

Bruselj, 10. junij 2022
(OR. fr, en)

9716/22

LIMITE

CYBER 198
TELECOM 255
CSC 228
CSCI 74
FIN 590

DOPIS O TOČKI POD „I/A“

Pošiljatelj:	Generalni sekretariat Sveta
Prejemnik:	Odbor stalnih predstavnikov/Svet
Št. predh. dok.:	9317/2/22 REV 2
Zadeva:	Osnutek sklepov 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“ – odobritev

1. Evropsko računsko sodišče je 30. marca 2022 objavilo posebno poročilo št. 05/2022 z naslovom „Kibernetska varnost institucij, organov in agencij EU – Raven pripravljenosti na splošno ni sorazmerna z grožnjami“.¹
2. Odbor stalnih predstavnikov je na seji 13. aprila 2022 posebno poročilo predal Horizontalni delovni skupini za kibernetična vprašanja.²

¹ Dok. 8040/22.

² Dok. 8041/22.

3. Predstavniki Računskega sodišča so 3. maja 2022 posebno poročilo predstavili Horizontalni delovni skupini za kibernetika vprašanja. Predsedstvo je po razpravah o poročilu na isti seji delovne skupine pripravilo osnutek sklepov Sveta, o katerem je delovna skupina razpravljala na seji 24. maja 2022.
4. Horizontalna delovna skupina za kibernetika vprašanja je 10. junija 2022 dosegla dogovor o priloženem besedilu.
5. Odbor stalnih predstavnikov naj odobri ta osnutek sklepov in Svetu predlaga, da ga sprejme na eni od prihodnjih sej.

OSNUTEK SKLEPOV 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 razrešnice³ –

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“⁴.
2. POUDARJA, kako pomembno in nujno je okrepiti raven kibernetike 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 Dok. 7515/00 + COR 1.

⁴ Dok. 8040/22.

3. OPOZARJA na sklepe Evropskega sveta z dne 20. junija 2019⁵, 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 kibernetскими 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.
4. OPOZARJA na sklepe, ki jih je sprejel 10. decembra 2019 o dopolnilnih prizadevanjih za krepitev odpornosti in preprečevanje hibridnih groženj⁶, 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 varnosti⁷.
5. OPOZARJA na svoje sklepe z dne 22. marca 2021 o strategiji EU za kibernetško varnost v digitalnem desetletju⁸, v katerih je poudaril, da je kibernetška varnost bistvena za delovanje javne uprave in institucij na nacionalni ravni in na ravni EU ter za našo družbo in gospodarstvo kot celoto.

⁵ Dok. EUCO 9/19.

⁶ Dok. 14972/19.

⁷ Dok. EUCO 9/19.

⁸ Dok. 6722/21.

6. OPOZARJA na svoje sklepe z dne 23. maja 2022 o vzpostavitvi stališča Evropske unije glede kibernetских vprašanj⁹, v katerih so bili institucije, organi in agencije EU pozvani, naj sodelujejo pri pregledu obstoječih orodij za varno komunikacijo na kibernetickem področju, o katerem bodo razpravljala ustrezna telesa Sveta, in z ustreznimi skupinami za sodelovanje, na primer mreža skupin CSIRT in organizacijska mreža za povezovanje v kiberneticki 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.
8. JE SEZNANJEN z ugotovitvami iz posebnega poročila, in sicer, da institucije, organi in agencije EU niso dosegli ravni kibernetiske pripravljenosti, ki bi bila sorazmerna z grožnjami, in imajo različne ravni zrelosti na področju kibernetiske varnosti. PRIZNAVA, da bi bilo treba izboljšati raven pripravljenosti institucij, organov in agencij EU na področju kibernetiske varnosti ter sinergije med njimi.
9. Zato odločno SPODBUJA institucije, organe in agencije EU, naj še naprej izvajajo ukrepe za obvladovanje kibernetickih tveganj, ki zagotavljajo sorazmerno raven kibernetiske varnosti, kot je predvideno v predlagani direktivi o ukrepih za visoko skupno raven kibernetiske 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 kibernetickimi grožnjami in sodelovanje pri vzpostavljanju doslednih standardov in specifikacij, zlasti za javna naročila, projekte in storitve, povezane s kiberneticko varnostjo, ter izboljšajo interoperabilnost svojih informacijskih sistemov, tudi zato, da se zagotovi varna komunikacija vsebin, ki niso tajne.

⁹ Dok. 9364/22.

11. POZIVA Agencijo Evropske unije za kibernetško varnost (ENISA) in skupino za odzivanje na računalniške grožnje za institucije, organe in agencije EU (CERT-EU), naj v okviru svojih pristojnosti okrepi sodelovanje pri podpiranju institucij, organov in agencij EU pri njihovih prizadevanjih na področju kibernetске varnosti, zlasti v zvezi s krepitvijo zmogljivosti tistih institucij, organov in agencij EU, ki imajo nižjo raven zrelosti na področju kibernetске 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 kibernetске varnosti ter sinergije med njimi znatno izboljšati. Institucije, organi in agencije EU bi morali imeti celovit okvir za obvladovanje tveganj na področju kibernetске varnosti ter izvajati redne ocene tveganja in revizije na podlagi skupne ali uveljavljene metodologije in mednarodnih standardov ter sistematizirati programe ozaveščanja in usposabljanja o kibernetски varnosti za osebje.
3. POUDARJA tudi, da bi morale institucije, organi in agencije EU dodeliti zadostna proračunska sredstva za zagotovitev izvajanja ukrepov za zaščito pred kibernetскими 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 kibernetски varnosti.
14. PRIZNAVA, da bi morala biti skupina CERT-EU nemudoma obveščena o večjih kibernetских 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 kibernetiski 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 kibernetisko 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 kibernetiske varnosti ter naj se zavzema za več sinergij med njimi.
