PAKEITIMAS 001-001
pateikė Pramonės, mokslinių tyrimų ir energetikos komitetas

Pranešimas
Lina Gálvez Muñoz **A9-0426/2023**
Kibernetinio solidarumo aktas

Pasiūlymas dėl reglamento (COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Pakeitimas 1

EUROPOS PARLAMENTO PAKEITIMAI*

Komisijos pasiūlymas

2023/0109 (COD)

Pasiūlymas

EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS

kuriuo nustatomos solidarumo stiprinimo ir pajėgumo aptikti kibernetinio saugumo grėsmes ir incidentus Sąjungoje, jiems pasirengti ir į juos reaguoti didinimo priemonės ***ir iš dalies keičiamas Reglamentas (ES) 2021/694***

EUROPOS PARLAMENTAS IR EUROPOS SĄJUNGOS TARYBA,

atsižvelgdami į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 173 straipsnio 3 dalį ir į 322 straipsnio 1 dalies a punktą,

---

* Pakeitimai: naujos arba iš dalies pakeistos teksto dalys žymimos pusjuodžiu kursyvu; išbrauktas tekstas nurodomas simboliu ▌.

atsižvelgdami į Europos Komisijos pasiūlymą,

teisėkūros procedūra priimamo akto projektą perdavus nacionaliniams parlamentams,

atsižvelgdami į Audito Rūmų nuomonę[1],

atsižvelgdami į Europos ekonomikos ir socialinių reikalų komiteto nuomonę[2],

atsižvelgdami į Regionų komiteto nuomonę[3],

laikydamiesi įprastos teisėkūros procedūros,

kadangi:

(1) informacinių ir ryšių technologijų naudojimas ir priklausomumas nuo jų tapo esminiais visų ekonominės veiklos sektorių ***ir demokratijos*** aspektais, ***tačiau kartu sudarė prielaidas atsirasti pažeidžiamumui,*** nes mūsų viešojo administravimo institucijos, įmonės ir piliečiai įvairiuose sektoriuose ir įvairiose valstybėse labiau susieti tarpusavyje ir vieni nuo kitų priklausomi, nei bet kada anksčiau;

(2) kibernetinio saugumo incidentų, įskaitant tiekimo grandinės išpuolius, kurių tikslas – kibernetinis šnipinėjimas, išpirkos reikalavimo programinė įranga arba veiklos sutrikdymas, mastas, dažnumas ir poveikis, ***kalbant apie incidentų metodus ir poveikį,*** didėja ***tiek Sąjungos, tiek pasaulio mastu***. 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 ***ekonomikai, demokratijai ir*** ypatingos svarbos infrastruktūros objektams ***visoje Sąjungoje***, 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 ***ir*** nusikaltėlių ▌. 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. ***Todėl būtinas glaudus ir koordinuotas viešojo sektoriaus, privačiojo sektoriaus, akademinės bendruomenės, pilietinės visuomenės ir žiniasklaidos bendradarbiavimas. Be to, Sąjungos atsakas turi būti koordinuojamas su tarptautinėmis institucijomis bei patikimais ir panašiai mąstančiais tarptautiniais partneriais. Patikimi ir panašiai mąstantys tarptautiniai partneriai – šalys, kurios pritaria Sąjungos vertybėms, t. y. demokratijai, įsipareigojimui gerbti žmogaus teises, veiksmingam daugiašališkumui ir taisyklėmis grindžiamai tvarkai pagal tarptautinio bendradarbiavimo sistemas ir susitarimus. Siekiant užtikrinti bendradarbiavimą su patikimais ir panašiai mąstančiais tarptautiniais partneriais ir apsaugą nuo sisteminių varžovų, subjektams, įsisteigusiems trečiosiose valstybėse, kurios nėra Sutarties dėl viešųjų pirkimų šalys, neturėtų būti leidžiama dalyvauti viešuosiuose pirkimuose pagal šį reglamentą;***

---

1 OL C […], […], p. […].
2 OL C , , p. .
3 OL C , , p. .

(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[1], būtina didinti piliečių, įmonių, ***visų pirma labai mažų įmonių, mažųjų ir vidutinių įmonių (MVĮ), įskaitant startuolius,*** ir subjektų, valdančių ypatingos svarbos infrastruktūros objektus, ***įskaitant vietos ir regionų valdžios institucijas,*** atsparumą didėjančioms kibernetinio saugumo grėsmėms, kurios gali turėti pražūtingą poveikį visuomenei ir ekonomikai. Todėl reikia investuoti į infrastruktūrą ir paslaugas ***ir kurti pajėgumus, kad būtų ugdomi kibernetinio saugumo įgūdžiai***, kurie 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;

(3a) kibernetiniai išpuoliai dažnai nukreipti prieš vietos, regionines ar nacionalines viešąsias paslaugas ir infrastruktūrą. Dėl finansinių ir žmogiškųjų išteklių trūkumo vietos valdžios institucijos yra vienas iš pažeidžiamiausių kibernetinių išpuolių taikinių. Todėl ypač svarbu, kad vietos lygmens politikos formuotojai būtų informuoti apie būtinybę didinti skaitmeninį atsparumą, didinti savo pajėgumus mažinti kibernetinių išpuolių poveikį ir pasinaudoti šiame reglamente numatytomis galimybėmis;

(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[2], Komisijos rekomendaciją (ES) 2017/1584[3], Europos Parlamento ir Tarybos direktyvą 2013/40/ES[4] ir Europos Parlamento ir Tarybos reglamentą (ES) 2019/881[5]. 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

---

1 https://futureu.europa.eu/lt/

2 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).

3 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).

4 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*).

5 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).

infrastruktūros objektų, naudojamų esminėms paslaugoms vidaus rinkoje teikti, atsparumą;

(5) dėl didėjančios kibernetinio saugumo rizikos ir apskritai sudėtingos grėsmių aplinkos, kai yra aiški rizika, kad kibernetiniai incidentai greitai išplis iš vienos valstybės narės į kitą ir iš trečiosios valstybės į Sąjungą, reikia stiprinti solidarumą Sąjungos lygmeniu, kad būtų galima geriau aptikti kibernetinio saugumo grėsmes ir incidentus, jiems pasirengti, ▌ į juos reaguoti ***ir atkurti veiklą po jų***. Valstybės narės Tarybos išvadose dėl ES kibernetinio saugumo būklės[1] taip pat paragino Komisiją pateikti pasiūlymą dėl naujo Reagavimo į kibernetinio saugumo krizes fondo;

(6) 2022 m. lapkričio 10 d. priimtame bendrame komunikate dėl ES kibernetinės gynybos politikos[2] paskelbta ES kibernetinio solidarumo iniciatyva, kuria siekiama šių tikslų: stiprinti bendrus ES aptikimo, informuotumo apie padėtį ir reagavimo pajėgumus, skatinant diegti ES saugumo operacijų centrų (toliau – SOC) ***tinklą***, remiant laipsnišką ES lygmens kibernetinio saugumo rezervo kūrimą, pasitelkiant patikimų privačių paslaugų teikėjų paslaugas ir, remiantis ES rizikos vertinimais, atlikti ypatingos svarbos subjektų galimų pažeidžiamumų testavimą;

(7) būtina stiprinti kibernetinių grėsmių ir incidentų aptikimą ir informuotumą apie padėtį visoje Sąjungoje, taip pat stiprinti solidarumą didinant valstybių narių ir Sąjungos parengtį bei pajėgumus ***užkirsti kelią*** reikšmingiems ir didelio masto kibernetinio saugumo incidentams ***ir*** į juos reaguoti. Taigi siekiant sukurti ir sustiprinti bendrus aptikimo ir informuotumo apie padėtį gebėjimus turėtų būti įdiegtas Europos masto SOC ***tinklas*** (Europos kibernetinio saugumo skydas)***, kuris sustiprintų Sąjungos grėsmių aptikimo ir keitimosi informacija pajėgumus,*** reikėtų sukurti Reagavimo į kibernetinio saugumo krizes mechanizmą siekiant padėti valstybėms narėms pasirengti reikšmingiems ir didelio masto kibernetinio saugumo incidentams, į juos reaguoti ir nedelsiant po jų atkurti veiklą, turėtų būti sukurtas Kibernetinio saugumo incidentų peržiūros mechanizmas, kad būtų galima peržiūrėti ir įvertinti konkrečius reikšmingus arba didelio masto incidentus. Šie veiksmai nedaro poveikio Sutarties dėl Europos Sąjungos veikimo (toliau – SESV) 107 ir 108 straipsniams;

(8) siekiant šių tikslų taip pat būtina tam tikrose srityse iš dalies pakeisti Europos Parlamento ir Tarybos reglamentą (ES) 2021/694[3]. Visų pirma šiuo reglamentu turėtų būti iš dalies pakeistas Reglamentas (ES) 2021/694, siekiant įtraukti naujus veiklos tikslus, susijusius su Europos kibernetinio saugumo skydu ir Reagavimo į kibernetinio saugumo krizes mechanizmu pagal Skaitmeninės Europos programos 3-ią konkretų tikslą, kuriuo siekiama užtikrinti bendrosios skaitmeninės rinkos atsparumą, vientisumą ir patikimumą, stiprinti kibernetinių išpuolių ir grėsmių stebėsenos bei reagavimo į juos pajėgumus ir stiprinti tarpvalstybinį bendradarbiavimą kibernetinio saugumo srityje. Be to, turėtų būti nustatytos specialios sąlygos, kuriomis šiems veiksmams gali būti skiriama finansinė parama, ir apibrėžti valdymo bei koordinavimo mechanizmai, būtini numatytiems tikslams pasiekti. Kiti Reglamento (ES) 2021/694 pakeitimai turėtų apimti

---

1 Tarybos išvados dėl Europos Sąjungos kibernetinio saugumo būklės raidos, kurias Taryba patvirtino 2022 m. gegužės 23 d. posėdyje (dok. 9364/22).

2 Bendras komunikatas Europos Parlamentui ir Tarybai „ES kibernetinės gynybos politika“, JOIN(2022) 49 final.

3 2021 m. balandžio 29 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/694, kuriuo nustatoma Skaitmeninės Europos programa ir panaikinamas Sprendimas (ES) 2015/2240 (OL L 166, 2021 5 11, p. 1).

siūlomų veiksmų pagal naujus veiklos tikslus aprašymus, taip pat išmatuojamus šių naujų veiklos tikslų įgyvendinimo stebėsenos rodiklius;

(9) veiksmų finansavimas pagal šį reglamentą turėtų būti numatytas Reglamente (ES) 2021/694, kuris turėtų ir toliau būti svarbus pagrindinis teisės aktas dėl šių veiksmų, įtvirtintų Skaitmeninės Europos programos 3-iame konkrečiame tiksle. Konkrečios dalyvavimo sąlygos, susijusios su kiekvienu veiksmu, bus numatytos atitinkamose darbo programose, laikantis taikytinos Reglamento (ES) 2021/694 nuostatos;

(9a) atsižvelgiant į geopolitinius pokyčius ir platėjančią kibernetinių grėsmių panoramą (EPP 52) ir siekiant užtikrinti šiame reglamente nustatytų priemonių, visų pirma Europos kibernetinio saugumo skydo ir Reagavimo į kibernetinio saugumo krizes mechanizmo, tęstinumą ir tolesnį plėtojimą po 2027 m., būtina užtikrinti, kad 2028–2034 m. daugiametėje finansinėje programoje būtų numatyta speciali biudžeto eilutė. Valstybės narės turėtų stengtis įsipareigoti remti visas būtinas priemones kibernetinėms grėsmėms ir incidentams visoje Sąjungoje mažinti ir solidarumui stiprinti;

(10) šiam reglamentui taikomos Europos Parlamento ir Tarybos pagal SESV 322 straipsnį priimtos horizontaliosios finansinės taisyklės. Tos taisyklės išdėstytos ***Europos Parlamento ir Tarybos reglamente (ES, Euratomas) 2018/1046***[1] – visų pirma jomis nustatoma Sąjungos biudžeto sudarymo ir įgyvendinimo tvarka ir numatoma finansų pareigūnų atsakomybės kontrolė. Pagal SESV 322 straipsnį priimtos taisyklės taip pat apima bendrąją Sąjungos biudžeto apsaugos sąlygų sistemą, kaip nustatyta Europos Parlamento ir Tarybos reglamentu (ES, Euratomas) 2020/2092[2];

(11) siekiant patikimo finansų valdymo, reikėtų nustatyti konkrečias taisykles dėl nepanaudotų įsipareigojimų ir mokėjimų asignavimų perkėlimo. Laikantis principo, kad Sąjungos biudžetas nustatomas kasmet, šiame reglamente, atsižvelgiant į nenuspėjamą, išskirtinį ir specifinį kibernetinio saugumo aplinkos pobūdį, turėtų būti numatyta galimybė nepanaudotas lėšas, be nustatytųjų ***Reglamente (ES, Euratomas) 2018/1046***, perkelti į kitą laikotarpį, taip kuo labiau padidinant Reagavimo į kibernetinio saugumo krizes mechanizmo pajėgumą padėti valstybėms narėms veiksmingai kovoti su kibernetinėmis grėsmėmis;

(11a) šiuo reglamentu sukurtas reagavimo į kibernetinio saugumo krizes mechanizmas ir ES kibernetinio saugumo rezervas yra naujos iniciatyvos ir nebuvo numatytos nustatant 2021–2027 m. daugiametę finansinę programą, o finansuojant šias iniciatyvas siekiama kuo mažiau sumažinti kitų Skaitmeninės Europos programos prioritetų finansavimą. Todėl ES kibernetinio saugumo rezervui skirta finansinių

---

1 ***2018 m. liepos 18 d. Europos Parlamento ir Tarybos reglamentas (ES, Euratomas) 2018/1046 dėl Sąjungos bendrajam biudžetui taikomų finansinių taisyklių, kuriuo iš dalies keičiami reglamentai (ES) Nr. 1296/2013, (ES) Nr. 1301/2013, (ES) Nr. 1303/2013, (ES) Nr. 1304/2013, (ES) Nr. 1309/2013, (ES) Nr. 1316/2013, (ES) Nr. 223/2014, (ES) Nr. 283/2014 ir Sprendimas Nr. 541/2014/ES bei panaikinamas Reglamentas (ES, Euratomas) Nr. 966/2012 (OL L 193, 2018 7 30, p. 1, ELI: https://eur-lex.europa.eu/eli/reg/2018/1046/oj?locale=lt).***

2 ***2020 m. gruodžio 16 d. Europos Parlamento ir Tarybos reglamentas (ES, Euratomas) 2020/2092 dėl bendro Sąjungos biudžeto apsaugos sąlygų režimo (OL L 433I, 2020 12 22, p. 1, ELI: https://eur-lex.europa.eu/eli/reg/2020/2092/oj?locale=lt).***

išteklių suma turėtų būti sumažinta ir pirmiausia turėtų būti gaunama iš nepaskirstytų maržų pagal daugiametės finansinės programos viršutines ribas arba mobilizuojama pagal netemines daugiametės finansinės programos specialiąsias priemones. Siekiant apsaugoti esamas programas, visų pirma programą „Erasmus+“, nuo neigiamo poveikio ir užtikrinti, kad tomis programomis būtų galima pasiekti joms nustatytus tikslus, bet koks lėšų skyrimas arba perskirstymas iš esamų programų turėtų būti kuo mažesnis;

(12) siekiant veiksmingiau užkirsti kelią kibernetinėms grėsmėms ir incidentams, juos įvertinti, į juos reaguoti ***ir atkurti veiklą po jų***, 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. ***Iniciatyvus požiūris į galimų kibernetinių grėsmių nustatymą, mažinimą ir prevenciją apima didesnius pažangių aptikimo gebėjimų pajėgumus, būtinus pažangioms nuolatinėms grėsmėms sustabdyti. Žvalgybos informacija apie grėsmes – tai informacija, kuri renkama, analizuojama ir interpretuojama siekiant suprasti galimas grėsmes ir riziką. Didžiulių duomenų kiekių analizė ir susiejimas padeda aptikti modelius, tendencijas ir užvaldymo rodiklius, kurie gali atskleisti kenkimo veiklą ar pažeidžiamumą.*** Turėtų būti įdiegtas SOC ***tinklas*** (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. ***Nacionalinis SOC – centralizuota tarnyba, atsakinga už nuolatinį žvalgybos informacijos apie grėsmes rinkimą ir nacionalinei jurisdikcijai priklausančių subjektų kibernetinio saugumo būklės gerinimą užkertant kelią kibernetinėms grėsmėms, jas nustatant ir analizuojant.*** 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[1];

(13) ***kad galėtų dalyvauti Kibernetinio saugumo skydo veikloje,*** kiekviena valstybė narė nacionaliniu lygmeniu turėtų paskirti viešąją įstaigą, kuriai būtų pavesta koordinuoti kibernetinių grėsmių aptikimo veiklą toje valstybėje narėje. ***Valstybės narės raginamos nacionalinio SOC pajėgumus įtraukti į savo esamą kibernetinę struktūrą ir valdymą, kad nebūtų sukurti papildomi valdymo lygmenys ir šis reglamentas būtų suderintas su galiojančiais teisės aktais, įskaitant Direktyvą (ES) 2022/2555.*** Šie nacionaliniai SOC turėtų veikti kaip nacionalinis atskaitos taškas, nuo kurio nacionaliniu lygmeniu ***privatiems ir viešiesiems subjektams, visų pirma jų nacionaliniams SOC,*** atsiveria galimybė dalyvauti Europos kibernetinio saugumo skydo veikloje, ir jie turėtų užtikrinti, kad iš viešųjų ir privačių subjektų gauta informacija apie kibernetines grėsmes būtų veiksmingai ir racionaliai dalijamasi ir ji būtų renkama nacionaliniu lygmeniu.

