



Odbor za promet i turizam

2023/0109(COD)

25.10.2023

MIŠLJENJE

Odbora za promet i turizam

upućeno Odboru za industriju, istraživanje i energetiku

o Prijedlogu uredbe Europskog parlamenta i Vijeća o utvrđivanju mjera za povećanje solidarnosti i kapaciteta u Uniji za otkrivanje kibersigurnosnih prijetnji i incidenata, pripremu za njih i odgovor na njih (COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Izvjestitelj za mišljenje: Gheorghe Falcă

PA_Legam

KRATKO OBRAZLOŽENJE

Organizacije pogodjene kibernapadima, među ostalim u prometnom sektoru, rijetko ih prijavljuju, posebno kada je riječ o poduzećima iz privatnog sektora, jer ih obično smatraju „lošim publicitetom”. Većina organizacija napade radije rješava interno, dok ih napadači često iznose u javnost. Dobra je vijest za EU da će se stupanjem na snagu Direktive 2022/2555 o sigurnosti mreže (poznate kao „Direktiva NIS 2”), koju države članice moraju prenijeti u svoja zakonodavstva do listopada 2024., uskladiti obveze prijavljivanja incidenata u svim državama članicama. Stoga će se u narednim godinama vjerojatno bolje razumjeti priroda i razmjer tog problema.

Agencija Europske unije za kibersigurnost (ENISA) nedavno je objavila izvješeć¹ koje sadržava informacije o kibersigurnosnim prijetnjama u prometnom sektoru i u kojem se naglašava da su kiberkriminalci odgovorni za više od polovine incidenata zabilježenih u izvještajnom razdoblju 2022. (55 %) te da su ti napadi većinom bili motivirani finansijskom dobiti. Također se napominje da je većina kibernapada u prometnom sektoru usmjerenata na IT sustave i da uzrokuje prekide u radu.

Kad je riječ o pripravnosti i odgovoru na kibersigurnosne incidente, potpora na razini Unije i solidarnost među državama članicama trenutno su ograničene. U zaključcima Vijeća iz svibnja 2022. istaknuta je potreba za uklanjanjem tih nedostataka i Komisija je pozvana da predstavi prijedlog o novom **Fondu za odgovor na hitne situacije u području kibersigurnosti**².

Predmetnom uredbom provodi se **Strategija EU-a za kibersigurnost** donesena u prosincu 2020. u kojoj je najavljenja uspostava **europskog kiberštita**, kojim bi se ojačali kapaciteti za otkrivanje kiberprijetnji i razmjeni informacija u Europskoj uniji putem saveza nacionalnih i prekograničnih centara za sigurnosne operacije (SOC-ovi). Mjere iz te uredbe podupirat će se **financiranjem u okviru strateškog cilja „Kibersigurnost“ programa Digitalna Europa**.

Ukupni proračun uključuje povećanje od 100 milijuna EUR, a ovom se uredbom predlaže da se taj iznos preraspodjeli iz drugih strateških ciljeva programa Digitalna Europa. Time će se novi ukupni iznos dostupan za mjere u području kibersigurnosti u okviru programa Digitalna Europa povećati na 842,8 milijuna EUR.

Jedan dio od tih dodatnih 100 milijuna EUR iskoristit će se za povećanje proračuna kojim upravlja Europski stručni centar u području kibersigurnosti kako bi se provele mjere za SOC-ove i pripravnost u okviru njihovih programa rada. Nadalje, dodatna sredstva poslužit će za potporu uspostavi kibersigurnosne pričuve EU-a. Njima se dopunjaje proračun koji je već predviđen za slična djelovanja u glavnom programu Digitalna Europa i programu rada u području kibersigurnosti programa Digitalna Europa za razdoblje 2023. – 2027., čime bi se ukupni iznos mogao povećati na 551 milijun za razdoblje 2023. – 2027., dok je iznos od 115 milijuna već bio izdvojen u obliku pilot-projekata za razdoblje 2021. – 2022. Kad se pribroje doprinosi država članica, ukupni bi proračun mogao iznositi do 1 109 milijardi EUR.

¹ [„Understanding Cyber Threats in Transport“](#) (Razumijevanje kiberprijetnji u prometu), ENISA, objavljeno 21. ožujka 2023.

² Zaključci Vijeća o razvoju položaja Europske unije u pogledu kiberprostora od 23. svibnja 2022., (9364/22).

Stajalište izvjestitelja

Izvjestitelj pozdravlja novi prijedlog i smatra da će on donijeti znatne koristi raznim dionicima. Izvjestitelj naglašava da je potrebno bolje razumjeti potrebe i zahtjeve u pogledu kibersigurnosti u prometu, kao i osigurati da ključni subjekti u području prometa imaju pristup odgovarajućim finansijskim sredstvima za pripravnost, djelovanje i rješavanje incidenata.

Izvjestitelj podržava „skup alata za kibersigurnost u prometu” kojim se nastoji doprinijeti većoj razini osviještenosti o kibersigurnosti i kiberhigijeni, posebno u području prometnog sektora. Namijenjen je organizacijama u prometnom sektoru, bez obzira na njihovu veličinu i područje djelovanja, i njime se također uzimaju u obzir ključna prometna infrastruktura i vojna mobilnost, posebno s obzirom na rat u Ukrajini, te je posebno, ali ne i isključivo, usmjeren na:

- zračne prijevoznike, upravljačka tijela zračnih luka, osnovne zračne luke, centre upravljanja zračnim prometom i kontrole zračnog prometa, Agenciju Europske unije za sigurnost zračnog prometa i Eurocontrol;
- upravitelje infrastrukture, željezničke prijevoznike i Europski sustav za upravljanje željezničkim prometom (ERTMS);
- kompanije za prijevoz putnika i tereta unutarnjim plovnim putovima, morem i duž obale, upravljačka tijela luka, uključujući njihove lučke objekte, subjekte koji upravljaju poslovima i opremom u lukama, operatore službe za nadzor i upravljanje prometovanjem plovila;
- tijela nadležna za ceste odgovorna za kontrolu upravljanja prometom, operatore inteligentnih prometnih sustava;
- poštanske i kurirske usluge.

