EURÓPAI SZÁMVEVŐSZÉK

HU

02/2023. sz. vélemény

(az EUMSZ 322. cikkének (1) bekezdése alapján)

a kiberbiztonsági fenyegetések és események észlelése, valamint az azokra való felkészülés és reagálás céljából az Unión belüli szolidaritás és képességek megerősítését célzó intézkedések meghatározásáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatról [intézményközi referencia: 2023/0109(COD), 2023. április 18.]

Tartalomjegyzék

	Bekezdés
Bevezetés	01–03
Általános megjegyzések	04–05
Egyedi kérdésekkel kapcsolatos észrevételek	06–40
A hatásvizsgálat hiánya	06–08
Nem teljes körű a finanszírozásra vonatkozó információ	09–12
Nem teljes körű a finanszírozásra és az emberi erőforrásra vonatkozó információ	09–10
Nem teljes körű az európai kiberpajzs pénzügyi felépítésére vonatkozó információ	11–12
Az európai kiberpajzssal kapcsolatos kockázatok	13–26
Nagyobb összetettség, több réteg	13–20
Információmegosztás	21–26
A kiberbiztonsági vészhelyzeti mechanizmushoz kapcsolódó kockázatok	27–34
Az uniós kiberbiztonsági tartalék kiépítése	27–29
Az évenkéntiség elvétől való eltérés	30–34
A kiberbiztonsági események felülvizsgálati mechanizmusához kapcsolódó kockázatok	35–36
A teljesítménymonitoring és a szakpolitikák értékelése	37–40
Záró megjegyzések	41–43
Melléklet. Az európai kiberbiztonsági galaxis	

Bevezetés

01 A Bizottság 2023. április 18-án közzétette a kiberbiztonsági fenyegetések és események észlelése, valamint az azokra való felkészülés és reagálás céljából az Unión belüli szolidaritás és képességek megerősítését célzó intézkedések meghatározásáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatát (a továbbiakban: „a kiberszolidaritásról szóló uniós jogszabály”).

02 A kiberszolidaritásról szóló javasolt uniós jogszabály intézkedéseket határoz meg a kiberbiztonsági fenyegetések és események észlelésére, az azokra való felkészülésre és reagálásra, különösen az alábbiak révén:

- az **európai kiberpajzs,** az összehangolt észlelési és helyzetismereti képességek kiépítése és javítása érdekében;
- a **kiberbiztonsági vészhelyzeti mechanizmus**, amely támogatja a tagállamokat a jelentős és nagyszabású kiberbiztonsági eseményekre való felkészülésben, az azokra való reagálásban és az azokat követő helyreállításban;
- a **kiberbiztonsági események felülvizsgálati mechanizmusa,** a jelentős vagy nagyszabású események felülvizsgálatára és értékelésére.

03 A Bizottság javaslatának jogalapja[1] értelmében kötelező konzultációt folytatni az Európai Számvevőszékkel. Az Európai Parlament és az Európai Unió Tanácsa 2023. június 2-i, illetve 7-i levelében ki is kérte véleményünket. A konzultáció követelményének jelen véleményünkkel teszünk eleget.

[1] Az Európai Unió működéséről szóló szerződés 322. cikkének (1) bekezdése.

Általános megjegyzések

04 Elsődlegesen a tagállamok felelősek az őket érintő kiberbiztonsági események és válságok megelőzéséért, az azokra való felkészülésért és reagálásért. Az Európai Unióról szóló szerződés 4. cikkének (2) bekezdésével összhangban a nemzeti szintű biztonság az egyes tagállamok kizárólagos felelőssége marad. A jelentős vagy nagyszabású kiberbiztonsági események potenciális hatását figyelembe véve azonban uniós szintű közös fellépésre is szükség lehet.

05 A Számvevőszék kedvezően értékeli a javaslat arra irányuló célkitűzéseit, hogy megerősítse az Unió kollektív kiberrezilienciáját. Véleményünkben konkrét észrevételeket teszünk a kiberszolidaritásról szóló javasolt uniós jogszabály három elemével kapcsolatban, és rámutatunk néhány kockázatra a hatásvizsgálat hiánya, egyes pénzügyi szempontok, valamint a javaslatban meghatározott intézkedések végrehajtásának módja kapcsán. Külön kiemeljük azt a kockázatot, hogy a rendeletjavaslat nyomán az egész uniós kiberbiztonsági galaxis összetettebbé válhat, és javaslatokat teszünk e kockázat csökkentésére (lásd: ***13***–***20***. bekezdés).

