Az Európai Unió
Tanácsa

Brüsszel, 2022. június 10.
(OR. fr, en)

9716/22

LIMITE

CYBER 198
TELECOM 255
CSC 228
CSCI 74
FIN 590

FELJEGYZÉS AZ „I/A” NAPIRENDI PONTHOZ

Küldi:	a Tanács Főtitkársága
Címzett:	az Állandó Képviselők Bizottsága/a Tanács
Előző dok. sz.:	9317/2/22 REV 2
Tárgy:	Tervezet – A Tanács következtetései az Európai Számvevőszék 05/2022. sz., „Az uniós intézmények, szervek és ügynökségek kiberbiztonsága: a felkészültség szintje összességében nem áll arányban a fenyegetésekkel” című különjelentéséről – Jóváhagyás

1. Az Európai Számvevőszék 2022. március 30-án közzétette a 05/2022. sz., „Az uniós intézmények, szervek és ügynökségek kiberbiztonsága: a felkészültség szintje összességében nem áll arányban a fenyegetésekkel” című különjelentését[1].

2. Az Állandó Képviselők Bizottsága a 2022. április 13-i ülésén a kiberkérdésekkel foglalkozó horizontális munkacsoportot bízta meg a különjelentés vizsgálatával[2].

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

3. A Számvevőszék képviselői 2022. május 3-án benyújtották a különjelentést a kiberkérdésekkel foglalkozó horizontális munkacsoportnak. Az elnökség – a munkacsoport ugyanezen ülésén a különjelentésről folytatott megbeszéléseket követően – tanácsi következtetéstervezetet készített, amelyet a munkacsoport a 2022. május 24-i ülésén vitatott meg.

4. A kiberkérdésekkel foglalkozó horizontális munkacsoport 2022. június 10-én megállapodásra jutott a mellékletben található szövegről.

5. Felkérjük az Állandó Képviselők Bizottságát, hogy hagyja jóvá a következtetéstervezetet és javasolja a Tanácsnak, hogy az egyik soron következő ülésén fogadja el azt.

MELLÉKLET

TERVEZET – A TANÁCS KÖVETKEZTETÉSEI

a Számvevőszék 5/2022. sz.,
„Az uniós intézmények, szervek és ügynökségek kiberbiztonsága: a felkészültség szintje összességében nem áll arányban a fenyegetésekkel”
című különjelentéséről

AZ EURÓPAI UNIÓ TANÁCSA,

EMLÉKEZTETVE a Számvevőszék által a mentesítési eljárás keretében készített különjelentések vizsgálatának javításáról szóló tanácsi következtetésekre[3];

1. NYUGTÁZZA a Számvevőszék 5/2022. sz., „Az uniós intézmények, szervek és ügynökségek kiberbiztonsága: a felkészültség szintje összességében nem áll arányban a fenyegetésekkel” című különjelentését[4].

2. KIEMELI az uniós intézmények, szervek és ügynökségek kiberbiztonsága megerősítésének fontosságát és sürgető mivoltát, tekintettel a digitális átállás intenzívebbé válására az intézményekben, az általuk kezelt érzékeny információkra, az uniós intézmények, szervek és ügynökségek ellen intézett egyre nagyobb számú és egyre súlyosabb támadásra, valamint arra, hogy milyen szintű fenyegetésekkel néznek szembe.

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

3. EMLÉKEZTET az Európai Tanács 2019. június 20-i következtetéseire[5], amelyben az Európai Tanács felkérte az uniós intézményeket, hogy a tagállamokkal közösen dolgozzanak ki olyan intézkedéseket, amelyek fokozzák az EU-nak az Unión kívülről érkező kiberfenyegetésekkel és hibrid fenyegetésekkel szembeni rezilienciáját, illetve javítják az EU biztonsági kultúráját, valamint amelyek hatékonyabb védelmet biztosítanak a rossz szándékú cselekmények minden formájával szemben az uniós információs és kommunikációs hálózatok és az EU döntéshozatali folyamatai számára.

4. EMLÉKEZTET a 2019. december 10-i, a reziliencia megerősítésére és a hibrid fenyegetések elleni küzdelemre irányuló kiegészítő jellegű erőfeszítésekről szóló következtetéseire[6], melyben felszólította az uniós intézményeket, szerveket és ügynökségeket, hogy a tagállamok támogatásával, egy átfogó fenyegetésértékelés alapján gondoskodjanak arról, hogy az Unió mindennemű rossz szándékú tevékenységgel szemben képes legyen megvédeni integritását, továbbá képes legyen fokozni az uniós információs és kommunikációs hálózatok, valamint döntéshozatali folyamatok biztonságát. A következtetésekben a Tanács megállapította, hogy e célból, saját biztonságuk garantálása érdekében az intézményeknek, a szerveknek és az ügynökségeknek – a tagállamok támogatásával – átfogó intézkedéscsomagot kell kidolgozniuk és végrehajtaniuk, az Európai Tanácstól 2019 júniusában kapott megbízással[7] összhangban.

5. EMLÉKEZTET a 2021. március 22-i, a digitális évtizedre vonatkozó uniós kiberbiztonsági stratégiáról szóló következtetéseire[8], melyben hangsúlyozta, hogy a kiberbiztonság mind nemzeti, mind uniós szinten létfontosságú a közigazgatás és az intézmények működése szempontjából, valamint társadalmaink és a gazdaság egésze számára.

