vojenskú mobilitu, najmä pokiaľ ide o vojnu na Ukrajine, ale nielen na ňu:

- Leteckí dopravcovia, riadiace orgány letísk, hlavné letiská, manažment letovej prevádzky a strediská riadenia letovej prevádzky, Agentúra Európskej únie pre bezpečnosť letectva a Eurocontrol;
- Manažéri infraštruktúry, železničné podniky a Európsky systém riadenia železničnej dopravy (ERTMS);
- Spoločnosti vnútrozemskej, námornej a pobrežnej osobnej a nákladnej vodnej dopravy, riadiace orgány prístavov vrátane ich prístavných zariadení, subjekty prevádzkujúce práce a zariadenia v prístavoch, prevádzkovatelia služieb lodnej dopravy;
- Cestné orgány zodpovedné za riadenie dopravy, prevádzkovatelia inteligentných dopravných systémov;
- Poštové a kuriérske služby.

Spravodajca sa domnieva, že pre úspešnosť fungovania **Fondu pre reakcie na núdzové situácie v oblasti kybernetickej bezpečnosti (ERFC)** bude rozhodujúca výška jeho rozpočtu; preto by mal byť dostatočne veľký na to, aby podporoval členské štáty **pri príprave na významné a rozsiahle kybernetické incidenty, pri reakcii na ne a pri zotavení sa z nich;** Podpora pri reakcii na incidenty sa sprístupní aj inštitúciám, orgánom, úradom a agentúram Únie.

Európskym kybernetickým štítom sa zlepšia spôsobilosti členských štátov v oblasti odhaľovania kybernetických hrozieb. **Mechanizmom na riešenie kybernetických núdzových situácií** sa doplnia opatrenia členských štátov prostredníctvom núdzovej podpory určenej na pripravenosť, reakciu a okamžité zotavenie sa/obnovenie fungovania základných služieb.

POZMEŇUJÚCI NÁVRH

Výbor pre dopravu a cestovný ruch vyzýva Výbor pre priemysel, výskum a energetiku, aby ako gestorský výbor vzal do úvahy:

Pozmeňujúci návrh 1

Návrh nariadenia
Odôvodnenie 2

Text predložený Komisiou	*Pozmeňujúci návrh*
(2) Rozsah, frekvencia a dosah kybernetických incidentov sa zvyšujú, pričom ide aj útoky na dodávateľský reťazec zamerané na kybernetickú špionáž, ransomware alebo narušenie. Tieto incidenty predstavujú závažnú hrozbu pre fungovanie sietí a informačných systémov. Hrozba možných rozsiahlych incidentov, ktoré by mohli významne narušiť alebo poškodiť kritické infraštruktúry, si vzhľadom na rýchly vývoj situácie v oblasti hrozieb vyžaduje vyššiu mieru pripravenosti na všetkých úrovniach rámca kybernetickej bezpečnosti v Únii. Táto hrozba nevyplýva len z ruskej vojenskej agresie voči Ukrajine a vzhľadom na veľký počet kriminálnych a haktivistických aktérov napojených na štát, ktorí sa podieľajú na aktuálnom geopolitickom napätí, môže pretrvávať. Takéto incidenty môžu zabraňovať poskytovaniu verejných služieb a realizácii hospodárskych činností, a to aj v kritických odvetviach alebo v odvetviach s vysokou úrovňou kritickosti, spôsobovať značné finančné straty, narúšať dôveru používateľa, spôsobovať značné škody hospodárstvu Únie a dokonca by mohli mať zdravie alebo život ohrozujúce dôsledky. Kybernetické incidenty sú navyše nepredvídateľné, keďže často vznikajú a vyvíjajú sa vo veľmi krátkom časovom intervale, nie sú obmedzené na konkrétnu geografickú oblasť a vyskytujú sa súčasne v mnohých krajinách alebo sa v nich ihneď rozširujú.	(2) Rozsah, frekvencia a dosah kybernetických incidentov sa zvyšujú, pričom ide aj útoky na dodávateľský reťazec zamerané na kybernetickú špionáž, ransomware alebo narušenie. Tieto incidenty predstavujú závažnú hrozbu pre fungovanie sietí a informačných systémov, ***ako aj pre kritické IT a fyzické infraštruktúry.*** Hrozba možných rozsiahlych incidentov, ktoré by mohli významne narušiť alebo poškodiť kritické infraštruktúry, si vzhľadom na rýchly vývoj situácie v oblasti hrozieb vyžaduje vyššiu mieru pripravenosti na všetkých úrovniach rámca kybernetickej bezpečnosti v Únii. Táto hrozba nevyplýva len z ruskej vojenskej agresie voči Ukrajine a vzhľadom na veľký počet kriminálnych a haktivistických aktérov napojených na štát, ktorí sa podieľajú na aktuálnom geopolitickom napätí, môže pretrvávať. Takéto incidenty môžu zabraňovať poskytovaniu verejných služieb, ***verejnej a súkromnej dopravy*** a realizácii hospodárskych činností, a to aj v kritických odvetviach alebo v odvetviach s vysokou úrovňou kritickosti, spôsobovať značné finančné straty, narúšať dôveru používateľa, spôsobovať značné škody hospodárstvu Únie, ***ako aj mobilite v rámci Únie,*** a dokonca by mohli mať zdravie alebo život ohrozujúce dôsledky. Kybernetické incidenty sú navyše nepredvídateľné, keďže často vznikajú a vyvíjajú sa vo veľmi krátkom časovom intervale, nie sú obmedzené na konkrétnu

geografickú oblasť a vyskytujú sa súčasne v mnohých krajinách alebo sa v nich ihneď rozširujú.