Egyedi kérdésekkel kapcsolatos észrevételek

A hatásvizsgálat hiánya

06 A Bizottság minőségi jogalkotásra vonatkozó iránymutatásai a szakpolitikai tervezési és végrehajtási lehetőségek átfogó elemzésének részeként hatásvizsgálatok és az érdekelt felekkel folytatott konzultációk alkalmazását javasolják. Megítélésünk szerint az átfogó hatásvizsgálatok alapvető eszközt jelentenek mind annak megítéléséhez, hogy szükség van-e uniós fellépésre, mind a javaslatok elfogadását megelőzően annak elemzéséhez, hogy a rendelkezésre álló megoldások milyen lehetséges hatásokkal járnának.

07 Ezt a rendeletjavaslatot illetően nem került sor hatásvizsgálatra. A kísérő indokolás 3. szakaszában a Bizottság kifejti: *„a javaslat sürgős jellegére tekintettel”* úgy döntött, hogy nem végez ilyen hatásvizsgálatot. A Bizottság hozzáteszi, hogy a javasolt rendelet által bevezetett intézkedéseket a Digitális Európa program (DEP) fogja támogatni, és hogy az intézkedések a Digitális Európa programról szóló, 2018-ban külön hatásvizsgálatnak alávetett rendelettel összhangban állnak. A Bizottság kifejti továbbá, hogy a javasolt intézkedéseket a főbb érdekelt felekkel és a tagállamokkal szoros együttműködésben, a korábbi intézkedésekből levont tanulságokat figyelembe véve alakították ki.

08 Megjegyezzük azonban, hogy a DEP-hatásvizsgálat nem terjed ki a rendeletjavaslat által bevezetett új intézkedésekre. Ezért kevés az információ a rendelkezésre álló szakpolitikai lehetőségekről és a javaslattal kapcsolatos költségekről.

Nem teljes körű a finanszírozásra vonatkozó információ

Nem teljes körű a finanszírozásra és az emberi erőforrásra vonatkozó információ

09 A kiberszolidaritásról szóló uniós jogszabályban meghatározott intézkedések finanszírozása a Digitális Európa programból fog származni. A Bizottság az indokolásának 4. szakaszában kifejti, hogy 115 millió eurót már korábban elkülönítettek az Európai Kiberpajzs keretében a 2021–2022-es időszakban folytatott

kísérleti projektekre. Kifejti még, hogy a javaslat belső átcsoportosítás révén 100 millió euróval megnövelné a Digitális Európa program „Kiberbiztonság és bizalom” egyedi célkitűzésére 2023–2027-re elkülönített 743 millió eurós költségvetést.

10 Az átcsoportosítást követően a kiberbiztonságra rendelkezésre álló uniós finanszírozás a 2023–2027-es időszakra 843 millió euró lesz. Megjegyezzük, hogy ez az összeg nemcsak a rendeletjavaslatban meghatározott intézkedéseket fedezi, hanem a Digitális Európa program egyéb kiberbiztonsági intézkedéseit is (például az iparnak vagy a szabványosításnak nyújtott támogatást). A javaslat nem tartalmaz becslést a javasolt intézkedések (az európai kiberpajzs, a kiberbiztonsági vészhelyzeti mechanizmus – beleértve a kiberbiztonsági tartalékot – és a kiberbiztonsági események felülvizsgálati mechanizmusa) bevezetésével és végrehajtásával kapcsolatos várható összköltségről. Mivel a javaslatot nem kíséri hatásvizsgálat, javasoljuk, hogy a Bizottság a jobb átláthatóság végett tegye elérhetővé a vonatkozó költségbecsléseket.

Nem teljes körű az európai kiberpajzs pénzügyi felépítésére vonatkozó információ

11 A rendeletjavaslat II. fejezete létrehozza a nemzeti biztonsági műveleti központokból (SOC központok) és a határokon átnyúló biztonsági műveleti központokból (határokon átnyúló SOC központok) álló „európai kiberpajzsot”.
A rendeletjavaslat rendelkezése szerint a támogatható nemzeti SOC központok eszközeik és infrastruktúrájuk beszerzési költségeinek legfeljebb 50%-áig és működési költségeik legfeljebb 50%-áig kaphatnak pénzügyi hozzájárulást. A határokon átnyúló SOC központok esetében az uniós társfinanszírozás az eszközök és infrastruktúra beszerzési költségeinek legfeljebb 75%-át, illetve működési költségeik legfeljebb 50%-át fedezi. A rendeletjavaslat nem tér ki arra, hogy miért van szükség több, magasabb arányú társfinanszírozással támogatott eszközre és infrastruktúrára határokon átnyúló SOC központok esetében ahhoz képest, amit a nemzeti SOC központok rendelkezésére álló eszközök konzorciumban történő alkalmazása jelentene.

