Svet
Evropske unije

Bruselj, 21. junij 2022
(OR. en)

10504/22

CYBER 232
TELECOM 288
CSC 286
CSCI 96
FIN 689

IZID POSVETOVANJA

Pošiljatelj:	Generalni sekretariat Sveta
Datum:	21. junij 2022
Prejemnik:	delegacije
Št. predh. dok.:	9716/22
Zadeva:	Sklepi Sveta o posebnem poročilu Evropskega računskega sodišča št. 05/2022 z naslovom „Kibernetska varnost institucij, organov in agencij EU – Raven pripravljenosti na splošno ni sorazmerna z grožnjami“ – sklepi Sveta, ki jih je Svet odobril na seji 21. junija 2022

V prilogi vam pošiljamo navedene sklepe Sveta, ki jih je Svet odobril na seji 21. junija 2022.

PRILOGA

SKLEPI SVETA

o posebnem poročilu Evropskega računskega sodišča št. 05/2022
z naslovom
„Kibernetska varnost institucij, organov in agencij EU – Raven pripravljenosti na splošno ni sorazmerna z grožnjami“

SVET EVROPSKE UNIJE –

OPOZARJAJOČ na sklepe, ki jih je sprejel v zvezi z izboljšanjem preučevanja posebnih poročil Računskega sodišča v okviru postopka razrešnice[1] –

1. JE SEZNANJEN s posebnim poročilom Evropskega računskega sodišča št. 05/2022 z naslovom „Kibernetska varnost institucij, organov in agencij EU – Raven pripravljenosti na splošno ni sorazmerna z grožnjami“[2].

2. POUDARJA, kako pomembno in nujno je okrepiti raven kibernetske varnosti v institucijah, organih in agencijah EU glede na nedavno pospešitev digitalne preobrazbe v institucijah, občutljive informacije, ki jih obdelujejo, vse večje število in resnost napadov na institucije, organe in agencije EU ter stopnjo njihove ogroženosti.

3. OPOZARJA na sklepe Evropskega sveta z dne 20. junija 2019[3], v katerih je Evropski svet institucije EU pozval, naj skupaj z državami članicami pripravijo ukrepe za okrepitev odpornosti in izboljšanje varnostne kulture EU v zvezi s kibernetskimi in hibridnimi grožnjami, ki prihajajo iz okolja zunaj EU, ter za boljšo zaščito informacijskih in komunikacijskih omrežij EU ter njenih postopkov odločanja pred raznovrstnimi zlonamernimi dejanji.

---

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

4. OPOZARJA na sklepe, ki jih je sprejel 10. decembra 2019 o dopolnilnih prizadevanjih za krepitev odpornosti in preprečevanje hibridnih groženj[4], v katerih je pozval institucije, organe in agencije EU, naj ob podpori držav članic na podlagi celovite ocene nevarnosti zagotovijo zmogljivosti Unije za zaščito njene integritete in okrepijo varnost informacijskih in komunikacijskih omrežij EU ter postopkov odločanja pred vsakovrstnimi zlonamernimi dejavnostmi. V sklepih je še zapisano, da bi morali v ta namen institucije, organi in agencije ob podpori držav članic v skladu z mandatom Evropskega sveta iz junija 2019 pripraviti in izvajati celovit sklop ukrepov za zagotavljanje varnosti[5].

5. OPOZARJA na svoje sklepe z dne 22. marca 2021 o strategiji EU za kibernetsko varnost v digitalnem desetletju[6], v katerih je poudaril, da je kibernetska varnost bistvena za delovanje javne uprave in institucij na nacionalni ravni in na ravni EU ter za našo družbo in gospodarstvo kot celoto.

6. OPOZARJA na svoje sklepe z dne 23. maja 2022 o vzpostavitvi stališča Evropske unije glede kibernetskih vprašanj[7], v katerih so bili institucije, organi in agencije EU pozvani, naj sodelujejo pri pregledu obstoječih orodij za varno komunikacijo na kibernetskem področju, o katerem bodo razpravljalia ustrezna telesa Sveta, in z ustreznimi skupinami za sodelovanje, na primer mreža skupin CSIRT in organizacijska mreža za povezovanje v kibernetski krizi (EU CyCLONe).

7. POUDARJA, da je treba obravnavati sistemsko tveganje, ki obstaja pri medsebojni povezanosti med institucijami, organi in agencijami EU, pa tudi med njimi in institucijami držav članic, kljub njihovi institucionalni neodvisnosti in upravni avtonomiji.

