EUROPOS AUDITO RŪMAI

LT

Nuomonė 02/ 2023

pagal SESV 322 straipsnio 1 dalį

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 [2023 m. balandžio 18 d. tarpinstitucinė byla 2023/0109(COD)]

Turinys

	Dalis
Įvadas	01–03
Bendrosios pastabos	04–05
Konkrečios pastabos	06–40
Nėra poveikio vertinimo	06–08
Dalinė informacija apie finansavimą	09–12
Dalinė informacija apie finansavimą ir žmogiškųjų išteklių poreikius	09–10
Dalinė informacija apie Europos kibernetinio saugumo skydo finansinę struktūrą	11–12
Su Europos kibernetinio saugumo skydu susijusi rizika	13–26
Padidėjęs sudėtingumas ir papildomi lygmenys	13–20
Dalijimasis informacija	21–26
Su Reagavimo į kibernetinio saugumo krizes mechanizmu susijusi rizika	27–34
ES kibernetinio saugumo rezervo panaudojimas	27–29
Nukrypimas nuo metinio periodiškumo principo	30–34
Su Kibernetinio saugumo incidentų peržiūros mechanizmu susijusi rizika	35–36
Veiksmingumo stebėsena ir politikos vertinimas	37–40
Baigiamosios pastabos	41–43
Priedas. Europos kibernetinio saugumo sistema	

Įvadas

01 2023 m. balandžio 18 d. Komisija paskelbė pasiūlymą 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 (toliau – ES kibernetinio solidarumo aktas).

02 Siūlomame ES kibernetinio solidarumo akte nustatytos kibernetinio saugumo grėsmių ir incidentų aptikimo, pasirengimo jiems ir reagavimo į juos priemonės, visų pirma:

- **Europos kibernetinio saugumo skydas**, skirtas koordinuotiems aptikimo ir informuotumo apie padėtį pajėgumams sukurti ir stiprinti;
- **Reagavimo į kibernetinio saugumo krizes mechanizmas**, skirtas padėti valstybėms narėms pasirengti reikšmingiems ir didelio masto kibernetinio saugumo incidentams, į juos reaguoti ir atkurti veiklą po jų;
- **Kibernetinio saugumo incidentų peržiūros mechanizmas**, skirtas reikšmingiems arba didelio masto incidentams peržiūrėti ir įvertinti.

03 Pagal Komisijos pasiūlymo teisinį pagrindą reikalaujama konsultuotis su Europos Audito Rūmais[1]. Europos Parlamentas ir Europos Sąjungos Taryba atitinkamai 2023 m. birželio 2 d. ir birželio 7 d. raštu paprašė mūsų pateikti savo nuomonę. Šia nuomone įvykdomas šis konsultavimosi reikalavimas.

[1] Sutarties dėl Europos Sąjungos veikimo 322 straipsnio 1 dalis.

Bendrosios pastabos

04 Pagrindinė atsakomybė už kibernetinio saugumo incidentų ir krizių prevenciją, pasirengimą jiems ir reagavimą į juos tenka jų paveiktoms valstybėms narėms. Pagal Europos Sąjungos sutarties 4 straipsnio 2 dalį, už nacionalinį saugumą ir toliau išlieka atsakinga kiekviena valstybė narė. Tačiau galimas reikšmingų arba didelio masto kibernetinio saugumo incidentų poveikis reiškia, kad gali prireikti imtis bendrų veiksmų ES lygmeniu.

05 Audito Rūmai palankiai vertina pasiūlymo tikslus stiprinti ES kolektyvinį kibernetinį atsparumą. Šioje nuomonėje pateikiame konkrečias pastabas dėl trijų siūlomo ES kibernetinio solidarumo akto komponentų ir atkreipiame dėmesį į tam tikrą mūsų nustatytą riziką, susijusią su neatliktu poveikio vertinimu, finansiniais aspektais ir tuo, kaip galėtų būti įgyvendinamos pasiūlyme nustatytos priemonės. Visų pirma pabrėžiame, kad dėl siūlomo reglamento visa ES kibernetinio saugumo sistema gali tapti sudėtingesnė, ir siūlome šios rizikos mažinimo būdus (žr. ***13***–***20*** dalis).