12 A rendeletjavaslat azt sem határozza meg, hogy az Unió mennyi ideig társfinanszírozza a nemzeti és a határokon átnyúló SOC központok működési költségeit. Ez azzal a kockázattal jár, hogy az európai kiberpajzs működése és fenntarthatósága az uniós finanszírozástól fog függeni.

Az európai kiberpajzssal kapcsolatos kockázatok

Nagyobb összetettség, több réteg

13 A 02/2019. számú áttekintésünkben[2] észrevételeztük, hogy az Unió kiberbiztonsági környezete összetett és többrétegű. Számos magán- és közszereplő tevékenykedik benne regionális, nemzeti és uniós szinten a polgári szférában, köztük bűnüldöző szervek és pénzügyi hírszerző egységek is. A kiberbiztonság a nemzetbiztonságnak és nemzetvédelemnek is kulcsfontosságú alkotóeleme. Véleményünk ***mellékletében*** bemutatjuk az Unió új kiberbiztonsági galaxisának térképét, amely a szövegdobozok egyikében sorolja fel a javaslatban bevezetett valamennyi mechanizmust és komponenst, jól mutatva, hogy a rendelet növeli az összetettséget és a rétegek számát.

14 A rendeletjavaslat II. fejezetében bevezetett európai kiberpajzs célja, hogy magas fokú uniós képességeket fejlesszen ki a kiberfenyegetésekre és -eseményekre vonatkozó adatok észlelésére, elemzésére és feldolgozására. A kiberpajzsot a nemzeti biztonsági műveleti központok és a határokon átnyúló biztonsági műveleti központok összekapcsolt, páneurópai infrastruktúrája fogja alkotni.

15 Az európai kiberpajzsban való részvételre a tagállamok kijelölnek legalább egy nemzeti SOC központot, amelynek közjogi szervnek kell lennie. A nemzeti SOC központok ezután legalább három tagállam SOC központjaiból álló, határokon átnyúló SOC központokat hoznak létre, amelyek elkötelezik magukat az együttműködés mellett és összehangolják a kiberbiztonsági események észlelésére és a kiberfenyegetések nyomon követésére irányuló tevékenységeiket.

16 Az elmúlt években az Unió megerősítette kiberbiztonsági szabályozási keretét. Ennek egyik legfontosabb eszköze a hálózati és információs rendszerek biztonságáról szóló 2016. évi irányelv (a továbbiakban: NIS-irányelv), illetve annak 2022. évi felülvizsgálata (a NIS 2 irányelv). A NIS 2 irányelv értelmében a tagállamoknak nemzeti szinten létre kell hozniuk egy vagy több számítógép-biztonsági eseményekre reagáló csoportot (CSIRT). Uniós szinten a NIS 2 irányelv létrehozza a Kiberbiztonsági Együttműködési Csoportot, a CSIRT csoportok hálózatát és az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatát (EU CyCLONe).

[2] 02/2019. sz. áttekintés: „Az eredményes uniós kiberbiztonsági politika előtt álló kihívások”.

17 2021-ben az Unió létrehozta az Európai Kiberbiztonsági Kompetenciaközpontot. A 2023 májusában megnyílt központot tagállamonként egy-egy, összesen 27 nemzeti koordinációs központból álló hálózat fogja támogatni, amely központok némelyike egyben nemzeti SOC központ is. Ez a Központ felel majd a Digitális Európa program kiberbiztonsági komponensének végrehajtásáért, az uniós kiberbiztonsági tartalék kivételével. Ez utóbbit a Bizottság hajtja végre, de működtetésével és igazgatásával megbízhatja az ENISA-t.

18 A Bizottság közös kiberbiztonsági egységet is felállított. Az egység létrehozását 2020-ban az Unió kiberbiztonsági stratégiája jelentette be, és pontosabb meghatározása egy 2021. évi bizottsági ajánlásban történt meg.

19 2023 áprilisában a Bizottság bejelentette a Kiberkészségek Akadémiájának elindítását. Az új kezdeményezés célja a kiberbiztonsági szakemberhiány megszüntetése és az uniós „kibermunkaerő” kiépítése.

