Rada
Evropské unie

Brusel 10. června 2022
(OR. fr, en)

9716/22

LIMITE

CYBER 198
TELECOM 255
CSC 228
CSCI 74
FIN 590

POZNÁMKA K BODU „I/A“

Odesílatel:	Generální sekretariát Rady
Příjemce:	Výbor stálých zástupců / Rada
Č. předchozího dokumentu:	9317/2/22 REV 2
Předmět:	Návrh závěrů Rady ke zvláštní zprávě Evropského účetního dvora č. 5/2022 nazvané „Kybernetická bezpečnost orgánů, institucí a jiných subjektů EU: úroveň připravenosti obecně není úměrná hrozbám“ – schválení

1. Dne 30. března 2022 zveřejnil Evropský účetní dvůr zvláštní zprávu č. 5/2022 nazvanou „Kybernetická bezpečnost orgánů, institucí a jiných subjektů EU: úroveň připravenosti obecně není úměrná hrozbám“.[1]

2. Na zasedání dne 13. dubna 2022 svěřil Výbor stálých zástupců práci na této zvláštní zprávě Horizontální pracovní skupině pro otázky týkající se kybernetiky.[2]

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

3. Zástupci Účetního dvora předložili dotčenou zvláštní zprávu Horizontální pracovní skupině pro otázky týkající se kybernetiky dne 3. května 2022. V návaznosti na jednání o uvedené zprávě na témže zasedání pracovní skupiny vypracovalo předsednictví návrh závěrů Rady, který byl projednán na zasedání pracovní skupiny dne 24. května 2022.

4. Dne 10. června 2022 dosáhla Horizontální pracovní skupina pro otázky týkající se kybernetiky dohody o znění uvedeném v příloze.

5. Výbor stálých zástupců se vyzývá, aby tento návrh závěrů schválil a aby navrhl Radě jeho přijetí na některém ze svých nadcházejících zasedání.

PŘÍLOHA

NÁVRH ZÁVĚRŮ RADY

k zvláštní zprávě Evropského účetního dvora č. 5/2022
nazvané
„Kybernetická bezpečnost orgánů, institucí a jiných subjektů EU: úroveň připravenosti obecně není úměrná hrozbám“

RADA EVROPSKÉ UNIE,

PŘIPOMÍNAJÍC své závěry o zlepšení posuzování zvláštních zpráv vypracovaných Účetním dvorem v souvislosti s postupem udělování absolutoria[3];

1. BERE NA VĚDOMÍ zvláštní zprávu Evropského účetního dvora č. 5/2022 nazvanou „Kybernetická bezpečnost orgánů, institucí a jiných subjektů EU: úroveň připravenosti obecně není úměrná hrozbám“[4].

2. ZDŮRAZŇUJE význam a naléhavost zvýšení úrovně kybernetické bezpečnosti v rámci orgánů, institucí a jiných subjektů EU s ohledem na nedávné zintenzivnění digitální transformace v orgánech EU, citlivé informace, které zpracovávají, stále rostoucí počet a závažnost útoků na orgány, instituce a jiné subjekty EU a na úroveň hrozby, jíž čelí.

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

3. PŘIPOMÍNÁ závěry Evropské rady ze zasedání dne 20. června 2019[5], v nichž Evropská rada vyzývá orgány EU, aby společně s členskými státy pracovaly na opatřeních ke zvýšení odolnosti a zlepšení kultury bezpečnosti EU vůči kybernetickým a hybridním hrozbám majícím původ mimo EU, jakož i za účelem lepší ochrany informačních a komunikačních sítí EU a jejích rozhodovacích procesů před nepřátelskými činnostmi všeho druhu.

4. PŘIPOMÍNÁ své závěry ze dne 10. prosince 2019 o dalším úsilí za účelem posílení odolnosti a boje proti hybridním hrozbám[6], v nichž vyzvala orgány, instituce a jiné subjekty EU, aby s podporou členských států zajistily, že Unie bude schopna chránit svou integritu a zvýšit úroveň zabezpečení informačních a komunikačních sítí a rozhodovacích procesů EU vůči nepřátelským činnostem všeho druhu, a to na základě komplexního posouzení hrozeb. Za tímto účelem se v závěrech uvádí, že by orgány, instituce a jiné subjekty měly v souladu s mandátem Evropské rady z června 2019 a s podporou členských států vypracovat a provádět komplexní soubor opatření k zajištění své bezpečnosti[7].

5. PŘIPOMÍNÁ své závěry ze dne 22. března 2021 týkající se Strategie kybernetické bezpečnosti EU pro digitální dekádu[8], v nichž zdůrazňuje, že kybernetická bezpečnost má zásadní význam jak pro fungování veřejné správy a veřejných orgánů na vnitrostátní i unijní úrovni, tak i pro naši společnost a hospodářství jako celek.

