HU 2022

05

Különjelentés

Az uniós intézmények, szervek és ügynökségek kiberbiztonsága:

a felkészültség szintje összességében nem áll arányban a fenyegetésekkel

EURÓPAI SZÁMVEVŐSZÉK

Tartalomjegyzék

Mellékletek

Összefoglaló

I Az uniós kiberbiztonsági jogszabályban foglalt fogalommeghatározás szerint a kiberbiztonság azoknak a tevékenységeknek az összessége, „amelyek a kiberfenyegetésekkel érintett hálózati és információs rendszereknek, az ilyen rendszerek felhasználóinak és más személyeknek a védelméhez szükségesek”. Az általuk kezelt érzékeny információk miatt az uniós intézmények, szervek és ügynökségek (a továbbiakban: uniós szervek) vonzó célpontok a potenciális támadók és különösen azon csoportok számára, amelyek kiberkémkedési és egyéb célokból képesek rendkívül kifinomult lopakodó támadásokat végrehajtani. Intézményi függetlenségük és igazgatási autonómiájuk ellenére az uniós szervek szoros kapcsolatban állnak egymással. Így az egyes uniós szervek gyengeségei más uniós szerveket is biztonsági fenyegetéseknek tehetnek ki.

II Tekintettel arra, hogy az uniós szerveket célzó kibertámadások száma meredeken emelkedik, ellenőrzésünk célja annak megállapítása, hogy az uniós szervek összességében megfelelő intézkedéseket vezettek-e be a kiberfenyegetések elleni védelmük érdekében. Megállapítottuk, hogy az uniós szervek kiberfelkészültsége összességében nem arányos a fenyegetések mértékével.

III Úgy találtuk, hogy a legfontosabb kiberbiztonsági bevált gyakorlatok (ideértve bizonyos alapvető kontrollokat is) végrehajtására nem minden esetben került sor, és néhány uniós szerv nyilvánvalóan túlságosan keveset költ a kiberbiztonságra. Bizonyos uniós szerveknél a kiberbiztonsági irányítás sem megbízható: az informatikai biztonsági stratégiák sok esetben hiányoznak vagy azokat a felsővezetés nem hagyta jóvá, a biztonsági szabályzatok nem minden esetben öltenek hivatalos formát, a kockázatértékelések pedig nem vizsgálják a teljes informatikai környezetet. Nem mindegyik uniós szerv veti alá rendszeres független ellenőrzésnek kiberbiztonsági intézkedéseit.

IV Nem minden esetben kerül sor szisztematikusan kiberbiztonsági képzésekre. Az uniós szervek alig több mint fele kínál folyamatosan kiberbiztonsági képzéseket informatikai alkalmazottainak és informatikai biztonsági szakembereinek. Kevés uniós szerv nyújt kötelező kiberbiztonsági képzést az érzékeny információkat tartalmazó informatikai rendszerekért felelős vezetők számára. Az adathalászati gyakorlatok a személyzet képzésének és a figyelemfelkeltésnek fontos eszközei, azonban nem mindegyik uniós szerv él módszeresen ezzel a lehetőséggel.

V Jóllehet az uniós szervek bevezettek a kiberbiztonsággal kapcsolatos együttműködésre és információcserére szolgáló struktúrákat, megállapítottuk, hogy a lehetséges szinergiákat nem használják ki teljes mértékben. Az uniós szervek nem osztják meg egymással szisztematikusan a kiberbiztonsági projektekre, biztonsági értékelésekre és szolgáltatási szerződésekre vonatkozó információkat. Emellett az alapvető kommunikációs eszközök – például a titkosított e-mailek és videokonferencia-eszközök – nem teljes mértékben interoperábilisak, ami kevésbé biztonságos információcseréhez, párhuzamos munkavégzéshez és megnövekedett költségekhez vezethet.

VI Az európai intézmények, szervek és hivatalok hálózatbiztonsági vészhelyzeteket elhárító csoportja (CERT-EU) és az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) az a két fő szervezet, amelyek feladata az uniós szervek támogatása a kiberbiztonság terén. Az erőforrások korlátozottsága vagy más területek előnyben részesítése miatt azonban a CERT-EU és az ENISA nem volt képes az uniós szerveknek megadni mindazt a támogatást, amelyre szükségük van, különös tekintettel a kevésbé fejlett uniós szervek kapacitásépítésére. Jóllehet a CERT-EU-t nagyon méltányolják az uniós szervek, eredményességét veszélyezteti a növekvő munkaterhelés, a bizonytalan finanszírozás és személyi állomány, valamint egyes uniós szervek passzivitása, amelyek nem osztják meg mindig kellő időben az általuk elszenvedett, potenciálisan más szereplőket is fenyegető sebezhetőségekkel és jelentős kiberbiztonsági eseményekkel kapcsolatos információkat.

VII E következtetések alapján az alábbiakat javasoljuk:

- a Bizottság egy valamennyi uniós szervre nézve kötelező, közös kiberbiztonsági szabályokat megállapító jogszabályjavaslat és a CERT-EU forrásainak növelése révén javítsa az uniós szervek kiberbiztonsági felkészültségét;

- a Bizottság a digitális transzformációval foglalkozó intézményközi bizottságon keresztül igyekezzen bizonyos kiválasztott területeken még több szinergiát kihasználni az uniós szervek között;

- a CERT-EU és az ENISA fordítson több figyelmet azokra az uniós szervekre, amelyek a kiberbiztonság terén kevésbé fejlettek.

Bevezetés

Mi a kiberbiztonság?

01 Az uniós kiberbiztonsági jogszabályban[1] foglalt fogalommeghatározás szerint a kiberbiztonság azoknak a tevékenységeknek az összessége, „amelyek a kiberfenyegetésekkel érintett hálózati és információs rendszereknek, az ilyen rendszerek felhasználóinak és más személyeknek a védelméhez szükségesek”. A kiberbiztonság az információbiztonságon alapul, amely a (fizikai vagy elektronikus formátumú) információk bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzését jelenti[2]. Ezen túlmenően az ilyen információk tárolására szolgáló hálózati és információs rendszerek védelmét informatikai (IT-) biztonságnak nevezzük (lásd: ***1. ábra***).

1. ábra. A kiberbiztonság összefügg az információbiztonsággal és az informatikai biztonsággal

Forrás: Európai Számvevőszék.

02 A kiberbiztonság mint szakterület a kiberbiztonsági események azonosítását, megelőzését, felderítését, az azokra való reagálást és a helyreállítást foglalja magában. Kiberbiztonsági eseménynek minősül többek között az információk szándékolatlan nyilvánosságra hozatala, a kritikus infrastruktúrák veszélyeztetését célzó támadás vagy a személyazonosság és személyes adatok ellopása[3].

---

[1] Az (EU) 2019/881 rendelet.

[2] ISO/IEC 27 000:2018.

[3] Európai Számvevőszék, 2/2019. sz. áttekintés: Az eredményes uniós kiberbiztonsági politika előtt álló kihívások (tájékoztató).

03 A kiberbiztonsági keretrendszer számos elemet tartalmaz, többek között a hálózatok és az információs rendszerek biztonságára vonatkozó követelményeket és technikai kontrollokat, valamint megfelelő irányítási intézkedéseket és az alkalmazottaknak biztosított, a kiberbiztonsági tudatosság fokozását célzó képzéseket.

Az uniós intézmények, szervek és ügynökségek kiberbiztonsága

04 Az általuk kezelt érzékeny információk miatt az uniós intézmények, szervek és ügynökségek (a továbbiakban: uniós szervek) vonzó célpontok a potenciális támadók és különösen azon csoportok számára, amelyek kiberkémkedési és egyéb célokból képesek rendkívül kifinomult lopakodó támadásokat („magas szintű állandó fenyegetés”) végrehajtani[4]. Az uniós szervekkel szembeni sikeres kibertámadásoknak potenciálisan súlyos következményei lehetnek, árthatnak az Unió általános megítélésének, és aláásható az intézményekbe vetett bizalmat.

05 A Covid19-világjárvány hatására az uniós szervek – világszerte sok más szervezethez hasonlóan – arra kényszerültek, hogy hirtelen felgyorsítsák a digitális átállást és bevezessék a távmunkát. Ez jelentősen megnövelte a támadók számára potenciális hozzáférést adó pontok számát (az úgynevezett „támadási felületet”), mivel a szervezetek határait kiterjesztette az internetre csatlakoztatott otthonokra és mobileszközökre is, ami azt jelenti, hogy a támadók új sebezhetőségeket tudnak kihasználni. Az uniós szerveket magas szintű állandó fenyegetésnek kitevő csoportok leggyakrabban a távoli hozzáférési szolgáltatásokat használják fel arra, hogy első lépésben hozzáférést szerezzenek az uniós szervek hálózataihoz[5].

06 A kiberbiztonsági események száma egyre nő, és különösen aggasztó tendencia az uniós szerveket érintő jelentős biztonsági események drámai mértékű – 2021-ben minden eddigi szintet meghaladó – növekedése[6]. Jelentősnek minősül minden olyan esemény, amely nem ismétlődő vagy alapvető jellegű. Ezeknél jellemzően új módszereket és technológiákat alkalmaznak, így a kivizsgálás és a helyreállítás hetekbe vagy akár hónapokba telhet. A 2018 és 2021 közötti időszakban a jelentős biztonsági események száma több mint tízszeresére nőtt[7]. Csupán az elmúlt két évben legalább

---

[4] CERT-EU, *Threat Landscape Report*, 2021. június.

[5] Ugyanott.

[6] Ugyanott.

[7] Ugyanott.

22 különböző uniós szervnél következett be jelentős biztonsági esemény. Az egyik közelmúltbeli példa erre az Európai Gyógyszerügynökség elleni kibertámadás, amelynek során érzékeny adatokat szivárogtattak ki és manipuláltak oly módon, hogy az aláássa az oltásokba vetett bizalmat[8].

07 Az uniós szervek igen heterogén csoportot alkotnak, amely intézményekből, ügynökségekből és nagyszámú különböző szervből áll. A hét uniós intézményt a Szerződések hozták létre. Az Unió decentralizált ügynökségeit és egyéb szerveit ezzel szemben másodlagos jogi aktusok hozták létre, és mindegyikük különálló jogi személynek tekintendő. Az ügynökségek jogi szempontból különböző típusokba tartoznak: hat közülük bizottsági végrehajtó ügynökség, a többi 37 pedig decentralizált uniós ügynökség[9]. Az uniós szervek közé tartoznak továbbá az uniós hivatalok, egy diplomáciai testület (az Európai Külügyi Szolgálat), valamint a közös vállalkozások és egyéb szervek. Az uniós szervek mindegyike maga felelős saját kiberbiztonsági előírásainak meghatározásáért és biztonsági intézkedéseinek végrehajtásáért.

08 Az uniós szervek kiberbiztonságának megerősítése érdekében a Bizottság 2012-ben létrehozta az európai intézmények, szervek és hivatalok hálózatbiztonsági vészhelyzeteket elhárító csoportját (CERT-EU), amely állandó munkacsoportnak minősül. A CERT-EU a kiberbiztonsági információk cseréjét és az incidensekre való reagálást koordináló központként funkcionál az uniós szervek számára, együttműködve a tagállamok számítógépes biztonsági incidensekre reagáló egyéb csoportjaival (CSIRT) és az informatikai biztonságra szakosodott vállalatokkal. A CERT-EU szervezetét és működését jelenleg az általa kiszolgált uniós szervekkel, más néven „védett szervezetekkel" kötött 2018. évi intézményközi megállapodás[10] szabályozza. Jelenleg 87 védett szervezet van.

09 Az uniós szervek támogatásában kulcsszerepet játszik továbbá az Európai Uniós Kiberbiztonsági Ügynökség (ENISA), amelynek feladata, hogy az Unió egész területén magas szintű kiberbiztonságot biztosítson. A 2004-ben létrehozott ENISA célkitűzése az információs és kommunikációs technológiai (IKT) termékek, folyamatok és szolgáltatások megbízhatóságának fokozása kiberbiztonsági tanúsítási rendszerek alkalmazásával, az uniós szervekkel és a tagállamokkal folytatott együttműködés, valamint az uniós szervek és a tagállamok kiberfenyegetésekre való felkészülésének

---

[8] *Cyberattack on EMA – update 6*, 2021.01.25.

[9] A Számvevőszék 22/2020. sz. különjelentése: „Az uniós ügynökségek jövője – A nagyobb rugalmasság és a szorosabb együttműködés lehetőségei" (1. bekezdés).

[10] HL C 12., 2018.1.13., 1. o.

segítése. Az ENISA támogatja az uniós szerveket a kapacitásépítésben és az operatív együttműködésben.

10 Intézményi függetlenségük ellenére az uniós szervek szoros kapcsolatban állnak egymással. Napi rendszerességgel közölnek egymással információkat, és több közös rendszert és hálózatot használnak. Az egyes uniós szervek gyengeségei más uniós szerveket is kitehetnek biztonsági fenyegetéseknek, tekintettel arra, hogy a kibertámadók sok esetben több lépésben érik el céljukat, illetve jutnak el végső célpontjukhoz[11]. Egy gyengébb uniós szerv elleni sikeres támadás adott esetben más uniós szervek elleni támadások előkészítése lehet. Az uniós szervek emellett más tagállami köz- és magánszervezetekkel is kapcsolatban állnak, és ha nem kellőképpen felkészültek a kibertámadásokkal szemben, ezeket is kiberfenyegetéseknek tehetik ki.

11 Jelenleg nincs hatályban olyan jogi keret, amely az uniós szervek információbiztonságát és kiberbiztonságát szabályozná. Az uniós szervekre nem terjed ki sem a kiberbiztonságra vonatkozó legáltalánosabb uniós jogszabálynak (a 2016. évi hálózat- és információbiztonsági (NIS) irányelvnek[12]), sem pedig javasolt felülvizsgált változatának (NIS2)[13] a hatálya. Arról sem áll rendelkezésre átfogó információ, hogy az uniós szervek mekkora összegeket költenek a kiberbiztonságra.

12 2020 júliusában a Bizottság közleményt tett közzé a biztonsági unióra vonatkozó, a 2020 és 2025 közötti időszakra érvényes uniós stratégiáról[14]. A legfőbb intézkedések közé tartozik a „valamennyi uniós szerv által alkalmazandó, az információbiztonságra és a kiberbiztonságra vonatkozó közös szabályok meghatározása”. Az új keretnek elő kell segítenie az erős és hatékony operatív együttműködést, amelynek középpontjában CERT-EU áll. Az Unió digitális évtizedre szóló kiberbiztonsági stratégiájáról szóló dokumentumban[15], amelyet 2020 decemberében tettek közzé, a Bizottság vállalta, hogy az összes uniós szervre vonatkozó közös kiberbiztonsági szabályokról szóló rendeletre tesz javaslatot. Javasolta továbbá a CERT-EU új jogalapjának létrehozását a szervezet megbízatásának és finanszírozásának megerősítése érdekében.