20 Mindezek alapján úgy véljük: fennáll annak a kockázata, hogy a rendeletjavaslat még összetettebbé teszi az uniós kiberbiztonsági galaxis egészét. Átfedések mutatkozhatnak a CSIRT csoportok meglévő hálózata és a SOC központok között. Noha a Bizottság az indokolása 1. szakaszában kifejti, hogy a határokon átnyúló SOC-platformoknak a CSIRT csoportok hálózatához képest új, kiegészítő képességeket kell biztosítaniuk, mi észrevételezzük, hogy feladataik és célkitűzéseik egy részét illetően a nemzeti SOC központok, a határokon átnyúló SOC központok, a CSIRT csoportok és a CSIRT csoportok hálózata hasonlóságokat mutatnak. Ilyen, átfedések által érintett terület többek között a fenyegetések észlelése és elhárítása, a kiberfenyegetésekkel kapcsolatos hírszerzés és a helyzetismeret. Ez a kockázat elvben csökkenthető az érintett struktúrák – elsősorban a nemzeti SOC központok és CSIRT csoportok, valamint a határokon átnyúló SOC központok – fokozatos konszolidációjával. A javaslatnak továbbá világossá kellene tennie, hogy egyértelmű irányítási rendszerek és felelősségi körök meghatározása révén hogyan működjenek együtt ezek a struktúrák az eredményes koordináció és szinergiák biztosítása érdekében.

Információmegosztás

21 A 05/2022. sz. különjelentésünkben[3] megállapítottuk, hogy az uniós intézmények, szervek és ügynökségek nem osztották meg egymással szisztematikusan a

[3] 05/2022. sz. különjelentés: „Az uniós intézmények, szervek és ügynökségek kiberbiztonsága: a felkészültség szintje összességében nem áll arányban a fenyegetésekkel”.

legfontosabb releváns kiberbiztonsági információkat, még akkor sem, ha kötelezve voltak erre. Az információmegosztás eredményességét csorbították a biztonságos kommunikációt akadályozó interoperabilitási gondok is. Bár megállapításunk az uniós szereplőknek erre a viszonylag kicsi és homogén csoportjára vonatkozott, megítélésünk szerint ez a kihívás tagállami szinten, az összetettebb és változatosabb kiberbiztonsági galaxisban még jelentősebb lesz.

22 A rendeletjavaslat 4. cikke értelmében a nemzeti SOC központoknak „referenciapontként és átjáróként” kell szolgálniuk más nemzeti szintű állami és magánszervezetek számára a kiberbiztonsági fenyegetésekkel és eseményekkel kapcsolatos információk gyűjtése és elemzése terén. Jelenleg azonban nincsen uniós szinten előírva, hogy az állami és magánszervezetek (köztük a nemzeti CSIRT csoportok, a privát szférában működő SOC központok és a NIS 2 irányelv értelmében vett „alapvető és fontos szervezetek”) milyen beszámolási kötelezettséggel bírnak a nemzeti SOC központok felé. Ezért fennáll annak a kockázata, hogy a nemzeti SOC központok nem kapják meg az igényeik szerinti adatokat vagy információkat.

23 A javaslatot kísérő pénzügyi kimutatás 2.2.2. szakaszában a Bizottság rámutat annak kockázatára, hogy a tagállamok nem osztják meg „elegendő mennyiségben” a kiberfenyegetésekkel kapcsolatos releváns információt sem a határokon átnyúló SOC-platformokon belül, sem pedig ezen platformok és más releváns uniós szintű szervezetek között. Az információmegosztás ilyen hiánya csorbíthatja az európai kiberpajzs eredményességét és csökkentheti az általa képviselt hozzáadott értéket.

24 Ezért örömmel látjuk, hogy a javaslat 4., 5. és 6. cikke külön rendelkezéseket tartalmaz az információmegosztás hiányának kockázatát enyhítendő. A javaslat értelmében a nemzeti SOC központok csak akkor részesülhetnek uniós finanszírozásban, ha kötelezettséget vállalnak a határokon átnyúló SOC központokban történő részvételre. Megjegyezzük azonban, hogy az első két évben kapott pénzügyi támogatást akkor sem kell visszatéríteni, ha a nemzeti SOC központ nem csatlakozik egy határokon átnyúló SOC központhoz. A rendeletjavaslat azt is előírja a határokon átnyúló SOC központok tagjai számára, hogy vállaljanak kötelezettséget „jelentős mennyiségű adat” kölcsönös megosztására és irányítási keret írásbeli konzorciumi megállapodás révén történő létrehozására.