[1] 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).

Nacionaliniai SOC turėtų stiprinti viešųjų ir privačiųjų subjektų bendradarbiavimą ir keitimąsi informacija, kad būtų panaikintos šiuo metu egzistuojančios uždaros ryšių sistemos. Tai darydami jie gali remti keitimosi duomenimis modelių kūrimą ir turėtų palengvinti bei skatinti keitimąsi informacija patikimoje ir saugioje aplinkoje. Glaudus ir koordinuotas viešųjų ir privačių subjektų bendradarbiavimas yra labai svarbus stiprinant Sąjungos atsparumą kibernetinio saugumo srityje;

(14) kaip Europos kibernetinio saugumo skydo dalis, turėtų būti įsteigti keli tarpvalstybiniai kibernetinio saugumo operacijų centrai (toliau – tarpvalstybiniai SOC). Jie turėtų suburti nacionalinius SOC iš bent trijų valstybių narių, kad būtų galima visapusiškai pasinaudoti tarpvalstybinio grėsmių aptikimo, dalijimosi informacija ir valdymo privalumais. Bendras tarpvalstybinių SOC tikslas turėtų būti stiprinti gebėjimus analizuoti kibernetinio saugumo grėsmes, užkirsti joms kelią bei jas aptikti ir remti kokybiškų žvalgybos duomenų apie kibernetinio saugumo grėsmes rengimą***, įskaitant duomenų ir informacijos apie galimus kenkėjiškus įsilaužimus, naujai sukurtas piktavališkas grėsmes ir saugumo spragų išnaudojimo būdus, kurie dar nebuvo panaudoti kibernetiniuose incidentuose, rinkimą ir dalijimąsi jais, taip pat analizės pastangas,*** visų pirma dalijantis duomenimis iš įvairių viešųjų ar privačių šaltinių, dalijantis naujausiomis priemonėmis ir jas bendrai naudojant, taip pat bendrai plėtojant aptikimo, analizės ir prevencijos pajėgumus patikimoje ***ir saugioje*** aplinkoje***, padedant ENISA, su valstybių narių operatyviniu bendradarbiavimu susijusiais klausimais***. ***Tarpvalstybiniai SOC turėtų palengvinti ir paskatinti keitimąsi informacija patikimoje ir saugioje aplinkoje ir*** suteikti naujų papildomų pajėgumų, kurie remsis esamų SOC ir reagavimo į kompiuterių saugumo incidentus tarnybų (CSIRT) bei kitų atitinkamų subjektų veikla ir ją papildys;

(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 ***būtų įtraukti į esamą kibernetinio saugumo infrastruktūrą, visų pirma į*** CSIRT tinklą, kaupiant viešųjų ir privačių subjektų***, ypač jų SOC,*** 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 ***technologinio suverenumo, jos atviro strateginio savarankiškumo, konkurencingumo ir atsparumo bei reikšmingos kibernetinio saugumo ekosistemos kūrimo, be kita ko, bendradarbiaujant su patikimais ir panašiai mąstančiais tarptautiniais partneriais***; .

(16) tarpvalstybiniai SOC turėtų veikti kaip centrinis punktas, leidžiantis sutelkti daug svarbių duomenų ir kibernetinių grėsmių žvalgybos informaciją, sudaryti sąlygas skleisti informaciją apie grėsmes dideliam įvairių dalyvių ratui (pvz., kompiuterinių incidentų tyrimo tarnyboms (toliau – CERT), CSIRT, keitimosi informacija ir jos analizės centrams (toliau – ISAC), ypatingos svarbos infrastruktūros objektų operatoriams)***, kad būtų lengviau panaikinti šiuo metu egzistuojančias uždaras komunikacijos sistemas***. ***Tai darydami tarpvalstybiniai SOC taip pat galėtų remti keitimosi duomenimis modelių kūrimą visoje Sąjungoje.*** Informacija, kuria keičiasi tarpvalstybinio SOC dalyviai, galėtų apimti tinklų ir jutiklių duomenis, grėsmių žvalgybos informacijos santraukas, užvaldymo rodiklius ir kontekstinę informaciją apie incidentus, grėsmes ir pažeidžiamumus***, įskaitant duomenų ir informacijos apie galimus kenkėjiškus įsilaužimus, naujai sukurtas piktavališkas grėsmes ir saugumo spragų išnaudojimo būdus, kurie dar nebuvo panaudoti kibernetiniuose incidentuose,***

rinkimą ir dalijimąsi jais, taip pat analizės pastangas. Be to, tarpvalstybiniai SOC taip pat turėtų sudaryti bendradarbiavimo susitarimus su kitais tarpvalstybiniais SOC;

(17) atitinkamų institucijų bendras informuotumas apie padėtį yra būtina Sąjungos masto parengties reikšmingiems ir didelio masto kibernetinio saugumo incidentams ir koordinavimo veiksmų sąlyga. Siekiant remti koordinuotą didelio masto kibernetinio saugumo incidentų ir krizių valdymą operatyviniu lygmeniu ir užtikrinti reguliarų keitimąsi svarbia informacija tarp valstybių narių ir Sąjungos institucijų, įstaigų ir agentūrų, Direktyva (ES) 2022/2555 įsteigiamas EU-CyCLONe. Rekomendacijoje (ES) 2017/1584 dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes apibūdinamas visų susijusių subjektų vaidmuo. Be to, Direktyvoje (ES) 2022/2555 primenama Komisijos atsakomybė pagal Sąjungos civilinės saugos mechanizmą (toliau – SCSM), nustatytą Europos Parlamento ir Tarybos sprendimu Nr. 1313/2013/ES[1], taip pat už analitinių ataskaitų dėl integruoto politinio atsako į krizes mechanizmo (toliau – IPCR) teikimą pagal ***Tarybos*** įgyvendinimo sprendimą (ES) 2018/1993[2]. Todėl tais atvejais, kai tarpvalstybiniai SOC gauna informacijos, susijusios su galimu arba vykstančiu didelio masto kibernetinio saugumo incidentu, jie turėtų teikti atitinkamą informaciją EU-CyCLONe, CSIRT tinklui ir Komisijai ***pagal Direktyvą (ES) 2022/2555***. Visų pirma, priklausomai nuo situacijos, informacija, kuria turi būti dalijamasi, galėtų apimti techninę informaciją, informaciją apie užpuoliko arba potencialaus užpuoliko pobūdį bei motyvus ir aukštesnio lygio netechninę informaciją apie galimą arba vykstantį didelio masto kibernetinio saugumo incidentą. Šiomis aplinkybėmis reikėtų deramai atsižvelgti į būtinybės žinoti principą ir į galimai neskelbtiną informacijos, kuria dalijamasi, pobūdį;

(18) Europos kibernetinio saugumo skydo veikloje dalyvaujantys subjektai turėtų užtikrinti aukšto lygio tarpusavio sąveikumą, be kita ko, kai tinkama, duomenų formatų, taksonomijos, duomenų tvarkymo ir duomenų analizės priemonių, taip pat saugių ryšio kanalų, minimalaus taikomųjų programų saugumo lygio, informuotumo apie padėtį suvestinės ir rodiklių atžvilgiu. Priimant bendrą taksonomiją ir parengiant padėties ataskaitų šabloną kibernetinio saugumo incidentų techninėms priežastims ir poveikiui apibūdinti turėtų būti atsižvelgiama į šiuo metu vykdomą pranešimo apie incidentus darbą įgyvendinant Direktyvą (ES) 2022/2555;

(19) siekiant sudaryti sąlygas didele apimtimi ir patikimoje ***bei saugioje*** aplinkoje keistis duomenimis apie kibernetinio saugumo grėsmes iš įvairių šaltinių, Europos kibernetinio saugumo skydo veikloje dalyvaujantys subjektai turėtų turėti naujausias ir labai saugias priemones, įrangą ir infrastruktūros objektus ***ir kvalifikuotus darbuotojus***. Tai turėtų sudaryti sąlygas pagerinti kolektyvinius nustatymo pajėgumus ir laiku įspėti valdžios institucijas ir atitinkamus subjektus, visų pirma naudojant naujausias dirbtinio intelekto ir duomenų analizės technologijas;

(20) renkant duomenis, jais dalijantis bei keičiantis, Europos kibernetinio saugumo skydas turėtų stiprinti Sąjungos technologinį suverenumą***, jos atvirą strateginį savarankiškumą, konkurencingumą bei atsparumą ir ES reikšmingą kibernetinio***

---

1 ***2013 m. gruodžio 17 d. Europos Parlamento ir Tarybos sprendimas Nr. 1313/2013/ES dėl Sąjungos civilinės saugos mechanizmo (Tekstas svarbus EEE)*** (OL L 347, 2013 12 20, p. 924, ***ELI:*** https://eur-lex.europa.eu/eli/dec/2013/1313/oj?locale=lt***).***

2 ***2018 m. gruodžio 11 d. Tarybos įgyvendinimo sprendimas (ES) 2018/1993 dėl ES integruoto politinio atsako į krizes mechanizmo*** **(OL L 320, 2018 12 17, p. 28,** ***ELI: https://eur-lex.europa.eu/eli/dec_impl/2018/1993/oj?locale=lt).***

saugumo ekosistemą. Kokybiškų patikrintų duomenų sutelkimas taip pat turėtų padėti plėtoti pažangias dirbtinio intelekto ir duomenų analizės technologijas. ***Dirbtinis intelektas yra veiksmingiausias tuomet, kai jis derinamas su žmogaus atliekama analize. Todėl norint kaupti kokybiškus duomenis kvalifikuota darbo jėga išlieka labai svarbi.*** Tai turėtų būti lengviau padaryti sujungiant Europos kibernetinio saugumo skydą su visos Europos našiosios kompiuterijos infrastruktūra, sukurta Tarybos reglamentu (ES) 2021/1173[1];

(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 specialias ***prieigos sąlygas ir apsaugos priemonių*** protokolus ir standartus, kad būtų galima bendradarbiauti su kibernetinės gynybos bendruomene, įskaitant tikrinimo ir saugumo sąlygas***, atsižvelgiant į įstaigų civilinį pobūdį ir finansavimo paskirtį, todėl naudojant gynybos bendruomenei prieinamas lėšas***. Kuriant Europos kibernetinio saugumo skydą turėtų būti svarstoma galimybė ateityje, glaudžiai bendradarbiaujant su vyriausiuoju įgaliotiniu ***ir visapusiškai užtikrinant teises ir laisves***, bendradarbiauti su tinklais ir platformomis, atsakingais už dalijimąsi informacija kibernetinės gynybos bendruomenėje;

(22) Europos kibernetinio saugumo skydo dalyviai turėtų dalytis informacija laikydamiesi galiojančių teisinių reikalavimų, visų pirma Sąjungos ir nacionalinės duomenų apsaugos teisės, taip pat Sąjungos konkurencijos taisyklių, kuriomis reglamentuojamas keitimasis informacija. Jei būtina tvarkyti asmens duomenis, informacijos gavėjas turėtų įgyvendinti technines ir organizacines priemones, kuriomis būtų apsaugotos duomenų subjektų teisės ir laisvės, ir sunaikinti duomenis, kai tik jie tampa nebereikalingi nurodytam tikslui, ir informuoti duomenis teikiančią įstaigą, kad duomenys sunaikinti;

(23) nedarant poveikio SESV 346 straipsniui, keitimasis konfidencialia informacija pagal Sąjungos arba nacionalinę ***teisę*** turėtų apsiriboti tik tuo, kas yra svarbu ir proporcinga to keitimosi tikslais. Keičiantis tokia informacija turėtų būti saugomas informacijos konfidencialumas ir atitinkamų subjektų saugumo bei komerciniai interesai, visapusiškai saugant komercines ir verslo paslaptis;

(24) atsižvelgiant į didėjančią riziką ir poveikį valstybėms narėms darančių kibernetinių incidentų skaičių, būtina nustatyti paramos krizės atveju priemonę, kuria būtų didinamas Sąjungos atsparumas reikšmingiems ir didelio masto kibernetinio saugumo incidentams ir papildomi valstybių narių veiksmai teikiant skubią pasirengimo, reagavimo ir neatidėliojamo esminių paslaugų atkūrimo finansinę paramą. Ta priemonė turėtų sudaryti sąlygas greitai ***ir veiksmingai*** suteikti pagalbą nustatytomis aplinkybėmis bei aiškiomis sąlygomis ir sudaryti sąlygas atidžiai stebėti ir vertinti, kaip naudojami ištekliai. Reagavimo į kibernetinio saugumo krizes mechanizmu skatinamas valstybių narių solidarumas pagal Europos Sąjungos sutarties (toliau – ES sutartis) 3 straipsnio

[1] 2021 m. liepos 13 d. Tarybos reglamentas (ES) 2021/1173 dėl Europos našiosios kompiuterijos bendrosios įmonės įsteigimo ir kuriuo panaikinamas Reglamentas (ES) 2018/1488 (OL L 256, 2021 7 19, p. 3, ***ELI: https://eur-lex.europa.eu/eli/reg/2021/1173/oj?locale=lt***).

