Europos Sąjungos
Taryba

Briuselis, 2022 m. spalio 31 d.
(OR. en)

14128/22

Tarpinstitucinė byla:
2022/0085(COD)

CYBER 343
TELECOM 428
INST 396
CSC 472
CSCI 157
INF 176
FIN 1158
BUDGET 22
DATAPROTECT 294
CODEC 1617

PRANEŠIMAS DĖL „I/A“ PUNKTO

nuo:	Tarybos generalinio sekretoriato
kam:	Nuolatinių atstovų komitetui (COREPER II) / Tarybai
Ankstesnio dokumento Nr.:	10097/5/22 REV 5
Komisijos dok. Nr.:	7474/22 + ADD 1
Dalykas:	Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento, kuriuo nustatomos priemonės aukštam bendram kibernetinio saugumo lygiui Sąjungos institucijose, įstaigose, organuose ir agentūrose užtikrinti – Bendras požiūris

ĮVADAS

1. 2022 m. kovo 22 d. Komisija priėmė pasiūlymą dėl Reglamento, kuriuo nustatomos priemonės aukštam bendram kibernetinio saugumo lygiui Sąjungos institucijose, įstaigose, organuose ir agentūrose užtikrinti. Šis pasiūlymas buvo viena iš priemonių, numatytų ES skaitmeninio dešimtmečio kibernetinio saugumo strategijoje[1], kuria siekiama stiprinti Sąjungos kolektyvinį atsparumą kibernetinėms grėsmėms.

1 Dok. 14133/20.

2021 m. kovo 22 d. išvadose dėl šios strategijos[2] Taryba pabrėžė, kad „kibernetinis saugumas ir globalus bei atviras internetas yra gyvybiškai svarbūs tiek nacionalinio, tiek ES lygmens viešojo administravimo įstaigų ir institucijų veikimui, taip pat mūsų visuomenei ir visai ekonomikai apskritai“.

2. Komisijos pasiūlymu, grindžiamu Sutarties dėl Europos Sąjungos veikimo 298 straipsniu, siekiama nustatant bendrą sistemą gerinti kibernetinio saugumo lygį Sąjungos institucijose, įstaigose, organuose ir agentūrose, tinkamai atsižvelgiant į kiekvieno Sąjungos subjekto savarankiškumą. Visų pirma, pasiūlymo tikslai yra šie:

   – sustiprinti CERT-EU (savarankiškos tarpinstitucinės Sąjungos subjektų kompiuterinių incidentų tyrimo tarnybos) įgaliojimus ir finansavimą;

   – sukurti tarpinstitucinę struktūrą (Tarpinstitucinę kibernetinio saugumo tarybą), kuri suburtų visų Sąjungos subjektų atstovus, kad būtų užtikrintas tinkamas reglamento įgyvendinimas;

   – nustatyti pareigą Sąjungos subjektams dalytis (neįslaptinta) informacija apie incidentus su CERT-EU ir pranešti apie dideles grėsmes, didelį pažeidžiamumą bei reikšmingus incidentus, ir

   – skatinti veiksmų koordinavimą ir bendradarbiavimą reaguojant į reikšmingus incidentus.

3. Europos Parlamento Pramonės, mokslinių tyrimų ir energetikos (ITRE) komitetas už šį dokumentą atsakinga pranešėja paskyrė Henna Virkkunen (EPP). Pranešimo projektas buvo paskelbtas 2022 m. spalio 7 d.

4. Europos duomenų apsaugos priežiūros pareigūnas nuomonę pateikė 2022 m. gegužės 17 d.[3].

---

[2] Dok. 6722/21.
[3] Dok. 9252/22.

5. Taryboje pasiūlymas pradėtas nagrinėti pirmininkaujant Prancūzijai Kibernetinių klausimų horizontaliojoje darbo grupės (HWPCI) 2022 m. kovo 29 d. posėdyje. Pirmininkaujanti Prancūzija parengė pirmąjį kompromisinį tekstą; jį 2022 m. birželio mėn. aptarė HWPCI darbo grupė ir 2022 m. birželio 21 d. pateikė Tarybai pažangos ataskaitą[4].

6. Pirmininkaujant Čekijai HWPCI darbo grupė surengė aštuonis posėdžius[5], skirtus diskusijoms dėl pasiūlymo ir dėl kelių vienas po kito pateiktų kompromisinių tekstų.

7. 2022 m. gegužės 23 d. pirmininkaujanti valstybė narė paprašė Tarybos Saugumo komiteto (TSK) pateikti nuomonę dėl pasiūlymo aspektų, susijusių su informacijos saugumu, visų pirma su įslaptinta informacija. TSK savo nuomonę pateikė 2022 m. rugsėjo 19 d.[6]. Kaip nurodė TSK, ES įslaptinta informacija aiškiai nėra įtraukta į reglamento taikymo sritį. Atitinkamai buvo pakeistos nuostatos, susijusios su išimtimis, taikomomis dalijimosi informacija, gauta iš ne Sąjungos subjektų, ir pranešimo pareigoms.

8. 2022 m. spalio 28 d. posėdyje HWPCI darbo grupė pasiekė susitarimą dėl pirmininkaujančios valstybės narės kompromisinio teksto, išdėstyto priede.

---

4 Dok. 9719/22.
5 2022 m. liepos 6 ir 20 d., rugsėjo 13, 21 ir 28 d., spalio 5, 19 ir 28 d.
6 Dok. 12603/22 + COR 1.

PAGRINDINIAI KLAUSIMAI

9. Valstybės narės palankiai įvertino pasiūlymą, nes jis pateiktas laiku ir papildo būsimą direktyvą dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti (TIS 2 direktyva), ir pritarė jo bendriesiems tikslams. Tačiau valstybės narės paragino padaryti papildomų suderinimų su TIS 2, užtikrinti didesnį abipusiškumą keičiantis informacija tarp Sąjungos subjektų bei valstybių narių ir atkreipė dėmesį į pernelyg savanorišką kai kurių siūlomų priemonių pobūdį. Valstybės narės taip pat nurodė pageidaujančios, kad būtų išbrauktos nuorodos į Jungtinį kibernetinio saugumo padalinį, kadangi jo įgaliojimai ir sudėtis dar nėra nustatyti.

10. Remiantis diskusijų HWPCI darbo grupėje rezultatais nustatyti šie pagrindiniai politiniai klausimai:

a) Suderinimas su būsima TIS 2 direktyva

Valstybių narių prašymu buvo padaryta papildomų suderinimų su būsima TIS 2 direktyva, *inter alia*:

– kelios apibrėžtys (3 straipsnis) suderintos su TIS 2 apibrėžtimis;

– įtrauktas TIS 2 atitinkantis naujas 7a straipsnis dėl savanoriškų tarpusavio vertinimų, kurie pritaikyti prie Sąjungos subjektų poreikių;

– 20 straipsnyje nustatytos pranešimo pareigos suderintos su TIS 2 nustatytomis pareigomis.

b) Tarpinstitucinės kibernetinio saugumo tarybos (TKST) sudėtis (9 straipsnis)

Po diskusijų dėl atitinkamo valstybių narių atstovų dalyvavimo TKST veikloje buvo pasiektas kompromisas – į posėdžio protokolą įtrauktas Tarybos pareiškimas.

c) Institucinis savarankiškumas

Užtikrinta pusiausvyra tarp valstybių narių ryžto stiprinti atitikties užtikrinimo mechanizmus ir poreikio laikytis institucinio savarankiškumo principo, visų pirma kiek tai susiję su auditu ir drausminėmis priemonėmis (11 straipsnis).

Galiausiai iš 8 konstatuojamosios dalies išbraukta nuoroda į kibernetiniam saugumui skirto IT biudžeto konkrečią procentinę dalį.

IŠVADA

11. Nuolatinių atstovų komiteto prašoma:

a) patvirtinti priede išdėstytą kompromisinį tekstą, kuris vėliau taps derybų su Europos Parlamentu įgaliojimais;

b) paprašyti Tarybos 2022 m. lapkričio 18 d. posėdyje patvirtinti priede išdėstytą kompromisinį tekstą ir į posėdžio protokolą įtraukti šio dokumento papildyme išdėstytą Tarybos pareiškimą.

PRIEDAS

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 [...] **subjektai**, padėtis nuolat kinta. Grėsmę keliančių subjektų naudojama taktika, metodai ir procedūros nuolat vystosi, tačiau aiškūs tokių išpuolių motyvai vargiai kinta: vertingos konfidencialios informacijos vagystės siekiant užsidirbti pinigų, 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 [...] **subjektų** IT aplinkose yra tarpusavyje priklausomų elementų ir integruotų duomenų srautų, o jų naudotojai glaudžiai bendradarbiauja. Šis tarpusavio ryšys reiškia, kad bet koks sutrikdymas, net jei iš pradžių jis susijęs tik su vien**u** Sąjungos [...] **subjektu**, gali turėti platesnį pakopinį poveikį, o šis gali turėti plataus masto ir ilgalaikių neigiamų padarinių kitiems subjektams. Be to, tam tikra [...] **Sąjungos subjektų** 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; **Sąjungos subjektai taip pat tvarko didelius valstybių narių informacijos, kuri dažnai yra neskelbtina, kiekius, todėl incidentai galėtų turėti neigiamos įtakos ir valstybėms narėms. Dėl šios priežasties Sąjungos subjektų kibernetinis saugumas taip pat yra labai svarbus valstybėms narėms. Su incidentais susijusi informacija taip pat gali padėti aptikti panašias kibernetines grėsmes ar incidentus, darančius poveikį valstybėms narėms;**

(4) Sąjungos [...] **subjektai** 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 [...] **subjektai** užtikrintų aukštą bendrą kibernetinio saugumo lygį, **įgyvendindami kibernetinio saugumo priemone**s, [...] keis**damiesi** informacija ir bendradar**biaudami**;

(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 [...] **subjektai** to laikytųsi, užtikrindam**i** taisykles, kurios derėtų su Direktyva [pasiūlymas dėl TIS 2] ir atspindėtų jos užmojų mastą;

(6) aukštam bendram kibernetinio saugumo lygiui pasiekti būtina, kad kiekvien**as** Sąjungos [...] **subjektas** sukurtų vidaus kibernetinio saugumo rizikos valdymo ir kontrolės sistemą, kuria būtų užtikrinamas veiksmingas ir apdairus visų rizikos kibernetiniam saugumui veiksnių valdymas [...]. **Sistemoje turėtų būti nustatyta kibernetinio saugumo politika, įskaitant įgyvendintų kibernetinio saugumo priemonių veiksmingumo vertinimo procedūras. Sistema turėtų būti grindžiama visus pavojus apimančiu požiūriu, ja turėtų būti siekiama apsaugoti tinklus ir informacines sistemas ir tų sistemų fizinę aplinką nuo tokių įvykių kaip vagystė, gaisras, potvynis, telekomunikacijų ar energijos tiekimo triktys arba nuo neleistinos fizinės prieigos prie Sąjungos subjekto informacijos ir informacijos tvarkymo objektų ir žalos jiems ar jų trikdžių, kurie galėtų kelti pavojų saugomų, perduodamų, tvarkomų arba per tinklus ir informacines sistemas prieinamų duomenų prieinamumui, autentiškumui, vientisumui ar konfidencialumui. Sistemoje turėtų atsispindėti rizikos analizės išvados, atsižvelgiant į visą atitinkamą techninę, operacinę ir organizacinę riziką atitinkamo Sąjungos subjekto kibernetiniam saugumui;**

