Vijeće
Europske unije

Bruxelles, 21. lipnja 2022.
(OR. en)

10504/22

CYBER 232
TELECOM 288
CSC 286
CSCI 96
FIN 689

ISHOD POSTUPAKA

Od:	Glavno tajništvo Vijeća
Na datum:	21. lipnja 2022.
Za:	Delegacije
Br. preth. dok.:	9716/22
Predmet:	Zaključci Vijeća o tematskom izvješću Europskog revizorskog suda br. 05/2022 naslovljenom „Kibersigurnost institucija, tijela i agencija EU-a: razina pripravnosti općenito nije razmjerna prijetnjama” – zaključci Vijeća koje je odobrilo Vijeće na sastanku 21. lipnja 2022.

Za delegacije se u Prilogu nalaze navedeni zaključci Vijeća, kako ih je odobrilo Vijeće na sastanku 21. lipnja 2022.

PRILOG

ZAKLJUČCI VIJEĆA

o tematskom izvješću br. 05/2022 Europskog revizorskog suda
naslovljenom
„Kibersigurnost institucija, tijela i agencija EU-a: razina pripravnosti općenito nije razmjerna prijetnjama”

VIJEĆE EUROPSKE UNIJE,

PODSJEĆAJUĆI na svoje zaključke o poboljšanju ispitivanja tematskih izvješća koja sastavlja Revizorski sud u kontekstu postupka davanja razrješnice[1]:

1. PRIMA NA ZNANJE tematsko izvješće Europskog revizorskog suda br. 05/2022 naslovljeno „Kibersigurnost institucija, tijela i agencija EU-a: razina pripravnosti općenito nije razmjerna prijetnjama”[2];

2. NAGLAŠAVA važnost i hitnost jačanja razine kibersigurnosti u institucijama, tijelima i agencijama EU-a s obzirom na nedavno intenziviranje digitalne transformacije unutar institucija, osjetljive informacije koje obrađuju, sve veći broj i rastuću ozbiljnost napada na institucije, tijela i agencije EU-a te na razinu prijetnje koja utječe na njih;

3. PODSJEĆA na zaključke Europskog vijeća od 20. lipnja 2019. [3] u kojima ono poziva institucije EU-a da zajedno s državama članicama rade na mjerama kako bi se pojačala otpornost i poboljšala kultura sigurnosti EU-a u pogledu kiberprijetnji i hibridnih prijetnji koje dolaze izvan EU-a i kako bi se informacijske i komunikacijske mreže EU-a te njegove postupke donošenja odluka bolje zaštitilo od zlonamjernih aktivnosti svih vrsta;

---

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

4. PODSJEĆA na svoje zaključke od 10. prosinca 2019. naslovljene „Dodatna nastojanja za jačanje otpornosti i suzbijanje hibridnih prijetnji”[4], u kojima je pozvalo institucije, tijela i agencije EU-a da, uz potporu država članica i na temelju sveobuhvatne procjene prijetnje, osiguraju sposobnost Unije da zaštiti svoj integritet i poboljša sigurnost informacijskih i komunikacijskih mreža EU-a te postupaka donošenja odluka od zlonamjernih aktivnosti svih vrsta. U tu bi svrhu, kako je navedeno u zaključcima, institucije, tijela i agencije, uz potporu država članica, trebale razviti i provesti sveobuhvatan skup mjera za osiguravanje svoje sigurnosti, u skladu s mandatom Europskog vijeća iz lipnja 2019.[5];

5. PODSJEĆA na svoje zaključke od 22. ožujka 2021. o Strategiji EU-a za kibersigurnost za digitalno desetljeće[6], u kojima je naglasilo da je kibersigurnost ključna za funkcioniranje javne uprave i institucija na nacionalnoj razini i razini EU-a te za naše društvo i gospodarstvo u cjelini;

6. PODSJEĆA na svoje zaključke od 23. svibnja 2022. o razvoju položaja Europske unije u pogledu kiberprostora[7], u kojima su institucije, tijela i agencije EU-a potaknuti da sudjeluju u izradi pregleda postojećih alata za sigurnu komunikaciju u kiberpodručju o kojima treba raspravljati u okviru relevantnih tijela Vijeća i s relevantnim skupinama za suradnju, kao što su mreža CSIRT-ova i EU-CyCLONe;

