Europos Sąjungos
Taryba

Briuselis, 2022 m. kovo 22 d.
(OR. en)

7474/22

Tarpinstitucinė byla:
2022/0085 (COD)

CYBER 93
TELECOM 116
JAI 383
INST 89
INF 32
CSC 119
CSCI 39
DATAPROTECT 81
FIN 353
BUDGET 2
CODEC 349
IA 30

PASIŪLYMAS

nuo:	Europos Komisijos generalinės sekretorės, kurios vardu pasirašo direktorė Martine DEPREZ
gavimo data:	2022 m. kovo 22 d.
kam:	Europos Sąjungos Tarybos generaliniam sekretoriui Jeppe TRANHOLMUI-MIKKELSENUI
Komisijos dok. Nr.:	COM(2022) 122 final
Dalykas:	Pasiūlymas dėl EUROPOS PARLAMENTO IR TARYBOS REGLAMENTO, kuriuo nustatomos priemonės aukštam bendram kibernetinio saugumo lygiui Sąjungos institucijose, įstaigose, organuose ir agentūrose užtikrinti

Delegacijoms pridedamas dokumentas COM(2022) 122 final.

Pridedama: COM(2022) 122 final

EUROPOS
KOMISIJA

Briuselis, 2022 03 22
COM(2022) 122 final

2022/0085 (COD)

Pasiūlymas

EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS

kuriuo nustatomos priemonės aukštam bendram kibernetinio saugumo lygiui Sąjungos institucijose, įstaigose, organuose ir agentūrose užtikrinti

{SWD(2022) 67 final} - {SWD(2022) 68 final}

AIŠKINAMASIS MEMORANDUMAS

1. PASIŪLYMO APLINKYBĖS

• Pasiūlymo pagrindimas ir tikslai

Šiuo pasiūlymu nustatoma sistema, kuria užtikrinamos bendros Sąjungos institucijų, įstaigų ir agentūrų kibernetinio saugumo taisyklės ir priemonės. Juo siekiama toliau didinti visų subjektų atsparumą ir reagavimo į incidentus pajėgumus. Jis atitinka Komisijos prioritetus užtikrinti, kad Europa prisitaikytų prie skaitmeninio amžiaus, ir kurti perspektyvią žmonėms tarnaujančią ekonomiką. Be to, saugaus ir atsparaus viešojo administravimo užtikrinimas yra skaitmeninės visos visuomenės pertvarkos kertinis akmuo.

Šis pasiūlymas grindžiamas ES saugumo sąjungos strategija (COM(2020) 605 *final*) ir ES skaitmeninio dešimtmečio kibernetinio saugumo strategija (JOIN(2020) 18 *final*).

Pasiūlymu modernizuojama esama CERT-EU teisinė sistema ir atsižvelgiama į pastaraisiais metais pasikeitusią ir aktyvesnę institucijų, įstaigų ir agentūrų skaitmenizaciją, taip pat į kintančią grėsmių kibernetiniam saugumui padėtį. Nuo COVID-19 krizės pradžios abu pokyčiai tapo dar labiau akivaizdūs, o incidentų skaičius toliau didėja ir iš įvairių šaltinių vykdomi išpuoliai tampa vis sudėtingesni.

Pasiūlymu CERT-EU iš Sąjungos institucijų, įstaigų ir agentūrų kompiuterinių incidentų tyrimo tarnybos pervadinama į Kibernetinio saugumo centrą, atsižvelgiant į pokyčius valstybėse narėse ir visame pasaulyje, kur daugelis CERT pervadintos kibernetinio saugumo centrais, tačiau dėl pavadinimo atpažinimo paliekamas trumpasis pavadinimas „CERT-EU“.

• Suderinamumas su toje pačioje politikos srityje galiojančiomis nuostatomis

Šiuo pasiūlymu siekiama didinti Sąjungos institucijų, įstaigų ir agentūrų kibernetinį atsparumą kibernetinėms grėsmėms, kartu suderinant jį su galiojančiais teisės aktais:

- Direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti. Jis taip pat dera su pasiūlymu dėl Direktyvos (ES) XXXX/XXXX dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria panaikinama Direktyva (ES) 2016/1148 (pasiūlymas dėl TIS 2];

- Reglamentu (EB) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo (Kibernetinio saugumo aktas);

- pasiūlymu dėl Reglamento (ES) XXXX/XXXX dėl Sąjungos institucijų, įstaigų, organų ir agentūrų informacijos saugumo;

- 2021 m. birželio 23 d. Komisijos rekomendacija dėl Jungtinio kibernetinio saugumo padalinio sukūrimo;

- 2017 m. rugsėjo 13 d. Komisijos rekomendacija (ES) 2017/1584 dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes.

2017 m. rugsėjo 13 d. Komisijos rekomendacijos (ES) 2017/1584 dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes priede pateiktas Koordinuoto atsako į didelio masto tarpvalstybinius kibernetinio saugumo incidentus ir krizes projektas.

2021 m. kovo 9 d. rezoliucijoje Europos Sąjungos Taryba pabrėžė, kad kibernetinis saugumas yra gyvybiškai svarbus viešojo administravimo veikimui tiek nacionaliniu, tiek ES lygmeniu, taip pat visai visuomenei ir ekonomikai, akcentuodama tvirtos ir nuoseklios saugumo sistemos svarbą siekiant apsaugoti visą ES personalą, duomenis, ryšių tinklus, informacines sistemas ir sprendimų priėmimo procesus. Visų pirma tai turi būti pasiekta didinant Sąjungos institucijų, įstaigų ir agentūrų atsparumą ir gerinant jų saugumo kultūrą. Turi būti skirta pakankamai išteklių ir pajėgumų, be kita ko, stiprinant CERT-EU įgaliojimus.

2. TEISINIS PAGRINDAS, SUBSIDIARUMO IR PROPORCINGUMO PRINCIPAI

• Teisinis pagrindas

Šio reglamento teisinis pagrindas yra Sutarties dėl Europos Sąjungos veikimo (SESV) 298 straipsnis, kuriame numatyta, kad Sąjungos institucijos, įstaigos, organai ir agentūros, vykdydami savo užduotis, remiasi atvira, veiksminga ir nepriklausoma Europos administracija. Vadovaudamiesi pagal 336 straipsnį priimtais Tarnybos nuostatais ir įdarbinimo sąlygomis, Europos Parlamentas ir Taryba tuo tikslu patvirtina nuostatas, priimdami reglamentus pagal įprastą teisėkūros procedūrą.

Informacinės technologijos suteikė naujų būdų Sąjungos institucijoms, įstaigoms ir agentūroms dirbti, bendrauti su piliečiais ir gerinti bendrą veiklą. Technologijos toliau vystosi, todėl kartu su jomis kinta ir kibernetinių grėsmių padėtis. Sąjungos institucijos, įstaigos ir agentūros tapo labai patraukliais sudėtingų kibernetinių išpuolių taikiniais. Nustatant kibernetinio saugumo užtikrinimo sistemą ir reikalavimus, regis, prisidedama prie Europos administracijos veiksmingumo ir nepriklausomumo, kad Sąjungos institucijos, įstaigos, organai ir agentūros, vykdydami savo užduotis, galėtų efektyviau veikti skaitmeniniame pasaulyje.

Be to, kaip paaiškinta 3 skirsnyje, dabartiniai Sąjungos institucijų, įstaigų ir agentūrų kibernetinio saugumo būklės ir požiūrio kibernetinio saugumo srityje skirtumai yra dar viena kliūtis atvirai, veiksmingai ir nepriklausomai Europos administracijai. Jei nebūtų bendro požiūrio, Sąjungos institucijų, įstaigų ir agentūrų kibernetinio saugumo būklė toliau plėtotųsi skirtingomis kryptimis. Todėl šis teisinis pagrindas yra tinkamas, nes reglamentu siekiama sukurti Sąjungos institucijoms, įstaigoms, organams ir agentūroms skirtą bendrą kibernetinio saugumo teisinę sistemą.

• Subsidiarumo principas

Reglamentas, kuriuo nustatomos priemonės aukštam bendram kibernetinio saugumo lygiui visose Sąjungos institucijose, įstaigose, organuose ir agentūrose užtikrinti, priklauso išimtinei Sąjungos kompetencijai.

- **Proporcingumo principas**

Šiame reglamente siūlomomis taisyklėmis neviršijama to, kas būtina konkretiems tikslams tinkamai pasiekti. Numatytos priemonės padės pasiekti aukštą bendrą kibernetinio saugumo lygį neviršijant to, kas būtina tikslui pasiekti, atsižvelgiant į vis didesnę joms kylančią riziką.

- **Priemonės pasirinkimas**

Reglamentas, kuris yra tiesiogiai taikomas, laikomas tinkama pasirinkta teisine priemone Sąjungos institucijoms, įstaigoms ir agentūroms nustatytiems įpareigojimams apibrėžti ir racionalizuoti. Reglamentas yra tinkamiausia teisinė priemonė, taikytina siekiant sudaryti sąlygas tiksliniams patobulinimams.

3. *EX ANTE* VERTINIMO, KONSULTACIJŲ SU SUINTERESUOTOSIOMIS ŠALIMIS IR POVEIKIO VERTINIMO REZULTATAI

- ***Ex ante* vertinimai**

CERT-EU atliko pagrindinių kibernetinių grėsmių, su kuriomis šiuo metu susiduria arba artimoje ateityje gali susidurti Sąjungos institucijos, įstaigos ir agentūros, vertinimą.

Buvo analizuojamos stebimos trijų kategorijų grėsmės:

- bandymai pažeisti Sąjungos institucijų, įstaigų ir agentūrų IT infrastruktūrą (kai jie sėkmingai įgyvendinami, jie laikomi incidentais, kitais atvejais jie vis dar registruojami kaip nustatyti bandymai);
- grėsmės, nustatytos netoli Sąjungos institucijų, įstaigų ir agentūrų (pvz., susijusiuose sektoriuose, suinteresuotųjų subjektų bendruomenėse arba Europoje);
- pasaulyje stebimos pagrindinės grėsmių tendencijos.

Be to, analizėje svarstyta, kokį poveikį vykstantys esminiai pokyčiai daro Sąjungos institucijų IT infrastruktūros ir paslaugų valdymo ir naudojimo būdams. Tokie pokyčiai apima:

- dažniau taikomą nuotolinį darbą;
- sistemų perkėlimą į debesiją;
- išaugusį IT paslaugų perdavimo išorės paslaugų teikėjams mastą.

2019–2021 m. labai padaugėjo reikšmingų incidentų[1], darančių poveikį Sąjungos institucijoms, įstaigoms ir agentūroms, kuriuos sukėlė vadinamieji aukšto lygio tęstinės grėsmės (*advanced persistent threat, APT*) subjektai. Per 2021 m. pirmąjį pusmetį reikšmingų incidentų įvyko tiek, kiek per visus 2020 m. Tai taip pat matyti iš to, kad 2020 m. CERT-EU išanalizuotų kriminalistinių vaizdų (paveiktų sistemų ar įrenginių turinio momentinių nuotraukų), palyginti su 2019 m., padaugėjo tris kartus, o reikšmingų incidentų skaičius, palyginti su 2018 m., išaugo daugiau nei dešimt kartų.

[1] Reikšmingas incidentas – bet koks incidentas, išskyrus tokį, kurio poveikis nedidelis ir kurio sukėlimo metodai arba technologijos veikiausiai jau yra gerai perprasti.

2020 m. CERT-EU valdančioji taryba nustatė naują strateginį CERT-EU tikslą užtikrinti visapusišką visų institucijų, įstaigų ir agentūrų kibernetinės gynybos lygį, tinkamą jos mastą ir išsamumo laipsnį, taip pat nuolatinį prisitaikymą prie esamų ar galimų grėsmių, įskaitant išpuolius prieš mobiliuosius įrenginius, debesijos aplinką ir daiktų interneto įrenginius.

Be CERT-EU grėsmių analizės, Komisija atliko 20 Sąjungos institucijų, įstaigų ir agentūrų kibernetinio saugumo sistemos veikimo vertinimą. Tai suteikė įžvalgų apie nusistovėjusią kibernetinio saugumo praktiką ir kibernetinio saugumo valdymo pajėgumus, atliekant kai kurių techninių saugumo kontrolės priemonių išorės lyginamąją analizę.

Šis vertinimas buvo grindžiamas klausimynais, į kuriuos šios institucijos, įstaigos ir agentūros atsakė, viešai prieinamais duomenimis ir pačių Sąjungos institucijų, įstaigų ir agentūrų tiesiogiai pateiktais duomenimis. Jame pateikiama pakankamai įžvalgų apie dabartinę padėtį, kad būtų galima padaryti šias išvadas:

- vertinamų Sąjungos institucijų, įstaigų ir agentūrų kibernetinio saugumo branda, IT infrastruktūros dydis ir pajėgumų lygiai labai skiriasi;

- nors daugelis Sąjungos institucijų, įstaigų ir agentūrų apskritai turi brandžių aptikimo ir reagavimo pajėgumų, jų kibernetinio saugumo valdymo pajėgumų integruoto rizikos valdymo lygmenys skiriasi;

- kadangi vertintų Sąjungos institucijų, įstaigų ir agentūrų kibernetinio saugumo sistemos (strategija, politika ir taisyklių bazė) apskritai yra gerai įtvirtintos pagrindinėse kibernetinio saugumo srityse, išvardytose reglamento I priede, kai kuriose Sąjungos institucijose, įstaigose ir agentūrose trūksta brandaus veiklos tęstinumo valdymo, atitikties, audito ir nuolatinio tobulinimo.

- Nustatyta, kad vertintos Sąjungos institucijos, įstaigos ir agentūros nevienodai taiko geriausia patirtimi laikomas technines priemones.

Apibendrinant, iš 20 Sąjungos institucijų, įstaigų ir agentūrų analizės matyti, kad jų valdymas, kibernetinė higiena, bendri pajėgumai ir branda labai nevienodi. Todėl reikalavimas, kad visos Sąjungos institucijos, įstaigos ir agentūros įgyvendintų pagrindines kibernetinio saugumo priemones, yra labai svarbus siekiant pašalinti šį brandos lygio skirtumą ir užtikrinti, kad visos Sąjungos institucijos, įstaigos ir agentūros pasiektų aukštą bendrą kibernetinio saugumo lygį.

Iki šiol nėra nė vieno Sąjungos teisės akto, kuriame daugiausiai dėmesio būtų skirta Sąjungos institucijų, įstaigų ir agentūrų kibernetiniam saugumui ir kuriuo būtų visapusiškai sprendžiami kibernetinių grėsmių ir dėl skaitmeninimo atsirandančios IT rizikos klausimai.

- **Konsultacijos su suinteresuotosiomis šalimis**

Komisija konsultavosi su suinteresuotaisiais subjektais iš visų Sąjungos institucijų, įstaigų ir agentūrų, taip pat su valstybių narių atstovais Taryboje ir suinteresuotaisiais subjektais Europos Parlamente. 2021 m. birželio 25 d. valstybių narių atstovai ir atitinkamos Sąjungos institucijos, įstaigos ir agentūros dalyvavo Komisijos surengtame seminare būsimo pasiūlymo dėl reglamento turiniui aptarti.

- **Poveikio vertinimas**

Šio pasiūlymo poveikį patirs Sąjungos institucijos, įstaigos ir agentūros. Todėl konkretus poveikio vertinimas nebūtinas, nes jis nebus taikomas valstybėms narėms.

