Europos Sąjungos
Taryba

Briuselis, 2022 m. birželio 21 d.
(OR. en)

10504/22

CYBER 232
TELECOM 288
CSC 286
CSCI 96
FIN 689

POSĖDŽIO REZULTATAI

nuo:	Tarybos generalinio sekretoriato
data:	2022 m. birželio 21 d.
kam:	Delegacijoms
Ankstesnio dokumento Nr.:	9716/22
Dalykas:	Tarybos išvados dėl Europos Audito Rūmų specialiosios ataskaitos Nr. 05/2022 „ES institucijų, įstaigų ir agentūrų kibernetinis saugumas: parengties lygis iš esmės neatitinka grėsmių“ – Tarybos išvados, Tarybos patvirtintos 2022 m. birželio 21 d. posėdyje

Delegacijoms priede pateikiamos pirmiau nurodytos Tarybos išvados, kurias 2022 m. birželio 21 d. posėdyje patvirtino Taryba.

PRIEDAS

TARYBOS IŠVADOS

dėl Europos Audito Rūmų specialiosios ataskaitos

Nr. 05/2022

„ES institucijų, įstaigų ir agentūrų kibernetinis saugumas: parengties lygis iš esmės neatitinka grėsmių“

EUROPOS SĄJUNGOS TARYBA,

PRIMINDAMA savo išvadas dėl Audito Rūmų parengtų specialiųjų ataskaitų nagrinėjimo gerinimo atsižvelgiant į biudžeto įvykdymo patvirtinimo procedūrą[1],

1. ATKREIPIA DĖMESĮ į Europos Audito Rūmų specialiąją ataskaitą Nr. 05/2022 „ES institucijų, įstaigų ir agentūrų kibernetinis saugumas: parengties lygis iš esmės neatitinka grėsmių“[2];

2. PABRĖŽIA, kad svarbu ir skubu stiprinti kibernetinio saugumo lygį ES institucijose, įstaigose ir agentūrose, atsižvelgiant į pastaruoju metu suintensyvėjusią skaitmeninę transformaciją institucijose, jų tvarkomą neskelbtiną informaciją, vis didėjantį išpuolių prieš ES institucijas, įstaigas ir agentūras skaičių ir rimtumą bei jų patiriamos grėsmės lygį;

3. PRIMENA 2019 m. birželio 20 d. Europos Vadovų Tarybos išvadas[3], kuriose Europos Vadovų Taryba paprašė ES institucijų kartu su valstybėmis narėmis rengti priemones, kuriomis siekiama didinti ES atsparumą ir stiprinti jos saugumo kultūrą kibernetinių ir hibridinių grėsmių, kylančių už ES ribų, atžvilgiu ir geriau apsaugoti ES informacijos bei ryšių tinklus ir jos sprendimų priėmimo procesus nuo visų rūšių kenkimo veiklos;

---

1 Dok. 7515/00 + COR 1.
2 Dok. 8040/22.
3 Dok. EUCO 9/19.

4. PRIMENA savo 2019 m. gruodžio 10 d. išvadas dėl papildomų pastangų siekiant didinti atsparumą ir kovoti su hibridinėmis grėsmėmis[4], kuriose paragino ES institucijas, įstaigas ir agentūras su valstybių narių parama užtikrinti Sąjungos gebėjimą apsaugoti savo vientisumą ir sustiprinti ES informacijos bei ryšių tinklų ir jos sprendimų priėmimo procesų apsaugą nuo visų rūšių kenkimo veiklos, remiantis išsamiu grėsmių įvertinimu. Išvadose nurodyta, kad tuo tikslu institucijos, įstaigos ir agentūros, remiamos valstybių narių, turėtų parengti ir įgyvendinti išsamų savo saugumo užtikrinimo priemonių rinkinį, vadovaudamosi 2019 m. birželio mėn. Europos Vadovų Tarybos suteiktais įgaliojimais[5];

5. PRIMENA savo 2021 m. kovo 22 d. išvadas dėl ES skaitmeninio dešimtmečio kibernetinio saugumo strategijos[6], kuriose pabrėžė, kad kibernetinis saugumas yra gyvybiškai svarbus tiek nacionalinio, tiek ES lygmens viešojo administravimo įstaigų ir institucijų veikimui, taip pat mūsų visuomenei ir visai ekonomikai apskritai;

6. PRIMENA savo 2022 m. gegužės 23 d. išvadas dėl Europos Sąjungos pozicijos kibernetiniais klausimais parengimo[7], kuriose ES institucijos, įstaigos ir agentūros buvo paragintos dalyvauti rengiant esamų saugios komunikacijos kibernetinėje erdvėje priemonių sąrašą, kuris turi būti aptartas atitinkamuose Tarybos organuose ir su atitinkamomis bendradarbiavimo grupėmis, pavyzdžiui, CSIRT tinklu ir EU CyCLONe;

7. PABRĖŽIA, kad reikia spręsti ES institucijų, įstaigų ir agentūrų tarpusavio sąsajoje, taip pat sąsajoje tarp jų ir valstybių narių institucijų esančią sisteminę riziką, nepaisant jų institucinio nepriklausomumo ir administracinio savarankiškumo;