(6a) kad galėtų valdyti pagal sistemą nustatytą riziką, kiekvienas Sąjungos subjektas turėtų užtikrinti, kad būtų imamasi tinkamų ir proporcingų techninių, operacinių ir organizacinių priemonių. Jos turėtų apimti sritis, įskaitant šiame reglamente nustatytas kibernetinio saugumo priemones, kuriomis siekiama stiprinti kiekvieno Sąjungos subjekto kibernetinį saugumą;

(6b) **sistemoje nustatytas turtas ir rizika, taip pat reguliarių kibernetinio saugumo brandos vertinimų išvados turėtų atsispindėti kiekvieno Sąjungos subjekto parengtame kibernetinio saugumo plane. Į kibernetinio saugumo planą turėtų būti įtrauktos patvirtintos kibernetinio saugumo priemonės, siekiant padidinti bendrą atitinkamo Sąjungos subjekto kibernetinį saugumą;**

(6c) **kadangi kibernetinio saugumo užtikrinimas yra nuolatinis procesas, turėtų būti reguliariai peržiūrimas visų priemonių tinkamumas ir veiksmingumas, atsižvelgiant į kintančią Sąjungos subjektams kylančią riziką, jų kintantį turtą ir kibernetinio saugumo brandą. Sistema turėtų būti reguliariai bent kas trejus metus peržiūrima, o kibernetinio saugumo planas turėtų būti peržiūrimas bent kas dvejus metus arba po kiekvieno kibernetinio saugumo brandos vertinimo ar po kiekvienos atliktos sistemos peržiūros;**

(6d) **Sąjungos subjektai turėtų reguliariai keistis atitinkama informacija, be kita ko, susijusia su atitinkamais incidentais ir kibernetinėmis grėsmėmis, kartu užtikrindami pranešančiojo Sąjungos subjekto pateikiamos informacijos konfidencialumą ir tinkamą apsaugą;**

(6e) **turėtų būti įgyvendintas mechanizmas, kuriuo būtų užtikrinamas veiksmingas Sąjungos subjektų keitimasis informacija, veiksmų koordinavimas ir bendradarbiavimas didelių incidentų atveju, įskaitant aiškų susijusių Sąjungos subjektų vaidmenų ir atsakomybės nustatymą. Į informaciją, kuria keičiamasi, turėtų atsižvelgti paskirtas EU-CyCLONe kontaktinis asmuo, kai atitinkama informacija dalijamasi su EU-CyCLONe ir taip prisidedama prie bendro informuotumo apie padėtį;**

(7) dėl Sąjungos [...] **subjektų** 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 [...] **subjektų** užduočių vykdymą arba kėsinamasi į jų institucinį savarankiškumą. Todėl tie **Sąjungos subjektai** turėtų sukurti savo kibernetinio saugumo rizikos valdymo, valdymo ir kontrolės sistemas, **parengti kibernetinio saugumo planus** ir patvirtinti [...] kibernetinio saugumo [...] **priemones**. **Įgyvendinant tokias priemones turėtų būti tinkamai atsižvelgiama į esamas Sąjungos subjektų tarpusavio sinergijas, kad būtų tinkamai valdomi ištekliai ir optimizuotos išlaidos. Taip pat reikėtų tinkamai atsižvelgti į tai, kad priemonės nedarytų neigiamo poveikio veiksmingam Sąjungos subjektų keitimuisi informacija ir operacijoms su kitais Sąjungos subjektais ir nacionalinėmis kompetentingomis institucijomis;**

(8) siekiant neužkrauti Sąjungos [...] **subjektams** finansinės ir administracinės naštos, kibernetinio saugumo rizikos valdymo reikalavimai turėtų būti proporcingi rizikai, kurią kelia atitinkama tinklų ir informacinė sistema, atsižvelgiant į tokių priemonių modernumą. Kiekvien**as** Sąjungos [...] **subjektas** turėtų siekti skirti tinkamą savo IT biudžeto procentinę dalį tikslui padidinti savo kibernetinio saugumo lygį. **Kibernetinio saugumo brandos vertinime taip pat turėtų būti įvertinta, ar Sąjungos subjekto išlaidos kibernetiniam saugumui yra proporcingos jo patiriamai rizikai;**

(9) siekiant užtikrinti aukštą bendrą kibernetinio saugumo lygį kibernetinį saugumą turi prižiūrėti kiekvien**o** Sąjungos [...] **subjekto** aukščiausio lygmens vadovybė. [...] **Aukščiausio lygmens vadovybė turėtų prižiūrėti šio reglamento įgyvendinimą, įskaitant rizikos valdymo, valdymo bei kontrolės sistemos ir kibernetinio saugumo planų, apimančių kibernetinio saugumo priemones, sukūrimą.** Kibernetinio saugumo kultūra, t. y. kasdienė kibernetinio saugumo praktika, yra neatsiejama [...] vis**ų** Sąjungos [...] **subjektų** kibernetinio saugumo **sistemos** dalis;

(10) [...] [...] **kibernetinio saugumo** priemonės turėtų būti [...] kibernetinio saugumo **plano** [...] dalis ir jos turėtų būti išsamiau išdėstytos CERT-EU parengtose gairėse arba rekomendacijose. Nustatant priemones ir gaires reikėtų tinkamai atsižvelgti į **moderniausius ir, kai taikytina, aktualius Europos ir tarptautinius standartus, taip pat** 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. **Kai tikslinga, CERT-EU turėtų bendradarbiauti su ENISA;**

(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 darbo organizavimo ir veiklos[7]. Šiuo [...] **reglamentu** turėtų būti [...] **nustatytos išsamios taisyklės dėl CERT-EU darbo organizavimo, veikimo ir veiklos. Šio reglamento nuostatos yra viršesnės už 2017 m. gruodžio mėn. sudaryto Tarpinstitucinio susitarimo dėl CERT-EU darbo organizavimo ir veiklos nuostatas**;

[...]

[7] OL C 12, 2018 1 13, p. 1–11.

(13) daugelis kibernetinių išpuolių yra platesnių kampanijų, nukreiptų prieš Sąjungos [...] **subjektų** grupes arba interesų bendruomenes, įskaitant Sąjungos [...] **subjektus**, dalis. Kad būtų galima imtis proaktyvių aptikimo, reagavimo į incidentus ar rizikos mažinimo priemonių, Sąjungos [...] **subjektai** turėtų pranešti CERT-EU apie [...] kibernetines grėsmes, [...] pažeidžiamumą, **vos neįvykusius incidentus ir** [...] incidentus ir dalytis tinkama technine informacija, kad būtų galima nustatyti arba sumažinti panašias kibernetines grėsmes, **pažeidžiamumą, vos neįvykusius incidentus ir** incidentus kit**uose** Sąjungos [...] **subjektuose** arba į juos reaguoti. Vadovaujantis tokiu pačiu požiūriu, koks yra numatytas Direktyvoje [pasiūlymas dėl TIS 2], **Sąjungos** subjektams sužinojus apie reikšmingą incidentą, turėtų būti reikalaujama, kad jie per 24 valandas CERT-EU pateiktų [...] **išankstinį perspėjimą**. Toks keitimasis informacija turėtų sudaryti sąlygas CERT-EU skleisti informaciją kit**iems** Sąjungos [...] **subjektams**, taip pat atitinkamiems partneriams, siekiant padėti apsaugoti Sąjungos IT aplinką ir Sąjungos partnerių IT aplinką nuo panašių incidentų [...];

(13a) šiuo reglamentu nustatomas kelių etapų požiūris į pranešimų apie reikšmingus incidentus teikimą, siekiant užtikrinti tinkamą pusiausvyrą tarp, viena vertus, greito pranešimų teikimo, kuris padeda sumažinti galimą reikšmingų incidentų plitimą ir sudaro sąlygas Sąjungos subjektams prašyti pagalbos, ir, kita vertus, išsamių pranešimų, kuriuose atsižvelgiama į vertingą atskirų incidentų metu įgytą patirtį ir kuriais laikui bėgant didinamas atskirų Sąjungos subjektų kibernetinis atsparumas. Šiuo atžvilgiu į šį reglamentą turėtų būti įtraukti pranešimai apie incidentus, kurie, remiantis Sąjungos subjekto atliktu pradiniu vertinimu, galėtų sukelti didelių Sąjungos subjekto veikimo sutrikdymų arba padaryti finansinių nuostolių atitinkamam Sąjungos subjektui, arba padaryti poveikį kitiems fiziniams ar juridiniams asmenims, sukeldami didelę turtinę ar neturtinę žalą. Atliekant tokį pradinį vertinimą turėtų būti atsižvelgiama, *inter alia*, į paveiktus tinklus ir informacines sistemas, visų pirma į jų svarbą Sąjungos subjekto veikimui, kibernetinės grėsmės rimtumą bei technines charakteristikas ir bet kokį pagrindinį pažeidžiamumą, kuriuo pasinaudojama, taip pat į Sąjungos subjekto patirtį, įgytą panašių incidentų metu. Nustatant, ar veiklos sutrikdymas yra didelis, svarbus vaidmuo galėtų tekti tokiems rodikliams kaip poveikio Sąjungos subjekto veikimui mastas, incidento trukmė arba paveiktų fizinių ar juridinių asmenų skaičius;

(13b) kadangi atitinkamo Sąjungos subjekto ir valstybės narės, kurioje yra tas Sąjungos subjektas, infrastruktūra ir tinklai yra tarpusavyje susiję, labai svarbu, kad ta valstybė narė būtų nepagrįstai nedelsiant informuojama apie reikšmingą incidentą tame Sąjungos subjekte. Tuo tikslu paveiktas Sąjungos subjektas turėtų apie reikšmingą incidentą pranešti CERT-EU nacionaliniam partneriui, kurį valstybė narė paskyrė pagal Direktyvą [pasiūlymas dėl TIS 2], laikydamasis tokio paties termino, iki kurio jis apie tokį incidentą turėtų pranešti CERT-EU. Sužinojęs apie valstybėje narėje įvykusį reikšmingą incidentą CERT-EU taip pat turėtų apie tai pranešti šiam nacionaliniam partneriui, nebent apie jį jau yra pranešęs paveiktas Sąjungos subjektas;

