Rada
Európskej únie

V Bruseli 21. júna 2022
(OR. en)

10504/22

CYBER 232
TELECOM 288
CSC 286
CSCI 96
FIN 689

VÝSLEDOK ROKOVANIA

Od:	Generálny sekretariát Rady
Dátum:	21. júna 2022
Komu:	Delegácie
Č. predch. dok.:	9716/22
Predmet:	Závery Rady k osobitnej správe Európskeho dvora audítorov č. 5/2022 s názvom „Kybernetická bezpečnosť inštitúcií, orgánov a agentúr EÚ: celková úroveň pripravenosti nezodpovedá hrozbám“ – závery Rady schválené Radou na zasadnutí 21. júna 2021

Delegáciám v prílohe zasielame uvedené závery Rady v znení, ktoré Rada schválila na svojom zasadnutí 21. júna 2022.

PRÍLOHA

ZÁVERY RADY

k osobitnej správe Európskeho dvora audítorov č. 5/2022 s názvom „Kybernetická bezpečnosť inštitúcií, orgánov a agentúr EÚ: celková úroveň pripravenosti nezodpovedá hrozbám“

RADA EURÓPSKEJ ÚNIE,

PRIPOMÍNA svoje závery o zlepšení skúmania osobitných správ Dvora audítorov v súvislosti s postupom udeľovania absolutória[1];

1. BERIE NA VEDOMIE osobitnú správu Európskeho dvora audítorov č. 5/2022 s názvom „Kybernetická bezpečnosť inštitúcií, orgánov a agentúr EÚ: celková úroveň pripravenosti nezodpovedá hrozbám“[2].

2. ZDÔRAZŇUJE význam a naliehavosť posilnenia úrovne kybernetickej bezpečnosti v inštitúciách, orgánoch a agentúrach EÚ vzhľadom na nedávne zintenzívnenie digitálnej transformácie v rámci inštitúcií, citlivé informácie, ktoré spracúvajú, neustále sa zvyšujúci počet a závažnosť útokov na inštitúcie, orgány a agentúry EÚ a úroveň hrozby, ktorá sa ich týka.

3. PRIPOMÍNA závery Európskej rady z 20. júna 2019[3], v ktorých Európska rada vyzvala inštitúcie EÚ, aby spolu s členskými štátmi pracovali na opatreniach na zvýšenie odolnosti a posilnenie bezpečnostnej kultúry EÚ v súvislosti s kybernetickými a hybridnými hrozbami z krajín mimo EÚ, ako aj na lepšiu ochranu informačných a komunikačných sietí EÚ a jej rozhodovacích procesov pred škodlivými aktivitami každého druhu.

---

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

4. PRIPOMÍNA svoje závery z 10. decembra 2019 o komplementárnom úsilí zameranom na zvyšovanie odolnosti a boj proti hybridným hrozbám[4], v ktorých vyzvala inštitúcie, orgány a agentúry EÚ, podporované členskými štátmi, aby na základe komplexného posúdenia hrozieb zabezpečili schopnosť Únie brániť svoju integritu a zvyšovať bezpečnosť svojich informačných a komunikačných sietí a rozhodovacích procesov pred škodlivými činnosťami všetkých druhov. Na tento účel sa v záveroch uviedlo, že inštitúcie, orgány a agentúry, podporované členskými štátmi by mali vypracovať a zaviesť komplexný súbor opatrení na zaistenie svojej bezpečnosti v súlade s mandátom Európskej rady z júna 2019[5].

5. PRIPOMÍNA svoje závery z 22. marca 2021 o stratégii kybernetickej bezpečnosti EÚ v digitálnej dekáde[6], v ktorých zdôraznila, že kybernetická bezpečnosť má zásadný význam pre fungovanie verejnej správy a inštitúcií na vnútroštátnej úrovni aj na úrovni EÚ, ako aj pre našu spoločnosť a hospodárstvo ako celok.

6. PRIPOMÍNA svoje závery z 23. mája 2022 o vývoji prístupu Európskej únie ku kybernetickej bezpečnosti[7], v ktorých boli inštitúcie, orgány a agentúry EÚ vyzvané, aby sa zapojili do mapovania existujúcich nástrojov bezpečnej komunikácie v kybernetickej oblasti, o ktorých sa má diskutovať v príslušných orgánoch Rady a s príslušnými skupinami pre spoluprácu, ako je sieť jednotiek CSIRT a EU CyCLONe.

7. ZDÔRAZŇUJE potrebu riešiť systémové riziko, ktoré predstavuje prepojenie medzi inštitúciami, orgánmi a agentúrami EÚ, ako aj medzi nimi a inštitúciami členských štátov, a to aj napriek ich inštitucionálnej nezávislosti a administratívnej autonómii.

