Europos Parlamentas
2019-2024

Transporto ir turizmo komitetas

2023/0109(COD)

25.10.2023

NUOMONĖ

Transporto ir turizmo komiteto

pateikta Pramonės, mokslinių tyrimų ir energetikos komitetui

dėl pasiūlymo dėl Europos Parlamento ir Tarybos reglamento, kuriuo nustatomos solidarumo stiprinimo ir pajėgumo aptikti kibernetinio saugumo grėsmes ir incidentus Sąjungoje, jiems pasirengti ir į juos reaguoti didinimo priemonės
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Nuomonės referentas: Gheorghe Falcă

PA_Legam

TRUMPAS PAGRINDIMAS

Nuo kibernetinių išpuolių nukentėjusios organizacijos, be kita ko, transporto sektoriuje, retai praneša apie juos, ypač privačiojo sektoriaus įmonės, nes jos linkusios tai laikyti bloga reklama. Dauguma organizacijų linkusios tokius incidentus spręsti organizacijos viduje, o dažnai juos paviešina patys užpuolikai. ES gera žinia yra ta, kad įsigaliojus Direktyvai 2022/2555 dėl tinklo saugumo (žinoma kaip TIS 2 direktyva), kurią valstybės narės turi perkelti į nacionalinę teisę iki 2024 m. spalio mėn., visose valstybėse narėse suderinamos pranešimo apie incidentus prievolės. Todėl tikėtina, kad ateinančiais metais bus geriau suprastas problemos pobūdis ir mastas.

Europos Sąjungos kibernetinio saugumo agentūra (ENISA) neseniai paskelbė ataskaitą[1], kurioje pateikiama informacija apie kibernetinio saugumo grėsmes transporto sektoriuje, kurioje pabrėžiama, kad kibernetiniai nusikaltėliai buvo atsakingi už daugiau nei pusę 2022 m. ataskaitiniu laikotarpiu nustatytų incidentų (55 proc.), o pagrindinė šių išpuolių motyvacija buvo finansinė nauda. Ji taip pat pažymi, kad dauguma kibernetinių išpuolių transporto sektoriuje nukreiptos į IT sistemas, dėl kurių kyla veiklos sutrikimų.

Kalbant apie parengtį kibernetinio saugumo incidentams ir reagavimą į juos, šiuo metu Sąjungos lygmeniu teikiama parama ir valstybių narių solidarumas yra riboti. 2022 m. gegužės mėn. Tarybos išvadose pabrėžiama, kad šias spragas reikia šalinti, ir Komisija raginama pateikti pasiūlymą dėl naujo ***Reagavimo į kibernetinio saugumo krizes fondo***[1].

Šiuo reglamentu taip pat įgyvendinama 2020 m. gruodžio mėn. priimta **ES kibernetinio saugumo strategija,** kurioje paskelbta apie **Europos kibernetinio saugumo skydo** sukūrimą, taip stiprinant kibernetinių grėsmių aptikimo ir keitimosi informacija pajėgumus Europos Sąjungoje, sujungiant nacionalinius ir tarpvalstybinius SOC. Šiame reglamente numatyti veiksmai bus remiami **finansavimu pagal Skaitmeninės Europos programos strateginį tikslą „Kibernetinis saugumas“.**

Numatytas bendro biudžeto padidinimas 100 mln. EUR; šią sumą šiame reglamente siūloma perskirstyti iš kitų Skaitmeninės Europos programos strateginių tikslų. Tai leis naują bendrą sumą, skirtą kibernetinio saugumo veiksmams pagal Skaitmeninės Europos programą, padidinti iki 842,8 mln. EUR.

Dalimi papildomos 100 mln. EUR sumos bus sustiprintas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centro ECCC valdomas biudžetas, skirtas įgyvendinti veiksmams, susijusiems su SOC ir parengtimi, pagal jų darbo programą (-as). Be to, papildomu finansavimu bus remiamas ES kibernetinio saugumo rezervo sukūrimas. Juo nuo 2023–2027 m. laikotarpio papildomas jau numatytas biudžetas, skirtas panašiems veiksmams pagal pagrindinę Skaitmeninės Europos programą ir Skaitmeninės Europos programos kibernetinio saugumo darbo programą, taigi bendra suma 2023–2027 m. galėtų sudaryti 551 mln. EUR, o 115 mln. EUR jau buvo skirta 2021–2022 m. vykdant bandomuosius

[1] Tarybos išvados dėl Europos Sąjungos pozicijos kibernetiniais klausimais parengimo, 2022 m. gegužės 23 d., dok. 9364/22.

projektus. Įskaitant valstybių narių įnašus, bendras biudžetas galėtų sudaryti iki 1,109 mlrd. EUR.

Nuomonės referento pozicija

Pranešėjas palankiai vertina naująjį pasiūlymą ir mano, kad jis bus labai naudingas įvairiems suinteresuotiesiems subjektams. Pranešėjas pabrėžia, kad būtina geriau suprasti kibernetinio saugumo transporto srityje poreikius ir reikalavimus, taip pat suteikti transporto ypatingos svarbos subjektams galimybę gauti tinkamą finansavimą pasirengimui incidentams, reagavimui į juos ir jų sprendimui.

Pranešėjas pritaria transporto kibernetinio saugumo priemonių rinkiniui, kuriuo siekiama prisidėti prie didesnio informuotumo kibernetinėje erdvėje ir kibernetinės higienos lygio, ypatingą dėmesį skiriant transporto sektoriui. Jis skirtas transporto organizacijoms, nepriklausomai nuo jų dydžio ir veiklos srities, taip pat atsižvelgiant į ypatingos svarbos transporto infrastruktūrą ir karinį mobilumą, ypač atsižvelgiant į karą Ukrainoje, visų pirma, bet neapsiribojant:

- oro vežėjams, oro uostus valdančioms įstaigoms, pagrindiniams oro uostams, oro eismo valdymo ir skrydžių valdymo centrams, Europos Sąjungos aviacijos saugos agentūrai ir Eurokontrolei;
- infrastruktūros valdytojams, geležinkelio įmonėms ir Europos geležinkelių eismo valdymo sistemai (ERTMS);
- vidaus vandenų, jūrų ir pakrančių keleivinio ir krovininio vandens transporto bendrovėms, uostų valdymo įstaigoms, įskaitant jų uosto įrenginius, subjektams, uostuose atliekantiems darbus ir eksploatuojantiems įrangą, laivų eismo paslaugų teikėjams;
- kelių direkcijoms, atsakingoms už eismo valdymo kontrolę, intelektinių transporto sistemų operatoriams;
- pašto ir kurjerių paslaugoms.