3 dalį, tačiau pirminė atsakomybė už kibernetinio saugumo incidentų ir krizių prevenciją, pasirengimą jiems ir reagavimą į juos pirmiausia tenka valstybėms narėms;

(25) Reagavimo į kibernetinio saugumo krizes mechanizmas turėtų padėti valstybėms narėms papildyti jų pačių priemones bei išteklius ir kitas esamas paramos reaguoti į reikšmingus ir didelio masto kibernetinio saugumo incidentus ir nedelsiant po jų atkurti veiklą galimybes, pavyzdžiui, Europos Sąjungos kibernetinio saugumo agentūros (toliau – ENISA) jos kompetencijos srityje teikiamas paslaugas, koordinuotą reagavimą ir CSIRT tinklo pagalbą, EU-CyCLONe poveikio mažinimo paramą, taip pat valstybių narių savitarpio pagalbą, be kita ko, pagal ES sutarties 42 straipsnio 7 dalį, PESCO greitojo reagavimo į kibernetinius incidentus komandas[1] ir greitojo reagavimo į hibridines grėsmes grupes. Juo turėtų būti atsižvelgiama į poreikį užtikrinti, kad būtų specialių priemonių, kuriomis būtų remiamas pasirengimas kibernetinio saugumo incidentams ir reagavimas į juos visoje Sąjungoje ir trečiosiose valstybėse;

(26) šia priemone nedaroma poveikio Sąjungos lygmens reagavimo į krizes koordinavimo procedūroms ir sistemoms, visų pirma SCSM[2], IPCR[3] ir Direktyvai (ES) 2022/2555. Ji gali padėti įgyvendinti veiksmus, įgyvendinamus pagal ES sutarties 42 straipsnio 7 dalį arba SESV 222 straipsnyje apibrėžtais atvejais, arba juos papildyti. Be to, šios priemonės naudojimas, kai tinkama, turėtų būti koordinuojamas su kibernetinio saugumo diplomatijos priemonių rinkinio priemonių įgyvendinimu;

(27) pagal šį reglamentą teikiama pagalba turėtų būti remiami ir papildomi veiksmai, kurių valstybės narės imasi nacionaliniu lygmeniu. Šiuo tikslu turėtų būti užtikrintas glaudus Komisijos***, ENISA*** ir paveiktos valstybės narės bendradarbiavimas ir konsultacijos. Prašydama paramos pagal reagavimo į kibernetinio saugumo krizes mechanizmą, valstybė narė turėtų pateikti atitinkamą informaciją, pagrindžiančią paramos poreikį;

(28) Direktyvoje (ES) 2022/2555 reikalaujama, kad valstybės narės paskirtų arba įsteigtų vieną ar daugiau kibernetinio saugumo krizių valdymo institucijų ir užtikrintų, kad jos turėtų tinkamų išteklių ir galėtų veiksmingai ir efektyviai vykdyti joms pavestas užduotis. Joje taip pat reikalaujama, kad valstybės narės nustatytų, kokius pajėgumus, objektus ir procedūras galima panaudoti krizės atveju, taip pat priimtų nacionalinį reagavimo į didelio masto kibernetinio saugumo incidentus ir krizes planą, kuriame išdėstomi didelio masto kibernetinio saugumo incidentų ir krizių valdymo tikslai ir tvarka. Taip pat reikalaujama, kad valstybės narės įsteigtų vieną ar daugiau CSIRT, kurioms būtų pavesta atsakomybė už incidentų valdymą pagal aiškiai apibrėžtą procesą, apimant bent sektorius, subsektorius ir subjektų rūšis, patenkančius į tos direktyvos taikymo sritį, ir užtikrintų, kad jos turėtų tinkamų išteklių savo užduotims veiksmingai vykdyti. Šiuo reglamentu nedaroma poveikio Komisijos vaidmeniui užtikrinti, kad valstybės narės laikytųsi Direktyvoje (ES) 2022/2555 nustatytų pareigų. Pagal reagavimo į kibernetinio saugumo krizes mechanizmą turėtų būti teikiama pagalba veiksmams, kuriais siekiama stiprinti parengtį, taip pat reagavimo į incidentus

---

1 2017 m. gruodžio 11 d. TARYBOS SPRENDIMAS (BUSP) 2017/2315, kuriuo nustatomas nuolatinis struktūrizuotas bendradarbiavimas (PESCO) ir nustatomas dalyvaujančių valstybių narių sąrašas.

2 2013 m. gruodžio 17 d. Europos Parlamento ir Tarybos sprendimas Nr. 1313/2013/ES dėl Sąjungos civilinės saugos mechanizmo (OL L 347, 2013 12 20, p. 924).

3 Integruotas politinio atsako į krizes mechanizmas (IPCR) pagal 2017 m. rugsėjo 13 d. Komisijos rekomendaciją (ES) 2017/1584 dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes.

veiksmams, kuriais siekiama sušvelninti reikšmingų ir didelio masto kibernetinio saugumo incidentų poveikį, remti nedelsiamą veiklos ir (arba) esminių paslaugų veikimo atkūrimą;

(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 Direktyvos (ES) 2022/2555 22 straipsnį, ir skaitmeninės veiklos atsparumo testavimą, kaip numatyta Europos Parlamento ir Tarybos reglamente (ES) 2022/2554[1]. Atrenkant sektorius taip pat reikėtų atsižvelgti į Tarybos rekomendaciją dėl Sąjungos suderinto požiūrio į ypatingos svarbos infrastruktūros atsparumo didinimą;

(30) be to, pagal reagavimo į kibernetinio saugumo krizes mechanizmą turėtų būti teikiama parama kitiems pasirengimo veiksmams ir parama parengčiai kituose sektoriuose, kuriems netaikomas koordinuotas itin svarbiuose sektoriuose veikiančių subjektų testavimas. Tie veiksmai galėtų apimti įvairių rūšių nacionalinę pasirengimo veiklą;

(31) pagal reagavimo į kibernetinio saugumo krizes mechanizmą parama taip pat turėtų būti teikiama reagavimo į incidentus veiksmams, kuriais siekiama sušvelninti reikšmingų ir didelio masto kibernetinio saugumo incidentų poveikį, remti nedelsiamą veiklos arba esminių paslaugų veikimo atkūrimą. Kai tinkama, jis turėtų papildyti SCSM, kad būtų užtikrintas visapusiškas požiūris į reagavimą į kibernetinių incidentų poveikį piliečiams;

(32) Reagavimo į kibernetinio saugumo krizes mechanizmu turėtų būti remiama valstybių narių teikiama pagalba valstybei narei, nukentėjusiai nuo reikšmingo ar didelio masto kibernetinio saugumo incidento, be kita ko, teikiama per CSIRT tinklą, įsteigtą pagal Direktyvos (ES) 2022/2555 15 straipsnį. Pagalbą teikiančioms valstybėms narėms turėtų būti leidžiama teikti prašymus padengti išlaidas, susijusias su ekspertų grupių

[1] 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.

siuntimu teikiant savitarpio pagalbą. Tinkamos finansuoti išlaidos galėtų apimti kibernetinio saugumo ekspertų kelionės, apgyvendinimo ir dienpinigių išlaidas;

(33) turėtų būti palaipsniui sukurtas Sąjungos lygmens kibernetinio saugumo rezervas, kurį sudarytų privačių valdomų saugumo paslaugų teikėjų paslaugos, kuriomis būtų remiami reagavimo ir nedelsiamo veiklos atkūrimo veiksmai reikšmingų arba didelio masto kibernetinio saugumo incidentų atvejais. ES kibernetinio saugumo rezervas turėtų užtikrinti paslaugų prieinamumą ir parengtį***, kartu stiprinant Sąjungos atsparumą, įskaitant Europos valdomų saugumo paslaugų teikėjų, kurie yra MVĮ, dalyvavimą ir užtikrinant kibernetinio saugumo ekosistemos, visų pirma labai mažų įmonių, MVĮ, įskaitant startuolius, kūrimą, investuojant į mokslinius tyrimus ir inovacijas (MTI), kad būtų plėtojamos pažangiosios technologijos, pavyzdžiui, susijusios su debesija ir dirbtiniu intelektu. Patikimi paslaugų teikėjai, įskaitant MVĮ, turėtų turėti galimybę bendradarbiauti tarpusavyje, kad atitiktų pirmiau nurodytus kriterijus.*** ES kibernetinio saugumo rezervo paslaugos turėtų padėti nacionalinėms institucijoms teikti pagalbą paveiktiems subjektams, veikiantiems ypatingos svarbos ar itin svarbiuose sektoriuose, papildant jų pačių veiksmus nacionaliniu lygmeniu. ***Todėl kibernetinio saugumo rezervu turėtų būti skatinamos investicijos į mokslinius tyrimus ir inovacijas, kad būtų didinama šių technologijų plėtra. Kai tinkama, galėtų būti vykdomos bendros pratybos su patikimais kibernetinio saugumo rezervo paslaugų teikėjais ir potencialiais naudotojais, kad prireikus būtų užtikrintas veiksmingas rezervo veikimas.*** Prašydamos paramos iš ES kibernetinio saugumo rezervo, valstybės narės turėtų nurodyti, kokia parama atitinkamam subjektui teikiama nacionaliniu lygmeniu, ir į tai turėtų būti atsižvelgta vertinant valstybės narės prašymą. ES kibernetinio saugumo rezervo paslaugos taip pat gali būti naudingos panašiomis sąlygomis teikiant paramą Sąjungos institucijoms, įstaigoms***, organams*** ir agentūroms. ***Komisija turėtų užtikrinti, kad valstybės narės dalyvautų ir su jomis būtų plačiai keičiamasi informacija, siekiant išvengti dubliavimo su panašiomis iniciatyvomis, be kita ko, Šiaurės Atlanto sutarties organizacijoje (NATO);***

(34) siekiant atrinkti privačius paslaugų teikėjus, kurie teiktų paslaugas pagal ES kibernetinio saugumo rezervą, būtina nustatyti minimaliuosius kriterijus, kurie turėtų būti įtraukti į kvietimą teikti pasiūlymus tiems paslaugų teikėjams atrinkti, siekiant užtikrinti, kad būtų tenkinami valstybių narių institucijų ir subjektų, veikiančių ypatingos svarbos ar itin svarbiuose sektoriuose, poreikiai. ***Turėtų būti skatinamas mažesnių paslaugų teikėjų, veikiančių regionų ir vietos lygmeniu, dalyvavimas;***

(35) siekdama paremti ES kibernetinio saugumo rezervo sukūrimą, Komisija galėtų apsvarstyti galimybę prašyti ENISA pagal Reglamentą (ES) 2019/881 parengti potencialią valdomų saugumo paslaugų sertifikavimo schemą srityse, kurioms taikomas reagavimo į kibernetinio saugumo krizes mechanizmas. ***Kad ENISA galėtų vykdyti papildomas užduotis, susijusias su šia nuostata, jai turėtų būti skiriamas pakankamas papildomas finansavimas;***

(36) siekiant remti šio reglamento tikslus skatinti bendrą informuotumą apie padėtį, didinti Sąjungos atsparumą ir sudaryti sąlygas veiksmingai reaguoti į reikšmingus ir didelio masto kibernetinio saugumo incidentus, EU-CyCLONe, CSIRT tinklas arba Komisija turėtų turėti galimybę prašyti ENISA peržiūrėti ir įvertinti grėsmes, pažeidžiamumus ir poveikio švelninimo veiksmus, susijusius su konkrečiu reikšmingu ar didelio masto kibernetinio saugumo incidentu. Užbaigusi incidento peržiūrą ir vertinimą, ENISA, bendradarbiaudama su atitinkamais suinteresuotaisiais subjektais, įskaitant privačiojo sektoriaus, valstybių narių, Komisijos ir kitų atitinkamų ES institucijų, įstaigų***, organų***

ir agentūrų atstovus, turėtų parengti incidento peržiūros ataskaitą. Kalbant apie privatųjį sektorių, ENISA kuria informacijos mainų su specializuotais paslaugų teikėjais, įskaitant valdomų saugumo sprendinių teikėjus ir pardavėjus, kanalus, siekdama prisidėti prie ENISA misijos pasiekti aukštą bendrą kibernetinio saugumo lygį visoje Sąjungoje. Remiantis bendradarbiavimu su suinteresuotaisiais subjektais, įskaitant privatųjį sektorių, konkrečių incidentų peržiūros ataskaitoje turėtų būti siekiama įvertinti incidento priežastis, poveikį ir padarinių švelninimą po incidento. Ypač daug dėmesio turėtų būti skiriama informacijai ir patirčiai, kuria dalijasi valdomų saugumo paslaugų teikėjai, atitinkantys aukščiausio profesinio sąžiningumo, nešališkumo ir reikiamos techninės kompetencijos sąlygas, kaip reikalaujama šiame reglamente. Ataskaita turėtų būti pateikta EU-CyCLONe, CSIRT tinklui ir Komisijai ir ja turėtų būti remiamasi jų darbe. Kai incidentas susijęs su trečiąja valstybe, Komisija turėtų ja pasidalyti ir su vyriausiuoju įgaliotiniu;

(37) atsižvelgiant į nenuspėjamą kibernetinio saugumo išpuolių pobūdį ir į tai, kad jie neretai nėra susiję su konkrečia geografine vietove ir kelia didelę šalutinio poveikio riziką, didinant kaimyninių šalių atsparumą ir stiprinant gebėjimą veiksmingai reaguoti į reikšmingus ir didelio masto kibernetinio saugumo incidentus prisidedama prie visos Sąjungos apsaugos. Todėl su Skaitmeninės Europos programa asocijuotos trečiosios valstybės gali būti remiamos ES kibernetinio saugumo rezervo lėšomis, jei tai numatyta atitinkamame Skaitmeninės Europos programos asociacijos susitarime. Sąjunga turėtų remti asocijuotųjų trečiųjų valstybių finansavimą pagal toms valstybėms skirtas atitinkamas partnerystes ir finansavimo priemones. Parama turėtų būti skiriama paslaugoms, susijusioms su reagavimu į reikšmingus arba didelio masto kibernetinio saugumo incidentus ir nedelsiamu veiklos atkūrimu po jų. Šiame reglamente ES kibernetinio saugumo rezervui ir patikimiems paslaugų teikėjams nustatytos sąlygos turėtų būti taikomos teikiant paramą Skaitmeninės Europos programos asocijuotosioms trečiosioms valstybėms;

(37a) trečiosios valstybės galėtų gauti išteklių ir paramos pagal šį reglamentą, naudodamosi ES kibernetinio saugumo rezervo teikiama reagavimo į kibernetinius incidentus parama. Be to, konkrečioms ES kibernetinio saugumo rezervo paslaugoms teikti gali prireikti reagavimo į incidentus paslaugų teikėjų iš trečiųjų valstybių, įskaitant Skaitmeninės Europos programos asocijuotąsias trečiąsias valstybes arba kitas tarptautines šalis partneres ir NATO nares. Nukrypstant nuo Reglamento (ES, Euratomas) 2018/1046, siekiant stiprinti Sąjungos technologinį suverenumą, jos atvirą strateginį savarankiškumą, konkurencingumą bei atsparumą ir apsaugoti Sąjungos ypatingos svarbos turtą, interesus ar saugumą, subjektams, įsisteigusiems trečiosiose valstybėse, kurios nėra Sutarties dėl viešųjų pirkimų šalys ir kurių atžvilgiu nebuvo atliktas tikrinimas, kaip tai suprantama Europos Parlamento ir Tarybos reglamente (ES) 2019/452[1], ir prireikus taikomos švelninimo priemonėms, atsižvelgiant į šio reglamento tikslus, neturėtų būti leidžiama dalyvauti. Šio reglamento išorės aspektas turėtų atitikti asociacijos susitarimo pagal Skaitmeninės Europos programą nuostatas. Trečiųjų valstybių dalyvavimas turėtų būti viešai tikrinamas dalyvaujant teisėkūros institucijoms, siekiant užtikrinti, kad piliečiai galėtų dalyvauti šiame procese;

---

[1] 2019 m. kovo 19 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/452, kuriuo nustatoma tiesioginių užsienio investicijų į Sąjungą tikrinimo sistema (OL L 79I, 2019 3 21, p. 1, ELI: https://eur-lex.europa.eu/eli/reg/2019/452/oj?locale=lt).