Konkrečios pastabos

Nėra poveikio vertinimo

06 Komisijos geresnio reglamentavimo gairėse atliekant išsamią politikos rengimo ir įgyvendinimo galimybių analizę siūloma naudoti poveikio vertinimus ir konsultacijas su suinteresuotaisiais subjektais. Manome, kad išsamūs poveikio vertinimai yra pagrindinė priemonė siekiant nustatyti, ar reikia ES veiksmų, ir išanalizuoti galimą siūlomų sprendimų poveikį prieš priimant bet kokį pasiūlymą.

07 Šio siūlomo reglamento poveikio vertinimas nebuvo atliktas. Pridedamo aiškinamojo memorandumo 3 skirsnyje Komisija paaiškino nusprendusi tokio vertinimo neatlikti, nes *pasiūlymas yra skubus*. Ji taip pat teigė, kad siūlomu reglamentu nustatytos priemonės bus remiamos pagal Skaitmeninės Europos programą (SEP) ir atitinka SEP reglamentą, kurio konkretus poveikio vertinimas atliktas 2018 m. Be to, Komisija paaiškino, kad siūlomos priemonės buvo grindžiamos ankstesniais veiksmais, parengtais glaudžiai bendradarbiaujant su pagrindiniais suinteresuotaisiais subjektais ir valstybėmis narėmis, įtraukiant įgytą patirtį.

08 Tačiau pažymime, kad SEP poveikio vertinimas neapima siūlomu reglamentu nustatytų naujų priemonių. Todėl turima nedaug informacijos apie esamas politikos galimybes ir su pasiūlymu susijusias išlaidas.

Dalinė informacija apie finansavimą

Dalinė informacija apie finansavimą ir žmogiškųjų išteklių poreikius

09 ES kibernetinio solidarumo akte nustatytos priemonės bus finansuojamos pagal SEP. Aiškinamojo memorandumo 4 skirsnyje Komisija nurodė, kad 115 milijonų eurų Europos kibernetinio saugumo skydui jau buvo skirta 2021–2022 m. vykdant bandomuosius projektus. Ji taip pat nurodė, kad pasiūlymu 2023–2027 m. SEP konkrečiam kibernetinio saugumo ir pasitikėjimo tikslui skirtas 743 milijonų eurų biudžetas bus padidintas 100 milijonų eurų, perskirstant lėšas viduje.

10 Po šio perskirstymo kibernetiniam saugumui skirtas ES finansavimas 2023–2027 m. sudarys 843 milijonus eurų. Pažymime, kad ši suma apima ne tik siūlomame reglamente nustatytus veiksmus, bet ir kitus SEP kibernetinio saugumo veiksmus

(pavyzdžiui, paramą pramonei arba standartizacijai). Pasiūlyme nepateikiama visų numatomų išlaidų, susijusių su siūlomų priemonių (Europos kibernetinio saugumo skydo, Reagavimo į kibernetinio saugumo krizes mechanizmo (įskaitant ES kibernetinio saugumo rezervą) ir Kibernetinio saugumo incidentų peržiūros mechanizmo) nustatymu ir įgyvendinimu, sąmata. Kadangi prie pasiūlymo nepridedamas poveikio vertinimas, Komisijai siūlome pateikti šias išlaidų sąmatas, kad būtų padidintas skaidrumas.

Dalinė informacija apie Europos kibernetinio saugumo skydo finansinę struktūrą

11 Siūlomo reglamento II skyriuje sukuriamas Europos kibernetinio saugumo skydas, kurį sudaro nacionaliniai saugumo operacijų centrai (nacionaliniai SOC) ir tarpvalstybiniai saugumo operacijų centrai (tarpvalstybiniai SOC). Siūlomame reglamente nustatyta, kad reikalavimus atitinkantys nacionaliniai SOC gali gauti ES finansinį įnašą, kuriuo padengiama iki 50 % jų priemonių ir infrastruktūros įsigijimo išlaidų ir iki 50 % jų veiklos išlaidų. Tarpvalstybinių SOC atveju pagal bendrąjį ES finansavimą padengiama iki 75 % priemonių ir infrastruktūros įsigijimo išlaidų ir iki 50 % veiklos išlaidų. Siūlomame reglamente nenurodoma, kodėl tarpvalstybiniams SOC reikia papildomų priemonių ir infrastruktūros, kurie remiami taikant didesnę bendro finansavimo normą, palyginti su priemonėmis, skirtomis konsorciumą sudarantiems nacionaliniams SOC.

12 Siūlomame reglamente taip pat nenurodyta, kiek laiko ES bendrai finansuos nacionalinių ir tarpvalstybinių SOC veiklos išlaidas. Dėl to kyla rizika, kad Europos kibernetinio skydo veikimas ir jo tvarumas taps priklausomi nuo ES finansavimo.