---

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

8. BERIE NA VEDOMIE pripomienky uvedené v osobitnej správe, konkrétne, že inštitúcie, orgány a agentúry EÚ nedosiahli úroveň kybernetickej pripravenosti zodpovedajúcu hrozbám a majú rôznu úroveň vyspelosti v oblasti kybernetickej bezpečnosti. UZNÁVA, že by sa mala zlepšiť úroveň pripravenosti inštitúcií, orgánov a agentúr EÚ v oblasti kybernetickej bezpečnosti, ako aj synergie medzi nimi.

9. Dôrazne preto NABÁDA inštitúcie, orgány a agentúry EÚ, aby pokračovali vo vykonávaní opatrení na zníženie kybernetických rizík, ktorými sa zabezpečí primeraná úroveň kybernetickej bezpečnosti, ako sa predpokladá v navrhovanej smernici o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii a o zrušení smernice (EÚ) 2016/1148, s cieľom zlepšiť svoju úroveň pripravenosti.

10. VYZÝVA inštitúcie, orgány a agentúry EÚ, aby zintenzívnili svoje úsilie o ochranu pred kybernetickými hrozbami, ako aj spoluprácu pri vypracúvaní jednotných noriem a špecifikácií, najmä pre verejné obstarávanie, projekty a služby súvisiace s kybernetickou bezpečnosťou, a aby zlepšili interoperabilitu svojich informačných systémov, a to aj s cieľom zabezpečiť bezpečnú komunikáciu neutajovaného obsahu.

11. VYZÝVA Agentúru Európskej únie pre kybernetickú bezpečnosť (ENISA) a tím reakcie na núdzové počítačové situácie v európskych inštitúciách, orgánoch a agentúrach (CERT-EU), aby v rámci svojich právomocí zintenzívnili spoluprácu pri podpore inštitúcií, orgánov a agentúr EÚ v ich úsilí v oblasti kybernetickej bezpečnosti, najmä pokiaľ ide o budovanie kapacít pre tie inštitúcie, orgány a agentúry EÚ, ktoré majú nižšiu úroveň vyspelosti v oblasti kybernetickej bezpečnosti.

12. BERIE NA VEDOMIE závery a odporúčania z osobitnej správy a UZNÁVA, že by sa mala významne zlepšiť úroveň pripravenosti inštitúcií, orgánov a agentúr EÚ v oblasti kybernetickej bezpečnosti, ako aj synergie medzi nimi. Inštitúcie, orgány a agentúry EÚ by mali mať komplexný rámec riadenia rizík v oblasti kybernetickej bezpečnosti, vykonávať pravidelné posúdenia a audity rizík na základe spoločnej alebo všeobecne známej metodiky a medzinárodných noriem a systematizovať osvetové a vzdelávacie programy v oblasti kybernetickej bezpečnosti pre zamestnancov.

13. ZDÔRAZŇUJE tiež, že inštitúcie, orgány a agentúry EÚ by mali vyčleniť dostatočný rozpočet na zabezpečenie vykonávania ochranných opatrení proti kybernetickým hrozbám pri súčasnom dodržiavaní viacročného finančného rámca, a BERIE NA VEDOMIE odporúčanie z osobitnej správy, podľa ktorého by sa mal určiť orgán zastupujúci všetky inštitúcie, orgány a agentúry EÚ a mal by sa mu udeliť primeraný mandát a prostriedky na monitorovanie dodržiavania spoločných pravidiel v oblasti kybernetickej bezpečnosti.

14. UZNÁVA, že tím CERT-EU by mal byť bezodkladne informovaný o závažných kybernetických incidentoch v inštitúciách, orgánoch a agentúrach EÚ a na tento účel by mal byť vybavený primeranými zdrojmi, ktoré sú predvídateľné a prispôsobené súčasnej úrovni ohrozenia a potrebám inštitúcií, orgánov a agentúr EÚ, najmä pokiaľ ide o personál, technické vybavenie a infraštruktúru.

15. KONŠTATUJE, že by sa mala posilniť a systematizovať spolupráca a výmena informácií o kybernetickej bezpečnosti, ako aj interoperabilita bezpečných komunikačných kanálov medzi inštitúciami, orgánmi a agentúrami EÚ. VYZÝVA, aby takáto spolupráca a výmena informácií zahŕňala aj orgány verejnej moci zodpovedné za kybernetickú bezpečnosť v členských štátoch.

16. Berie NA VEDOMIE odpovede Komisie, tímu CERT-EU a agentúry ENISA pripojené k osobitnej správe.

17. VYZÝVA Komisiu, aby zohľadnila odporúčania z osobitnej správy a bola ambiciózna pri navrhovaní politík v oblasti kybernetickej bezpečnosti inštitúcií, orgánov a agentúr EÚ a aby sa zasadzovala za väčšiu súčinnosť medzi nimi.