Pozmeňujúci návrh 2

Návrh nariadenia
Odôvodnenie 2 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(2a) Štátom podporovaní aktéri, páchatelia počítačovej kriminality a hackeri, ktorí sa zameriavajú na orgány, prevádzkovateľov, výrobcov, dodávateľov a poskytovateľov služieb v leteckej, námornej, železničnej a cestnej doprave, predstavujú pre odvetvie dopravy čoraz vážnejšiu kybernetickú hrozbu. Agentúra Európskej únie pre kybernetickú bezpečnosť (ENISA) zaznamenala v roku 2022 nárast priemerného mesačného počtu nahlásených incidentov, ktoré zasiahli odvetvie dopravy o 25 % v porovnaní s úrovňami z roku 2021. Väčšina útokov na odvetvie dopravy sa zameriava na systémy informačných technológií (IT), čo môže viesť k narušeniu prevádzky[14a].
	[14b] ENISA (2023), ENISA, Prehľad hrozieb: odvetvie dopravy, s. 7 a 17.

Pozmeňujúci návrh 3

Návrh nariadenia
Odôvodnenie 2 b (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(2b) Nevyprovokovaná invázia Ruska na Ukrajinu viedla k výraznému nárastu kybernetických incidentov vrátane distribuovaných kybernetických útokov odmietnutia služby, ktoré sa zameriavajú na odvetvie dopravy v EÚ a oblasti v

	blízkosti EÚ, najmä letiská, železnice a dopravné orgány[14b]. Tento nárast útokov bude s veľkou pravdepodobnosťou pokračovať.
	[14b] ENISA (2023), ENISA, Prehľad hrozieb: odvetvie dopravy, s. 9.

Pozmeňujúci návrh 4

Návrh nariadenia
Odôvodnenie 2 c (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(2c) Kybernetické útoky sa zameriavajú na orgány a subjekty vo všetkých pododvetviach dopravy, pričom dotknuté sú železničné podniky a správcovia infraštruktúry, ako aj prevádzkovatelia prístavov. Pokiaľ ide o odvetvie cestnej dopravy, terčom útokov boli výrobcovia pôvodného zariadenia, dodávatelia a poskytovatelia služieb, ako aj prevádzkovatelia verejnej dopravy. V odvetví leteckej dopravy boli hlavnými cieľmi letecké spoločnosti a prevádzkovatelia letísk, po ktorých nasledovali poskytovatelia služieb, prevádzkovatelia povrchovej dopravy a dodávateľský reťazec[14c].
	[14c] ENISA (2023), ENISA, Prehľad hrozieb: odvetvie dopravy, s. 17.

Pozmeňujúci návrh 5

Návrh nariadenia
Odôvodnenie 3

Text predložený Komisiou	*Pozmeňujúci návrh*
(3) Je nevyhnutné posilniť konkurenčnú pozíciu odvetví priemyslu a služieb v Únii v rámci celého	(3) Je nevyhnutné posilniť konkurenčnú pozíciu odvetví priemyslu a služieb v Únii v rámci celého

digitalizovaného hospodárstva a podporiť ich digitálnu transformáciu, a to posilnením úrovne kybernetickej bezpečnosti na digitálnom jednotnom trhu. Podľa odporúčaní v troch rôznych návrhoch Konferencie o budúcnosti Európy[16] je nevyhnutné zvýšiť odolnosť občanov, podnikov a subjektov pôsobiacich v kritických infraštruktúrach voči čoraz väčším kybernetickým hrozbám, ktoré môžu mať zničujúce spoločenské a hospodárske dôsledky. Sú preto potrebné investície do infraštruktúr a služieb, ktorými sa podporí rýchlejšie odhaľovanie kybernetických hrozieb a incidentov a reakcia na ne, a členské štáty potrebujú pomoc, aby sa mohli lepšie pripraviť na významné a rozsiahle kybernetické incidenty a aby na ne mohli lepšie reagovať. Únia by takisto mala zvýšiť svoje kapacity v týchto oblastiach, predovšetkým v súvislosti so zberom a analýzou údajov o kybernetických hrozbách a incidentoch.

digitalizovaného hospodárstva a podporiť ich digitálnu transformáciu, a to posilnením úrovne kybernetickej bezpečnosti na digitálnom jednotnom trhu. Podľa odporúčaní v troch rôznych návrhoch Konferencie o budúcnosti Európy[16] je nevyhnutné zvýšiť odolnosť občanov, podnikov, ***prevádzkovateľov dopravy*** a subjektov pôsobiacich v kritických infraštruktúrach voči čoraz väčším kybernetickým hrozbám, ktoré môžu mať zničujúce spoločenské a hospodárske dôsledky. Sú preto potrebné investície do infraštruktúr a služieb, ktorými sa podporí rýchlejšie odhaľovanie kybernetických hrozieb a incidentov a reakcia na ne, a členské štáty potrebujú pomoc, aby sa mohli lepšie pripraviť na významné a rozsiahle kybernetické incidenty a aby na ne mohli lepšie reagovať. Únia by takisto mala zvýšiť svoje kapacity v týchto oblastiach, predovšetkým v súvislosti so zberom a analýzou údajov o kybernetických hrozbách a incidentoch, ***ako aj o stave a vývoji trhu práce v oblasti kybernetickej bezpečnosti, keďže zohráva kľúčovú úlohu pri poskytovaní potrebných služieb odhaľovania a reakcie.***

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

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

Pozmeňujúci návrh 6

Návrh nariadenia
Odôvodnenie 4

Text predložený Komisiou	*Pozmeňujúci návrh*
(4) Únia už prijala niekoľko opatrení na zníženie zraniteľnosti a zvýšenie odolnosti kritických infraštruktúr a subjektov voči kybernetickobezpečnostným rizikám, najmä smernicu Európskeho parlamentu a Rady (EÚ) 2022/2555[17], odporúčanie Komisie (EÚ) 2017/1584[18], smernicu	(4) Únia už prijala niekoľko opatrení na zníženie zraniteľnosti a zvýšenie odolnosti kritických infraštruktúr a subjektov voči kybernetickobezpečnostným rizikám, najmä smernicu Európskeho parlamentu a Rady (EÚ) 2022/2555[17], odporúčanie Komisie (EÚ) 2017/1584[18], smernicu