Su Europos kibernetinio saugumo skydu susijusi rizika

Padidėjęs sudėtingumas ir papildomi lygmenys

13 Savo Apžvalgoje 02/2019[2] pažymėjome, kad ES kibernetinio saugumo aplinka yra sudėtinga ir daugiasluoksnė. Ji apima daug privačiojo ir viešojo sektorių subjektų regioniniu, nacionaliniu ir ES lygmenimis civilinėje srityje, įskaitant teisėsaugos subjektus ir finansinės žvalgybos padalinius. Kibernetinis saugumas taip pat yra vienas iš pagrindinių nacionalinio saugumo ir gynybos elementų. Šios nuomonės ***priede***

[2] Apžvalga 02/2019„Veiksmingos ES kibernetinio saugumo politikos iššūkiai“.

pateikiame ES naujos kibernetinio saugumo sistemos schemą; joje, viename iš spalvotų langelių, pateikti visi pasiūlyme nurodyti mechanizmai ir komponentai. Iš schemos matyti, kiek dėl reglamento sistema tampa sudėtingesnė ir daugiasluoksniškesnė.

14 Siūlomo reglamento II skyriuje nustatyto Europos kibernetinio saugumo skydo tikslas – plėtoti pažangius ES pajėgumus, siekiant aptikti kibernetines grėsmes ir incidentus, juos analizuoti ir tvarkyti duomenis apie juos. Tai bus tarpusavyje sujungta visos Europos nacionalinių saugumo operacijų centrų ir tarpvalstybinių saugumo operacijų centrų infrastruktūra.

15 Kad galėtų dalyvauti Europos kibernetinio saugumo skydo veikloje, valstybė narė paskiria bent vieną nacionalinį SOC, kuris turi būti viešoji įstaiga. Nacionaliniai SOC savo ruožtu turėtų sukurti tarpvalstybinius SOC, t. y. konsorciumus, kuriuos sudarys SOC bent iš trijų valstybių narių, įsipareigojusių bendradarbiauti ir koordinuoti savo kibernetinio saugumo incidentų aptikimo ir kibernetinių grėsmių stebėsenos veiklą.

16 Pastaraisiais metais ES sustiprino savo kibernetinio saugumo reguliavimo sistemą. Viena iš pagrindinių jos priemonių yra 2016 m. Tinklų ir informacijos saugumo direktyva (TIS direktyva) ir 2022 m. peržiūrėta jos redakcija (TIS 2 direktyva). Pagal TIS 2 direktyvą, valstybės narės nacionaliniu lygmeniu turėtų įsteigti vieną ar daugiau reagavimo į kompiuterių saugumo incidentus tarnybų (CSIRT). ES lygmeniu TIS 2 direktyva taip pat įsteigiama TIS bendradarbiavimo grupė, CSIRT tinklas ir Europos ryšių palaikymo dėl kibernetinių krizių organizacinis tinklas (EU-CyCLONe).

17 2021 m. ES įsteigė Europos kibernetinio saugumo kompetencijos centrą. Šiam 2023 m. gegužės mėn. atidarytam centrui padės 27 nacionalinių koordinavimo centrų tinklas – po vieną centrą kiekvienai valstybei narei, ir dalis jų taip pat yra nacionaliniai SOC. Centras bus atsakingas už SEP kibernetinio saugumo komponento įgyvendinimą, išskyrus ES kibernetinio saugumo rezervą. Tai įgyvendins Komisija, tačiau ENISA gali būti pavesta rūpintis jo veikimu ir administravimu.

18 Komisija taip pat įsteigė Jungtinį kibernetinio saugumo padalinį. Apie šį padalinį paskelbta 2020 m. ES kibernetinio saugumo strategijoje ir jis išsamiau apibrėžtas 2021 m. Komisijos rekomendacijoje.

19 2023 m. balandžio mėn. Komisija paskelbė, kad pradės veikti Kibernetinio saugumo įgūdžių akademija; tai nauja iniciatyva, kuria siekiama panaikinti kibernetinio saugumo srities talentų trūkumą ir skatinti ES kibernetinės srities darbo jėgą.