Izvjestitelj smatra da će iznos proračuna za funkcioniranje **Fonda za odgovor na hitne situacije u području kibersigurnosti** (ERFC) odrediti njegovu uspješnost; stoga bi on trebao biti dovoljno velik kako bi se državama članicama pomoglo u **pripremi** za značajne kibersigurnosne incidente i kibersigurnosne incidente velikih razmjera, **odgovoru na njih i hitnom oporavku od njih**. Potpora za odgovor na incidente stavlja se na raspolaganje i institucijama, tijelima, uredima i agencijama Unije.

Europskim kiberštitom poboljšat će se sposobnosti država članica za otkrivanje kiberprijetnji. **Mehanizmom za izvanredne kibersigurnosne situacije** dopunit će se mjere država članica osiguravanjem hitne potpore za pripravnost, odgovor i hitni oporavak / ponovnu uspostavu funkcioniranja ključnih usluga.

AMANDMANI

Odbor za promet i turizam poziva Odbor za industriju, istraživanje i energetiku da kao nadležni odbor uzme u obzir sljedeće:

Amandman 1

Prijedlog uredbe Uvodna izjava 2.

Tekst koji je predložila Komisija

(2) Povećavaju se razmjeri i učestalost te pogoršavaju posljedice kiberincidenata, uključujući napade na lance opskrbe s ciljem kiberšpijunaže, napad ucjenjivačkim softverom ili izazivanje poremećaja. Oni predstavljaju veliku prijetnju funkcioniranju mrežnih i informacijskih sustava. S obzirom na to da se prijetnje brzo mijenjaju, mogući incidenti velikih razmjera koji uzrokuju znatne poremećaje ili štetu na kritičnoj infrastrukturi zahtijevaju povećanu pripravnost na svim razinama okvira Unije za kibersigurnost. Ta prijetnja nadilazi rusku vojnu agresiju na Ukrajinu i vjerojatno će se nastaviti s obzirom na mnoštvo državi bliskih, kriminalnih i haktivističkih aktera umiješanih u trenutačne geopolitičke napetosti. Takvi incidenti mogu ometati pružanje javnih usluga i obavljanje gospodarskih djelatnosti, među ostalim u kritičnim ili visokokritičnim sektorima, uzrokovati znatne finansijske gubitke, narušiti povjerenje korisnika, nanijeti veliku štetu gospodarstvu Unije te čak imati zdravstvene ili po život opasne posljedice. K tomu, kibersigurnosni incidenti su nepredvidivi jer se često pojavljuju i razvijaju u vrlo kratkim vremenskim razdobljima, nisu ograničeni na određeno zemljopisno područje i događaju se istodobno u mnogim zemljama ili se brzo šire na mnoge zemlje.

Izmjena

(2) Povećavaju se razmjeri i učestalost te pogoršavaju posljedice kiberincidenata, uključujući napade na lance opskrbe s ciljem kiberšpijunaže, napad ucjenjivačkim softverom ili izazivanje poremećaja. Predstavljaju veliku prijetnju funkcioniranju mrežnih i informacijskih sustava **te kritične IT i fizičke infrastrukture**. S obzirom na to da se prijetnje brzo mijenjaju, mogući incidenti velikih razmjera koji uzrokuju znatne poremećaje ili štetu na kritičnoj infrastrukturi zahtijevaju povećanu pripravnost na svim razinama okvira Unije za kibersigurnost. Ta prijetnja nadilazi rusku vojnu agresiju na Ukrajinu i vjerojatno će se nastaviti s obzirom na mnoštvo državi bliskih, kriminalnih i haktivističkih aktera umiješanih u trenutačne geopolitičke napetosti. Takvi incidenti mogu ometati pružanje javnih usluga **te usluga javnog i privatnog prijevoza** i obavljanje gospodarskih djelatnosti, među ostalim u kritičnim ili visokokritičnim sektorima, uzrokovati znatne finansijske gubitke, narušiti povjerenje korisnika, nanijeti veliku štetu gospodarstvu Unije, **kao i mobilnosti unutar Unije** te čak imati zdravstvene ili po život opasne posljedice. K tomu, kibersigurnosni incidenti su nepredvidivi jer se često pojavljuju i razvijaju u vrlo kratkim vremenskim razdobljima, nisu ograničeni na određeno zemljopisno područje i događaju se istodobno u

mnogim zemljama ili se brzo šire na mnoge zemlje.

Amandman 2

Prijedlog uredbe

Uvodna izjava 2.a (nova)

Tekst koji je predložila Komisija

Izmjena

(2a) Sve ozbiljniju kibersigurnosnu prijetnju prometnom sektoru predstavljaju akteri pod pokroviteljstvom države, kiberkriminalci i haktivisti kojima su mete nadležna tijela, operatori, proizvođači, dobavljači i pružatelji usluga u zračnom, pomorskom, željezničkom i cestovnom prometu. Agencija Europske unije za kibersigurnost (ENISA) zabilježila je 2022. povećanje prosječnog mjesecnog broja prijavljenih incidenata koji utječe na prometni sektor za 25 % u odnosu na razine iz 2021. Većina napada na prometni sektor usmjereni su na sustave informacijske tehnologije (IT), a oni mogu uzrokovati prekide u radu^{14a}.

^{14b} ENISA (2023.), Izvješće ENISA-e o prijetnjama: Prometni sektor, stranice 7. i 17.

Amandman 3

Prijedlog uredbe

Uvodna izjava 2.b (nova)

Tekst koji je predložila Komisija

Izmjena

(2b) Ničim izazvana ruska invazija na Ukrajinu dovela je do znatnog povećanja kibersigurnosnih incidenata, uključujući distribuirane kibernapade uskraćivanjem usluga (DDoS), usmjereni na prometni sektor u EU-u i područjima u blizini EU-a, uglavnom zračne luke, željeznice i tijela nadležna za promet^{14b}. Vrlo je vjerojatno

da će se taj porast napada nastaviti.