---

4 Dok. 14972/19.
5 Dok. EUCO 9/19.
6 Dok. 6722/21.
7 Dok. 9364/22.

8. ATKREIPIA DĖMESĮ į specialiojoje ataskaitoje pateiktas pastabas, t. y. į tai, kad ES institucijos, įstaigos ir agentūros nėra pasiekusios tokio kibernetinės parengties lygio, kuris atitiktų grėsmes, ir kibernetinio saugumo brandos lygiai skiriasi. PRIPAŽĮSTA, kad turėtų būti pagerintas ES institucijų, įstaigų ir agentūrų kibernetinio saugumo parengties lygis, taip pat jų tarpusavio sinergija;

9. todėl RAGINA ES institucijas, įstaigas ir agentūras toliau įgyvendinti kibernetinės rizikos valdymo priemones, kuriomis būtų užtikrinamas grėsmes atitinkantis kibernetinio saugumo lygis, kaip numatyta siūlomoje direktyvoje dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria panaikinama Direktyva (ES) 2016/1148, kad būtų pagerintas jų parengties lygis;

10. PRAŠO ES institucijų, įstaigų ir agentūrų intensyvinti tiek savo pastangas apsisaugoti nuo kibernetinių grėsmių, tiek savo bendradarbiavimą nustatant nuoseklius standartus ir specifikacijas, visų pirma su kibernetiniu saugumu susijusiems viešiesiems pirkimams, projektams bei paslaugoms, ir gerinti savo IT sistemų sąveikumą, be kita ko, siekiant užtikrinti saugų neįslaptinto turinio perdavimą;

11. PRAŠO Europos Sąjungos kibernetinio saugumo agentūros (ENISA) ir ES institucijų, įstaigų ir agentūrų kompiuterinių incidentų tyrimo tarnybos (CERT-EU) pagal savo kompetencijas aktyviau bendradarbiauti remiant ES institucijų, įstaigų ir agentūrų pastangas kibernetinio saugumo srityje, visų pirma stiprinant tų ES institucijų, įstaigų ir agentūrų, kurių kibernetinio saugumo brandos lygis yra žemesnis, gebėjimus;

12. ATKREIPIA DĖMESĮ į specialiojoje ataskaitoje pateiktas išvadas ir rekomendacijas ir PRIPAŽĮSTA, kad turėtų būti gerokai pagerintas ES institucijų, įstaigų ir agentūrų kibernetinio saugumo parengties lygis, taip pat jų tarpusavio sinergija. ES institucijos, įstaigos ir agentūros turėtų turėti visapusišką kibernetinio saugumo rizikos valdymo sistemą, reguliariai atlikti rizikos vertinimus ir auditus, grindžiamus bendra arba gerai žinoma metodika ir tarptautiniais standartais, ir susisteminti darbuotojų informuotumo apie kibernetinį saugumą ir mokymo tuo klausimu programas;

13. taip pat AKCENTUOJA, kad ES institucijos, įstaigos ir agentūros turėtų skirti pakankamą biudžetą, kad būtų užtikrintas apsaugos nuo kibernetinių grėsmių priemonių įgyvendinimas, kartu laikantis daugiametės finansinės programos, ir ATKREIPIA DĖMESĮ į specialiojoje ataskaitoje pateiktą rekomendaciją, kad turėtų būti paskirta visoms ES institucijoms, įstaigoms ir agentūroms atstovaujanti įstaiga, kuriai būtų suteikti atitinkami įgaliojimai ir priemonės stebėti, kaip laikomasi bendrų kibernetinio saugumo taisyklių;

14. PRIPAŽĮSTA, kad CERT-EU turėtų būti nedelsiant informuojama apie reikšmingus kibernetinius incidentus ES institucijose, įstaigose ir agentūrose ir šiuo tikslu ji turėtų būti aprūpinta pakankamais ištekliais, kurie būtų nuspėjami ir pritaikyti prie dabartinio grėsmės lygio bei ES institucijų, įstaigų ir agentūrų poreikių visų pirma personalo, techninės įrangos ir infrastruktūros atžvilgiais;

15. PAŽYMI, kad turėtų būti stiprinamas ir susistemintas ES institucijų, įstaigų ir agentūrų bendradarbiavimas ir keitimasis informacija apie kibernetinį saugumą, taip pat saugių ryšių kanalų sąveikumas; RAGINA į tokį bendradarbiavimą ir keitimąsi informacija įtraukti ir valstybių narių valdžios institucijas, atsakingas už kibernetinį saugumą;

16. ATKREIPIA DĖMESĮ į Komisijos, CERT-EU ir ENISA atsakymus, pridedamus prie specialiosios ataskaitos;

17. PRAŠO Komisijos atsižvelgti į specialiojoje ataskaitoje pateiktas rekomendacijas ir laikytis plataus užmojo projektuojant ES institucijų, įstaigų ir agentūrų kibernetinio saugumo politiką ir propaguoti didesnę jų tarpusavio sinergiją.