(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), kuriai**, siekiant sudaryti palankesnes sąlygas aukštam bendram Sąjungos subjektų kibernetinio saugumo lygiui užtikrinti,** turėtų **būti suteiktas išskirtinis vaidmuo** [...] stebint, kaip Sąjungos [...] **subjektai** įgyvendina šį reglamentą, ir prižiūrint, kaip CERT-EU įgyvendina bendruosius prioritetus ir tikslus, bei numatant CERT-EU strateginę kryptį. **Todėl** TKST turėtų užtikrinti atstovavimą institucijoms ir į ją turėtų būti įtraukta agentūrų ir įstaigų atstovų, vykdančių veiklą per Sąjungos agentūrų tinklą. **TKST veiklos organizavimas ir veikimas turėtų būti išsamiau reglamentuojami jos vidaus darbo tvarkos taisyklėmis, kurios gali apimti išsamesnį reguliarių TKST posėdžių, įskaitant metinius politinio lygmens susirinkimus, kuriuose kiekvieno TKST nario aukščiausio lygmens vadovybės atstovai sudarytų sąlygas TKST surengti strategines diskusijas ir teikti strategines gaires TKST, apibūdinimą. Be to, TKST gali įsteigti vykdomąjį komitetą, kuris padėtų jai atlikti savo darbą, ir deleguoti jam kai kurias savo užduotis ir įgaliojimus, visų pirma užduotis, kurioms atlikti reikia specialių jo narių ekspertinių žinių, pavyzdžiui, paslaugų katalogo ir visų vėlesnių jo atnaujinimų patvirtinimą, susitarimų dėl paslaugų lygio sąlygų patvirtinimą, Sąjungos subjektų TKST pagal šį reglamentą pateiktų dokumentų ir ataskaitų vertinimą, arba užduotis, susijusias su sprendimų dėl TKST patvirtintų atitikties užtikrinimo priemonių rengimu ir jų įgyvendinimo stebėsena. TKST turėtų nustatyti vykdomojo komiteto darbo tvarkos taisykles, įskaitant jo užduotis bei įgaliojimus;**

(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 [...] **subjektai** raginami imtis per nustatytą laikotarpį. **TKST gali nurodyti CERT-EU paskelbti, atsiimti arba pakeisti pasiūlymą dėl rekomendacinių dokumentų ar rekomendacijų arba raginimą imtis veiksmų;**

(16) TKST turėtų stebėti, kaip laikomasi šio reglamento ir kaip įgyvendinami tolesni veiksmai, susiję su [...] rekomendaciniais dokumentais ir rekomendacijomis bei paskelbtais raginimais imtis veiksmų. TKST techniniais klausimais turėtų remti jos savo nuožiūra nustatytos sudėties techninės patariamosios grupės, kurios prireikus turėtų glaudžiai bendradarbiauti su CERT-EU, Sąjungos [...] **subjektais** ir kitais suinteresuotaisiais subjektais. [...] **Jei TKST nustato, kad Sąjungos subjektai netaikė arba neįgyvendino šio reglamento, įskaitant pagal šį reglamentą paskelbtus rekomendacinius dokumentus, rekomendacijas ar raginimus imtis veiksmų, nedarydama poveikio atitinkamo Sąjungos subjekto vidaus procedūroms TKST gali imtis atitikties užtikrinimo priemonių. Atitikties užtikrinimo priemonių sistema turėtų būti taikoma laipsniškai, t. y. kai TKST patvirtina atitikties užtikrinimo priemones, ji iš pradžių turėtų pateikti perspėjimą – mažiausiai griežtą priemonę ir tada prireikus palaipsniui imtis priemonių iki griežčiausios priemonės – paskelbti patariamojo pobūdžio raštą, kuriame būtų rekomenduojama laikinai sustabdyti duomenų srautus į atitinkamą Sąjungos subjektą; tokia priemonė būtų taikoma išskirtiniais atvejais, kai atitinkamas subjektas ilgą laiką, tyčia ir (arba) rimtai nesilaiko savo pareigos pagal šį reglamentą;**

(16a) perspėjimas yra mažiausiai griežta atitikties užtikrinimo priemonė, kuria siekiama pašalinti nustatytus Sąjungos subjekto trūkumus, ir ji apima rekomendacijas per nustatytą laikotarpį iš dalies pakeisti jo kibernetinio saugumo dokumentus. Įspėjimas turėtų būti prieinamas visiems Sąjungos subjektams, nebent jis būtų atitinkamai apribotas pagal šį reglamentą;

(16b) TKST taip pat gali rekomenduoti atlikti Sąjungos subjekto auditą. Šiuo tikslu Sąjungos subjektas gali naudotis savo vidaus audito funkcija. TKST taip pat galėtų prašyti, kad auditą atliktų trečiosios šalies audito tarnyba, įskaitant abipusiai sutartą privačiojo sektoriaus paslaugų teikėją;

(16c) TKST, remdamasi pagal savo rekomendaciją arba prašymą atlikto audito rezultatais, taip pat gali prašyti Sąjungos subjekto užtikrinti, kad kibernetinio saugumo rizikos valdymas, valdymas ir kontrolė atitiktų šio reglamento nuostatas;

(16d) kadangi valstybės narės su atitinkamais Sąjungos subjektais dalijasi informacija, kuri gali būti neskelbtino pobūdžio, valstybėms narėms labai svarbus tokios informacijos gavėjo kibernetinis saugumas. Todėl išskirtiniais atvejais, kai Sąjungos subjektas ilgą laiką, tyčia, pakartotinai ir (arba) rimtai nevykdo pareigos, TKST kaip kraštutinę priemonę gali paskelbti patariamojo pobūdžio raštą visoms valstybėms narėms ir Sąjungos subjektams, kuriame būtų rekomenduojama laikinai sustabdyti duomenų srautus į tą Sąjungos subjektą; ši priemonė turėtų būti taikoma tol, kol bus ištaisyta šio subjekto kibernetinio saugumo padėtis. Apie šį patariamojo pobūdžio raštą visoms valstybėms narėms ir Sąjungos subjektams turėtų būti pranešama naudojantis saugiais ryšių kanalais;

(16e) **siekiant užtikrinti tinkamą šio reglamento įgyvendinimą, jei, TKST nuomone, Sąjungos subjekto nuolatinį šio reglamento pažeidimą tiesiogiai sukėlė jo darbuotojo, įskaitant aukščiausio lygmens vadovybę, veiksmai ar neveikimas, ji turėtų prašyti atitinkamo Sąjungos subjekto pagal Tarnybos nuostatus ir kitas lygiavertes tam tikriems Sąjungos subjektams taikomas taisykles imtis atitinkamų veiksmų to darbuotojo atžvilgiu. Šie veiksmai gali apimti, pavyzdžiui, drausmines procedūras ir, kai tinkama, konkrečiu Sąjungos agentūrų atveju – prašymą kompetentingai institucijai imtis būtinų veiksmų, susijusių su galimu asmens, kuris galėtų būti atsakingas už nuolatinį šio reglamento pažeidimą, pašalinimu iš pareigų;**

(17) CERT-EU turėtų būti pavesta prisidėti prie visų Sąjungos [...] **subjektų** IT aplinkos saugumo. **Svarstydama, ar Sąjungos subjekto prašymu teikti technines konsultacijas ar informaciją atitinkamais politikos klausimais, CERT-EU turėtų užtikrinti, kad tai jai netrukdytų vykdyti kitų šiame reglamente nustatytų užduočių;**

(17a) CERT-EU turėtų veikti kaip Sąjungos[...] **subjektų** paskirto koordinatoriaus atitikmuo suderinto pažeidžiamumų atskleidimo Europos pažeidžiamumų registrui tikslais, kaip nurodyta Direktyvos [pasiūlymas dėl TIS 2] 6 straipsnyje**, ir turėtų parengti politiką dėl pažeidžiamumų valdymo, apimančią savanoriško suderinto pažeidžiamumų atskleidimo skatinimą ir palengvinimą;**

[...]

(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[8] CERT-EU turėtų bendradarbiauti ir koordinuoti reagavimo veiksmus su atitinkamais suinteresuotaisiais subjektais. Siekdama prisidėti 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;

[8] 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).

(20) siekdama remti operatyvinį kibernetinį saugumą CERT-EU turėtų pasinaudoti Europos Sąjungos kibernetinio saugumo agentūros **(ENISA)** ekspertinėmis žiniomis, vykdydama Europos Parlamento ir Tarybos reglamente (ES) 2019/88l[9] 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 [...] **ENISA** grėsmių analizės srityje ir reguliariai dalytis su ja grėsmių padėties ataskaita;

[...]

(22) **CERT-EU veikla ir informacijos tvarkymas pagal šį reglamentą gali apimti asmens duomenų tvarkymą.** Visi pagal šį reglamentą tvarkomi asmens duomenys turėtų būti tvarkomi laikantis duomenų apsaugos teisės aktų, įskaitant Europos Parlamento ir Tarybos reglamentą (ES) 2018/1725[10]. **Kai pagal šį reglamentą asmens duomenys perduodami Sąjungoje įsisteigusiems gavėjams, kurie nėra Sąjungos subjektai, tai turėtų būti daroma pagal Reglamento (ES) 2018/1725 9 straipsnį;**

---

9 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).

10 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).

(23) CERT-EU ir Sąjungos [...] **subjektų** vykdomas informacijos tvarkymas turėtų atitikti **taikomas** taisykles [...] dėl informacijos saugumo [...];

(23a) dalijimosi informacija tikslais matomomis žymomis nurodoma, kad informacijos gavėjai turi dalytis informacija laikydamiesi tam tikrų ribų, visų pirma remdamiesi informacijos neatskleidimo susitarimais arba neoficialiais informacijos neatskleidimo susitarimais, pavyzdžiui, srauto kontrolės protokolu arba kitais aiškiais šaltinio nurodymais. Srauto kontrolės protokolas turi būti suprantamas kaip būdas teikti informaciją apie bet kokius apribojimus, susijusius su tolesniu informacijos skleidimu. Juo naudojasi beveik visos reagavimo į kompiuterių saugumo incidentus tarnybos (CSIRT) ir kai kurie informacijos analizės ir dalijimosi ja centrai;

(24) **šis reglamentas ir naujos CERT-EU skirtos užduotys neturės poveikio bendroms išlaidoms pagal daugiametę finansinę programą.** Kadangi CERT-EU paslaugos ir užduotys atitinka visų Sąjungos [...] **subjektų** interesus, kiekvien**as** IT išlaidų turintis Sąjungos [...] **subjektas** turėtų sąžiningai prisidėti prie tų paslaugų teikimo ir užduočių vykdymo. Tie įnašai nedaro poveikio Sąjungos [...] **subjektų** biudžetiniam savarankiškumui. **Visi Sąjungos subjektai ir jų administracijos turėtų užtikrinti savo išteklių optimizavimą dabartiniu lygmeniu ir didinti veiksmingumą, be kita ko, stiprindami tarpinstitucinį bendradarbiavimą kibernetinio saugumo srityje. Todėl pirmenybė turėtų būti teikiama bendram požiūriui į administracinių išlaidų sutelkimą, o ne individualizuotoms Sąjungos subjektų išlaidoms;**

(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. **Be to, Europos Audito Rūmų prašoma reguliariai vertinti CERT-EU veikimą,**

PRIĖMĖ ŠĮ REGLAMENTĄ:

I skyrius
BENDROSIOS NUOSTATOS

1 straipsnis

Dalykas

1. Šiuo reglamentu nustatomos **priemonės, kuriomis siekiama užtikrinti aukštą bendrą kibernetinio saugumo lygį Sąjungos subjektuose** [...].

2. Tuo tikslu šiuo reglamentu nustatomos:

c) **kiekvienam** Sąjungos [...] **subjektui** taikomos pareigos sukurti [...] kibernetinio saugumo rizikos valdymo, valdymo ir kontrolės sistemą;

d) Sąjungos [...] **subjektų** kibernetinio saugumo rizikos valdymo**,** pranešimų teikimo **ir dalijimosi informacija** pareigos;

e) taisyklės dėl **savarankiškos tarpinstitucinės** Sąjungos [...] **subjektų kompiuterinių incidentų tyrimo tarnybos** (CERT-EU) darbo organizavimo, **veikimo** bei veiklos ir Tarpinstitucinės kibernetinio saugumo tarybos **(TKST)** darbo organizavimo, **veikimo** ir veiklos;

f) taisyklės, susijusios su šio reglamento įgyvendinimo stebėsena.