^{14b} ENISA (2023.), Izvješće ENISA-e o prijetnjama: Prometni sektor, stranica 9.

Amandman 4

Prijedlog uredbe Uvodna izjava 2.c (nova)

Tekst koji je predložila Komisija

Izmjena

(2c) Kibernapadi su usmjereni na tijela vlasti i tijela u svim prometnim podsektorima, pri čemu su pogodjeni željeznički prijevoznici i upravitelji infrastrukture, kao i lučka poduzeća. Kad je riječ o cestovnom sektoru, ciljani su bili proizvođači originalne opreme, dobavljači i pružatelji usluga, kao i javni prijevoznici. U zrakoplovnom sektoru glavni su ciljevi bili zračni prijevoznici i upravitelji zračnih luka, a slijede ih pružatelji usluga, operateri površinskog prijevoza i lanac opskrbe^{14c}.

^{14c} ENISA (2023.), Izvješće ENISA-e o prijetnjama: Prometni sektor, stranica 17.

Amandman 5

Prijedlog uredbe Uvodna izjava 3.

Tekst koji je predložila Komisija

Izmjena

(3) Neophodno je ojačati konkurentni položaj industrije i uslužnih sektora u Uniji u cijelom digitaliziranom gospodarstvu i poduprijeti njihovu digitalnu transformaciju povećanjem razine kibersigurnosti na jedinstvenom digitalnom tržištu. Kako je preporučeno u trima različitim prijedlozima Konferencije o budućnosti Europe¹⁶, potrebno je povećati

(3) Neophodno je ojačati konkurentni položaj industrije i uslužnih sektora u Uniji u cijelom digitaliziranom gospodarstvu i poduprijeti njihovu digitalnu transformaciju povećanjem razine kibersigurnosti na jedinstvenom digitalnom tržištu. Kako je preporučeno u trima različitim prijedlozima Konferencije o budućnosti Europe¹⁶, potrebno je povećati

otpornost građana, poduzeća i subjekata koji upravljaju kritičnim infrastrukturnama na sve veće kibersigurnosne prijetnje koje mogu imati razorne društvene i gospodarske posljedice. Stoga su potrebna ulaganja u infrastrukturu i usluge kojima će se omogućiti brže otkrivanje kibersigurnosnih prijetnji i incidenata i odgovor na njih, a državama članicama potrebna je pomoći u boljoj pripremi za značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera i odgovoru na njih. Unija bi isto tako trebala povećati svoje kapacitete u tim područjima, posebno u pogledu prikupljanja i analize podataka o kibersigurnosnim prijetnjama i incidentima.

¹⁶ <https://futureu.europa.eu/hr/>

otpornost građana, poduzeća, *prijevoznika* i subjekata koji upravljaju kritičnim infrastrukturnama na sve veće kibersigurnosne prijetnje koje mogu imati razorne društvene i gospodarske posljedice. Stoga su potrebna ulaganja u infrastrukturu i usluge kojima će se omogućiti brže otkrivanje kibersigurnosnih prijetnji i incidenata i odgovor na njih, a državama članicama potrebna je pomoći u boljoj pripremi za značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera i odgovoru na njih. Unija bi isto tako trebala povećati svoje kapacitete u tim područjima, posebno u pogledu prikupljanja i analize podataka o kibersigurnosnim prijetnjama i incidentima ***te o stanju i razvoju tržišta rada u području kibersigurnosti jer ima ključnu ulogu u pružanju potrebnih usluga otkrivanja i odgovora.***

¹⁶ <https://futureu.europa.eu/hr/>

Amandman 6

Prijedlog uredbe Uvodna izjava 4.

Tekst koji je predložila Komisija

(4) Unija je već poduzela niz mjera za smanjenje ranjivosti i povećanje otpornosti kritičnih infrastruktura i subjekata u pogledu kibersigurnosnih rizika, koje posebice uključuju Direktivu (EU) 2022/2555 Europskog parlamenta i Vijeća¹⁷, Preporuku Komisije (EU) 2017/1584¹⁸, Direktivu 2013/40/EU Europskog parlamenta i Vijeća¹⁹ i Uredbu (EU) 2019/881 Europskog parlamenta i Vijeća²⁰. Nапослјетку, у Препоруци Вijeća о координiranom pristupu на razini Unije radi jačanja otpornosti kritične infrastrukture države članice se pozivaju da poduzmu hitne i učinkovite mjere te da surađuju lojalno, učinkovito, solidarno i

Izmjena

(4) Unija je već poduzela niz mjera za smanjenje ranjivosti i povećanje otpornosti kritičnih infrastruktura i subjekata u pogledu kibersigurnosnih rizika, koje posebice uključuju Direktivu (EU) 2022/2555 Europskog parlamenta i Vijeća¹⁷, Preporuku Komisije (EU) 2017/1584¹⁸, Direktivu 2013/40/EU Europskog parlamenta i Vijeća¹⁹ i Uredbu (EU) 2019/881 Europskog parlamenta i Vijeća²⁰, ***kao i Prijedlog uredbe o smjernicama za razvoj transeuropske prometne mreže te Prijedlog uredbe o horizontalnim kibersigurnosnim zahtjevima za proizvode s digitalnim elementima (Akt o kiberotpornosti).***

koordinirano međusobno, s Komisijom i drugim relevantnim javnim tijelima te predmetnim subjektima kako bi se povećala otpornost kritične infrastrukture koja se koristi za pružanje osnovnih usluga na unutarnjem tržištu.

Naposljetku, u Preporuci Vijeća o koordiniranom pristupu na razini Unije radi jačanja otpornosti kritične infrastrukture države članice se pozivaju da poduzmu hitne i učinkovite mjere te da surađuju lojalno, učinkovito, solidarno i koordinirano međusobno, s Komisijom i drugim relevantnim javnim tijelima te predmetnim subjektima kako bi se povećala otpornost kritične infrastrukture koja se koristi za pružanje osnovnih usluga na unutarnjem tržištu.

¹⁷ Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (SL L 333, 27.12.2022.).