25 Emellett a javaslat 7. cikke kimondja, hogy potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági eseményekről a releváns információkat a határokon átnyúló SOC központoknak „indokolatlan késedelem nélkül” el kell juttatniuk az EU-CyCLONe-nak, a CSIRT csoportok hálózatának és a Bizottságnak. Hangsúlyozzuk annak fontosságát, hogy ezt a rendelkezést megfelelően végre kell hajtani.

26 A rendeletjavaslat 6. cikke értelmében a Bizottság végrehajtási jogi aktusok útján meghatározhatja a határokon átnyúló SOC központok közötti interoperabilitás feltételeit. A 8. cikk értelmében a Bizottság végrehajtási jogi aktusokat fogadhat el, amelyekben technikai követelményeket állapít meg a tagállamok számára az infrastruktúra magas szintű adat- és fizikai biztonságának biztosítása érdekében. Ezekről a követelményekről és feltételekről gyorsan meg kell állapodni, hogy el lehessen kerülni egymással összeegyeztethetetlen rendszerek párhuzamos kifejlesztését és csökkenteni lehessen a költségeket.

A kiberbiztonsági vészhelyzeti mechanizmushoz kapcsolódó kockázatok

Az uniós kiberbiztonsági tartalék kiépítése

27 A 05/2022. sz. különjelentésünkben észrevételeztük, hogy a CERT-EU – az Unió saját számítógépes vészhelyzeteket elhárító csoportja, amely reagálási támogatást nyújt az uniós intézményeknek, szerveknek és ügynökségeknek – ellenőrzésünk idején nem működött a hét minden napján, napi 24 órában.

28 A rendeletjavaslat 14. cikke úgy rendelkezik, hogy a kiberbiztonsági tartalékból nyújtott támogatás iránti megkereséseket a Bizottság az ENISA közreműködésével bírálja el, és a választ „haladéktalanul” megküldi. Mivel előfordulhat, hogy több párhuzamos megkeresés rangsorolást tesz szükségessé, a rendeletjavaslat megállapít néhány döntéshozatali kritériumot. A 13. cikk meghatározza, hogy a Bizottság végrehajtási jogi aktusok útján pontosíthatja a tartalék allokációjára vonatkozó részletes szabályokat.

29 Alapvető fontosságúnak tartjuk, hogy a kiberbiztonsági tartalék nyújtotta támogatási szolgáltatás iránti megkeresés és a Bizottság válasza közötti időbeli eltérés ne legyen túl nagy a megkeresés időzítése miatt. A javaslat azonban nem ad meg előre meghatározott határidőt, és nem ír elő szervezeti lépéseket e határidő betartásának biztosítására.

Az évenkéntiség elvétől való eltérés

30 Az uniós költségvetés egyik alapelve a költségvetés évenkéntisége, vagyis hogy a költségvetésben szereplő előirányzatokat egy adott pénzügyi évre, december 31-éig engedélyezik. A fel nem használt kötelezettségvállalási és kifizetési előirányzatok nem

kerülnek automatikusan átvitelre a következő pénzügyi évre. Ezt az elvet a költségvetési rendelet 2. fejezete rögzíti.

31 A 19. cikkben a rendeletjavaslat eltérést engedélyez ettől az elvtől a kiberbiztonsági vészhelyzeti mechanizmus intézkedéseinek finanszírozása tekintetében. A cikk értelmében a felkészültséggel, reagálással és kölcsönös segítségnyújtással kapcsolatos intézkedésekre vonatkozó, fel nem használt kötelezettségvállalási és kifizetési előirányzatok automatikusan átvihetők a következő pénzügyi évre, és terhükre a következő év december 31-éig kötelezettségek vállalhatók és kifizetések teljesíthetők. Indokolásának 2. szakaszában a Bizottság kifejtette, hogy erre a rugalmasságra a költségvetési gazdálkodásban *„a kiberbiztonsági környezet és a kiberfenyegetések kiszámíthatatlan, rendkívüli és egyedi jellege”* miatt van szükség.

32 A felkészültséget illetően úgy ítéljük meg, hogy a szervezetek összehangolt felkészültségi tesztelésének tervezett tevékenységnek kell lennie, ezért az általában nem tekintendő kiszámíthatatlannak vagy rendkívülinek. Álláspontunk szerint az ilyen tervezett tevékenységek esetében nem szükséges eltérni az évenkéntiség alapelvétől.

33 Mivel az uniós kiberbiztonsági tartalékot és a kölcsönös segítségnyújtást csak kiszámíthatatlan eseményekre történő reagálás kapcsán fogják felhasználni, megítélésünk szerint az eltérés csak ilyen esetben indokolható.