2 straipsnis

Taikymo sritis

1. Šis reglamentas taikomas [...] visiems Sąjungos [...] **subjektams**, [...] CERT-EU ir **TKST** [...].

2. Šis reglamentas taikomas nedarant poveikio Sutartyse numatytam instituciniam savarankiškumui.

3. Išskyrus 12 straipsnio 7 dalį, šis reglamentas netaikomas tinklams ir informacinėms sistemoms, kuriuose tvarkoma ES įslaptinta informacija (ESĮI).

3 straipsnis

Apibrėžtys

Šiame reglamente vartojamų terminų apibrėžtys:

1) Sąjungos [...] **subjektai** – Sąjungos institucijos, įstaigos, organai ir agentūros, įsteigti Europos Sąjungos sutartimi, Sutartimi dėl Europos Sąjungos veikimo arba Europos atominės energijos bendrijos steigimo sutartimi arba jomis remiantis;

2) tinklas ir informacinė sistema – tinklas ir informacinė sistema, kaip apibrėžta Direktyvos [pasiūlymas dėl TIS 2] 4 straipsnio 1 punkte;

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

4) kibernetinis saugumas – kibernetinis saugumas, **kaip apibrėžta Reglamento (ES) 2019/881 2 straipsnio 1 punkte**;

5) aukščiausio lygmens vadovybė – aukščiausio administracinio lygmens **sprendimų priėmimo įgaliojimus turintis** vadovas, valdymo arba koordinavimo ir priežiūros organas, atsižvelgiant į kiekvie**no** Sąjungos [...] **subjekto** aukšto lygmens valdymo tvarką;

5a) vos neįvykęs incidentas – vos neįvykęs incidentas, kaip apibrėžta Direktyvos [pasiūlymas dėl TIS 2] 4 straipsnio 4a punkte;

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

[...]

8) didelis **incidentas** [...] – incidentas, **kurio sukelto sutrikdymo mastas viršija Sąjungos subjekto ir CERT-EU pajėgumą į jį reaguoti arba kuris daro didelį poveikį bent dviem Sąjungos subjektams**; [...]

(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;

[...]

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

[...]

14) [...] rizika – **rizika, kaip tai suprantama Direktyvos [pasiūlymas dėl TIS 2] 4 straipsnio 7b punkte**;

[...]

[...]

3a straipsnis

Asmens duomenų tvarkymas

1) CERT-EU, TKST arba Sąjungos subjektai asmens duomenis pagal šį reglamentą tvarko laikydamiesi Reglamento (ES) 2018/1725.

2) CERT-EU, TKST ir Sąjungos subjektai tvarko asmens duomenis ir jais keičiasi tiek, kiek tai būtina, ir tik tam, kad įvykdytų atitinkamas savo pareigas pagal šį reglamentą.

II skyrius
PRIEMONĖS AUKŠTAM BENDRAM KIBERNETINIO SAUGUMO LYGIUI UŽTIKRINTI

4 straipsnis

Rizikos valdymo, valdymo ir kontrolės sistema

1. Kiekvien**as** Sąjungos [...] **subjektas** sukuria savo [...] kibernetinio saugumo rizikos valdymo, valdymo ir kontrolės sistemą (toliau – sistema), kuri padėtų atlikti subjekto misiją [...]. [...] Siekiant užtikrinti veiksmingą ir apdairų visų rūšių rizikos kibernetiniam saugumui valdymą, **šią sistemą** prižiūri subjekto aukščiausio lygmens vadovybė. Sistema parengiama ne vėliau kaip... [15 mėnesių po šio reglamento įsigaliojimo].

2. Sistema apima visą atitinkam**o Sąjungos** [...] **subjekto** neįslaptintą IT aplinką, įskaitant bet kokią vietoje esančią IT aplinką, **operacinį technologijų tinklą**, 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. Sistema **grindžiama visus pavojus apimančiu požiūriu ir kibernetinio saugumo brandos vertinimu pagal 6 straipsnį, apimančiais visą atitinkamą techninę, operacinę ir organizacinę riziką, kuri gali daryti poveikį atitinkamo Sąjungos subjekto kibernetiniam saugumui** [...].

2a. **Sistemoje nustatoma kibernetinio saugumo politika, įskaitant tinklų ir informacinių sistemų saugumo tikslus ir prioritetus, taip pat politika ir procedūros, kuriomis siekiama įvertinti įgyvendintų kibernetinio saugumo rizikos valdymo priemonių veiksmingumą ir apibrėžti darbuotojų vaidmenis ir atsakomybę.**

2b. Sistema peržiūrima reguliariai bent kas trejus metus, atsižvelgiant į kintančią Sąjungos subjektui kylančią riziką, jo kintantį turtą ir kibernetinio saugumo brandą.

3. Kiekvien**o** Sąjungos [...] **subjekto** aukščiausio lygmens vadovybė prižiūri, kaip **jo** organizacija laikosi pareigų, susijusių su kibernetinio saugumo rizikos valdymu, valdymu ir kontrole, nedarydama poveikio oficialiai kitų lygmenų vadovybės atsakomybei laikytis įpareigojimų ir valdyti riziką jų atitinkamose atsakomybės srityse.

3a. **Kai tikslinga ir nedarant poveikio kiekvieno Sąjungos subjekto aukščiausio lygmens vadovybės atsakomybei už šio reglamento įgyvendinimą, ši vadovybė gali kitiems atitinkamo subjekto vyresniesiems pareigūnams deleguoti konkrečią pareigą pagal šį reglamentą. Nepriklausomai nuo to, ar konkreti jos pareiga gali būti perduota, aukščiausio lygmens vadovybė gali būti laikoma atsakinga už tai, kad subjektai nesilaiko šiame reglamente nustatytų pareigų.**

3b. Kiekvieno Sąjungos subjekto aukščiausio lygmens vadovybė užtikrina, kad Sąjungos subjektai, remdamiesi savo rizikos analize, patvirtintų kibernetinio saugumo planą, į kurį būtų įtrauktos kibernetinio saugumo rizikos valdymo priemonės, kad sistema būtų įgyvendinama pagal šį reglamentą.

[...]

5. Kiekvien**as** Sąjungos [...] **subjektas** paskiria vietos kibernetinio saugumo pareigūną arba lygiavertę funkciją atliekantį pareigūną, kuris visais kibernetinio saugumo aspektais veikia kaip vienas kontaktinis asmuo.

Vietos kibernetinio saugumo pareigūnas sudaro palankesnes sąlygas įgyvendinti šį reglamentą ir aukščiausio lygmens vadovybei reguliariai tiesiogiai teikia ataskaitas apie įgyvendinimo padėtį.

Nedarant poveikio tam, kad vietos kibernetinio saugumo pareigūnas veikia kaip vienas kontaktinis asmuo kiekviename Sąjungos subjekte, Sąjungos subjektas gali CERT-EU deleguoti tam tikras vietos kibernetinio saugumo pareigūno užduotis, susijusias su šio reglamento įgyvendinimu, remdamasis to Sąjungos subjekto ir CERT-EU sudarytu susitarimu dėl paslaugų lygio. TKST, atsižvelgdama į atitinkamo Sąjungos subjekto žmogiškuosius ir finansinius išteklius, nusprendžia, ar šios paslaugos turi būti teikiamos kaip CERT-EU pagrindinių paslaugų dalis. Kiekvienas Sąjungos subjektas nepagrįstai nedelsdamas praneša CERT-EU apie paskirtus vietos kibernetinio saugumo pareigūnus ir apie visus vėlesnius jų pakeitimus. CERT-EU nuolat atnaujina paskirtų vietos kibernetinio saugumo pareigūnų sąrašą.

6. Kiekvieno Sąjungos subjekto vyresnieji pareigūnai, kaip tai suprantama Tarnybos nuostatų[11] 29 straipsnio 2 dalyje, arba kiti lygiaverčio lygmens pareigūnai reguliariai dalyvauja specialiuose mokymuose, kad įgytų pakankamai žinių ir įgūdžių, kurių reikia siekiant suprasti ir įvertinti riziką kibernetiniam saugumui ir jos valdymo praktiką bei jų poveikį organizacijoms operacijoms.

11 1968 m. vasario 29 d. Tarybos reglamentas Nr. 259/68, nustatantis Europos Bendrijų pareigūnų tarnybos nuostatus ir kitų Europos Bendrijų tarnautojų įdarbinimo sąlygas (OL L 56, 1968 3 4).

7. Kiekvienas Sąjungos subjektas įdiegia veiksmingus mechanizmus, kuriais užtikrinama, kad kibernetiniam saugumui būtų išleidžiama tinkama IT biudžeto lėšų procentinė dalis. Nustatant šią procentinę dalį tinkamai atsižvelgiama į sistemą.

5 straipsnis

Kibernetinio saugumo <u>rizikos valdymo priemonės</u> [...]

1. [...] **Kiekvienas Sąjungos subjektas, prižiūrimas jo** aukščiausio lygmens vadovybės [...] **užtikrina, kad būtų imtasi tinkamų ir proporcingų techninių, operacinių ir organizacinių priemonių, skirtų rizikai, nustatytai taikant 4 straipsnio 1 dalyje nurodytą sistemą, valdyti ir incidentų prevencijai ir (arba) jų poveikiui sumažinti. Atsižvelgiant į moderniausius ir, kai taikytina, aktualius Europos ir tarptautinius standartus, taip pat į įgyvendinimo sąnaudas, tomis priemonėmis užtikrinamas tinklų ir informacinių sistemų saugumo lygis, atitinkantis keliamą riziką. Vertinant tų priemonių proporcingumą, tinkamai atsižvelgiama į subjekto patiriamos rizikos laipsnį, jo dydį, incidentų tikimybę ir jų rimtumą, įskaitant jų poveikį visuomenei ir ekonomikai.**

[...]

3. Sąjungos subjektai, įgyvendindami savo kibernetinio saugumo planuose nustatytas kibernetinio saugumo rizikos valdymo priemones, vadovaudamiesi TKSV rekomendaciniais dokumentais ir rekomendacijomis, imasi priemonių bent šiose konkrečiose srityse:

a) kibernetinio saugumo politikos įrankių ir priemonių, reikalingų 4 straipsnyje ir 5 straipsnio 4 dalyje nurodytiems tikslams ir prioritetams pasiekti, nustatymo;

b) rizikos analizės ir informacinių sistemų saugumo politikos;

c) kibernetinio saugumo organizavimo, įskaitant vaidmenų ir atsakomybės apibrėžimą;

d) turto valdymo, įskaitant IT turto aprašo ir IT tinklo kartografijos sudarymą;

e) žmogiškųjų išteklių saugumo ir prieigos kontrolės;

f) operacijų saugumo;

g) ryšių saugumo;

h) sistemos įsigijimo, plėtojimo ir techninės priežiūros, įskaitant pažeidžiamumo valdymą ir atskleidimą;

i) tiekimo grandinės saugumo, įskaitant saugumo aspektus, susijusius su kiekvieno Sąjungos subjekto ir jo tiesioginių tiekėjų ar paslaugų teikėjo santykiais. Sąjungos subjektai atsižvelgia į kiekvienam tiesioginiam tiekėjui ir paslaugų teikėjui būdingą pažeidžiamumą ir bendrą jų tiekėjų bei paslaugų teikėjų produktų kokybę ir kibernetinio saugumo praktiką, įskaitant jų saugaus kūrimo procedūras;

j) incidentų valdymo ir bendradarbiavimo su CERT-EU, pavyzdžiui, saugumo stebėsenos ir registravimo užtikrinimo;

k) veiklos tęstinumo valdymo, pvz., atsarginių kopijų valdymo ir veiklos atkūrimo po ekstremaliųjų įvykių, ir krizių valdymo, ir

l) švietimo, įgūdžių, informuotumo didinimo, pratybų ir mokymo programų kibernetinio saugumo srityje skatinimo ir plėtojimo.