---

[11] ENISA, Threat Landscape 2020*, Sectoral/thematic threat analysis*.

[12] (EU) 2016/1148 irányelv a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.

[13] Javaslat az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről szóló irányelvről.

[14] COM(2020) 605 final.

[15] JOIN(2020) 18 final.

Az ellenőrzés hatóköre és módszere

13 Tekintettel arra, hogy a kibertámadások száma meredeken emelkedik, és hogy egy uniós szerv gyengeségei más uniós szerveket is biztonsági fenyegetéseknek tehetnek ki, ellenőrzésünk célja annak megállapítása volt, hogy az uniós szervek összességében megfelelő intézkedéseket vezettek-e be a kiberfenyegetésekkel szembeni védelmük érdekében. E fő ellenőrzési kérdés megválaszolásához az alábbi három alkérdést vizsgáltuk:

1) Valamennyi uniós szerv alkalmaz alapvető kiberbiztonsági gyakorlatokat?

2) A kiberbiztonság terén hatékony együttműködés zajlik az uniós szervek között?

3) Az ENISA és a CERT-EU megfelelő támogatást nyújt az uniós szervek számára a kiberbiztonság terén?

14 Az ellenőrzés időzítését a biztonsági unióra vonatkozó uniós stratégiához igazítottuk. Az uniós szervek jelenlegi kiberbiztonsági intézkedéseinek értékelésével az a célunk, hogy feltárjuk azokat a területeket, ahol fejlesztésre van szükség, és amelyeket a Bizottság figyelembe vehet az összes uniós szervre nézve kötelező, közös kiberbiztonsági szabályokra irányuló jogalkotási javaslat kidolgozásakor.

15 Az ellenőrzés a kiberbiztonság terén a 2018. január (a CERT-EU intézményközi megállapodásának időpontja) és 2021. október közötti időszakban bekövetkezett fejleményekre és kezdeményezésekre terjedt ki.

16 Az ellenőrzés hatókörét a kiberrezilienciára és a nem minősített rendszerekre korlátoztuk. Figyelmünket a felkészültség aspektusaira (az azonosításhoz, védelemhez és felderítéshez kapcsolódó tevékenységekre) összpontosítottuk. A reagálás és a helyreállítás nem tartozott ellenőrzésünk hatókörébe. Megvizsgáltuk azonban a biztonsági eseményekre való reagálás bizonyos szervezeti elemeit. Az adatvédelem, a bűnüldözés, a kibervédelem és a kiberdiplomáciai aspektusok szintén kívül estek ellenőrzésünk hatókörén (lásd: ***2. ábra***).

2. ábra. Az ellenőrzés hatóköre

** A biztonsági eseményekre való reagálás bizonyos szervezeti elemei közül csak néhányat vizsgáltunk. A többi aspektus nem tartozott a vizsgálat hatókörébe.*

Forrás: Európai Számvevőszék.

17 Ellenőrzésünk megállapításai a hozzáférhető dokumentumok átfogó elemzésén alapultak, amelyet interjúkkal egészítettünk ki. Hatvanöt uniós szerv bevonásával végeztünk önértékelésen alapuló felmérést azzal a céllal, hogy információkat gyűjtsünk kiberbiztonsági intézkedéseikről, valamint az intézményközi együttműködéssel kapcsolatos meglátásaikról. Megvizsgáltuk az összes olyan uniós szervet, amelyek fölött a Számvevőszék ellenőrzési jogokkal rendelkezik és amelyek maguk kezelik informatikai infrastruktúrájukat, továbbá górcső alá vettük saját intézményünket is. Ez a csoport intézményeket, decentralizált ügynökségeket, közös vállalkozásokat és egyéb szerveket is magában foglalt. Megkérdeztünk továbbá polgári missziókat is, amelyek az uniós költségvetéséből finanszírozott, informatikai szempontból független, ideiglenes autonóm egységek. A felmérésben részt vevő uniós szervek teljes listáját az ***I. melléklet*** tartalmazza. Az ellenőrzés nem terjedt ki az európai ombudsmanra és az európai adatvédelmi biztosra.

18 A felmérés során a válaszadási arány 100%-os volt; a felmérés a további elemzések kiindulópontjaként szolgált. Emellett kiválasztottunk egy hét uniós szervből álló, az uniós szervek heterogenitására nézve reprezentatív mintát, és válaszaik nyomán interjúkat készítettünk velük és dokumentumokat kértünk be tőlük.
A kiválasztás során kritériumként vettük figyelembe a jogalapot, a méretet (a személyi állomány és a költségvetés tekintetében) és az ágazatot. A mintába felvett uniós szervek a következők voltak: Európai Bizottság, Európai Parlament, Európai Uniós

Kiberbiztonsági Ügynökség (ENISA), Európai Bankhatóság (EBH), Európai Tengerészeti Biztonsági Ügynökség (EMSA), az Európai Unió ukrajnai tanácsadó missziója (EUAM Ukrajna) és az Innovatív Gyógyszerek Kezdeményezés közös vállalkozás (IMI JU).

19 Emellett videomegbeszéléseket folytattunk a CERT-EU-val, az Uniós Ügynökségek Hálózatának IKT tanácsadó bizottságával (ICTAC), a digitális transzformációval foglalkozó intézményközi bizottsággal (ICDT) és más érintettekkel.

Észrevételek

Az uniós szervek kiberbiztonsági fejlettségi szintje eltérő, és nem mindig alkalmazzák a bevált gyakorlatokat

20 Az alábbi szakasz az uniós szervek egyedi intézkedéseit és kiberbiztonsági kereteit vizsgálja. Értékeltük, hogy az informatikai biztonsági irányítás, a kockázatkezelés, az erőforrások elosztása, a tudatosság fokozását szolgáló képzések, a kontrollok és a független biztosítékok szempontjából egységesen és megfelelően közelítik-e meg a kiberbiztonság kérdését.

Az uniós szervek informatikai biztonsági irányítása sok esetben nem kellően fejlett, és a kockázatértékelés nem átfogó

Számos uniós szervnél hiányosságok figyelhetők meg az informatikai biztonsági irányítás terén

21 A jó irányítás az információs és informatikai rendszerek biztonságát szolgáló eredményes keret kulcsfontosságú eleme, mivel meghatározza a szervezet célkitűzéseit, valamint a prioritások meghatározása és a döntéshozatal útján felvázolja a haladás irányát is. Az Információrendszer-ellenőrök Egyesülete (ISACA)[16] szerint egy informatikai biztonsági irányítási keretnek általában a következő elemeket kell magában foglalnia:

- átfogó biztonsági stratégia, amely szorosan kapcsolódik a vállalati célkitűzésekhez;
- irányadó biztonsági szabályzatok, amelyek a stratégia, a kontrollok és a szabályozás valamennyi aspektusát érintik;
- minden egyes szabályzat vonatkozásában teljes körű szabványok, amelyek leírják a szabályzatnak való megfeleléshez szükséges operatív lépéseket;
- intézményesített nyomonkövetési folyamatok, amelyek a megfelelés biztosítását és az eredményességgel kapcsolatos visszajelzést szolgálják;
- eredményes szervezeti struktúra, amelyben nincsenek összeférhetetlenségek.

[16] ISACA, *Certified Information System Auditor review manual*, 2019.

22 Az informatikai biztonsági irányítás terén számos uniós szervnél hiányosságokat tártunk fel. Az uniós szerveknek csupán 58%-a (a 65-ből 38) rendelkezik igazgatótanácsi/felsővezetői szinten jóváhagyott informatikai biztonsági stratégiával vagy legalább informatikai biztonsági tervvel. Ennek a számadatnak az uniós szerv típusa szerinti bontása azt mutatja, hogy a százalékos arányok a polgári missziók és a decentralizált ügynökségek (amelyek együttesen a felmérésben részt vevő uniós szervek 71%-át teszik ki) esetében a legalacsonyabbak (lásd: ***1. táblázat***). Ha nem áll rendelkezésre felsővezetői szinten jóváhagyott informatikai biztonsági stratégia vagy informatikai biztonsági terv, az azzal a kockázattal jár, hogy a felsővezetés nincs tudatában az informatikai biztonsági problémáknak, vagy nem megfelelően állítja fel a fontossági sorrendet.

1. táblázat. A felsővezetői szinten jóváhagyott informatikai biztonsági stratégiával vagy tervvel rendelkező uniós szervek százalékos aránya

Bontás a személyi állomány létszáma alapján

Személyi állomány létszáma: < 100 (22 uniós szerv)	Személyi állomány létszáma: 100–249 (17 uniós szerv)	Személyi állomány létszáma: 250–1000 (16 uniós szerv)	Személyi állomány létszáma: > 1000 (10 szerv)
45%	53%	69%	80%

Bontás az uniós szerv típusa alapján

Decentralizált ügynökségek (35 uniós szerv)	Polgári missziók (11 uniós szerv)	Egyéb szervek (4 uniós szerv)	Intézmények (6 uniós szerv)	Közös vállalkozások (9 uniós szerv)
45%	56%	75%	83%	89%

Forrás: Az Európai Számvevőszék felmérése.

23 Megvizsgáltuk a mintában szereplő hét uniós szerv által benyújtott informatikai biztonsági stratégiákat, illetve terveket (lásd: ***18***. bekezdés). Úgy találtuk, hogy az uniós szervek stratégiái észszerű mértékben kapcsolódnak a főtevékenységükkel kapcsolatos célkitűzésekhez. A Bizottság informatikai biztonsági stratégiája például az Európai Bizottság digitális stratégiájának[17] informatikai biztonsági dimenzióját foglalja magában, és annak ütemtervét és célkitűzéseit hivatott támogatni. Azonban a mintában szereplő uniós szervek közül csak három szerepeltetett konkrét

[17] Közlemény a Bizottságnak: „Az Európai Bizottság digitális stratégiája – Egy digitálisan átalakult, felhasználó-központú és adatvezérelt Bizottság”, C(2018) 7118 final, 2018.11.21.

célkitűzéseket, illetve az azok megvalósításához kapcsolódó menetrendeket informatikai biztonsági stratégiájában, illetve tervében.

24 A biztonsági szabályzatok határozzák meg azokat a szabályokat és eljárásokat, amelyeket az információkat és az informatikai erőforrásokat használó vagy kezelő személyek kötelesek betartani. E szabályzatok segítenek a kiberbiztonsági kockázatok enyhítésében, és tájékoztatást adnak arról, hogy mi a teendő biztonsági események bekövetkezésekor. Megállapítottuk, hogy az uniós szervek 78%-a rendelkezik hivatalos információbiztonsági szabályzattal, de csupán 60%-uk hivatalos informatikai biztonsági szabályozással (az információbiztonság és az informatikai biztonság fogalommeghatározását lásd: ***1. ábra***). Megállapítottuk továbbá, hogy a mintánkban szereplő hét uniós szerv közül négy rendelkezik olyan biztonsági szabályokkal, amelyek összhangban állnak informatikai biztonsági stratégiáikkal. Azonban e négy közül három esetében az informatikai biztonsági szabályzatokhoz csak részben tartoznak naprakész, részletes biztonsági szabványok, amelyek leírják a szabályzatok végrehajtásához szükséges operatív lépéseket. A hivatalos biztonsági szabványok hiánya növeli annak kockázatát, hogy az informatikai biztonsági problémákat adott esetben nem kezelik megfelelően és az adott uniós szerven belül egységes módon. Amellett ez megnehezíti annak felmérését is, hogy az adott szervezet mennyire tartja be saját informatikai biztonsági szabályzatát. A mintában szereplő hét uniós szerv közül csak a Bizottság rendelkezik strukturált eljárásokkal annak nyomon követésére, hogy megfelelően végrehajtja-e saját informatikai biztonsági szabályzatait és szabványait, de ezeket az eljárásokat ott is csak korlátozott számú főigazgatóság (DG) alkalmazza (lásd: ***1. háttérmagyarázat***).

1. háttérmagyarázat

Az informatikai biztonsági szabályok követése a Bizottságnál

A Bizottság decentralizált informatikai irányításának megfelelően az egyes főigazgatóságok vezetője a szolgáltatástulajdonos, és ő felel, illetve ő elszámoltatható azért, hogy a főigazgatóság rendszerei megfeleljenek az informatikai biztonsági szabványoknak. Az Informatikai Főigazgatóság (DG DIGIT) és a Humánerőforrásügyi és Biztonsági Főigazgatóság (DG HR) felügyeli és segíti a megfelelőség biztosítását és ellenőrzését célzó gyakorlatok végrehajtását. A DG DIGIT kidolgozott egy eszközt (az úgynevezett GRC-t), amely lehetővé teszi a főigazgatóságok számára, hogy mérjék az informatikai biztonsági szabályzatoknak való megfelelésüket, illetve beszámoljanak arról.

Az 580 kontroll három kategóriára tagozódik: általános kontrollok (ezek főként az irányítást érintik), főigazgatóság-specifikus kontrollok és rendszerspecifikus kontrollok. Az eszköz működik, de jelenleg csupán öt főigazgatóság használja. Ez azt jelenti, hogy a DG DIGIT nem látja át a megfelelőséget az egész Bizottságra kiterjedően. Ugyanakkor a Bizottság Informatikai és Kiberbiztonsági Tanácsa (ITCB) felkérheti a DG DIGIT-et egy adott szabványnak való megfelelés kivizsgálására (2021-ben például ilyen volt a többfaktoros hitelesítés), és nem kötelező érvényű véleményeket és ajánlásokat – illetve kritikus kockázatok esetében hivatalos követelményeket – adhat ki.