Pranešėjas mano, kad nuo **Reagavimo į nelaimes fondo kibernetiniam saugumui užtikrinti** veiklos biudžeto dydžio priklausys jo sėkmė; todėl jis turėtų būti pakankamai didelis, kad padėtų valstybėms narėms **pasirengti reikšmingiems didelio masto kibernetiniams incidentams, į juos reaguoti ir atkurti veiklą jiems įvykus.** Reagavimo į incidentus parama taip pat teikiama Sąjungos institucijoms, įstaigoms, organams ir agentūroms.

ES kibernetinio saugumo skydas pagerins valstybių narių kibernetinių grėsmių aptikimo pajėgumus. **Reagavimo į kibernetinio saugumo krizes mechanizmas** papildys valstybių narių veiksmus, pagal jį teikiant skubią paramą pasirengti, reaguoti ir kuo greičiau atkurti veiklą ir (arba) atkurti pagrindinių paslaugų veikimą.

PAKEITIMAS

Transporto ir turizmo komitetas ragina atsakingą Pramonės, mokslinių tyrimų ir energetikos komitetą atsižvelgti į šiuos pakeitimus:

Pakeitimas 1

Pasiūlymas dėl reglamento
2 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(2) kibernetinio saugumo incidentų, įskaitant tiekimo grandinės išpuolius, kurių tikslas – kibernetinis šnipinėjimas, išpirkos reikalavimo programinė įranga arba veiklos sutrikdymas, mastas, dažnumas ir poveikis didėja. Tai kelia didelę grėsmę tinklų ir informacinių sistemų veikimui. Turint omenyje sparčiai kintančias grėsmių aplinkybes, dėl galimų didelio masto incidentų, dėl kurių gali kilti didelių sutrikimų ar būti padaryta žala ypatingos svarbos infrastruktūros objektams, grėsmės reikia didinti parengtį visais Sąjungos kibernetinio saugumo sistemos lygmenimis. Ši grėsmė yra susijusi ne vien su Rusijos karine agresija prieš Ukrainą ir, tikėtina, išliks, atsižvelgiant į tai, kad dabartinę geopolitinę įtampą lemia daugybė su valstybe susijusių subjektų, nusikaltėlių ir įsilaužėlių aktyvistų. Tokie incidentai gali trukdyti teikti viešąsias paslaugas ir vykdyti ekonominę veiklą, be kita ko, ypatingos svarbos ar itin svarbiuose sektoriuose, sukelti didelių finansinių nuostolių, pakenkti naudotojų pasitikėjimui, padaryti didelės žalos Sąjungos ekonomikai ir jų padariniai gali būti pavojingi net žmonių sveikatai ar gyvybei. Be to, kibernetinio saugumo incidentai yra nenuspėjami, nes dažnai kyla ir išsiplėtoja per labai trumpą laiką, nėra susiję su jokia konkrečia geografine teritorija ir vyksta vienu metu arba akimirksniu išplinta daugelyje šalių;	(2) kibernetinio saugumo incidentų, įskaitant tiekimo grandinės išpuolius, kurių tikslas – kibernetinis šnipinėjimas, išpirkos reikalavimo programinė įranga arba veiklos sutrikdymas, mastas, dažnumas ir poveikis didėja. Tai kelia didelę grėsmę tinklų ir informacinių sistemų veikimui***, taip pat ypatingos svarbos IT ir fizinei infrastruktūrai***. Turint omenyje sparčiai kintančias grėsmių aplinkybes, dėl galimų didelio masto incidentų, dėl kurių gali kilti didelių sutrikimų ar būti padaryta žala ypatingos svarbos infrastruktūros objektams, grėsmės reikia didinti parengtį visais Sąjungos kibernetinio saugumo sistemos lygmenimis. Ši grėsmė yra susijusi ne vien su Rusijos karine agresija prieš Ukrainą ir, tikėtina, išliks, atsižvelgiant į tai, kad dabartinę geopolitinę įtampą lemia daugybė su valstybe susijusių subjektų, nusikaltėlių ir įsilaužėlių aktyvistų. Tokie incidentai gali trukdyti teikti viešąsias paslaugas***, užtikrinti visuomeninį ir privatųjį transportą*** ir vykdyti ekonominę veiklą, be kita ko, ypatingos svarbos ar itin svarbiuose sektoriuose, sukelti didelių finansinių nuostolių, pakenkti naudotojų pasitikėjimui, padaryti didelės žalos Sąjungos ekonomikai***, taip pat judumui Sąjungoje,*** ir jų padariniai gali būti pavojingi net žmonių sveikatai ar gyvybei. Be to, kibernetinio saugumo incidentai yra nenuspėjami, nes dažnai kyla ir išsiplėtoja per labai trumpą laiką, nėra susiję su jokia konkrečia geografine teritorija ir vyksta

vienu metu arba akimirksniu išplinta daugelyje šalių;

Pakeitimas 2

Pasiūlymas dėl reglamento
2 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(2a) vis didesnę kibernetinę grėsmę transporto sektoriui kelia valstybės remiami subjektai, kibernetiniai nusikaltėliai ir įsilaužėliai aktyvistai, nusikalstamą veiką vykdantys prieš institucijas, operatorius, gamintojus, tiekėjus ir paslaugų teikėjus aviacijos, jūrų, geležinkelių ir kelių transporto srityse. Europos Sąjungos kibernetinio saugumo agentūra (ENISA) pastebėjo, kad 2022 m. vidutinis mėnesinis transporto sektoriui poveikį darančių incidentų, apie kuriuos pranešta, skaičius, palyginti su 2021 m. skaičiumi, išaugo 25 proc. Dauguma šių išpuolių prieš transporto sektorių yra vykdomi prieš informacinių technologijų (IT) sistemas, dėl to gali sutrikti veikla[14a];
	[14b] ENISA, 2023, „ENISA threat landscape: Transport sector“, 7 ir 17 psl.

Pakeitimas 3

Pasiūlymas dėl reglamento
2 b konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	***(2b) dėl neišprovokuotos Rusijos invazijos į Ukrainą labai padaugėjo kibernetinių incidentų, įskaitant paskirstytojo paslaugos trikdymo (DDoS) kibernetinių atakų, nukreiptų prieš transporto sektorių ES ir netoli ES esančiose vietovėse, daugiausia oro**

	uostus, geležinkelius ir transporto institucijas[14b]. Labai tikėtina, kad tokių išpuolių vis daugės;
	[14b] ENISA, 2023, „ENISA threat landscape: Transport sector“, 9 psl.