Európskeho parlamentu a Rady 2013/40/EÚ[19] a nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881[20]. V odporúčaní Rady o celoúnijnom koordinovanom prístupe k posilneniu odolnosti kritickej infraštruktúry sa členské štáty navyše vyzývajú, aby bezodkladne prijali účinné opatrenia a aby v duchu solidarity zabezpečili lojálnu, účinnú a koordinovanú spoluprácu medzi sebou, s Komisiou a inými príslušnými verejnými orgánmi, ako aj dotknutými subjektmi, a zvýšili tak odolnosť kritickej infraštruktúry, ktorá sa využíva pri poskytovaní základných služieb na vnútornom trhu.

Európskeho parlamentu a Rady 2013/40/EÚ[19] a nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881[20], ***ako aj návrh nariadenia o usmerneniach pre rozvoj transeurópskej dopravnej siete a návrh nariadenia o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami (akt o kybernetickej odolnosti).*** V odporúčaní Rady o celoúnijnom koordinovanom prístupe k posilneniu odolnosti kritickej infraštruktúry sa členské štáty navyše vyzývajú, aby bezodkladne prijali účinné opatrenia a aby v duchu solidarity zabezpečili lojálnu, účinnú a koordinovanú spoluprácu medzi sebou, s Komisiou a inými príslušnými verejnými orgánmi, ako aj dotknutými subjektmi, a zvýšili tak odolnosť kritickej infraštruktúry, ktorá sa využíva pri poskytovaní základných služieb na vnútornom trhu.

---

[17] Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (Ú. v. EÚ L 333, 27.12.2022, s. 80).

[18] Odporúčanie Komisie (EÚ) 2017/1584 z 13. septembra 2017 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu (Ú. v. EÚ L 239, 19.9.2017, s. 36).

[19] Smernica Európskeho parlamentu a Rady 2013/40/EÚ z 12. augusta 2013 o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SVV (Ú. v. EÚ L 218, 14.8.2013, s. 8).

[20] Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti

[17] Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (Ú. v. EÚ L 333, 27.12.2022, s. 80).

[18] Odporúčanie Komisie (EÚ) 2017/1584 z 13. septembra 2017 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu (Ú. v. EÚ L 239, 19.9.2017, s. 36).

[19] Smernica Európskeho parlamentu a Rady 2013/40/EÚ z 12. augusta 2013 o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SVV (Ú. v. EÚ L 218, 14.8.2013, s. 8).

[20] Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti

informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (Ú. v. EÚ L 151, 7.6.2019, s. 15).	informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (Ú. v. EÚ L 151, 7.6.2019, s. 15).

Pozmeňujúci návrh 7

Návrh nariadenia
Odôvodnenie 4 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(4a) Hoci víta súbor nástrojov Európskej komisie pre kybernetickú bezpečnosť v oblasti dopravy[2a], ktorý obsahuje základné informácie o hrozbách, ktoré môžu mať vplyv na dopravné organizácie (šírenie malvéru, odmietnutie služby, neoprávnený prístup a krádež a manipulácia so softvérom) a uvádza zoznam osvedčených postupov na zmiernenie hrozieb, prevádzkovateľom dopravy by sa mala poskytnúť riadna odborná príprava v oblasti kybernetickej bezpečnosti a vhodné nástroje na predchádzanie kybernetickým hrozbám. Rozpočet Únie by mal pokrývať aj podporu, ako je odborná príprava, ktorú poskytuje agentúra ENISA s cieľom umožniť prevádzkovateľom dopravy účinne uplatňovať osvedčené postupy na zmiernenie rizík uvedené v súbore nástrojov.
	[1a] ENISA, Prehľad hrozieb: odvetvie dopravy/ENISA, marec 2023
	[2a] Európska komisia, 2021. Súbor nástrojov pre kybernetickú bezpečnosť v oblasti dopravy, k dispozícii na https://transport.ec.europa.eu/transport-themes/security-safety/cybersecurity_en

Pozmeňujúci návrh 8

Návrh nariadenia
Odôvodnenie 4 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(4a) Celoúnijný koordinovaný prístup k posilneniu pripravenosti a odolnosti kritickej infraštruktúry, ako je dopravná infraštruktúra, je založený na budovaní kapacít členských štátov. Ako sa uznáva v nedávnom oznámení Komisie Európskemu parlamentu a Rade s názvom Riešenie nedostatku odborníkov v oblasti kybernetickej bezpečnosti s cieľom posilniť konkurencieschopnosť, rast a odolnosť EÚ, bezpečnosť EÚ nemožno zaručiť bez najcennejšieho aktíva EÚ: jej obyvateľov.
	Oznámenie Komisie Európskemu parlamentu a Rade: Riešenie nedostatku odborníkov v oblasti kybernetickej bezpečnosti s cieľom posilniť konkurencieschopnosť, rast a odolnosť EÚ (Akadémia zručností v oblasti kybernetickej bezpečnosti), COM(2023) 207 final