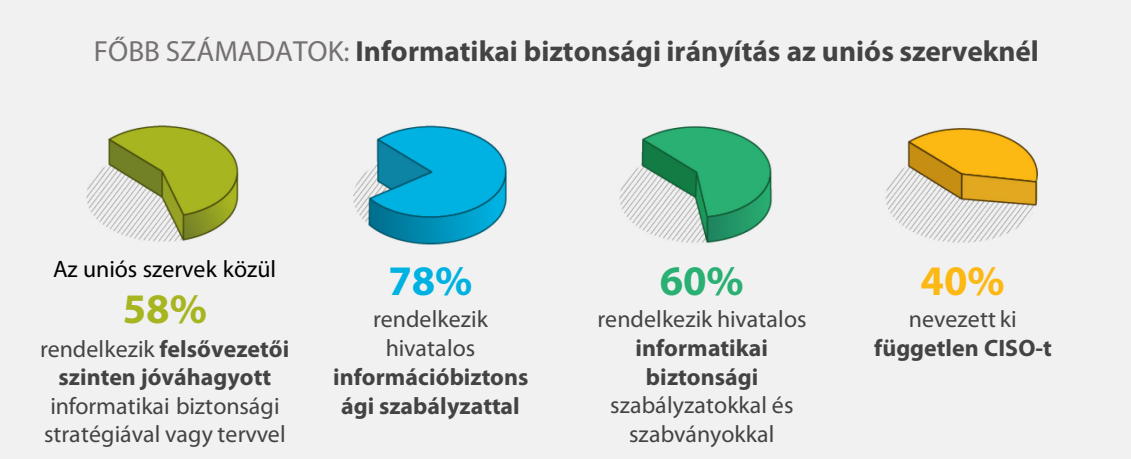
25 A jó kiberbiztonsági irányítás további fontos eleme az információbiztonsági vezető (CISO) kinevezése. Jóllehet az ISO 27 000 kategóriába tartozó szabványok[18] ezt nem írják elő kifejezetten, a CISO (vagy egyenértékű szerepet betöltő személy) alkalmazása széles körben elterjedt gyakorlat a szervezetekben, és az ISACA iránymutatásai is kitérnek rá. Jellemzően a CISO az, aki teljes körű felelősséggel tartozik az adott szervezet információbiztonsági és informatikai biztonsági programjaiért. Az összeférhetetlenség elkerülése érdekében a CISO-nak bizonyos mértékben függetlennek kell lennie az informatikai funkciótól/részlegtől[19].

26 Felmérésünk eredményei szerint az uniós szervek 60%-a nem jelölt ki független CISO-t vagy egyenértékű szerepet betöltő személyt. Még ha ki is neveztek CISO-t (vagy hasonlót), a különböző uniós szervek igen eltérő jellegű szerepet szánnak nekik, illetve funkcióikat is igen eltérően értelmezik. Különösen a kis és közepes méretű uniós szerveknél figyelhető meg, hogy a CISO-k feladata jellemzően az operatívabb jellegű szerepkörökhöz kapcsolódik, és a CISO-k funkcionálisan nem függetlenek az

[18] A 27 000:2018 ISO/IEC szabvány, 5. fejezet.

[19] *COBIT 5 for Information Security*, 4.2. szakasz.

informatikai részlegtől.
Ez korlátozhatja a CISO autonómiáját a biztonsági prioritások érvényesítése terén. Az ENISA jelenleg dolgozik a kiberbiztonsági készségek uniós keretének kidolgozásán, amelynek célja többek között a szerepek, a hatáskörök és a készségek egységes értelmezésének biztosítása.



Az esetek többségében az uniós szervek biztonsági kockázati értékelései nem terjednek ki informatikai környezetük egészére

27 Az informatikai biztonságra vonatkozó valamennyi nemzetközi szabvány hangsúlyozza az informatikai rendszereket és az azokban tárolt adatokat érintő biztonsági kockázatok kiértékelésére és kezelésére szolgáló megfelelő módszer kidolgozásának fontosságát. Ezeket a kockázatértékeléseket a szervezet információbiztonsági követelményeiben, továbbá a szervezetet érintő kockázatokban bekövetkezett változások figyelembevétele érdekében rendszeresen el kell végezni[20]. Az értékelés nyomán kockázatenyhítési tervet (vagy informatikai biztonsági tervet) kell készíteni.

28 A felmérésben részt vevő uniós szervek többsége (65-ből 58) jelezte, hogy az informatikai rendszereiken végzett kockázatértékelések során egy bizonyos keretrendszert vagy módszertant követnek. Az uniós szervek azonban nem rendelkeznek közös módszertannal. Legalább 26 uniós szerv részben vagy egészben a Bizottság által kidolgozott módszertanokat használja; ezen belül az uniós szervek 31%-a az informatikai biztonsági kockázatok kezelését szolgáló 2018. évi módszertant (ITSRM2) alkalmazza. A többiek ismert ágazati szabványokon – például az ISO27001 vagy ISO27005 szabványon, a Nemzeti Szabványügyi és Technológiai Hivatal (National Institute of Standards and Technology) kiberbiztonsági keretrendszerén (NIST-CSF)

[20] Lásd például: ISO/IEC 27 000:2018, 4.5. szakasz.

vagy az Internetbiztonsági Központ (Center for Internet Security, CIS) kontrolljain – alapuló módszereket követnek, vagy egyéb belső módszertanokat alkalmaznak.

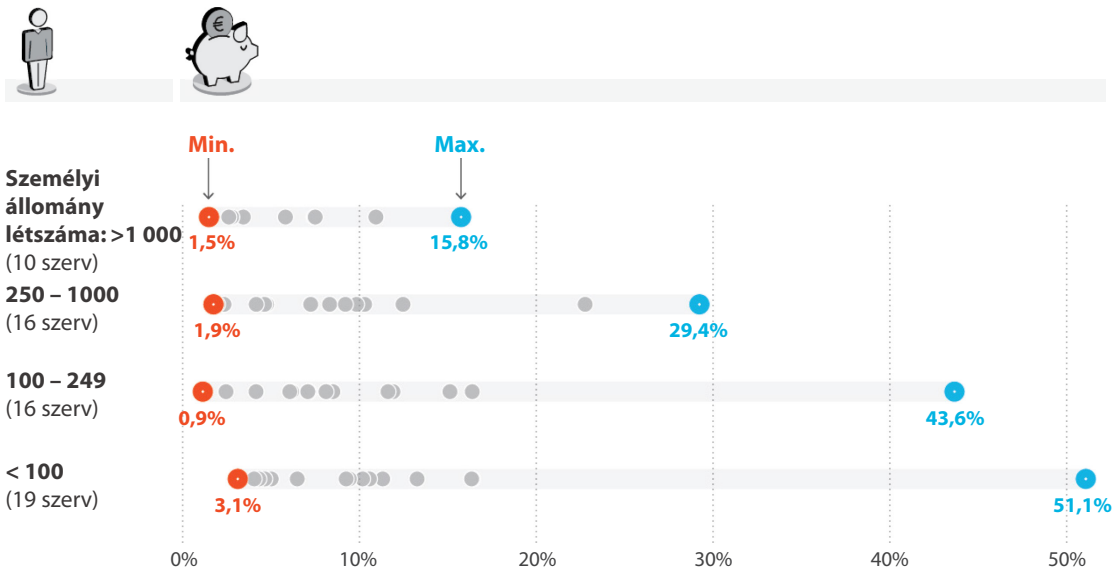
29 A mintában szereplő hét uniós szerv közül csupán kettő végez olyan átfogó kockázatértékeléseket, amelyek az informatikai környezet egészére (vagyis valamennyi informatikai rendszerükre) kiterjednek. A legtöbb uniós szerv csak a legfontosabb informatikai rendszerein végez egyedi kockázatértékelést. Több példát is találtunk arra, hogy új rendszerek bevezetése előtt kockázatértékelésre került sor. Nem találtunk viszont arra mutató bizonyítékot, hogy később nyomon követési célú kockázatértékelésekre is sor került volna például a rendszerek/infrastruktúra későbbi módosításaihoz kapcsolódóan.

Az uniós szervek nem egységesen közelítik meg a kiberbiztonság kérdését, és sok esetben az alapvető kontrollokat sem hajtják végre

Az uniós szervek körében nagyban különböznek a kiberbiztonsági célokra előirányzott összegek

30 A felmérés során felkértük az uniós szerveket: ismertessék, hogy 2020-ban mekkora volt a teljes informatikai kiadásuk, illetve hogy ezen belül körülbelül mennyit költöttek a kiberbiztonságra. Az adatok azt mutatják, hogy jelentős különbségek vannak az uniós szervek között abban a tekintetben, hogy informatikai kiadásaiknak hány százalékát fordítják a kiberbiztonságra. Ez a jelenség a személyi állomány létszámát tekintve azonos méretű uniós szervek esetében is megfigyelhető. Ahogy a ***3. ábra*** is mutatja, e különbségek főként a kisebb létszámú személyzettel működő uniós szervek esetében nagyok.

3. ábra. Kiberbiztonsági kiadások a teljes informatikai kiadások százalékában kifejezve (az uniós szervek a személyzet létszáma alapján csoportosítva)



Megjegyzés: Négy uniós szerv nem szolgáltatott adatokat a kiberbiztonsági kiadásairól.

Forrás: Az Európai Számvevőszék felmérése.

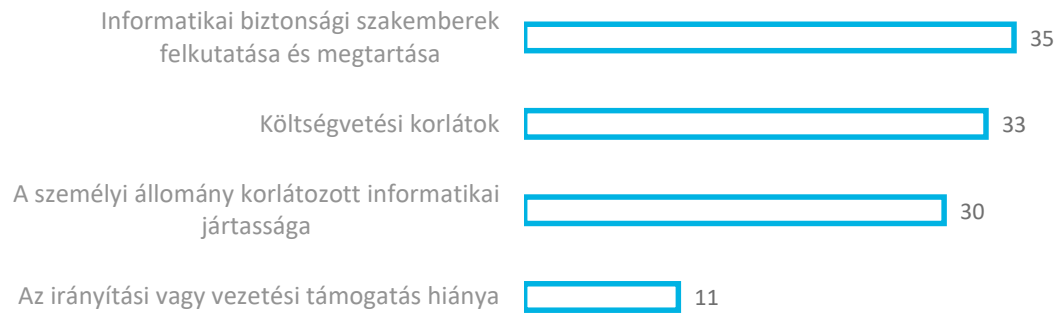
31 A kiberbiztonsági kiadások optimális szintjét nehéz abszolút értékben meghatározni. Számos tényezőtől függ: ilyen például az adott szervezet támadási felülete, az általa kezelt adatok érzékenysége, a szervezet kockázati profilja és hajlandósága, valamint az ágazati jogi és szabályozási követelmények összessége. Adataink azonban jelentős különbségekre világítanak rá, melyek okai nem minden esetben nyilvánvalóak. Néhány uniós szerv jóval kevesebbet költ a kiberbiztonságra, mint hasonló méretű társai, ami arra utalhat, hogy hasonló fenyegetettség és kockázatok esetén e kiadások szintje elmarad a kívánatostól.

32 A legtöbb uniós szerv kis- vagy közepes méretű, személyzeti állománya és informatikai kiadásai szempontjából egyaránt: az uniós szervek kétharmadánál a személyi állomány kevesebb mint 350 főből áll. A legkisebb uniós szerv személyzetének létszáma mindössze 15 fő. A kisebb uniós szervek számára a kiberbiztonsági kérdések kezelése nagyobb kihívást jelent, és magasabb az erőforrásigénye is. A legtöbb esetben nem tudják kihasználni a méretgazdaságosság előnyeit, és nem rendelkeznek megfelelő belső szakértelemmel. Felmérésünk és az interjúk alapján megállapítható, hogy a legnagyobb intézmények – például a Bizottság és az Európai Parlament – rendelkeznek olyan szakértői csoportokkal, melyek tagjai teljes munkaidőben a kiberbiztonsággal foglalkoznak. Azonban a kisebb uniós szerveknél, ahol a személyi állomány és az erőforrások különösen korlátozottak, egyáltalán nem dolgoznak

szakemberek, és a kiberbiztonsági kérdéseket a személyzet informatikai háttérrel rendelkező tagjai kezelik munkaidejük egy részében. Tekintettel arra, hogy az uniós szervek szoros kapcsolatban állnak egymással, ez fokozott veszélyt jelent (lásd még: ***10***. bekezdés).

33 Felmérésünkben megkérdeztük az uniós szerveket, melyek a legnagyobb kihívások, amelyekkel az eredményes kiberbiztonsági szabályzatoknak a szervezeteikben történő végrehajtása során szembesülnek (lásd: ***4. ábra***). A legnagyobb kihívást az jelenti, hogy kevés a kiberbiztonsági szakember, és – a magánszektorral és a többi uniós szervvel való verseny miatt – sok uniós szerv számára jelent nehézséget az ilyen szakemberek toborzása. Visszatérő problémát jelentenek az időigényes toborzási eljárások, a nem versenyképes szerződéses feltételek és a vonzó karrierlehetőségek hiánya. A kiberbiztonság kérdésének eredményes kezelésére nézve jelentős kockázatnak számít a szakértelemmel rendelkező személyzet hiánya.

4. ábra. Kihívások az eredményes kiberbiztonsági szabályzatok uniós szerveknél történő végrehajtása terén (több választ is meg lehetett jelölni)



Forrás: Az Európai Számvevőszék felmérése.

A legtöbb uniós szerv kínál kibertudatossági képzéseket, de ezek nem szisztematikusak és nem megfelelően célzottak

34 A potenciális támadók nem csupán a rendszerek és eszközök sebezhetőségének kihasználásával képesek kárt okozni. Adathalászattal vagy pszichológiai manipulációval (social engineering) a felhasználókat is rávehetik, hogy érzékeny információkat adjanak ki vagy rosszindulatú szoftvereket töltsenek le. Minden szervezet esetében a személyzet is az első védelmi vonalba tartozik. Ezért a kiberbiztonsággal kapcsolatos tudatosság növelését célzó és képzési programok az eredményes kiberbiztonsági keretrendszer kulcsfontosságú elemei.

35 A felmérésben részt vevő uniós szervek túlnyomó többsége (95%) nyújtott bizonyos formában a kiberbiztonsággal kapcsolatos tudatosság növelését célzó képzéseket a személyi állomány minden tagja számára: ezt mindössze három uniós szerv nem tette meg. Ugyanakkor az uniós szerveknek csak 41%-a szervez specifikus vagy tudatosságot növelő képzéseket a vezetők számára, és csak 29%-uk biztosít kötelező kiberbiztonsági képzést az érzékeny információkat tartalmazó informatikai rendszerekért felelős vezetők számára. Az eredményes kiberbiztonsági irányításnak elengedhetetlen feltétele a vezetők tudatossága és elkötelezettsége. Azon tizenegy uniós szerv közül, amely említést tett arról, hogy a vezetőség részéről érkező támogatás hiánya kihívást jelent az eredményes kiberbiztonság terén, csupán három nyújtott tudatosságnövelő képzést a vezetők számára bizonyos formában. Informatikai alkalmazottainak az uniós szervek 58%-a, informatikai biztonsági szakembereinek pedig azok 51%-a kínál folyamatosan kiberbiztonsági képzéseket.