Pakeitimas 4

Pasiūlymas dėl reglamento
2 c konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(2c) kibernetiniai išpuoliai rengiami prieš visų transporto subsektorių valdžios institucijas ir įstaigas, o tai daro poveikį geležinkelio įmonėms ir infrastruktūros valdytojams, taip pat uostų operatoriams. Kelių sektoriuje išpuoliai buvo rengiami prieš pirminės įrangos gamintojus, tiekėjus ir paslaugų teikėjus, taip pat viešojo transporto operatorius. Aviacijos sektoriuje pagrindiniai taikiniai yra oro transporto bendrovės ir oro uostų operatoriai, taip pat paslaugų teikėjai, antžeminio transporto operatoriai ir tiekimo grandinė[14c];
	[14b] ENISA, 2023, „ENISA threat landscape: Transport sector“, 17 psl.

Pakeitimas 5

Pasiūlymas dėl reglamento
3 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(3) būtina stiprinti Sąjungos pramonės ir paslaugų sektorių konkurencinę padėtį skaitmeninėje ekonomikoje ir remti jų skaitmeninę transformaciją, didinant kibernetinio saugumo lygį bendrojoje skaitmeninėje rinkoje. Kaip	(3) būtina stiprinti Sąjungos pramonės ir paslaugų sektorių konkurencinę padėtį skaitmeninėje ekonomikoje ir remti jų skaitmeninę transformaciją, didinant kibernetinio saugumo lygį bendrojoje skaitmeninėje rinkoje. Kaip

rekomenduojama trijuose skirtinguose Konferencijos dėl Europos ateities pasiūlymuose[16], būtina didinti piliečių, įmonių ir subjektų, valdančių ypatingos svarbos infrastruktūros objektus, atsparumą didėjančioms kibernetinio saugumo grėsmėms, kurios gali turėti pražūtingą poveikį visuomenei ir ekonomikai. Todėl reikia investuoti į infrastruktūrą ir paslaugas, kurios padėtų greičiau aptikti kibernetinio saugumo grėsmes bei incidentus ir į juos reaguoti, o valstybėms narėms reikia pagalbos geriau pasirengti reikšmingiems ir didelio masto kibernetinio saugumo incidentams ir į juos reaguoti. Sąjunga taip pat turėtų didinti savo pajėgumus šiose srityse, visų pirma susijusius su duomenų apie kibernetinio saugumo grėsmes ir incidentus rinkimu ir analize;	rekomenduojama trijuose skirtinguose Konferencijos dėl Europos ateities pasiūlymuose[16], būtina didinti piliečių, įmonių***, vežėjų*** ir subjektų, valdančių ypatingos svarbos infrastruktūros objektus, atsparumą didėjančioms kibernetinio saugumo grėsmėms, kurios gali turėti pražūtingą poveikį visuomenei ir ekonomikai. Todėl reikia investuoti į infrastruktūrą ir paslaugas, kurios padėtų greičiau aptikti kibernetinio saugumo grėsmes bei incidentus ir į juos reaguoti, o valstybėms narėms reikia pagalbos geriau pasirengti reikšmingiems ir didelio masto kibernetinio saugumo incidentams ir į juos reaguoti. Sąjunga taip pat turėtų didinti savo pajėgumus šiose srityse, visų pirma susijusius su duomenų apie kibernetinio saugumo grėsmes ir incidentus rinkimu ir analize***, taip pat duomenų apie kibernetinio saugumo darbo rinkos būklę ir raidą rinkimu ir analize, nes ji atlieka svarbų vaidmenį teikiant būtinas aptikimo ir reagavimo paslaugas***;
[16] https://futureu.europa.eu/lt/	[16] https://futureu.europa.eu/lt/

Pakeitimas 6

Pasiūlymas dėl reglamento
4 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(4) Sąjunga jau ėmėsi tam tikrų priemonių, kuriomis siekiama sumažinti ypatingos svarbos infrastruktūros objektų ir subjektų pažeidžiamumą ir padidinti jų atsparumą kibernetinio saugumo rizikai, visų pirma priėmė Europos Parlamento ir Tarybos direktyvą (ES) 2022/2555[17], Komisijos rekomendaciją (ES) 2017/1584[18], Europos Parlamento ir Tarybos direktyvą 2013/40/ES[19] ir Europos Parlamento ir Tarybos reglamentą (ES) 2019/881[20]. Be to, Tarybos rekomendacijoje dėl Sąjungos suderinto	(4) Sąjunga jau ėmėsi tam tikrų priemonių, kuriomis siekiama sumažinti ypatingos svarbos infrastruktūros objektų ir subjektų pažeidžiamumą ir padidinti jų atsparumą kibernetinio saugumo rizikai, visų pirma priėmė Europos Parlamento ir Tarybos direktyvą (ES) 2022/2555[17], Komisijos rekomendaciją (ES) 2017/1584[18], Europos Parlamento ir Tarybos direktyvą 2013/40/ES[19] ir Europos Parlamento ir Tarybos reglamentą (ES) 2019/881[20]***, taip pat pasiūlymą dėl reglamento dėl Sąjungos transeuropinio***

požiūrio į ypatingos svarbos infrastruktūros atsparumo didinimą valstybės narės raginamos imtis skubių ir veiksmingų priemonių ir lojaliai, veiksmingai, solidariai bei koordinuotai bendradarbiauti tarpusavyje, su Komisija ir kitomis atitinkamomis valdžios institucijomis bei atitinkamais subjektais, siekiant padidinti ypatingos svarbos infrastruktūros objektų, naudojamų esminėms paslaugoms vidaus rinkoje teikti, atsparumą;

transporto tinklo plėtros gairių ir pasiūlymą dėl reglamento dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų skaitmeninių elementų turintiems produktams (Kibernetinio atsparumo aktas). Be to, Tarybos rekomendacijoje dėl Sąjungos suderinto požiūrio į ypatingos svarbos infrastruktūros atsparumo didinimą valstybės narės raginamos imtis skubių ir veiksmingų priemonių ir lojaliai, veiksmingai, solidariai bei koordinuotai bendradarbiauti tarpusavyje, su Komisija ir kitomis atitinkamomis valdžios institucijomis bei atitinkamais subjektais, siekiant padidinti ypatingos svarbos infrastruktūros objektų, naudojamų esminėms paslaugoms vidaus rinkoje teikti, atsparumą;

---

[17] 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (OL L 333, 2022 12 27).

[18] 2017 m. rugsėjo 13 d. Komisijos rekomendacija (ES) 2017/1584 dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes (OL L 239, 2017 9 19, p. 36).

[19] 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR (OL L 218, 2013 8 14, p. 8).