20 Atsižvelgdami į tai, manome, kad dėl siūlomo reglamento visa ES kibernetinio saugumo sistema gali tapti sudėtingesnė. Esamo CSIRT tinklo ir SOC veikla gali dubliuotis. Nors Komisija savo aiškinamojo memorandumo 1 skirsnyje nurodė, kad tarpvalstybinės SOC platformos turėtų sudaryti naujus pajėgumus, kurie papildytų CSIRT tinklą, pažymime, kad kai kurios nacionalinių SOC, tarpvalstybinių SOC, CSIRT ir CSIRT tinklo užduotys ir tikslai yra panašūs. Tai apima grėsmių aptikimą ir reagavimą į jas, žvalgybos informaciją apie kibernetines grėsmes ir informuotumą apie padėtį. Iš esmės šią riziką būtų galima sumažinti palaipsniui konsoliduojant susijusias struktūras, visų pirma nacionalinius SOC bei CSIRT ir tarpvalstybinius SOC. Be to, pasiūlyme turėtų būti paaiškinta, kaip šios struktūros turėtų sąveikauti, nustatant aiškią valdymo tvarką ir atsakomybę, kad būtų užtikrintas veiksmingas koordinavimas ir pasiekta sinergija.

Dalijimasis informacija

21 Savo Specialiojoje ataskaitoje 05/2022[3] nustatėme, kad ES institucijos, įstaigos ir agentūros dalijosi pagrindine svarbia kibernetinio saugumo informacija nesistemingai, net jei jų buvo reikalaujama tai daryti. Veiksmingai dalytis informacija trukdė ir sąveikumo problemos, dėl kurių negalėjo būti užtikrinta saugi komunikacija. Nors mūsų išvada buvo susijusi su šia palyginti maža ir vienalyte ES subjektų grupe, manome, kad su šiuo iššūkiu bus vis labiau susiduriama sudėtingesnėje ir įvairesnėje kibernetinio saugumo sistemoje valstybių narių lygmeniu.

22 Siūlomo reglamento 4 straipsnyje nurodyta, kad nacionaliniai SOC turėtų veikti kaip atskaitos taškas ir sąsaja su kitomis viešosiomis ir privačiosiomis nacionalinio lygmens organizacijomis, kad rinktų ir analizuotų informaciją apie kibernetinio saugumo grėsmes ir incidentus. Tačiau šiuo metu viešosioms ir privačiosioms organizacijoms (įskaitant nacionalines CSIRT, privačiuosius SOC ir organizacijas, kurios pagal TIS 2 direktyvą vadinamos „esminiais ir svarbiais subjektais“) ES lygmeniu netaikomi ataskaitų teikimo nacionalinėms SOC reikalavimai. Todėl kyla rizika, kad nacionaliniai SOC negaus pakankamai duomenų ar informacijos savo poreikiams patenkinti.

23 Prie pasiūlymo pridedamos finansinės teisės akto pasiūlymo pažymos 2.2.2 skirsnyje Komisija nurodo riziką, kad valstybės narės „nepakankamai dalysis“ atitinkama informacija apie kibernetines grėsmes tarpvalstybinėse SOC platformose ar tarpvalstybinėse platformose bendraudamos su kitais atitinkamais ES lygmens

[3] Specialioji ataskaita 05/2022„ES institucijų, įstaigų ir agentūrų kibernetinis saugumas. Parengties lygis iš esmės neatitinka grėsmių“.

subjektais. Toks nepakankamas keitimasis informacija galėtų pakenkti Europos kibernetinio saugumo skydo veiksmingumui ir pridėtinei vertei.

24 Todėl palankiai vertiname tai, kad pasiūlymo 4, 5 ir 6 straipsniuose yra konkrečių nuostatų, kuriomis siekiama sumažinti su nepakankamu dalijimusi informacija susijusią riziką. Pasiūlyme numatyta, kad nacionaliniai SOC galės gauti ES finansavimą tik tuo atveju, jei jie įsipareigos dalyvauti tarpvalstybinio SOC veikloje. Tačiau pažymime, kad per pirmuosius dvejus metus gauta finansinė parama nekompensuojama, jei nacionalinis SOC neprisijungia prie tarpvalstybinio SOC tinklo. Siūlomame reglamente taip pat reikalaujama, kad tarpvalstybinių SOC nariai įsipareigotų tarpusavyje dalytis „dideliu duomenų kiekiu“ ir rašytiniame konsorciumo susitarime nustatytų valdymo sistemą.

25 Be to, pasiūlymo 7 straipsnyje nurodyta, kad tarpvalstybiniai SOC atitinkamą informaciją, susijusią su galimu arba tebesitęsiančiu didelio masto kibernetinio saugumo incidentu, „nepagrįstai nedelsdami“ turi pateikti EU-CyCLONe, CSIRT tinklui ir Komisijai. Pabrėžiame, kad svarbu užtikrinti tinkamą šios nuostatos vykdymą.