36 Nem mindegyik uniós szerv rendelkezik olyan mechanizmusokkal, amelyek a személyi állomány kiberbiztonsági képzéseken való részvételének, valamint a tudatosságukban és viselkedésükben bekövetkezett változásoknak a nyomon követését szolgálja. Különösen a kisebb szervezeteknél figyelhető meg, hogy a kiberbiztonsággal kapcsolatos tudatosság növelését szolgáló képzésekre informális személyzeti értekezletek keretében is sor kerülhet. A szervezetek elsősorban úgy mérik a személyi állomány tagjainak a tudatosságát, hogy rendszeresen tesztelik viselkedésüket (többek között a fejlettséget vizsgáló felmérésekkel vagy adathalászati gyakorlatokkal). Az utóbbi öt évben az uniós szervek 55%-a szervezett egy vagy több szimulált adathalászati kampányt (vagy hasonló gyakorlatot). Tekintettel arra, hogy az adathalászat az egyik legkomolyabb fenyegetés a közigazgatásban dolgozók számára[21], az ilyen gyakorlatok fontos szerepet játszanak a személyi állomány képzésében és tudatosságának növelésében. Úgy találtuk, hogy a Bizottság által a kiberbiztonsággal kapcsolatos tudatosság terén végzett tevékenységek bevált gyakorlatnak tekinthetők, és más érdeklődő uniós szervek számára is hozzáférhetők (lásd: ***2. háttérmagyarázat***).

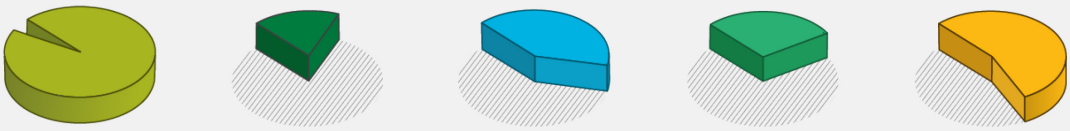
[21] ENISA, *Thread Landscape 2020, Sectoral/Thematic threat analysis*.

2. háttérmagyarázat

A kiberbiztonsággal kapcsolatos tudatosság növelését szolgáló képzések a Bizottságnál

A Bizottságnak a DG DIGIT-en belül van egy kifejezetten ezzel a területtel foglalkozó, „Cyber Aware” elnevezésű csoportja. Ez a csoport vezeti a kibertudatosság növelését szolgáló szervezeti programot. A programot a Humánerőforrásügyi és Biztonsági Főigazgatóság (DG HR), a Főtitkárság, A Tartalmak, Technológiák és Kommunikációs Hálózatok Főigazgatósága (DG CNECT) és a CERT-EU közösen irányítja és működteti. A képzés magas színvonalú, és sok esetben intézményközi szinten valósul meg. A képzési alkalmakról a „Learning Bulletin” című hírlevél ad tájékoztatást, amely mintegy 65 000 uniós munkavállalóhoz jut el. A „Cyber Aware” platform révén a Bizottság 15 adathalászati gyakorlatot szervezett az utóbbi öt évben, a közelmúltban pedig végrehajtotta az első olyan gyakorlatot, amely a Bizottság egészére kiterjedt.

FŐBB SZÁMADATOK: **Kibertudatossági képzések az uniós szerveknél**



95%
kínál **az általános tudatosság növelését célzó képzéseket** a személyi állomány számára

19%
nem tájékoztatja/képzi szisztematikusan az újonnan belépő dolgozókat

41%
kínál specifikus **képzést a vezetők számára**

2 %
biztosít **kötelező képzést** az érzékeny információkat tartalmazó IT rendszerekért felelős vezetők számára

55%
tesztelte személyi állománya tagjait **szimulált adathalászattal**

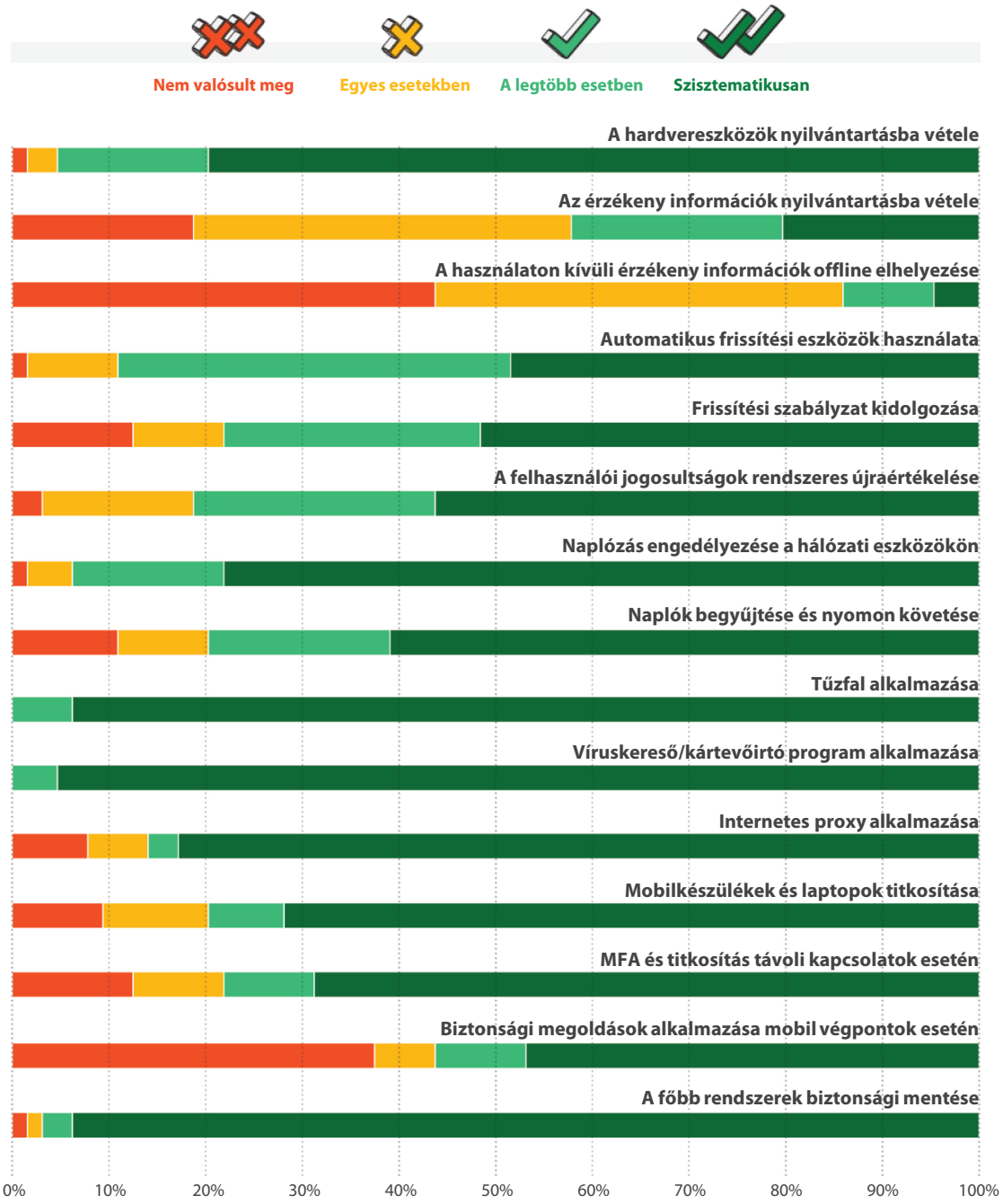
Az alapvető kontrollokat nem mindig hajtják végre vagy öntik hivatalos szabvány formájába

37 Felkértük az uniós szerveket arra, hogy bizonyos kiválasztott alapvető kontrollok alkalmazása kapcsán végezzenek önértékelést[22]. Olyan bevált gyakorlatokat választottunk ki, amelyeknek alkalmazására még a kisebb szervezetek is észszerű

[22] A bevált gyakorlatoknak az Internetbiztonsági Központ által összeállított kerete (CIS Controls 7.1) alapján meghatározott kontrollok.

keretek között képesek[23]. A mintákon kapott eredményeket az *5. ábra* mutatja be. A felmérésben részt vevő uniós szervek többsége bevezette a kiválasztott alapvető kontrollokat. Egyes területeken azonban a kontroll az uniós szervek legalább 20%-ánál láthatólag elégtelen vagy korlátozott.

5. ábra. Az alapvető kontrollok alkalmazása az uniós szerveknél (az önértékelés eredményei)



Forrás: Az Európai Számvevőszék felmérése.

[23] A CIS Controls 1. végrehajtási csoportja (IG1).

38 A mintában szereplő hét uniós szervtől minden olyan ellenőrzés kapcsán kikértük az alátámasztó dokumentumokat és szabványokat/szabályzatokat, amelyeket nyilatkoztuk szerint végrehajtottak. E dokumentumokat a kontrollok 62%-a esetében kaptuk meg. Amint kérdésünkre az interjúk során kiderült, számos esetben bár alkalmaztak technikai kontrollokat, azokat – ezidáig – nem formalizálták szabványok vagy előírások formájában, ami növeli annak kockázatát, hogy az informatikai biztonsági problémákat nem kezelik egységesen az egész uniós szerven belül (lásd még: ***24***. bekezdés).

Több uniós szerv nem veti alá rendszeres független ellenőrzésnek kiberbiztonsági intézkedéseit

39 Az ISACA[24] szerint a belső ellenőrzés a szervezetek három alapvető védelmi vonalának egyike (a másik kettő a vezetés és a kockázatkezelés). A belső ellenőrzések hozzájárulnak az információbiztonsági és informatikai biztonsági irányítás javításához. Megvizsgáltuk, hogy az uniós szervek milyen gyakorisággal vetik alá független ellenőrzésnek informatikai biztonsági keretrendszerüket belső vagy külső ellenőrzésekkel és kibervédelmi eszközeik proaktív tesztelésével.

40 A Bizottság Belső Ellenőrzési Szolgálata (IAS) feladatai közé tartozik a Bizottság, a decentralizált ügynökségek, a közös vállalkozások és az EKSZ informatikai ellenőrzése. A szolgálat megbízatása a felmérésünkben megkérdezett 65 uniós szerv közül 46-ra (70%) terjed ki. Az elmúlt öt évben az IAS hat különböző uniós szervnél végzett informatikai biztonsági ellenőrzést. Emellett a DG HR hatáskörébe tartozik a technikai információbiztonsági szempontokra kiterjedő informatikai biztonsági vizsgálatok elvégzése[25]. A többi uniós szerv közül hét számolt be arról, hogy rendelkezik informatikai szempontokra kiterjedő belső ellenőrzési funkcióval; tizenkét uniós szerv esetében a felmérésünkre adott válaszokból nem volt megállapítható, hogy rendelkeznek-e ilyen belső ellenőrzési kapacitással.

41 A független szervezetek által végzett külső informatikai biztonsági ellenőrzések további lehetőséget biztosítanak a független ellenőrzésre. Annak ellenére, hogy a kiberkörnyezet gyorsan változik, az uniós szervek 34%-ánál a 2015 kezdete és 2021 első negyedéve közötti időszakban sem belső, sem külső informatikai biztonsági ellenőrzésre nem került sor. E számadat uniós szervtípusok szerinti bontása azt

---

[24] ISACA, *Auditing Cyber Security: Evaluating Risk and Auditing Controls*, 2017.

[25] (EU) 2017/46 határozat az Európai Bizottság kommunikációs és információs rendszereinek biztonságáról.

mutatja, hogy 2015 óta az egyéb uniós szervek 75%-a, a közös vállalkozások 66%-a és a polgári missziók 45%-a nem esett át sem belső, sem külső informatikai biztonsági ellenőrzésen.

42 A belső és külső ellenőrzések mellett a szervezetek úgy is megbizonyosodhatnak informatikai biztonsági keretrendszerük működéséről, hogy a sebezhetőségek azonosítása érdekében proaktívan tesztelik kibervédelmüket. Ennek egyik módszere a behatolási tesztelés (más néven az etikus hackelés), amelynek során az egyes számítógépes rendszerek ellen szimulált, engedélyezett kibertámadásokat indítanak. Felmérésünkre adott válaszaikban az uniós szervek 69%-a nyilatkozott úgy, hogy az elmúlt öt évben legalább egyszer végzett behatolási tesztelést. Ezeknek az eseteknek a 45%-ában a behatolási tesztelést végző szervezet a CERT-EU volt.

43 Az úgynevezett red team (valósághű támadásszimulációs) gyakorlatok során szintén szimulált támadások útján tesztelik a kibervédelmet, és ehhez a tényleges közelmúltbeli támadások során alkalmazott technikákat használják. A behatolási teszteléshez képest ezek összetettebb és átfogóbb gyakorlatok, mivel több rendszerre és több potenciális támadási lehetőségre terjednek ki. Az uniós szervek ezeket a gyakorlatokat ritkábban végzik: az uniós szervek 46%-a nyilatkozott úgy, hogy az elmúlt öt évben legalább egyszer sor került red team gyakorlatra. Ezeknek 75%-át a CERT-EU végezte el. E gyakorlatok előkészítéséhez és végrehajtásához jelentős munkára van szükség, és a CERT-EU-nak jelenleg legfeljebb évi öt-hat gyakorlat végrehajtására van kapacitása.

44 A két közelmúltban létrehozott uniós szervet leszámítva a felmérésben részt vevő uniós szervek közül 16-nál (25%) az elmúlt öt évben nem került sor behatolási tesztelésre vagy red team gyakorlatra. Összességében hét uniós szerv (10%) – egy közös vállalkozás, egy decentralizált ügynökség és öt polgári misszió – semmilyen formában nem vetette alá független külső ellenőrzésnek informatikai biztonsági intézkedéseit.

Az uniós szervek létrehoztak együttműködési mechanizmusokat, de vannak hiányosságok

45 Az alábbi szakasz az uniós szervek közötti kiberbiztonsági együttműködés előmozdítására létrehozott szereplőket és bizottságokat, valamint az intézményközi irányítási és koordinációs intézkedéseket tárgyalja. Vizsgálatunk ezen belül két intézményközi szereplőre (ENISA és CERT-EU) és két intézményközi bizottságra – a digitális transzformációval foglalkozó intézményközi bizottságra (ICDT) és különösen annak kiberbiztonsági alcsoportjára (CSSG), valamint az Információs és Kommunikációs Technológiai Tanácsadó Bizottságra (ICTAC) – terjedt ki. Értékeltük azt is, hogy ezek milyen mértékben valósítottak meg olyan szinergiákat, amelyek az uniós szervek kiberbiztonsági felkészültségének növelését szolgálták.