[20] 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES)

[17] 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (OL L 333, 2022 12 27).

[18] 2017 m. rugsėjo 13 d. Komisijos rekomendacija (ES) 2017/1584 dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes (OL L 239, 2017 9 19, p. 36).

[19] 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR (OL L 218, 2013 8 14, p. 8).

[20] 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES)

Nr. 526/2013 (Kibernetinio saugumo aktas) (OL L 151, 2019 6 7, p. 15).	Nr. 526/2013 (Kibernetinio saugumo aktas) (OL L 151, 2019 6 7, p. 15).

Pakeitimas 7

Pasiūlymas dėl reglamento
4 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(4a) palankiai vertina Europos Komisijos Transporto kibernetinio saugumo priemonių rinkinį[2a], kuriame pateikiama pagrindinė informacija apie transporto organizacijoms galinčias kilti grėsmes (kenkimo programinės įrangos sklaida, paslaugų trikdymas, neteisėta prieiga ir vagystė, programinės įrangos manipuliavimas), ir išvardijama geroji poveikio mažinimo patirtis, tačiau vežėjams turėtų būti rengiami tinkami mokymai kibernetinio saugumo klausimais ir jiems turėtų būti suteiktos tinkamos kibernetinių grėsmių prevencijos priemonės. Iš Sąjungos biudžeto taip pat turėtų būti finansuojama ENISA teikiama parama, pavyzdžiui, mokymas, kad vežėjai galėtų veiksmingai įgyvendinti į šį priemonių rinkinį įtrauktą geriausią poveikio mažinimo patirtį;
	[1a] „ENISA threat landscape: transport sector“, ENISA, 2023 m. gegužės mėn.
	[2a] Europos Komisija, 2021. „Transport Cybersecurity Toolkit“, prieinamas adresu https://transport.ec.europa.eu/transport-themes/security-safety/cybersecurity_lt.

Pakeitimas 8

Pasiūlymas dėl reglamento
4 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*

(4a) Sąjungos mastu koordinuojamas požiūris siekiant gerinti ypatingos svarbos infrastruktūros, pvz., transporto infrastruktūros, pasirengimą ir atsparumą, grindžiamas valstybių narių pajėgumų stiprinimu. Kaip pripažinta neseniai paskelbtame Komisijos komunikate Europos Parlamentui ir Tarybai „Kibernetinio saugumo srities talentų trūkumo problemos sprendimas siekiant didinti ES konkurencingumą ir atsparumą bei skatinti jos augimą“[19a], ES saugumo negalima užtikrinti be didžiausio ES turto – jos žmonių;

[19a] Komisijos komunikatas Europos Parlamentui ir Tarybai „Kibernetinio saugumo srities talentų trūkumo problemos sprendimas siekiant didinti ES konkurencingumą ir atsparumą bei skatinti jos augimą (Kibernetinio saugumo įgūdžių akademija)“ (COM(2023) 207 final).

Pakeitimas 9

Pasiūlymas dėl reglamento
12 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(12) siekiant veiksmingiau užkirsti kelią kibernetinėms grėsmėms ir incidentams, juos įvertinti ir į juos reaguoti, būtina kaupti daugiau žinių apie Sąjungos teritorijoje esančiam ypatingos svarbos turtui ir infrastruktūros objektams kylančias grėsmes, įskaitant jų geografinį pasiskirstymą, sąsajas ir galimą poveikį tuos infrastruktūros objektus veikiančių kibernetinių išpuolių atveju. Turėtų būti įdiegta didelio masto Sąjungos SOC infrastruktūra (toliau – Europos kibernetinio saugumo skydas), kurią sudarytų kelios sąveikios tarpvalstybinės platformos, jungiančios po kelis nacionalinius SOC. Ta infrastruktūra turėtų	(12) iekiant veiksmingiau užkirsti kelią kibernetinėms grėsmėms ir incidentams, juos įvertinti ir į juos reaguoti, būtina kaupti daugiau žinių apie Sąjungos teritorijoje esančiam ypatingos svarbos turtui ir infrastruktūros objektams kylančias grėsmes, įskaitant jų geografinį pasiskirstymą, sąsajas ir galimą poveikį tuos infrastruktūros objektus veikiančių kibernetinių išpuolių atveju. ***Šis ypatingos svarbos turtas ir infrastruktūra apima intelektines transporto sistemas, kurios, nors ir labai svarbios automatizuotam ir daugiarūšiam judumui, veikia remdamosi itin svarbiais neskelbtinų duomenų mainais.*** Turėtų būti įdiegta didelio masto

būti naudinga nacionaliniams ir Sąjungos kibernetinio saugumo interesams ir poreikiams, naudojant naujausias pažangių duomenų rinkimo ir analizės priemonių technologijas, stiprinant kibernetinio saugumo grėsmių aptikimo ir valdymo pajėgumus ir užtikrinant informuotumą apie padėtį tikruoju laiku. Ta infrastruktūra turėtų padėti geriau aptikti kibernetinio saugumo grėsmes ir incidentus ir taip papildyti ir remti Sąjungos subjektus ir tinklus, atsakingus už krizių valdymą Sąjungoje, visų pirma ES ryšių palaikymo dėl kibernetinių krizių organizacinį tinklą (EU-CyCLONe), kaip apibrėžta Europos Parlamento ir Tarybos direktyvoje (ES) 2022/2555[24];	Sąjungos SOC infrastruktūra (toliau – Europos kibernetinio saugumo skydas), kurią sudarytų kelios sąveikios tarpvalstybinės platformos, jungiančios po kelis nacionalinius SOC. Ta infrastruktūra turėtų būti naudinga nacionaliniams ir Sąjungos kibernetinio saugumo interesams ir poreikiams, naudojant naujausias pažangių duomenų rinkimo ir analizės priemonių technologijas, stiprinant kibernetinio saugumo grėsmių aptikimo ir valdymo pajėgumus ir užtikrinant informuotumą apie padėtį tikruoju laiku. Ta infrastruktūra turėtų padėti geriau aptikti kibernetinio saugumo grėsmes ir incidentus ir taip papildyti ir remti Sąjungos subjektus ir tinklus, atsakingus už krizių valdymą Sąjungoje, visų pirma ES ryšių palaikymo dėl kibernetinių krizių organizacinį tinklą (EU-CyCLONe), kaip apibrėžta Europos Parlamento ir Tarybos direktyvoje (ES) 2022/2555[24];
[24] 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva) (OL L 333, 2022 12 27, p. 80).	[24] 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva) (OL L 333, 2022 12 27, p. 80).