(38) siekiant užtikrinti vienodas šio reglamento įgyvendinimo sąlygas, Komisijai turėtų būti suteikti įgyvendinimo įgaliojimai nustatyti tarpvalstybinių SOC sąveikumo sąlygas, nustatyti tarpvalstybinių SOC ir Sąjungos subjektų dalijimosi informacija, susijusia su galimu arba vykstančiu didelio masto kibernetinio saugumo incidentu, procedūrinę tvarką, nustatyti techninius reikalavimus, kuriais užtikrinamas Europos kibernetinio saugumo skydo saugumas, nurodyti reagavimo paslaugų, kurių reikia ES kibernetinio saugumo rezervui, rūšis ir skaičių ir išsamiau nustatyti ES kibernetinio saugumo rezervo paramos paslaugų skyrimo tvarką. Tais įgaliojimais turėtų būti naudojamasi laikantis Europos Parlamento ir Tarybos reglamento (ES) Nr. 182/2011*;

---

* ***2011 m. vasario 16 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 182/2011, kuriuo nustatomos valstybių narių vykdomos Komisijos naudojimosi įgyvendinimo įgaliojimais kontrolės mechanizmų taisyklės ir bendrieji principai (OL L 55, 2011 2 28, p. 13, ELI: http://data.europa.eu/eli/reg/2011/182/oj).***

(38a) kvalifikuoti darbuotojai, galintys patikimai teikti atitinkamas kibernetinio saugumo paslaugas laikantis aukščiausių standartų, yra būtini siekiant veiksmingai įgyvendinti Europos kibernetinio saugumo skydo ir Reagavimo į kibernetinio saugumo krizes mechanizmą. Todėl susirūpinimą kelia tai, kad Sąjunga susiduria su darbuotojų trūkumu, nes trūksta kvalifikuotų specialistų, ir tuo pat metu ji susiduria su sparčiai kintančia grėsmių aplinka, kaip pripažinta 2023 m. balandžio 18 d. Komisijos komunikate dėl Kibernetinio saugumo įgūdžių akademijos. Svarbu panaikinti šį specialistų trūkumą stiprinant įvairių suinteresuotųjų subjektų, įskaitant privatųjį sektorių, akademinę bendruomenę, valstybes nares, Komisiją ir ENISA, bendradarbiavimą ir koordinavimą, siekiant plėsti investicijas į švietimą ir mokymą ir kurti jų sinergiją visose teritorijose, plėtoti viešojo ir privačiojo sektorių partnerystes, remti mokslinių tyrimų ir inovacijų iniciatyvas, plėtoti ir tarpusavyje pripažinti bendrus standartus ir kibernetinio saugumo įgūdžių sertifikavimą, be kita ko, pasitelkiant Europos kibernetinio saugumo įgūdžių sistemą. Tai taip pat turėtų palengvinti kibernetinio saugumo specialistų judumą Sąjungoje. Šiuo reglamentu turėtų būti siekiama skatinti didesnę kibernetinio saugumo darbuotojų įvairovę. Visoms priemonėms, kuriomis siekiama didinti kibernetinio saugumo įgūdžius, reikalingos apsaugos priemonės, kad būtų išvengta protų nutekėjimo ir pavojaus darbo jėgos judumui;

(38b) reikia stiprinti specializuotus, tarpdalykinius ir bendruosius įgūdžius ir kompetencijas visoje Sąjungoje, ypatingą dėmesį skiriant moterims, nes kibernetinio saugumo srityje vis dar egzistuoja lyčių nelygybė – moterys sudaro 20 proc. vidutinio šios srities darbuotojų skaičiaus visame pasaulyje. Moterys turi dalyvauti kuriant skaitmeninę ateitį ir ją valdant;

(38c) kibernetinio saugumo mokslinių tyrimų ir inovacijų (MTI) stiprinimu siekiama padidinti Sąjungos atsparumą ir atvirą strateginį savarankiškumą. Taip pat svarbu kurti sinergiją su MTI programomis ir esamomis priemonėmis bei institucijomis ir stiprinti įvairių suinteresuotųjų subjektų, įskaitant privatųjį sektorių, pilietinę visuomenę, akademinę bendruomenę, valstybes nares, Komisiją ir ENISA, bendradarbiavimą ir koordinavimą;

(38d) šiuo reglamentu turėtų būti prisidedama siekiant Europos deklaracijoje dėl skaitmeninio dešimtmečio skaitmeninių teisių ir principų nustatyto įsipareigojimo apsaugoti mūsų demokratinių valstybių, žmonių, įmonių ir viešųjų institucijų interesus nuo kibernetinio saugumo pavojų ir kibernetinių nusikaltimų, įskaitant duomenų saugumo pažeidimus ir tapatybės vagystę ar manipuliavimą tapatybe. Šio reglamento taikymas taip pat turėtų padėti gerinti kitų teisės aktų, pavyzdžiui, susijusių su dirbtiniu intelektu, duomenų privatumu ir duomenų reguliavimu, įgyvendinimą kibernetinio saugumo ir kibernetinio atsparumo požiūriu;

(38e) Siekiant sėkmingai įgyvendinti šį reglamentą, labai svarbu stiprinti kibernetinio saugumo kultūrą, kurioje saugumas, įskaitant skaitmeninės aplinkos saugumą, suvokiamas kaip viešoji gėrybė. Todėl priemonių, kuriomis siekiama įtraukti piliečius ir didinti jų informuotumą, rengimas turėtų būti dar viena priemonė, padedanti užtikrinti mūsų demokratinių valstybių ir pagrindinių vertybių apsaugą;

(38f) siekiant papildyti tam tikras neesmines šio reglamento nuostatas, pagal SESV 290 straipsnį Komisijai turėtų būti suteikti įgaliojimai priimti aktus, kuriais nustatomos tarpvalstybinių SOC sąveikumo sąlygos, procedūrinė keitimosi informacija tarp tarpvalstybinių SOC ir EU-CyCLONe, CSIRT tinklo ir Komisijos tvarka, reagavimo paslaugų, reikalingų ES kibernetinio saugumo rezervui, rūšys ir skaičius, taip pat išsami ES kibernetinio saugumo rezervo paramos paslaugų paskirstymo tvarka. Ypač svarbu, kad atlikdama parengiamąjį darbą Komisija tinkamai konsultuotųsi, taip pat ir su ekspertais, ir kad tos konsultacijos būtų vykdomos vadovaujantis 2016 m. balandžio 13 d. Tarpinstituciniame susitarime dėl geresnės teisėkūros* nustatytais principais. Visų pirma siekiant užtikrinti vienodas galimybes dalyvauti atliekant su deleguotaisiais aktais susijusį parengiamąjį darbą, Europos Parlamentas ir Taryba visus dokumentus gauna tuo pačiu metu kaip ir valstybių narių ekspertai, o jų ekspertams sistemingai suteikiama galimybė dalyvauti Komisijos ekspertų grupių, kurios atlieka su deleguotaisiais aktais susijusį parengiamąjį darbą, posėdžiuose;

****OL L 123, 2016 5 12, p. 1, ELI: https://eurlex.europa.eu/eli/agree_interinstit/2016/512/oj.?locale=lt***

(39) ***kadangi šio reglamento tikslų, t. y. sustiprinti Sąjungos kibernetinių grėsmių prevencijos, nustatymo, reagavimo į jas ir veiklos atkūrimo po jų pajėgumus ir sukurti bendrą sistemą, pagal kurią būtų naikinamos uždaros komunikacijos sistemos, valstybės narės negali deramai pasiekti, tų tikslų*** geriau siekti Sąjungos lygmeniu. Todėl, laikydamasi Europos Sąjungos sutarties 5 straipsnyje nustatytų subsidiarumo ir proporcingumo principų, Sąjunga gali patvirtinti priemones. ***Pagal tame straipsnyje nustatytą proporcingumo principą*** šiame reglamente nenumatyta nieko, kas nėra būtina siekiant to tikslo,

PRIĖMĖ ŠĮ REGLAMENTĄ:

I skyrius

BENDRIEJI TIKSLAI, DALYKAS IR APIBRĖŽTYS

1 straipsnis

Dalykas ir tikslai

1. Šiuo reglamentu nustatomos priemonės, kuriomis Sąjungoje stiprinami pajėgumai aptikti kibernetinio saugumo grėsmes ir incidentus, jiems pasirengti ir į juos reaguoti, visų pirma imantis šių veiksmų:

a) diegti visos Europos saugumo operacijų centrų ***tinklą*** (Europos kibernetinio saugumo skydą) siekiant sukurti ir sustiprinti bendrus aptikimo ir informuotumo apie padėtį pajėgumus;

b) sukurti Reagavimo į kibernetinio saugumo krizes mechanizmą, skirtą padėti valstybėms narėms pasirengti reikšmingiems ir didelio masto kibernetinio saugumo incidentams, į juos reaguoti ir nedelsiant po jų atkurti veiklą;

c) sukurti Europos kibernetinio saugumo incidentų peržiūros mechanizmą reikšmingiems arba didelio masto incidentams peržiūrėti ir įvertinti.

2. Šiuo reglamentu siekiama stiprinti Sąjungos lygmens solidarumą siekiant šių konkrečių tikslų:

a) stiprinti bendrą Sąjungos kibernetinių grėsmių ir incidentų aptikimą ir informuotumą apie padėtį, taip sudarant sąlygas ***remti Sąjungos ir valstybių narių pramonės pajėgumus kibernetinio saugumo sektoriuje ir*** stiprinti Sąjungos pramonės***, visų pirma labai mažų įmonių, MVĮ, įskaitant startuolius,*** ir paslaugų sektorių konkurencinę padėtį visoje skaitmeninėje ekonomikoje ir prisidėti prie Sąjungos technologinio suverenumo***, jos atviro strateginio savarankiškumo, konkurencingumo ir atsparumo tame sektoriuje, stiprinant kibernetinio saugumo ekosistemą, siekiant užtikrinti tvirtus Sąjungos pajėgumus, be kita ko, bendradarbiaujant su tarptautiniais partneriais***;

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;

c) didinti Sąjungos atsparumą ir prisidėti prie veiksmingo reagavimo peržiūrint ir vertinant reikšmingus arba didelio masto incidentus, be kita ko, apibendrinant įgytą patirtį ir, kai tinkama, rengiant rekomendacijas;

ca) koordinuotai ugdyti darbo jėgos įgūdžius, praktinę patirtį ir kompetenciją, kad būtų užtikrintas kibernetinis saugumas ir sukurta sinergija su Kibernetinio saugumo

įgūdžių akademija.

3. Šiuo reglamentu nedaroma poveikio pagrindinei valstybių narių atsakomybei už nacionalinį saugumą, visuomenės saugumą ir nusikalstamų veikų prevenciją, tyrimą, atskleidimą ir baudžiamąjį persekiojimą už jas.

2 straipsnis

Terminų apibrėžtys

Šiame reglamente vartojamų terminų apibrėžtys:

-1a) nacionalinis saugumo operacijų centras arba nacionalinis SOC – centralizuota nacionalinė tarnyba, nuolat renkanti ir analizuojanti žvalgybos informaciją apie kibernetines grėsmes ir gerinanti kibernetinio saugumo būklę pagal 4 straipsnį;

1) **tarpvalstybinis saugumo operacijų centras** ***arba*** **tarpvalstybinis SOC** – daugiašalė platforma, kuri į koordinuojamą tinklo struktūrą sujungia nacionalinius SOC ***pagal 5 straipsnį***;

2) **viešoji įstaiga** – viešosios teisės reglamentuojami ***subjektai***, apibrėžti Europos Parlamento ir Tarybos direktyvos 2014/24/ES[1] 2 straipsnio 1 dalies 4 punkte;

3) **prieglobos konsorciumas** – konsorciumas, sudarytas iš dalyvaujančių valstybių, kurioms atstovauja nacionaliniai SOC ***pagal 5 straipsnį***;

4) **subjektas** – subjektas, apibrėžtas Direktyvos (ES) 2022/2555 6 straipsnio 38 punkte;

4a) ypatingos svarbos subjektas – ypatingos svarbos subjektas, apibrėžtas Europos Parlamento ir Tarybos direktyvos (ES) 2022/2557[2] 2 straipsnio 1 dalies 1 punkte;

5) **ypatingos svarbos arba itin svarbiuose sektoriuose veikiantys subjektai** – subjektai, ***veikiantys*** Direktyvos (ES) 2022/2555 I ir II prieduose išvardytuose ***sektoriuose***;

5a) incidento valdymas – incidento valdymas, apibrėžtas Direktyvos (ES) 2022/2555 6 straipsnio 8 punkte;

5b) rizika – rizika, apibrėžta Direktyvos (ES) 2022/2555 6 straipsnio 9 punkte;

6) **kibernetinė grėsmė** – kibernetinė grėsmė, apibrėžta Reglamento (ES) 2019/881 2 straipsnio 8 punkte;

6a) didelė kibernetinė grėsmė – didelė kibernetinė grėsmė, kaip apibrėžta Direktyvos (ES) 2022/2555 6 straipsnio 11 punkte;

---

1 2014 m. vasario 26 d. Europos Parlamento ir Tarybos direktyva 2014/24/ES dėl viešųjų pirkimų, kuria panaikinama Direktyva 2004/18/EB (OL L 94, 2014 3 28, p. 65).

2 ***2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2557 dėl ypatingos svarbos subjektų atsparumo, kuria panaikinama Tarybos direktyva 2008/114/EB (OL L 333, 2022 12 27, p. 164, ELI: https://eur-lex.europa.eu/eli/dir/2022/2557/oj?locale=lt).***

7) **reikšmingas kibernetinio saugumo incidentas** – kibernetinio saugumo incidentas, atitinkantis Direktyvos (ES) 2022/2555 23 straipsnio 3 dalyje nustatytus kriterijus;

8) **didelio masto kibernetinio saugumo incidentas** – incidentas, apibrėžtas Direktyvos (ES) 2022/2555 6 straipsnio 7 punkte;

9) **parengtis** – parengties būsena ir pajėgumas užtikrinti veiksmingą greitą reagavimą į reikšmingą arba didelio masto kibernetinio saugumo incidentą, atlikus rizikos vertinimą ir iš anksto ėmusis stebėsenos veiksmų;

10) **reagavimas** – veiksmai reikšmingo arba didelio masto kibernetinio saugumo incidento atveju, tokio incidento metu ar jam pasibaigus, kuriais siekiama pašalinti jo tiesioginius ir trumpalaikius neigiamus padarinius;

10a) valdomų saugumo paslaugų teikėjas – teikėjas, apibrėžtas Direktyvos (ES) 2022/2555 6 straipsnio 40 punkte;

11) **patikimi *valdomų saugumo paslaugų* teikėjai** – valdomų saugumo paslaugų teikėjai, atrinkti***, kad būtų įtraukti į ES kibernetinio saugumo rezervą*** pagal šio reglamento 16 straipsnį.

II skyrius

EUROPOS KIBERNETINIO SAUGUMO SKYDAS

3 straipsnis

Europos kibernetinio saugumo skydo sukūrimas

1. Siekiant plėtoti pažangius Sąjungos pajėgumus aptikti kibernetines grėsmes, jas analizuoti ir tvarkyti duomenis apie jas bei ***užkirsti kelią*** incidentams Sąjungoje sukuriamas saugumo operacijų centrų ***tinklas*** (toliau – Europos kibernetinio saugumo skydas). Ją sudaro visi nacionaliniai saugumo operacijų centrai (nacionaliniai SOC) ir tarpvalstybiniai saugumo operacijų centrai (tarpvalstybiniai SOC).