Pozmeňujúci návrh 9

Návrh nariadenia
Odôvodnenie 12

Text predložený Komisiou	*Pozmeňujúci návrh*
(12) S cieľom účinnejšie predchádzať kybernetickým hrozbám a incidentom, posudzovať ich a reagovať na ne sa musia vybudovať komplexnejšie znalosti o hrozbách pre kritické aktíva a infraštruktúry na území Únie vrátane ich geografického rozloženia, vzájomného prepojenia a potenciálnych účinkov v prípade kybernetických útokov, ktoré by zasiahli tieto infraštruktúry. Zaviesť by sa mala rozsiahla infraštruktúra centier bezpečnostných operácií Únie	(12) S cieľom účinnejšie predchádzať kybernetickým hrozbám a incidentom, posudzovať ich a reagovať na ne sa musia vybudovať komplexnejšie znalosti o hrozbách pre kritické aktíva a infraštruktúry na území Únie vrátane ich geografického rozloženia, vzájomného prepojenia a potenciálnych účinkov v prípade kybernetických útokov, ktoré by zasiahli tieto infraštruktúry. ***Medzi tieto kritické aktíva a infraštruktúry patria inteligentné dopravné systémy, ktoré sú***

(tzv. európsky kybernetický štít), ktorú by tvorilo niekoľko spolupracujúcich cezhraničných platforiem, z ktorých každá by združovala niekoľko vnútroštátnych centier bezpečnostných operácií. Táto infraštruktúra by mala slúžiť záujmom a potrebám v oblasti kybernetickej bezpečnosti na vnútroštátnej úrovni a na úrovni Únie, pričom by mala v plnej miere využívať najmodernejšie technológie vyspelých nástrojov na zber a analýzu údajov, čím by sa zlepšili spôsobilosti týkajúce sa odhaľovania a zvládania kybernetických hrozieb a poskytovanie situačnej informovanosti v reálnom čase. Táto infraštruktúra by mala slúžiť na zlepšenie odhaľovania kybernetických hrozieb a incidentov, a tak dopĺňať a podporovať subjekty a siete Únie zodpovedné za krízové riadenie v Únii, predovšetkým Európsku sieť styčných organizácií pre kybernetické krízy (ďalej len „EU-CyCLONe“), ako je vymedzená v smernici Európskeho parlamentu a Rady (EÚ) 2022/2555[24].	***nevyhnutné pre automatizovanú a multimodálnu mobilitu a fungujú na základe kľúčovej výmeny citlivých údajov.*** Zaviesť by sa mala rozsiahla infraštruktúra centier bezpečnostných operácií Únie (tzv. európsky kybernetický štít), ktorú by tvorilo niekoľko spolupracujúcich cezhraničných platforiem, z ktorých každá by združovala niekoľko vnútroštátnych centier bezpečnostných operácií. Táto infraštruktúra by mala slúžiť záujmom a potrebám v oblasti kybernetickej bezpečnosti na vnútroštátnej úrovni a na úrovni Únie, pričom by mala v plnej miere využívať najmodernejšie technológie vyspelých nástrojov na zber a analýzu údajov, čím by sa zlepšili spôsobilosti týkajúce sa odhaľovania a zvládania kybernetických hrozieb a poskytovanie situačnej informovanosti v reálnom čase. Táto infraštruktúra by mala slúžiť na zlepšenie odhaľovania kybernetických hrozieb a incidentov, a tak dopĺňať a podporovať subjekty a siete Únie zodpovedné za krízové riadenie v Únii, predovšetkým Európsku sieť styčných organizácií pre kybernetické krízy (ďalej len „EU-CyCLONe“), ako je vymedzená v smernici Európskeho parlamentu a Rady (EÚ) 2022/2555[24].
[24] Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2) (Ú. v. EÚ L 333, 27.12.2022, s. 80).	[24] Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2) (Ú. v. EÚ L 333, 27.12.2022, s. 80).

Pozmeňujúci návrh 10

Návrh nariadenia
Odôvodnenie 14 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(14a) Odvetvie dopravy sa čoraz viac stáva jednou z najlukratívnejších oblastí podnikania pre páchateľov počítačovej kriminality, pričom údaje o zákazníkoch sú považované za veľmi cenný tovar a dodávateľský reťazec v doprave sa stáva čoraz viac terčom útokov. Z tohto dôvodu by sa dopravná infraštruktúra, ktorá sa vyznačuje cezhraničným charakterom alebo výmenou údajov prostredníctvom bezdrôtových technológií, mala považovať za kľúčový objekt analýzy a monitorovania pre vnútroštátne, a najmä cezhraničné centrá bezpečnostných operácií. Napríklad nedávny návrh na revíziu nariadenia o TEN-T vyžaduje väčšiu solidaritu a spoluprácu pri výmene informácií o cezhraničných kybernetických hrozbách, ktorým by táto nadnárodná sieť mohla čeliť. Podobne, hoci sú inteligentné dopravné systémy (IDS) nevyhnutné na zvýšenie bezpečnosti, efektívnosti a udržateľnosti dopravy, zvyšujú zraniteľnosť dopravných systémov voči kybernetickým útokom, ktoré môžu spôsobiť nehody, dopravné zápchy alebo hospodárske straty súkromným a verejným prevádzkovateľom. S cieľom zaistiť bezpečnosť cestujúcich, ochranu údajov používateľov a poskytovateľov a zabrániť finančným škodám je nevyhnutné, aby program vykonávania revidovanej smernice o inteligentných dopravných systémoch obsahoval ustanovenia a nástroje na posilnenie spolupráce medzi členskými štátmi pri odhaľovaní kybernetickobezpečnostných hrozieb a incidentov, príprave na ne a reakcii na ne.