26 Siūlomo reglamento 6 straipsnyje nustatyta, kad Komisija tarpvalstybinių SOC sąveikumo sąlygas gali nustatyti įgyvendinimo aktais. 8 straipsnyje nustatyta, kad Komisija taip pat gali priimti įgyvendinimo aktus, kuriais nustatomi techniniai reikalavimai, kurių laikydamosi valstybės narės užtikrina aukštą duomenų ir infrastruktūros fizinio saugumo lygį. Dėl šių sąlygų ir reikalavimų turėtų būti greitai susitarta, kad būtų išvengta tarpusavyje nesuderinamų sistemų kūrimo ir sumažintos išlaidos.

Su Reagavimo į kibernetinio saugumo krizes mechanizmu susijusi rizika

ES kibernetinio saugumo rezervo panaudojimas

27 Savo Specialiojoje ataskaitoje 05/2022 pažymėjome, kad CERT-EU, pačios ES kompiuterinių incidentų tyrimo tarnyba, kuri teikia reagavimo paramą ES institucijoms, įstaigoms ir agentūroms, audito metu neveikė visą parą 7 dienas per savaitę.

28 Siūlomo reglamento 14 straipsnyje nustatyta, kad prašymus suteikti paramą iš ES kibernetinio saugumo rezervo vertins Komisija, padedama ENISA, ir kad atsakymas bus išsiųstas „nedelsiant“. Kadangi vienu metu gali būti pateikta daug prašymų ir reikia nustatyti jų pirmenybę, siūlomame reglamente nustatyti tam tikri sprendimų priėmimo

kriterijai. 13 straipsnyje nurodyta, kad Komisija gali priimti įgyvendinimo aktus, kuriais išsamiau nustatoma išsami rezervo skyrimo tvarka.

29 Manome, jog labai svarbu, kad laikotarpis nuo prašymo gauti paramos paslaugas iš ES kibernetinio saugumo rezervo iki Komisijos atsakymo nebūtų uždelstas dėl prašymo pateikimo laiko. Tačiau pasiūlyme nenurodytas iš anksto nustatytas terminas ir nereikalaujama, kad siekiant laikytis šio termino būtų imtasi organizacinių veiksmų.

Nukrypimas nuo metinio periodiškumo principo

30 Vienas iš pagrindinių ES biudžeto principų yra jo metinis periodiškumas, t. y. į biudžetą įrašyti asignavimai patvirtinami finansiniams metams iki gruodžio 31 d. Nepanaudoti įsipareigojimai ir mokėjimų asignavimai nėra automatiškai perkeliami į kitus finansinius metus. Šis principas nustatytas Finansinio reglamento 2 skyriuje.

31 Siūlomo reglamento 19 straipsnyje nuo šio principo nukrypstama finansuojant veiksmus pagal Reagavimo į kibernetinio saugumo krizes mechanizmą. Jame nustatyta, kad nepanaudoti įsipareigojimų ir mokėjimų asignavimai, skirti veiksmams, susijusiems su pasirengimu, reagavimu ir savitarpio pagalba, perkeliami automatiškai ir gali būti skirti ir išmokėti iki kitų finansinių metų gruodžio 31 d. Aiškinamojo memorandumo 2 skirsnyje Komisija paaiškino, kad toks biudžeto valdymo lankstumas reikalingas atsižvelgiant į *„nenuspėjamą, išskirtinį ir specifinį kibernetinio saugumo aplinkos ir kibernetinių grėsmių pobūdį“*.

32 Kalbant apie parengtį, manome, kad koordinuotas subjektų parengties testavimas turėtų būti planuojama veikla, todėl apskritai jis nėra nei nenuspėjamas, nei išskirtinis. Mūsų nuomone, dėl tokios planuojamos veiklos nereikia nukrypti nuo pagrindinio metinio periodiškumo principo.

33 Tačiau, kadangi ES kibernetinio saugumo rezervas ir savitarpio pagalba bus naudojami tik reaguojant į nenuspėjamus įvykius, manome, kad šio nukrypimo loginis pagrindas gali būti pateisinamas tik šiuo atveju.