Az uniós szervek rendelkeznek formalizált struktúrával tevékenységeik összehangolására, azonban vannak irányítási problémák

46 Az ICDT és az ICTAC az uniós szervek közötti informatikai együttműködést elősegítő két fő bizottság. Az ICDT, amely az uniós intézmények és szervek informatikai vezetőit tömöríti, az információcsere és az együttműködés előmozdítását célzó fórum. Az ICDT-nek van egy kiberbiztonsági alcsoportja (ICDT CSSG), amely az ICDT-nek felel, és konkrét kérdésekben javaslatokat tehet döntésekre. Az ICTAC az Uniós Ügynökségek Hálózatának (EUAN) alcsoportja: ez az uniós ügynökségek vezetői által létrehozott informális hálózat az ügynökségek és a közös vállalkozások közötti együttműködésre fókuszál. Mind az ICDT-nek, mind az ICTAC-nak egyértelműen meghatározott, egymást kiegészítő szerepe van: az ICTAC tevékenysége a decentralizált ügynökségekre és a közös vállalkozásokra, az ICDT-é pedig az intézményekre és egyéb szervekre terjed ki. Az ICDT és az ICTAC jellegüket tekintve inkább informális tanácsadó csoportok, illetve az információk és a bevált gyakorlatok cseréjére szolgáló fórumok. Ezekkel az

intézményközi bizottságokkal kapcsolatban a ***II. mellékletben*** olvashatók további információk.

Az uniós szervek képviselete a releváns fórumokon nem minden esetben megfelelő

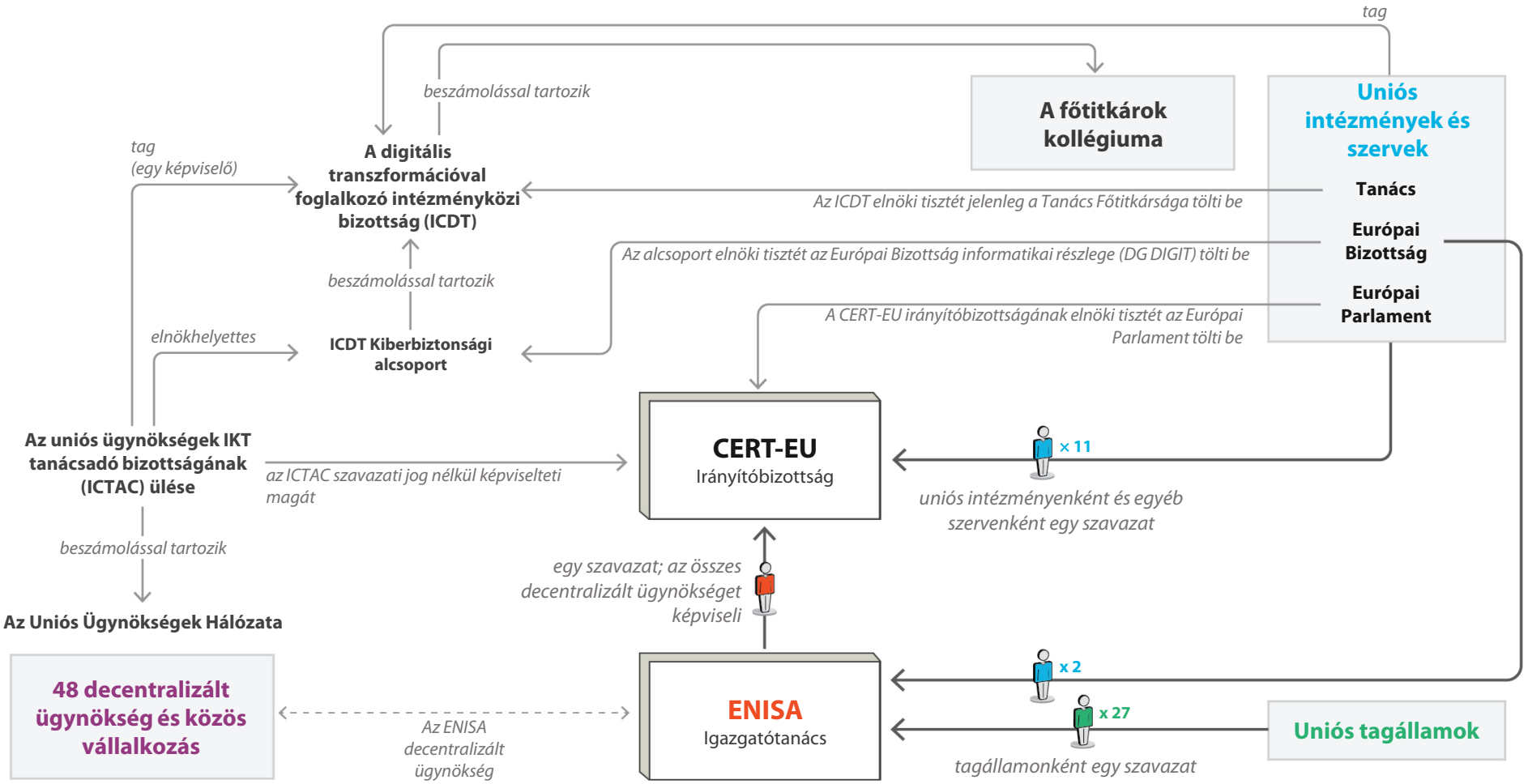
47 Bár a képviseleti struktúrák egyértelműek, nem mindegyik uniós szerv véli úgy, hogy jelenlegi képviselete elégséges lenne. Felmérésünkben arra kértük az uniós szerveket, hogy mondjanak véleményt a következő állításról: „Igényeinket megfelelő módon figyelembe veszik a releváns intézményközi fórumokon, és uniós szervünk megfelelő képviselettel rendelkezik a döntéshozó testületekben”. Az állítással az uniós szervek 42%-a nem értett egyet. A legkisebbek között volt néhány, amely úgy ítélte meg, hogy nem rendelkezik elegendő erőforrással az intézményközi fórumokon való aktív részvételhez.

48 A CERT-EU irányítóbizottsága (fő döntéshozó szerve) szintén nem reprezentálja az általa védett szervezetek összességét. A CERT-EU 87 uniós szerv és három nem uniós szerv részére nyújt szolgáltatást. Irányítóbizottsága azonban csak az intézményközi megállapodást aláíró 11 fél (a hét uniós intézmény, valamint az EKSZ, a Gazdasági és Szociális Bizottság, a Régiók Bizottsága és az Európai Beruházási Bank) képviselőiből és az ENISA egy képviselőjéből áll; mindegyik képviselő egy szavazattal rendelkezik[26].

49 A CERT-EU védett szervezeteinek több mint fele uniós decentralizált ügynökség és közös vállalkozás, amelyek összesen körülbelül 12 000 alkalmazottat foglalkoztatnak. Érdekeiket hivatalosan az ENISA képviseli a CERT-EU irányítóbizottságában. Azonban az ENISA-nak az uniós ügynökségek és közös vállalkozások képviseletére irányuló megbízatása gyenge, mivel nem közvetlenül az érintettek nevezték ki vagy választották meg erre a feladatra. A decentralizált ügynökségek és a közös vállalkozások véleményét a gyakorlatban az ICTAC egy képviselője ismerteti az irányítóbizottsági üléseken, akinek azért engedélyezik a részvételt, hogy támogassa az ENISA-t az ügynökségek képviseletének ellátásában. Bár az ICTAC képviselője 48 uniós szerv véleményét és érdekeit képviseli, jelenleg nem rendelkezik hivatalos hellyel és szavazati joggal az irányítóbizottságban. 2021 áprilisában az ICTAC hivatalos kérelmet küldött a CERT-EU irányítóbizottsága elnökének, amelyben szavazati jogot kért az igazgatótanácsban. Jelentésünk elkészítése idején ezt a kérést még nem teljesítették. Az uniós szervek döntéshozó testületekben és bizottságokban való képviseletének áttekintését a ***6. ábra*** tartalmazza.

[26] A 2017. december 20-án aláírt intézményközi megállapodás 7. cikke.

6. ábra. Kiberbiztonsági irányítás és a döntéshozó testületekben/bizottságokban való képviselet (áttekintés)



Forrás: Európai Számvevőszék.

50 Az uniós szervek intézményközi kiberbiztonsági irányítása fragmentált. Jelenleg egyetlen szervezetnek sincs átfogó rálátása az uniós szervek kiberbiztonsági fejlettségére, és nincs felhatalmazása arra, hogy vezető szerepet vállaljon vagy kötelező közös szabályokat érvényesítsen. Mind az ENISA, mind a CERT-EU csak „támogatni" vagy „segíteni" tudja az uniós szerveket. Az érintett bizottságok nem rendelkeznek döntéshozói hatáskörrel, és csak ajánlásokat fogalmazhatnak meg az uniós szervek számára. Hozzá kell tenni, hogy a felmérésben részt vevő uniós szervek egyötöde számára nem egyértelmű, hová fordulhatnak egyedi szolgáltatások, eszközök vagy megoldások kapcsán.

A kulcsszereplők között vannak egyetértési megállapodások, de ezek ezidáig nem hoztak kézzelfogható eredményeket

51 Az ENISA, a CERT-EU, az Europol Számítástechnikai Bűnözés Elleni Európai Központja (EC3) és az Európai Védelmi Ügynökség (EDA) közötti egyetértési megállapodást 2018 májusában írták alá. A dokumentum öt együttműködési területre összpontosít: információcsere, oktatás és képzés, kibergyakorlatok, technikai együttműködés, valamint stratégiai és igazgatási kérdések. Jóllehet ez az egyetértési megállapodás segíthetne elkerülni a megkettőződéseket egy közös munkaprogram révén, nem találtunk bizonyítékot arra, hogy a megállapodás kézzelfogható eredményekhez és közös fellépésekhez vezetett volna.

52 A kiberbiztonsági jogszabály (CSA), amely 2019 júniusában lépett hatályba, a CERT-EU és az ENISA közötti új egyedi együttműködési megállapodás aláírását irányozta elő. Figyelemreméltó, hogy az egyetértési megállapodás aláírásához (2021. február) több mint másfél évre volt szükség. Az egyetértési megállapodás célja, hogy strukturált együttműködést alakítson ki a CERT-EU és az ENISA között. Meghatározza az együttműködés területeit (kapacitásépítés, operatív együttműködés, tudás- és információmenedzsment) és a hozzávetőleges feladatmegosztást: a CERT-EU játszik vezető szerepet az uniós szerveknek nyújtott támogatásban, az ENISA pedig segíti őt ebben. Az egyetértési megállapodás nem tartalmaz gyakorlati intézkedéseket, mivel azokat az éves együttműködési terv ismerteti. A 2021-re vonatkozó első éves együttműködési tervet az ENISA vezetői testülete 2021 júliusában, a CERT-EU irányítóbizottsága pedig 2021 szeptemberében fogadta el. Ezért még túl korai lenne értékelni, hogy a terv hozott-e kézzelfogható eredményt vagy sem.

53 Mivel az ***51***. és az ***52***. bekezdésben említett egyetértési megállapodások azonos célokra és együttműködési területekre (például képzés, gyakorlatok, információcsere) irányulnak, fennáll az átfedések és a megkettőződés kockázata.

Az együttműködésben rejlő potenciális szinergiákat jelenleg még nem használják ki teljes mértékben

Pozitív lépések történtek a szinergiák megvalósítása érdekében

54 Az ICTAC és az ICDT CSSG bizottsági munkaprogramjai meghatározzák azokat a releváns területeket, ahol együttműködéssel hatékonyságnövekedést lehet elérni. Néhány gyakorlati példa olyan kezdeményezésekre, amelyek lehetővé tették az uniós szervek számára a szinergiák kihasználását:

- intézményközi keretszerződések;
- a közös vészhelyzeti helyreállító központ, amelyet az Európai Unió Szellemi Tulajdoni Hivatala (EUIPO) 2019 óta üzemeltet a decentralizált ügynökségek számára, és amely a piaci árakhoz képest legalább 20%-os költségmegtakarítást tesz lehetővé (kilenc ügynökség választotta ezt a vészhelyzeti helyreállítási megoldást);
- az ugyanazon épületben található hat közös vállalkozás közötti megállapodások, amelyek a közös infrastruktúrára és a közös informatikai biztonsági keretrendszerre irányulnak (2014 óta).

55 További fontos példa az úgynevezett „GovSec”, egy olyan rendszer, amely támogatást nyújt az uniós szervek részére abban, hogy a felhőalapú megoldások bevezetése céljából kockázatértékelést végezzenek. Felmérésünk eredményei azt mutatják, hogy az uniós szervek 75%-a már használja valamelyik nyilvános felhőplatformot, illetve több olyan van, amely jelenleg még nem használ ilyet, de tervezi a felhőre való áttérést. 2019 óta a Bizottság olyan megközelítést alkalmaz, amely a felhő használatát tekinti prioritásnak („cloud-first” approach) és egy biztonságos hibrid, több felhőből álló szolgáltatási ajánlatot irányoz elő[27]. A Bizottság a „Felhő II” keretszerződés szerint valamennyi uniós szerv esetében felhőszolgáltatás-közvetítőként is fellép. A hagyományos „helyhez kötött” informatikai infrastruktúrához képest a felhőalapú platformok biztonsági és adatvédelmi kockázatainak kezeléséhez új készségekre és más megközelítésre van szükség. A felhőben végzett eredményes információbiztonsági kockázatkezelés valamennyi uniós szerv számára kihívást jelent. A GovSec példa egy olyan megoldásra, amely több (vagy akár az összes) uniós szerv igényeinek megfelelhet.

[27] Európai Bizottság, *The European Commission Cloud Strategy*, 2019.

Az uniós szervek közötti együttműködés és a gyakorlatok megosztása továbbra is elmarad az optimálistól

56 Az intézményközi bizottságok létezése nem eredményez automatikusan szinergiákat, és az uniós szervek nem minden esetben osztják meg egymással a bevált gyakorlatokat, szakértelmet, módszereket és tanulságokat. Emellett minden uniós szerv maga dönt arról, milyen mértékben kíván hozzájárulni az ICDT CSSG munkájához. Az ICDT CSSG tagjai – jóllehet jelen vannak az üléseken – csak olyan mértékben tudnak részt venni a munkában, amennyire azt az uniós szervekben betöltött rendes feladataik megengedik. Ez már jelenleg is lassítja az előrehaladást az egyes munkacsoportok által elfogadott intézkedések végrehajtása terén.