Pakeitimas 10

Pasiūlymas dėl reglamento
14 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(14a) transporto sektorius vis dažniau tampa vienu iš pelningiausių veiklos laukų kibernetiniams nusikaltėliams – klientų duomenys laikomi labai vertinga preke, o transporto tiekimo grandinė vis dažniau tampa taikiniu. Dėl šios

	priežasties transporto infrastruktūra, kuri yra tarpvalstybinė arba kurioje keičiamasi duomenimis naudojant belaidžio ryšio technologijas, turėtų būti laikoma pagrindiniu nacionalinių ir ypač tarpvalstybinių SOC analizės ir stebėsenos objektu. Pavyzdžiui, neseniai pateiktame pasiūlyme dėl TEN-T reglamento peržiūros reikalaujama daugiau solidarumo ir bendradarbiavimo dalijantis informacija apie tarpvalstybines kibernetines grėsmes, su kuriomis gali susidurti šis tarptautinis tinklas. Intelektinės transporto sistemos (ITS) taip pat yra labai svarbios siekiant, kad transportas taptų saugesnis, efektyvesnis ir tvaresnis, tačiau dėl jų transporto sistemos tampa pažeidžiamesnės kibernetiniams išpuoliams, dėl kurių gali įvykti nelaimingų atsitikimų, susidaryti eismo spūstys arba atsirasti ekonominių nuostolių tiek privatiesiems, tiek viešiesiems vežėjams. Siekiant užtikrinti keleivių saugumą, naudotojų ir teikėjų duomenų apsaugą ir išvengti finansinės žalos, labai svarbu, kad į peržiūrėtos Intelektinių transporto sistemų direktyvos įgyvendinimo programą būtų įtrauktos nuostatos ir priemonės, kuriomis būtų stiprinamas valstybių narių bendradarbiavimas siekiant aptikti kibernetinio saugumo grėsmes ir incidentus, jiems pasirengti ir į juos reaguoti;

Pakeitimas 11

Pasiūlymas dėl reglamento
15 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(15) nacionaliniu lygmeniu kibernetinių grėsmių stebėseną, aptikimą ir analizę paprastai užtikrina viešųjų ir privačių subjektų SOC kartu su CSIRT. Be to, CSIRT keičiasi informacija CSIRT tinkle pagal Direktyvą (ES) 2022/2555.	(15) nacionaliniu lygmeniu kibernetinių grėsmių stebėseną, aptikimą ir analizę paprastai užtikrina viešųjų ir privačių subjektų SOC kartu su CSIRT. Be to, CSIRT keičiasi informacija CSIRT tinkle pagal Direktyvą (ES) 2022/2555.

Tarpvalstybiniai SOC turėtų sukurti naujus pajėgumus, kurie papildytų CSIRT tinklą, kaupiant viešųjų ir privačių subjektų duomenis apie grėsmes kibernetiniam saugumui bei jais dalijantis, didinant tokių duomenų vertę atliekant ekspertų analizę bei kartu įsigyjant infrastruktūros objektus ir taikant pažangiausias priemones, taip pat prisidedant prie Sąjungos pajėgumų ir technologinio suverenumo plėtojimo;	Tarpvalstybiniai SOC turėtų sukurti naujus pajėgumus, kurie papildytų CSIRT tinklą, kaupiant viešųjų ir privačių subjektų duomenis apie grėsmes kibernetiniam saugumui bei jais dalijantis, didinant tokių duomenų vertę atliekant ekspertų analizę bei kartu įsigyjant infrastruktūros objektus ir taikant pažangiausias priemones, taip pat prisidedant prie Sąjungos pajėgumų ir technologinio suverenumo plėtojimo. ***Šiuo atžvilgiu, siekiant sustiprinti Sąjungos savarankiškumą kibernetinėje srityje ir atsižvelgiant į pasiūlymo dėl Reglamento dėl transeuropinio transporto tinklo plėtros gairių (COM(2021)0812) 47 straipsnio 4 dalį, taip pat būtina užkirsti kelią prieigai prie duomenų, dėl kurios kyla kibernetinės grėsmės, užtikrinant patikimą reguliavimo sistemą, kuria reglamentuojama užsienio subjektų nuosavybė ir investicijos į ypatingos svarbos infrastruktūros objektus, pavyzdžiui, transporto sektoriuje;***

Pakeitimas 12

Pasiūlymas dėl reglamento
21 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(21) nors Europos kibernetinio saugumo skydas yra civilinis projektas, kibernetinės gynybos bendruomenei galėtų būti naudingi stipresni civiliniai aptikimo ir informuotumo apie padėtį pajėgumai, sukurti ypatingos svarbos infrastruktūrai apsaugoti. Tarpvalstybiniai SOC, padedami Komisijos ir Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centro (toliau – ECCC) bei bendradarbiaudami su Sąjungos vyriausiuoju įgaliotiniu užsienio reikalams ir saugumo politikai (toliau – vyriausiasis įgaliotinis), turėtų palaipsniui parengti specialius protokolus ir standartus, kad būtų galima bendradarbiauti su kibernetinės gynybos bendruomene,	(21) nors Europos kibernetinio saugumo skydas yra civilinis projektas, kibernetinės gynybos bendruomenei galėtų būti naudingi stipresni civiliniai aptikimo ir informuotumo apie padėtį pajėgumai, sukurti ypatingos svarbos infrastruktūrai apsaugoti. Tarpvalstybiniai SOC, padedami Komisijos ir Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centro (toliau – ECCC) bei bendradarbiaudami su Sąjungos vyriausiuoju įgaliotiniu užsienio reikalams ir saugumo politikai (toliau – vyriausiasis įgaliotinis), turėtų palaipsniui parengti specialius protokolus ir standartus, kad būtų galima bendradarbiauti su kibernetinės gynybos bendruomene,

įskaitant tikrinimo ir saugumo sąlygas. Kuriant Europos kibernetinio saugumo skydą turėtų būti svarstoma galimybė ateityje, glaudžiai bendradarbiaujant su vyriausiuoju įgaliotiniu, bendradarbiauti su tinklais ir platformomis, atsakingais už dalijimąsi informacija kibernetinės gynybos bendruomenėje;	įskaitant tikrinimo ir saugumo sąlygas. Kuriant Europos kibernetinio saugumo skydą turėtų būti svarstoma galimybė ateityje, glaudžiai bendradarbiaujant su vyriausiuoju įgaliotiniu, bendradarbiauti su tinklais ir platformomis, atsakingais už dalijimąsi informacija kibernetinės gynybos bendruomenėje. ***Juo taip pat turėtų būti sudarytos sąlygos sinergijai su Karinio mobilumo veiksmų planu 2.0. Gerai veikiantis karinio mobilumo tinklas turi būti atsparus, be kita ko, atsižvelgiant į kibernetines ir kitas hibridines grėsmes, kurios galėtų paveikti kritinius dvejopo naudojimo transporto sistemos mazgus. Pavyzdžiui, kibernetinis išpuolis prieš oro uostuose, jūrų uostuose ar geležinkeliuose naudojamas sistemas arba kibernetinis išpuolis prieš karinius objektus gali turėti didelių pasekmių. Todėl skaitmeninant procesus ir procedūras, be kita ko, susijusius su būtinu civiliniu ir kariniu bendradarbiavimu, kovojant su kibernetinėmis grėsmėmis reikės stiprinti kompiuterines informacines sistemas;***