¹⁸ Preporuka Komisije (EU) 2017/1584 od 13. rujna 2017. o koordiniranom odgovoru na kiberincidente i kiberkrise velikih razmjera (SL L 239, 19.9.2017., str. 36.).

¹⁹ Direktiva 2013/40/EU Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP (SL L 218, 14.8.2013., str. 8.).

²⁰ Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti), (SL L 151, 7.6.2019., str. 15.).

¹⁷ Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (SL L 333, 27.12.2022.).

¹⁸ Preporuka Komisije (EU) 2017/1584 od 13. rujna 2017. o koordiniranom odgovoru na kiberincidente i kiberkrise velikih razmjera (SL L 239, 19.9.2017., str. 36.).

¹⁹ Direktiva 2013/40/EU Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP (SL L 218, 14.8.2013., str. 8.).

²⁰ Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti), (SL L 151, 7.6.2019., str. 15.).

Amandman 7

Prijedlog uredbe Uvodna izjava 4.a (nova)

Tekst koji je predložila Komisija

Izmjena

(4a) Iako pozdravlja skup alata Europske komisije za kibersigurnost u prometu^{2a}, koji sadržava osnovne informacije o prijetnjama koje mogu utjecati na prometne organizacije (širenje zlonamjernog softvera, uskraćivanje usluge, neovlašten pristup i krađa te manipulacija softverom) i u kojem se navode dobre prakse ublažavanja, prijevoznici bi trebali dobiti odgovarajuće osposobljavanje o kibersigurnosti i odgovarajuće alate za sprečavanje kiberprijetnji. Proračun Unije trebao bi pokrivati i potporu, kao što je osposobljavanje, koju pruža ENISA kako bi se prijevoznicima omogućila učinkovita provedba najboljih praksi ublažavanja uključenih u taj skup alata.

^{1a} Izvješće ENISA-e o prijetnjama: prometni sektor/ENISA, ožujak 2023.

^{2a} Europska komisija (2021.). Skup alata za kibersigurnost u prometu, dostupan na https://transport.ec.europa.eu/transport-themes/security-safety/cybersecurity_hr

Amandman 8

Prijedlog uredbe Uvodna izjava 4.a (nova)

Tekst koji je predložila Komisija

Izmjena

(4a) Koordinirani pristup na razini Unije za jačanje pripravnosti i otpornosti kritične infrastrukture, kao što je prometna infrastruktura, temelji se na izgradnji kapaciteta država članica. Kako je potvrđeno u nedavnoj komunikaciji Komisije Europskom parlamentu i Vijeću naslovljenoj „Povećanjem broja stručnjaka za kibersigurnost do veće konkurentnosti, rasta i otpornosti Unije”^{19a}, sigurnost EU-a nije moguće

zajamčiti bez sudjelovanja njezina najvrednijeg kapitala: njezinih stanovnika.

^{19a} Komunikacija Komisije Europskom parlamentu i Vijeću: Povećanjem broja stručnjaka za kibersigurnost do veće konkurentnosti, rasta i otpornosti Unije („Akademija za vještine u području kibersigurnosti” COM(2023) 207 final

Amandman 9

Prijedlog uredbe Uvodna izjava 12.

Tekst koji je predložila Komisija

(12) Kako bi se učinkovitije spriječile i procijenile kiberprijetnje i kiberincidenti te na njih odgovorilo, potrebno je steći sveobuhvatnije znanje o prijetnjama ključnim resursima i infrastrukturi na području Unije, uključujući njihovu geografsku raspoređenost, međusobnu povezanost i potencijalne posljedice u slučaju kibernapada koji poguđaju te infrastrukture. Trebalo bi uvesti opsežnu infrastrukturu EU-a za SOC-ove („europski kiberštit”), koja se sastoji od nekoliko interoperabilnih prekograničnih platformi, od kojih svaka okuplja nekoliko nacionalnih SOC-ova. Ta bi infrastruktura trebala služiti kibersigurnosnim interesima i potrebama na nacionalnoj razini i razini Unije, koristeći se najsuvremenijom tehnologijom za napredne alate za prikupljanje i analizu podataka, jačajući kapacitete otkrivanja i upravljanja kibertehnologijama i osiguravajući informiranost o stanju u stvarnom vremenu. Ta bi infrastruktura trebala služiti za bolje otkrivanje kibersigurnosnih prijetnji i incidenata te na taj način dopunjavati i podržavati subjekte i mreže Unije odgovorne za upravljanje krizama u Uniji, posebno Europsku mrežu

Izmjena

(12) Kako bi se učinkovitije spriječile i procijenile kiberprijetnje i kiberincidenti te na njih odgovorilo, potrebno je steći sveobuhvatnije znanje o prijetnjama ključnim resursima i infrastrukturi na području Unije, uključujući njihovu geografsku raspoređenost, međusobnu povezanost i potencijalne posljedice u slučaju kibernapada koji poguđaju te infrastrukture. *Ti kritični resursi i infrastrukture uključuju inteligentne prometne sustave, koji, iako su ključni za automatiziranu i multimodalnu mobilnost, djeluju na temelju ključnih razmjena osjetljivih podataka.* Trebalo bi uvesti opsežnu infrastrukturu EU-a za SOC-ove („europski kiberštit”), koja se sastoji od nekoliko interoperabilnih prekograničnih platformi, od kojih svaka okuplja nekoliko nacionalnih SOC-ova. Ta bi infrastruktura trebala služiti kibersigurnosnim interesima i potrebama na nacionalnoj razini i razini Unije, koristeći se najsuvremenijom tehnologijom za napredne alate za prikupljanje i analizu podataka, jačajući kapacitete otkrivanja i upravljanja kibertehnologijama i osiguravajući informiranost o stanju u stvarnom vremenu. Ta bi infrastruktura

organizacija za vezu za kiberkrize („EU-CyCLONe”), kako je definirana u Direktivi (EU) 2022/2555 Europskog parlamenta i Vijeća²⁴.

trebala služiti za bolje otkrivanje kibersigurnosnih prijetnji i incidenata te na taj način dopunjavati i podržavati subjekte i mreže Unije odgovorne za upravljanje krizama u Uniji, posebno Europsku mrežu organizacija za vezu za kiberkrize („EU-CyCLONe”), kako je definirana u Direktivi (EU) 2022/2555 Europskog parlamenta i Vijeća²⁴.