- **Pagrindinės teisės**

Europos Sąjunga yra įsipareigojusi užtikrinti aukštus pagrindinių teisių apsaugos standartus. Visi šiuo reglamentu grindžiami informacijos mainai būtų vykdomi patikimoje aplinkoje, visapusiškai gerbiant teisę į asmens duomenų apsaugą, kaip nustatyta Europos Sąjungos pagrindinių teisių chartijos 8 straipsnyje ir atitinkamuose duomenų apsaugos teisės aktuose, visų pirma Europos Parlamento ir Tarybos reglamente (ES) 2018/1725.

4. POVEIKIS BIUDŽETUI

Iš rinkos lyginamosios analizės ir tyrimų[2] matyti, kad tiesioginės išlaidos kibernetiniam saugumui paprastai sudarė 4–7 proc. visų organizacijose patiriamų IT išlaidų. Vis dėlto iš CERT-EU atliktos grėsmių analizės, kuria grindžiamas šis pasiūlymas dėl teisėkūros procedūra priimamo akto, matyti, kad tarptautinės įstaigos ir politinės organizacijos susiduria su padidėjusia rizika, todėl 10 proc. IT išlaidų kibernetiniam saugumui lygis, regis, būtų tinkamesnis tikslas. Tiksliai nustatyti, kokios bus tokių pastangų sąnaudos, negalima, nes trūksta išsamios informacijos apie Sąjungos institucijų, įstaigų ir agentūrų IT išlaidas ir atitinkamą kibernetinio saugumo išlaidų dalį.

Todėl, nors tikėtina, kad daugelis Sąjungos institucijų, įstaigų ir agentūrų kibernetinio saugumo srityje išleidžia mažiau nei turėtų, dėl šio reglamento tos einamosios išlaidos nepadidės. Net ir be reglamento kiekvienas subjektas turėtų užtikrinti tinkamą kibernetinio saugumo lygį. Reglamentu tęsiamas ankstesnis bendradarbiavimas CERT-EU valdančiojoje taryboje ir įforminamas šiuo metu iš dalies jau egzistuojantis keitimosi informacija lygmuo. Kaip išsamiai išdėstyta finansinėje teisės akto pasiūlymo pažymoje, CERT-EU reikės papildomų išteklių, kad galėtų atlikti išplėstą vaidmenį, ir šie ištekliai turėtų būti perskirstyti iš Sąjungos institucijų, įstaigų ir agentūrų, kurios naudojasi CERT-EU paslaugomis.

5. KITI ELEMENTAI

- **Įgyvendinimas, stebėsena, vertinimas ir ataskaitų teikimo tvarka**

Tarpinstitucinė kibernetinio saugumo taryba (TKST) turėtų, padedant CERT-EU, peržiūrėti šio reglamento veikimą, atlikti vertinimus ir pateikti Komisijai ataskaitą su savo išvadomis. Komisija turėtų užtikrinti, kad Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui būtų teikiamos reguliarios ataskaitos.

---

[2] Šaltinis: Gartner „Identifying the Real Information Security Budget“ (2016). Dar yra netiesioginės IT saugumo išlaidos, pvz., išlaidos tinklo saugumui užtikrinti, kaip antai išlaidos, susijusios su užkardomis, antivirusinėmis programomis ir sistemos savininko pareigų vykdymu, pvz., rizikos vertinimu ir saugumo kontrolės priemonių įgyvendinimu. 2020 m. dokumente nurodoma, kad finansų įstaigų kibernetinio saugumo išlaidos sudaro 10–11 proc. IT išlaidų, šaltinis: DI_2020-FS-ISAC-Cybersecurity.pdf (deloitte.com).

CERT-EU gali parengti pasiūlymą dėl rekomendacinio dokumento arba rekomendacijos, kuriuos TKST gali nuspręsti priimti. Rekomendacinis dokumentas yra visoms Sąjungos institucijoms, įstaigoms ir agentūroms ar jų daliai skirtas patariamasis dokumentas, o rekomendacija skirta atskiroms Sąjungos institucijoms, įstaigoms ir agentūroms. Kvietimas imtis veiksmų yra CERT-EU patariamasis dokumentas, kuriame išdėstomos skubios saugumo priemonės, kurių Sąjungos institucijos, įstaigos ir agentūros raginamos imtis per nustatytą laikotarpį.

- **Išsamus konkrečių pasiūlymo nuostatų paaiškinimas**

Bendrosios nuostatos

Reglamentu nustatomos priemonės aukštam bendram kibernetinio saugumo lygiui užtikrinti ir jis taikomas Sąjungos institucijoms, įstaigoms ir agentūroms, kad jos galėtų atvirai, veiksmingai ir nepriklausomai vykdyti atitinkamas savo užduotis. (1–3 ir 23–25 straipsniai)

Priemonės aukštam bendram kibernetinio saugumo lygiui užtikrinti

Sąjungos institucijos, įstaigos ir agentūros yra įpareigotos sukurti vidaus rizikos kibernetiniam saugumui valdymo ir kontrolės sistemą, kuria būtų užtikrintas veiksmingas ir apdairus visų kibernetinio saugumo rizikos veiksnių valdymas. Be to, institucijos, įstaigos ir agentūros turi patvirtinti pagrindinius kibernetinio saugumo standartus, kuriais siekiama mažinti pagal sistemą nustatytą riziką, reguliariai vykdo kibernetinio saugumo brandos vertinimą ir priima kibernetinio saugumo planą. (4–8 straipsniai)

Tarpinstitucinė kibernetinio saugumo taryba

Įsteigiama Tarpinstitucinė kibernetinio saugumo taryba, kuriai pavedama pareiga stebėti, kaip Sąjungos institucijos, įstaigos ir agentūros įgyvendina šį reglamentą, taip pat prižiūrėti, kaip CERT-EU įgyvendina bendruosius prioritetus ir tikslus, ir nustatyti CERT-EU strateginę kryptį. (9–11 straipsniai)

CERT-EU

CERT-EU prisideda prie visų Sąjungos institucijų, įstaigų ir agentūrų IT aplinkos saugumo, konsultuodamas jas, padėdamas užkirsti kelią incidentams, juos aptikti, sušvelninti jų poveikį ir į juos reaguoti, taip pat veikdamas kaip jų keitimosi kibernetinio saugumo informacija ir reagavimo į incidentus koordinavimo centras. (12–17 straipsniai)

Bendradarbiavimas ir pareiga teikti ataskaitas

Siekiant didinti pasitikėjimą reglamentu užtikrinamas CERT-EU ir Sąjungos institucijų, įstaigų ir agentūrų bendradarbiavimas ir keitimasis informacija. Šiuo tikslu CERT-EU gali prašyti Sąjungos institucijų, įstaigų ir agentūrų suteikti jam atitinkamą informaciją ir jis su Sąjungos institucijomis, įstaigomis ir agentūromis gali keistis su incidentais susijusia informacija, kad būtų lengviau nustatyti panašias kibernetines grėsmes ar incidentus be nukentėjusio dalyvio sutikimo. CERT-EU gali keistis su incidentu susijusia informacija, kurioje atskleidžiama kibernetinio incidento taikinio tapatybė, tik gavęs nukentėjusio dalyvio sutikimą.

Visos Sąjungos institucijos, įstaigos ir agentūros apie reikšmingas kibernetines grėsmes, reikšmingą pažeidžiamumą ir reikšmingus incidentus nepagrįstai nedelsdamos ir bet kuriuo atveju ne vėliau kaip per 24 valandas nuo tada, kai apie juos sužino, praneša CERT-EU. (18–22 straipsniai)

2022/0085 (COD)

Pasiūlymas

EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS

kuriuo nustatomos priemonės aukštam bendram kibernetinio saugumo lygiui Sąjungos institucijose, įstaigose, organuose ir agentūrose užtikrinti

EUROPOS PARLAMENTAS IR EUROPOS SĄJUNGOS TARYBA,

atsižvelgdami į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 298 straipsnį,

atsižvelgdami į Europos atominės energijos bendrijos steigimo sutartį, ypač į jos 106a straipsnį,

atsižvelgdami į Europos Komisijos pasiūlymą,

teisėkūros procedūra priimamo akto projektą perdavus nacionaliniams parlamentams,

laikydamiesi įprastos teisėkūros procedūros,

kadangi:

(1) skaitmeniniame amžiuje informacinės ir ryšių technologijos yra atviros, veiksmingos ir nepriklausomos Sąjungos administracijos kertinis akmuo. Dėl technologijų raidos ir didesnio skaitmeninių sistemų sudėtingumo bei tarpusavio sąsajų didėja rizika kibernetiniam saugumui, todėl Sąjungos administracija tampa labiau pažeidžiama dėl kibernetinių grėsmių ir incidentų, o tai galiausiai kelia grėsmę administracijos veiklos tęstinumui ir pajėgumui apsaugoti savo duomenis. šiuo metu visai Sąjungos administracinių subjektų veiklai būdingas platus debesijos paslaugų naudojimas, visapusiškas informacinių technologijų naudojimas, skaitmeninimas, nuotolinis darbas ir besivystančios technologijos bei junglumas, tačiau skaitmeninis atsparumas dar užtikrintas nepakankamai;

(2) kibernetinių grėsmių, su kuriomis susiduria Sąjungos institucijos, įstaigos ir agentūros, padėtis nuolat kinta. Grėsmę keliančių subjektų naudojama taktika, metodai ir procedūros nuolat vystosi, tačiau aiškūs tokių išpuolių motyvai vargiai kinta: vertingos konfidencialios informacijos vagystės, pinigų pritrukimas, manipuliavimas viešąja nuomone ar kenkimas skaitmeninei infrastruktūrai. Jų kibernetinių išpuolių vykdymo tempas vis didėja, o jų kampanijos tampa vis sudėtingesnės ir automatizuotos ir yra nukreiptos į matomą išpuolių perimetrą, kuris toliau plečiasi ir kuriame greitai išnaudojamas pažeidžiamumas;

(3) Sąjungos institucijų, įstaigų ir agentūrų IT aplinkose yra tarpusavyje priklausomų elementų ir integruotų duomenų srautų, o jų naudotojai glaudžiai bendradarbiauja. Šis tarpusavio ryšys reiškia, kad bet koks sutrikimas, net jei iš pradžių jis susijęs tik su viena Sąjungos institucija, įstaiga ar agentūra, gali turėti platesnį pakopinį poveikį, o

šis gali turėti plataus masto ir ilgalaikių neigiamų padarinių kitoms institucijoms. Be to, tam tikra institucijų, įstaigų ir agentūrų IT aplinka yra susijusi su valstybių narių IT aplinka, tad incidentas viename Sąjungos subjekte kelia pavojų atitinkamos valstybių narių IT aplinkos kibernetiniam saugumui ir atvirkščiai;

(4) Sąjungos institucijos, įstaigos ir agentūros yra patrauklūs taikiniai, kurie susiduria su aukštos kvalifikacijos ir išteklių turinčiais priešiškais subjektais ir kitomis grėsmėmis. Be to, tų institucijų, įstaigų ir agentūrų kibernetinio atsparumo lygis ir branda, gebėjimas aptikti kibernetinę kenkimo veiklą ir į ją reaguoti labai skiriasi. Todėl tam, kad Europos administracija veiktų, būtina, kad Sąjungos institucijos, įstaigos ir agentūros užtikrintų aukštą bendrą kibernetinio saugumo lygį, nustatydamos pagrindinius kibernetinio saugumo standartus (būtiniausias kibernetinio saugumo taisykles, kurias turi atitikti tinklų ir informacinės sistemos ir laikytis jų operatoriai bei naudotojai, kad būtų kuo labiau sumažinta rizika kibernetiniam saugumui), keistųsi informacija ir bendradarbiautų;

(5) Direktyva [pasiūlymas dėl TIS 2] dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti siekiama toliau didinti viešųjų ir privačiųjų subjektų, nacionalinių kompetentingų institucijų ir įstaigų ir visos Sąjungos kibernetinio saugumo sistemos atsparumą ir reagavimo į incidentus pajėgumus. Todėl būtina, kad Sąjungos institucijos, įstaigos ir agentūros to laikytųsi, užtikrindamos taisykles, kurios derėtų su Direktyva [pasiūlymu dėl TIS 2] ir atspindėtų jos užmojų mastą;

(6) aukštam bendram kibernetinio saugumo lygiui pasiekti būtina, kad kiekviena Sąjungos institucija, įstaiga ir agentūra nustatytų vidaus kibernetinio saugumo rizikos valdymo ir kontrolės sistemą, kuria būtų užtikrinamas veiksmingas ir apdairus visų rizikos kibernetiniam saugumui veiksnių valdymas ir atsižvelgiama į veiklos tęstinumą ir krizių valdymą;

(7) dėl Sąjungos institucijų, įstaigų ir agentūrų skirtumų įgyvendinimo srityje reikia lankstumo, nes vieno visiems tinkančio sprendimo nėra. Priemonės aukštam bendram kibernetinio saugumo lygiui užtikrinti neturėtų apimti jokių įpareigojimų, kuriais būtų tiesiogiai kišamasi į Sąjungos institucijų, įstaigų ir agentūrų užduočių vykdymą arba kėsinamasi į jų institucinį savarankiškumą. Todėl tos institucijos, įstaigos ir agentūros turėtų sukurti savo rizikos kibernetiniam saugumui valdymo ir kontrolės sistemas ir patvirtinti savo pagrindinius standartus bei kibernetinio saugumo planus;

(8) siekiant neužkrauti Sąjungos institucijoms, įstaigoms ir agentūroms finansinės ir administracinės naštos, rizikos kibernetiniam saugumui valdymo reikalavimai turėtų būti proporcingi rizikai, kurią kelia atitinkama tinklų ir informacinė sistema, atsižvelgiant į tokių priemonių modernumą. Kiekviena Sąjungos institucija, įstaiga ir agentūra turėtų siekti skirti tinkamą savo IT biudžeto procentinę dalį tikslui padidinti savo kibernetinio saugumo lygį; ilguoju laikotarpiu tam turėtų būti skiriama maždaug 10 proc. IT biudžeto;

(9) siekiant užtikrinti aukštą bendrą kibernetinio saugumo lygį kibernetinis saugumas turi būti prižiūrimas aukščiausiu kiekvienos Sąjungos institucijos, įstaigos ir agentūros valdymo lygmeniu; jose turėtų būti patvirtinti pagrindiniai kibernetinio saugumo standartai, kurie turėtų padėti mažinti riziką, nustatytą pagal kiekvienoje institucijoje, įstaigoje ir agentūroje sukurtą sistemą. Kibernetinio saugumo kultūra, t. y. kasdienė

kibernetinio saugumo praktika, yra neatsiejama pagrindinių kibernetinio saugumo standartų visose Sąjungos institucijose, įstaigose ir įstaigose dalis;

(10) Sąjungos institucijos, įstaigos ir agentūros turėtų įvertinti riziką, susijusią su santykiais su tiekėjais ir paslaugų teikėjais, įskaitant duomenų saugojimo ir tvarkymo paslaugų teikėjus arba valdomas saugumo paslaugas, ir imtis tinkamų priemonių jai sumažinti. Šios priemonės turėtų būti pagrindinių kibernetinio saugumo standartų dalis ir jos turėtų būti išsamiau išdėstytos CERT-EU parengtose gairėse arba rekomendacijose. Nustatant priemones ir gaires reikėtų tinkamai atsižvelgti į atitinkamus ES teisės aktus ir politiką, įskaitant TIS bendradarbiavimo grupės pateiktus rizikos vertinimus ir rekomendacijas, pavyzdžiui, ES suderintą rizikos vertinimą ir ES 5G kibernetinio saugumo priemonių rinkinį. Be to, pagal konkrečias ES kibernetinio saugumo sertifikavimo schemas, priimtas pagal Reglamento (ES) 2019/881 49 straipsnį, galėtų būti reikalaujama sertifikuoti atitinkamus IRT produktus, paslaugas ir procesus;

(11) 2011 m. gegužės mėn. Sąjungos institucijų ir įstaigų generaliniai sekretoriai nusprendė įsteigti Sąjungos institucijų, įstaigų ir agentūrų kompiuterinių incidentų tyrimo tarnybos (CERT-EU), kurią prižiūri tarpinstitucinė valdančioji taryba, išankstinės sudėties grupę. 2012 m. liepos mėn. generaliniai sekretoriai patvirtino praktinę tvarką ir sutarė išlaikyti CERT-EU kaip nuolatinį subjektą, kuris toliau padėtų gerinti bendrą Sąjungos institucijų, įstaigų ir agentūrų informacinių technologijų saugumo lygį, kaip matomo tarpinstitucinio bendradarbiavimo kibernetinio saugumo srityje pavyzdį. 2012 m. rugsėjo mėn. CERT-EU buvo įsteigta kaip Europos Komisijos darbo grupė, turinti tarpinstitucinius įgaliojimus. 2017 m. gruodžio mėn. Sąjungos institucijos ir įstaigos sudarė tarpinstitucinį susitarimą dėl CERT-EU organizavimo ir veiklos[3]. Šis susitarimas turėtų būti toliau plėtojamas, siekiant remti šio reglamento įgyvendinimą.