4. Sąjungos subjektai, įgyvendindami savo kibernetinio saugumo planuose nustatytas kibernetinio saugumo rizikos valdymo priemones, vadovaudamiesi TKSV rekomendaciniais dokumentais ir rekomendacijomis, imasi bent šių konkrečių kibernetinio saugumo rizikos valdymo priemonių, apimančių:

a) tikslus ir prioritetus, susijusius su debesijos kompiuterijos paslaugų naudojimu, kaip tai suprantama Direktyvos [pasiūlymas dėl TIS 2] 4 straipsnio 19 punkte, ir techninėmis priemonėmis, kuriomis sudaromos sąlygos nuotoliniam darbui;

b) konkrečius veiksmus siekiant ateityje pereiti prie nulinio pasitikėjimo principų, įskaitant saugumo modelį, ir suderintą kibernetinio saugumo ir sistemos valdymo strategiją, grindžiamą pripažinimu, kad grėsmės egzistuoja tiek tradiciniuose tinkluose, tiek už jų ribų;

c) daugiaveiksnio tapatumo nustatymą, kuris taptų visuose tinkluose ir informacinėse sistemose taikomu standartu;

d) programinės įrangos tiekimo grandinės saugumo užtikrinimą taikant saugios programinės įrangos kūrimo ir vertinimo kriterijus;

e) viešųjų pirkimų taisyklių sugriežtinimą, kad būtų sudarytos palankesnės sąlygos užtikrinti aukštą bendrą kibernetinio saugumo lygį:

i) pašalinant sutartines kliūtis, kuriomis ribojamas IT paslaugų teikėjų dalijimasis informacija apie incidentus, pažeidžiamumą ir kibernetines grėsmes su CERT-EU;

ii) nustatant sutartinę prievolę pranešti apie incidentus, pažeidžiamumą bei kibernetines grėsmes, taip pat užtikrinant tinkamą reagavimą į incidentus bei jų stebėseną;

f) kriptografijos ir šifravimo, visų pirma ištisinio šifravimo, naudojimą;

g) saugias ryšių sistemas organizacijoje.

6 straipsnis

Kibernetinio saugumo brandos vertinimai

1. Kiekvienas Sąjungos [...] **subjektas**, **kai tinkama padedant specializuotai trečiajai šaliai**, bent kas trejus metus atlieka [...] kibernetinio saugumo brandos vertinimą, apimantį visus jo IT aplinkos elementus, kaip aprašyta 4 straipsnyje, atsižvelgdam**as** į atitinkamus pagal 13 straipsnį priimtus rekomendacinius dokumentus ir rekomendacijas.

2. TKST, remdamasi CERT-EU rekomendacija ir pasikonsultavusi su Europos Sąjungos kibernetinio saugumo agentūra (ENISA), per keturis mėnesius po šio reglamento įsigaliojimo priima metodines kibernetinio saugumo brandos vertinimo atlikimo gaires.

3. Atlikę kibernetinio saugumo brandos vertinimą [...], Sąjungos subjektai jį pateikia TKST. Pirmasis kibernetinio saugumo brandos vertinimas atliekamas ne vėliau kaip [12 mėnesių po šio reglamento įsigaliojimo].

7 straipsnis

Kibernetinio saugumo planai

1. Remdamasi išvadomis, padarytomis atlikus kibernetinio saugumo brandos vertinimą, ir atsižvelgdama į turtą bei riziką, nustatytus pagal 4 straipsnį, kiekvien**o** Sąjungos [...] **subjekto** aukščiausio lygmens vadovybė nepagrįstai nedelsdama, po to kai nustatoma [...] sistema, **patvirtinamos** kibernetinio saugumo **rizikos valdymo priemonės** [...] **ir atliekamas kibernetinio saugumo brandos vertinimas, ne vėliau kaip praėjus 21 mėnesiui po šio reglamento įsigaliojimo** patvirtina [...] kibernetinio saugumo planą. **Kibernetinio saugumo** planu siekiama padidinti bendrą atitinkamo **Sąjungos** subjekto kibernetinį saugumą ir taip prisidėti prie aukšto bendro visų Sąjungos [...] **subjektų** kibernetinio saugumo lygio [...] padidinimo. [...] Į **kibernetinio saugumo** planą įtraukiamos bent **pagal 5 straipsnį nustatytos kibernetinio saugumo rizikos valdymo priemonės** [...]. **Kibernetinio saugumo** planas peržiūrimas bent kas **dvejus** [...] metus **arba** po **kiekvieno** kibernetinio saugumo brandos vertinimo, [...] atlikto pagal 6 straipsnį, **arba po kiekvienos pagal 4 straipsnį atliktos sistemos peržiūros**.

2. [...]

3. Kibernetinio saugumo plane **atsižvelgiama į** [...] visus taikomus rekomendacinius dokumentus ir rekomendacijas, paskelbtus **pagal 13 straipsnį** [...].

4. **Parengtą kibernetinio saugumo planą Sąjungos subjektas pateikia TKST.**

7a straipsnis

Tarpusavio vertinimas

1. TKST, vadovaudamasi CERT-EU rekomendacija ir pasikonsultavusi su ENISA, ne vėliau kaip... [24 mėnesiai po šio reglamento įsigaliojimo], taikydama tarpusavio vertinimų metodiką ir įsivertinimo metodiką pagal Direktyvos [pasiūlymas dėl TIS 2] 16 straipsnį, prireikus pritaikytas prie Sąjungos subjektų poreikių, nustato tarpusavio vertinimo metodiką ir organizacinius aspektus siekiant pasinaudoti bendra patirtimi, stiprinti tarpusavio pasitikėjimą, užtikrinti aukštą bendrą kibernetinio saugumo lygį, taip pat plėtoti Sąjungos subjektų kibernetinio saugumo pajėgumus ir politiką, būtinus šiam reglamentui įgyvendinti. Dalyvavimas tarpusavio vertinimo veikloje yra savanoriškas. Valstybių narių atstovai gali dalyvauti tarpusavio vertinime kaip stebėtojai. Tarpusavio vertinimus atlieka bent dviejų Sąjungos subjektų paskirti kibernetinio saugumo ekspertai, kurie nepriklauso vertinamiems Sąjungos subjektams, ir jo metu įvertinamas bent vienas iš šių aspektų:

i) 5 ir 20 straipsniuose nurodytų kibernetinio saugumo rizikos valdymo priemonių ir pranešimo pareigų įgyvendinimas;

ii) pajėgumų lygis, įskaitant turimus finansinius, techninius ir žmogiškuosius išteklius;

iii) 19 straipsnyje nurodytos dalijimosi informacija sistemos įgyvendinimas;

iv) konkretūs tarpsektorinio pobūdžio klausimai.

2. Sąjungos subjektai gali nustatyti konkrečius 1 dalies iv punkte nurodytus klausimus, kurie turi būti įvertinti. Apie įvertinimo taikymo sritį, įskaitant nustatytus klausimus, dalyvaujantiems Sąjungos subjektams pranešama prieš pradedant tarpusavio vertinimą.

3. Prieš pradėdami tarpusavio vertinimą, Sąjungos subjektai gali atlikti vertinamų aspektų įsivertinimą ir to įsivertinimo rezultatus pateikti paskirtiems ekspertams.

4. Tarpusavio vertinimai apima fizinius arba virtualius apsilankymus vietoje ir keitimąsi informacija ne vietoje. Atsižvelgiant į gero bendradarbiavimo principą, Sąjungos subjektai, kuriuose atliekamas tarpusavio vertinimas, paskirtiems ekspertams pateikia vertinimui reikalingą informaciją, nedarydami poveikio nacionalinės ar Sąjungos teisės aktams dėl neskelbtinos ar įslaptintos informacijos apsaugos. Visa tarpusavio vertinimo proceso metu gauta informacija naudojama tik tuo tikslu. Tarpusavio vertinime dalyvaujantys ekspertai jokioms trečiosioms šalims neatskleidžia jokios tos peržiūros metu gautos neskelbtinos ar konfidencialios informacijos.

5. Atlikus tarpusavio vertinimą, Sąjungos subjektų tų pačių įvertintų aspektų papildomas tarpusavio vertinimas tuose Sąjungos subjektuose neatliekamas dvejus metus po tarpusavio vertinimo užbaigimo, nebent to paprašo Sąjungos subjektai arba dėl to susitariama gavus TKST pasiūlymą.

6. Sąjungos subjektai užtikrina, kad prieš pradedant tarpusavio vertinimą kitiems Sąjungos subjektams ir TKST būtų atskleista bet kokia paskirtųjų ekspertų interesų konflikto rizika. Sąjungos subjektai, kuriuose atliekamas tarpusavio vertinimas, dėl tinkamai pagrįstų priežasčių, apie kurias jie praneša ekspertus skiriantiems Sąjungos subjektams, gali prieštarauti dėl konkrečių ekspertų skyrimo.

7. **Tarpusavio vertinimuose dalyvaujantys ekspertai parengia vertinimo metu nustatytų faktų ir išvadų ataskaitas. Sąjungos subjektams leidžiama pateikti pastabas dėl joms skirtų atitinkamų ataskaitų projektų; šios pastabos pridedamos prie ataskaitos. Ataskaitose pateikiamos rekomendacijos, kad būtų galima pagerinti aspektus, kuriems taikytas tarpusavio vertinimas. Kai tinkama, ataskaitos pateikiamos TKST ir CSIRT tinklui. Vertinami Sąjungos subjektai gali nuspręsti viešai paskelbti jiems skirtą ataskaitą arba jos santrauką.**

8 straipsnis

Įgyvendinimas

1. [...]

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

3. **TKST prašymu Sąjungos subjektai teikia ataskaitas dėl konkrečių šio skyriaus aspektų.**

III skyrius
TARPINSTITUCINĖ KIBERNETINIO SAUGUMO VALDYBA

9 straipsnis

Tarpinstitucinė kibernetinio saugumo taryba

1. Įsteigiama Tarpinstitucinė kibernetinio saugumo taryba (TKST).