Pakeitimas 13

Pasiūlymas dėl reglamento
21 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(21a) kibernetinio saugumo krizės atveju veiksmingas keitimasis informacija yra labai svarbus siekiant užtikrinti karinio ir civilinio transporto sektorių informuotumą apie padėtį. Šiuo keitimusi informacija taip pat turėtų būti skatinamas atitinkamų sektorių institucijų, atsakingų už transportą, kompetentingų kibernetinio saugumo institucijų, SOC ir CSIRT bendradarbiavimas;

Pakeitimas 14

Pasiūlymas dėl reglamento
29 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(29) vykdant pasirengimo veiksmus, siekiant skatinti nuoseklų požiūrį ir stiprinti saugumą visoje Sąjungoje ir jos vidaus rinkoje, turėtų būti teikiama parama Direktyvoje (ES) 2022/2555 nustatytuose itin svarbiuose sektoriuose veikiančių subjektų kibernetinio saugumo koordinuotam testavimui ir vertinimui. Šiuo tikslu Komisija, padedama ENISA ir bendradarbiaudama su Direktyva (ES) 2022/2555 įsteigta TIS bendradarbiavimo grupe, turėtų reguliariai nustatyti, kurie atitinkami sektoriai ar subsektoriai turėtų būti tinkami gauti finansinę paramą koordinuotam Sąjungos lygmens testavimui. Sektoriai arba subsektoriai turėtų būti atrinkti iš Direktyvos (ES) 2022/2555 I priedo („Ypatingos svarbos sektoriai“). Koordinuotas testavimas turėtų būti grindžiamas bendrais rizikos scenarijais ir metodikomis. Atrenkant sektorius ir rengiant rizikos scenarijus turėtų būti atsižvelgiama į atitinkamus Sąjungos masto rizikos vertinimus ir rizikos scenarijus, įskaitant poreikį vengti dubliavimosi, kaip antai rizikos vertinimą ir rizikos scenarijus, kuriuos Tarybos išvadose dėl Europos Sąjungos kibernetinio saugumo būklės raidos Komisija, vyriausiasis įgaliotinis ir TIS bendradarbiavimo grupė raginami parengti, derindami veiksmus su atitinkamomis civilinėmis ir karinėmis įstaigomis bei agentūromis ir sukurtais tinklais, įskaitant EU-CyCLONe, taip pat ryšių tinklų ir infrastruktūrų rizikos vertinimą, kurio buvo paprašyta Nevere paskelbtame bendrame ministrų raginime ir kurį atlieka TIS bendradarbiavimo grupė, padedant Komisijai bei ENISA ir bendradarbiaujant su Europos elektroninių ryšių reguliuotojų institucija (BEREC), koordinuotus rizikos vertinimus, kurie turi būti atliekami pagal	(29) vykdant pasirengimo veiksmus, siekiant skatinti nuoseklų požiūrį ir stiprinti saugumą visoje Sąjungoje ir jos vidaus rinkoje, turėtų būti teikiama parama Direktyvoje (ES) 2022/2555 nustatytuose itin svarbiuose sektoriuose veikiančių subjektų kibernetinio saugumo koordinuotam testavimui ir vertinimui. Šiuo tikslu Komisija, padedama ENISA ir bendradarbiaudama su Direktyva (ES) 2022/2555 įsteigta TIS bendradarbiavimo grupe, turėtų reguliariai nustatyti, kurie atitinkami sektoriai ar subsektoriai turėtų būti tinkami gauti finansinę paramą koordinuotam Sąjungos lygmens testavimui. Sektoriai arba subsektoriai turėtų būti atrinkti iš Direktyvos (ES) 2022/2555 I priedo („Ypatingos svarbos sektoriai“). ***Ypatingą dėmesį reikėtų skirti transporto sektoriui ir jo pasektoriams (oro, geležinkelių, vandens, kelių), nes jie apima ypatingos svarbos infrastruktūrą, kurioje kibernetiniai incidentai ir išpuoliai galėtų labai pakenkti keleivių ir vežėjų saugai.*** Koordinuotas testavimas turėtų būti grindžiamas bendrais rizikos scenarijais ir metodikomis. Atrenkant sektorius ir rengiant rizikos scenarijus turėtų būti atsižvelgiama į atitinkamus Sąjungos masto rizikos vertinimus ir rizikos scenarijus, įskaitant poreikį vengti dubliavimosi, kaip antai rizikos vertinimą ir rizikos scenarijus, kuriuos Tarybos išvadose dėl Europos Sąjungos kibernetinio saugumo būklės raidos Komisija, vyriausiasis įgaliotinis ir TIS bendradarbiavimo grupė raginami parengti, derindami veiksmus su atitinkamomis civilinėmis ir karinėmis įstaigomis bei agentūromis ir sukurtais tinklais, įskaitant EU-CyCLONe, taip pat ryšių tinklų ir infrastruktūrų rizikos vertinimą, kurio buvo paprašyta Nevere paskelbtame bendrame

Direktyvos (ES) 2022/2555 22 straipsnį, ir skaitmeninės veiklos atsparumo testavimą, kaip numatyta Europos Parlamento ir Tarybos reglamente (ES) 2022/2554[29]. Atrenkant sektorius taip pat reikėtų atsižvelgti į Tarybos rekomendaciją dėl Sąjungos suderinto požiūrio į ypatingos svarbos infrastruktūros atsparumo didinimą;	ministrų raginime ir kurį atlieka TIS bendradarbiavimo grupė, padedant Komisijai bei ENISA ir bendradarbiaujant su Europos elektroninių ryšių reguliuotojų institucija (BEREC), koordinuotus rizikos vertinimus, kurie turi būti atliekami pagal Direktyvos (ES) 2022/2555 22 straipsnį, ir skaitmeninės veiklos atsparumo testavimą, kaip numatyta Europos Parlamento ir Tarybos reglamente (ES) 2022/2554[29]. Atrenkant sektorius taip pat reikėtų atsižvelgti į Tarybos rekomendaciją dėl Sąjungos suderinto požiūrio į ypatingos svarbos infrastruktūros atsparumo didinimą;
[29] 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/2554 dėl skaitmeninės veiklos atsparumo finansų sektoriuje, kuriuo iš dalies keičiami reglamentai (EB) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 ir (ES) 2016/1011.	[29] 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/2554 dėl skaitmeninės veiklos atsparumo finansų sektoriuje, kuriuo iš dalies keičiami reglamentai (EB) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 ir (ES) 2016/1011.