(12) CERT-EU iš Sąjungos institucijų, įstaigų ir agentūrų kompiuterinių incidentų tyrimo tarnybos turėtų būti pervadinta į Kibernetinio saugumo centrą, atsižvelgiant į pokyčius valstybėse narėse ir visame pasaulyje, kur daugelis CERT pervadintos kibernetinio saugumo centrais, tačiau dėl pavadinimo atpažinimo paliekamas trumpasis pavadinimas „CERT-EU“;

(13) daugelis kibernetinių išpuolių yra platesnių kampanijų, nukreiptų prieš Sąjungos institucijų, įstaigų ir agentūrų grupes arba interesų bendruomenes, įskaitant Sąjungos institucijas, įstaigas ir agentūras, dalis. Kad būtų galima imtis aktyvaus aptikimo, reagavimo į incidentus ar rizikos mažinimo priemonių, Sąjungos institucijos, įstaigos ir agentūros turėtų pranešti CERT-EU apie reikšmingas kibernetines grėsmes, reikšmingą pažeidžiamumą bei reikšmingus incidentus ir dalytis tinkama technine informacija, kad būtų galima nustatyti arba sumažinti panašias kibernetines grėsmes, pažeidžiamumą ir incidentus kitose Sąjungos institucijose, įstaigose ir agentūrose arba į juos reaguoti. Vadovaujantis tokiu pačiu požiūriu, koks yra numatytas Direktyvoje [pasiūlymas dėl TIS 2], subjektui sužinojus apie didelį incidentą, jis privalėtų per 24 valandas pateikti pirminį pranešimą CERT-EU. Toks keitimasis informacija turėtų sudaryti sąlygas CERT-EU skleisti informaciją kitoms Sąjungos institucijoms, įstaigoms ir agentūroms, taip pat atitinkamiems partneriams, siekiant padėti apsaugoti Sąjungos IT aplinką ir Sąjungos partnerių IT aplinką nuo panašių incidentų, grėsmių ir pažeidžiamumo;

[3] OL C 12, 2018 1 13, p. 1–11.

(14) CERT-EU turėtų būti ne tik pavesta daugiau užduočių ir išplėstas jos vaidmuo, bet taip pat turėtų būti įsteigta Tarpinstitucinė kibernetinio saugumo taryba (TKST), kuri turėtų padėti užtikrinti aukštą bendrą Sąjungos institucijų, įstaigų ir agentūrų kibernetinio saugumo lygį, stebint, kaip Sąjungos institucijos, įstaigos ir agentūros įgyvendina šį reglamentą, ir prižiūrint, kaip CERT-EU įgyvendina bendruosius prioritetus ir tikslus, bei numatant CERT-EU strateginę kryptį. TKST turėtų užtikrinti atstovavimą institucijoms ir į ją turėtų būti įtraukta agentūrų ir įstaigų atstovų, vykdančių veiklą per Sąjungos agentūrų tinklą;

(15) CERT-EU turėtų padėti įgyvendinti priemones, skirtas aukštam bendram kibernetinio saugumo lygiui užtikrinti, teikdama pasiūlymus dėl rekomendacinių dokumentų ir rekomendacijų TKST arba skelbdama raginimus imtis veiksmų. Tokius rekomendacinius dokumentus ir rekomendacijas turėtų tvirtinti TKST. Prireikus CERT-EU turėtų skelbti raginimus imtis veiksmų, kuriuose aprašomos skubios saugumo priemonės, kurių Sąjungos institucijos, įstaigos ir agentūros raginamos imtis per nustatytą laikotarpį;

(16) TKST turėtų stebėti, kaip laikomasi šio reglamento ir kaip įgyvendinami tolesni veiksmai, susiję su CERT-EU pateiktais rekomendaciniais dokumentais ir rekomendacijomis bei paskelbtais raginimais imtis veiksmų. TKS valdybą techniniais klausimais turėtų remti jos savo nuožiūra nustatytos sudėties techninės patariamosios grupės, kurios prireikus turėtų glaudžiai bendradarbiauti su CERT-EU, Sąjungos institucijomis, įstaigomis ir agentūromis bei kitais suinteresuotaisiais subjektais. Prireikus TKST turėtų skelbti neprivalomus įspėjimus ir rekomenduoti auditus;

(17) CERT-EU turėtų būti pavesta prisidėti prie visų Sąjungos institucijų, įstaigų ir agentūrų IT aplinkos saugumo. CERT-EU turėtų veikti kaip Sąjungos institucijų, įstaigų ir agentūrų paskirto koordinatoriaus atitikmuo suderinto pažeidžiamumų atskleidimo Europos pažeidžiamumų registrui tikslais, kaip nurodyta Direktyvos [pasiūlymas dėl TIS 2] 6 straipsnyje;

(18) 2020 m. CERT-EU valdančioji taryba nustatė naują strateginį CERT-EU tikslą užtikrinti visapusišką visų Sąjungos institucijų, įstaigų ir agentūrų kibernetinės gynybos lygį, tinkamą jos mastą ir išsamumo laipsnį, taip pat nuolatinį prisitaikymą prie esamų ar galimų grėsmių, įskaitant išpuolius prieš mobiliuosius įrenginius, debesijos aplinką ir daiktų interneto įrenginius. Jos strateginis tikslas taip pat apima plataus masto saugumo operacijų centrus (SOC), kurie stebi tinklus, ir visą parą kasdien vykdomą labai didelių grėsmių stebėseną. Didesnių Sąjungos institucijų, įstaigų ir agentūrų atveju CERT-EU turėtų padėti jų IT saugumo grupėms, be kita ko, visą parą kasdien vykdant pirminę stebėseną. Mažesnėms ir kai kurioms vidutinio dydžio Sąjungos institucijoms, įstaigoms ir agentūroms CERT-EU turėtų teikti visas paslaugas;

(19) CERT-EU taip pat turėtų atlikti Direktyvoje [pasiūlymas dėl TIS 2] numatytą vaidmenį, susijusį su bendradarbiavimu ir keitimusi informacija su reagavimo į kompiuterių saugumo incidentus tarnybų (CSIRT) tinklu. Be to, pagal Komisijos rekomendaciją (ES) 2017/1584[4] CERT-EU turėtų bendradarbiauti ir koordinuoti reagavimo veiksmus su atitinkamais suinteresuotaisiais subjektais; siekdama prisidėti

[4] 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).

prie aukšto kibernetinio saugumo lygio visoje Sąjungoje, CERT-EU turėtų dalytis su incidentais susijusia informacija su analogiškais nacionaliniais centrais. gavusi išankstinį TKST pritarimą CERT-EU taip pat turėtų bendradarbiauti su kitais viešaisiais ir privačiaisiais partneriais, įskaitant NATO;

(20) siekdama remti operatyvinį kibernetinį saugumą CERT-EU turėtų pasinaudoti Europos Sąjungos kibernetinio saugumo agentūros ekspertinėmis žiniomis, vykdydama Europos Parlamento ir Tarybos reglamente (ES) 2019/881[5] numatytą struktūrinį bendradarbiavimą. Kai tinkama, turėtų būti sudaryti specialūs šių dviejų organizacijų susitarimai, siekiant nustatyti, kaip toks bendradarbiavimas bus įgyvendinamas praktiškai, ir išvengti veiklos dubliavimo. CERT-EU turėtų bendradarbiauti su Europos Sąjungos kibernetinio saugumo agentūra grėsmių analizės srityje ir reguliariai dalytis su ja grėsmių padėties ataskaita;

(21) remdamas Jungtinį kibernetinio saugumo padalinį, įsteigtą pagal 2021 m. birželio 23 d. Komisijos rekomendaciją[6], CERT-EU turėtų bendradarbiauti ir keistis informacija su suinteresuotaisiais subjektais, kad būtų skatinamas operatyvinis bendradarbiavimas ir sudarytos sąlygos esamiems tinklams išnaudoti visą savo potencialą apsaugant Sąjungą;

(22) visi pagal šį reglamentą tvarkomi asmens duomenys turėtų būti tvarkomi laikantis duomenų apsaugos teisės aktų, įskaitant Europos Parlamento ir Tarybos reglamentą (ES) 2018/1725[7];

(23) CERT-EU ir Sąjungos institucijos, įstaigos ir agentūros turėtų tvarkyti informaciją pagal Reglamente [siūlomas reglamentas dėl informacijos saugumo] nustatytas taisykles. Siekiant užtikrinti koordinavimą sprendžiant saugumo klausimus, apie bet kokius ryšius su CERT-EU, kuriuos inicijuoja arba siekia inicijuoti nacionalinės saugumo ir žvalgybos tarnybos, turėtų būti nepagrįstai nedelsiant pranešama Komisijos Saugumo direktoratui ir TKST pirmininkui;

(24) kadangi CERT-EU paslaugos ir užduotys atitinka visų Sąjungos institucijų, įstaigų ir agentūrų interesus, kiekviena IT išlaidų turinti Sąjungos institucija, įstaiga ir agentūra turėtų sąžiningai prisidėti prie tų paslaugų teikimo ir užduočių vykdymo. Tie įnašai nedaro poveikio Sąjungos institucijų, įstaigų ir agentūrų biudžetiniam savarankiškumui.

(25) TKST, padedant CERT-EU, turėtų peržiūrėti ir įvertinti šio reglamento įgyvendinimą ir pateikti savo išvadas Komisijai. Remdamasi ta informacija Komisija turėtų teikti ataskaitas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui,

---

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).

6 2021 m. birželio 23 d. Komisijos rekomendacija C(2021) 4520 dėl Jungtinio kibernetinio saugumo padalinio sukūrimo.

7 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002/EB (OL L 295, 2018 11 21, p. 39).

PRIĖMĖ ŠĮ REGLAMENTĄ:

I skyrius
BENDROSIOS NUOSTATOS

1 straipsnis
Dalykas

Šiuo reglamentu nustatomi:

(a) Sąjungos institucijų, įstaigų ir agentūrų įpareigojimai sukurti vidaus rizikos kibernetiniam saugumui valdymo ir kontrolės sistemą;

(b) Sąjungos institucijų, įstaigų ir agentūrų rizikos kibernetiniam saugumui valdymo ir ataskaitų teikimo pareigos;

(c) Sąjungos institucijų, įstaigų ir agentūrų kibernetinio saugumo centro (CERT-EU) organizavimo ir veiklos taisyklės ir Tarpinstitucinės kibernetinio saugumo tarybos organizavimo ir veiklos taisyklės.

2 straipsnis
Taikymo sritis

Šis reglamentas taikomas visų Sąjungos institucijų, įstaigų ir agentūrų rizikos kibernetiniam saugumui valdymui ir kontrolei, taip pat CERT-EU ir Tarpinstitucinės kibernetinio saugumo tarybos organizavimui ir veiklai.

3 straipsnis
Terminų apibrėžtys

Šiame reglamente vartojamų terminų apibrėžtys:

(1) Sąjungos institucijos, įstaigos ir agentūros – Sąjungos institucijos, įstaigos ir agentūros, įsteigtos Europos Sąjungos sutartimi, Sutartimi dėl Europos Sąjungos veikimo arba Europos atominės energijos bendrijos steigimo sutartimi arba jomis remiantis;

(2) tinklų ir informacinė sistema – tinklų ir informacinė sistema, kaip apibrėžta Direktyvos [pasiūlymas dėl TIS 2] 4 straipsnio 1 dalyje;

(3) tinklų ir informacinių sistemų saugumas – tinklų ir informacinių sistemų saugumas, kaip apibrėžta Direktyvos [pasiūlymas dėl TIS 2] 4 straipsnio 2 dalyje;

(4) kibernetinis saugumas – kibernetinis saugumas, kaip apibrėžta Direktyvos [pasiūlymas dėl TIS 2] 4 straipsnio 3 punkte;

(5) aukščiausias valdymo lygmuo – aukščiausio administracinio lygmens vadovas, valdymo arba koordinavimo ir priežiūros organas, atsižvelgiant į kiekvienos Sąjungos institucijos, įstaigos ar agentūros aukšto lygio valdymo tvarką;

(6) incidentas – incidentas, kaip apibrėžta Direktyvos [pasiūlymas dėl TIS 2] 4 straipsnio 5 punkte;

(7) reikšmingas incidentas – bet koks incidentas, išskyrus tokį, kurio poveikis nedidelis ir kurio sukėlimo metodai arba technologijos veikiausiai jau yra gerai perprasti;

(8) didelis išpuolis – incidentas, kurio atveju reikia daugiau išteklių nei turima nukentėjusioje Sąjungos institucijoje, įstaigoje ar agentūroje ir CERT-EU;

(9) incidento valdymas – incidento valdymas, kaip apibrėžta Direktyvos [pasiūlymas dėl TIS 2] 4 straipsnio 6 punkte;

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

(11) reikšminga kibernetinė grėsmė – kibernetinė grėsmė, keliama ketinant, turint galimybę ir gebant sukelti reikšmingą incidentą;

(12) pažeidžiamumas – pažeidžiamumas, kaip apibrėžta Direktyvos [pasiūlymas dėl TIS 2] 4 straipsnio 8 punkte;

(13) reikšmingas pažeidžiamumas – pažeidžiamumas, dėl kurio, jei juo bus pasinaudota, gali kilti reikšmingas incidentas;

(14) rizika kibernetiniam saugumui – pagrįstai nustatoma aplinkybė ar įvykis, galintis turėti neigiamą poveikį tinklų ir informacinių sistemų saugumui;

(15) Jungtinis kibernetinio saugumo padalinys – virtuali ir fizinė įvairių Sąjungos kibernetinio saugumo bendruomenių bendradarbiavimo platforma, kurioje daugiausia dėmesio skiriama operatyviniam ir techniniam koordinavimui kovojant su didelėmis tarpvalstybinėmis kibernetinėmis grėsmėmis ir incidentais, kaip apibrėžta 2021 m. birželio 23 d. Komisijos rekomendacijoje;

(16) pagrindiniai kibernetinio saugumo standartai – rinkinys būtiniausių kibernetinio saugumo taisyklių, kurias privalo atitikti tinklų ir informacinės sistemos ir kurių privalo laikytis jų operatoriai ir naudotojai, kad būtų kuo labiau sumažinta rizika kibernetiniam saugumui.