Veiksmai, kuriais įgyvendinamas Europos kibernetinio saugumo skydas, remiami Skaitmeninės Europos programos lėšomis ir įgyvendinami pagal Reglamentą (ES) 2021/694, visų pirma jo 3 konkretų tikslą.

2. Europos kibernetinio saugumo skydas:

a) per tarpvalstybinius SOC telkia įvairių šaltinių duomenis apie kibernetines grėsmes ir incidentus ir jais dalijasi***, taip pat prireikus keičiasi informacija su CSIRT tinklu***;

b) rengia aukštos kokybės informaciją, kuria remiantis galima imtis veiksmų, ir žvalgybos informaciją apie kibernetines grėsmes, naudodamas naujausias priemones, visų pirma dirbtinio intelekto ir duomenų analizės technologijas;

c) padeda geriau apsisaugoti nuo kibernetinių grėsmių ir į jas reaguoti***, be kita ko, teikiant konkrečias rekomendacijas subjektams***;

d) padeda sparčiau aptikti kibernetines grėsmes ir didinti informuotumą apie padėtį visoje Sąjungoje;

e) teikia paslaugas ir vykdo veiklą, skirtas kibernetinio saugumo bendruomenei Sąjungoje, be kita ko, padėdamas kurti pažangias dirbtinio intelekto ir duomenų analizės priemones.

Jis plėtojamas bendradarbiaujant su visos Europos našiosios kompiuterijos infrastruktūra, sukurta pagal Reglamentą (ES) 2021/1173.

4 straipsnis

Nacionaliniai saugumo operacijų centrai

1. ***Kad galėtų*** dalyvauti Europos kibernetinio saugumo skydo veikloje, kiekviena valstybė narė paskiria bent po vieną nacionalinį SOC. Nacionalinis SOC yra ***centralizuota*** viešosios įstaigos ***tarnyba***. ***Kai įmanoma, nacionaliniai SOC įtraukiami į CSIRT arba kitas esamas kibernetinio saugumo infrastruktūras ir valdymą.***

Nacionalinis SOC yra pajėgus veikti kaip atskaitos taškas ir kreiptis į kitas viešąsias ir privačias nacionalinio lygmens organizacijas, ***visų pirma į jų SOC,*** kad rinktų ir analizuotų informaciją apie kibernetinio saugumo grėsmes ir incidentus ***ir prireikus dalytųsi šia informacija su tos valstybės narės CSIRT tinklo nariais***, taip pat prisidėtų prie tarpvalstybinio SOC veiklos. Jis aprūpinamas naujausiomis technologijomis, kuriomis galima ***apsaugoti***, aptikti, kaupti ir analizuoti su kibernetinio saugumo grėsmėmis ir incidentais susijusius duomenis.

Nacionalinis SOC arba CSIRT gali prašyti valdomų saugumo paslaugų teikėjų, kurie teikia paslaugą ypatingos svarbos subjektui, pateikti jų nacionalinių ypatingos svarbos subjektų telemetrijos, jutiklių ar registravimo duomenis. Šiais duomenimis dalijamasi laikantis Sąjungos duomenų apsaugos teisės aktų ir tik tam, kad būtų galima padėti nacionaliniams SOC arba CSIRT nustatyti kibernetinio saugumo grėsmes ir incidentus bei užkirsti jiems kelią.

2. Paskelbus kvietimą pareikšti susidomėjimą, Europos kibernetinio saugumo kompetencijos centras (ECCC) ***gali*** atrinkti nacionalinius SOC dalyvauti bendruose viešuosiuose priemonių ir infrastruktūros pirkimuose su ECCC. ECCC atrinktiems nacionaliniams SOC gali skirti dotacijas šių priemonių ir infrastruktūros veikimui finansuoti. Sąjungos finansiniu įnašu padengiama iki 50 proc. priemonių ir infrastruktūros įsigijimo išlaidų ir iki 50 proc. veiklos išlaidų, o likusias išlaidas padengia valstybė narė. Prieš pradėdami priemonių ir infrastruktūros įsigijimo procedūrą, ECCC ir nacionalinis SOC sudaro prieglobos ir naudojimo susitarimą, kuriuo reglamentuojamas priemonių ir infrastruktūros naudojimas.

3. Pagal 2 dalį atrinktas nacionalinis SOC įsipareigoja pateikti paraišką dalyvauti tarpvalstybiniame SOC per dvejus metus nuo priemonių ir infrastruktūros įsigijimo arba

finansavimo dotacijos gavimo dienos, priklausomai nuo to, kuri iš tų datų yra ankstesnė. Jei iki to laiko nacionalinis SOC nepradeda dalyvauti tarpvalstybinio SOC veikloje, jis negali gauti papildomos Sąjungos paramos pagal šį reglamentą.

5 straipsnis

Tarpvalstybiniai saugumo operacijų centrai

1. Teisę dalyvauti steigiant tarpvalstybinį SOC turi prieglobos konsorciumas, kurį sudaro bent trys valstybės narės, atstovaujamos nacionalinių SOC, įsipareigojusių bendradarbiauti koordinuojant savo kibernetinių grėsmių aptikimo ir stebėsenos veiklą. ***Tarpvalstybinis SOC skirtas aptikti ir analizuoti kibernetines grėsmes, užkirsti kelią incidentams ir remti kokybiškos žvalgybos informacijos rengimą, visų pirma keičiantis duomenimis iš įvairių viešųjų ir privačių šaltinių, taip pat dalijantis naujausiomis priemonėmis ir bendrai plėtojant kibernetinių incidentų aptikimo, analizės, prevencijos ir apsaugos pajėgumus patikimoje ir saugioje aplinkoje.***

2. Paskelbus kvietimą pareikšti susidomėjimą, ECCC ***gali*** atrinkti prieglobos konsorciumą dalyvauti bendruose viešuosiuose priemonių ir infrastruktūros pirkimuose su ECCC. ECCC atrinktam prieglobos konsorciumui gali skirti dotaciją priemonių ir infrastruktūros veikimui finansuoti. Sąjungos finansiniu įnašu padengiama iki 75 proc. priemonių ir infrastruktūros įsigijimo išlaidų ir iki 50 proc. veiklos išlaidų, o likusias išlaidas padengia prieglobos konsorciumas. Prieš pradėdami priemonių ir infrastruktūros įsigijimo procedūrą, ECCC ir prieglobos konsorciumas sudaro prieglobos ir naudojimo susitarimą, kuriuo reglamentuojamas priemonių ir infrastruktūros naudojimas.

2a. Nukrypstant nuo Reglamento (ES, Euratomas) 2018/1046 176 straipsnio, subjektai, įsisteigę trečiosiose valstybėse, kurios nėra Sutarties dėl viešųjų pirkimų šalys, nedalyvauja bendruose priemonių ir infrastruktūros viešuosiuose pirkimuose.

3. Prieglobos konsorciumo nariai sudaro rašytinį konsorciumo susitarimą, kuriame nustatoma prieglobos ir naudojimo susitarimo įgyvendinimo vidaus tvarka.

4. Tarpvalstybiniam SOC teisiškai atstovauja koordinuojantysis nacionalinis SOC arba prieglobos konsorciumas, jei jis turi juridinio asmens statusą. Koordinuojantysis SOC yra atsakingas už prieglobos ir naudojimo susitarimo ir šio reglamento reikalavimų laikymąsi.

6 straipsnis

Bendradarbiavimas ir keitimasis informacija tarpvalstybiniuose SOC ir tarp jų

1. Prieglobos konsorciumo nariai tarpvalstybiniame SOC keičiasi svarbia informacija, įskaitant informaciją, susijusią su kibernetinėmis grėsmėmis, vos neįvykusiais incidentais, pažeidžiamumais, metodais ir procedūromis, užvaldymo rodikliais, priešiška taktika, konkrečių grėsmių ir dalyvių informacija, kibernetinio saugumo įspėjimais ir rekomendacijomis dėl kibernetinio saugumo priemonių konfigūracijos siekiant aptikti kibernetinius išpuolius rekomendacijomis, kai tokiu dalijimusi informacija:

a) ***gerinamas nacionalinių ir tarpvalstybinių SOC ir pramonės ISAC keitimasis žvalgybos informacija apie kibernetines grėsmes, siekiant užkirsti kelią grėsmėms, jas aptikti ar sušvelninti jų poveikį;***

b) didinamas kibernetinis saugumas, visų pirma didinant informuotumą apie kibernetines grėsmes, ribojant arba sustabdant tokių grėsmių plitimo galimybes, remiant įvairius gynybos pajėgumus, pažeidžiamumų ištaisymą ir atskleidimą, grėsmių aptikimo, sustabdymo ir prevencijos metodus, švelninimo strategijas ar reagavimo ir veiklos atkūrimo etapus arba skatinant bendradarbiavimu grindžiamus viešųjų ir privačių subjektų atliekamus kibernetinių grėsmių mokslinius tyrimus.

2. 5 straipsnio 3 dalyje nurodytame rašytiniame konsorciumo susitarime nustatoma:

a) įsipareigojimas dalytis ▌ 1 dalyje nurodytais ***svarbiais*** duomenimis ir sąlygos, kuriomis turi būti keičiamasi ta informacija;

b) valdymo sistema, kuria visi dalyviai skatinami dalytis informacija;

c) prisidėjimo prie pažangių dirbtinio intelekto ir duomenų analizės priemonių kūrimo tikslai.

3. Siekiant skatinti tarpvalstybinius SOC keistis informacija tarpusavyje ***ir su pramonės ISAC***, tarpvalstybiniai SOC užtikrina aukštą tarpusavio sąveikos ***ir, kai įmanoma, sąveikos su pramonės ISAC lygį***. Siekiant palengvinti tarpvalstybinių SOC ***ir pramonės ISAC*** sąveiką***, dalijimosi informacija standartai ir protokolai gali būti suderinti su tarptautiniais standartais ir geriausia pramonės praktika***. ***Taip pat skatinami bendri kibernetinės infrastruktūros, paslaugų ir priemonių viešieji pirkimai. Be to,*** Komisija, pasikonsultavus su ECCC ***ir ENISA, pagal 20a straipsnį įgaliojama ne vėliau kaip ... [šeši mėnesiai nuo šio reglamento įsigaliojimo dienos] priimti deleguotuosius aktus, kuriais šis reglamentas būtų papildytas nustatant šios sąveikos sąlygas, glaudžiai koordinuojant veiksmus su tarpvalstybiniais SOC ir remiantis tarptautiniais standartais bei geriausia pramonės praktika.***

4. Tarpvalstybiniai SOC sudaro tarpusavio bendradarbiavimo ***ir, kai tinkama, bendradarbiavimo su pramonės ISAC*** susitarimus, kuriuose nustatomi tarpvalstybinių platformų keitimosi informacija ***ir sąveikos*** principai***, atsižvelgiant į jau esamus atitinkamus keitimosi informacija mechanizmus, numatytus Direktyvoje (ES) 2022/2555***. ***Kai tinkama, tarpvalstybiniai SOC sudaro bendradarbiavimo susitarimus su pramonės ISAC. Galimo arba vykstančio didelio masto kibernetinio saugumo incidento atveju keitimosi informacija mechanizmai turi atitikti atitinkamas Direktyvos (ES) 2022/2555 nuostatas.***

7 straipsnis

Bendradarbiavimas ir dalijimasis informacija su *CSIRT tinklu*

1. Kai tarpvalstybiniai SOC gauna informacijos, susijusios su galimu arba tebesitęsiančiu didelio masto kibernetinio saugumo incidentu, ***kad būtų galima dalytis informacija apie padėtį, koordinuojantis SOC nepagrįstai nedelsdamas*** pateikia atitinkamą informaciją ***savo CSIRT arba kompetentingai institucijai, kuri apie tai praneša*** Europos ryšių palaikymo dėl kibernetinių krizių organizaciniam tinklui (EU-CyCLONe), reagavimo į kompiuterių saugumo incidentus tarnybų (CSIRT) tinklui, Komisijai ***ir ENISA, pagal*** jų atitinkamus krizių valdymo vaidmenis ***ir procedūras*** pagal Direktyvą (ES) 2022/2555. ***Šia dalimi viešiesiems ar privatiesiems subjektams nenustatomos papildomos pareigos pranešti apie galimą ar vykstantį didelio masto kibernetinio saugumo incidentą, kad jie galėtų vykdyti Direktyvoje (ES) 2022/2555 nustatytas pareigas.***

2. ***Komisijai pagal 20a straipsnį suteikiami įgaliojimai, pasikonsultavus su CSIRT tinklu, priimti deleguotuosius aktus, kuriais šis reglamentas papildomas nustatant šio straipsnio*** 1 dalyje nurodyto dalijimosi informacija procedūrinę tvarką ***ir laikantis Direktyvos (ES) 2022/2555.***

8 straipsnis

Saugumas

1. Europos kibernetinio saugumo skydo veikloje dalyvaujančios valstybės narės užtikrina aukštą Europos kibernetinio saugumo skydo infrastruktūros ***konfidencialumo***, duomenų saugumo ir fizinio saugumo lygį ir užtikrina, kad infrastruktūra būtų tinkamai valdoma ir kontroliuojama taip, kad būtų apsaugota nuo grėsmių ir būtų užtikrintas jos ir sistemų, įskaitant duomenis, kuriais keičiamasi per infrastruktūrą, saugumas.

2. Europos kibernetinio saugumo skydo veikloje dalyvaujančios valstybės narės užtikrina, kad dalijimasis informacija Europos kibernetinio saugumo skydo sistemoje su subjektais, kurie nėra valstybių narių viešosios įstaigos, nedarytų neigiamo poveikio Sąjungos saugumo interesams.

3. Komisija gali priimti įgyvendinimo aktus, kuriais nustatomi techniniai reikalavimai, kurių laikydamosi valstybės narės vykdo 1 ir 2 dalyse nustatytą pareigą. Tie įgyvendinimo aktai priimami laikantis šio reglamento 21 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros. ***Jie turi atitikti direktyvas (ES) 2022/2555 ir (ES) 2022/2557.*** Komisija, padedama vyriausiojo įgaliotinio, ***savo įgyvendinimo aktuose*** atsižvelgia į atitinkamus gynybos lygio saugumo standartus, kad palengvintų bendradarbiavimą su kariniais subjektais.

III skyrius

REAGAVIMO Į KIBERNETINIO SAUGUMO KRIZES MECHANIZMAS

9 straipsnis

Reagavimo į *kibernetinio saugumo* krizes mechanizmo sukūrimas

1. Siekiant padidinti Sąjungos atsparumą didelėms kibernetinio saugumo grėsmėms ir solidariai pasirengti trumpalaikiam reikšmingų ir didelio masto kibernetinio saugumo incidentų poveikiui

ir jį sušvelninti, sukuriamas Reagavimo į kibernetinio saugumo krizes mechanizmas (toliau – mechanizmas).

2. Veiksmai, kuriais įgyvendinamas ▌mechanizmas, remiami Skaitmeninės Europos programos lėšomis ir įgyvendinami pagal Reglamentą (ES) 2021/694, visų pirma jo 3 konkretų tikslą.

10 straipsnis

Veiksmų rūšys

1. Mechanizmu remiami šių rūšių veiksmai:

a) pasirengimo veiksmai, įskaitant koordinuotą subjektų, veikiančių itin svarbiuose sektoriuose visoje Sąjungoje, parengties testavimą;

b) reagavimo veiksmai, kuriais remiamas reagavimas į reikšmingus ir didelio masto kibernetinio saugumo incidentus ir nedelsiamas veiklos atkūrimas po jų ir kuriuos turi vykdyti patikimi ***valdomų saugumo*** paslaugų teikėjai, dalyvaujantys ES kibernetinio saugumo rezerve, sukurtame pagal 12 straipsnį;

c) savitarpio pagalbos veiksmai, t. y. pagalba, kurią vienos valstybės narės nacionalinės institucijos teikia kitai valstybei narei, visų pirma kaip nustatyta Direktyvos (ES) 2022/2555 11 straipsnio 3 dalies f punkte.