34 Siekdami aiškumo ir atsižvelgdami į kitų reglamentų, pavyzdžiui, dėl Sąjungos civilinės saugos mechanizmo arba Kaimynystės, vystomojo ir tarptautinio bendradarbiavimo priemonės „Globali Europa“, rengimą, taip pat manome, kad siūlomame reglamente turėtų būti nurodyta, kad nepanaudoti įsipareigojimai automatiškai turėtų būti perkelti tik į kitus metus.

Su Kibernetinio saugumo incidentų peržiūros mechanizmu susijusi rizika

35 Siūlomo reglamento 18 straipsnyje nurodyta, kad Komisijos, EU-CyCLONe arba CSIRT tinklo prašymu ENISA peržiūri ir įvertina su konkrečiu reikšmingu arba didelio masto kibernetinio saugumo incidentu susijusias grėsmes, pažeidžiamumą ir poveikio švelninimo veiksmus. Bendradarbiaudama su visais atitinkamais suinteresuotaisiais subjektais, ENISA turi pateikti incidento peržiūros ataskaitą, kurioje būtų nurodytos pagrindinės priežastys, pažeidžiamumas ir įgyta patirtis.

36 Manome, kad tai yra svarbus grįžtamojo ryšio mechanizmas, siekiant nuolat stiprinti ES aptikimo, parengties ir reagavimo pajėgumus kibernetinio saugumo grėsmių ir incidentų atveju. Tačiau siūlome reglamente nustatyti, per kokį maksimalų terminą po bet kokio incidento ENISA turi pateikti ataskaitą, siekiant užtikrinti, kad grįžtamoji informacija būtų pateikta laiku. Be to, pasiūlyme nurodyta, kad, kai tinkama, ataskaitoje turėtų būti pateikta rekomendacijų, kaip pagerinti Sąjungos kibernetinio saugumo būklę, tačiau nenurodyta, kaip reikėtų į šias rekomendacijas atsižvelgti.

Veiksmingumo stebėsena ir politikos vertinimas

37 Siūlomo reglamento 19 straipsniu keičiamas SEP reglamento II priedas nustatant naują išmatuojamą rodiklį, t. y. *„veiksmų, kuriais remiamas pasirengimas kibernetinio saugumo incidentams ir reagavimas į juos pagal Reagavimo į kibernetinio saugumo krizes mechanizmą, skaičių“*. Šis rodiklis papildo du esamus rodiklius, skirtus stebėti pažangai, padarytai siekiant konkretaus SEP kibernetinio saugumo ir pasitikėjimo tikslo, ir ataskaitoms apie ją teikti, t. y. *„bendrai įsigytų kibernetinės infrastruktūros objektų arba priemonių ar tiek objektų, tiek priemonių skaičių“* ir *„naudotojų ir jų bendruomenių, kurie gauna prieigą prie Europos kibernetinio saugumo įrenginių, skaičių“*.

38 Mūsų nuomone, siūlomu nauju rodikliu vertinami tik išdirbiai ir jis suteiks mažai informacijos apie Europos kibernetinio saugumo skydo ir Reagavimo į kibernetinio saugumo krizes mechanizmo naudojimą ir rezultatus.

39 Pasiūlymo 20 straipsnyje reikalaujama, kad Komisija Europos Parlamentui ir Tarybai pateiktų šio reglamento vertinimo ir peržiūros ataskaitą, praėjus ketveriems metams nuo reglamento taikymo pradžios dienos.

40 Nors manome, kad vertinimas turėtų būti grindžiamas pakankamais ir patikimais duomenimis, dėl sparčiai kintančios grėsmių padėties ES ir jos valstybės narės turi nuolat prisitaikyti ir diegti inovacijas. Todėl manome, rengiantis naujam programavimo laikotarpiui šiuo metu siūlomas vertinimo terminas gali būti per vėlus. Be to, iki 2027 m. pabaigos SEP konkrečiam kibernetinio saugumo ir pasitikėjimo tikslui bus skirta visa biudžete numatyta suma.

Baigiamosios pastabos

41 Siūlomame ES kibernetinio solidarumo akte nustatytos kibernetinio saugumo grėsmių ir incidentų aptikimo, pasirengimo jiems ir reagavimo į juos priemonės. Audito Rūmai palankiai vertina pasiūlymo tikslus stiprinti ES kolektyvinį kibernetinį atsparumą.