II skyrius
PRIEMONĖS AUKŠTAM BENDRAM KIBERNETINIO SAUGUMO LYGIUI UŽTIKRINTI

4 straipsnis
Rizikos valdymas ir kontrolė

1. Kiekviena Sąjungos institucija, įstaiga ir agentūra nustato savo vidaus kibernetiniam saugumui kylančios rizikos valdymo ir kontrolės sistemą (toliau – sistema), kuria remiama jos misija ir įgyvendinamas jos institucinis savarankiškumas. Siekiant užtikrinti veiksmingą ir apdairų visų rizikos kibernetiniam saugumui veiksnių valdymą, šis darbas prižiūrimas subjekto aukščiausiu valdymo lygmeniu. Sistema parengiama ne vėliau kaip... [15 mėnesių po šio reglamento įsigaliojimo].

2. Sistema apima visą atitinkamos institucijos, įstaigos ar agentūros IT aplinką, įskaitant bet kokią vietoje esančią IT aplinką, užsakomąjį turtą ir paslaugas debesijos kompiuterijos aplinkoje arba kurių prieglobą teikia trečiosios šalys, mobiliuosius įrenginius, įmonių tinklus, prie interneto neprijungtus verslo tinklus ir bet kokius su IT aplinka susijusius įrenginius. Sistemoje atsižvelgiama į veiklos tęstinumą, krizių valdymą ir tiekimo grandinės saugumą, taip pat į žmogaus sukeltos rizikos, kuri galėtų daryti poveikį atitinkamos Sąjungos institucijos, įstaigos ar agentūros kibernetiniam saugumui, valdymą.

3. Kiekviena Sąjungos institucija, įstaiga ir agentūra aukščiausiu valdymo lygmeniu prižiūri, kaip jų organizacija laikosi įpareigojimų, susijusių su rizikos kibernetiniam saugumui valdymu ir kontrole, nedarant poveikio oficialioms kitų lygmenų vadovybės pareigoms laikytis įpareigojimų ir valdyti riziką jų atitinkamose atsakomybės srityse.

4. Kiekviena Sąjungos institucija, įstaiga ir agentūra sukuria ir įdiegia veiksmingus mechanizmus, kuriais užtikrinama, kad kibernetiniam saugumui būtų išleidžiama tinkama IT biudžeto lėšų procentinė dalis.

5. Kiekviena Sąjungos institucija, įstaiga ir agentūra paskiria vietos kibernetinio saugumo pareigūną arba lygiavertę funkciją atliekantį pareigūną, kuris visais kibernetinio saugumo aspektais veikia kaip vienas kontaktinis asmuo.

5 straipsnis
Pagrindiniai kibernetinio saugumo standartai

1. Kiekviena Sąjungos institucija, įstaiga ir agentūra aukščiausiu valdymo lygmeniu patvirtina savo pagrindinius kibernetinio saugumo standartus, kuriais siekiama mažinti pagal 4 straipsnio 1 dalyje nurodytą sistemą nustatytą riziką. Standartais remiama jos misija ir įgyvendinamas jos institucinis savarankiškumas. Pagrindiniai kibernetinio saugumo standartai turi būti nustatyti ne vėliau kaip …. [18 mėnesių nuo šio reglamento įsigaliojimo] ir apimti I priede išvardytas sritis ir II priede išvardytas priemones.

2. Kiekvienos Sąjungos institucijos, įstaigos ir agentūros vyresnioji vadovybė reguliariai dalyvauja specialiame mokyme, kad įgytų pakankamai žinių ir įgūdžių, kurių reikia siekiant suprasti ir įvertinti riziką kibernetiniam saugumui ir su ja susijusią valdymo praktiką bei jos poveikį organizacijos veiklai.

6 straipsnis
Brandos vertinimai

Kiekviena Sąjungos institucija, įstaiga ir agentūra ne rečiau kaip kas trejus metus atlieka kibernetinio saugumo brandos vertinimą, apimantį visus jos IT aplinkos elementus, kaip aprašyta 4 straipsnyje, atsižvelgdama į atitinkamus pagal 13 straipsnį priimtus rekomendacinius dokumentus ir rekomendacijas.

7 straipsnis
Kibernetinio saugumo planai

1. Remdamasi išvadomis, padarytomis atlikus brandos vertinimą, ir atsižvelgdama į turtą bei riziką, nustatytą pagal 4 straipsnį, kiekviena Sąjungos institucija, įstaiga ir agentūra aukščiausiu valdymo lygmeniu nepagrįstai nedelsdama, nustačius rizikos valdymo ir kontrolės sistemą ir pagrindinius kibernetinio saugumo standartus, patvirtina kibernetinio saugumo planą. Planu siekiama padidinti bendrą atitinkamo subjekto kibernetinį saugumą ir taip prisidėti prie aukšto bendro visų Sąjungos institucijų, įstaigų ir agentūrų kibernetinio saugumo lygio pasiekimo arba padidinimo. Siekiant remti subjekto misiją, paremtą subjekto instituciniu savarankiškumu, į planą įtraukiamos bent I priede išvardytos sritys, II priede išvardytos priemonės ir priemonės, susijusios su pasirengimu incidentams, reagavimu į juos ir atkūrimu po jų, pavyzdžiui, saugumo stebėsena ir registravimas. Planas, atlikus brandos vertinimus pagal 6 straipsnį, peržiūrimas ne rečiau kaip kas trejus metus.

2. Kibernetinio saugumo plane nurodomos darbuotojų funkcijos ir atsakomybė už jo įgyvendinimą.

3. Kibernetinio saugumo plane atsižvelgiama į visus taikytinus CERT-EU parengtus rekomendacinius dokumentus ir rekomendacijas.

8 straipsnis
Įgyvendinimas

1. Atlikusios brandos vertinimus, Sąjungos institucijos, įstaigos ir agentūros pateikia juos Tarpinstitucinei kibernetinio saugumo tarybai. Įgyvendinusios saugumo planus, Sąjungos institucijos, įstaigos ir agentūros praneša Tarpinstitucinei kibernetinio saugumo tarybai apie jų užbaigimą. Valdybos prašymu jos teikia ataskaitas dėl konkrečių šio skyriaus aspektų.

2. Pagal 13 straipsnį paskelbti rekomendaciniai dokumentai ir rekomendacijos padeda įgyvendinti šio skyriaus nuostatas.

III skyrius
TARPINSTITUCINĖ KIBERNETINIO SAUGUMO TARYBA

9 straipsnis
Tarpinstitucinė kibernetinio saugumo taryba

1. Įsteigiama Tarpinstitucinė kibernetinio saugumo taryba (TKST).

2. TKST pareigos:

   (a) stebėti, kaip Sąjungos institucijos, įstaigos ir agentūros įgyvendina šį reglamentą;

   (b) prižiūrėti, kaip CERT-EU įgyvendina bendruosius prioritetus ir tikslus, ir nustatyti CERT-EU strateginę kryptį.

3. TKST sudaro trys atstovai, kuriuos savo IRT patariamojo komiteto siūlymu skiria Sąjungos agentūrų tinklas, kad jie atstovautų agentūrų ir įstaigų, kurios valdo savo pačių IT aplinką, interesams, ir po vieną kiekvienas iš šių subjektų skiriamą atstovą:

   (a) Europos Parlamentas;

   (b) Europos Sąjungos Taryba;

   (c) Europos Komisija;

   (d) Europos Sąjungos Teisingumo Teismas;

   (e) Europos Centrinis Bankas;

   (f) Europos Audito Rūmai;

   (g) Europos išorės veiksmų tarnyba;

   (h) Europos ekonomikos ir socialinių reikalų komitetas;

   (i) Europos regionų komitetas;

   (j) Europos investicijų bankas;

   (k) Europos Sąjungos kibernetinio saugumo agentūra.

   Nariams gali padėti pakaitiniai nariai. Pirmininkas gali kviesti kitus pirmiau išvardytų organizacijų arba kitų Sąjungos institucijų, įstaigų ir agentūrų atstovus dalyvauti TKST posėdžiuose be balsavimo teisės.

4. TKST patvirtina savo vidaus darbo tvarkos taisykles.

5. Pagal savo vidaus darbo tvarkos taisykles TKST iš savo narių ketverių metų laikotarpiui paskiria pirmininką. Jo pakaitinis narys tam pačiam laikotarpiui tampa tikruoju TKST nariu.

6. TKST renkasi savo pirmininko iniciatyva, CERT-EU prašymu arba bet kurio iš jos narių prašymu.

7. Kiekvienas TKST narys turi po vieną balsą. TKST sprendimai priimami paprasta balsų dauguma, išskyrus atvejus, kai šiame reglamente numatyta kitaip. Pirmininkas nebalsuoja, išskyrus atvejus, kai balsai pasiskirsto po lygiai, tuomet jis gali pasinaudoti lemiamo balso teise.

8. TKST gali priimti sprendimus taikant supaprastintą rašytinę procedūrą, inicijuotą pagal TKST vidaus darbo tvarkos taisykles. Pagal tą procedūrą laikoma, kad atitinkamas sprendimas yra patvirtintas per pirmininko nustatytą laikotarpį, išskyrus atvejus, kai narys paprieštarauja.

9. CERT-EU vadovas arba jo pakaitinis narys dalyvauja TKST posėdžiuose, išskyrus atvejus, kai TKST nusprendžia kitaip.

10. Sekretoriato paslaugas TKST teikia Komisija.

11. IRT patariamojo komiteto siūlymu Sąjungos agentūrų tinklo paskirti atstovai perduoda TKST sprendimus Sąjungos agentūroms ir bendrosioms įmonėms. Bet kuri Sąjungos agentūra ir įstaiga turi teisę pateikti TKST atstovams ar pirmininkui bet kokį klausimą, į kurį, jos nuomone, turėtų būti atkreiptas TKST dėmesys.

12. TKST gali priimti sprendimus taikant pirmininko inicijuotą supaprastintą rašytinę procedūrą, pagal kurią atitinkamas sprendimas laikomas patvirtintu per pirmininko nustatytą terminą, išskyrus atvejus, kai kuris nors narys pareiškia prieštaravimą.

13. TKST gali paskirti vykdomąjį komitetą, kuris padėtų jam vykdyti savo darbą, ir perduoti jam kai kurias savo užduotis ir įgaliojimus. TKST nustato vykdomojo komiteto darbo tvarkos taisykles, įskaitant jo užduotis bei įgaliojimus ir jo narių kadencijos trukmę.

10 straipsnis
TKST užduotys

Vykdydama savo pareigas TKST visų pirma:

(a) peržiūri visas ataskaitas, kurių prašoma iš CERT-EU, dėl to, kaip Sąjungos institucijos, įstaigos ir agentūros įgyvendina šį reglamentą;

(b) CERT-EU vadovo siūlymu tvirtina CERT-EU metinę darbo programą ir stebi, kaip ji įgyvendinama;

(c) CERT-EU vadovo siūlymu tvirtina CERT-EU paslaugų katalogą;

(d) CERT-EU vadovo siūlymu tvirtina metinį finansinį CERT-EU veiklos pajamų ir išlaidų, įskaitant personalą, planavimą;

(e) CERT-EU vadovo siūlymu tvirtina susitarimų dėl paslaugų lygio sąlygas;

(f) nagrinėja ir tvirtina CERT-EU vadovo parengtą metinę ataskaitą, kurioje aptariama CERT-EU veikla ir lėšų valdymas;

(g) tvirtina CERT-EU pagrindinius veiklos rezultatų rodiklius, kurie nustatomi remiantis CERT-EU vadovo siūlymu, ir stebi jų įgyvendinimą;

(h) tvirtina CERT-EU ir kitų subjektų bendradarbiavimo susitarimus, susitarimus dėl paslaugų lygio arba sutartis pagal 17 straipsnį;

(i) įsteigia tiek techninių patariamųjų grupių, kiek reikia siekiant prisidėti prie TKST darbo, tvirtina jų įgaliojimus ir skiria atitinkamus jų pirmininkus.

11 straipsnis
Reikalavimų laikymasis

TKST stebi, kaip įgyvendinamas šis reglamentas ir priimti rekomendaciniai dokumentai, rekomendacijos ir raginimai Sąjungos institucijoms, įstaigoms ir agentūroms imtis veiksmų. Jei TKST nustato, kad Sąjungos institucijos, įstaigos ar agentūros veiksmingai netaikė arba neįgyvendino šio reglamento arba rekomendacinių dokumentų, rekomendacijų ir raginimų imtis veiksmų pagal šį reglamentą, nedarant poveikio atitinkamos Sąjungos institucijos, organo ar agentūros vidaus procedūroms TKST gali:

(a) pateikti įspėjimą; kai tai būtina atsižvelgiant į akivaizdžią riziką kibernetiniam saugumui, tinkamai apriboti auditoriją, kuriai perspėjimas skirtas;

(b) rekomenduoti atitinkamai audito tarnybai atlikti auditą.

IV skyrius
CERT-EU

12 straipsnis
CERT-EU misija ir užduotys

1. CERT-EU, savarankiško tarpinstitucinio visų Sąjungos institucijų, įstaigų ir agentūrų kibernetinio saugumo centro, misija – padėti užtikrinti visų Sąjungos institucijų, įstaigų ir agentūrų neįslaptintos IT aplinkos saugumą jas konsultuojant kibernetinio saugumo klausimais, padedant užkirsti kelią incidentams, juos aptikti, sušvelninti jų poveikį ir į juos reaguoti, taip pat atliekant jų keitimosi kibernetinio saugumo informacija ir reagavimo į incidentus koordinavimo centro funkciją.

2. CERT-EU Sąjungos institucijoms, įstaigoms ir agentūroms atlieka šias užduotis:

   (a) padeda joms įgyvendinti šį reglamentą ir prisideda prie šio reglamento taikymo koordinavimo taikydama 13 straipsnio 1 dalyje išvardytas priemones arba teikdama TKST prašomas *ad hoc* ataskaitas;

   (b) padeda joms teikti paslaugas iš paslaugų kataloge aprašyto kibernetinio saugumo paslaugų paketo (toliau – pagrindinės paslaugos);

   (c) prižiūri kolegų ir partnerių tinklą paslaugoms teikti, kaip nurodyta 16 ir 17 straipsniuose;

(d) atkreipia TKST dėmesį į visus probleminius klausimus, susijusius su šio reglamento įgyvendinimu ir rekomendacinių dokumentų, rekomendacijų ir raginimų imtis veiksmų įgyvendinimu;

(e) praneša apie kibernetines grėsmes, su kuriomis susiduria Sąjungos institucijos, įstaigos ir agentūros, ir prisideda prie ES informuotumo apie kibernetinę padėtį.