²⁴ Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2) (SL L 333, 27.12.2022., str. 80.).

²⁴ Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2) (SL L 333, 27.12.2022., str. 80.).

Amandman 10

Prijedlog uredbe Uvodna izjava 14.a (nova)

Tekst koji je predložila Komisija

Izmjena

(14a) Prometni sektor sve više postaje jedno od najunosnijih područja poslovanja za kiberkriminalce, pri čemu se podaci o kupcima smatraju vrlo vrijednom robom, a sve se više cilja na lanac opskrbe u prijevozu. Zbog toga bi se prometna infrastruktura koju karakterizira prekogranična priroda ili razmjena podataka bežičnim tehnologijama trebala smatrati ključnim predmetom analize i praćenja za nacionalne, a posebno za prekogranične SOC-ove. Na primjer, nedavni prijedlog revizije Uredbe o mreži TEN-T zahtijeva veću solidarnost i suradnju u razmjeni informacija o prekograničnim kiberprijetnjama s kojima bi se ta transnacionalna mreža mogla suočiti. Isto tako, inteligentni prometni sustavi (ITS) ključni su za sigurniji, učinkovitiji i održiviji promet, ali zbog njih su prometni

sustavi osjetljiviji na kibernapade koji mogu prouzročiti nesreće, prometne gužve ili uzrokovati gospodarske gubitke i privatnim i javnim subjektima. Kako bi se osigurala sigurnost putnika te zaštita podataka korisnika i pružatelja usluga i izbjegla finansijska šteta, ključno je da program provedbe revidirane direktive o inteligentnim prometnim sustavima sadržava odredbe i alate za jačanje suradnje među državama članicama u otkrivanju kibersigurnosnih prijetnji i incidenata te pripremi za njih i odgovaranju na njih.

Amandman 11

Prijedlog uredbe Uvodna izjava 15.

Tekst koji je predložila Komisija

(15) Na nacionalnoj razini praćenje, otkrivanje i analizu kiberprijetnji obično osiguravaju SOC-ovi javnih i privatnih subjekata, u kombinaciji sa CSIRT-ovima. Osim toga, CSIRT-ovi razmjenjuju informacije u kontekstu mreže CSIRT-ova, u skladu s Direktivom (EU) 2022/2555. Prekogranični SOC-ovi trebali bi predstavljati nove kapacitete koji su komplementarni mreži CSIRT-ova jer bi objedinjavali i dijelili podatke o kibersigurnosnim prijetnjama dobivene od javnih i privatnih subjekata, povećavali vrijednost takvih podataka stručnom analizom i zajednički nabavljenom infrastrukturom i najsvremenijim alatima te doprinosili razvoju sposobnosti i tehnološke suverenosti Unije.

Izmjena

(15) Na nacionalnoj razini praćenje, otkrivanje i analizu kiberprijetnji obično osiguravaju SOC-ovi javnih i privatnih subjekata, u kombinaciji sa CSIRT-ovima. Osim toga, CSIRT-ovi razmjenjuju informacije u kontekstu mreže CSIRT-ova, u skladu s Direktivom (EU) 2022/2555. Prekogranični SOC-ovi trebali bi predstavljati nove kapacitete koji su komplementarni mreži CSIRT-ova jer bi objedinjavali i dijelili podatke o kibersigurnosnim prijetnjama dobivene od javnih i privatnih subjekata, povećavali vrijednost takvih podataka stručnom analizom i zajednički nabavljenom infrastrukturom i najsvremenijim alatima te doprinosili razvoju sposobnosti i tehnološke suverenosti Unije. *U tom pogledu, kako bi se ojačala autonomija Unije u području kibersigurnosti i s obzirom na članak 47. stavak 4. Prijedloga uredbe o smjernicama za razvoj transeuropske prometne mreže (COM(2021)0812), potrebno je i spriječiti pristup podacima koji dovode do kiberprijetnji provedbom čvrstog*

regulatornog okvira kojim se uređuju strano vlasništvo i ulaganja u kritičnu infrastrukturu, kao što je promet.

Amandman 12

Prijedlog uredbe Uvodna izjava 21.

Tekst koji je predložila Komisija

(21) Iako je europski kiberštit civilni projekt, zajednica za kiberobranu mogla bi imati koristi od bolje sposobnosti za civilno otkrivanje i informiranost o stanju koji su razvijeni za zaštitu kritične infrastrukture. Prekogranični SOC-ovi, uz potporu Komisije i Europskog stručnog centra u području kibersigurnosti (ECCC) te u suradnji s Visokim predstavnikom Unije za vanjske poslove i sigurnosnu politiku („Visoki predstavnik”), trebali bi postupno razvijati namjenske protokole i standarde kako bi se omogućila suradnja sa zajednicom za kiberobranu, uključujući uvjete provjere i sigurnosti. Razvoj europskog kiberštita trebao bi biti popraćen razmatranjem načina na koji bi se omogućila buduća suradnja s mrežama i platformama odgovornima za dijeljenje informacija u zajednici za kiberobranu, u bliskoj suradnji s Visokim predstavnikom.

Izmjena

(21) Iako je europski kiberštit civilni projekt, zajednica za kiberobranu mogla bi imati koristi od bolje sposobnosti za civilno otkrivanje i informiranost o stanju koji su razvijeni za zaštitu kritične infrastrukture. Prekogranični SOC-ovi, uz potporu Komisije i Europskog stručnog centra u području kibersigurnosti (ECCC) te u suradnji s Visokim predstavnikom Unije za vanjske poslove i sigurnosnu politiku („Visoki predstavnik”), trebali bi postupno razvijati namjenske protokole i standarde kako bi se omogućila suradnja sa zajednicom za kiberobranu, uključujući uvjete provjere i sigurnosti. Razvoj europskog kiberštita trebao bi biti popraćen razmatranjem načina na koji bi se omogućila buduća suradnja s mrežama i platformama odgovornima za dijeljenje informacija u zajednici za kiberobranu, u bliskoj suradnji s Visokim predstavnikom.