34 Az egyértelműség érdekében, valamint hogy a rendelet megfogalmazása összhangban legyen más rendeletek, így az uniós polgári védelmi mechanizmusról vagy a Szomszédsági, Fejlesztési és Nemzetközi Együttműködési Eszközről (Globális Európa) szóló rendelet megfogalmazásával, véleményünk szerint a rendeletjavaslatnak elő kell írnia, hogy a fel nem használt kötelezettségvállalások automatikus átvitele csak a következő évre vonatkozzon.

A kiberbiztonsági események felülvizsgálati mechanizmusához kapcsolódó kockázatok

35 A rendeletjavaslat 18. cikke értelmében a Bizottságnak, az EU-CyCLONe-nak vagy a CSIRT csoportok hálózatának felkérésére az ENISA felülvizsgálja és értékeli az egy adott jelentős vagy nagyszabású kiberbiztonsági eseményhez kapcsolódó fenyegetéseket, sebezhetőségeket és mérséklési intézkedéseket. Az ENISA együttműködik az összes érdekelt féllel, majd az eseményt értékelve benyújt egy jelentést a fő okokról, a sebezhetőségekről és a levont tanulságokról.

36 Megítélésünk szerint ez fontos visszajelzési mechanizmus a kiberbiztonsági fenyegetésekkel és eseményekkel szembeni uniós észlelési, felkészültségi és reagálási képességek folyamatos megerősítéséhez. Javasoljuk azonban, hogy a rendeletjavaslat határozza meg, hogy az ENISA legkésőbb meddig nyújtsa be az egyes eseményeket követő jelentéseit ahhoz, hogy a visszajelzés kellő időben megtörténjen. A javaslat kiköti, hogy a jelentés adott esetben tartalmazzon ajánlásokat az Unió kiberbiztonsági helyzetének javítására. Azt azonban nem írja elő a javaslat, hogy az ajánlások hasznosulását hogyan kell nyomon követni.

A teljesítménymonitoring és a szakpolitikák értékelése

37 A rendeletjavaslat 19. cikke egy új, mérhető mutató bevezetésével módosítja a Digitális Európa programról szóló rendelet II. mellékletét, a következőképp: *„a kiberbiztonsági eseményekre való felkészültséget és reagálást támogató intézkedések száma a kiberbiztonsági vészhelyzeti mechanizmus keretében”.* Ez a mutató kiegészít két meglévő mutatót, amelyek célja, hogy nyomon kövessék a Digitális Európa program kiberbiztonságra és bizalomra vonatkozó egyedi célkitűzésének megvalósítása terén elért előrehaladást és beszámoljanak arról. Ez a két mutató: *„a közös beszerzésű kiberbiztonsági infrastruktúrák és/vagy eszközök száma”*, valamint *„az európai kiberbiztonsági létesítményekhez hozzáféréssel rendelkező felhasználók és felhasználói közösségek száma”.*

38 Véleményünk szerint a javasolt új mutató csak az outputot méri, és kevéssé szemlélteti az európai kiberpajzs és a kiberbiztonsági vészhelyzeti mechanizmus használatát és eredményeit.

39 A javaslat 20. cikke előírja a Bizottság számára, hogy négy évvel a rendelet alkalmazásának kezdőnapját követően jelentést nyújtson be az Európai Parlamentnek és a Tanácsnak a rendelet értékeléséről és felülvizsgálatáról.

40 Az értékelésnek véleményünk szerint is elegendő és megbízható adaton kell alapulnia, ugyanakkor a gyorsan változó fenyegetettségi helyzet az Unió és tagállamai részéről folyamatos alkalmazkodást és innovációt tesz szükségessé. Ezért az időzítést tekintve úgy véljük, hogy a jelenlegi javaslat szerint az értékelésre az új programozási időszakon belül túl későn kerülne sor. Ezenkívül a Digitális Európa program kiberbiztonságra és bizalomra vonatkozó egyedi célkitűzésére előirányzott teljes összeg már 2027 végéig le lesz kötve.

Záró megjegyzések

41 A kiberszolidaritásról szóló javasolt uniós jogszabály intézkedéseket határoz meg a kiberbiztonsági fenyegetések és események észlelésére, az azokra való felkészülésre és reagálásra. A Számvevőszék kedvezően értékeli a javaslat arra irányuló célkitűzéseit, hogy megerősítse az Unió kollektív kiberrezilienciáját.