3. CERT-EU prisideda prie Jungtinio kibernetinio saugumo padalinio, sukurto pagal 2021 m. birželio 23 d. Komisijos rekomendaciją, veiklos, be kita ko, šiose srityse:

(a) parengties, incidentų koordinavimo, keitimosi informacija ir reagavimo į krizes techniniu lygmeniu su Sąjungos institucijomis, įstaigomis ir agentūromis susijusiais atvejais;

(b) operatyvinio bendradarbiavimo reagavimo į kompiuterių saugumo incidentus tarnybų (CSIRT) tinkle, be kita ko, savitarpio pagalbos klausimais, ir su platesne kibernetinio saugumo bendruomene srityje;

(c) žvalgybos informacijos apie kibernetines grėsmes, įskaitant informuotumą apie padėtį, srityje;

(d) bet kurio klausimo, kuriam reikalingos CERT-EU techninės kibernetinio saugumo žinios, srityje.

4. CERT-EU vykdo struktūrinį bendradarbiavimą su Europos Sąjungos kibernetinio saugumo agentūra pajėgumų stiprinimo, operatyvinio bendradarbiavimo ir ilgalaikės strateginės kibernetinių grėsmių analizės srityse pagal Europos Parlamento ir Tarybos reglamentą (ES) 2019/881.

5. CERT-EU gali teikti šias paslaugas, kurios nėra apibūdintos jos paslaugų kataloge (toliau – apmokestinamosios paslaugos):

(a) paslaugas, kuriomis remiamas Sąjungos institucijų, įstaigų ir agentūrų IT aplinkos kibernetinis saugumas, išskyrus 2 dalyje nurodytas paslaugas, teikiamas remiantis susitarimais dėl paslaugų lygio ir atsižvelgiant į turimus išteklius;

(b) paslaugas, kuriomis remiamos Sąjungos institucijų, įstaigų ir agentūrų kibernetinio saugumo operacijos ar projektai, išskyrus tuos, kuriais jos siekia apsaugoti savo IT aplinką, teikiamas remiantis rašytiniais susitarimais ir gavus išankstinį TKST pritarimą;

(c) paslaugas, kuriomis remiamas organizacijų, kurios nėra Sąjungos institucijos, įstaigos ir agentūros, bet glaudžiai bendradarbiauja su jomis bendradarbiauja, pavyzdžiui, vykdo pagal Sąjungos teisę pavestas užduotis ar pareigas, IT aplinkos saugumas, teikiamas remiantis rašytiniais susitarimais ir iš anksto gavus TKST pritarimą.

6. CERT-EU gali rengti kibernetinio saugumo pratybas arba rekomenduoti dalyvauti vykdomose pratybose, kai tinkama glaudžiai bendradarbiaudama su Europos

Sąjungos kibernetinio saugumo agentūra, kad patikrintų Sąjungos institucijų, įstaigų ir agentūrų kibernetinio saugumo lygį.

7. CERT-EU gali teikti pagalbą Sąjungos institucijoms, įstaigoms ir agentūroms dėl incidentų įslaptintoje IT aplinkoje, jei atitinkamas dalyvis to aiškiai paprašo.

13 straipsnis
Rekomendaciniai dokumentai, rekomendacijos ir raginimai imtis veiksmų

1. CERT-EU padeda įgyvendinti šį reglamentą, teikdamas:

   (a) raginimus imtis veiksmų, kuriuose aprašomos skubios saugumo priemonės, kurių Sąjungos institucijos, įstaigos ir agentūros raginamos imtis per nustatytą laikotarpį;

   (b) pasiūlymus TKST dėl rekomendacinių dokumentų, skirtų visoms Sąjungos institucijoms, įstaigoms ir agentūroms arba jų daliai;

   (c) pasiūlymus TKST dėl atskiroms Sąjungos institucijoms, įstaigoms ir agentūroms skirtų rekomendacijų.

2. Rekomendaciniai dokumentai ir rekomendacijos gali apimti:

   (a) kibernetinio saugumo rizikos valdymo ir pagrindinių kibernetinio saugumo standartų laikymosi užtikrinimo būdus arba patobulinimus šiose srityse,

   (b) brandos vertinimo ir kibernetinio saugumo planų sąlygas ir,

   (c) kai tinkama, bendrų technologijų, architektūros ir susijusios geriausios praktikos naudojimą siekiant užtikrinti sąveiką ir bendrus standartus, kaip apibrėžta Direktyvos [pasiūlymas dėl TIS 2] 4 straipsnio 10 dalyje.

3. TKST CERT-EU siūlymu gali priimti rekomendacinius dokumentus arba rekomendacijas.

4. TKST gali nurodyti CERT-EU paskelbti, atsiimti arba pakeisti pasiūlymą dėl rekomendacinių dokumentų ar rekomendacijų arba kvietimo imtis veiksmų.

14 straipsnis
CERT-EU vadovas

CERT-EU vadovas reguliariai teikia ataskaitas TKST ir TKST pirmininkui apie CERT-EU veiklos rezultatus, finansinį planavimą, pajamas, biudžeto vykdymą, susitarimus dėl paslaugų lygio ir sudarytus rašytinius susitarimus, bendradarbiavimą su kolegomis ir partneriais ir darbuotojų vykdomas misijas, įskaitant 10 straipsnio 1 dalyje nurodytas ataskaitas.

15 straipsnis

Finansiniai ir personalo formavimo klausimai

1. Komisija, gavusi vieningą TKST pritarimą, skiria CERT-EU vadovą. Su TKST konsultuojamasi visais procedūros etapais prieš paskiriant CERT-EU vadovą, visų pirma rengiant pranešimus apie laisvas darbo vietas, nagrinėjant paraiškas ir skiriant atrankos komisijas dėl šios pareigybės.

2. Taikydamas administracines ir finansines procedūras, CERT-EU vadovas vadovaujasi Komisijos nurodymais.

3. CERT-EU užduotys ir veikla, įskaitant pagal 12 straipsnio 2, 3, 4, 6 dalis ir 13 straipsnio 1 dalį CERT-EU teikiamas paslaugas Sąjungos institucijoms, įstaigoms ir agentūroms, finansuojamas pagal daugiametės finansinės programos išlaidų kategoriją, skirtą Europos viešajam administravimui, finansuojamos pagal atskirą Komisijos biudžeto eilutę. CERT-EU paskirti etatai išsamiai nurodomi Komisijos etatų plano išnašoje.

4. Kitos nei 3 dalyje nurodytos Sąjungos institucijos, įstaigos ir agentūros pagal tą 3 dalį skiria CERT-EU metinį finansinį įnašą CERT-EU teikiamų paslaugų sąnaudoms padengti. Atitinkami įnašai nustatomi remiantis TKST pateiktomis gairėmis ir dėl jų kiekvienas subjektas ir CERT-EU susitaria paslaugų lygio susitarimuose. Įnašai sudaro teisingą ir proporcingą visų suteiktų paslaugų sąnaudų dalį. Jos gaunamos pagal 3 dalyje nurodytą atskirą biudžeto eilutę kaip asignuotosios pajamos, kaip numatyta Europos Parlamento ir Tarybos reglamento (ES, Euratomas) 2018/1046[8] 21 straipsnio 3 dalies c punkte.

5. Su 12 straipsnio 5 dalyje apibrėžtomis užduotimis susijusios išlaidos susigrąžinamos iš CERT-EU paslaugas gaunančių Sąjungos institucijų, įstaigų ir agentūrų. Pajamos priskiriamos išlaidoms padengti skirtoms biudžeto eilutėms.

16 straipsnis

CERT-EU bendradarbiavimas su partneriais iš valstybių narių

1. CERT-EU bendradarbiauja ir keičiasi informacija su atitinkamais nacionaliniais partneriais iš valstybių narių, įskaitant CERT, nacionalinius kibernetinio saugumo centrus, CSIRT ir Direktyvos [pasiūlymas dėl TIS 2] 8 straipsnyje nurodytus bendrus kontaktinius asmenis, klausimais, susijusiais su kibernetinėmis grėsmėmis, pažeidžiamumu ir incidentais, galimomis atsakomosiomis priemonėmis, ir visais klausimais, susijusiais su Sąjungos institucijų, įstaigų ir agentūrų IT aplinkos apsaugos gerinimu, be kita ko, pasitelkiant Direktyvos [pasiūlymas dėl TIS 2] 13 straipsnyje nurodytą CSIRT tinklą.

2. CERT-EU gali keistis su incidentais susijusia informacija su atitinkamais partneriais iš valstybių narių, kad būtų lengviau nustatyti panašias kibernetines grėsmes ar

[8] 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).

incidentus be nukentėjusio dalyvio sutikimo. CERT-EU gali keistis su incidentu susijusia informacija, kurioje atskleidžiama kibernetinio saugumo incidento taikinio tapatybė, tik gavusi nukentėjusio dalyvio sutikimą.

17 straipsnis
CERT-EU bendradarbiavimas su partneriais iš ne valstybių narių

1. CERT-EU gali bendradarbiauti su partneriais iš ne valstybių narių, įskaitant sektoriaus partnerius, klausimais, susijusiais su priemonėmis ir metodais, pavyzdžiui, specialia metodika, taktika, procedūromis ir geriausios praktikos pavyzdžiais, taip pat su kibernetinėmis grėsmėmis bei pažeidžiamumu. CERT-EU dėl bet kokio bendradarbiavimo su tokiais partneriais, be kita ko, sistemose, kuriose ES nepriklausančių šalių partneriai bendradarbiauja su atitinkamais nacionaliniais partneriais iš valstybių narių, siekia gauti išankstinį TKST pritarimą.

2. CERT-EU gali bendradarbiauti su kitais partneriais, pavyzdžiui, komerciniais subjektais, tarptautinėmis organizacijomis, ne Europos Sąjungos nacionaliniais subjektais arba atskirais ekspertais, kad surinktų informaciją apie bendro pobūdžio ir konkrečias kibernetines grėsmes, pažeidžiamumą ir galimas atsakomąsias priemones. Kad galėtų platesniu mastu bendradarbiauti su tokiais partneriais CERT-EU turi gauti išankstinį TKST pritarimą.

3. CERT-EU, gavęs nuo incidento nukentėjusio dalyvio sutikimą, gali teikti su incidentu susijusią informaciją partneriams, kurie gali prisidėti prie jo analizės.

V skyrius
BENDRADARBIAVIMAS IR PAREIGA TEIKTI ATASKAITAS

18 straipsnis
Duomenų tvarkymas

1. CERT-EU ir Sąjungos institucijos, įstaigos ir agentūros laikosi pareigos saugoti profesinę paslaptį pagal Sutarties dėl Europos Sąjungos veikimo 339 straipsnį arba lygiavertes taikytinas sistemas.

2. Paraiškoms dėl galimybės visuomenei susipažinti su CERT-EU turimais dokumentais taikomos Europos Parlamento ir Tarybos reglamento (EB) Nr. 1049/2001[9] nuostatos, įskaitant tame reglamente nustatytą pareigą konsultuotis su kitomis Sąjungos institucijomis, įstaigomis ir agentūromis, kai prašymas susijęs su jų dokumentais.

3. Pagal šį reglamentą atliekamam asmens duomenų tvarkymui taikomas Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725.

[9] 2001 m. gegužės 30 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1049/2001 dėl galimybės visuomenei susipažinti su Europos Parlamento, Tarybos ir Komisijos dokumentais (OL L 145, 2001 5 31, p. 43).

4. CERT-EU ir Sąjungos institucijos, įstaigos ir agentūros turėtų tvarkyti informaciją pagal taisykles, nustatytas [siūlomas reglamentas dėl informacijos saugumo].

5. Apie bet kokius ryšius su CERT-EU, kuriuos inicijuoja arba siekia inicijuoti nacionalinės saugumo ir žvalgybos tarnybos, turėtų būti nepagrįstai nedelsiant pranešama Komisijos Saugumo direktoratui ir TKST pirmininkui.

19 straipsnis
Pareiga dalytis informacija

1. Kad CERT-EU galėtų koordinuoti pažeidžiamumų valdymą ir reagavimą į incidentus, ji gali prašyti Sąjungos institucijų, įstaigų ir agentūrų pateikti jai informaciją iš savo atitinkamų IT sistemų aprašų, kuri yra svarbi CERT-EU paramos atžvilgiu. Institucija, įstaiga ar agentūra, į kurią kreipiamasi, nepagrįstai nedelsdama perduoda prašomą informaciją ir visus vėlesnius jos atnaujinimus.

2. Sąjungos institucijos, įstaigos ir agentūros CERT-EU prašymu nepagrįstai nedelsdamos suteikia jai skaitmeninę informaciją, sukurtą naudojant elektroninius įtaisus, susijusius su atitinkamais incidentais. CERT-EU gali išsamiau paaiškinti, kokios rūšies skaitmeninės informacijos jai reikia informuotumo apie padėtį ir reagavimo į incidentus tikslais.

3. CERT-EU gali keistis su incidentu susijusia informacija, kurioje atskleidžiama nuo kibernetinio saugumo incidento nukentėjusios Sąjungos institucijos, įstaigos ar agentūros tapatybė, tik gavusi to subjekto sutikimą. CERT-EU gali keistis su incidentu susijusia informacija, kurioje atskleidžiama kibernetinio saugumo incidento taikinio tapatybė, tik gavusi dėl incidento nukentėjusio subjekto sutikimą.

4. Pareigos dalytis netaikomos ES įslaptintai informacijai (ESĮI) ir informacijai, kurią Sąjungos institucijai, įstaigai ar agentūrai pateikė valstybės narės saugumo ar žvalgybos tarnyba arba teisėsaugos agentūra, keldama aiškią sąlygą, kad ja nebūtų dalijamasi su CERT-EU.

20 straipsnis
Pareiga pranešti

1. Visos Sąjungos institucijos, įstaigos ir agentūros pateikia CERT-EU pirminį pranešimą apie reikšmingas kibernetines grėsmes, reikšmingą pažeidžiamumą ir reikšmingus incidentus nepagrįstai nedelsdamos ir bet kuriuo atveju ne vėliau kaip per 24 valandas nuo tada, kai apie juos sužino.

   Tinkamai pagrįstais atvejais ir sutarus su CERT-EU, atitinkama Sąjungos institucija, įstaiga ar agentūra gali nukrypti nuo ankstesnėje dalyje nustatyto termino.

2. Sąjungos institucijos, įstaigos ir agentūros taip pat nepagrįstai nedelsdamos pateikia CERT-EU atitinkamą techninę informaciją apie kibernetines grėsmes, pažeidžiamumą ir incidentus, kuri suteikia galimybę incidentus aptikti, į juos reaguoti arba imtis jų poveikio švelninimo priemonių. Pranešime pateikiama ši informacija (jei turima):

(a) atitinkami užvaldymo rodikliai;

(b) atitinkami aptikimo mechanizmai;

(c) galimas poveikis;

(d) atitinkamos poveikio švelninimo priemonės.

3. CERT-EU kas mėnesį teikia ENISA apibendrinamąją ataskaitą, įskaitant nuasmenintus ir apibendrintus duomenis apie reikšmingas kibernetines grėsmes, reikšmingą pažeidžiamumą ir reikšmingus incidentus, apie kuriuos pranešta pagal 1 dalį.