Njime bi se također trebale omogućiti sinergije s Akcijskim planom za vojnu mobilnost 2.0. Funkcionalna mreža vojne mobilnosti mora biti otporna, među ostalim u okolnostima kiberprijetnji i drugih hibridnih prijetnji koje bi mogle utjecati na ključna čvorista u prometnom sustavu s dvojnom namjenom. Na primjer, kibernapad na sustave koji se upotrebljavaju u zračnim lukama, lukama ili željeznicama ili kibernapad na vojna sredstva mogao bi imati znatne posljedice. Stoga će digitalizacija procesa i postupaka, među ostalim za potrebnu civilnu i vojnu suradnju, zahtijevati jačanje računalnih informacijskih sustava

za borbu protiv kiberprijetnji.

Amandman 13

Prijedlog uredbe Uvodna izjava 21.a (nova)

Tekst koji je predložila Komisija

Izmjena

(21a) U slučaju kibersigurnosne krize učinkovita razmjena informacija ključna je za osiguravanje informiranosti o stanju u vojnem i civilnom prometnom sektoru. Tom razmjenom informacija trebala bi se poticati i suradnja između relevantnih sektorskih tijela odgovornih za promet, nadležnih tijela za kibersigurnost, SOCOva i CSIRT-ova.

Amandman 14

Prijedlog uredbe Uvodna izjava 29.

Tekst koji je predložila Komisija

Izmjena

(29) U okviru mjera pripravnosti, radi promicanja dosljednog pristupa i jačanja sigurnosti u cijeloj Uniji i na njezinu unutarnjem tržištu, trebalo bi pružiti potporu koordiniranom testiranju i procjeni kibersigurnosti subjekata koji djeluju u visokokritičnim sektorima utvrđenima u skladu s Direktivom (EU) 2022/2555. U tu bi svrhu Komisija, uz potporu ENISA-e i u suradnji sa Skupinom za suradnju u području sigurnosti mrežnih i informacijskih sustava osnovanom Direktivom (EU) 2022/2555, trebala redovito utvrđivati relevantne sektore ili podsektore koji bi trebali biti prihvatljivi za primanje financijske potpore za koordinirano testiranje na razini Unije. Sektore ili podsektore trebalo bi odabrati iz Priloga I. Direktivi (EU) 2022/2555 („Sektori visoke kritičnosti“). Koordinirane vježbe testiranja trebale bi se temeljiti na

(29) U okviru mjera pripravnosti, radi promicanja dosljednog pristupa i jačanja sigurnosti u cijeloj Uniji i na njezinu unutarnjem tržištu, trebalo bi pružiti potporu koordiniranom testiranju i procjeni kibersigurnosti subjekata koji djeluju u visokokritičnim sektorima utvrđenima u skladu s Direktivom (EU) 2022/2555. U tu bi svrhu Komisija, uz potporu ENISA-e i u suradnji sa Skupinom za suradnju u području sigurnosti mrežnih i informacijskih sustava osnovanom Direktivom (EU) 2022/2555, trebala redovito utvrđivati relevantne sektore ili podsektore koji bi trebali biti prihvatljivi za primanje financijske potpore za koordinirano testiranje na razini Unije. Sektore ili podsektore trebalo bi odabrati iz Priloga I. Direktivi (EU) 2022/2555 („Sektori visoke kritičnosti“). **Posebnu pozornost trebalo bi posvetiti prometnom**

zajedničkim scenarijima i metodama procjene rizika. Pri odabiru sektora i razvoju scenarija rizika trebalo bi uzeti u obzir relevantne procjene rizika i scenarije rizika na razini Unije, uključujući potrebu za izbjegavanjem njihova udvostručavanja, kao što su procjena rizika i scenariji rizika zatraženi u Zaključcima Vijeća o razvoju položaja Europske unije u pogledu kiberprostora koje trebaju provesti Komisija, Visoki predstavnik i Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava, u koordinaciji s relevantnim civilnim i vojnim tijelima i agencijama te uspostavljenim mrežama, uključujući mrežu EU-CyCLONe, procjena rizika komunikacijskih mreža i infrastruktura koju je zatražila Zajednička ministarska skupina u Neversu i koju je provela Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava, uz potporu Komisije i ENISA-e te u suradnji s Tijelom europskih regulatora za električke komunikacije (BEREC), koordinirane procjene rizika koje treba provesti na temelju članka 22. Direktive (EU) 2022/2555 i testiranje digitalne operativne otpornosti predviđeno Uredbom (EU) 2022/2554 Europskog parlamenta i Vijeća²⁹. Pri odabiru sektora trebalo bi uzeti u obzir i Preporuku Vijeća o koordiniranom pristupu na razini Unije za jačanje otpornosti kritične infrastrukture.

sektoru i njegovim podsektorima (zračnom, željezničkom, vodnom i cestovnom) jer uključuju kritičnu infrastrukturu u kojoj bi kiberincidenti i kibernapadi mogli ozbiljno ugroziti sigurnost putnika i prijevoznika.

Koordinirane vježbe testiranja trebale bi se temeljiti na zajedničkim scenarijima i metodama procjene rizika. Pri odabiru sektora i razvoju scenarija rizika trebalo bi uzeti u obzir relevantne procjene rizika i scenarije rizika na razini Unije, uključujući potrebu za izbjegavanjem njihova udvostručavanja, kao što su procjena rizika i scenariji rizika zatraženi u Zaključcima Vijeća o razvoju položaja Europske unije u pogledu kiberprostora koje trebaju provesti Komisija, Visoki predstavnik i Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava, u koordinaciji s relevantnim civilnim i vojnim tijelima i agencijama te uspostavljenim mrežama, uključujući mrežu EU-CyCLONe, procjena rizika komunikacijskih mreža i infrastruktura koju je zatražila Zajednička ministarska skupina u Neversu i koju je provela Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava, uz potporu Komisije i ENISA-e te u suradnji s Tijelom europskih regulatora za električke komunikacije (BEREC), koordinirane procjene rizika koje treba provesti na temelju članka 22. Direktive (EU) 2022/2555 i testiranje digitalne operativne otpornosti predviđeno Uredbom (EU) 2022/2554 Europskog parlamenta i Vijeća²⁹. Pri odabiru sektora trebalo bi uzeti u obzir i Preporuku Vijeća o koordiniranom pristupu na razini Unije za jačanje otpornosti kritične infrastrukture.