42 Mūsų nuomonėje atkreipiamas dėmesys į tam tikrą mūsų nustatytą riziką ir į tai, kaip būtų galima įgyvendinti pasiūlyme nustatytas priemones. Visų pirma atkreipiame dėmesį į riziką, kad Europos kibernetinio saugumo skydo veikimas ir jo tvarumas taps priklausomi nuo ES finansavimo, kad jo veikimui trukdo nepakankamas keitimasis informacija ir kad dėl pasiūlyme nustatytų priemonių visa ES kibernetinio saugumo sistema tampa sudėtingesnė.

43 Peržiūrėję pasiūlymą dėl teisėkūros procedūra priimamo akto, **Komisijai ir teisės aktų leidėjams siūlome**:

— pateikti su siūlomų priemonių nustatymu ir įgyvendinimu susijusias išlaidų sąmatas, kad būtų padidintas skaidrumas (žr. ***10*** dalį);

— paaiškinti, kaip turėtų sąveikauti nacionaliniai SOC, tarpvalstybiniai SOC, CSIRT ir CSIRT tinklas, nustatant aiškią valdymo tvarką ir atsakomybę, kad būtų užtikrintas veiksmingas koordinavimas ir pasiekta sinergija (***20*** dalis);

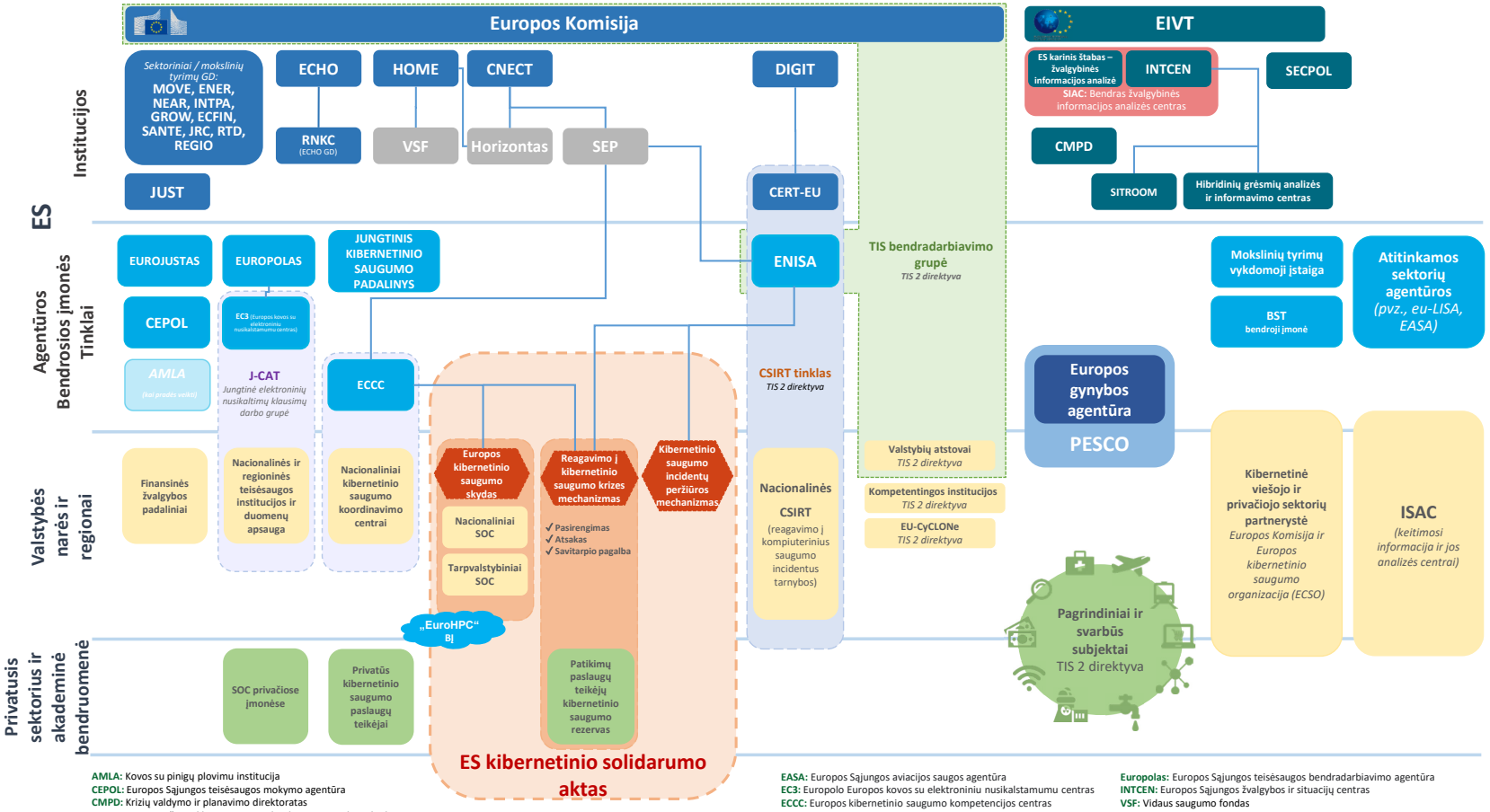
— užtikrinti, kad laikotarpis nuo prašymo gauti paramą iš ES kibernetinio saugumo rezervo iki Komisijos atsakymo nebūtų uždelstas dėl prašymo pateikimo laiko (***29*** dalis);