---

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

8. JE SEZNANJEN z ugotovitvami iz posebnega poročila, in sicer, da institucije, organi in agencije EU niso dosegli ravni kibernetske pripravljenosti, ki bi bila sorazmerna z grožnjami, in imajo različne ravni zrelosti na področju kibernetske varnosti. PRIZNAVA, da bi bilo treba izboljšati raven pripravljenosti institucij, organov in agencij EU na področju kibernetske varnosti ter sinergije med njimi.

9. Zato odločno SPODBUJA institucije, organe in agencije EU, naj še naprej izvajajo ukrepe za obvladovanje kibernetskih tveganj, ki zagotavljajo sorazmerno raven kibernetske varnosti, kot je predvideno v predlagani direktivi o ukrepih za visoko skupno raven kibernetske varnosti v Uniji in razveljavitvi Direktive (EU) 2016/1148, da bi izboljšali svojo raven pripravljenosti.

10. POZIVA institucije, organe in agencije EU, naj okrepijo svoja prizadevanja za zaščito pred kibernetskimi grožnjami in sodelovanje pri vzpostavljanju doslednih standardov in specifikacij, zlasti za javna naročila, projekte in storitve, povezane s kibernetsko varnostjo, ter izboljšajo interoperabilnost svojih informacijskih sistemov, tudi zato, da se zagotovi varna komunikacija vsebin, ki niso tajne.

11. POZIVA Agencijo Evropske unije za kibernetsko varnost (ENISA) in skupino za odzivanje na računalniške grožnje za institucije, organe in agencije EU (CERT-EU), naj v okviru svojih pristojnosti okrepita sodelovanje pri podpiranju institucij, organov in agencij EU pri njihovih prizadevanjih na področju kibernetske varnosti, zlasti v zvezi s krepitvijo zmogljivosti tistih institucij, organov in agencij EU, ki imajo nižjo raven zrelosti na področju kibernetske varnosti.

12. JE SEZNANJEN s sklepi in priporočili iz posebnega poročila ter PRIZNAVA, da bi bilo treba raven pripravljenosti institucij, organov in agencij EU na področju kibernetske varnosti ter sinergije med njimi znatno izboljšati. Institucije, organi in agencije EU bi morali imeti celovit okvir za obvladovanje tveganj na področju kibernetske varnosti ter izvajati redne ocene tveganja in revizije na podlagi skupne ali uveljavljene metodologije in mednarodnih standardov ter sistematizirati programe ozaveščanja in usposabljanja o kibernetski varnosti za osebje.

13. POUDARJA tudi, da bi morale institucije, organi in agencije EU dodeliti zadostna proračunska sredstva za zagotovitev izvajanja ukrepov za zaščito pred kibernetskimi grožnjami, pri tem pa upoštevati večletni finančni okvir, in SE SEZNANJA s priporočilom iz posebnega poročila, da bi bilo treba imenovati organ, ki bi zastopal vse institucije, organe in agencije EU, ter mu dodeliti ustrezen mandat in sredstva za spremljanje skladnosti s skupnimi pravili o kibernetski varnosti.

14. PRIZNAVA, da bi morala biti skupina CERT-EU nemudoma obveščena o večjih kibernetskih incidentih v institucijah, organih in agencijah EU, v ta namen pa bi morala imeti na voljo ustrezne vire, ki bi bili predvidljivi in prilagojeni trenutni stopnji ogroženosti ter potrebam institucij, organov in agencij EU, zlasti kar zadeva osebje, tehnično opremo in infrastrukturo.

15. UGOTAVLJA, da bi bilo treba okrepiti in sistematizirati sodelovanje in izmenjavo informacij o kibernetski varnosti ter interoperabilnost varnih komunikacijskih kanalov med institucijami, organi in agencijami EU. POZIVA, naj to sodelovanje in izmenjava informacij vključujeta tudi javne organe, pristojne za kibernetsko varnost v državah članicah.

16. JE SEZNANJEN z odgovori Komisije, skupine CERT-EU in agencije ENISA, priloženimi posebnemu poročilu.

17. POZIVA Komisijo, naj upošteva priporočila iz posebnega poročila in naj bo ambiciozna pri oblikovanju politik institucij, organov in agencij EU na področju kibernetske varnosti ter naj se zavzema za več sinergij med njimi.