---

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

6. PŘIPOMÍNÁ své závěry ze dne 23. května 2022 o rozvoji kybernetické pozice Evropské unie[9], v nichž se orgány, instituce a agentury EU vyzývají, aby se zapojily do zmapování stávajících nástrojů pro zabezpečenou komunikaci v kybernetické oblasti, které budou projednány v příslušných orgánech Rady a s příslušnými skupinami pro spolupráci, jako jsou sítě CSIRT a EU CyCLONe.

7. ZDŮRAZŇUJE, že je třeba řešit systémové riziko, které existuje v propojení mezi orgány, institucemi a jinými subjekty EU, jakož i mezi nimi a orgány členských států, navzdory jejich institucionální nezávislosti a správní samostatnosti.

8. BERE NA VĚDOMÍ připomínky uvedené ve zvláštní zprávě, konkrétně to, že orgány, instituce a jiné subjekty EU nedosáhly úrovně kybernetické připravenosti úměrné hrozbám a mají rozdílnou úroveň vyspělosti kybernetické bezpečnosti. UZNÁVÁ, že je zapotřebí úroveň kybernetické připravenosti orgánů, institucí a jiných subjektů EU zlepšit, stejně jako jejich vzájemnou součinnost.

9. Důrazně proto VYBÍZÍ orgány, instituce a jiné subjekty EU, aby pokračovaly v provádění opatření v oblasti řízení rizik pro kybernetickou bezpečnost, jež zajistí přiměřenou úroveň kybernetické bezpečnosti, jak se předpokládá v navrhované směrnici o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148, za účelem zlepšení jejich úrovně připravenosti.

10. VYZÝVÁ orgány, instituce a jiné subjekty EU, aby zintenzivnily své úsilí o vlastní ochranu před kybernetickými hrozbami, jakož i spolupráci, pokud jde o zavedení jednotných standardů a specifikací, zejména pro veřejné zakázky, projekty a služby týkající se kybernetické bezpečnosti, a aby zlepšily interoperabilitu svých IT systémů, mimo jiné s ohledem na zajištění bezpečného sdílení neutajovaných informací.

[9] Dokument 9364/22.

11. VYZÝVÁ Agenturu Evropské unie pro kybernetickou bezpečnost (ENISA) a skupinu pro reakci na počítačové hrozby v orgánech, institucích a jiných subjektech EU (CERT-EU), aby v rámci svých pravomocí zintenzivnily spolupráci při podpoře orgánů, institucí a jiných subjektů EU v jejich úsilí o kybernetickou bezpečnost, zejména s ohledem na budování kapacit těch orgánů, institucí a jiných subjektů EU, které mají nižší úroveň vyspělosti kybernetického zabezpečení.

12. BERE NA VĚDOMÍ závěry a doporučení obsažená ve zvláštní zprávě a UZNÁVÁ, že je zapotřebí výrazně zlepšit úroveň kybernetické připravenosti orgánů, institucí a jiných subjektů EU, jakož i jejich vzájemnou součinnost. Orgány, instituce a jiné subjekty EU by měly mít komplexní rámec řízení rizik v oblasti kybernetické bezpečnosti, provádět pravidelná posuzování rizik a audity na základě společné nebo všeobecně známé metodiky a mezinárodních standardů a systematizovat osvětové a školicí programy v oblasti kybernetické bezpečnosti pro zaměstnance.

13. ZDŮRAZŇUJE také, že orgány, instituce a jiné subjekty EU by měly vyčlenit dostatečné rozpočtové prostředky na zajištění provádění ochranných opatření proti kybernetickým hrozbám při současném respektování víceletého finančního rámce, a BERE NA VĚDOMÍ doporučení, aby byl jmenován zástupce všech orgánů, institucí a jiných subjektů EU, jemuž je třeba udělit příslušný mandát a prostředky na monitorování souladu se společnými pravidly v oblasti kybernetické bezpečnosti.

14. UZNÁVÁ, že skupina CERT-EU by měla být neprodleně informována o závažných kybernetických incidentech v rámci orgánů, institucí a jiných subjektů EU a za tímto účelem by měla být vybavena odpovídajícími zdroji, které jsou předvídatelné a přizpůsobené současné úrovni hrozby a potřebám orgánů, institucí a jiných subjektů EU, zejména pokud jde o zaměstnance, technické vybavení a infrastrukturu.

15. KONSTATUJE, že by měla být mezi orgány, institucemi a jinými subjekty EU posílena a systematizována spolupráce a výměna informací o kybernetické bezpečnosti, jakož i interoperabilita zabezpečených komunikačních kanálů. VYZÝVÁ, aby tato spolupráce a výměna informací zahrnovala rovněž orgány veřejné správy odpovědné za kybernetickou bezpečnost v členských státech.

16. BERE NA VĚDOMÍ odpovědi Komise, skupiny CERT-EU a agentury ENISA, které jsou připojeny k této zvláštní zprávě.

17. VYZÝVÁ Komisi, aby zohlednila doporučení obsažená ve zvláštní zprávě a aby byla ambiciózní při navrhování politik v oblasti kybernetické bezpečnosti orgánů, institucí a jiných subjektů EU a aby se též zasazovala o větší součinnosti mezi nimi.