42 Véleményünkben rámutatunk néhány általunk azonosított kockázatra, és arra, hogyan lehet végrehajtani a javaslatban meghatározott intézkedéseket. Különösen ezeket a kockázatokat emeljük ki: az európai kiberpajzs működése és fenntarthatósága függővé válhat az uniós finanszírozástól; a pajzs működését akadályozhatja az információmegosztás hiánya; a javaslat által bevezetett intézkedések összetettebbé tehetik az uniós kiberbiztonsági galaxis egészét.

43 A jogalkotási javaslat felülvizsgálatának eredményeként javasoljuk, hogy **a Bizottság és a jogalkotók mérlegeljék a következőket:**

— a javasolt intézkedések kidolgozásával és végrehajtásával kapcsolatos költségbecslések hozzáférhetővé tétele az átláthatóság növelése érdekében (lásd: ***10***. bekezdés);

— annak tisztázása, hogyan működjenek együtt a nemzeti SOC központok, a határokon átnyúló SOC központok és a CSIRT csoportok hálózata azáltal, hogy egyértelmű irányítási szabályokat és felelősségi köröket határoznak meg az eredményes koordináció biztosítása és a szinergiák elérése érdekében (***20***. bekezdés);

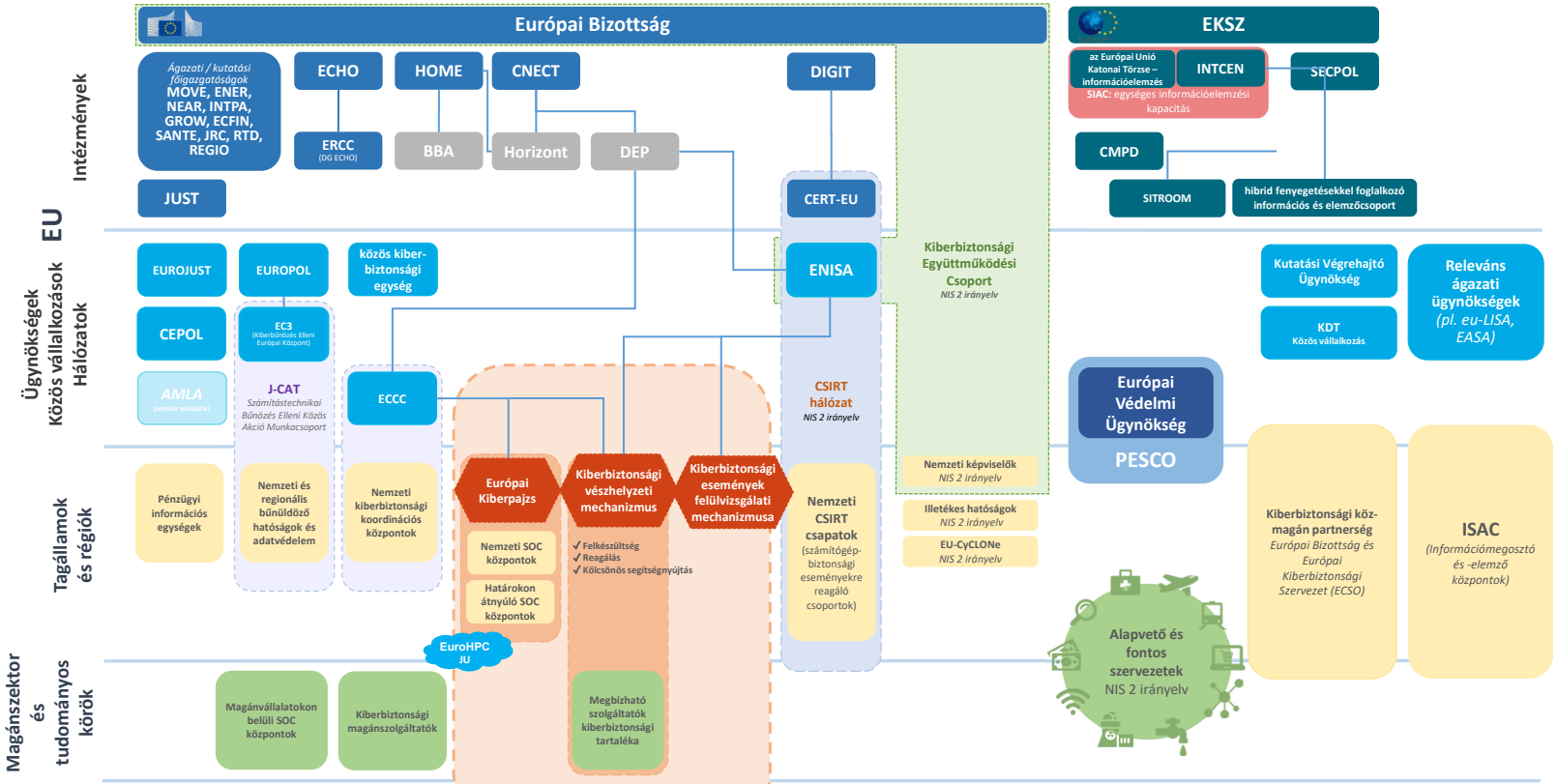
— annak biztosítása, hogy a kiberbiztonsági tartalék nyújtotta támogatási szolgáltatás iránti megkeresés és a Bizottság válasza közötti időbeli eltérés ne legyen túl nagy a megkeresés időzítése miatt (***29***. bekezdés);