2. TKST pareigos:

   a) stebėti, kaip **Sąjungos** [...] **subjektai** įgyvendina šį reglamentą;

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

3. TKST sudaro**:**

   a) po vieną atstovą, paskirtą toliau nurodytų subjektų:

      i) Europos Parlamento;

      ii) Europos Vadovų Tarybos;

      iii) Europos Sąjungos Tarybos;

      iv) Europos Komisijos;

      v) Europos Sąjungos Teisingumo Teismo;

      vi) Europos Centrinio Banko;

vii) Europos Audito Rūmų;

viii) Europos išorės veiksmų tarnybos;

ix) Europos ekonomikos ir socialinių reikalų komiteto;

x) Europos regionų komiteto;

xi) Europos investicijų banko;

xii) Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centro ir

xiii) Europos Sąjungos kibernetinio saugumo agentūros;

b) [...] trys atstovai, kuriuos, remdamasis [...] IRT patariamojo komiteto siūlymu **paskiria** Sąjungos agentūrų tinklas **(SAT)**, kad jie atstovautų agentūrų ir įstaigų, kurios valdo savo pačių IT aplinką, interesams. [...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

3a. Nariams gali padėti pakaitiniai nariai. Pirmininkas gali kviesti kitus pirmiau išvardytų **subjektų** [...] arba kitų Sąjungos [...] **subjektų** 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 [...] **dvejų** metų laikotarpiui paskiria pirmininką. Jo pakaitinis narys tam pačiam laikotarpiui tampa tikruoju TKST nariu.

6. TKST renkasi **bent tris kartus per metus** savo pirmininko iniciatyva **ir (arba)** CERT-EU prašymu, **ir** (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, **TIS bendradarbiavimo grupės pirmininkas, EU-CyCLONe pirmininkas ir CSIRT tinklo pirmininkas** arba **jų** pakaitin**iai** nar**iai gali stebėtojų teisėmis** dalyvau**ti** TKST posėdžiuose, išskyrus atvejus, kai TKST nusprendžia kitaip.

10. Sekretoriato paslaugas TKST teikia **ENISA** [...] **ir ji yra atskaitinga TKST pirmininkui**.

11. IRT patariamojo komiteto siūlymu SAT paskirti atstovai perduoda TKST sprendimus **SAT nariams** [...]. 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. [...]

13. TKST gali **įsteigti** [...] vykdomąjį komitetą, kuris padėtų jai vykdyti darbą, ir deleguoti jam kai kurias savo užduotis ir įgaliojimus**, visų pirma nurodytus 10 straipsnio c ir e punktuose**. TKST nustato vykdomojo komiteto darbo tvarkos taisykles, įskaitant jo užduotis bei įgaliojimus ir jo narių kadencijos trukmę.

14. TKST kas 12 mėnesių pateikia Tarybai ataskaitą, kurioje išsamiai apibūdinama pažanga, padaryta įgyvendinant šį reglamentą, ir visų pirma nurodomas CERT-EU bendradarbiavimo su nacionaliniais partneriais kiekvienoje valstybėje narėje mastas. Ši ataskaita įtraukiama į kas dvejus metus pagal Direktyvos [pasiūlymas dėl TIS 2] 15 straipsnį rengiamą ataskaitą dėl kibernetinio saugumo padėties Sąjungoje tuo pačiu laikotarpiu.

10 straipsnis

TKST užduotys

Vykdydama savo pareigas TKST visų pirma:

a) [...] **veiksmingai stebi ir prižiūri** šio reglamento **taikymą** [...] **ir padeda** Sąjungos [...] **subjektams stiprinti savo kibernetinį saugumą; šiuo tikslu TKST gali prašyti CERT-EU ir Sąjungos subjektų *ad hoc* ataskaitų;**

aa) **po strateginių diskusijų priima daugiametę strategiją dėl kibernetinio saugumo lygio didinimo Sąjungos subjektuose ir reguliariai, bent kas penkerius metus, ją įvertina ir prireikus iš dalies pakeičia;**

b) remdamasi CERT-EU vadovo **pateiktu** pasiūlymu tvirtina CERT-EU metinę darbo programą ir stebi, kaip ji įgyvendinama;

c) remdamasi CERT-EU vadovo siūlymu tvirtina CERT-EU paslaugų katalogą **ir visus jo vėlesnius atnaujinimus**;

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 [...] techni**nes** patariam**ąsias** grup**es** [...] siekiant prisidėti prie TKST darbo, tvirtina jų įgaliojimus ir skiria atitinkamus jų pirmininkus.

j) **priima rekomendacinius dokumentus ir rekomendacijas, remdamasi CERT-EU pasiūlymu pagal 13 straipsnį, ir nurodo CERT-EU paskelbti, atsiimti arba pakeisti pasiūlymą dėl rekomendacinių dokumentų ar rekomendacijų arba raginimą imtis veiksmų;**

k) gauna ir vertina Sąjungos subjektų pagal šį reglamentą pateiktus dokumentus ir ataskaitas;

l) remia neformalios visų subjektų vietos kibernetinio saugumo pareigūnų grupės įsteigimą ir taip palengvina keitimąsi geriausios praktikos pavyzdžiais ir informacija, susijusiais su šio reglamento įgyvendinimu;

m) parengia kibernetinių krizių valdymo planą, kuris padėtų operaciniu lygmeniu suderintai valdyti didelius incidentus, darančius poveikį Sąjungos subjektams, ir prisidėti prie reguliaraus keitimosi atitinkama informacija, visų pirma apie didelių incidentų poveikį bei rimtumą ir galimus poveikio sumažinimo būdus.

11 straipsnis

Reikalavimų laikymasis

1. TKST **pagal 9 straipsnio 2 dalį ir 10 straipsnį veiksmingai** stebi, kaip įgyvendinamas šis reglamentas ir priimti rekomendaciniai dokumentai, rekomendacijos ir raginimai Sąjungos [...] **subjektams** imtis veiksmų. **Šiuo tikslu TKST gali prašyti informacijos ar dokumentų, būtinų siekiant įvertinti, ar Sąjungos subjektai tinkamai taiko reglamento nuostatas. Atitikties užtikrinimo priemonių priėmimo pagal šį straipsnį tikslais atitinkamam Sąjungos subjektui balsavimo teisės nesuteikiamos.**

2. Jei TKST nustato, kad Sąjungos [...] **subjektai** veiksmingai netaikė arba neįgyvendino šio reglamento arba rekomendacinių dokumentų, rekomendacijų ir raginimų imtis veiksmų pagal šį reglamentą, nedarydama poveikio atitinkamo Sąjungos [...] **subjekto** vidaus procedūroms **ir suteikusi galimybę atitinkamam subjektui arba asmeniui pateikti savo nuomonę,** TKST gali:

a) paskelbti perspėjimą**, kad per konkretų laikotarpį būtų pašalinti nustatyti trūkumai, įskaitant rekomendacijas iš dalies pakeisti kibernetinio saugumo dokumentus, kuriuos Sąjungos subjektai priėmė remdamiesi šiuo reglamentu;** kai tai būtina atsižvelgiant į akivaizdžią riziką kibernetiniam saugumui, tinkamai apriboti auditoriją, kuriai perspėjimas skirtas;

aa) Sąjungos subjektui pateikti pagrįstą pranešimą, jei per konkretų laikotarpį nebuvo visiškai pašalinti anksčiau paskelbtame perspėjime nustatyti trūkumai, ir oficialiai pranešti apie tą nuomonę Tarybai, Europos Parlamentui ir Komisijai;

b) **visų pirma paskelbti:** [...]

i. rekomendaciją atlikti Sąjungos subjekto auditą;

ii. prašymą, kad auditą atliktų trečiosios šalies audito tarnyba;

c) prašyti, kad Sąjungos subjektas kibernetinės rizikos valdymą, valdymą ir kontrolę suderintų su šio reglamento nuostatomis, kai tinkama, nustatytu būdu ir per nustatytą laikotarpį;

d) pateikti patariamojo pobūdžio raštą visoms valstybėms narėms ir Sąjungos subjektams, rekomenduodama laikinai sustabdyti duomenų srautus į Sąjungos subjektą.

3. Jeigu TKST yra patvirtinusi priemones pagal 2 dalies a-d punktus, atitinkamas Sąjungos subjektas pateikia išsamią ataskaitą apie priemones ir veiksmus, kurių imtasi TKST nustatytiems įtariamiems trūkumams pašalinti. Sąjungos subjektas pateikia šią sąskaitą per pagrįstą laikotarpį, dėl kurio turi būti susitarta su TKST.

4. **Jeigu TKST mano, kad Sąjungos subjektas nuolat pažeidžia šio reglamento nuostatas tiesiogiai dėl Sąjungos subjekto pareigūno ar kito tarnautojo, įskaitant aukščiausio lygmens vadovybę, veiksmų ar neveikimo, TKST prašo atitinkamo subjekto imtis atitinkamų, be kita ko, drausminio pobūdžio, veiksmų, visų pirma laikantis Tarnybos nuostatuose ir kitų Europos Sąjungos tarnautojų įdarbinimo sąlygose nustatytų taisyklių. Šiuo tikslu TKST perduoda reikiamą informaciją atitinkamam subjektui.**

IV skyrius
CERT-EU

12 straipsnis

CERT-EU misija ir užduotys

1. [...] [...] **CERT-EU misija** – prisidėti prie visų Sąjungos [...] **subjektų neįslaptintos** IT aplinkos saugumo, konsultuo**jant juos kibernetinio saugumo klausimais**, padedant **jiems** užkirsti kelią incidentams, juos aptikti, sušvelninti jų poveikį ir į juos reaguoti, taip pat veiki**ant** kaip jų keitimosi kibernetinio saugumo informacija ir reagavimo į incidentus koordinavimo centras.

1a. CERT-EU neįslaptintoje IRT infrastruktūroje renka, tvarko, analizuoja informaciją apie grėsmes, pažeidžiamumą bei incidentus ir ja dalijasi su Sąjungos subjektais. Ji koordinuoja reagavimą į incidentus tarpinstituciniu ir Sąjungos subjektų lygmeniu, be kita ko, teikdama specializuotą operatyvinę pagalbą arba koordinuodama jos teikimą.

2. CERT-EU Sąjungos [...] **subjektams** atlieka šias užduotis:

a) padeda **jiems** įgyvendinti šį reglamentą ir prisideda prie šio reglamento taikymo koordinavimo taikydama 13 straipsnio 1 dalyje išvardytas [...] **nuostatas** arba teikdama TKST prašomas *ad hoc* ataskaitas;

b) [...] **visiems Sąjungos subjektams siūlo standartines CSIRT 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) **remdamasi 1a dalyje nurodyta informacija** [...] **ir glaudžiai bendradarbiaudama su ENISA** prisideda prie informuotumo apie kibernetinę padėtį ES. **Tokia informacija dalijamasi su TKST, taip pat CSIRT tinklu ir EU INTCEN;**

f) veikia kaip paskirto Sąjungos subjektų koordinatoriaus, kaip nurodyta Direktyvos [pasiūlymas dėl TIS 2] 6 straipsnyje, atitikmuo.

[...]

[...]

[...]

[...]

[...]

4. **Savo kompetencijos srityje** CERT-EU vykdo struktūrinį bendradarbiavimą su [...] **ENISA** 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 [...] **subjektų** 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 [...] **subjektų** kibernetinio saugumo operacijos ar projektai, išskyrus tas, kuriomis jie siekia apsaugoti savo IT aplinką, teikiamas remiantis rašytiniais susitarimais ir gavus išankstinį TKST pritarimą;

   c) paslaugas, kuriomis remiamas organizacijų, kurios nėra Sąjungos [...] **subjektai**, bet glaudžiai su jais 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 jose dalyvauti**, arba rekomenduoti dalyvauti vykdomose pratybose, kai tinkama, glaudžiai bendradarbiaudama su [...] **ENISA**, kad patikrintų Sąjungos [...] **subjektų** kibernetinio saugumo lygį.