57 Találtunk olyan konkrét területeket, ahol nincsenek érvényben olyan mechanizmusok, amelyek lehetővé tennék az uniós szervek számára, hogy tapasztalataikat és kezdeményezéseiket megosszák egymással. A „Hálózatvédelmi képesség” (Network Defence Capability, NDC) keretszerződés értelmében például az uniós szervek kérelmezhetik tanulmány készítését a kiberbiztonsági követelmények konszolidálása és megoldások azonosítása érdekében. Azonban az elkészített vagy az uniós szervek által kérelmezett tanulmányok nem kerülnek be egy adatbázisba, így előfordulhat, hogy az uniós szervek többször is kérelmezik ugyanazt a tanulmányt. Emellett az uniós szervek nem közlik szisztematikusan egymással, hogy szerződéses kapcsolatban állnak bizonyos beszállítókkal vagy egy bizonyos szoftvermegoldást használnak. Ennek az ismerethiánynak a következtében megnövekedhetek a költségek, és elmaradhat a szinergiák megvalósulása.

58 Az uniós szervek az általuk végrehajtott kiberbiztonsági projektekkel kapcsolatos információkat sem osztják meg egymással szisztematikusan, még akkor sem, ha a projekteknek intézményközi szintű hatásaik lehetnek. Az ICDT CSSG megbízatása tartalmaz egy rendelkezést, amelynek értelmében az uniós szervek kötelesek megosztani egymással az olyan új projektekkel kapcsolatos információkat, amelyek potenciálisan érinthetik a többi uniós szerv kiberbiztonságát, illetve a többi uniós szervtől származó információk védelmét. Az ICDT CSSG azonban nem kap folyamatos tájékoztatást az ilyen projektekről.

59 Amikor egy új ügynökséget hoznak létre, az ügynökségnek úgymond a semmiből kell felépítenie informatikai infrastruktúráját és informatikai biztonsági keretrendszerét. Az új ügynökségek számára nincsenek elérhető „szolgáltatási katalógusok”, eszköztárak vagy egyértelmű iránymutatások/előírások. Ennek következtében az uniós szervek informatikai környezetére nagy mértékű heterogenitás jellemző: potenciálisan mindegyik szervezet megteheti, hogy egymástól függetlenül

szerzi be a szoftvereket, a hardvereket, az infrastruktúrákat és a szolgáltatásokat. Ugyanez figyelhető meg az informatikai biztonsági keretrendszernél is, tekintettel a közös követelmények és szabványok hiányára. E helyzet miatt fennáll a lehetősége annak, hogy az erőfeszítések megkettőződnek és az uniós pénzügyi források felhasználása nem hatékonyan történik. Emellett a CERT-EU számára bonyolultabbá válik a támogatásnyújtás.

Az érzékeny információk cseréje terén gyakorlati hiányosságok tapasztalhatók

60 Egyes uniós szervek továbbra sem rendelkeznek megfelelő megoldásokkal a nem minősített, de érzékeny információk cseréje terén. Azok pedig, amelyek rendelkeznek ilyen megoldásokkal, többnyire saját, egymástól eltérő termékeket és rendszereket használnak, ami interoperabilitási problémákhoz vezet. Közös biztonságos platformok csak adott célokhoz kapcsolódóan léteznek: ilyenek például azok a platformok, amelyeket a CERT-EU biztosít és ahol az összes védett szervezet megoszthatja egymással a biztonsági eseményekkel, fenyegetésekkel és sebezhetőségekkel kapcsolatos érzékeny információkat.

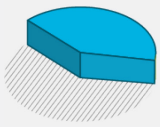
61 Az uniós szerveknek például több mint 20%-a nem rendelkezik titkosított e-mail szolgáltatással. Azok, amelyek rendelkeznek ilyennel, sok esetben szembesülnek interoperabilitási problémákkal, és egymás tanúsítványait nem ismerik el kölcsönösen. Az ICTAC és az ICDT évek óta tárgyal a méretezhető és interoperábilis megoldási lehetőségekről, amely kapcsán 2018-ban sor került egy kísérleti projektre is. A problémát azonban még nem oldották meg.

62 További gondot jelent a nem minősített érzékeny információk közös jelölése. A jelölések a kategorizálást szolgálják, és az információ birtokosainak adnak tájékoztatást az adott információra vonatkozó egyedi védelmi követelményekről. Az uniós szervek más-más jelöléseket használnak, ami megnehezíti az információ cseréjét és megfelelő kezelését.

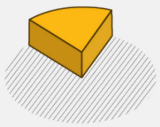
63 2020-ban a Covid19-világjárvány során az uniós szervek arra kényszerültek, hogy üzletmenetük folytonosságának biztosítása érdekében széles körben alkalmazzanak kommunikációs és videokonferencia-eszközöket. Megállapítottuk, hogy az uniós szervek legalább 15 különböző videokonferenciaszoftver-megoldást használnak. Az interoperabilitás sok esetben még akkor sem valósul meg, amikor a különböző uniós szervek ugyanazt a megoldást vagy platformot alkalmazzák, és az összes fél ugyanazt a szoftvermegoldást használja. Emellett az egyes uniós szervek eltérő iránymutatásokat adnak arra nézve, hogy – az érzékenység szempontjából – mely információkat lehet megosztani vagy megvitatni egy adott platformon. Ezek a problémák csökkenthetik a

gazdasági és működési hatékonyságot, és adott esetben biztonsági problémákat eredményezhetnek.

FŐBB SZÁMADATOK: **Az érzékeny információk cseréjét szolgáló eszközök**



az uniós szervek **40%-a** **nem gondolja úgy**, hogy az **érzékeny** (nem minősített) **információk cseréjéhez** megfelelő eszközöket alkalmaz



az uniós szervek **20%-a** **nem** rendelkezik **titkosított e-mail** szolgáltatással

több mint 15 **videokonferencia-megoldást** használnak az uniós szervek; az **érzékeny információkat** érintő használatukra vonatkozó **iránymutatások nem egységesek**

Mind a titkosított e-mail megoldások, mind a videokonferencia-megoldások esetében **interoperabilitási problémák** állnak fenn

Az ENISA és a CERT-EU egyelőre nem ad meg minden szükséges támogatást az uniós szervek számára

64 E szakaszban az ENISA-t és a CERT-EU-t vizsgáljuk meg, vagyis azt a két fő szervezetet, amelynek feladata az uniós szervek kiberbiztonsági támogatása. Értékeljük, hogy a két szervezet által nyújtott támogatás eljut-e az uniós szervekhez és kielégíti-e igényeiket, valamint rávilágítunk a feltárt hiányosságok okaira is.

Az ENISA az uniós kiberbiztonsági környezet kulcsfontosságú szereplője, de támogatása ezidáig csak igen kevés uniós szervhez jutott el

65 2019 júniusában hatályba lépett a kiberbiztonsági jogszabály (CSA)[28], amely az ENISA korábbi jogalapjának[29] helyébe lépett, és erősebb megbízatást adott az ügynökségnek. Nevezetesen úgy rendelkezik, hogy az ENISA kapacitásépítés, az operatív együttműködés bővítése és szinergiák kialakítása útján köteles aktívan támogatni a tagállamokat és az uniós szerveket a kiberbiztonság javításában.

[28] Az ENISA feladatait az (EU) 2019/881 rendelet II. fejezete ((5)–(12) cikk) sorolja fel.

[29] A Európai Parlament és a Tanács 526/2013/EU rendelete; az ENISA e jogszabályban előírt feladatait lásd a (3) cikkben.

A kapacitásépítés terén az ENISA-nak immár megbízatása van arra, hogy segítse az uniós szerveket „a kiberfenyegetések és a biztonsági események megelőzésének, észlelésének és elemzésének (…) javítására irányuló erőfeszítéseikben, különösen a CERT-EU megfelelő támogatása révén”[30]. Az ENISA feladata, hogy támogassa az uniós intézményeket az uniós kiberbiztonsági stratégiák kidolgozásában és felülvizsgálatában, e stratégiák terjesztésének előmozdításában és végrehajtásuk figyelemmel kísérésében.

66 Jóllehet a kiberbiztonsági jogszabály egyértelműen úgy rendelkezik, hogy az ENISA köteles támogatást nyújtani az uniós szervek részére a kiberbiztonság javítása terén, az ENISA még nem dolgozott ki cselekvési tervet az uniós szervek kapacitásépítésének támogatásához kapcsolódó célkitűzésére nézve (részletesen lásd: ***3. háttérmagyarázat***).

[30] A 2019/881/EU rendelet (6) cikke.

3. háttérmagyarázat

Az ENISA célkitűzései nem állnak kellőképpen összhangban az uniós szervekkel kapcsolatos outputjaival

Az ENISA 2018 és 2020 közötti időszakra vonatkozó többéves munkaprogramjában a 3.2. („Az uniós intézmények kapacitásépítésének támogatása”) célkitűzés alatt felsorolt hároméves prioritások többek között az alábbiak:

- „Proaktív tanácsadás az uniós intézmények részére a hálózat- és információbiztonság megerősítésével kapcsolatban (a hálózat- és információbiztonsági kapacitásépítésre leginkább igényt tartó uniós ügynökségek és szervek esetében a prioritások azonosítása rendszeres interakció bevezetésével, például éves munkaértekezletek útján, és az ezen prioritásokra való összpontosítás)”.

- „Törekvés az uniós intézmények részére nyújtott támogatásra és segítségre a hálózat- és információbiztonsági megközelítések terén (partnerség kialakítása a CERT-EU-val és az erős hálózat- és információbiztonsági kapacitással rendelkező intézményekkel az e célkitűzéshez kapcsolódó fellépéseinek támogatása érdekében.)”

Az ENISA 2018., 2019. és 2020. évi munkaprogramjában csupán két operatív célkitűzés (output) szerepel a 3.2. célkitűzés alatt:

- „Részvétel a CERT-EU irányítóbizottságban; a CERT-EU szolgáltatását igénybe vevő uniós ügynökségek képviselete”.

- „Együttműködés az érintett uniós szervekkel a feladataikhoz kapcsolódó hálózat- és információbiztonsági aspektust érintő kezdeményezések terén (ideértve a következőket: EASA, CERT-EU, EDA, EC3)”.

Az operatív célkitűzések nem tartalmaznak olyan tevékenységeket, amelyek a proaktív tanácsadáshoz kapcsolódnának. Ezenkívül a legnagyobb szükségletekkel rendelkező ügynökségek prioritásainak meghatározásához kapcsolódó célkitűzés nyomán sem születettek operatív outputok, mivel ezt az a célkitűzés váltotta fel, hogy az ügynökségek igényeinek a CERT-EU irányítóbizottságában való képviselete érdekében kapcsolatot kell tartani az ügynökségekkel.

67 Az ENISA fő döntéshozó szerve az igazgatótanács, amely a 27 tagállam mindegyike által kinevezett egy-egy tagból és a Bizottság által kinevezett két tagból áll[31] (lásd: ***6. ábra***). Minden tag egy szavazattal rendelkezik; a döntéseket többségi

[31] A kiberbiztonsági jogszabály 14. cikke.

szavazással hozzák[32]. Ennek eredményeképpen a tagállamokat érintő intézkedések adott esetben prioritást élvezhetnek az uniós szerveket érintő intézkedésekkel szemben. Az ENISA 2018. évi munkaprogramjában az igazgatótanács például úgy döntött, hogy – tekintettel a forráshiányra – bizonyos tevékenységeket priorizál, hármat pedig töröl. Ez utóbbiak egyike „az uniós intézményekben érvényben lévő hálózat- és információbiztonsági szabályzatok/eljárások/gyakorlatok értékelésének támogatása" volt, amely arra irányult, hogy az ENISA a jövőbeni célzott fellépések alapjául szolgáló áttekintést készíthessen az uniós szervek gyakorlatáról és indikatív kiberbiztonsági fejlettségéről.

68 Emiatt az ENISA azon – a stratégiai célkitűzésekben megfogalmazott – célkitűzése nyomán, miszerint proaktív támogatást kíván nyújtani az uniós szervek részére, nem fogalmazódtak meg operatív célkitűzések és nem került sor konkrét intézkedésekre. A kapacitásépítés és az operatív együttműködés területén a támogatás ezidáig csak kérésre történt és néhány uniós szervre korlátozódott.

69 A kiberbiztonsági jogszabály azt is előírja, hogy az ENISA az uniós szervek kapacitásépítés terén való segítése érdekében köteles megfelelő támogatást nyújtani a CERT-EU részére. Az ellenőrzés idején e támogatás néhány konkrét intézkedésre korlátozódott. Példa erre, hogy az ENISA 2019-ben elvégezte a CERT-EU szakértői értékelését a hálózati és információs rendszerek biztonságáról szóló irányelv által létrehozott uniós CSIRT-hálózatban való tagságával összefüggésben.

70 A felmérésünkre adott válaszok szerint az ENISA színvonalas jelentéseket és iránymutatásokat tesz közzé a kiberbiztonság témakörében; ezek között több olyan is van, amelyeket az uniós szervek használnak. Nem léteznek azonban olyan egyedi iránymutatások, amelyek kifejezetten az uniós szerveket, azok környezetét és igényeit érintenék. Az uniós szerveknek (és különösen azoknak, amelyek a kiberbiztonság terén kevésbé fejlettek) nem csak azzal kapcsolatban van szükségük iránymutatásra, hogy „mit" kell tenniük, hanem azzal kapcsolatban is, hogy „hogyan". Ezidáig az ENISA és a CERT-EU csak rendszertelenül és korlátozott mértékben nyújtott ilyen támogatást.

71 Az ENISA tartott néhány kiberbiztonsági témájú képzést, elsősorban tagállami hatóságok számára, de néhányan uniós szervek részéről is részt vettek ilyen képzésben. Az ügynökség csak két önálló tanuláson alapuló képzést nyújtott kifejezetten uniós szervek számára. Az ENISA a weboldalán is elérhetővé tesz online képzési anyagokat, amelyekhez az uniós szervek is hozzáférhetnek, azonban ezidáig

[32] A kiberbiztonsági jogszabály 18. cikke.

ezek főként a CSIRT-ek műszaki szakembereinek szóló tanfolyamok voltak, és emiatt a legtöbb uniós szerv számára nem voltak hasznosak.

72 A képzések mellett az ENISA kiberbiztonsági gyakorlatok útján is nyújthat támogatást az uniós szervek számára. 2020 októberében az ENISA – a CERT-EU-val együttműködésben – segített az ICTAC-nak egy kiberbiztonsági gyakorlat lebonyolításában. Ez volt az egyetlen olyan gyakorlat, amelyet az ENISA kifejezetten az uniós szervektől érkező résztvevők számára szervezett. Emellett az ENISA egyes uniós szervek (pl. eu-LISA, EMSA, az Európai Parlament és az Europol) kérésére segített több gyakorlat megszervezésében is, amelyek főként a tagállami hatóságoknál működő érdekelt feleket célozták meg, de az uniós szervek néhány munkatársa is részt vett azokon.