7. NAGLAŠAVA potrebu za suočavanjem sa sustavnim rizikom koji postoji u međusobnoj povezanosti institucija, tijela i agencija EU-a, kao i između njih i institucija država članica, unatoč njihovoj institucijskoj neovisnosti i administrativnoj autonomiji;

---

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

8. PRIMA NA ZNANJE opažanja iz tematskog izvješća, odnosno da institucije, tijela i agencije EU-a nisu dosegnuli razinu kiberpripravnosti koja bi bila razmjerna prijetnjama i na različitim su stupnjevima razvoja u pogledu kibersigurnosti; PREPOZNAJE da bi trebalo poboljšati razinu pripravnosti institucija, tijela i agencija EU-a u pogledu kibersigurnosti, kao i sinergiju među njima;

9. stoga snažno POTIČE institucije, tijela i agencije EU-a da nastave s provedbom mjera za upravljanje kiberrizicima kojima se osigurava razmjerna razina kibersigurnosti, kako je predviđeno Prijedlogom direktive o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije i stavljanju izvan snage Direktive (EU) 2016/1148, kako bi se poboljšala njihova razina pripravnosti;

10. POZIVA institucije, tijela i agencije EU-a da pojačaju svoje napore kako bi se zaštitili od kiberprijetnji i svoju suradnju u uspostavi dosljednih standarda i specifikacija, posebno za javnu nabavu, projekte i usluge povezane s kibersigurnošću, te da poboljšaju interoperabilnost svojih IT sustava, među ostalim u cilju osiguravanja sigurne komunikacije neklasificiranog sadržaja;

11. POZIVA Agenciju Europske unije za sigurnost (ENISA) i tim za hitne računalne intervencije institucija, tijela i agencija EU-a (CERT-EU) da u okviru svojih nadležnosti pojačaju suradnju u pružanju potpore institucijama, tijelima i agencijama EU-a u njihovim nastojanjima u području kibersigurnosti, posebno u pogledu izgradnje kapaciteta onih institucija, tijela i agencija EU-a koji su na nižem stupnju razvoja u pogledu kibersigurnosti;

12. PRIMA NA ZNANJE zaključke i preporuke tematskog izvješća te PREPOZNAJE da bi trebalo znatno poboljšati razinu pripravnosti institucija, tijela i agencija EU-a u pogledu kibersigurnosti, kao i sinergiju među njima. Institucije, tijela i agencije EU-a trebali bi imati sveobuhvatan okvir za upravljanje rizicima u području kibersigurnosti, provoditi redovite procjene rizika i revizije na temelju zajedničke ili dobro poznate metodologije i međunarodnih standarda te sistematizirati osviještenost o kibersigurnosti i programe osposobljavanja za osoblje;

13. ujedno ISTIČE da bi institucije, tijela i agencije EU-a trebali dodijeliti dostatna proračunska sredstva kako bi se osigurala provedba mjera zaštite od kiberprijetnji uz istodobno poštovanje višegodišnjeg financijskog okvira i PRIMA NA ZNANJE preporuku iz tematskog izvješća da bi trebalo imenovati tijelo koje bi bilo predstavnik svih institucija, tijela i agencija EU-a i dati mu odgovarajuće ovlasti i sredstva za praćenje usklađenosti sa zajedničkim pravilima o kibersigurnosti;

14. PREPOZNAJE da bi CERT-EU trebao bez odgode biti obaviješten o ozbiljnim kiberincidentima u institucijama, tijelima i agencijama EU-a i u tu bi svrhu trebao raspolagati odgovarajućim resursima koji su predvidljivi i prilagođeni trenutačnoj razini prijetnje i potrebama institucija, tijela i agencija EU-a, posebno u pogledu osoblja, tehničke opreme i infrastrukture;

15. NAPOMINJE da bi trebalo ojačati i sistematizirati suradnju i razmjenu informacija o kibersigurnosti, kao i interoperabilnost sigurnih informacijskih kanala među institucijama, tijelima i agencijama EU-a; POZIVA na to da se u tu suradnju i razmjenu informacija uključe i javna tijela odgovorna za kibersigurnost u državama članicama;

16. PRIMA NA ZNANJE odgovore Komisije, CERT-EU-a i ENISA-e priložene tematskom izvješću;

17. POZIVA Komisiju da uzme u obzir preporuke iz tematskog izvješća i da bude ambiciozna pri osmišljavanju kibersigurnosnih politika institucija, tijela i agencija EU-a te da se zalaže za veću sinergiju među njima.