²⁹ Uredba (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i

²⁹ Uredba (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i

(EU) 2016/1011.

(EU) 2016/1011.

Amandman 15

Prijedlog uredbe Uvodna izjava 30.a (nova)

Tekst koji je predložila Komisija

Izmjena

(30a) S obzirom na kritičnost sektora i posljedice kiberprijetnji na mobilnost, a time i na živote putnika i pješaka, prometni sektor trebao bi imati prioritet u pogledu koordiniranog testiranja pripravnosti subjekata.

Amandman 16

Prijedlog uredbe Uvodna izjava 35.a (nova)

Tekst koji je predložila Komisija

Izmjena

(35a) S obzirom na povećane zadaće i odgovornosti koje su ENISA-i dodijeljene ovim prijedlogom i prijedlogom Akta o kiberotpornosti, potrebno je donijeti izmjenu proračuna 1/2022 ENISA-e za pilot-provedbu potpornog djelovanja u području kibersigurnosti. Nadalje, s obzirom na relevantne interese Unije, ENISA-i bi trebalo dodijeliti dodatne finansijske i ljudske resurse.

Amandman 17

Prijedlog uredbe Uvodna izjava 38.a (nova)

Tekst koji je predložila Komisija

Izmjena

(38a) Stoga bi razvoj vještina i kompetencija trebao biti u središtu pozornosti u svim sektorima, posebno onima koji su osjetljivi na kibersigurnosne prijetnje, kao što je

osoblje koje radi na infrastrukturnama masovnog tranzita ili kritičnim infrastrukturnama, uključujući sustave kontrole vlakova i digitalne alate za planiranje prometa za sve vrste prijevoza. Uvođenje i daljnji razvoj kulture kibersigurnosti stoga su ključni za uspjeh provedbe ove Uredbe, kako u smislu osviještenosti građana tako i u smislu stručnog znanja u svim sektorima kritične infrastrukture.

Amandman 18

Prijedlog uredbe

Članak 1. – stavak 2. – točka a

Tekst koji je predložila Komisija

(a) poboljšanje zajedničkog otkrivanja kiberprijetnji i kiberincidenata te zajedničke informiranosti o njihovu stanju u Uniji da bi se omogućilo učvršćivanje konkurentnog položaja industrijskog i uslužnog sektora u Uniji u cijelom digitalnom gospodarstvu te doprinijelo tehnološkom suverenitetu Unije u području kibersigurnosti;

Izmjena

(a) poboljšanje zajedničkog otkrivanja kiberprijetnji i kiberincidenata te zajedničke informiranosti o njihovu stanju u Uniji da bi se omogućilo učvršćivanje konkurentnog položaja industrijskog sektora, **sektora prometne infrastrukture** i uslužnog sektora u Uniji u cijelom digitalnom gospodarstvu te doprinijelo tehnološkom suverenitetu Unije u području kibersigurnosti;

Amandman 19

Prijedlog uredbe

Članak 1. – stavak 2. – točka b

Tekst koji je predložila Komisija

(b) podizanje pripravnosti subjekata koji djeluju u kritičnim i visokokritičnim sektorima u Uniji i jačanje solidarnosti razvojem zajedničkih kapaciteta za odgovor na značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera, među ostalim stavljanjem potpore Unije za odgovor na kibersigurnosne incidente na raspolaganje trećim zemljama pridruženima programu

Izmjena

(b) podizanje pripravnosti subjekata koji djeluju u kritičnim i visokokritičnim sektorima u Uniji i jačanje solidarnosti razvojem zajedničkih kapaciteta za odgovor na značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera, **uz posvećivanje posebne pozornosti kritičnoj IT i fizičkoj infrastrukturi**, među ostalim stavljanjem potpore Unije za odgovor na

Digitalna Europa („DEP”);

kibersigurnosne incidente na raspolaganje trećim zemljama pridruženima programu Digitalna Europa („DEP”);

Amandman 20

Prijedlog uredbe

Članak 1. – stavak 2. – točka ca (nova)

Tekst koji je predložila Komisija

Izmjena

(ca) jačanje pripravnosti, suradnje i učinkovitosti Unije u zaštiti prometne infrastrukture i usluga u državama članicama od kiberincidenata kako bi se osigurali kontinuirano funkcioniranje prometnog sektora, integritet lanaca opskrbe i mobilnost diljem Unije.

Amandman 21

Prijedlog uredbe

Članak 3. – stavak 2. – podstavak 1. – točka c

Tekst koji je predložila Komisija

Izmjena

(c) doprinosi boljoj zaštiti i odgovoru na kiberprijetnje;

(c) doprinosi boljoj zaštiti i odgovoru na kiberprijetnje, **među ostalim za prometnu infrastrukturu prekogranične prirode, kao što je mreža TEN-T, ili prometnu infrastrukturu kojoj je svojstvena razmjena podataka bežičnim tehnologijama, kao što su inteligentni prometni sustavi.**

Amandman 22

Prijedlog uredbe

Članak 3. – stavak 2. – podstavak 2.

Tekst koji je predložila Komisija

Izmjena

Razvija se u suradnji s paneuropskom infrastrukturom računalstva visokih performansi uspostavljenom na temelju Uredbe (EU) 2021/1173.

Razvija se u suradnji s paneuropskom infrastrukturom računalstva visokih performansi uspostavljenom na temelju Uredbe (EU) 2021/1173. **Njime se putem**

posebnih protokola i standarda omogućuje suradnja sa zajednicom za kiberobranu kako bi se osigurao razvoj snažnijih sposobnosti civilnog otkrivanja i informiranosti o stanju za zaštitu kritične infrastrukture. U tom pogledu razvijaju se sinergije i s Akcijskim planom za vojnu mobilnost 2.0 te se osigurava učinkovita razmjena informacija kako bi se pružila informiranost o stanju u vojnem i civilnom prometnom sektoru.