Pozmeňujúci návrh 11

Návrh nariadenia
Odôvodnenie 15

Text predložený Komisiou	*Pozmeňujúci návrh*
(15) Na vnútroštátnej úrovni zabezpečujú monitorovanie, odhaľovanie a analýzu kybernetických hrozieb zvyčajne centrá bezpečnostných operácií verejných a súkromných subjektov v kombinácii s jednotkami CSIRT. Jednotky CSIRT si okrem toho v súlade so smernicou (EÚ) 2022/2555 vymieňajú informácie v rámci siete jednotiek CSIRT. Cezhraničné centrá bezpečnostných operácií by mali predstavovať novú kapacitu, ktorá bude dopĺňať sieť jednotiek CSIRT tým, že budú zhromažďovať údaje o kybernetickobezpečnostných hrozbách od verejných a súkromných subjektov a zabezpečovať spoločné využívanie týchto údajov, zvyšovať ich hodnotu prostredníctvom odborných analýz, spoločne nadobudnutých infraštruktúr a najmodernejších nástrojov a prispievať k rozvoju spôsobilostí a technologickej suverenity Únie.	(15) Na vnútroštátnej úrovni zabezpečujú monitorovanie, odhaľovanie a analýzu kybernetických hrozieb zvyčajne centrá bezpečnostných operácií verejných a súkromných subjektov v kombinácii s jednotkami CSIRT. Jednotky CSIRT si okrem toho v súlade so smernicou (EÚ) 2022/2555 vymieňajú informácie v rámci siete jednotiek CSIRT. Cezhraničné centrá bezpečnostných operácií by mali predstavovať novú kapacitu, ktorá bude dopĺňať sieť jednotiek CSIRT tým, že budú zhromažďovať údaje o kybernetickobezpečnostných hrozbách od verejných a súkromných subjektov a zabezpečovať spoločné využívanie týchto údajov, zvyšovať ich hodnotu prostredníctvom odborných analýz, spoločne nadobudnutých infraštruktúr a najmodernejších nástrojov a prispievať k rozvoju spôsobilostí a technologickej suverenity Únie. ***V tejto súvislosti je v záujme posilnenia autonómie Únie v kybernetickej oblasti a s odkazom na článok 47 ods. 4 návrhu nariadenia o usmerneniach Únie pre rozvoj transeurópskej dopravnej siete (COM(2021)0812) takisto potrebné zabrániť prístupu k údajom vedúcim ku kybernetickým hrozbám presadzovaním pevného regulačného rámca, ktorý upravuje zahraničné vlastníctvo a investície do kritickej infraštruktúry, ako je doprava.***

Pozmeňujúci návrh 12

Návrh nariadenia
Odôvodnenie 21

Text predložený Komisiou	*Pozmeňujúci návrh*
(21) Hoci je európsky kybernetický štít civilný projekt, komunita kybernetickej obrany by mohla ťažiť zo silnejších civilných spôsobilostí týkajúcich sa	(21) Hoci je európsky kybernetický štít civilný projekt, komunita kybernetickej obrany by mohla ťažiť zo silnejších civilných spôsobilostí týkajúcich sa

odhaľovania a situačnej informovanosti vyvinutých na ochranu kritickej infraštruktúry. Cezhraničné centrá bezpečnostných operácií s podporou Komisie a Európskeho centra priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti (ďalej len „kompetenčné centrum“) a v spolupráci s vysokým predstaviteľom Únie pre zahraničné veci a bezpečnostnú politiku (ďalej len „vysoký predstaviteľ“) by mali postupne vypracovať osobitné protokoly a normy umožňujúce spoluprácu s komunitou kybernetickej obrany vrátane podmienok preverovania a bezpečnostných podmienok. Vývoj európskeho kybernetického štítu by mali sprevádzať úvahy umožňujúce v úzkej kooperácii s vysokým predstaviteľom budúcu spoluprácu so sieťami a s platformami zodpovednými za výmenu informácií v komunite kybernetickej obrany.	odhaľovania a situačnej informovanosti vyvinutých na ochranu kritickej infraštruktúry. Cezhraničné centrá bezpečnostných operácií s podporou Komisie a Európskeho centra priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti (ďalej len „kompetenčné centrum“) a v spolupráci s vysokým predstaviteľom Únie pre zahraničné veci a bezpečnostnú politiku (ďalej len „vysoký predstaviteľ“) by mali postupne vypracovať osobitné protokoly a normy umožňujúce spoluprácu s komunitou kybernetickej obrany vrátane podmienok preverovania a bezpečnostných podmienok. Vývoj európskeho kybernetického štítu by mali sprevádzať úvahy umožňujúce v úzkej kooperácii s vysokým predstaviteľom budúcu spoluprácu so sieťami a s platformami zodpovednými za výmenu informácií v komunite kybernetickej obrany. ***Mal by tiež umožniť synergie s akčným plánom v oblasti vojenskej mobility 2.0. Dobre fungujúca sieť vojenskej mobility musí byť odolná, a to aj v kontexte kybernetických a iných hybridných hrozieb, ktoré by mohli ovplyvniť kritické uzly v dopravnom systéme, ktoré majú dvojaké využitie. Závažné dôsledky by mohol mať napríklad kybernetický útok na systémy používané na letiskách, prístavoch alebo železniciach alebo kybernetický útok na vojenské prostriedky. Digitalizácia procesov a postupov vrátane potrebnej civilnej a vojenskej spolupráce si preto bude vyžadovať posilnenie počítačových informačných systémov (CIS) proti kybernetickým hrozbám.***

Pozmeňujúci návrh 13

Návrh nariadenia
Odôvodnenie 21 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(21a) V prípade krízy v oblasti kybernetickej bezpečnosti je účinná výmena informácií kľúčová pre zabezpečenie situačného povedomia medzi vojenským a civilným dopravným odvetvím. Táto výmena informácií by mala stimulovať aj spoluprácu medzi príslušnými odvetvovými orgánmi zodpovednými za dopravu, príslušnými orgánmi pre kybernetickú bezpečnosť, centrami bezpečnostných operácií a jednotkami CSIRT.