1a. Aktyvavus mechanizmą, Komisija kiekvienais metais įvertina ir paskelbia ataskaitą, kurioje įvertinamas teigiamas ir neigiamas mechanizmo veikimas, taip pat ir tai, ar reikalingi papildomi bendradarbiavimo ar mokymo reikalavimai.

11 straipsnis

Koordinuotas subjektų parengties testavimas

1. Siekdama remti koordinuotą 10 straipsnio 1 dalies a punkte nurodytą subjektų parengties testavimą visoje Sąjungoje, Komisija, pasikonsultavusi su TIS bendradarbiavimo grupe ir ENISA, iš Direktyvos (ES) 2022/2555 I priede išvardytų ypatingos svarbos sektorių atrenka sektorius arba subsektorius, kurių subjektams gali būti taikomas koordinuotas parengties testavimas, atsižvelgdama į esamus ir planuojamus suderintus rizikos vertinimus ir atsparumo bandymus Sąjungos lygmeniu ***pagal Direktyvos (ES) 2022/2555 I priede išvardytoms ypatingos svarbos sektorių subjektams nustatytą tvarką.***

2. TIS bendradarbiavimo grupė, bendradarbiaudama su Komisija, ENISA, vyriausiuoju įgaliotiniu, ***ir subjektais, kuriems taikomas koordinuotas parengties testavimas pagal 1 dalį,*** parengia bendrus rizikos scenarijus ir koordinuoto ***parengties*** testavimo metodikas***, kurių rezultatas – suderintas darbo planas***. ***Subjektai, kuriems taikomas koordinuotas parengties testavimas, parengia ir įgyvendina koregavimo planą, kuriame pateikiamos rekomendacijos, parengtos atlikus parengties testus.***

TIS bendradarbiavimo grupė gali informuoti apie tai, kokiems sektoriams ar subsektoriams

teikiama pirmenybė vykdant koordinuotą parengties testavimą.

12 straipsnis

ES kibernetinio saugumo rezervo sukūrimas

1. Siekiant padėti 3 dalyje nurodytiems naudotojams reaguoti į reikšmingus arba didelio masto kibernetinio saugumo incidentus arba teikti reagavimo į tokius incidentus ir nedelsiamo veiklos atkūrimo po jų paramą, sukuriamas ES kibernetinio saugumo rezervas.

Kai paaiškėja, kad įsigytos paslaugos negali būti visiškai panaudotos paramai reaguojant į reikšmingus ar didelio masto incidentus, šios paslaugos išimties tvarka gali būti pakeistos pratybomis ar mokymais, skirtais incidentų valdymui, ir jas naudotojams paprašius gali teikti perkančioji organizacija.

2. ES kibernetinio saugumo rezervą sudaro reagavimo į incidentus paslaugos, kurias teikia patikimi ***valdomų saugumo*** paslaugų teikėjai, atrinkti pagal 16 straipsnyje nustatytus kriterijus. Į ***ES kibernetinio saugumo*** rezervą įtraukiamos iš anksto įsipareigotos teikti paslaugos. Paslaugos diegiamos visose valstybėse narėse***, jomis stiprinamas Sąjungos technologinis suverenumas, atviras strateginis savarankiškumas, konkurencingumas ir atsparumas kibernetinio saugumo sektoriuje, be kita ko, visoje Sąjungoje skatinant inovacijas bendrojoje skaitmeninėje rinkoje.***

3. Be kitų, ES kibernetinio saugumo rezervo paslaugų naudotojai yra:

a) valstybių narių kibernetinio saugumo krizių valdymo institucijos ir CSIRT, nurodyti atitinkamai Direktyvos (ES) 2022/2555 9 straipsnio 1 ir 2 dalyse ir 10 straipsnyje;

b) Sąjungos institucijos, įstaigos ir agentūros***, kaip nurodyta Europos Parlamento ir Tarybos reglamento (ES) 2019/2023[1] 3 straipsnio 1 punkte, ir CERT-EU***;

4. 3 dalies a punkte nurodyti naudotojai naudojasi ES kibernetinio saugumo rezervo paslaugomis, kad reaguotų į reikšmingus arba didelio masto incidentus, darančius poveikį ypatingos svarbos ar itin svarbiuose sektoriuose veikiantiems subjektams, arba padėtų į juos reaguoti ir nedelsiant po jų atkurti veiklą.

5. Komisijai tenka bendra atsakomybė už ES kibernetinio saugumo rezervo įgyvendinimą. Komisija, ***koordinuodama veiksmus su TIS 2 koordinavimo grupe ir*** atsižvelgdama į 3 dalyje nurodytų naudotojų poreikius, nustato ES kibernetinio saugumo rezervo prioritetus ir raidą, prižiūri jo įgyvendinimą ir užtikrina papildomumą, nuoseklumą, sinergiją ir sąsajas su kitais paramos veiksmais pagal šį reglamentą, taip pat su kitais Sąjungos veiksmais ir programomis.

6. Komisija, sudarydama susitarimus dėl įnašų, ***paveda*** ENISA visiškai arba iš dalies užtikrinti ES kibernetinio saugumo rezervo veikimą ir administravimą.

---

[1] ***Reglamentas (ES).../2023, kuriuo nustatomos priemonės aukštam bendram kibernetinio saugumo lygiui Sąjungos institucijose, įstaigose, organuose ir agentūrose užtikrinti (OL C..., ..., p., ..., ELI: ...).***

7. Siekdama padėti Komisijai sukurti ES kibernetinio saugumo rezervą, ENISA, pasikonsultavusi su valstybėmis narėmis, Komisija ***ir, kai tinkama, valdomų saugumo paslaugų teikėjais ir kitais kibernetinio saugumo pramonės atstovais***, parengia reikiamų paslaugų aprašą***, įskaitant reikiamus kibernetinio saugumo darbuotojų įgūdžius ir kompetenciją***. ENISA, pasikonsultavusi su Komisija, ***valdomų saugumo paslaugų teikėjais ir, kai tinkama, su kitais kibernetinio saugumo pramonės atstovais***, parengia panašų aprašą, kad nustatytų trečiųjų valstybių, galinčių gauti paramą iš ES kibernetinio saugumo rezervo pagal 17 straipsnį, poreikius. Kai tikslinga, Komisija konsultuojasi su vyriausiuoju įgaliotiniu ***ir informuoja Tarybą apie trečiųjų valstybių poreikius***.

8. Komisijai ***pagal 20a straipsnį suteikiami įgaliojimai priimti deleguotuosius aktus, kuriais šis reglamentas papildomas nustatant*** ES kibernetinio saugumo rezervui reikalingų reagavimo paslaugų rūšis ir skaičių. ▌..

13 straipsnis

Prašymai suteikti paramą iš ES kibernetinio saugumo rezervo

1. 12 straipsnio 3 dalyje nurodyti naudotojai gali prašyti ES kibernetinio saugumo rezervo paslaugų, kad padėtų reaguoti į reikšmingus arba didelio masto kibernetinio saugumo incidentus ir nedelsiant po jų atkurti veiklą.

2. Kad gautų paramą iš ES kibernetinio saugumo rezervo, 12 straipsnio 3 dalyje nurodyti naudotojai imasi priemonių incidento, dėl kurio prašoma paramos, poveikiui sušvelninti, įskaitant tiesioginės techninės pagalbos ir kitų išteklių, skirtų padėti reaguoti į incidentą, teikimą ir pastangas nedelsiant atkurti veiklą.

3. Šio reglamento 12 straipsnio 3 dalies a punkte nurodytų naudotojų paramos prašymai Komisijai ir ENISA perduodami per valstybės narės pagal Direktyvos (ES) 2022/2555 8 straipsnio 3 dalį paskirtą arba įsteigtą bendrą kontaktinį punktą.

4. Valstybės narės informuoja CSIRT tinklą ir, kai tinkama, EU-CyCLONe apie savo prašymus suteikti reagavimo į incidentus ir nedelsiamo veiklos atkūrimo paramą pagal šį straipsnį.

5. Prašyme suteikti reagavimo į incidentus ir nedelsiamo veiklos atkūrimo paramą pateikiama:

a) tinkama informacija apie paveiktą subjektą ir galimą incidento poveikį bei planuojamą prašomos paramos panaudojimą, taip pat nurodant numatomus poreikius;

b) informacija apie priemones, kurių imtasi incidento, dėl kurio prašoma paramos, poveikiui sušvelninti, kaip nurodyta 2 dalyje;

c) informacija apie kitų formų paramą, kurią gali gauti paveiktas subjektas, įskaitant sutartinius susitarimus dėl reagavimo į incidentus ir nedelsiamo veiklos atkūrimo paslaugų, taip pat apie draudimo sutartis, kurios gali apimti tokio pobūdžio incidentus.

6. ENISA, bendradarbiaudama su Komisija ir TIS bendradarbiavimo grupe, parengia šabloną, kad būtų lengviau teikti prašymus suteikti paramą iš ES kibernetinio saugumo rezervo.

7. Komisijai ***pagal 20a straipsnį suteikiami įgaliojimai priimti deleguotuosius aktus,*** kuriais ***šis reglamentas papildomas*** išsamiau nustatant išsamią ES kibernetinio saugumo rezervo paramos paslaugų skyrimo tvarką. ▌

14 straipsnis

ES kibernetinio saugumo rezervo paramos įgyvendinimas

1. Prašymus suteikti paramą iš ES kibernetinio saugumo rezervo vertina Komisija, padedama ENISA arba kaip nustatyta susitarimuose dėl įnašų pagal 12 straipsnio 6 dalį, o atsakymas ***nepagrįstai*** nedelsiant ***ir bet kuriuo atveju per 24 valandas*** perduodamas 12 straipsnio 3 dalyje nurodytiems naudotojams.

2. Kai tuo pačiu metu gaunama daug prašymų, jų pirmenybė nustatoma, kai aktualu, atsižvelgiant į šiuos kriterijus:

a) kibernetinio saugumo incidento sunkumą;

b) paveikto subjekto rūšį, pirmenybę teikiant incidentams, darantiems poveikį esminiams subjektams, apibrėžtiems Direktyvos (ES) 2022/2555 3 straipsnio 1 dalyje;

c) galimą poveikį paveiktai valstybei narei (-ėms) ar naudotojams;

d) galimą tarpvalstybinį incidento ***mastą ir*** pobūdį ir išplitimo į kitas valstybes nares ar persidavimo kitiems naudotojams riziką;

e) priemones, kurių naudotojas ėmėsi siekdamas padėti reaguoti, ir nedelsiamo veiklos atkūrimo pastangas, nurodytas 13 straipsnio 2 dalyje ir 13 straipsnio 5 dalies b punkte.

3. ES kibernetinio saugumo rezervo paslaugos teikiamos pagal konkrečius paslaugų teikėjo ir naudotojo, kuriam teikiama parama iš ES kibernetinio saugumo rezervo, susitarimus. Į tuos susitarimus įtraukiamos atsakomybės sąlygos ***ir visos kitos nuostatos, kurios, susitarimo šalių nuomone, yra būtinos atitinkamai paslaugai teikti***.

4. 3 dalyje nurodyti susitarimai grindžiami šablonais, kuriuos parengė ENISA, pasikonsultavusi su valstybėmis narėmis ***ir prireikus su kitais ES kibernetinio saugumo rezervo naudotojais***.

5. Komisija ir ENISA neprisiima sutartinės atsakomybės už žalą, trečiosioms šalims padarytą dėl paslaugų, teikiamų įgyvendinant ES kibernetinio saugumo rezervą, ***išskyrus didelio aplaidumo vertinant paslaugų teikėjo paraišką atvejus arba tuo atveju, kai Komisija arba ENISA yra ES kibernetinio saugumo rezervo naudotojos pagal 14 straipsnio 3 dalį.***

6. Per vieną mėnesį nuo paramos veiksmo pabaigos naudotojai pateikia Komisijai, ENISA***, CSIRT tinklui ir, kai aktualu, EU-CyCLONe*** apibendrinamąją suteiktos paslaugos, pasiektų rezultatų ir įgytos patirties ataskaitą. Kai naudotojas yra iš trečiosios valstybės, kaip nurodyta 17 straipsnyje, tokia ataskaita dalijamasi su vyriausiuoju įgaliotiniu.
Ataskaitoje turi būti laikomasi Sąjungos ar nacionalinės teisės aktų dėl neskelbtinos ir įslaptintos informacijos apsaugos.

7. Komisija ***reguliariai ir bent du kartus per metus*** teikia TIS bendradarbiavimo grupei paramos panaudojimo ir rezultatų ataskaitas. ***Konfidenciali informacija joje apsaugoma pagal Sąjungos ir nacionalinę teisę dėl neskelbtinos ar įslaptintos informacijos apsaugos.***

15 straipsnis

Koordinavimas su krizių valdymo mechanizmais

1. Tais atvejais, kai reikšmingo arba didelio masto kibernetinio saugumo incidento priežastis arba pasekmė yra Sprendime 1313/2013/ES[1] apibrėžta nelaimė, reagavimo į tokius incidentus parama pagal šį reglamentą papildo pagal Sprendimą Nr. 1313/2013/ES vykdomus veiksmus ir nedaro poveikio jo taikymui.

2. Didelio masto tarpvalstybinio kibernetinio saugumo incidento, kai pradedamas taikyti integruoto politinio atsako į krizes mechanizmas (IPCR), atveju pagal šį reglamentą teikiama reagavimo į tokį incidentą parama valdoma pagal atitinkamus IPCR protokolus ir procedūras.

3. Konsultuojantis su vyriausiuoju įgaliotiniu, parama pagal reagavimo į kibernetinio saugumo krizes mechanizmą gali papildyti pagal bendrą užsienio ir saugumo politiką ir bendrą saugumo ir gynybos politiką teikiamą pagalbą, be kita ko, pasitelkiant greitojo reagavimo į kibernetines grėsmes grupes. Ji taip pat gali papildyti vienos valstybės narės kitai valstybei narei teikiamą pagalbą pagal Europos Sąjungos sutarties 42 straipsnio 7 dalį arba ja gali būti prisidedama prie tokios pagalbos.

4. Parama pagal reagavimo į kibernetinio saugumo krizes mechanizmą gali būti kaip bendro Sąjungos ir valstybių narių atsako Sutarties dėl Europos Sąjungos veikimo 222 straipsnyje nurodytose situacijose dalis.