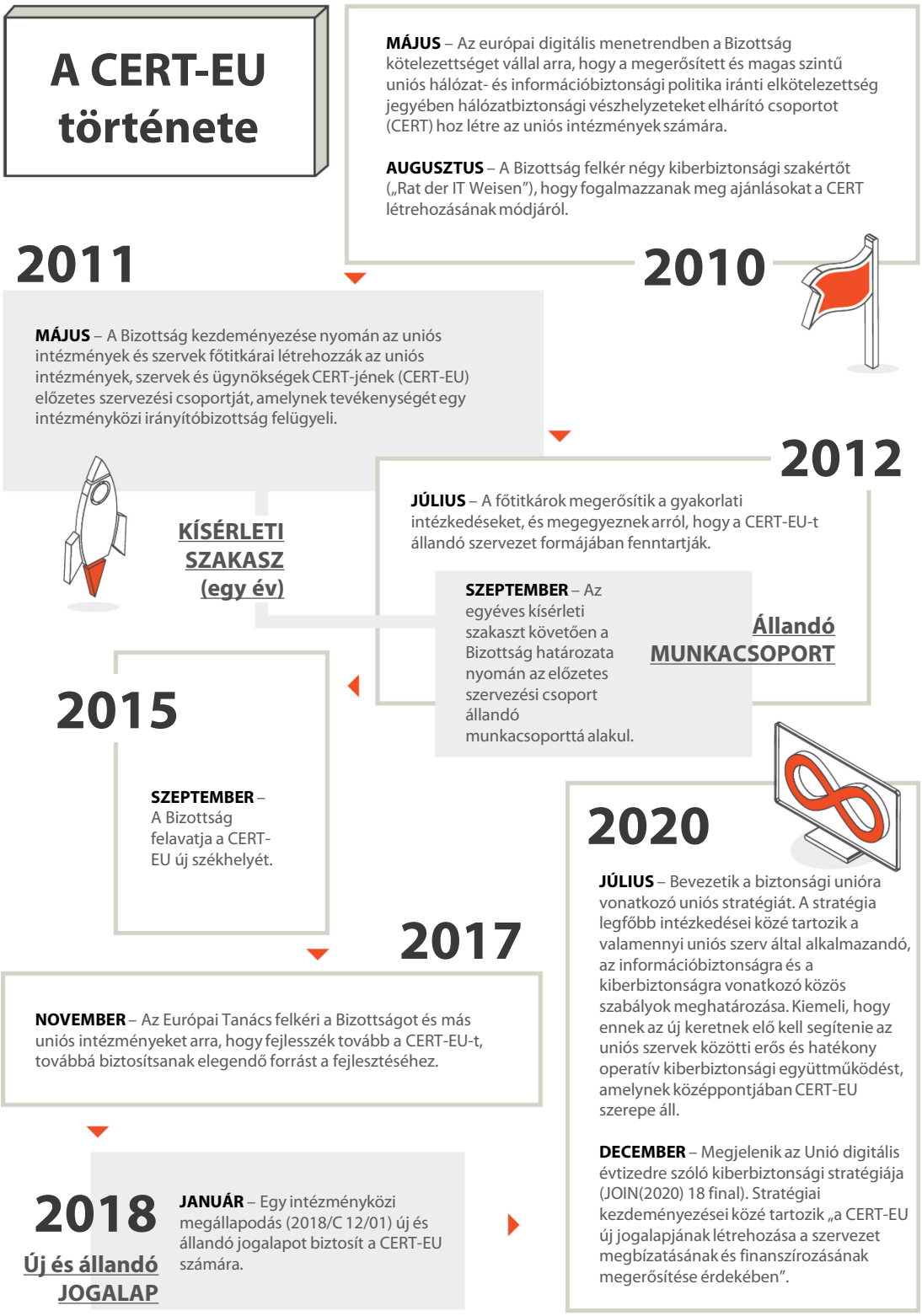
73 A kiberbiztonsági jogszabály új feladatkörrel is felruházta az ENISA-t: ezentúl kérésre a sebezhetőséggel kapcsolatos adatközlési szabályzataik kapcsán is támogatást nyújt az uniós szerveknek. Az ENISA-nak azonban továbbra sincs rálátása az egyes uniós szervek sebezhetőséggel kapcsolatos adatközlési szabályzataira, illetve nem is támogatja az uniós szerveket ilyen szabályzatok kidolgozásában és alkalmazásában.

A CERT-EU-t nagyra értékelik védett szervezetei, de eszközei nincsenek arányban a jelenlegi kiberbiztonsági kihívásokkal

74 Több kezdeményezést követően (lásd: ***7. ábra***) 2012 szeptemberében egy bizottsági határozat[33] létrehozta a hálózatbiztonsági vészhelyzeteket elhárító csoportot (CERT-EU), amely az uniós szervek állandó munkacsoportjaként működik (lásd: ***08***. bekezdés).

[33] Az Európai Bizottság sajtóközleménye: „Sikeres kísérleti projekt hatására nőtt az uniós intézmények kiberbiztonsága”.

7. ábra. A CERT-EU története



Forrás: Európai Számvevőszék.

75 Bár tevékenységét tekintve független, a CERT-EU továbbra is munkacsoportként működik, és nem rendelkezik jogi személyiséggel. Adminisztratív szempontból az Európai Bizottsághoz (DG DIGIT) tartozik, és a Bizottságtól kap logisztikai és adminisztratív támogatást. A CERT-EU célja az uniós szervek IKT-infrastruktúrájának biztonságosabbá tétele azzal, hogy javítja a kiberfenyegetések és sebezhetőségek kezelésére, valamint a kibertámadások megelőzésére, felderítésére, illetve az azokra történő reagálásra való képességüket. A CERT-EU állománya körülbelül 40 főből áll, akik többek között a kiberfenyegetettségi információkkal, a digitális kriminalisztikával és a biztonsági eseményekre való reagálással foglalkozó szakértői csoportokba szerveződve végzik munkájukat.

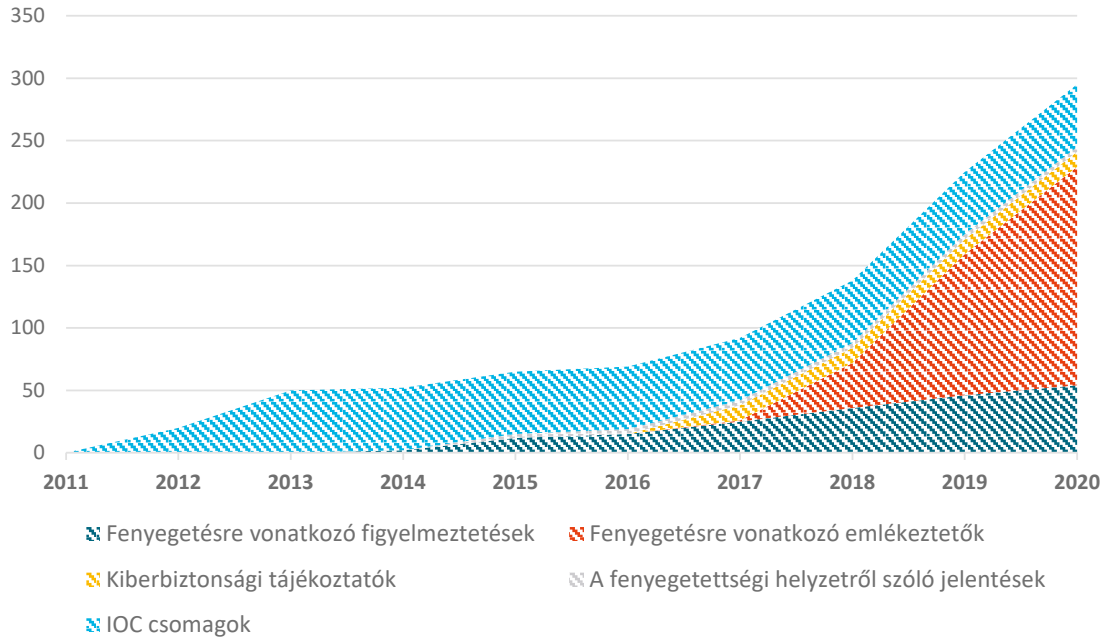
A CERT-EU megbecsült partner, amelynek munkaterhelése egyre nő

76 A CERT-EU negyedévente megrendezett munkaértekezleteken és évenkénti kétoldalú találkozókon, valamint elégedettségi felmérések útján kér visszajelzést és javaslatokat védett szervezeteitől. Az elégedettségi felmérések és saját felmérésünk eredményei azt mutatják, hogy a védett szervezetek nagyrészt elégedettek a CERT-EU által nyújtott szolgáltatásokkal. A CERT-EU szolgáltatási katalógusának fejlődése is mutatja, hogy a CERT-EU erőfeszítéseket tesz annak érdekében, hogy alkalmazkodjon az uniós szervek igényeihez.

77 Míg a jelentős belső kapacitással rendelkező nagyobb uniós szervek a CERT-EU-t jellemzően főként információmegosztó központként és a fenyegetettségi információk forrásaként használják, addig a kisebb uniós szervek szolgáltatások szélesebb skáláját veszik igénybe (például naplófigyelés, behatolási tesztelések, red team gyakorlatok és a biztonsági eseményekre való reagálást érintő támogatás). A CERT-EU szolgáltatásai különösen a kisebb uniós szervek számára értékesek, mivel ezeknél kevesebb belső szakértelem áll rendelkezésre, és nem tudják kihasználni a méretgazdaságosság előnyeit (lásd: ***31***. és ***33***. bekezdés).

78 A fenyegetések és biztonsági események számának drámai növekedésére reagálva a CERT-EU az utóbbi években megerősítette kapacitását és eljárásait. A CERT-EU információs termékeinek – ezen belül különösen a fenyegetésekre vonatkozó figyelmeztetések és emlékeztetők – száma folyamatosan nő (***8. ábra***). 2020-ban a CERT-EU 171 fenyegetésre vonatkozó emlékeztetőt és 53 fenyegetésre vonatkozó figyelmeztetést adott ki, ami jóval több, mint a várakozásuk szerinti 80 emlékeztető és 40 riasztás.

8. ábra. A fenyegetéseket érintő információkhoz kapcsolódó termékek számának növekedése



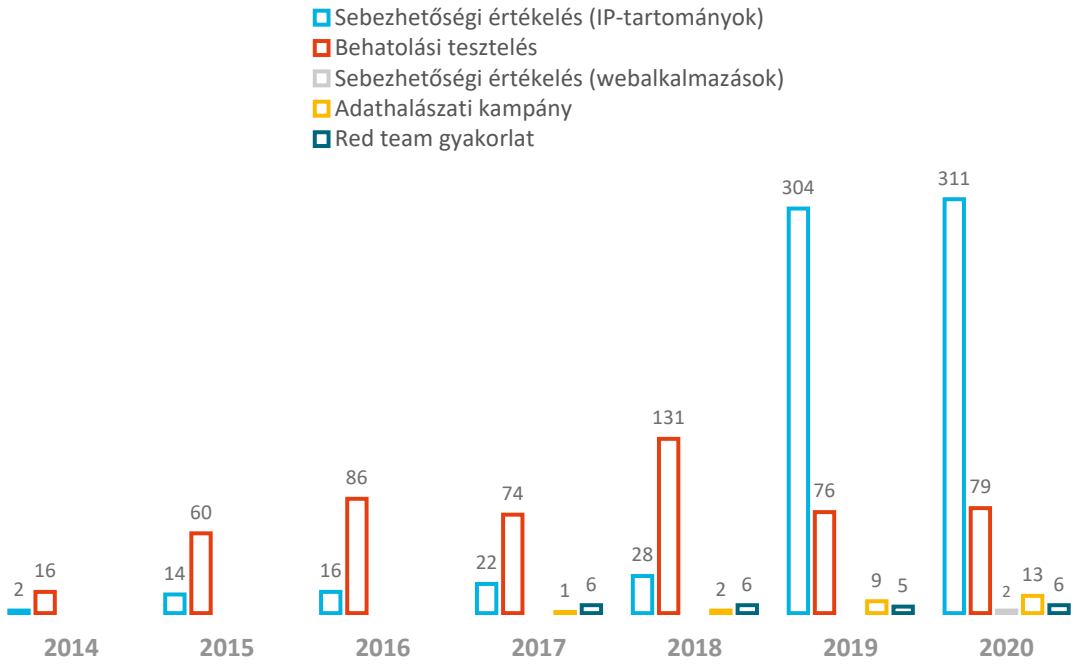
Forrás: Európai Számvevőszék, a CERT-EU adatai alapján.

79 Az CERT-EU a kiberbiztonsági események kezelésében is segíti az uniós szerveket. Míg az uniós szervek 52%-ánál van a biztonsági eseményekre reagáló belső munkacsoport vagy legalábbis a biztonsági események koordinációjáért felelős személy, addig 48%-uk a CERT-EU, illetve más külső szolgáltató szolgáltatásait veszi igénybe biztonsági esemény bekövetkezésekor. Előfordul azonban az is, hogy a belső reagálási kapacitással rendelkező nagy uniós szervek is kérnek támogatást a CERT-EU-tól az összetett események kezeléséhez.

80 2019 és 2020 között a CERT-EU által kezelt biztonsági események teljes száma 561-ről 884-re nőtt. Ezen belül a jelentős incidensek száma 2018 és 2020 között 1-ről 13-ra emelkedett. 2021-ben a jelentős biztonsági események száma elérte a 17-et: 2020 már a maga összesen 13 ilyen eseményével is rekordévnek számított. Ezeket a jelentős biztonsági eseményeket általában rendkívül összetett fenyegetések okozzák, amelyek több uniós szervet érinthetnek, a hatóságok bevonását is szükségessé tehetik, és az érintetteknek, illetve a CERT-EU-nak akár hetekig vagy hónapokig kell dolgozniuk a kivizsgálásukon és felszámolásukon.

81 Emellett az uniós szervek kibervédelmét érintő proaktív értékelések és tesztelések terén is a CERT-EU a fő szolgáltatásnyújtó. E területen végzett tevékenységét a ***9. ábra*** foglalja össze. 2020-tól kezdődően a CERT-EU külső hálózati ellenőrzéseket is végez.

9. ábra. A CERT-EU által elvégzett tesztek és értékelések



Forrás: Európai Számvevőszék, a CERT-EU adatai alapján.