Pozmeňujúci návrh 14

Návrh nariadenia
Odôvodnenie 29

Text predložený Komisiou	*Pozmeňujúci návrh*
(29) V rámci opatrení v oblasti pripravenosti a v záujme presadzovania jednotného prístupu a zvýšenia bezpečnosti v celej Únii a na jej vnútornom trhu by sa mala poskytovať koordinovaná podpora na testovanie a posudzovanie kybernetickej bezpečnosti subjektov pôsobiacich v odvetviach s vysokou úrovňou kritickosti určených v súlade so smernicou (EÚ) 2022/2555. Na tento účel by Komisia s podporou agentúry ENISA a v spolupráci so skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti zriadenou na základe smernice (EÚ) 2022/2555 mala pravidelne určovať relevantné odvetvia alebo pododvetvia, ktoré by mali byť oprávnené prijímať finančnú podporu na koordinované testovanie na úrovni Únie. Odvetvia alebo pododvetvia by sa mali vyberať z prílohy I k smernici (EÚ) 2022/2555 (ďalej len „odvetvia s vysokou úrovňou kritickosti“). Výkon koordinovaného testovania by mal vychádzať zo spoločných scenárov rizika a metodík. Aj vzhľadom na potrebu zabrániť duplicite by sa pri výbere odvetví	(29) V rámci opatrení v oblasti pripravenosti a v záujme presadzovania jednotného prístupu a zvýšenia bezpečnosti v celej Únii a na jej vnútornom trhu by sa mala poskytovať koordinovaná podpora na testovanie a posudzovanie kybernetickej bezpečnosti subjektov pôsobiacich v odvetviach s vysokou úrovňou kritickosti určených v súlade so smernicou (EÚ) 2022/2555. Na tento účel by Komisia s podporou agentúry ENISA a v spolupráci so skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti zriadenou na základe smernice (EÚ) 2022/2555 mala pravidelne určovať relevantné odvetvia alebo pododvetvia, ktoré by mali byť oprávnené prijímať finančnú podporu na koordinované testovanie na úrovni Únie. Odvetvia alebo pododvetvia by sa mali vyberať z prílohy I k smernici (EÚ) 2022/2555 (ďalej len „odvetvia s vysokou úrovňou kritickosti“). ***Osobitná pozornosť by sa mala venovať odvetviu dopravy a jeho pododvetviam (letecká, železničná, vodná, cestná), keďže zahŕňajú kritickú infraštruktúru, kde by***

a vypracúvaní scenárov rizika mali zohľadniť relevantné posúdenia rizík a scenáre rizika pre celú Úniu, ako sú napríklad hodnotenia rizík a scenáre rizika požadované v záveroch Rady o vývoji prístupu Európskej únie ku kybernetickej bezpečnosti, ktoré má vykonávať Komisia, vysoký predstaviteľ a skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti v spolupráci s príslušnými civilnými a vojenskými orgánmi a agentúrami a vytvorenými sieťami vrátane siete EU-CyCLONe, ako aj posúdenie rizika komunikačných sietí a infraštruktúr požadované v spoločnej ministerskej výzve z Nevers, ktoré vykonáva skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti s podporou Komisie a agentúry ENISA a v spolupráci s Orgánom európskych regulátorov pre elektronické komunikácie, koordinované posúdenia rizík, ktoré sa majú vykonávať podľa článku 22 smernice (EÚ) 2022/2555, a testovanie digitálnej prevádzkovej odolnosti stanovené v nariadení Európskeho parlamentu a Rady (EÚ) 2022/2554[29]. Pri výbere odvetví by sa malo zohľadniť aj odporúčanie Rady o celoúnijnom koordinovanom prístupe k posilneniu odolnosti kritickej infraštruktúry.

[29] Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011.

kybernetické incidenty a útoky mohli vážne ohroziť bezpečnosť cestujúcich a prevádzkovateľov. Výkon koordinovaného testovania by mal vychádzať zo spoločných scenárov rizika a metodík. Aj vzhľadom na potrebu zabrániť duplicite by sa pri výbere odvetví a vypracúvaní scenárov rizika mali zohľadniť relevantné posúdenia rizík a scenáre rizika pre celú Úniu, ako sú napríklad hodnotenia rizík a scenáre rizika požadované v záveroch Rady o vývoji prístupu Európskej únie ku kybernetickej bezpečnosti, ktoré má vykonávať Komisia, vysoký predstaviteľ a skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti v spolupráci s príslušnými civilnými a vojenskými orgánmi a agentúrami a vytvorenými sieťami vrátane siete EU-CyCLONe, ako aj posúdenie rizika komunikačných sietí a infraštruktúr požadované v spoločnej ministerskej výzve z Nevers, ktoré vykonáva skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti s podporou Komisie a agentúry ENISA a v spolupráci s Orgánom európskych regulátorov pre elektronické komunikácie, koordinované posúdenia rizík, ktoré sa majú vykonávať podľa článku 22 smernice (EÚ) 2022/2555, a testovanie digitálnej prevádzkovej odolnosti stanovené v nariadení Európskeho parlamentu a Rady (EÚ) 2022/2554[29]. Pri výbere odvetví by sa malo zohľadniť aj odporúčanie Rady o celoúnijnom koordinovanom prístupe k posilneniu odolnosti kritickej infraštruktúry.

[29] Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011.

Pozmeňujúci návrh 15

Návrh nariadenia
Odôvodnenie 30 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(30a) Vzhľadom na kritickosť tohto odvetvia a dôsledky kybernetických hrozieb na mobilitu a v dôsledku toho aj na ľudské životy cestujúcich a chodcov by sa odvetvie dopravy malo uprednostniť, pokiaľ ide o koordinované testovanie pripravenosti subjektov.

Pozmeňujúci návrh 16

Návrh nariadenia
Odôvodnenie 35 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(35a) Vzhľadom na rozšírenie úloh a povinností agentúry ENISA, ktoré vyplývajú z tohto návrhu, ako aj z návrhu aktu o kybernetickej odolnosti, je potrebné prijať opravný rozpočet agentúry ENISA č. 1/2022 na pilotné vykonávanie opatrení na podporu kybernetickej bezpečnosti. Okrem toho by sa vzhľadom na dotknuté záujmy Únie mali agentúre ENISA prideliť dodatočné finančné a ľudské zdroje.