Amandman 23

Prijedlog uredbe

Članak 8. – stavak 2.a (novi)

Tekst koji je predložila Komisija

Izmjena

2.a Komisija uključuje europski kiberštít, a posebno prekogranične SOC-ove, u svoje mišljenje upućeno državama članicama u okviru Prijedloga uredbe o transeuropskoj prometnoj mreži (COM(2021)0812) kad god bi sudjelovanje ili doprinos bilo koje vrste fizičke osobe iz treće zemlje ili poduzeća iz treće zemlje mogli utjecati na kibersigurnost prekogranične kritične infrastrukture, kao što je TEN-T.

Amandman 24

Prijedlog uredbe

Članak 10. – stavak 1. – točka a

Tekst koji je predložila Komisija

Izmjena

(a) mjere pripravnosti, uključujući koordinirano testiranje pripravnosti subjekata koji djeluju u visokokritičnim sektorima u Uniji;

(a) mjere pripravnosti, uključujući koordinirano testiranje pripravnosti subjekata koji djeluju u visokokritičnim sektorima u Uniji, s *posebnim naglaskom na prometnoj infrastrukturi i njezinim podsektorima iz Priloga I. Direktivi (EU) 2022/255*;

Amandman 25

Prijedlog uredbe Članak 18. – stavak 2.

Tekst koji je predložila Komisija

2. ENISA u pripremi izvješća o istraživanju incidenta iz stavka 1. surađuje sa svim relevantnim dionicima, uključujući predstavnike država članica, Komisije, drugih relevantnih institucija, tijela i agencija EU-a, pružatelja upravljanih sigurnosnih usluga i korisnika usluga kibersigurnosti. ENISA prema potrebi surađuje i sa subjektima pogodenima značajnim kibersigurnosnim incidentom ili kibersigurnosnim incidentom velikih razmjera. Kao pomoć u istraživanju, ENISA se može savjetovati i s drugim vrstama dionika. Konzultirani predstavnici dužni su dati informacije o svakom mogućem sukobu interesa.

Izmjena

2. ENISA u pripremi izvješća o istraživanju incidenta iz stavka 1. surađuje sa svim relevantnim dionicima, uključujući predstavnike država članica, Komisije, drugih relevantnih institucija, tijela i agencija EU-a, pružatelja upravljanih sigurnosnih usluga i korisnika usluga kibersigurnosti. ENISA prema potrebi surađuje i sa subjektima pogodenima značajnim kibersigurnosnim incidentom ili kibersigurnosnim incidentom velikih razmjera, **uključujući prijevoznike**. Kao pomoć u istraživanju, ENISA se može savjetovati i s drugim vrstama dionika. Konzultirani predstavnici dužni su dati informacije o svakom mogućem sukobu interesa.

Amandman 26

Prijedlog uredbe Članak 19. – stavak 1. – točka 1. – podtočka b Uredba (EU) 2021/694 Članak 6. – stavak 2.a (novi)

Tekst koji je predložila Komisija

Izmjena

2.a S obzirom na relevantne interese Unije, u vezi s odgovornostima ENISA-e za pripremu prijedloga programa certifikacije u skladu s Uredbom (EU) 2019/881, njezinim odgovornostima za preispitivanje i procjenu kiberprijetnji i ranjivosti te njihovo ublažavanje, pripremu izvješća o istraživanju incidenata za mehanizam za istraživanje kibersigurnosnih incidenata, kao i za pružanje sposobljavanja operatora kritične infrastrukture protiv kibernapada i incidenata te s obzirom na odgovornosti koje su joj nedavno dodijeljene u okviru

Prijedloga akta o kiberotpornosti, ENISA-i se u skladu s primjenjivim zakonodavstvom osiguravaju potrebna sredstva iz proračuna Unije.

Amandman 27

Prijedlog uredbe

Članak 19. – stavak 1. – točka 1.a (nova)

Uredba (EU) 2021/694

Članak 7. – stavak 1. – točka ca (nova)

Tekst koji je predložila Komisija

Izmjena

(1a) članak 7. mijenja se kako slijedi:

(a) stavak 1. mijenja se kako slijedi:

(1) umeće se sljedeća točka (ca):

(ca) podupiranje visokokvalitetnog osposobljavanja prijevoznika te upravitelja i radne snage u području kritične infrastrukture u sektoru prometa, među ostalim u cilju učinkovite razmjene i provedbe praksi ublažavanja u slučaju kibernapada ili incidenta u području kritične infrastrukture, kao što su one koje pruža skup alata za kibersigurnost u prometu.

POSTUPAK U ODBORU KOJI DAJE MIŠLJENJE

Naslov	Utvrđivanje mjera za povećanje solidarnosti i kapaciteta u Uniji za otkrivanje kibersigurnosnih prijetnji i incidenata, pripremu za njih i odgovor na njih
Referentni dokumenti	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Nadležni odbor Datum objave na plenarnoj sjednici	ITRE 1.6.2023
Odbori koji su dali mišljenje Datum objave na plenarnoj sjednici	TRAN 1.6.2023
Izvjestitelj(ica) za mišljenje Datum imenovanja	Gheorghe Falcă 7.7.2023
Datum usvajanja	25.10.2023

Rezultat konačnog glasovanja	+: -: 0:	38 0 0
Zastupnici nazočni na konačnom glasovanju	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	
Zamjenici nazočni na konačnom glasovanju	Sara Cerdas, Josianne Cutajar, Roman Haider, Pär Holmgren, Pierre Karleskind, Colm Markey, Ljudmila Novak, Dorien Rookmaker	

POIMENIČNO KONAČNO GLASOVANJE U ODBORU KOJI DAJE MIŠLJENJE

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

Korišteni znakovi:

- + : za
- : protiv
- 0 : suzdržani