— az évenkéntiség elvétől való eltérésnek a válaszintézkedésekre és a kölcsönös segítségnyújtásra való korlátozása, és annak egyértelművé tétele, hogy a fel nem használt kötelezettségvállalások automatikus átvitele a következő évre korlátozódik (***32***–***34***. bekezdés);

— legkésőbbi határidő meghatározása az egyes eseményeket követő ENISA-jelentések benyújtására annak biztosítására, hogy a kellő időben sor kerüljön visszajelzésre (***36***. bekezdés);

— a rendelet értékeléséről és felülvizsgálatáról szóló jelentés Bizottság általi benyújtására vonatkozó határidő előrehozatala (***40***. bekezdés).

Melléklet. Az európai kiberbiztonsági galaxis

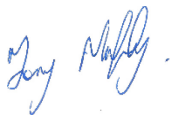


Forrás: Európai Számvevőszék.

AMLA: Pénzmosás Elleni Hatóság
CEPOL: Az Európai Unió Bűnüldözési Képzési Ügynöksége
CMPD: Válságkezelési és Tervezési Igazgatóság
DG CONNECT: A Tartalmak, Technológiák és Kommunikációs Hálózatok Főigazgatósága
DG ECFIN: Gazdasági és Pénzügyi Főigazgatóság
DG ECHO: Az Európai Polgári Védelem és Humanitárius Segítségnyújtási Műveletek Főigazgatósága
DG ENER: Energiaügyi Főigazgatóság
DG GROW: Belső Piaci, Ipar-, Vállalkozás- és Kkv-politikai Főigazgatóság
DG HOME: Migrációügyi és Uniós Belügyi Főigazgatóság
DG INTPA: A Nemzetközi Partnerségek Főigazgatósága
DG JUST: Jogérvényesülési és Fogyasztópolitikai Főigazgatóság
DG MOVE: Mobilitáspolitikai és Közlekedési Főigazgatóság
DG NEAR: Az Európai Szomszédságpolitika és a Csatlakozási Tárgyalások Főigazgatósága
DG REGIO: Regionális és Várospolitikai Főigazgatóság
DG RTD: Kutatási és Innovációs Főigazgatóság
DG SANTE: Egészségügyi és Élelmiszerbiztonsági Főigazgatóság
DIGIT: Informatikai Főigazgatóság
EASA: Az Európai Unió Repülésbiztonsági Ügynöksége
EC3: az Europol Kiberbűnözés Elleni Európai Központja
ECCC: Európai Kiberbiztonsági Kompetenciaközpont
ECSO: Európai Kiberbiztonsági Szervezet
EDA: Európai Védelmi Ügynökség
EKSZ: Európai Külügyi Szolgálat
ERCC: Veszélyhelyzet-reagálási Koordinációs Központ
EU-CyCLONe: az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózata
EuroHPC: Európai Nagy Teljesítményű Számítástechnika
EUROJUST: Az Európai Unió Büntető Igazságügyi Együttműködési Ügynöksége
EUROPOL: A Bűnüldözési Együttműködés Európai Uniós Ügynöksége
INTCEN: az Európai Unió Helyzetelemző Központja
BBA: Belső Biztonsági Alap
JRC: Közös Kutatóközpont
KDT: Kulcsfontosságú Digitális Technológiák
NIS-irányelv: Hálózat- és információbiztonsági irányelv
PESCO: állandó strukturált együttműködési keret
SECPOL: Biztonságpolitika és Konfliktusmegelőzés
SITROOM: helyzetelemző központ
SOC: biztonsági műveleti központ

A jelentést 2023. szeptember 26-i luxembourgi ülésén fogadta el a Bettina Jakobsen számvevőszéki tag elnökölte III. Kamara.

a Számvevőszék nevében



Tony Murphy elnök

SZERZŐI JOGOK