---

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

6. EMLÉKEZTET az Európai Unió kiberbiztonsági helyzetének javításáról szóló 2022. május 23-i következtetéseire[9], amelyben ösztönözte az uniós intézményeket, szerveket és ügynökségeket arra, hogy vegyenek részt a kiberterületen történő biztonságos kommunikáció már létező eszközeinek feltérképezésében a releváns tanácsi szervekben és a releváns együttműködési csoportokkal – így a CSIRT-ek hálózatával és az EU-CyCLONe-nal – való megvitatás céljából.

7. HANGSÚLYOZZA, hogy kezelni kell azt a rendszerszintű kockázatot, amely az uniós intézmények, szervek és ügynökségek közötti, valamint a közöttük és a tagállami intézmények közötti kölcsönös összeköttetésben rejlik, intézményi függetlenségük és igazgatási autonómiájuk ellenére.

8. NYUGTÁZZA a különjelentésben foglalt megállapításokat, nevezetesen azt, hogy az uniós intézmények, szervek és ügynökségek kiberfelkészültsége összességében nem arányos a fenyegetések mértékével, valamint hogy kiberbiztonsági fejlettségi szintjük eltérő. ELISMERI, hogy javítani kell az uniós intézmények, szervek és ügynökségek kiberbiztonsági felkészültségét, valamint a közöttük lévő szinergiákat.

9. Ezért erőteljesen SZORGALMAZZA, hogy az uniós intézmények, szervek és ügynökségek – felkészültségi szintjük javítása érdekében – folytassák a kiberbiztonság arányos szintjét biztosító kiberkockázat-kezelési intézkedések végrehajtását, az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről szóló, az (EU) 2016/1148 irányelvet hatályon kívül helyező, javasolt irányelvben előirányzottaknak megfelelően.

10. FELKÉRI az uniós intézményeket, szerveket és ügynökségeket, hogy egyrészt fokozzák erőfeszítéseiket a kiberfenyegetésekkel szembeni védelmük érdekében, másrészt folytassanak intenzívebb együttműködést a konzisztens szabványok és előírások kialakítása céljából, különösen a közbeszerzések, valamint a kiberbiztonsággal kapcsolatos projektek és szolgáltatások tekintetében, továbbá javítsák informatikai rendszereik interoperabilitását, többek között a nem minősített tartalmak biztonságos továbbításának garantálása érdekében.

[9] 9364/22.

11. FELKÉRI az Európai Uniós Kiberbiztonsági Ügynökséget (ENISA) és az európai intézmények, szervek és hivatalok számítógépes vészhelyzeteket elhárító csoportját (CERT-EU), hogy hatáskörük keretein belül fokozzák együttműködésüket az uniós intézmények, szervek és ügynökségek kiberbiztonsági erőfeszítéseinek támogatása érdekében, különös tekintettel az alacsonyabb kiberbiztonsági fejlettségi szinttel rendelkező uniós intézmények, szervek és ügynökségek kapacitásépítésére.

12. NYUGTÁZZA a különjelentésben foglalt megállapításokat és ajánlásokat, és ELISMERI, hogy számottevően javítani kell az uniós intézmények, szervek és ügynökségek kiberbiztonsági felkészültségét, valamint a közöttük lévő szinergiákat. Az uniós intézményeknek, szerveknek és ügynökségeknek átfogó kiberbiztonsági kockázatkezelési keretrendszerrel kell rendelkezniük, közös vagy jól ismert módszertanon és nemzetközi szabványokon alapuló rendszeres kockázatértékeléseket és ellenőrzéseket kell tartaniuk, valamint szisztematikus, a kiberbiztonsági tudatosság fokozását célzó és képzési programokat kell biztosítaniuk a személyzet számára.

13. HANGSÚLYOZZA továbbá, hogy az uniós intézményeknek, szerveknek és ügynökségeknek – a többéves pénzügyi keret tiszteletben tartása mellett – megfelelő költségvetést kell elkülöníteniük a kiberfenyegetésekkel szembeni védelmi intézkedések végrehajtásának biztosítására, valamint NYUGTÁZZA a különjelentésben foglalt ajánlást, miszerint ki kell jelölni egy, valamennyi uniós intézményt, szervet és ügynökséget képviselő testületet, amely megfelelő felhatalmazással és eszközökkel bír annak nyomon követésére, hogy minden uniós szerv betartja-e a közös kiberbiztonsági szabályokat.

14. ELISMERI, hogy a CERT-EU-t haladéktalanul tájékoztatni kell az uniós intézményeken, szerveken és ügynökségeken belüli jelentős kiberbiztonsági eseményekről, és ebből a célból a CERT-EU számára megfelelő, kiszámítható, a jelenlegi fenyegetettségi szinthez és az uniós intézmények, szervek és ügynökségek szükségleteihez igazított erőforrásokat kell biztosítani, mindenekelőtt a személyzet, a technikai felszerelések és az infrastruktúra tekintetében.

15. MEGÁLLAPÍTJA, hogy a kiberbiztonsággal kapcsolatos együttműködést és információcserét, valamint az uniós intézmények, szervek és ügynökségek közötti biztonságos kommunikációs csatornák interoperabilitását meg kell erősíteni és szisztematikussá kell tenni. Arra SZÓLÍT FEL, hogy az említett együttműködésbe és információcserébe vonják be a tagállamok kiberbiztonságért felelős hatóságait is.

16. NYUGTÁZZA a Bizottságnak, a CERT-EU-nak és az ENISA-nak a különjelentéshez mellékelt válaszait.

17. FELKÉRI a Bizottságot, hogy az uniós intézmények, szervek és ügynökségek kiberbiztonsági politikáinak kialakítása során vegye figyelembe a különjelentésben foglalt ajánlásokat, tűzzön ki ambiciózus célokat és szorgalmazza az uniós intézmények, szervek és ügynökségek közötti szinergiák fokozását.