Pozmeňujúci návrh 17

Návrh nariadenia
Odôvodnenie 38 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(38a) Rozvoj zručností a kompetencií by sa preto mal dostať do popredia vo všetkých odvetviach, v neposlednom rade aj v tých, ktoré sú vystavené kybernetickým hrozbám, ako sú zamestnanci pracujúci v hromadnej preprave alebo v kritickej infraštruktúre vrátane systémov riadenia vlakov a

	digitálnych nástrojov na plánovanie dopravy pre všetky druhy dopravy. Zavedenie a ďalší rozvoj kultúry kybernetickej bezpečnosti má preto prvoradý význam pre úspech vykonávania tohto nariadenia, pokiaľ ide o informovanosť občanov aj znalosti odborníkov vo všetkých odvetviach kritickej infraštruktúry.

Pozmeňujúci návrh 18

Návrh nariadenia
Článok 1 – odsek 2 – písmeno a

Text predložený Komisiou	*Pozmeňujúci návrh*
a) posilniť spoločné odhaľovanie kybernetických hrozieb a incidentov a situačnú informovanosť o nich v Únii, v dôsledku čoho bude možné posilniť konkurenčnú pozíciu odvetví priemyslu a služieb v Únii v rámci celého digitálneho hospodárstva a prispievať k technologickej suverenite Únie v oblasti kybernetickej bezpečnosti;	a) posilniť spoločné odhaľovanie kybernetických hrozieb a incidentov a situačnú informovanosť o nich v Únii, v dôsledku čoho bude možné posilniť konkurenčnú pozíciu odvetví priemyslu, ***dopravnej infraštruktúry*** a služieb v Únii v rámci celého digitálneho hospodárstva a prispievať k technologickej suverenite Únie v oblasti kybernetickej bezpečnosti;

Pozmeňujúci návrh 19

Návrh nariadenia
Článok 1 – odsek 2 – písmeno b

Text predložený Komisiou	*Pozmeňujúci návrh*
b) posilniť pripravenosť subjektov pôsobiacich v kritických odvetviach a v odvetviach s vysokou úrovňou kritickosti z celej Únie a posilniť solidaritu rozvíjaním kapacít spoločnej reakcie na významné alebo rozsiahle kybernetické incidenty, a to aj sprístupnením podpory Únie týkajúcej sa reakcie na kybernetické incidenty tretím krajinám pridruženým k programu Digitálna Európa;	b) posilniť pripravenosť subjektov pôsobiacich v kritických odvetviach a v odvetviach s vysokou úrovňou kritickosti z celej Únie a posilniť solidaritu rozvíjaním kapacít spoločnej reakcie na významné alebo rozsiahle kybernetické incidenty ***s osobitným dôrazom na kritickú IT a fyzickú infraštruktúru,*** a to aj sprístupnením podpory Únie týkajúcej sa reakcie na kybernetické incidenty tretím krajinám pridruženým k programu Digitálna Európa;

Pozmeňujúci návrh 20

Návrh nariadenia
Článok 1 – odsek 2 – písmeno c a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	ca) posilniť pripravenosť, spoluprácu a účinnosť Únie pri ochrane dopravnej infraštruktúry a služieb v členských štátoch pred kybernetickými incidentmi s cieľom zabezpečiť nepretržité fungovanie odvetvia dopravy, integritu dodávateľských reťazcov a mobilitu v celej Únii.

Pozmeňujúci návrh 21

Návrh nariadenia
Článok 3 – odsek 2 – pododsek 1 – písmeno c

Text predložený Komisiou	*Pozmeňujúci návrh*
c) prispieva k lepšej ochrane a reakcii na kybernetické hrozby;	c) prispieva k lepšej ochrane a reakcii na kybernetické hrozby ***a to aj v prípade dopravnej infraštruktúry, ktorá sa vyznačuje cezhraničným charakterom, ako je sieť TEN-T, alebo výmenou údajov prostredníctvom bezdrôtových technológií, ako sú inteligentné dopravné systémy.***

Pozmeňujúci návrh 22

Návrh nariadenia
Článok 3 – odsek 2 – pododsek 2

Text predložený Komisiou	*Pozmeňujúci návrh*
Vyvíja sa v spolupráci s celoeurópskou infraštruktúrou vysokovýkonnej výpočtovej techniky zriadenou na základe nariadenia (EÚ) 2021/1173.	Vyvíja sa v spolupráci s celoeurópskou infraštruktúrou vysokovýkonnej výpočtovej techniky zriadenou na základe nariadenia (EÚ) 2021/1173. ***Umožňuje spoluprácu s komunitou kybernetickej obrany prostredníctvom špecializovaných protokolov a noriem s cieľom zabezpečiť***

rozvoj silnejších spôsobilosti týkajúcich sa odhaľovania a situačnej informovanosti na ochranu kritickej infraštruktúry. V tejto súvislosti sa vytvoria synergie aj s akčným plánom v oblasti vojenskej mobility 2.0 a zabezpečí sa účinná výmena informácií s cieľom zabezpečiť situačnú informovanosť medzi vojenským a civilným odvetvím dopravy.

Pozmeňujúci návrh 23

Návrh nariadenia
Článok 8 – odsek 2 a (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	2a. Komisia zahrnie európsky kybernetický štít, najmä cezhraničné centrá bezpečnostných operácií, do svojho stanoviska pre členské štáty v rámci návrhu nariadenia o transeurópskej dopravnej sieti (COM(2021)0812) vždy, keď je pravdepodobné, že účasť alebo akýkoľvek príspevok fyzickej osoby z tretej krajiny alebo podniku z tretej krajiny ovplyvní kybernetickú bezpečnosť cezhraničnej kritickej infraštruktúry, ako je TEN-T.

