Eiropas Savienības
Padome

Briselē, 2022. gada 10. jūnijā
(OR. fr, en)

9716/22

LIMITE

CYBER 198
TELECOM 255
CSC 228
CSCI 74
FIN 590



**"I/A" PUNKTA PIEZĪME**

| | |
|---|---|
| Sūtītājs: | Padomes Ģenerālsekretariāts |
| Saņēmējs: | Pastāvīgo pārstāvju komiteja / Padome |
| Iepr. dok. Nr.: | 9317/2/22 REV 2 |
| Temats: | Projekts – Padomes secinājumi par Eiropas Revīzijas palātas Īpašo ziņojumu Nr. 05/2022 "ES iestāžu, struktūru un aģentūru kiberdrošība: sagatavotības līmenis kopumā neatbilst apdraudējumam"<br>– apstiprināšana |

1. Eiropas Revīzijas palāta 2022. gada 30. martā publicēja savu Īpašo ziņojumu Nr. 05/2022 "ES iestāžu, struktūru un aģentūru kiberdrošība: sagatavotības līmenis kopumā neatbilst apdraudējumam". [1]

2. Pastāvīgo pārstāvju komiteja 2022. gada 13. aprīļa sanāksmē īpašo ziņojumu uzticēja Kiberjautājumu horizontālajai darba grupai. [2]

[1] 8040/22.
[2] 8041/22.

3. Revīzijas palātas pārstāvji 2022. gada 3. maijā iepazīstināja Kiberjautājumu horizontālo darba grupu ar īpašo ziņojumu. Pēc diskusijām par ziņojumu, kuras notika tajā pašā darba grupas sanāksmē, prezidentvalsts izstrādāja Padomes secinājumu projektu, ko darba grupa apsprieda 2022. gada 24. maija sanāksmē.

4. Kiberjautājumu horizontālā darba grupa 2022. gada 10. jūnijā panāca vienošanos par pielikumā izklāstīto tekstu.

5. Pastāvīgo pārstāvju komiteja tiek aicināta apstiprināt šo secinājumu projektu un ierosināt Padomei kādā no nākamajām sanāksmēm tos pieņemt.

**PIELIKUMS**

**PROJEKTS – PADOMES SECINĀJUMI**



**par Eiropas Revīzijas palātas Īpašo ziņojumu Nr. 05/2022**
**"ES iestāžu, struktūru un aģentūru kiberdrošība: sagatavotības līmenis kopumā neatbilst apdraudējumam"**

EIROPAS SAVIENĪBAS PADOME,

ATGĀDINOT savus secinājumus par Revīzijas palātas izstrādāto īpašo ziņojumu izskatīšanas uzlabošanu saistībā ar budžeta izpildes apstiprinājuma procedūru [3];

1. PIEŅEM ZINĀŠANAI Eiropas Revīzijas palātas Īpašo ziņojumu Nr. 05/2022 "ES iestāžu, struktūru un aģentūru kiberdrošība: sagatavotības līmenis kopumā neatbilst apdraudējumam" [4].

2. UZSVER, ka ir svarīgi stiprināt kiberdrošības līmeni ES iestādēs, struktūrās un aģentūrās un ka tas ir jādara steidzami, ņemot vērā neseno digitālās pārveides intensifikāciju iestādēs, to apstrādāto sensitīvo informāciju, uzbrukumu ES iestādēm, struktūrām un aģentūrām arvien pieaugošo skaitu un smagumu un to apdraudējuma līmeni.

[3] 7515/00 + COR 1.
[4] 8040/22.

3. ATGĀDINA Eiropadomes 2019. gada 20. jūnija secinājumus [5], kuros Eiropadome aicināja ES iestādes kopā ar dalībvalstīm strādāt pie pasākumiem, lai uzlabotu ES drošības kultūru un palielinātu tās spēju izturēt kiberdraudus un hibrīddraudus, kuri rodas ārpus ES, un lai ES informācijas un sakaru tīklus un lēmumu pieņemšanas procesus labāk aizsargātu pret visu veidu ļaunprātīgām darbībām.

4. ATGĀDINA savus 2019. gada 10. decembra secinājumus par papildu centieniem uzlabot noturību un novērst hibrīddraudus [6], kuros tā aicināja ES iestādes, struktūras un aģentūras, ko atbalsta dalībvalstis, pamatojoties uz visaptverošu apdraudējuma novērtējumu, nodrošināt Savienības spēju aizsargāt tās integritāti un uzlabot ES informācijas un komunikāciju tīklu un lēmumu pieņemšanas procesu drošību pret visu veidu ļaunprātīgām darbībām. Secinājumos paziņots, ka šajā nolūkā iestādēm, struktūrām un aģentūrām, ko atbalsta dalībvalstis, saskaņā ar 2019. gada jūnija Eiropadomes pilnvarojumu būtu jāizstrādā un jāīsteno visaptverošs pasākumu kopums to drošības nodrošināšanai [7].

5. ATGĀDINA savus 2021. gada 22. marta secinājumus par ES kiberdrošības stratēģiju digitālajai desmitgadei [8], kuros uzsvērts, ka kiberdrošība ir ļoti svarīga valsts pārvaldes un iestāžu darbībai gan valstu, gan ES līmenī, kā arī mūsu sabiedrībai un ekonomikai kopumā.