4. TKST gali paskelbti rekomendacinius dokumentus arba rekomendacijas dėl pranešimo sąlygų ir turinio. CERT-EU platina atitinkamą techninę informaciją, kad Sąjungos institucijos, įstaigos ir agentūros galėtų aktyviai aptikti incidentus, reaguoti į juos arba imtis rizikos mažinimo priemonių.

5. Pareigos pranešti netaikomos ESĮI ir informacijai, kurią Sąjungos institucijai, įstaigai ar agentūrai pateikė valstybės narės saugumo ar žvalgybos tarnyba arba teisėsaugos agentūra, keldama aiškią sąlygą, kad ja nebūtų dalijamasi su CERT-EU.

21 straipsnis

Reagavimo į incidentus koordinavimas ir bendradarbiavimas reikšmingų incidentų atveju

1. CERT-EU, veikdamas kaip keitimosi kibernetinio saugumo informacija ir reagavimo į incidentus koordinavimo centras, palengvina keitimąsi informacija apie kibernetines grėsmes, pažeidžiamumą ir incidentus tarp:

(a) Sąjungos institucijų, įstaigų ir agentūrų;

(b) 16 ir 17 straipsniuose nurodytų partnerių.

2. CERT-EU palengvina Sąjungos institucijų, įstaigų ir agentūrų reagavimo į incidentus koordinavimą, susijusį, be kita ko, su:

(a) nuoseklia išorės komunikacija;

(b) savitarpio pagalba;

(c) optimaliu veiklos išteklių naudojimu;

(d) koordinavimu su kitais reagavimo į krizes mechanizmais Sąjungos lygmeniu.

3. CERT-EU teikia paramą Sąjungos institucijoms, įstaigoms ir agentūroms, siekiant didinti jų informuotumą apie padėtį, susijusią su kibernetinėmis grėsmėmis, pažeidžiamumu ir incidentais.

4. TKST parengia reagavimo į incidentus koordinavimo ir bendradarbiavimo reikšmingų incidentų atveju gaires. Kai įtariama, kad incidentas yra nusikalstamas, CERT-EU pataria, kaip pranešti apie incidentą teisėsaugos institucijoms.

22 straipsnis
Dideli išpuoliai

1. CERT-EU koordinuoja Sąjungos institucijų, įstaigų ir agentūrų atsaką į didelius išpuolius. Ji tvarko techninių ekspertinių žinių, kurių reikėtų reaguojant į incidentus tokių išpuolių atveju, aprašą.

2. Sąjungos institucijos, įstaigos ir agentūros prisideda prie techninių ekspertinių žinių aprašo, pateikdamos kasmet atnaujinamą atitinkamose jų organizacijose turimų ekspertų sąrašą, kuriame išsamiai nurodomi jų konkretūs techniniai įgūdžiai.

3. Gavęs atitinkamų Sąjungos institucijų, įstaigų ir agentūrų pritarimą, CERT-EU taip pat gali pakviesti ekspertus iš 2 dalyje nurodyto sąrašo prisidėti reaguojant į didelį išpuolį valstybėje narėje, laikantis Jungtinio kibernetinio saugumo padalinio veiklos procedūrų.

VI skyrius
BAIGIAMOSIOS NUOSTATOS

23 straipsnis
Pradinis biudžeto perskirstymas

Komisija siūlo perkelti atitinkamų Sąjungos institucijų, įstaigų ir agentūrų darbuotojus ir finansinius išteklius į Komisijos biudžetą. Perskirstymas įsigalioja tuo pačiu metu kaip ir pirmasis biudžetas, priimtas įsigaliojus šiam reglamentui.

24 straipsnis
Peržiūra

1. TKST, padedant CERT-EU, periodiškai tekia Komisijai šio reglamento įgyvendinimo ataskaitą. TKST taip pat gali teikti rekomendacijas Komisijai siūlyti šio reglamento pakeitimus.

2. Komisija pateikia Europos Parlamentui ir Tarybai šio reglamento įgyvendinimo ataskaitą ne vėliau kaip per 48 mėnesius nuo šio reglamento įsigaliojimo, o vėliau – kas trejus metus.

3. Komisija ne anksčiau kaip po penkerių metų nuo šio reglamento įsigaliojimo įvertina jo veikimą ir pateikia ataskaitą Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui.

25 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 Briuselyje

Europos Parlamento vardu
Pirmininkas

Tarybos vardu
Pirmininkas

FINANSINĖ TEISĖS AKTO PASIŪLYMO PAŽYMA

1. PASIŪLYMO (INICIATYVOS) STRUKTŪRA

1.1. Pasiūlymo (iniciatyvos) pavadinimas

1.2. Atitinkama (-os) politikos sritis (-ys)

1.3. Pasiūlymas (iniciatyva) susijęs (-usi) su:

1.4. Tikslas (-ai)

1.4.1. Bendrasis (-ieji) tikslas (-ai)

1.4.2. Konkretus (-ūs) tikslas (-ai)

1.4.3. Numatomas (-i) rezultatas (-ai) ir poveikis

1.4.4. Veiklos rezultatų rodikliai

1.5. Pasiūlymo (iniciatyvos) pagrindas

1.5.1. Trumpalaikiai arba ilgalaikiai poreikiai, įskaitant išsamų pradinio iniciatyvos įgyvendinimo etapo tvarkaraštį.

1.5.2. Sąjungos dalyvavimo pridėtinė vertė (gali būti susijusi su įvairiais veiksniais, pvz., koordinavimo nauda, teisiniu tikrumu, didesniu veiksmingumu ar papildomumu). Šiame punkte „Sąjungos dalyvavimo pridėtinė vertė“ – dalyvaujant Sąjungai užtikrinama vertė, papildanti vertę, kuri būtų užtikrinta vien valstybių narių veiksmais.

1.5.3. Panašios patirties išvados

1.5.4. Suderinamumas su daugiamete finansine programa ir galima sąveika su kitomis atitinkamomis priemonėmis

1.5.5. Įvairių turimų finansavimo galimybių, įskaitant perskirstymo galimybę, vertinimas

1.6. Pasiūlymo (iniciatyvos) trukmė ir finansinis poveikis

1.7. Numatytas (-i) valdymo būdas (-ai)

2. VALDYMO PRIEMONĖS

2.1. Stebėsenos ir ataskaitų teikimo taisyklės

2.2. Valdymo ir kontrolės sistema (-os)

2.2.1. Valdymo būdo (-ų), finansavimo įgyvendinimo mechanizmo (-ų), mokėjimo tvarkos ir siūlomos kontrolės strategijos pagrindimas

2.2.2. Informacija apie nustatytą riziką ir jai sumažinti įdiegtą (-as) vidaus kontrolės sistemą (-as)

2.2.3. Kontrolės išlaidų efektyvumo apskaičiavimas ir pagrindimas (kontrolės sąnaudų ir susijusių valdomų lėšų vertės santykis) ir numatomo klaidų rizikos lygio vertinimas (atliekant mokėjimą ir užbaigiant programą)

2.3. Sukčiavimo ir pažeidimų prevencijos priemonės

3. NUMATOMAS PASIŪLYMO (INICIATYVOS) FINANSINIS POVEIKIS

3.1. Daugiametės finansinės programos išlaidų kategorija (-os) ir biudžeto išlaidų eilutė (-ės), kurioms daromas poveikis

3.2. Numatomas pasiūlymo finansinis poveikis asignavimams

3.2.1. Numatomo poveikio veiklos asignavimams santrauka

3.2.2. Numatomas veiklos asignavimais finansuojamas atliktas darbas

3.2.3. Numatomo poveikio administraciniams asignavimams santrauka

3.2.4. Suderinamumas su dabartine daugiamete finansine programa

3.2.5. Trečiųjų šalių įnašai

3.3. Numatomas poveikis pajamoms

FINANSINĖ TEISĖS AKTO PASIŪLYMO PAŽYMA

1. PASIŪLYMO (INICIATYVOS) STRUKTŪRA

1.1. Pasiūlymo (iniciatyvos) pavadinimas

Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento, kuriuo nustatomos priemonės aukštam bendram kibernetinio saugumo lygiui Sąjungos institucijose, įstaigose, organuose ir agentūrose užtikrinti

1.2. Atitinkama (-os) politikos sritis (-ys)

Europos viešasis administravimas

Pasiūlymas susijęs su priemonėmis, kuriomis užtikrinamas aukštas bendras kibernetinio saugumo lygis Sąjungos institucijose, įstaigose ir agentūrose

1.3. Pasiūlymas (iniciatyva) susijęs (-usi) su:

☑nauju veiksmu

☐ nauju veiksmu, kai bus įgyvendintas bandomasis projektas ir (arba) atlikti parengiamieji veiksmai[10]

☐ esamo veiksmo galiojimo pratęsimu

☑ vieno ar daugiau veiksmų sujungimu arba nukreipimu į kitą / naują veiksmą

1.4. Tikslas (-ai)

1.4.1. Bendrasis (-ieji) tikslas (-ai)

– Sukurti sistemą, kuria būtų užtikrintas aukštas bendras kibernetinio saugumo lygis Sąjungos institucijose, įstaigose ir agentūrose.

– Suteikti naują CERT-EU teisinį pagrindą, kad būtų sustiprinti jo įgaliojimai ir finansavimas.

1.4.2. Konkretus (-ūs) tikslas (-ai)

(1) Nustatyti Sąjungos institucijų, įstaigų ir agentūrų įpareigojimus sukurti vidaus rizikos kibernetiniam saugumui valdymo ir kontrolės sistemą.

(2) Nustatyti Sąjungos institucijų, įstaigų ir agentūrų įpareigojimus pranešti apie savo rizikos kibernetiniam saugumui valdymo ir kontrolės sistemą ir apie kibernetinius incidentus.

[10] Kaip nurodyta Finansinio reglamento 58 straipsnio 2 dalies a arba b punkte.

(3) Nustatyti Sąjungos institucijų, įstaigų ir agentūrų kibernetinio saugumo centro (CERT-EU) ir Tarpinstitucinės kibernetinio saugumo tarybos (TKST) organizavimo ir veiklos taisykles.

(4) Prisidėti prie Jungtinio kibernetinio saugumo padalinio veiklos

1.4.3. Numatomas (-i) rezultatas (-ai) ir poveikis

Nurodyti poveikį, kurį pasiūlymas (iniciatyva) turėtų padaryti tiksliniams gavėjams (tikslinėms grupėms).

– Vidaus kibernetinio saugumo rizikos valdymo ir kontrolės sistemos, pagrindiniai kibernetinio saugumo standartai, reguliarūs brandos vertinimai ir kibernetinio saugumo planai Sąjungos institucijose, įstaigose ir agentūrose – Sąjungos institucijų, įstaigų ir agentūrų kibernetinio atsparumo ir reagavimo į incidentus pajėgumų didinimas – CERT-EU modernizavimas – Indėlis į Jungtinio kibernetinio saugumo padalinio veiklą

1.4.4. Veiklos rezultatų rodikliai

Nurodyti pažangos ir pasiekimų stebėsenos rodiklius.

– Sąjungos institucijose, įstaigose ir agentūrose taikomos sistemos ir pagrindiniai standartai, reguliarūs brandos vertinimai ir kibernetinio saugumo planai – Geresnis incidentų valdymas – Didesnis Sąjungos institucijų, įstaigų ir agentūrų vyresniosios vadovybės informuotumas apie riziką kibernetiniam saugumui – IRT saugumo išlaidų lygio, išreikšto visų IRT išlaidų procentine dalimi, nustatymas – Tvirtas TKST ir CERT-EU vadovavimas – Aktyvesnis keitimasis informacija tarp Sąjungos institucijų, įstaigų ir agentūrų, taip pat su atitinkamomis įstaigomis ir suinteresuotaisiais subjektais ES – Glaudesnis bendradarbiavimas kibernetinio saugumo srityje su atitinkamomis ES įstaigomis ir suinteresuotaisiais subjektais per CERT-EU ir ENISA

1.5. Pasiūlymo (iniciatyvos) pagrindas

1.5.1. Trumpalaikiai arba ilgalaikiai poreikiai, įskaitant išsamų pradinio iniciatyvos įgyvendinimo etapo tvarkaraštį.

Pasiūlymu siekiama padidinti Sąjungos institucijų, įstaigų ir agentūrų kibernetinio atsparumo lygį, sumažinti šių subjektų atsparumo lygio skirtumus ir padidinti bendro

informuotumo apie padėtį lygį bei kolektyvinius pasirengimo ir reagavimo pajėgumus.

Pasiūlymas visiškai dera su kitomis susijusiomis iniciatyvomis, visų pirma su pasiūlymu dėl Direktyvos dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria panaikinama Direktyva (ES) 2016/1148 [pasiūlymas dėl TIS 2].

Pasiūlymas yra esminė ES saugumo sąjungos strategijos ir ES skaitmeninio dešimtmečio kibernetinio saugumo strategijos dalis.

Numatoma, kad reglamentą Europos Komisija pasiūlys 2021 m. spalio mėn., Europos Parlamentas ir Taryba turėtų jį priimti 2022 m., o nuostatos bus taikomos nuo reglamento įsigaliojimo dienos. Numatoma, kad šioje finansinėje teisės akto pasiūlymo pažymoje nurodytas finansinis poveikis ir poveikis žmogiškiesiems ištekliams pradės reikštis 2023 m. Parengiamasis laikotarpis jau prasidėjo 2021 m., tačiau 2021 ir 2022 m. parengiamajai veiklai pasiūlymas nedaro finansinio poveikio.

1.5.2. Sąjungos dalyvavimo pridėtinė vertė (gali būti susijusi su įvairiais veiksniais, pvz., koordinavimo nauda, teisiniu tikrumu, didesniu veiksmingumu ar papildomumu). Šiame punkte „Sąjungos dalyvavimo pridėtinė vertė“ – dalyvaujant Sąjungai užtikrinama vertė, papildanti vertę, kuri būtų užtikrinta vien valstybių narių veiksmais.

Priežastys imtis Europos lygmens veiksmų (*ex ante*)

2019–2021 m. labai padaugėjo reikšmingų incidentų, darančių poveikį Sąjungos institucijoms, įstaigoms ir agentūroms, kuriuos sukėlė vadinamieji aukšto lygio tęstinės grėsmės subjektai. Per 2021 m. pirmąjį pusmetį reikšmingų incidentų įvyko tiek, kiek per visus 2020 m. Tai taip pat matyti iš to, kad 2020 m. CERT-EU išanalizuotų kriminalistinių vaizdų (paveiktų sistemų ar įrenginių turinio momentinių nuotraukų), palyginti su 2019 m., padaugėjo tris kartus, o reikšmingų incidentų skaičius, palyginti su 2018 m., išaugo daugiau nei dešimt kartų.

Įvairių subjektų kibernetinio saugumo brandos lygis labai skiriasi[11]. Šiuo reglamentu užtikrinama, kad visos Sąjungos institucijos, įstaigos ir agentūros įgyvendintų pagrindines saugumo priemones ir bendradarbiautų tarpusavyje siekdamos atviro ir veiksmingo Sąjungos administracijos veikimo.

Saugotinos sistemos priklauso Sąjungos institucijų, įstaigų ir agentūrų autonomijai ir yra jų valdomos; valstybės narės negalėjo sukurti siūlomų veiksmų.