Pakeitimas 15

Pasiūlymas dėl reglamento
30 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(30a) atsižvelgiant į sektoriaus svarbą ir kibernetinių grėsmių poveikį judumui, taigi, ir keleivių bei pėsčiųjų gyvenimui, transporto sektoriuje pirmenybę reikėtų teikti koordinuojamiems subjektų parengties bandymams;

Pakeitimas 16

Pasiūlymas dėl reglamento
35 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*

	(35a) atsižvelgiant į šiuo pasiūlymu ir pasiūlymu dėl Kibernetinio atsparumo akto agentūrai ENISA suteiktas didesnes užduotis ir atsakomybę, būtina priimti ENISA taisomąjį biudžetą Nr. 1/2022 dėl bandymo įgyvendinti paramos kibernetiniam saugumui veiksmus. Be to, atsižvelgiant į Sąjungos interesus, agentūrai ENISA reikėtų skirti papildomų finansinių ir žmogiškųjų išteklių;

Pakeitimas 17

Pasiūlymas dėl reglamento
38 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(38a) todėl įgūdžių ir kompetencijų ugdymui reikėtų skirti daugiausia dėmesio visuose sektoriuose, ypač tuose, kurie yra pažeidžiami kibernetinio saugumo grėsmių, pavyzdžiui, daugiausiai dėmesio turėtų sulaukti darbuotojai, dirbantys masinio tranzito srityje arba ypatingos svarbos infrastruktūros objektuose, įskaitant traukinių kontrolės sistemas ir skaitmenines visų rūšių transporto planavimo priemones. Todėl kibernetinio saugumo kultūros įdiegimas ir tolesnis plėtojimas visuose ypatingos svarbos infrastruktūros sektoriuose yra labai svarbūs siekiant sėkmingai įgyvendinti šį reglamentą tiek piliečių informuotumo, tiek specialistų žinių požiūriu;

Pakeitimas 18

Pasiūlymas dėl reglamento
1 straipsnio 2 dalies a punktas

Komisijos siūlomas tekstas	*Pakeitimas*
a) stiprinti bendrą Sąjungos kibernetinių grėsmių ir incidentų aptikimą ir informuotumą apie padėtį, taip sudarant	a) stiprinti bendrą Sąjungos kibernetinių grėsmių ir incidentų aptikimą ir informuotumą apie padėtį, taip sudarant

sąlygas stiprinti Sąjungos pramonės ir paslaugų sektorių konkurencinę padėtį visoje skaitmeninėje ekonomikoje ir prisidėti prie Sąjungos technologinio suverenumo kibernetinio saugumo srityje;	sąlygas stiprinti Sąjungos pramonės***, transporto infrastruktūros*** ir paslaugų sektorių konkurencinę padėtį visoje skaitmeninėje ekonomikoje ir prisidėti prie Sąjungos technologinio suverenumo kibernetinio saugumo srityje;

Pakeitimas 19

Pasiūlymas dėl reglamento
1 straipsnio 2 dalies b punktas

Komisijos siūlomas tekstas	*Pakeitimas*
b) stiprinti subjektų, veikiančių ypatingos svarbos ir itin svarbiuose sektoriuose visoje Sąjungoje, parengtį ir solidarumą plėtojant bendrus reagavimo į reikšmingus arba didelio masto kibernetinio saugumo incidentus pajėgumus, be kita ko, teikiant Sąjungos paramą reaguojant į kibernetinio saugumo incidentus Skaitmeninės Europos programos (SEP) asocijuotosioms trečiosioms valstybėms;	b) stiprinti subjektų, veikiančių ypatingos svarbos ir itin svarbiuose sektoriuose visoje Sąjungoje, parengtį ir solidarumą plėtojant bendrus reagavimo į reikšmingus arba didelio masto kibernetinio saugumo incidentus pajėgumus, ***ypač daug dėmesio skiriant didelės svarbos IT ir fizinei infrastruktūrai,*** be kita ko, teikiant Sąjungos paramą reaguojant į kibernetinio saugumo incidentus Skaitmeninės Europos programos (SEP) asocijuotosioms trečiosioms valstybėms;

Pakeitimas 20

Pasiūlymas dėl reglamento
1 straipsnio 2 dalies c a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ca) stiprinti Sąjungos pasirengimą, bendradarbiavimą ir veiksmingumą valstybėse narėse apsaugant transporto infrastruktūrą ir paslaugas nuo kibernetinio saugumo incidentų, užtikrinti nuolatinį transporto sektoriaus veikimą, tiekimo grandinių vientisumą ir judumą visoje Sąjungoje;

Pakeitimas 21

Pasiūlymas dėl reglamento
3 straipsnio 2 dalies 1 pastraipos c punktas

Komisijos siūlomas tekstas	*Pakeitimas*
c) padeda geriau apsisaugoti nuo kibernetinių grėsmių ir į jas reaguoti;	c) padeda geriau apsisaugoti nuo kibernetinių grėsmių ir į jas reaguoti***, be kita ko, transporto infrastruktūrai, kuriai būdingas tarpvalstybiškumas, pvz., TEN-T, arba keičiantis duomenimis naudojant belaidžio ryšio technologijas, pvz., intelektines transporto sistemas***;

Pakeitimas 22

Pasiūlymas dėl reglamento
3 straipsnio 2 dalies 2 pastraipa

Komisijos siūlomas tekstas	*Pakeitimas*
Jis plėtojamas bendradarbiaujant su visos Europos našiosios kompiuterijos infrastruktūra, sukurta pagal Reglamentą (ES) 2021/1173.	Jis plėtojamas bendradarbiaujant su visos Europos našiosios kompiuterijos infrastruktūra, sukurta pagal Reglamentą (ES) 2021/1173. ***Ji sudaro sąlygas bendradarbiauti su kibernetinės gynybos bendruomene, pasitelkiant tam skirtus protokolus ir standartus, taip siekiant užtikrinti, kad būtų plėtojami tvirtesni civiliniai aptikimo ir informuotumo apie padėtį pajėgumai siekiant apsaugoti ypatingos svarbos infrastruktūrą. Šiuo atžvilgiu taip pat turi būti plėtojama sinergija su Karinio mobilumo veiksmų planu 2.0 ir užtikrinamas veiksmingas keitimasis informacija, kad karinio ir civilinio transporto sektoriai būtų informuoti apie padėtį.***

Pakeitimas 23

Pasiūlymas dėl reglamento
8 straipsnio 2 a dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	2a. Komisija įtraukia ES kibernetinio saugumo skydą, visų pirma

	tarpvalstybinius SOC, į savo nuomonę valstybėms narėms pagal pasiūlymą dėl reglamento dėl transeuropinio transporto tinklo (COM(2021)0812) tais atvejais, kai trečiosios valstybės fizinio asmens arba trečiosios valstybės įmonės dalyvavimas ar indėlis gali daryti poveikį tarpvalstybinės ypatingos svarbos infrastruktūros, pvz., TEN-T, kibernetiniam saugumui.