16 straipsnis

Patikimi paslaugų teikėjai

1. Viešojo pirkimo procedūrose, vykdomose siekiant sukurti ES kibernetinio saugumo rezervą, perkančioji organizacija veikia laikydamasi Reglamente (ES, Euratomas) 2018/1046 nustatytų principų ir šių principų:

a) užtikrinti, kad į ES kibernetinio saugumo rezervą būtų įtrauktos paslaugos, kurios gali būti diegiamos visose valstybėse narėse, visų pirma atsižvelgiant į nacionalinius tokių paslaugų teikimo reikalavimus, įskaitant sertifikavimo ar akreditavimo reikalavimus;

b) užtikrinti esminių Sąjungos ir jos valstybių narių saugumo interesų apsaugą;

c) užtikrinti, kad ES kibernetinio saugumo rezervas duotų ES pridėtinę vertę – padėtų siekti Reglamento (ES) 2021/694 3 straipsnyje nustatytų tikslų, be kita ko, skatinant kibernetinio saugumo įgūdžių ugdymą ES, ***užtikrinant lyčių pusiausvyrą šiame sektoriuje ir stiprinant Sąjungos technologinį suverenumą, atvirą strateginį savarankiškumą, konkurencingumą ir atsparumą.***

2. Pirkdama ES kibernetinio saugumo rezervui skirtas paslaugas, perkančioji organizacija į pirkimo dokumentus įtraukia šiuos atrankos kriterijus:

a) paslaugų teikėjas įrodo, kad jo darbuotojams būdingas aukščiausio lygio profesinis sąžiningumas, nepriklausomumas, atsakomybė ir dalykinė kompetencija, kad galėtų vykdyti veiklą savo konkrečioje srityje, ir užtikrina ekspertinių žinių pastovumą ir (arba) tęstinumą, taip pat reikiamus techninius išteklius;

b) paslaugų teikėjas, jo patronuojamosios įmonės ir subrangovai turi įdiegtą su paslauga susijusios neskelbtinos informacijos, visų pirma įrodymų, išvadų ir ataskaitų, apsaugos

[1] 2013 m. gruodžio 17 d. Europos Parlamento ir Tarybos sprendimas Nr. 1313/2013/ES dėl Sąjungos civilinės saugos mechanizmo (OL L 347, 2013 12 20, p. 924).

sistemą ir laikosi Sąjungos saugumo taisyklių dėl ES įslaptintos informacijos apsaugos;

c) paslaugų teikėjas tinkamai įrodo, kad jo valdymo struktūra yra skaidri, dėl jos nekyla pavojus jo nešališkumui ir paslaugų kokybei ir negali kilti interesų konfliktų;

d) paslaugų teikėjas yra atlikęs tinkamą patikimumo patikrinimą, bent jau personalo, kurį ketina dislokuoti paslaugoms teikti;

e) paslaugų teikėjas užtikrina tinkamą savo IT sistemų saugumo lygį;

f) paslaugų teikėjas turi ***naujausią*** techninę ir programinę įrangą, kurios reikia prašomai paslaugai teikti***, ir, kai taikytina, atitinka Europos Parlamento ir Tarybos reglamentą (ES).../...[1] (2022/0272(COD))***;

g) paslaugų teikėjas geba įrodyti, kad turi panašių paslaugų teikimo atitinkamoms nacionalinėms valdžios institucijoms ar subjektams, veikiantiems ypatingos svarbos ar itin svarbiuose sektoriuose, patirties;

h) paslaugų teikėjas geba suteikti paslaugą per trumpą laikotarpį valstybėje narėje (-ėse), kurioje (-iose) jis gali teikti paslaugą;

i) paslaugų teikėjas geba teikti paslaugą valstybės narės (-ių), kurioje (-iose) jis gali teikti paslaugą, vietos kalba ***arba viena iš ES institucijų darbo kalbų***;

j) kai pagal Reglamentą (ES) 2019/881 bus įdiegta valdomų saugumo paslaugų ***Europos kibernetinio saugumo*** sertifikavimo sistema, paslaugų teikėjas turės būti sertifikuotas pagal tą sistemą ***per dvejus metus nuo tos sistemos patvirtinimo***;

ja) paslaugų teikėjas turi galėti teikti paslaugą atskirai, o ne kaip paketo dalį, taip užtikrindamas naudotojui galimybę pasirinkti kitą paslaugų teikėją;

jb) 12 straipsnio 1 dalies tikslais paslaugų teikėjas į konkurso pasiūlymą įtraukia galimybę nepanaudotas reagavimo į incidentus paslaugas pakeisti pratybomis ar mokymais;

jc) paslaugų teikėjas turi būti įsisteigęs ir turėti vykdomojo valdymo struktūras Sąjungoje, asocijuotojoje šalyje arba trečiojoje šalyje, kuri yra Pasaulio prekybos organizacijos sudaromos Sutarties dėl viešųjų pirkimų šalis;

jd) paslaugų teikėjas negali būti kontroliuojamas neasocijuotosios trečiosios šalies ar neasocijuotosios trečiosios šalies subjekto, kuris nėra Sutarties dėl viešųjų pirkimų šalis, arba kaip alternatyva tokio subjekto atžvilgiu turi būti atliktas tikrinimas, kaip tai suprantama Reglamente (ES) 2019/452, ir prireikus taikomos švelninimo priemonės, atsižvelgiant į šio reglamento tikslus.

17 straipsnis

Parama trečiosioms valstybėms

[1] … m. … … d. Europos Parlamento ir Tarybos reglamentas (ES) .../... dėl ... (OL L ..., ..., ELI: ...).

1. Trečiosios valstybės gali prašyti paramos iš ES kibernetinio saugumo rezervo, jei tai numatyta sudarytuose asociacijos susitarimuose dėl jų dalyvavimo Skaitmeninės Europos programoje.

2. Parama iš ES kibernetinio saugumo rezervo teikiama pagal šį reglamentą ir visas 1 dalyje nurodytuose asociacijos susitarimuose nustatytas specialiąsias sąlygas.

3. Naudotojai iš asocijuotųjų trečiųjų valstybių, turintys teisę gauti paslaugas iš ES kibernetinio saugumo rezervo, apima kompetentingas institucijas, tokias kaip CSIRT ir kibernetinių krizių valdymo institucijas.

4. Kiekviena trečioji valstybė, atitinkanti paramos iš ES kibernetinio saugumo rezervo reikalavimus, paskiria instituciją, kuri šio reglamento tikslais veikia kaip vienas bendras kontaktinis punktas.

5. Prieš gaudamos paramą iš ES kibernetinio saugumo rezervo, trečiosios valstybės pateikia Komisijai ir vyriausiajam įgaliotiniui informaciją apie savo kibernetinį atsparumą ir rizikos valdymo pajėgumus, įskaitant bent informaciją apie nacionalines priemones, kurių imtasi siekiant pasirengti reikšmingiems ar didelio masto kibernetinio saugumo incidentams, taip pat informaciją apie atsakingus nacionalinius subjektus, įskaitant CSIRT arba lygiaverčius subjektus, jų pajėgumus ir jiems skirtus išteklius. Kai šio reglamento 13 ir 14 straipsnių nuostatose daroma nuoroda į valstybes nares, jos taikomos trečiosioms valstybėms, nurodytoms 1 dalyje.

6. Komisija gautų trečiųjų valstybių prašymų ir joms iš ES kibernetinio saugumo rezervo skirtos paramos įgyvendinimo klausimus ***nedelsdama praneša Tarybai ir*** koordinuoja su vyriausiuoju įgaliotiniu.

IV skyrius

KIBERNETINIO SAUGUMO INCIDENTŲ PERŽIŪROS MECHANIZMAS

18 straipsnis

Kibernetinio saugumo incidentų peržiūros mechanizmas

1. Komisijos, EU-CyCLONe arba CSIRT tinklo prašymu ENISA peržiūri ir įvertina su konkrečiu reikšmingu arba didelio masto kibernetinio saugumo incidentu susijusias grėsmes, pažeidžiamumus ir poveikio švelninimo veiksmus. Užbaigusi incidento peržiūrą ir vertinimą, ENISA pateikia incidento peržiūros ataskaitą CSIRT tinklui, EU-CyCLONe ir Komisijai, kad padėtų joms atlikti savo užduotis, visų pirma užduotis, nustatytas Direktyvos (ES) 2022/2555 15 ir 16 straipsniuose. Kai aktualu, Komisija ataskaita dalijasi su vyriausiuoju įgaliotiniu.

2. Rengdama 1 dalyje nurodytą incidento peržiūros ataskaitą, ENISA bendradarbiauja su visais atitinkamais suinteresuotaisiais subjektais, įskaitant valstybių narių, Komisijos, kitų atitinkamų ES institucijų, įstaigų, ***tarnybų*** ir agentūrų, ***nacionalinių ir tarpvalstybinių SOC*** valdomų saugumo paslaugų teikėjų ir kibernetinio saugumo paslaugų naudotojų atstovus, ***ir iš jų surenka grįžtamąją informaciją, kartu teikdama garantijas ir vykdydama stebėseną, kuri yra tinkama siekiant užtikrinti, kad kibernetinio saugumo paslaugų sektoriaus subjektai remtųsi įgyta patirtimi ir nustatytais geriausios praktikos pavyzdžiais.*** 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 apie bet kokį galimą interesų konfliktą.

3. Ataskaitoje pateikiama konkretaus reikšmingo arba didelio masto kibernetinio saugumo incidento apžvalga ir analizė, apimanti pagrindines priežastis, pažeidžiamumus ir įgytą patirtį. Konfidenciali informacija joje apsaugoma pagal Sąjungos ar nacionalinę teisę dėl neskelbtinos ar įslaptintos informacijos apsaugos. ***Jame nepateikiama jokios informacijos apie aktyviai išnaudojamus pažeidžiamumus, kurie lieka nepašalinti.***

3a. Šio straipsnio 1 dalyje nurodytoje ataskaitoje pateikiama patirtis, įgyta atlikus tarpusavio vertinimus pagal Direktyvos (ES) 2022/2555 1 straipsnį.

4. Kai tinkama, ataskaitoje pateikiamos rekomendacijos, ***be kita ko, skirtos visiems atitinkamiems suinteresuotiesiems subjektams,*** kaip pagerinti Sąjungos kibernetinio saugumo būklę.

5. Jei įmanoma, ataskaitos versija skelbiama viešai. Šioje versijoje pateikiama tik vieša informacija.

V skyrius

BAIGIAMOSIOS NUOSTATOS

19 straipsnis

Reglamento (ES) 2021/694 pakeitimai

Reglamentas (ES) 2021/694 iš dalies keičiamas taip:

1) 6 straipsnis iš dalies keičiamas taip:

a) 1 dalis iš dalies keičiama taip:

i) įterpiamas aa punktas:

„aa) remti ES kibernetinio saugumo skydo plėtojimą, įskaitant nacionalinių ir tarpvalstybinių SOC platformų, kurios padeda didinti informuotumą apie padėtį Sąjungoje ir stiprinti Sąjungos kibernetinių grėsmių žvalgybos pajėgumus, kūrimą, diegimą ir veikimą;“;

ii) pridedamas g punktas:

„g) sukurti ir valdyti reagavimo į kibernetinio saugumo krizes mechanizmą, skirtą padėti valstybėms narėms pasirengti reikšmingiems kibernetinio saugumo incidentams ir į juos reaguoti, papildant nacionalinius išteklius bei pajėgumus ir kitų formų Sąjungos lygmeniu teikiamą paramą, įskaitant ES kibernetinio saugumo rezervo sukūrimą.“;

b) 2 dalis pakeičiama taip:

„2. Veiksmai pagal 3 konkretų tikslą įgyvendinami visų pirma per Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centrą ir Nacionalinių koordinavimo centrų tinklą, vadovaujantis Europos Parlamento ir Tarybos reglamentu (ES) 2021/887*, išskyrus ES kibernetinio saugumo rezervo įgyvendinimo veiksmus, kuriuos įgyvendina Komisija ir ENISA.

_____

* 2021 m. gegužės 20 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/887, kuriuo įsteigiamas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras ir Nacionalinių koordinavimo centrų tinklas (OL L 202, 2021 6 8, p. 1–31).***ELI: http://data.europa.eu/eli/reg/2021/887/oj.“;***

2) 9 straipsnis iš dalies keičiamas taip:

a) 2 dalies b, c ir d punktai pakeičiami taip:

„b) 1 776 956 000 EUR skiriama 2 konkrečiam tikslui „Dirbtinis intelektas“;

c) ***1 620 566 000*** EUR skiriama 3 konkrečiam tikslui „Kibernetinis saugumas ir pasitikėjimas“;

d) ***500 347 000*** EUR skiriama 4 konkrečiam tikslui „Aukšto lygio skaitmeniniai įgūdžiai“;“;

aa) įterpiama nauja 2a dalis:

„2a). 2 dalies c punkte nurodyta suma visų pirma naudojama Programos 6 straipsnio 1 dalies a–f punktuose nurodytiems veiklos tikslams pasiekti.“;

ab) įterpiama nauja 2b dalis:

„2b). ES kibernetinio saugumo rezervo sukūrimui ir įgyvendinimui skiriama suma neviršija 27 mln. EUR numatomai reglamento galiojimo trukmei, kuriuo nustatomos solidarumo stiprinimo ir pajėgumo aptikti kibernetinio saugumo grėsmes ir incidentus Sąjungoje, jiems pasirengti ir į juos reaguoti didinimo priemonės.“;

b) pridedama 8 dalis:

„8. Nukrypstant nuo Reglamento (ES, Euratomas) 2018/1046 12 straipsnio 4 dalies, nepanaudoti įsipareigojimų ir mokėjimų asignavimai, skirti veiksmams***, susijusiems su ES kibernetinio saugumo rezervo įgyvendinimu***, kuriais siekiama šio reglamento 6 straipsnio 1 dalies g punkte nustatytų tikslų, perkeliami automatiškai ir gali būti paskirti ir išmokėti iki kitų finansinių metų gruodžio 31 d.“;

Komisija informuoja Parlamentą ir Tarybą apie asignavimus, perkeltus pagal Reglamento (ES, Euratomas) 2018/1046 12 straipsnio 6 dalį.

3) 14 straipsnio 2 dalis pakeičiama taip:

„2. Pagal Programą gali būti teikiamas bet kurios ***Reglamente (ES, Euratomas) 2018/1046*** nustatytos formos finansavimas, visų pirma įskaitant viešuosius pirkimus kaip pagrindinę formą arba dotacijas ir apdovanojimus.

Kai veiksmo tikslui pasiekti reikalingi novatoriškų prekių ir paslaugų viešieji pirkimai, dotacijos skiriamos tik tiems naudos gavėjams, kurie yra perkančiosios organizacijos arba perkantieji subjektai, apibrėžti Europos Parlamento ir Tarybos direktyvose 2014/24/ES27[27] ir 2014/25/ES28[28] .

Kai veiksmo tikslams pasiekti būtinas novatoriškų dideliu mastu komercinėmis sąlygomis dar neprieinamų prekių tiekimas ar paslaugų teikimas, perkančioji organizacija arba perkantysis subjektas gali leisti skirti kelias sutartis tos pačios viešųjų pirkimų procedūros metu.

Perkančioji organizacija arba perkantysis subjektas dėl tinkamai pagrįstų saugumo priežasčių gali reikalauti, kad sutarties vykdymo vieta būtų Sąjungos teritorijoje.

Įgyvendindamos Reglamento (ES) 2023/**...** 12 straipsniu įsteigtam ES kibernetinio saugumo rezervui skirtas viešųjų pirkimų procedūras, Komisija ir ENISA gali veikti kaip centrinė perkančioji organizacija, perkanti 10 straipsnio reikalavimus atitinkančioms Programos asocijuotosioms trečiosioms valstybėms arba jų vardu. Komisija ir ENISA gali veikti ir kaip didmenininkės, perkančios, sandėliuojančios ir perparduodančios arba dovanojančios prekes ir paslaugas, taip pat jas nuomojančios toms trečiosioms valstybėms. Nukrypstant nuo Reglamento (ES) **.../...** 169 straipsnio 3 dalies, pavienės trečiosios valstybės prašymo pakanka, kad Komisija arba ENISA būtų įgaliota imtis veiksmų.