---

5 EUCO 9/19.
6 14972/19.
7 EUCO 9/19.
8 6722/21.

6. ATGĀDINA savus 2022. gada 23. maija secinājumus par Eiropas Savienības pozīcijas kiberjautājumos izstrādi [9], kuros ES iestādes, struktūras un aģentūras tika mudinātas piedalīties kartēšanā attiecībā uz esošajiem drošo sakaru rīkiem kiberjomā, kuri jāapspriež attiecīgajās Padomes struktūrās un ar attiecīgajām sadarbības grupām, piemēram, *CSIRT* tīklu un ES *CyCLONe*.

7. UZSVER, ka ir jāpievēršas sistēmiskam riskam, kas pastāv savstarpējā savienotībā starp ES iestādēm, struktūrām un aģentūrām, kā arī starp tām un dalībvalstu iestādēm, neraugoties uz to institucionālo neatkarību un administratīvo autonomiju.

8. PIEŅEM ZINĀŠANAI īpašajā ziņojumā iekļautos apsvērumus, proti, to, ka ES iestādes, struktūras un aģentūras nav sasniegušas kibersagatavotības līmeni, kas būtu atbilstošs draudiem, un ka tām ir atšķirīgi kiberdrošības brieduma līmeņi. ATZĪST, ka būtu jāuzlabo ES iestāžu, struktūru un aģentūru kibersagatavotības līmenis, kā arī sinerģijas starp tām.

9. Tādēļ stingri MUDINA ES iestādes, struktūras un aģentūras – lai uzlabotu savu sagatavotības līmeni, turpināt īstenot kiberriska pārvaldības pasākumus, kuri nodrošina atbilstošu kiberdrošības līmeni, kā paredzēts ierosinātajā direktīvā par pasākumiem nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā un ar ko atceļ Direktīvu (ES) 2016/1148.

10. AICINA ES iestādes, struktūras un aģentūras pastiprināt gan centienus aizsargāt sevi pret kiberapdraudējumiem, gan sadarbību saskaņotu standartu un specifikāciju izveidē, jo īpaši attiecībā uz publisko iepirkumu, projektiem un pakalpojumiem, kas saistīti ar kiberdrošību, un uzlabot savu IT sistēmu sadarbspēju, tostarp, lai nodrošinātu drošus sakarus attiecībā uz neklasificētu saturu.

---

[9] 9364/22.

11. AICINA Eiropas Savienības Kiberdrošības aģentūru (*ENISA*) un ES iestāžu, struktūru un aģentūru datorapdraudējumu reaģēšanas vienību (*CERT-EU*) savas kompetences ietvaros pastiprināt sadarbību, lai atbalstītu ES iestāžu, struktūru un aģentūru centienus kiberdrošības jomā, jo īpaši attiecībā uz to ES iestāžu, struktūru un aģentūru spēju veidošanu, kurām ir zemāks kiberdrošības brieduma līmenis.

12. PIEŅEM ZINĀŠANAI īpašajā ziņojumā iekļautos secinājumus un ieteikumus un ATZĪST, ka būtu būtiski jāuzlabo ES iestāžu, struktūru un aģentūru kibersagatavotības līmenis, kā arī sinerģijas starp tām. ES iestādēm, struktūrām un aģentūrām vajadzētu būt visaptverošam riska pārvaldības satvaram kiberdrošības jomā, tām būtu jāveic regulāri riska novērtējumi un revīzijas, pamatojoties uz kopīgu vai labi zināmu metodiku un starptautiskiem standartiem, un tām būtu jāsistematizē personālam paredzētas kiberdrošības informētības un apmācības programmas.

13. UZSVER arī to, ka ES iestādēm, struktūrām un aģentūrām būtu jāpiešķir pietiekams budžets tam, lai nodrošinātu aizsardzības pasākumu pret kiberapdraudējumiem īstenošanu, vienlaikus ievērojot daudzgadu finanšu shēmu, un ŅEM VĒRĀ īpašajā ziņojumā iekļauto ieteikumu par to, ka būtu jāieceļ struktūra, kas pārstāv visas ES iestādes, struktūras un aģentūras, un tai būtu jāpiešķir attiecīgas pilnvaras un līdzekļi, lai uzraudzītu atbilstību kopīgajiem kiberdrošības noteikumiem.

14. ATZĪST, ka *CERT-EU* būtu nekavējoties jāinformē par būtiskiem kiberincidentiem ES iestādēs, struktūrās un aģentūrās un ka šajā nolūkā tā būtu jānodrošina ar pietiekamiem resursiem, kas ir paredzami un pielāgoti pašreizējam apdraudējuma līmenim un ES iestāžu, struktūru un aģentūru vajadzībām, jo īpaši personāla, tehniskā aprīkojuma un infrastruktūras ziņā.

15. NORĀDA, ka būtu jāstiprina un jāsistematizē sadarbība un informācijas apmaiņa kiberdrošības jomā, kā arī drošu sakaru kanālu sadarbspēja starp ES iestādēm, struktūrām un aģentūrām. AICINA šādā sadarbībā un informācijas apmaiņā ietvert arī publiskas iestādes, kas dalībvalstīs ir atbildīgas par kiberdrošību.

16. PIEŅEM ZINĀŠANAI Komisijas, *CERT-EU* un *ENISA* atbildes, kas pievienotas īpašajam ziņojumam.

17. AICINA Komisiju ņemt vērā īpašajā ziņojumā iekļautos ieteikumus un, izstrādājot ES iestāžu, struktūru un aģentūru kiberdrošības politiku, izvirzīt vērienīgus mērķus, un iestāties par lielāku sinerģiju starp tām.