7. CERT-EU gali teikti pagalbą Sąjungos [...] **subjektams** dėl incidentų įslaptintoje IT aplinkoje, jei to aiškiai paprašo **atitinkami Sąjungos subjektai pagal savo atitinkamas procedūras**. **Tokiu atveju šio reglamento 19–21 straipsniuose išdėstytos nuostatos netaikomos. CERT-EU pagalbos teikimas pagal šią dalį nedaro poveikio taikomoms valstybės narės ar Sąjungos taisyklėms dėl neskelbtinos ar įslaptintos informacijos apsaugos.**

8. CERT-EU informuoja Sąjungos subjektus apie incidentų valdymo procedūras ir procesus.

9. CERT-EU, gavusi atitinkamo Sąjungos subjekto sutikimą, gali stebėti Sąjungos subjektų tinklo srautą.

10. CERT-EU gali, jei to aiškiai paprašo Sąjungos subjektų politiniai skyriai, pateikti technines rekomendacijas arba nuomonę atitinkamais politiniais klausimais.

11. CERT-EU, bendradarbiaudama su Europos duomenų apsaugos priežiūros pareigūnu, padeda atitinkamiems Sąjungos subjektams pašalinti su asmens duomenų saugumo pažeidimais susijusius incidentus.

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 [...] **subjektai** raginam**i** imtis per nustatytą laikotarpį. Gavęs raginimą imtis veiksmų, atitinkamas Sąjungos subjektas nepagrįstai nedelsdamas informuoja CERT-EU apie tai, kaip tos priemonės buvo taikomos;

   b) pasiūlymus TKST dėl rekomendacinių dokumentų, skirtų visiems Sąjungos [...] **subjektams** arba jų daliai;

   c) pasiūlymus TKST dėl atskir**iems** Sąjungos [...] **subjektams** skirtų rekomendacijų.

2. Rekomendaciniai dokumentai ir rekomendacijos gali apimti:

   a) kibernetinio saugumo rizikos valdymo ir kibernetinio saugumo **rizikos valdymo priemonių** tobulinimo sąlygas [...];

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

   c) kai tinkama, bendrų technologijų, architektūros ir susijusios geriausios praktikos naudojimą siekiant užtikrinti sąveikumą ir bendrus standartus, **įskaitanti suderintą požiūrį į tiekimo grandinių saugumą** [...].

[...]

[...]

14 straipsnis

CERT-EU vadovas

1. Komisija, gavusi dviejų trečdalių TKST narių 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. CERT-EU vadovas yra atsakingas už sklandų CERT-EU veikimą ir eina pareigas savo kompetencijos srityje vadovaujant TKST. Jis yra atsakingas už TKST nustatytų strateginių krypčių, gairių, tikslų ir prioritetų įgyvendinimą, taip pat už CERT-EU valdymą, įskaitant jos finansinius ir žmogiškuosius išteklius. Jis reguliariai atsiskaito TKST pirmininkui.

3. CERT-EU vadovas padeda atsakingam įgaliotajam leidimus suteikiančiam pareigūnui pagal Finansinio reglamento 66 straipsnio 9 dalį parengti metinę veiklos ataskaitą, kurioje pateikiama finansinė ir valdymo informacija, įskaitant kontrolės rezultatus, ir reguliariai jam teikia ataskaitas dėl priemonių, kurių atžvilgiu jam buvo perdeleguoti įgaliojimai, įgyvendinimo.

4. CERT-EU vadovas kasmet parengia savo veiklos administracinių pajamų ir išlaidų finansinį planą, pasiūlymą dėl metinės darbo programos, pasiūlymą dėl CERT-EU paslaugų katalogo ir jo peržiūros, pasiūlymą dėl susitarimų dėl paslaugų lygio sąlygų ir pasiūlymą dėl CERT-EU pagrindinių veiklos rezultatų rodiklių, kuriuos pagal 10 straipsnį turi patvirtinti TKST.

Peržiūrėdamas CERT-EU paslaugų kataloge pateiktą paslaugų sąrašą, CERT-EU vadovas atsižvelgia į CERT-EU skirtus išteklius.

5. CERT-EU vadovas [...] teikia **metines** ataskaitas TKST [...] 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 [...] **a punkte** nurodytas ataskaitas.

15 straipsnis

Finansiniai ir personalo formavimo klausimai

[...]

1a. CERT-EU įsteigiama kaip savarankiška tarpinstitucinė paslaugų teikėja visiems Sąjungos subjektams, integruota į Komisijos generalinio direktorato administracinę struktūrą, kad galėtų naudotis Komisijos administracinėmis, finansinėmis, valdymo ir apskaitos pagalbinėmis struktūromis. Komisija praneša TKST apie CERT-EU vietą administracinėje struktūroje ir apie visus su tuo susijusius pokyčius. Šis metodas reguliariai vertinamas vėliausiai iki bet kurios daugiametės finansinės programos, nustatytos pagal SESV 312 straipsnį, pabaigos, kad būtų galima imtis atitinkamų veiksmų.

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

3. CERT-EU užduotys ir veikla, įskaitant pagal 12 straipsnio 2, [...] 4 bei 6 dalis ir 13 straipsnio 1 dalį CERT-EU teikiamas paslaugas Sąjungos [...] **subjektams**, 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. Kiti nei 3 dalyje nurodyt**i** Sąjungos [...] **subjektai** 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[12] 21 straipsnio 3 dalies c punkte.

5. Su 12 straipsnio 5 dalyje apibrėžtomis užduotimis susijusios išlaidos susigrąžinamos iš CERT-EU paslaugas gaunančių Sąjungos [...] **subjektų**. Pajamos priskiriamos išlaidoms padengti skirtoms biudžeto eilutėms.

[12] 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).

16 straipsnis

CERT-EU bendradarbiavimas su partneriais iš valstybių narių

1. CERT-EU **nepagrįstai nedelsdama** bendradarbiauja ir keičiasi informacija su nacionaliniais partneriais iš valstybių narių, **konkrečiai su** – [...] [...] [...] **Direktyvos [pasiūlymas dėl TIS 2] 9 straipsnyje nurodytais CSIRT ir (arba), kai taikytina, nacionalinėmis kompetentingomis institucijomis** ir Direktyvos [pasiūlymas dėl TIS 2] 8 straipsnyje nurodytais bendrais kontaktiniais asmenimis, klausimais, susijusiais su kibernetinėmis grėsmėmis, pažeidžiamumu ir incidentais, galimomis atsakomosiomis priemonėmis, ir visais klausimais, susijusiais su Sąjungos [...] **subjektų** IT aplinkos apsaugos gerinimu, be kita ko, pasitelkiant Direktyvos [pasiūlymas dėl TIS 2] 13 straipsnyje nurodytą CSIRT tinklą.

1a. Sužinojusi apie reikšmingus incidentus, įvykusius valstybės narės teritorijoje, CERT-EU nedelsdama apie tai praneša visiems 1 dalyje nurodytiems atitinkamiems nacionaliniams partneriams toje valstybėje narėje, nebent CERT-EU turi informacijos, kad paveiktas Sąjungos subjektas jau yra pranešęs apie tokį incidentą pagal 20 straipsnio 2a dalį.

2. CERT-EU **nepagrįstai nedelsdama** [...] pasikeičia su incidentais susijusia informacija su nacionaliniais partneriais iš valstybių narių, kad būtų lengviau aptikti panašias kibernetines grėsmes ar incidentus **arba prisidėti prie incidento analizės** [...] **neprašant** paveikto **Sąjungos subjekto** sutikimo. CERT-EU **nesikeičia** [...] su incidentu susijusia informacija, kurioje atskleidžiama kibernetinio saugumo incidento taikinio tapatybė, **nebent** [...]:

   a) yra gautas paveikto Sąjungos subjekto sutikimas;

   b) paveiktas Sąjungos subjektas jau paskelbė, kad jam buvo darytas poveikis;

c) paveiktas Sąjungos subjektas nėra davęs sutikimo, tačiau paskelbus paveikto Sąjungos subjekto tapatybę padidėtų tikimybė, kad bus išvengta incidentų arba jie bus sušvelninti kitur. Tokius sprendimus turi patvirtinti CERT-EU vadovas. Paveiktas Sąjungos subjektas informuojamas prieš informacijos paskelbimą.

17 straipsnis

CERT-EU bendradarbiavimas su kitais partneriais [...]

1. CERT-EU gali bendradarbiauti su partneriais [...] **Europos Sąjungoje, išskyrus nurodytus 16 straipsnyje,** įskaitant pramonės sektorių partnerius, klausimais, susijusiais su priemonėmis ir metodais, pavyzdžiui, specialia metodika, taktika, procedūromis ir geriausios praktikos pavyzdžiais, taip pat su kibernetinėmis grėsmėmis bei pažeidžiamumu. Kad galėtų visapusiškai [...] bendradarbiauti su tokiais partneriais CERT-EU **kiekvienu atskiru atveju** turi gauti išankstinį TKST pritarimą. **CERT-EU informuoja visus atitinkamus nacionalinius partnerius, nurodytus 16 straipsnio 1 dalyje, valstybėje narėje, kurioje tas partneris yra įsteigtas, kai CERT-EU užmezga bendradarbiavimą su tokiais partneriais.**

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 **kiekvienu atskiru atveju** turi gauti išankstinį TKST pritarimą.

3. **Jei su atitinkamu partneriu yra sudarytas informacijos neatskleidimo susitarimas arba sutartis,** CERT-EU, gavusi nuo incidento nukentėjusio **Sąjungos subjekto** sutikimą, gali **1 ir 2 dalyse nurodytiems** partneriams pateikti informaciją, susijusią su **konkrečiu** incidentu, t**ik tuo tikslu, kad prisidėtų** prie jo analizės. **Tokie informacijos neatskleidimo susitarimai arba sutartys yra teisiškai patikrinami pagal atitinkamas Komisijos vidaus procedūras. Informacijos neatskleidimo susitarimams arba sutartims nereikia išankstinio TKST pritarimo, tačiau apie tai informuojamas jos pirmininkas.**

4. **CERT-EU, gavusi išankstinį TKST pritarimą, išskirtiniais atvejais gali sudaryti susitarimus dėl paslaugų lygio su subjektais, kurie nėra Sąjungos subjektai.**

V skyrius
BENDRADARBIAVIMAS IR PRANEŠIMO PAREIGOS

18 straipsnis

Informacijos tvarkymas

1. CERT-EU ir Sąjungos [...] **subjektai** 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[13] nuostatos, įskaitant tame reglamente nustatytą pareigą konsultuotis su kit**ais** Sąjungos [...] **subjektais ir, kai tikslinga, su valstybėmis narėmis,** kai prašymas susijęs su jų dokumentais.

[...]

4. CERT-EU ir Sąjungos [...] **subjektų** vykdomas informacijos tvarkymas turėtų atitikti **taikomas** taisykles [...] dėl informacijos saugumo [...];

[...]

19 straipsnis

*[...] **Dalijimasis kibernetinio saugumo informacija***

-1. Sąjungos subjektai gali savanoriškai teikti CERT-EU informaciją apie jiems poveikį darančias kibernetines grėsmes, incidentus, vos neįvykusius incidentus ir pažeidžiamumą. Siekdama palengvinti dalijimąsi informacija su Sąjungos subjektais, CERT-EU užtikrina veiksmingas ryšio priemones. CERT-EU gali teikti pirmenybę ne savanoriškų, o privalomų pranešimų tvarkymui.