Įgyvendindamos Reglamento (ES) 2023/**...** 12 straipsniu įsteigtam ES kibernetinio saugumo rezervui skirtas viešųjų pirkimų procedūras, Komisija ir ENISA gali veikti kaip centrinė perkančioji organizacija, perkanti Sąjungos institucijoms, įstaigoms ir agentūroms arba jų vardu. Komisija ir ENISA gali veikti ir kaip didmenininkės, perkančios, sandėliuojančios ir perparduodančios arba dovanojančios prekes ir paslaugas, taip pat jas nuomojančios Sąjungos institucijoms, įstaigoms ir agentūroms. Nukrypstant nuo Reglamento (ES) **.../...** 169 straipsnio 3 dalies, pavienės Sąjungos institucijos, įstaigos ar agentūros prašymo pakanka, kad Komisija arba ENISA būtų įgaliota imtis veiksmų.

Pagal Programą finansavimas gali būti teikiamas ir finansinėmis priemonėmis, naudojant derinimo operacijas. “;

4) pridedamas 16a straipsnis:

„***16a straipsnis***

Veiksmų, kuriais įgyvendinamas Reglamento (ES) 2023/**...** 3 straipsniu sukurtas Europos kibernetinio saugumo skydas, atveju taikomos Reglamento (ES) 2023/**...** 4 ir 5 straipsniuose nustatytos taisyklės. Jei šio reglamento nuostatos prieštarauja Reglamento (ES) 2023/**...** 4 ir

5 straipsniams, pirmenybė teikiama pastarajam reglamentui ir jis taikomas tiems konkretiems veiksmams.“;

5) 19 straipsnis pakeičiamas taip:

„Programos dotacijos skiriamos ir valdomos pagal ***Reglamento (ES, Euratomas) 2018/1046*** VIII antraštinę dalį ir jomis galima padengti iki 100 proc. tinkamų finansuoti išlaidų, nedarant poveikio bendro finansavimo principui, nustatytam ***Reglamento (ES, Euratomas) 2018/1046*** 190 straipsnyje. Tokios dotacijos skiriamos ir valdomos kaip nurodyta kiekvieno konkretaus tikslo atveju.

Pagal ***Reglamento (ES, Euratomas) 2018/1046*** 195 straipsnio 1 dalies d punktą paramą dotacijų forma Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras (ECCC) gali tiesiogiai skirti Reglamento ***(ES) .../...*** 4 straipsnyje nurodytiems nacionaliniams saugumo operacijų centrams ir Reglamento ***(ES) .../...*** 5 straipsnyje nurodytam prieglobos konsorciumui, neskelbdamas kvietimo teikti pasiūlymus.

Pagal ***Reglamento (ES, Euratomas) 2018/1046*** 195 straipsnio 1 dalies d punktą ECCC valstybėms narėms gali tiesiogiai skirti Reglamento ***(ES) .../...*** 10 straipsnyje nustatytą reagavimo į kibernetinio saugumo krizes mechanizmo paramą dotacijų forma, neskelbdamas kvietimo teikti pasiūlymus.

Reglamento ***(ES) .../...*** 10 straipsnio 1 dalies c punkte nurodytų veiksmų atveju ECCC informuoja Komisiją ir ENISA apie valstybių narių prašymus skirti tiesiogines dotacijas neskelbiant kvietimo teikti pasiūlymus.

Teikiant savitarpio pagalbą reaguojant į reikšmingą arba didelio masto kibernetinio saugumo incidentą, kaip apibrėžta Reglamento ***(ES) .../...*** 10 straipsnio c punkte, ir pagal ***Reglamento (ES, Euratomas) 2018/1046*** 193 straipsnio 2 dalies antros pastraipos a punktą tinkamai pagrįstais atvejais išlaidos gali būti laikomos tinkamomis finansuoti, net jei jos buvo patirtos prieš pateikiant dotacijos paraišką.“;

6) Reglamento (ES) 2021/694 I ir II priedai iš dalies keičiami pagal šio reglamento priedą.

19a straipsnis
Papildomi ištekliai ENISA

ENISA skiriama papildomų išteklių šiame reglamente patikėtoms papildomoms užduotims vykdyti. Papildoma parama, įskaitant finansavimą, neturi trukdyti siekti kitų Sąjungos programų, visų pirma Skaitmeninės Europos programos, tikslų.

20 straipsnis

Vertinimas ***ir peržiūra***

1. Iki [***dveji*** metai nuo šio reglamento taikymo pradžios dienos] ***ir vėliau kas dvejus metus*** Komisija ***atlieka šiame reglamente nustatytų priemonių veikimo vertinimą ir pateikia*** Europos Parlamentui ir Tarybai ataskaitą.

2. Atliekant vertinimą visų pirma įvertinama:

a) tarpvalstybinių SOC naudojimas ir pridėtinė vertė, taip pat tai, kokiu mastu jie padeda greičiau nustatyti kibernetines grėsmes ir į jas reaguoti bei informuoti apie padėtį; aktyvus nacionalinių SOC dalyvavimas Europos kibernetinio saugumo skydo veikloje, įskaitant įsteigtų nacionalinių SOC ir tarpvalstybinių SOC skaičių ir tai, kokiu mastu jie prisidėjo prie kokybiškos operatyvinės informacijos ir žvalgybinės informacijos apie kibernetines grėsmes rengimo ir keitimosi ja; bendrai įsigytų kibernetinės infrastruktūros objektų arba priemonių ar tiek objektų, tiek priemonių, skaičius ir išlaidos; tarpvalstybinių SOC ir su pramonės ISAC sudarytų bendradarbiavimo susitarimų skaičius; incidentų, apie kuriuos pranešta CSIRT tinklui, skaičius ir poveikis CSIRT tinklo darbui;

b) teigiamas ir neigiamas kibernetinio saugumo ekstremaliųjų situacijų mechanizmo veikimas, taip pat ar reikalingi papildomi bendradarbiavimo ar mokymo reikalavimai;

c) šio reglamento indėlis stiprinant Sąjungos atsparumą ir atvirą strateginį suverenumą, didinant atitinkamų pramonės sektorių, labai mažų įmonių, MVĮ, įskaitant startuolius, konkurencingumą ir kibernetinio saugumo įgūdžių ugdymą Sąjungoje;

d) ES kibernetinio saugumo rezervo naudojimas ir pridėtinė vertė, įskaitant patikimų saugumo paslaugų teikėjų skaičių, kurie yra ES kibernetinio saugumo rezervo dalis; veiksmų, kuriais remiamas reagavimas į kibernetinio saugumo incidentus, skaičius, rūšis, išlaidos ir poveikis, taip pat jų naudotojai ir teikėjai; vidutinis laikas, per kurį Komisija turi pripažinti incidentą, pasitelkti ES kibernetinio saugumo rezervą ir reaguoti, o naudotojas – atsigauti po incidento; ar ES kibernetinio saugumo rezervo taikymo sritis turėtų būti išplėsta įtraukiant pasirengimo incidentams paslaugas ar bendras pratybas su patikimais valdomų saugumo paslaugų teikėjais ir potencialiais ES kibernetinio saugumo rezervo naudotojais, kad prireikus būtų užtikrintas veiksmingas ES kibernetinio saugumo rezervo veikimas;

e) šio reglamento indėlis plėtojant ir gerinant kibernetinio saugumo sektoriaus darbuotojų įgūdžius ir kompetencijas, kurių reikia siekiant stiprinti Sąjungos gebėjimą nustatyti kibernetinio saugumo grėsmes ir incidentus, užkirsti jiems kelią, į juos reaguoti ir po jų atsigauti;

f) šio reglamento indėlis diegiant ir plėtojant pažangiausias technologijas Sąjungoje.

3. Remdamasi 1 dalyje nurodyta ataskaita, Komisija, kai tikslinga, Europos Parlamentui ir Tarybai pateikia pasiūlymą dėl teisėkūros procedūra priimamo akto dėl šio reglamento dalinio keitimo.

20a straipsnis

Įgaliojimų delegavimas

1. Įgaliojimai priimti deleguotuosius aktus Komisijai suteikiami šiame straipsnyje nustatytomis sąlygomis.

2. 6 straipsnio 3 dalyje, 7 straipsnio 2 dalyje, 12 straipsnio 8 dalyje ir 13 straipsnio 7 dalyje nurodyti įgaliojimai priimti deleguotuosius aktus Komisijai suteikiami ... metams nuo ... [pagrindinio teisės akto įsigaliojimo data arba bet kuri kita teisėkūros institucijų nustatyta data]. Likus ne mažiau kaip devyniems mėnesiams iki ... metų laikotarpio pabaigos Komisija parengia naudojimosi deleguotaisiais įgaliojimais ataskaitą. Deleguotieji įgaliojimai savaime pratęsiami tokios pačios trukmės laikotarpiams, išskyrus atvejus, kai Europos Parlamentas arba Taryba pareiškia prieštaravimų dėl tokio pratęsimo likus ne mažiau kaip trims mėnesiams iki kiekvieno laikotarpio pabaigos.

3. Europos Parlamentas arba Taryba gali bet kada atšaukti 6 straipsnio 3 dalyje, 7 straipsnio 2 dalyje, 12 straipsnio 8 dalyje ir 13 straipsnio 7 dalyje nurodytus deleguotuosius įgaliojimus. Sprendimu dėl įgaliojimų atšaukimo nutraukiami tame sprendime nurodyti įgaliojimai priimti deleguotuosius aktus. Sprendimas įsigalioja kitą dieną po jo paskelbimo Europos Sąjungos oficialiajame leidinyje arba vėlesnę jame nurodytą dieną. Jis nedaro poveikio jau galiojančių deleguotųjų aktų galiojimui.

4. Prieš priimdama deleguotąjį aktą Komisija konsultuojasi su kiekvienos valstybės narės paskirtais ekspertais vadovaudamasi 2016 m. balandžio 13 d. Tarpinstituciniame susitarime dėl geresnės teisėkūros nustatytais principais.

5. Apie priimtą deleguotąjį aktą Komisija nedelsdama vienu metu praneša Europos Parlamentui ir Tarybai.

6. Pagal 6 straipsnio 3 dalį, 7 straipsnio 2 dalį, 12 straipsnio 8 dalį ar 13 straipsnio 7 dalį priimtas deleguotasis aktas įsigalioja tik tuo atveju, jeigu per du mėnesius nuo pranešimo Europos Parlamentui ir Tarybai apie šį aktą dienos nei Europos Parlamentas, nei Taryba nepareiškia prieštaravimų arba jeigu dar nepasibaigus šiam laikotarpiui ir Europos Parlamentas, ir Taryba praneša Komisijai, kad prieštaravimų nereikš. Europos Parlamento arba Tarybos iniciatyva šis laikotarpis pratęsiamas [dviem mėnesiais].

21 straipsnis

Komiteto procedūra

1. Komisijai padeda Skaitmeninės Europos programos koordinavimo komitetas, įsteigtas Reglamentu (ES) 2021/694. Tas komitetas – tai komitetas, kaip nustatyta Reglamente (ES) Nr. 182/2011.
2. Kai daroma nuoroda į šią dalį, taikomas Reglamento (ES) Nr. 182/2011 5 straipsnis.

22 straipsnis

Įsigaliojimas

Šis reglamentas įsigalioja dvidešimtą dieną po jo paskelbimo Europos Sąjungos oficialiajame leidinyje.

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Strasbūre

Europos Parlamento vardu	*Tarybos vardu*
Pirmininkas / Pirmininkė	*Pirmininkas / Pirmininkė*

PRIEDAS

Reglamentas (ES) 2021/694 iš dalies keičiamas taip:

(1) I priedo skirsnis / skyrius „3 konkretus tikslas: „Kibernetinis saugumas ir pasitikėjimas“ pakeičiamas taip:

„3 konkretus tikslas „Kibernetinis saugumas ir pasitikėjimas

Programa skatinamas pagrindinių pajėgumų apsaugoti Sąjungos skaitmeninę ekonomiką, visuomenę ir demokratiją stiprinimas, kūrimas ir įgijimas, stiprinant Sąjungos kibernetinio saugumo sektoriaus potencialą ir konkurencingumą, taip pat didinant tiek privačiojo, tiek viešojo sektorių pajėgumą apsaugoti piliečius ir įmones nuo kibernetinių grėsmių, įskaitant Direktyvos (ES) 2016/1148 įgyvendinimo rėmimą.

Pagal šį tikslą pradiniai ir prireikus tolesni veiksmai apima:

1. Bendrą investavimą su valstybėmis narėmis į pažangią kibernetinio saugumo įrangą, infrastruktūrą ir praktinę patirtį, kurios yra būtinos siekiant apsaugoti ypatingos svarbos infrastruktūros objektus ir bendrąją skaitmeninę rinką apskritai. Toks bendras investavimas galėtų apimti investicijas į kvantinės infrastruktūros objektus ir kibernetinio saugumo, informuotumo apie padėtį kibernetinėje erdvėje duomenų išteklius, įskaitant nacionalinius saugumo operacijų centrus ir tarpvalstybinius saugumo operacijų centrus, sudarančius Europos kibernetinio saugumo skydą, taip pat kitas viešajam ar privačiajam sektoriui skirtas priemones visoje Europoje.

2. Esamo technologinio pajėgumo išplėtimą ir kompetencijos centrų valstybėse narėse sujungimą į tinklą, taip pat užtikrinimą, kad tie pajėgumai atitiktų viešojo sektoriaus ir pramonės poreikius, įskaitant poreikius, susijusius su produktais ir paslaugomis, kuriais stiprinamas kibernetinis saugumas ir pasitikėjimas bendrojoje skaitmeninėje rinkoje.

3. Užtikrinimą, kad visose valstybėse narėse būtų plačiai diegiami veiksmingi pažangiausi kibernetinio saugumo ir pasitikėjimo sprendimai. Toks diegimas apima produktų saugumo ir saugos stiprinimą nuo jų kūrimo iki jų komercializacijos.

4. Paramą kibernetinio saugumo įgūdžių spragoms šalinti, ***ypatingą dėmesį skiriant lyčių pusiausvyros sektoriuje užtikrinimui,*** pavyzdžiui, suderinant kibernetinio saugumo įgūdžių programas, pritaikant jas prie konkrečių sektorių poreikių***, įskaitant tarpdisciplininį ir bendrąjį požiūrį,*** ir palengvinant galimybes dalyvauti tiksliniuose specializuotuose mokymuose***, sudarant sąlygas visiems asmenims ir teritorijoms, nedarant poveikio galimybei pasinaudoti šiame reglamente numatytomis galimybėmis.***

5. Valstybių narių solidarumo rengiantis dideliems kibernetinio saugumo incidentams ir į juos reaguojant skatinimą, tarpvalstybiniu mastu diegiant kibernetinio saugumo paslaugas, įskaitant paramą valdžios institucijų savitarpio pagalbai ir patikimų ***valdomų saugumo paslaugų*** teikėjų rezervo sukūrimą Sąjungos lygmeniu.“;

(2) II priedo skirsnis / skyrius „3 konkretus tikslas: „Kibernetinis saugumas ir pasitikėjimas“ pakeičiamas taip:

„3 konkretus tikslas „Kibernetinis saugumas ir pasitikėjimas

3.1. Bendrai įsigytų kibernetinės infrastruktūros objektų arba priemonių ar tiek objektų, tiek priemonių ***kaip kibernetinio saugumo skydo dalies***, skaičius.
3.2. Naudotojų ir jų bendruomenių, kurie gauna prieigą prie Europos kibernetinio saugumo įrenginių, skaičius.
3.3. Veiksmų, kuriais ***buvo*** remiamas pasirengimas kibernetinio saugumo incidentams ir reagavimas į juos pagal reagavimo į kibernetinio saugumo krizes mechanizmą***, skaičius, rūšis, išlaidos ir poveikis***. ***Kokiu mastu naudotojas įgyvendino ir vykdė parengties testavimo rekomendacijas, taip pat vidutinį laiką, per kurį Komisija pripažįsta incidentą, reaguojama aktyvuojant ES kibernetinio saugumo rezervą ir naudotojai atsigauna po incidentų.“***