Pakeitimas 24

Pasiūlymas dėl reglamento
10 straipsnio 1 dalies a punktas

Komisijos siūlomas tekstas	*Pakeitimas*
a) pasirengimo veiksmai, įskaitant koordinuotą subjektų, veikiančių itin svarbiuose sektoriuose visoje Sąjungoje, parengties testavimą;	a) pasirengimo veiksmai, įskaitant koordinuotą subjektų, veikiančių itin svarbiuose sektoriuose visoje Sąjungoje, parengties testavimą***, ypatingą dėmesį skiriant į Direktyvos (ES) 2022/2555 I priedą įtrauktai transporto infrastruktūrai ir jos pasektoriams***;

Pakeitimas 25

Pasiūlymas dėl reglamento
18 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
2. Rengdama 1 dalyje nurodytą incidento peržiūros ataskaitą, ENISA bendradarbiauja su visais atitinkamais suinteresuotaisiais subjektais, įskaitant valstybių narių, Komisijos, kitų atitinkamų ES institucijų, įstaigų ir agentūrų, valdomų saugumo paslaugų teikėjų ir kibernetinio saugumo paslaugų naudotojų atstovus. Kai tinkama, ENISA taip pat bendradarbiauja su reikšmingų arba didelio masto kibernetinio saugumo incidentų paveiktais subjektais. Atlikdama peržiūrą, ENISA gali konsultuotis ir su kitais suinteresuotaisiais subjektais. Atstovai, su kuriais konsultuojamasi, atskleidžia informaciją	2. Rengdama 1 dalyje nurodytą incidento peržiūros ataskaitą, ENISA bendradarbiauja su visais atitinkamais suinteresuotaisiais subjektais, įskaitant valstybių narių, Komisijos, kitų atitinkamų ES institucijų, įstaigų ir agentūrų, valdomų saugumo paslaugų teikėjų ir kibernetinio saugumo paslaugų naudotojų atstovus. Kai tinkama, ENISA taip pat bendradarbiauja su reikšmingų arba didelio masto kibernetinio saugumo incidentų paveiktais subjektais***, įskaitant vežėjus***. Atlikdama peržiūrą, ENISA gali konsultuotis ir su kitais suinteresuotaisiais subjektais. Atstovai, su kuriais konsultuojamasi,

apie bet kokį galimą interesų konfliktą.	atskleidžia informaciją apie bet kokį galimą interesų konfliktą.

Pakeitimas 26

Pasiūlymas dėl reglamento
19 straipsnio 1 pastraipos 1 punkto b papunktis
Reglamentas (ES) 2021/694
6 straipsnio 2 a dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	2a. Atsižvelgiant į aktualius Sąjungos interesus, kiek tai susiję su jos pareigomis parengti potencialias sertifikavimo schemas pagal Reglamentą (ES) 2019/881, jos atsakomybe peržiūrėti ir vertinti kibernetines grėsmes, pažeidžiamumą ir poveikio švelninimą, parengti incidentų peržiūros ataskaitą dėl kibernetinio saugumo incidentų peržiūros mechanizmo, taip pat rengti mokymus ypatingos svarbos infrastruktūros operatoriams kovos su kibernetiniais išpuoliais ir incidentais klausimais, taip pat atsižvelgiant į naujas pareigas, jai pavestas pagal pasiūlymą dėl Kibernetinio atsparumo akto, ENISA suteikiami reikiami ištekliai iš Sąjungos biudžeto, laikantis taikytinų teisės aktų.

Pakeitimas 27

Pasiūlymas dėl reglamento
19 straipsnio 1 pastraipos 1 a punktas (naujas)
Reglamentas (ES) 2021/694
7 straipsnio 1 punkto c a papunktis (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	1a) 7 straipsnis iš dalies keičiamas taip:
	a) 1 dalis iš dalies keičiama taip:
	1) įterpiamas šis ca punktas:
	ca) remti aukštos kokybės mokymus vežėjams ir transporto ypatingos svarbos

infrastruktūros objektų valdytojams ir darbuotojams, be kita ko, siekiant veiksmingai dalytis patirtimi, susijusia su kibernetiniais išpuoliais ar incidentais ypatingos svarbos infrastruktūros objektų atžvilgiu, ir įgyvendinti atitinkamas poveikio mažinimo priemones, pavyzdžiui, numatytas Transporto kibernetinio saugumo priemonių rinkinyje.

NUOMONĘ TEIKIANČIO KOMITETO PROCEDŪRA

Pavadinimas	Solidarumo stiprinimo ir pajėgumo aptikti kibernetinio saugumo grėsmes ir incidentus Sąjungoje, jiems pasirengti ir į juos reaguoti didinimo priemonių nustatymas
Nuorodos	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Atsakingas komitetas Paskelbimo plenariniame posėdyje data	ITRE 1.6.2023
Nuomonę pateikė Paskelbimo plenariniame posėdyje data	TRAN 1.6.2023
Nuomonės referentas (-ė) Paskyrimo data	Gheorghe Falcă 7.7.2023
Priėmimo data	25.10.2023
Galutinio balsavimo rezultatai	+: 38 –: 0 0: 0
Posėdyje per galutinį balsavimą dalyvavę nariai	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
Posėdyje per galutinį balsavimą dalyvavę pavaduojantys nariai	Sara Cerdas, Josianne Cutajar, Roman Haider, Pär Holmgren, Pierre Karleskind, Colm Markey, Ljudmila Novak, Dorien Rookmaker

GALUTINIS VARDINIS BALSAVIMAS NUOMONĘ TEIKIANČIAME KOMITETE

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

Sutartiniai ženklai:
+ : už
- : prieš
0 : susilaikė