[13] 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).

1. Kad [...] **galėtų vykdyti 12 straipsnyje apibrėžtą savo misiją ir užduotis**, CERT-EU [...] gali reikalauti, kad Sąjungos [...] **subjektai** jai teiktų informaciją iš savo atitinkamų IT sistemų aprašų, **įskaitant informaciją, susijusią su kibernetinėmis grėsmėmis, vos neįvykusiais incidentais, pažeidžiamumu, užvaldymo rodikliais, kibernetinio saugumo perspėjimais ir rekomendacijomis dėl kibernetinio saugumo priemonių, skirtų kibernetiniams incidentams aptikti, konfigūravimo** [...]. Sąjungos **subjektas**, į kurį kreipiamasi, nepagrįstai nedelsdam**as** perduoda prašomą informaciją ir visus vėlesnius jos atnaujinimus.

2. Sąjungos [...] **subjektai** CERT-EU prašymu nepagrįstai nedelsdam**i** 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 **su Sąjungos subjektais** keistis su incidentu susijusia informacija, kurioje atskleidžiama nuo kibernetinio saugumo incidento nukentėjus**io** Sąjungos [...] **subjekto** tapatybė, tik gavusi to subjekto sutikimą. **Jei sutikimas neduodamas, atitinkamas subjektas CERT-EU pateikia tinkamai pagrįstas priežastis.** [...]

4. Pareigos dalytis netaikomos ES įslaptintai informacijai (ESĮI) ir informacijai, **kurios platinti ne ją gaunančiam Sąjungos subjektui neleido informacijos rengėjas, ją aiškiai pažymėdamas, nebent informacijos rengėjas [...] aiškiai leidžia šia informacija dalytis su CERT-EU.** [...]

20 straipsnis

*[...] **Pranešimo** pareigos*

-1. Incidentas laikomas reikšmingu, jeigu:

a) jis sukėlė arba gali sukelti didelių Sąjungos subjekto veikimo sutrikdymų arba atitinkamam Sąjungos subjektui padarė ar gali padaryti finansinių nuostolių;

b) jis padarė arba gali padaryti poveikį kitiems fiziniams ar juridiniams asmenims, sukeldamas didelę turtinę ar neturtinę žalą.

1. Visi Sąjungos [...] **subjektai CERT-EU pateikia**: [...]

[...].

a) nepagrįstai nedelsdami ir bet kuriuo atveju per 24 valandas nuo to laiko, kai sužino apie reikšmingą incidentą – išankstinį perspėjimą, kuriame, kai taikytina, nurodoma, ar reikšmingą incidentą, kaip įtariama, sukėlė neteisėti ar piktavališki veiksmai ir ar jis daro ar galėtų daryti tarpvalstybinį poveikį;

b) nepagrįstai nedelsdami ir bet kuriuo atveju per 72 valandas nuo to laiko, kai sužino apie reikšmingą incidentą – pranešimą apie incidentą, kuriame, kai taikytina, atnaujinama a punkte nurodyta informacija ir nurodomas reikšmingo incidento, jo rimtumo ir poveikio **pradinis vertinimas**, taip pat užvaldymo **rodikliai**, jei tokių yra;

c) CERT-EU prašymu – tarpinę ataskaitą dėl atnaujintų duomenų apie padėtį;

d) ne vėliau kaip per vieną mėnesį nuo b punkte nurodyto pranešimo apie reikšmingą incidentą pateikimo – galutinę ataskaitą, kurioje pateikiama bent ši informacija:

i) išsamus reikšmingo incidento, jo rimtumo ir poveikio aprašymas;

ii) grėsmės arba pagrindinės priežasties, dėl kurios reikšmingas incidentas galėjo būti sukeltas, rūšis;

iii) taikomos ir įgyvendinamos poveikio sumažinimo priemonės;

iv) kai taikoma, reikšmingo incidento tarpvalstybinis poveikis;

e) jei d punkte nurodytos galutinės ataskaitos pateikimo metu įvyksta reikšmingi incidentai – iki tol padarytos pažangos ataskaitą, o per vieną mėnesį po to, kai incidentas buvo suvaldytas – galutinę ataskaitą.

[...]

g) [...]

h) [...]

i) [...]

j) [...]

2a. Visi Sąjungos subjektai pagal 1 dalį pateikta informacija per tą patį laikotarpį pasidalija su visais 16 straipsnio 1 dalyje nurodytais atitinkamais nacionaliniais partneriais jų įsteigimo vietoje.

3. CERT-EU [...] **kas tris mėnesius TKST, EU INTCEN ir CSIRT tinklui** [...] pateikia apibendrinamąją ataskaitą, įskaitant nuasmenintus ir apibendrintus duomenis apie [...] kibernetines grėsmes, [...] pažeidžiamumą **pagal 19 straipsnį**, **Sąjungos subjektų reagavimą į raginimus imtis veiksmų pagal 13 straipsnio 1 dalies a punktą** ir reikšmingus incidentus, apie kuriuos pranešta pagal 1 dalį. **Ta ataskaita įtraukiama į kas dvejus metus pagal Direktyvos [pasiūlymas dėl TIS 2] 15 straipsnį rengiamą ataskaitą dėl kibernetinio saugumo padėties Sąjungoje.**

4. TKST [...] **ne vėliau kaip [6 mėnesiai po šio reglamento įsigaliojimo dienos]** paskelb**ia** rekomendacinius dokumentus arba rekomendacijas, **kuriose tiksliau apibrėžiamos** pranešimo sąlyg**os**, **forma ir** turinys [...]. **Rekomendaciniuose dokumentuose arba rekomendacijose tinkamai atsižvelgiama į nuostatas, įgyvendinamas įgyvendinimo aktais pagal Direktyvos [pasiūlymas dėl TIS 2] 20 straipsnio 11 dalį.** CERT-EU platina atitinkamą techninę informaciją, kad Sąjungos [...] **subjektai** galėtų proaktyviai aptikti incidentus, reaguoti į juos arba imtis rizikos mažinimo priemonių.

5. [...] **Pranešimo** pareigos netaikomos ESĮI ir informacijai, **kurios platinti ne ją gaunančiam Sąjungos subjektui neleido informacijos rengėjas, ją aiškiai pažymėdamas, nebent informacijos rengėjas [...] aiškiai leidžia šia informacija dalytis su CERT-EU.** [...]

21 straipsnis

***Reagavimo į incidentus koordinavimas ir bendradarbiavimas** [...]*

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 [...] **subjektų**;

   b) 16 ir 17 straipsniuose nurodytų partnerių.

2. CERT-EU**, kai tinkama, glaudžiai bendradarbiaudama su ENISA pagal Kibernetinio saugumo akto[14] 7 straipsnio 7 dalies d punktą**, palengvina Sąjungos [...] **subjektų** reagavimo į incidentus koordinavimą, susijusį, be kita ko, su:

   a) nuoseklia išorės komunikacija;

   [...]

   c) optimaliu veiklos išteklių naudojimu;

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

3. CERT-EU**, glaudžiai bendradarbiaudama su ENISA,** teikia paramą Sąjungos [...] **subjektams**, siekiant didinti jų informuotumą apie padėtį, susijusią su kibernetinėmis grėsmėmis, pažeidžiamumu ir incidentais.

---

14 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).

4. TKST**, remdamasis CERT-EU pasiūlymu, ne vėliau kaip [12 mėnesių po šio reglamento įsigaliojimo dienos] priima** rekomendacinius **dokumentus arba rekomendacijas** dėl reagavimo į incidentus koordinavimo ir bendradarbiavimo reikšmingų incidentų atveju. Kai įtariama, kad incidentas yra nusikalstamas, CERT-EU pataria, kaip pranešti apie incidentą teisėsaugos institucijoms.

22 straipsnis

***Didelių <u>incidentų valdymas</u>** [...]*

-1. Siekdama remti suderintą didelių incidentų, darančių poveikį Sąjungos subjektams, valdymą operaciniu lygmeniu ir prisidėti prie reguliaraus Sąjungos subjektų tarpusavio keitimosi atitinkama informacija ir keitimosi ja su valstybėmis narėmis, TKST, glaudžiai bendradarbiaudama su CERT-EU ir ENISA, parengia kibernetinių krizių valdymo planą, grindžiamą 21 straipsnio 2 dalyje išsamiai išdėstyta veikla, į kurį įtraukiami bent šie aspektai:

a) Sąjungos subjektų veiksmų koordinavimo ir informacijos srautų valdymo sąlygos, susijusios su didelių incidentų valdymu operaciniu lygmeniu;

b) bendros standartinės veiksmų procedūros (SVP);

c) bendra didelių incidentų rimtumo ir krizę sukeliančių veiksnių taksonomija;

d) reguliarios pratybos;

e) naudotini saugūs ryšių kanalai;

f) EU-CyCLONe kontaktinis asmuo, kuris dalijasi atitinkama informacija su EU-CyCLONe taip prisidėdamas prie bendro informuotumo apie padėtį.

1. CERT-EU koordinuoja Sąjungos [...] **subjektų** atsaką į didelius [...] **incidentus**. Ji tvarko techninių ekspertinių žinių, kurių reikėtų reaguojant į **didelius incidentus** [...], aprašą.

2. Sąjungos [...] **subjektai** prisideda prie techninių ekspertinių žinių aprašo, pateikdam**i** kasmet atnaujinamą atitinkamose jų organizacijose turimų ekspertų sąrašą, kuriame išsamiai nurodomi jų konkretūs techniniai įgūdžiai.

3. Gavusi **konkretų valstybės narės, kurioje yra įsteigtas paveiktas Sąjungos subjektas, ir gavusi** [...] **paveikto** Sąjungos [...] **subjekto** pritarimą, CERT-EU taip pat taip pat gali pakviesti ekspertus iš 2 dalyje nurodyto sąrašo prisidėti reaguojant į didelį [...] **incidentą**, **įvykusį tame Sąjungos subjekte** [...].

VI skyrius
BAIGIAMOSIOS NUOSTATOS

23 straipsnis

Pradinis biudžeto perskirstymas

Komisija siūlo perkelti atitinkamų Sąjungos [...] **subjektų** 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, padedama CERT-EU, periodiškai tekia Komisijai šio reglamento įgyvendinimo ataskaitą. TKST taip pat gali teikti rekomendacijas Komisijai **peržiūrėti** [...] **šį** reglament**ą** [...].

2. Komisija pateikia Europos Parlamentui ir Tarybai šio reglamento įgyvendinimo ataskaitą ne vėliau kaip per **36** [...] mėnesius nuo šio reglamento įsigaliojimo, o vėliau – kas trejus metus.

3. Komisija ne **vėliau** [...] kaip po penkerių metų nuo šio reglamento įsigaliojimo dienos įvertina jo veikimą ir pateikia ataskaitą Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui. **Prireikus prie ataskaitos pridedamas pasiūlymas dėl teisėkūros procedūra priimamo akto.**

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	*Tarybos vardu*
Pirmininkas / Pirmininkė	*Pirmininkas / Pirmininkė*

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

II PRIEDAS

[...]

[...]

[...]

[...]

[...]

[...]

[...]