1.5.3. Panašios patirties išvados

TIS direktyva buvo pirmoji horizontalioji vidaus rinkos priemonė, kuria siekiama didinti Sąjungos tinklų ir sistemų atsparumą su kibernetiniu saugumu susijusiai rizikai. Nuo jos įsigaliojimo 2016 m. ji labai padėjo didinti bendrą valstybių narių

[11] Nuoroda: [Europos Audito Rūmų specialioji ataskaita dėl kibernetinio saugumo Sąjungos institucijose, įstaigose ir agentūrose].

kibernetinio saugumo lygį. Pasiūlymu dėl TIS 2 direktyvos siekiama toliau tobulinti šias priemones.

Reglamentu siekiama nustatyti panašias priemones, skirtas Sąjungos institucijoms, įstaigoms ir agentūroms.

1.5.4. Suderinamumas su daugiamete finansine programa ir galima sąveika su kitomis atitinkamomis priemonėmis

Pasiūlymas dera su daugiamete finansine programa ir yra esminė ES saugumo sąjungos strategijos, taip pat ES skaitmeninio dešimtmečio kibernetinio saugumo strategijos dalis.

Pasiūlyme numatoma taikyti Sąjungos institucijoms, įstaigoms ir agentūroms priemones aukštam bendram kibernetinio saugumo lygiui užtikrinti. Pasiūlymas atitinka pasiūlymą dėl Direktyvos dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria panaikinama Direktyva (ES) 2016/1148 [pasiūlymas dėl TIS 2].

1.5.5. Įvairių turimų finansavimo galimybių, įskaitant perskirstymo galimybę, vertinimas

CERT-EU užduotims valdyti reikia specialių profilių ir papildomo darbo krūvio, kurio negalima absorbuoti nepadidinus žmogiškųjų ir finansinių išteklių.

1.6. Pasiūlymo (iniciatyvos) trukmė ir finansinis poveikis

☐ **trukmė ribota**

– ☐ galioja nuo MMMM [MM DD] iki MMMM [MM DD],

– ☐ įsipareigojimų asignavimų finansinis poveikis nuo MMMM iki MMMM, o mokėjimų asignavimų – nuo MMMM iki MMMM;

☑ **trukmė neribota**

– Finansinis poveikis turėtų prasidėti nuo pirmojo biudžeto, priimto įsigaliojus reglamentui. Ištekliai iš Sąjungos institucijų ir pagrindinių įstaigų būtų perskirstyti Komisijai pirmaisiais metais, kurie laikomi pereinamaisiais metais; šis ir kitas (per)skirstymas bus vykdomas sudarant metinius biudžetus. Jei reglamentas bus priimtas 2022 m., 2023 finansiniai metai bus pereinamasis laikotarpis, o 2024 m. veiks visu mastu.

1.7. Numatytas (-i) valdymo būdas (-ai)[12]

☑ **Tiesioginis valdymas**, vykdomas Komisijos ir kiekvienos Sąjungos institucijos, įstaigos ir agentūros

– ☑ padalinių, įskaitant Sąjungos delegacijų darbuotojus;

– ☐ vykdomųjų įstaigų.

☐ **Pasidalijamasis valdymas** kartu su valstybėmis narėmis

☐ **Netiesioginis valdymas**, biudžeto vykdymo užduotis pavedant:

– ☐ trečiosioms valstybėms arba jų paskirtiems organams;

– ☐ tarptautinėms organizacijoms ir jų agentūroms (nurodyti);

– ☐ EIB ir Europos investicijų fondui;

– ☐ Finansinio reglamento 70 ir 71 straipsniuose nurodytoms įstaigoms;

– ☐ viešosios teisės reglamentuojamoms įstaigoms;

– ☐ įstaigoms, kurių veiklą reglamentuoja privatinė teisė ir kurioms pavesta teikti viešąsias paslaugas, jeigu jos pateikia pakankamas finansines garantijas;

– ☐ įstaigoms, kurių veiklą reglamentuoja valstybės narės privatinė teisė, kurioms pavesta įgyvendinti viešojo ir privačiojo sektorių partnerystę ir kurios pateikia pakankamas finansines garantijas;

[12] Informacija apie valdymo būdus ir nuorodos į Finansinį reglamentą pateikiamos svetainėje „BudgWeb“ https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

– ☐ atitinkamame pagrindiniame akte nurodytiems asmenims, kuriems pavesta vykdyti konkrečius veiksmus BUSP srityje pagal ES sutarties V antraštinę dalį.

– *Jei nurodomas daugiau kaip vienas valdymo būdas, išsamią informaciją pateikti šio punkto pastabų skiltyje.*

Pastabos

Taikydamas administracines ir finansines procedūras, CERT-EU vadovaujasi Komisijos nurodymais.

Papildomi ištekliai, susiję su reglamento projektu:

Įgyvendinus reglamento projekto 12 ir 13 straipsnius, bus sudarytas išplėstas paslaugų katalogas su papildomomis pagrindinėmis paslaugomis. Visapusiškai veikiant reikės šių papildomų išteklių (iki DFP pabaigos 2027 m. pabaigoje): 21 etato vieneto ir 14,05 mln. EUR.

Papildomi biudžeto ištekliai įvairioms užduotims paskirstyti taip:

(a) 12 straipsnio 2 dalies a, b, c ir e punktuose nurodytoms Sąjungos institucijoms, įstaigoms ir agentūroms skirtoms užduotims atlikti: 13,75 etato vienetų ir 11,275 mln. EUR;

(b) 12 straipsnio 3 dalyje nurodytoms užduotims (indėlis į Jungtinio kibernetinio saugumo padalinį) atlikti: 2 etato vienetai ir 381 000 EUR;

(c) 12 straipsnio 4 dalyje nurodytoms užduotims (struktūrizuotas bendradarbiavimas su ENISA) atlikti: 0,25 etato vieneto ir 236 000 EUR;

(d) 12 straipsnio 6 dalyje nurodytoms užduotims (kibernetinio saugumo pratybos) atlikti: 0,25 etato vieneto ir 79 000 EUR;

(e) 12 straipsnio 2 dalies d punkte ir 13 straipsnyje nurodytoms užduotims (reglamento įgyvendinimo analizė ir ataskaitų teikimas, rekomendacinių dokumentų, rekomendacijų ir raginimų imtis veiksmų rengimas) atlikti: 3,75 etato vienetų ir 2,079 mln. EUR.

(f) Užduotims, skirtoms padėti Tarpinstitucinės kibernetinio saugumo tarybos sekretoriatui, atlikti: 1 etato vienetas.

Dabartinių išteklių apžvalga ir perėjimas prie viso masto:

2021 m. rugsėjo mėn. CERT-EU veikė naudodamas šiuos išteklius:

nuolatiniai ir deleguotieji etatai: 14 etato vienetų,

– sutartininkai, finansuojami pagal susitarimus dėl paslaugų lygio: 24 etato vienetai,

– iš viso 38 etato vienetai.

2020 m. CERT-EU biudžetas buvo: 250 000 EUR iš Komisijos biudžeto, 3,5 mln. EUR iš asignuotųjų pajamų pagal susitarimus dėl paslaugų lygio. Iš viso: 3,75 mln. EUR. Tai sudarė

visą CERT-EU biudžetą, apimantį mokymą, aparatinę įrangą, programinę įrangą, užduotis, paramą, sutartininkus ir konferencijas.

Įsigaliojus reglamentui, numatoma, kad CERT-EU ištekliai ateityje bus:

– nuolatiniai etatai: 34 etato vienetai,

– sutartininkai: 15 etato vienetų,

– iš viso 49 etato vienetai, t. y. grynasis padidėjimas 11 etato vienetų.

Pasikeitus nuolatinių darbo vietų ir sutartininkų santykiui, sprendžiama problema, susijusi su kliūtimi įdarbinti ir išlaikyti vyresniuosius kibernetinio saugumo specialistus dėl jų trūkumo darbo rinkoje.

Be to, Komisijos Informatikos generaliniame direktorate reikės 1 etato vieneto sutartininko, kuris padėtų Tarpinstitucinei kibernetinio saugumo tarybai (TKST).

Taigi reglamentui įgyvendinti iš viso reikės 21 papildomo etato vieneto (20 etato vienetų CERT-EU ir 1 etato vienetas Komisijos Informatikos generaliniam direktoratui). Tai bus kompensuojama tuo pačiu metu sumažinus CERT-EU 9 etato vienetus sutartininkų, kurie anksčiau buvo finansuojami iš asignuotųjų pajamų pagal susitarimus dėl paslaugų lygio, skaičių.

2024 m. CERT-EU ir ES ne žmogiškiesiems ištekliams skirtas biudžetas po pereinamojo laikotarpio apims a–e punktuose išvardytas užduotis ir jį numatoma finansuoti taip:

– 8,921 mln. EUR per metus iš Sąjungos institucijų, finansuojamų pagal Sąjungos biudžeto 7 išlaidų kategoriją,

2,459 mln. EUR iš Sąjungos institucijų, įstaigų ir agentūrų, finansuojamų pagal Sąjungos biudžeto 1–6 išlaidų kategorijas,

–2 670 mln. EUR iš savo lėšomis finansuojamų Sąjungos institucijų, įstaigų ir agentūrų.

– Bendras CERT-EU biudžetas: 14,05 mln. EUR.

12 straipsnio 5 dalyje išvardytos užduotys jo paslaugų kataloge neaprašytos; tai yra apmokestinamosios paslaugos. Tai yra pagalbinės, palyginti mažos sumos, daugiausia laikinos, o šių paslaugų išlaidos bus susigrąžintos iš paslaugų gavėjų, sudarant susitarimus dėl paslaugų lygio arba rašytinius susitarimus.

Dėl įnašų CERT-EU personalui: Sąjungos institucijų ir pagrindinių įstaigų įnašas yra proporcingas atitinkamai organizacijos nuolatinių AD pareigybių daliai. Reikėtų išsiaiškinti, ar ECB ir EIB taip pat gali tinkamai prisidėti komandiruojant nuolatinius darbuotojus.

2. VALDYMO PRIEMONĖS

2.1. Stebėsenos ir ataskaitų teikimo taisyklės

Nurodyti dažnumą ir sąlygas.

Komisija, padedant TKST ir CERT-EU, periodiškai peržiūrės reglamento veikimą ir pirmą kartą ne vėliau kaip per 48 mėnesius nuo šio reglamento įsigaliojimo, o vėliau – kas trejus metus pateiks ataskaitą Europos Parlamentui ir Tarybai.

Atliekant peržiūras daugiausia būtų naudojami TKST ir CERT-EU duomenų šaltiniai. Be to, prireikus galėtų būti naudojamos konkrečios duomenų rinkimo priemonės, pvz., Sąjungos institucijų, įstaigų ir agentūrų, ENISA arba CSIRT tinklo apklausos.

2.2. Valdymo ir kontrolės sistema (-os)

2.2.1. Valdymo būdo (-ų), finansavimo įgyvendinimo mechanizmo (-ų), mokėjimo tvarkos ir siūlomos kontrolės strategijos pagrindimas

Pagal šį reglamentą vykdomi veiksmai bus valdomi kiekvienoje Sąjungos institucijoje, įstaigoje ir agentūroje pagal jų atitinkamas taikytinas taisykles ir reglamentus.

CERT-EU veiklos administracinis ir finansinis valdymas yra integruotas į Komisijos administraciją ir vykdomas laikantis jos taikomų valdymo ir įgyvendinimo mechanizmų, mokėjimo tvarkos ir kontrolės priemonių.

Komisijos vidaus auditorius CERT-EU atžvilgiu naudojasi tais pačiais įgaliojimais, kaip ir Komisijos padalinių atžvilgiu.

2.2.2. Informacija apie nustatytą riziką ir jai sumažinti įdiegtą (-as) vidaus kontrolės sistemą (-as)

Labai maža rizika, nes CERT-EU administraciniu požiūriu jau yra pavaldus Informatikos generaliniam direktoriui kaip Komisijos darbo grupė, o TKST modeliuojama pagal dabartinę CERT-EU valdančiąją tarybą. Taigi finansų valdymo ir vidaus kontrolės ekosistema jau veikia.

2.2.3. Kontrolės išlaidų efektyvumo apskaičiavimas ir pagrindimas (kontrolės sąnaudų ir susijusių valdomų lėšų vertės santykis) ir numatomo klaidų rizikos lygio vertinimas (atliekant mokėjimą ir užbaigiant programą)

Viešųjų pirkimų, finansų valdymo ir kontrolės procedūros jau įdiegtos ir gerai išbandytos. Kontrolės priemonių ekonominis efektyvumas ir klaidų rizikos lygiai atitinka kiekvienos Sąjungos institucijos, įstaigos ar agentūros, taip pat Komisijos kontrolės priemonių veiksmingumą ir klaidų rizikos lygius, taikomus CERT-EU veiklai.

2.3. Sukčiavimo ir pažeidimų prevencijos priemonės

Nurodyti dabartines arba numatytas prevencijos ir apsaugos priemones, pvz., išdėstytas Kovos su sukčiavimu strategijoje.

CERT-EU veiklai taikomos Komisijos finansų valdymo ir vidaus kontrolės sistemos.

Kad būtų kovojama su sukčiavimu, korupcija ir kita neteisėta veikla, be apribojimų taikomos 2013 m. rugsėjo 11 d. Europos Parlamento ir Tarybos reglamento (ES, Euratomas) Nr. 883/2013 dėl Europos kovos su sukčiavimu tarnybos (OLAF) atliekamų tyrimų nuostatos.

3. NUMATOMAS PASIŪLYMO (INICIATYVOS) FINANSINIS POVEIKIS

3.1. Daugiametės finansinės programos išlaidų kategorija (-os) ir biudžeto išlaidų eilutė (-ės), kurioms daromas poveikis

- Dabartinės biudžeto eilutės

Daugiametės finansinės programos išlaidų kategorijas ir biudžeto eilutes nurodyti eilės tvarka.

Daugiametės finansinės programos išlaidų kategorija	Biudžeto eilutė	Išlaidų rūšis	Įnašas			
	Numeris	DA / NDA[13]	ELPA šalių[14]	valstybių kandidačių [15]	trečiųjų valstybių	pagal Finansinio reglamento 21 straipsnio 2 dalies b punktą
1–6	Biudžeto eilutės, apimančios Sąjungos įnašus decentralizuotoms agentūroms ir įstaigoms	DA	NE	NE	NE	NE
7	Biudžeto eilutės, apimančios darbuotojų atlyginimus, IT išlaidas ir kitas administracines išlaidas įvairiuose ES biudžeto skirsniuose	NDA	NE	NE	NE	NE

- Prašomos sukurti naujos biudžeto eilutės

Daugiametės finansinės programos išlaidų kategorijas ir biudžeto eilutes nurodyti eilės tvarka.

Daugiametės finansinės programos išlaidų kategorija	Biudžeto eilutė	Išlaidų rūšis	Įnašas			
	Numeris	DA / NDA	ELPA šalių	valstybių kandidačių	trečiųjų valstybių	pagal Finansinio reglamento 21 straipsnio 2 dalies b punktą
	Nėra		TAIP / NE	TAIP / NE	TAIP / NE	TAIP / NE

[13] DA – diferencijuotieji asignavimai, NDA – nediferencijuotieji asignavimai.
[14] ELPA – Europos laisvosios prekybos asociacija.
[15] Valstybių kandidačių ir, kai taikoma, potencialių valstybių kandidačių iš Vakarų Balkanų.