— leisti nukrypti nuo metinio periodiškumo principo tik reagavimo veiksmų ir savitarpio pagalbos atveju ir paaiškinti, kad automatinis nepanaudotų įsipareigojimų perkėlimas turėtų būti taikomas tik kitiems metams (***32***–***34*** dalys);

— nustatyti maksimalų terminą, per kurį ENISA po bet kokio incidento turėtų pateikti ataskaitą, siekiant užtikrinti, kad grįžtamoji informacija būtų pateikta laiku (***36*** dalis);

— paankstinti laiką, per kurį Komisija turi pateikti reglamento vertinimo ir peržiūros ataskaitą (***40*** dalis).

Priedas. Europos kibernetinio saugumo sistema



AMLA: Kovos su pinigų plovimu institucija
CEPOL: Europos Sąjungos teisėsaugos mokymo agentūra
CMPD: Krizių valdymo ir planavimo direktoratas
CONNECT GD: Ryšių tinklų, turinio ir technologijų generalinis direktoratas
ECFIN GD: Ekonomikos ir finansų reikalų generalinis direktoratas
ECHO GD Europos civilinės saugos ir humanitarinės pagalbos operacijų generalinis direktoratas
ENER DG: Energetikos generalinis direktoratas
GROW GD: Vidaus rinkos, pramonės, verslumo ir MVĮ generalinis direktoratas
HOME GD: Migracijos ir vidaus reikalų generalinis direktoratas
INTPA GD: Tarptautinės partnerystės generalinis direktoratas

JUST GD: Teisingumo ir vartotojų reikalų generalinis direktoratas
MOVE GD: Mobilumo ir transporto generalinis direktoratas
NEAR GD: Kaimynystės politikos ir plėtros derybų generalinis direktoratas
REGIO GD: Regioninės ir miestų politikos generalinis direktoratas
RTD GD: Mokslinių tyrimų ir inovacijų generalinis direktoratas
SANTE GD: Sveikatos ir maisto saugos generalinis direktoratas
DIGIT: Informatikos generalinis direktoratas

EASA: Europos Sąjungos aviacijos saugos agentūra
EC3: Europolo Europos kovos su elektroniniu nusikalstamumu centras
ECCC: Europos kibernetinio saugumo kompetencijos centras
ECSO: Europos kibernetinio saugumo organizacija
EGA: Europos gynybos agentūra
EIVT: Europos išorės veiksmų tarnyba
RNKC: Reagavimo į nelaimes koordinavimo centras
EU-CyCLONe: Europos ryšių palaikymo dėl kibernetinių krizių organizacinis tinklas
„EuroHPC“: Europos našiosios kompiuterijos bendroji įmonė
Eurojustas: Europos Sąjungos bendradarbiavimo baudžiamosios teisenos srityje agentūra

Europolas: Europos Sąjungos teisėsaugos bendradarbiavimo agentūra
INTCEN: Europos Sąjungos žvalgybos ir situacijų centras
VSF: Vidaus saugumo fondas
JTC: Jungtinis tyrimų centras
BST: Bazinių skaitmeninių technologijų bendroji įmonė
TIS direktyva: Tinklų ir informacijos saugumo direktyva
PESCO: nuolatinis struktūrizuotas bendradarbiavimas
SECPOL: saugumo politika ir konfliktų prevencija
SITROOM: situacijų kabinetas
SOC: saugumo operacijų centras

Šaltinis: Audito Rūmai.

Šią nuomonę priėmė Audito Rūmų narės Bettinos Jakobsen vadovaujama III kolegija 2023 m. rugsėjo 26 d. Liuksemburge įvykusiame posėdyje.

Audito Rūmų vardu

Pirmininkas

Tony Murphy

AUTORIŲ TEISĖS