Pozmeňujúci návrh 24

Návrh nariadenia
Článok 10 – odsek 1 – písmeno a

Text predložený Komisiou	*Pozmeňujúci návrh*
a) opatrenia v oblasti pripravenosti vrátane koordinovaného testovania pripravenosti subjektov pôsobiacich v odvetviach s vysokou úrovňou kritickosti v celej Únii;	a) opatrenia v oblasti pripravenosti vrátane koordinovaného testovania pripravenosti subjektov pôsobiacich v odvetviach s vysokou úrovňou kritickosti v celej Únii ***s osobitným dôrazom na dopravnú infraštruktúru a jej pododvetvia uvedené v prílohe I k smernici (EÚ) 2022/2555;***

Pozmeňujúci návrh 25

Návrh nariadenia
Článok 18 – odsek 2

Text predložený Komisiou	*Pozmeňujúci návrh*
2. S cieľom vypracovať správu o preskúmaní incidentu uvedenú v odseku 1 agentúra ENISA spolupracuje so všetkými príslušnými zainteresovanými stranami vrátane zástupcov členských štátov, Komisie a iných relevantných inštitúcií, orgánov a agentúr EÚ, poskytovateľov riadených bezpečnostných služieb a používateľov služieb v oblasti kybernetickej bezpečnosti. V prípade potreby agentúra ENISA spolupracuje aj so subjektmi zasiahnutými významnými alebo rozsiahlymi kybernetickými incidentmi. Na podporu preskúmania môže agentúra ENISA uskutočniť konzultácie aj s ďalšími druhmi zainteresovaných strán. Zástupcovia, s ktorými sa uskutočňujú konzultácie, oznámia každý potenciálny konflikt záujmov.	2. S cieľom vypracovať správu o preskúmaní incidentu uvedenú v odseku 1 agentúra ENISA spolupracuje so všetkými príslušnými zainteresovanými stranami vrátane zástupcov členských štátov, Komisie a iných relevantných inštitúcií, orgánov a agentúr EÚ, poskytovateľov riadených bezpečnostných služieb a používateľov služieb v oblasti kybernetickej bezpečnosti. V prípade potreby agentúra ENISA spolupracuje aj so subjektmi zasiahnutými významnými alebo rozsiahlymi kybernetickými incidentmi ***vrátane prevádzkovateľov dopravy.*** Na podporu preskúmania môže agentúra ENISA uskutočniť konzultácie aj s ďalšími druhmi zainteresovaných strán. Zástupcovia, s ktorými sa uskutočňujú konzultácie, oznámia každý potenciálny konflikt záujmov.

Pozmeňujúci návrh 26

Návrh nariadenia
Článok 19 – odsek 1 – bod 1 – písmeno b
Nariadenie (EÚ) 2021/694
Článok 6 – odsek 2 a (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	2a. Vzhľadom na záujmy Únie, pokiaľ ide o jej zodpovednosť za prípravu kandidátskych systémov certifikácie podľa nariadenia (EÚ) 2019/881, jej zodpovednosť za preskúmanie a posudzovanie kybernetických hrozieb, zraniteľností a zmierňovania, prípravu správy o preskúmaní incidentov pre mechanizmus preskúmania kybernetických incidentov, ako aj poskytovanie odbornej prípravy v oblasti

	kybernetických útokov a incidentov prevádzkovateľom kritickej infraštruktúry a vzhľadom na jej novo pridelené povinnosti v rámci návrhu aktu o kybernetickej odolnosti sa agentúre ENISA poskytnú potrebné zdroje z rozpočtu Únie v súlade s platnými právnymi predpismi.

Pozmeňujúci návrh 27

Návrh nariadenia
Článok 19 – odsek 1 – bod 1 a (nový)
Nariadenie (EÚ) 2021/694
Článok 7 – odsek 1 – písmeno ca (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	1a) Článok 7 sa mení takto:
	a) odsek 1 sa mení takto:
	(1) vkladá sa toto písmeno ca):
	ca) podporovať vysokokvalitnú odbornú prípravu prevádzkovateľov dopravy a manažérov a pracovníkov kritickej infraštruktúry v oblasti dopravy, a to aj s cieľom účinne zdieľať a vykonávať postupy na zmiernenie následkov v súvislosti s kybernetickými útokmi alebo incidentmi na kritickú infraštruktúru, ako napríklad postupy, ktoré poskytuje nástroj kybernetickej bezpečnosti v doprave.

POSTUP – VÝBOR POŽIADANÝ O STANOVISKO

Názov	Stanovenie opatrení na posilnenie solidarity a kapacít v Únii na odhaľovanie kybernetických hrozieb a incidentov, prípravu a reakciu na ne
Referenčné čísla	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Gestorský výbor dátum oznámenia na schôdzi	ITRE 1.6.2023
Výbor, ktorý predložil stanovisko dátum oznámenia na schôdzi	TRAN 1.6.2023
Spravodajca výboru požiadaného o stanovisko dátum vymenovania	Gheorghe Falcă 7.7.2023
Dátum prijatia	25.10.2023
Výsledok záverečného hlasovania	+: 38 –: 0 0: 0
Poslanci prítomní na záverečnom hlasovaní	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
Náhradníci prítomní na záverečnom hlasovaní	Sara Cerdas, Josianne Cutajar, Roman Haider, Pär Holmgren, Pierre Karleskind, Colm Markey, Ljudmila Novak, Dorien Rookmaker

ZÁVEREČNÉ HLASOVANIE PODĽA MIEN VO VÝBORE POŽIADANOM O STANOVISKO

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

Vysvetlenie použitých znakov:
+ : za
- : proti
0 : zdržali sa hlasovania