3.2. Numatomas pasiūlymo finansinis poveikis asignavimams

3.2.1. Numatomo poveikio veiklos asignavimams santrauka

– ☐ Pasiūlymui (iniciatyvai) įgyvendinti veiklos asignavimai nenaudojami

– ☑ Pasiūlymui (iniciatyvai) įgyvendinti veiklos asignavimai naudojami taip:

mln. EUR (tūkstantųjų tikslumu)

Daugiametės finansinės programos išlaidų kategorija	1–6	Išlaidų kategorijos, apimančios įnašus decentralizuotoms agentūroms ir įstaigoms

GD: keli			**2023 m.**	**2024 m.**	**2025 m.**	**2026 m.**	**2027 m.**	**IŠ VISO**
○ Veiklos asignavimai								
Biudžeto eilutės, apimančios Sąjungos įnašus decentralizuotoms agentūroms (xx 10 xx xx)[16]	Įsipareigojimai	(1a)	2,459	2,459	2,459	2,459	2,459	12,293
	Mokėjimai	(2a)	2,459	2,459	2,459	2,459	2,459	12,293
Administracinio pobūdžio asignavimai, finansuojami iš konkrečių programų paketo lėšų[17]								
Biudžeto eilutė		(3)						
IŠ VISO asignavimų GD: keliems	Įsipareigojimai	=1a + 1b + 3	2,459	2,459	2,459	2,459	2,459	12,293
	Mokėjimai	=2a + 2b	2,459	2,459	2,459	2,459	2,459	12,293

[16] Pagal oficialią biudžeto nomenklatūrą.

[17] Techninė ir (arba) administracinė parama bei išlaidos ES programų ir (arba) veiksmų įgyvendinimui remti (buvusios BA eilutės), netiesioginiai moksliniai tyrimai, tiesioginiai moksliniai tyrimai.

		+3						

○ IŠ VISO veiklos asignavimų	Įsipareigojimai	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Mokėjimai	(5)	2,459	2,459	2,459	2,459	2,459	12,293
○ IŠ VISO administracinio pobūdžio asignavimų, finansuojamų iš konkrečių programų paketo lėšų		(6)						
IŠ VISO asignavimų pagal daugiametės finansinės programos 1–6 IŠLAIDŲ KATEGORIJAS	Įsipareigojimai	=4 + 6	2,459	2,459	2,459	2,459	2,459	12,293
	Mokėjimai	=5 + 6	2,459	2,459	2,459	2,459	2,459	12,293

<u>Jei pasiūlymas (iniciatyva) daro poveikį kelioms veiklos išlaidų kategorijoms, pakartokite pirmiau pateiktą dalį:</u>

○ IŠ VISO veiklos asignavimų (pagal visas veiklos išlaidų kategorijas)	Įsipareigojimai	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Mokėjimai	(5)	2,459	2,459	2,459	2,459	2,459	12,293
IŠ VISO administracinio pobūdžio asignavimų, finansuojamų iš konkrečių programų paketo lėšų (pagal visas veiklos išlaidų kategorijas)		(6)						
IŠ VISO asignavimų pagal daugiametės finansinės programos 1–6 IŠLAIDŲ KATEGORIJAS (Orientacinė suma)	Įsipareigojimai	=4 + 6	2,459	2,459	2,459	2,459	2,459	12,293
	Mokėjimai	=5 + 6	2,459	2,459	2,459	2,459	2,459	12,293

Daugiametės finansinės programos išlaidų kategorija	**7**	„Administracinės išlaidos“

Šią dalį pildyti naudojant administracinio pobūdžio biudžeto duomenų lentelę, kuri pirmiausia bus pateikta finansinės teisės akto pasiūlymo pažymos priede (Vidaus taisyklių V priedas) ir įkelta į DECIDE tarnybų tarpusavio konsultacijoms.

mln. EUR (tūkstantųjų tikslumu)

		2023 m.	**2024 m.**	**2025 m.**	**2026 m.**	**2027 m.**	**IŠ VISO**
GD: DIGIT (CERT-EU)							
○ Žmogiškieji ištekliai		1,184	2,126	2,754	3,225	3,225	12,514
○ Kitos administracinės išlaidos		7,938	8,921	8,921	8,921	8,921	43,622
IŠ VISO GD DIGIT (CERT-EU)	Asignavimai	9,122	11,047	11,675	12,146	12,146	56,136

IŠ VISO asignavimų pagal daugiametės finansinės programos **1–6 IŠLAIDŲ KATEGORIJAS**	(Iš viso įsipareigojimų = Iš viso mokėjimų)	9,122	11,047	11,675	12,146	12,146	**56,136**

mln. EUR (tūkstantųjų tikslumu)

		2023 m.	2024 m.	2025 m.	2026 m.	2027 m.	**IŠ VISO**
IŠ VISO asignavimų pagal daugiametės finansinės programos 1–7 IŠLAIDŲ KATEGORIJAS (*)	Įsipareigojimai	11,581	13,506	14,134	14,605	14,605	68,429
	Mokėjimai	11,581	13,506	14,134	14,605	14,605	68,429

Apskaičiuota, kad savo lėšomis finansuojamų Sąjungos institucijų, įstaigų ir agentūrų įnašai sudaro 2 670 mln. EUR per metus (iš viso per penkerius metus – 13 350 mln. EUR). Šie įnašai sudarys CERT-EU asignuotąsias pajamas. Į pirmiau pateiktas lenteles įtrauktas tik numatomas bendras poveikis Sąjungos biudžetui, o tie įnašai į jas neįtraukti.

3.2.2. Numatomas veiklos asignavimais finansuojamas atliktas darbas

Įsipareigojimų asignavimai mln. EUR (tūkstantųjų tikslumu)

Nurodyti tikslus ir atliktus darbus ⇩			**N m.**		**N+1 m.**		**N+2 m.**		**N+3 m.**		Atsižvelgiant į poveikio trukmę įterpti reikiamą metų skaičių (žr. 1.6 punktą)						**IŠ VISO**	
	ATLIKTI DARBAI																	
	Rūšis[18]	Vidutinės išlaidos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Skaičius	Sąnaudos	Bendras skaičius	Iš viso išlaidų
1 KONKRETUS TIKSLAS[19]...																		
Atliktas																		
Atliktas																		
Atliktas																		
1 konkretaus tikslo tarpinė suma																		
2 KONKRETUS TIKSLAS ...																		
Atliktas																		
2 konkretaus tikslo tarpinė suma																		
IŠ VISO																		

[18] Atlikti darbai – tai būsimi produktai ir paslaugos (pvz., finansuota studentų mainų, nutiesta kelių kilometrų ir kt.).

[19] Kaip apibūdinta 1.4.2 skirsnyje „Konkretus (-ūs) tikslas (-ai) ...“

3.2.3. Numatomo poveikio administraciniams asignavimams santrauka

– ☐ Pasiūlymui (iniciatyvai) įgyvendinti administracinio pobūdžio asignavimų nenaudojama

– ☑ Pasiūlymui (iniciatyvai) įgyvendinti administracinio pobūdžio asignavimai naudojami taip:

mln. EUR (tūkstantųjų tikslumu)

	2023 m.	2024 m.	2025 m.	2026 m.	2027 m.	**IŠ VISO**
Daugiametės finansinės programos 7 IŠLAIDŲ KATEGORIJA						
Žmogiškieji ištekliai						
Nuolatiniai darbuotojai (AD pareigų grupės lygių)	1,099	2,041	2,669	3,14	3,14	12,089
Sutartininkai	0,085	0,085	0,085	0,085	0,085	0,425
Kitos administracinės išlaidos	7,938	8,921	8,921	8,921	8,921	43,622
Daugiametės finansinės programos 7 IŠLAIDŲ KATEGORIJOS tarpinė suma	9,122	11,047	11,675	12,146	12,146	56,136
Neįtraukta į daugiametės finansinės programos 7 IŠLAIDŲ KATEGORIJĄ[20]						
Žmogiškieji ištekliai						
Kitos administracinio pobūdžio išlaidos						
Tarpinė suma, neįtraukta į daugiametės finansinės programos 7 IŠLAIDŲ KATEGORIJĄ						
IŠ VISO	9,122	11,047	11,675	12,146	12,146	56,136

[20] Techninė ir (arba) administracinė parama bei išlaidos ES programų ir (arba) veiksmų įgyvendinimui remti (buvusios BA eilutės), netiesioginiai moksliniai tyrimai, tiesioginiai moksliniai tyrimai.

Žmogiškųjų išteklių ir kitų administracinio pobūdžio išlaidų asignavimų poreikiai bus tenkinami iš GD asignavimų, jau paskirtų veiksmui valdyti ir (arba) perskirstytų generaliniame direktorate, ir prireikus finansuojami iš papildomų lėšų, kurios atsakingam GD gali būti skiriamos pagal metinę lėšų skyrimo procedūrą ir atsižvelgiant į biudžeto apribojimus.

3.2.3.1. Numatomi žmogiškųjų išteklių poreikiai

– ☐ Pasiūlymui (iniciatyvai) įgyvendinti žmogiškųjų išteklių nenaudojama.

– ☑ Pasiūlymui (iniciatyvai) įgyvendinti žmogiškieji ištekliai naudojami taip:

Sąmatą surašyti etato vienetais

		2023 m.	2024 m.	2025 m.	2026 m.	2027 m.
O Etatų plano pareigybės (pareigūnai ir laikinieji darbuotojai)						
20 01 02 01 (Komisijos būstinė ir atstovybės)		7	13	17	20	20
20 01 02 03 (Delegacijos)						
01 01 01 01 (Netiesioginiai moksliniai tyrimai)						
01 01 01 11 (Tiesioginiai moksliniai tyrimai)						
Kitos biudžeto eilutės (nurodyti)						
O Išorės darbuotojai (etato vienetais: EV)[21]						
20 02 01 (CA, SNE, INT finansuojami iš bendrojo biudžeto)		1	1	1	1	1
20 02 03 (CA, LA, SNE, INT ir JPD atstovybėse)						
XX 01 xx **yy zz** [22]	– būstinėje					
	– delegacijose					
01 01 01 02 (CA, SNE, INT – Netiesioginiai moksliniai tyrimai)						
01 01 01 12 (CA, SNE, INT – Tiesioginiai moksliniai tyrimai)						
Kitos biudžeto eilutės (nurodyti)						
IŠ VISO		**8**	**14**	**18**	**21**	**21**

XX yra atitinkama politikos sritis arba biudžeto antraštinė dalis.

Žmogiškųjų išteklių poreikiai bus tenkinami panaudojant GD darbuotojus, jau paskirtus veiksmui valdyti ir (arba) perskirstytus generaliniame direktorate, ir prireikus finansuojami iš papildomų lėšų, kurios atsakingam GD gali būti skiriamos pagal metinę lėšų skyrimo procedūrą ir atsižvelgiant į biudžeto apribojimus.

Vykdytinų užduočių aprašymas:

Pareigūnai ir laikinieji darbuotojai	Pareigūnai įgyvendins CERT-EU užduotis ir veiklą, kaip nustatyta Reglamente, visų pirma jo IV ir V skyriuose.
Išorės darbuotojai	Sutartininkas padės vykdyti Tarpinstitucinės kibernetinio saugumo tarybos sekretoriato funkcijas.

[21] CA – sutartininkai (angl. *Contract Staff*), LA – vietos darbuotojai (angl. *Local Staff*), SNE – deleguotasis nacionalinis ekspertas (angl. *Seconded National Expert*), INT – per agentūrą įdarbinti darbuotojai (angl. *agency staff*), JPD – jaunesnieji delegacijos specialistai (angl. *Junior Professionals in Delegations*).

[22] Neviršijant viršutinės ribos, nustatytos išorės darbuotojams, finansuojamiems iš veiklos asignavimų (buvusių BA eilučių).

3.2.4. Suderinamumas su dabartine daugiamete finansine programa

Pasiūlyme (iniciatyvoje):

– ☑ galima visiškai finansuoti perskirstant asignavimą atitinkamoje daugiametės finansinės programos (DFP) išlaidų kategorijoje.

Paaiškinti, kaip reikia pakeisti programavimą, ir nurodyti atitinkamas biudžeto eilutes bei sumas. Jeigu programavimas keičiamas iš esmės, pateikti „Excel“ lentelę.

– ☐ reikia panaudoti nepaskirstytą maržą pagal atitinkamą DFP išlaidų kategoriją ir (arba) specialias priemones, kaip apibrėžta DFP reglamente.

Paaiškinti, ką reikia atlikti, ir nurodyti atitinkamas išlaidų kategorijas, biudžeto eilutes bei sumas ir pasiūlytas naudoti priemones.

– ☐ reikia persvarstyti DFP.

Paaiškinti, ką reikia atlikti, ir nurodyti atitinkamas išlaidų kategorijas, biudžeto eilutes ir sumas.

3.2.5. Trečiųjų šalių įnašai

Pasiūlyme (iniciatyvoje):

– ☑ nenumatyta bendro su trečiosiomis šalimis finansavimo[23]

– ☐ numatytas trečiųjų šalių bendras finansavimas apskaičiuojamas taip:

Asignavimai mln. EUR (tūkstantųjų tikslumu)

	N m.[24]	**N+1 m.**	**N+2 m.**	**N+3 m.**	Atsižvelgiant į poveikio trukmę įterpti reikiamą metų skaičių (žr. 1.6 punktą)			Iš viso
Nurodyti bendrą finansavimą teikiančią įstaigą								
IŠ VISO bendrai finansuojamų asignavimų								

[23] Asignuotosios pajamos, gaunamos iš 12 straipsnio 5 dalies c punkte numatyto atsitiktinio paslaugų teikimo organizacijoms, kurios nėra klientės, nebuvo apskaičiuotos, nes jos turėtų būti nedidelės.

[24] N metai yra pasiūlymo (iniciatyvos) įgyvendinimo pradžios metai. Pakeiskite „N“ numatomais pirmaisiais įgyvendinimo metais (pavyzdžiui, 2021 m.) Atitinkamai pakeiskite vėlesnius metus.

3.3. Numatomas poveikis pajamoms

– ☑ Pasiūlymas (iniciatyva) neturi finansinio poveikio pajamoms.

– ☐ Pasiūlymas (iniciatyva) turi finansinį poveikį:

– ☐ nuosaviems ištekliams

– ☐ kitoms pajamoms

– nurodyti, jei pajamos priskirtos išlaidų eilutėms ☐

mln. EUR (tūkstantųjų tikslumu)

Biudžeto pajamų eilutė:	Einamųjų finansinių metų asignavimai	Pasiūlymo (iniciatyvos) poveikis[25]						
		N m.	**N+1 m.**	**N+2 m.**	**N+3 m.**	Atsižvelgiant į poveikio trukmę įterpti reikiamą metų skaičių (žr. 1.6 punktą)		
..... straipsnis								

Asignuotųjų pajamų atveju nurodyti biudžeto išlaidų eilutę (-es), kuriai (-oms) daromas poveikis.

Kitos pastabos (pvz., poveikio pajamoms apskaičiavimo metodas (formulė) arba kita informacija).

[25] Tradiciniai nuosavi ištekliai (muitai, cukraus mokesčiai) turi būti nurodomi grynosiomis sumomis, t. y. iš bendros sumos atskaičius 20 % surinkimo sąnaudų.