A védett szervezetek nem osztják meg megfelelő időben a releváns információkat a CERT-EU-val

82 Az intézményközi megállapodás[34] előírja, hogy a védett szervezetek kötelesek a CERT-EU-t értesíteni a jelentős kiberbiztonsági eseményekről. A gyakorlatban azonban ez nem mindig történt meg. Az intézményközi megállapodás nem rendelkezik olyan mechanizmusról, amely lehetővé tenné annak kikényszerítését, hogy a CERT-EU védett szervezetei kötelező jelleggel és kellő időben jelentsék a „jelentős” biztonsági eseményeket. Az intézményközi megállapodás a „jelentős esemény” fogalmát általánosságban határozza meg, amivel az uniós szervek mérlegelési jogkörébe utalja, hogy jelentést tesznek-e az ilyen eseményekről. A CERT-EU vezetősége szerint egyes védett szervezetek nem osztották meg kellő időben a jelentős biztonsági eseményekre vonatkozó információkat, ami akadályozza a CERT-EU-t abban, hogy ellássa a kiberbiztonsági információcserét és a biztonsági eseményekre való reagálás koordinációját szolgáló, valamennyi uniós szervet kiszolgáló központként rá rótt feladatokat. Az egyik védett szervezet például, amely nagyon összetett fenyegetéssel szembesült, nem tájékoztatta erről a CERT-EU-t, illetve nem kért tőle támogatást. Emiatt a CERT-EU nem jutott hozzá olyan értesülésekhez a kiberfenyegetésekkel kapcsolatban, amelyek az ugyanazon fenyegetéssel szembesülő más védett

[34] A 2017. december 20-án aláírt intézményközi megállapodás 3. cikkének (3) bekezdése.

szervezetek kapcsán hasznosak lettek volna. A szóban forgó támadás legalább hat uniós szervet érintett.

83 Ezen túlmenően a védett szervezetek nem osztották meg aktívan és kellő időben a CERT-EU-val az őket érintő kiberbiztonsági fenyegetésekkel és sebezhetőségekkel kapcsolatos információkat, annak ellenére sem, hogy az intézményközi megállapodás[35] ezt előírja számukra. A CERT-EU digitális kriminalisztikával és a biztonsági eseményekre való reagálással foglalkozó csoportja csak az általa aktívan vizsgált biztonsági események kapcsán kapott értesítést a sebezhetőségekről vagy a kontrollok terén megmutatkozó hiányosságokról. A védett szervezetek nem osztják meg proaktívan a belső vagy külső biztonsági ellenőrzések során megfogalmazott releváns megállapításokat.

84 Az intézményközi megállapodás emellett nem kötelezi az uniós szerveket arra, hogy az informatikai környezetükben bekövetkezett jelentős változásokat jelentsék a CERT-EU felé; emiatt a védett szervezetek nem tájékoztatták a CERT-EU-t szisztematikusan a releváns változásokról. Az uniós szervek például nem minden esetben tájékoztatják a CERT-EU-t az IP-tartományaikban (vagyis az infrastruktúrájuk internetcím-listájában) bekövetkezett változásokról. A CERT-EU-nak többek között azért van szüksége a frissített IP-tartományokra, hogy a jelentősebb sebezhetőségek azonosításakor ellenőrzéseket tudjon végezni. Ha az uniós szervek nem informálják a CERT-EU-t az ilyen jellegű változásokról, akkor a CERT-EU kevésbé lesz képes támogatást nyújtani nekik. A CERT-EU tájékoztatásának elmulasztása kihat a CERT-EU rendszermegfigyelési képességére is, és többletmunkát okoz számára, hogy a megfigyelést szolgáló eszközökben ki kell igazítania a pontatlan adatokat. Vezetőségének véleménye szerint a CERT-EU-nak esetenként addig nincs is tudomása bizonyos informatikai infrastruktúrák létezéséről, amíg egy-egy biztonsági esemény kezelése során nem értesül arról. Az egyedi esetek mellett megemlítendő az is, hogy a CERT-EU-nak jelenleg nincs rálátása az uniós szervek informatikai rendszereinek és hálózatainak egészére.

85 Mivel az intézményközi megállapodás nem rendelkezik végrehajtási mechanizmusról, a továbbiakban is rendszertelenek maradnak majd az uniós szervek által a CERT-EU részére megküldött értesítések, amelyek pedig alapvető fontosságúak annak biztosításához, hogy a CERT-EU kézben tarthassa az uniós szervek közösségének kiberfelkészültségét.

---

[35] Az intézményközi megállapodás 3. cikkének (2) bekezdése.

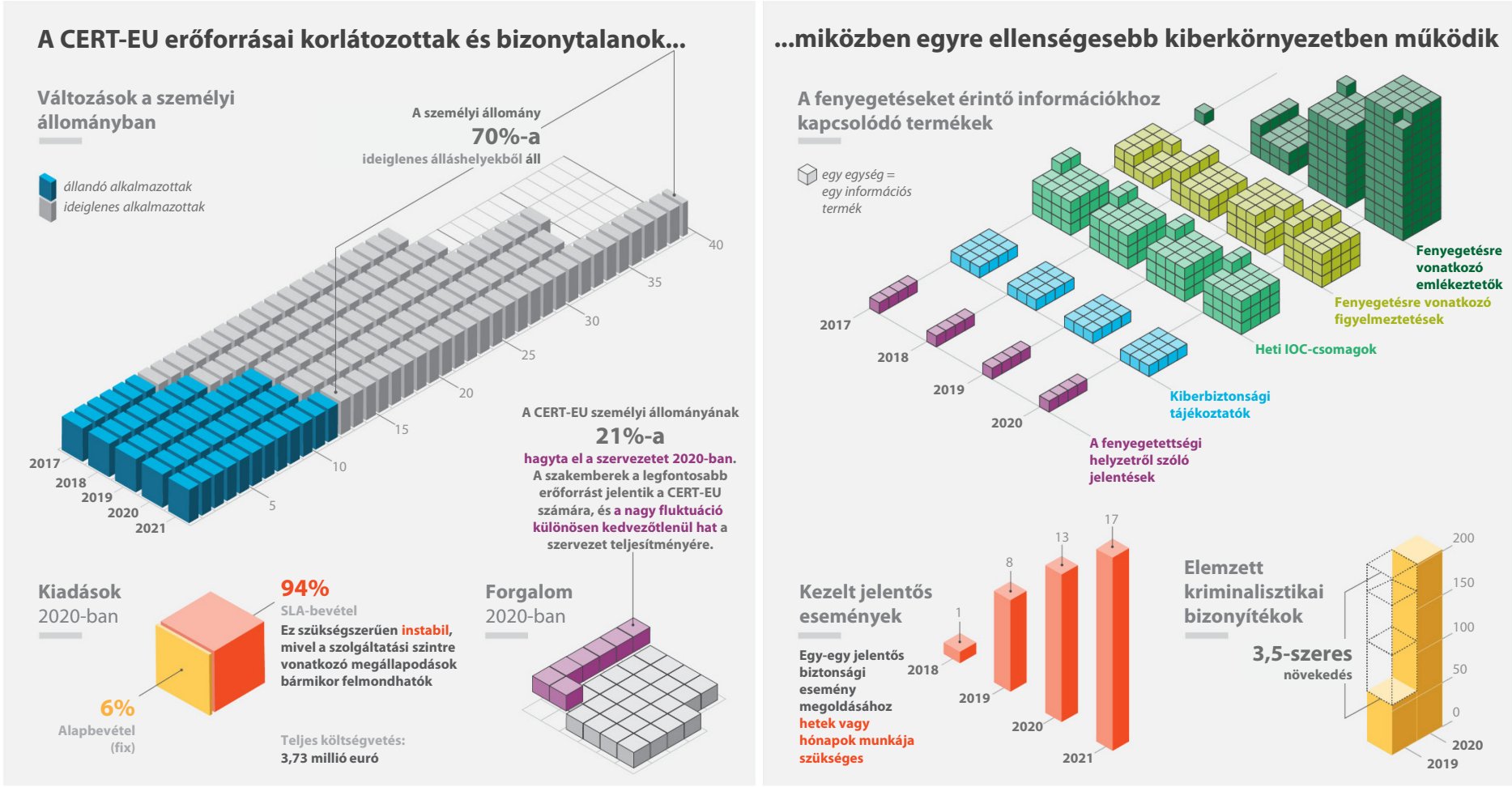
A CERT-EU erőforrásai bizonytalanok, és jelenleg nem arányosak az aktuális fenyegetettségi szinttel

86 Az intézményközi megállapodás[36] kimondja, hogy „a CERT-EU részére fenntartható finanszírozást és személyi állományt kell biztosítani, és mindeközben gondoskodni kell a ráfordítás arányosságáról és megfelelő számú állandó személyzetről.” A CERT-EU legfontosabb erőforrása magasan képzett és specializált személyi állománya. A ***10. ábra*** bemutatja, hogy a 2011-es létrehozásától kezdve a mai napig hogyan alakult a CERT-EU személyi állományának létszáma.

87 A CERT-EU személyi állományának több mint kétharmada határozott idejű szerződéssel rendelkezik. Fizetésük nem számít igazán versenyképesnek a kiberbiztonsági szakértők munkaerőpiacán, és a CERT-EU vezetése szerint egyre nagyobb gondot okoz felvételük és megtartásuk. Ha a fizetések nem eléggé vonzóak a tapasztaltabb jelöltek számára, akkor a CERT-EU kénytelen kevesebb tapasztalattal rendelkező munkatársakat felvenni, majd időt fordítani a képzésükre. Emellett a szerződések maximális időtartama hat év, ami azt jelenti, hogy a CERT-EU a szerződéses állománynak éppen a legnagyobb szakértelemmel rendelkező tagjaitól kénytelen megválni. A munkavállalók fluktuációja különösen magas volt 2020-ban: a CERT-EU állományának 21%-a távozott, és nem mindenki helyett sikerült új munkatársat felvenni. Ami a korábbi éveket illeti, 2019-ben a személyi állomány 9%-a, 2018-ban pedig 13%-a hagyta el a szervezetet.

[36] Az intézményközi megállapodás (7) preambulumbekezdése.

10. ábra. A CERT-EU erőforrásai és kapcsolódó problémái



Forrás: Európai Számvevőszék, a CERT-EU adatai alapján.

88 A CERT-EU vezetősége felhívta a figyelmet arra, hogy jelenleg a CERT-EU digitális kriminalisztikával és a biztonsági eseményekre való reagálással foglalkozó csoportja gyakran túl van terhelve, és többi csoportja sem tud lépést tartani az igényekkel. Ennek következtében a CERT-EU kénytelen volt visszafogni tevékenységeit. Például forráshiány miatt a CERT-EU jelenleg nem vállalja az ellenőrzött szervezetek fejlettségének ellenőrzését. Az CERT-EU gyanús tevékenységekkel kapcsolatos figyelmeztetési szolgáltatása a várt időpontnál később kezdődött meg, szintén forráshiány miatt. Emellett az interjúk során több védett szervezett is megjegyezte, hogy sokáig kellett várniuk arra, hogy hozzáférhessenek az CERT-EU szolgáltatásaihoz.

89 A források korlátozottsága miatt a CERT-EU ezidáig arra kényszerült, hogy főként a hagyományos, „helyhez kötött” informatikai infrastruktúrának a (jellemzően nemzetállamok által támogatott) csoportok jelentette magas szintű állandó fenyegetésekkel szembeni védelmére összpontosítsa a figyelmét. A vezetőség szerint azonban az uniós szervek kiterjesztett informatikai határai – amelyek immár a felhőt, a mobileszközöket és a távmunkához használt eszközöket is magukban foglalják – fokozott felügyeletet és védelmet tesznek szükségessé, és az alacsonyabb szintű fenyegetésekre (például a kiberbűnözésre és a zsarolóvírusokra) is nagyobb figyelmet kell fordítani.

90 Az intézményközi megállapodás nem rendelkezik arról, hogy a CERT-EU-nak a nap huszonnégy órájában és a hét minden napján operatív kapacitással kellene rendelkeznie. A CERT-EU jelenleg nem rendelkezik a szükséges erőforrásokkal, illetve megfelelő humánerőforrás-kerettel ahhoz, hogy állandó és strukturált jelleggel képes legyen a szokásos munkaidőn túl is működni, márpedig a kiberbiztonsági támadások nem igazodnak a munkaidőhöz. Az uniós szervek kapcsán megjegyzendő, hogy a felmérésben részt vevő 65 uniós szerv közül csupán 35-nél dolgozik olyan informatikai tisztviselő, aki a szokásos munkaidőn túl is elérhető.

91 A CERT-EU működésének finanszírozása céljából az irányítóbizottság 2012-ben jóváhagyott egy szolgáltatási szintre vonatkozó megállapodáson (SLA) alapuló modellt. Eszerint valamennyi védett szervezet ingyenesen kapja az alapszolgáltatásokat, és szolgáltatási szintre vonatkozó megállapodás aláírásával, fizetés ellenében bővített szolgáltatásokat is igénybe vehet. A CERT-EU 2020. évi költségvetése 3 745 000 euró volt, amelyből 6%-ot az uniós költségvetésből, 94%-ot pedig a szolgáltatási szintre vonatkozó megállapodásokból finanszíroztak. A védett szervezetek azonban igen heterogének. Vannak köztük olyanok, amelyek fejlett informatikai biztonsági követelményekkel rendelkeznek, míg mások szerény informatikai költségvetésből működnek és kiberbiztonsági fejlettségük igen alacsony szintű. Emiatt a szolgáltatási szintre vonatkozó megállapodásokat érintő tárgyalások nyomán az a kép rajzolódik ki,

hogy egyes uniós szervek magas szintű biztonsági követelményeket szabnak, míg mások esetében viszonylag alacsony a hozzájárulásra való hajlandóság vagy képesség.

92 Hozzá kell tenni azt is, hogy a szolgáltatási szintre vonatkozó megállapodásokat évente és külön-külön meg kell újítani. Ez – amellett, hogy adminisztratív terhet jelent – pénzforgalmi problémákat is okoz, mivel a CERT-EU-hoz nem egyszerre folynak be az összes szolgáltatási szintre vonatkozó megállapodásból származó források. Emellett az ügynökségek bármikor felmondhatják a szolgáltatási szintre vonatkozó megállapodásokat. Emiatt fennáll annak a veszélye, hogy beindul egy ördögi kör: a kieső bevételek következtében a CERT-EU kénytelen szűkíteni a szolgáltatásait és nem tud lépést tartani a kereslettel, ami viszont további uniós szerveket ösztönöz arra, hogy felmondják a szolgáltatási szintre vonatkozó megállapodásaikat, és magánszolgáltatókhoz forduljanak. E megfontolások alapján elmondható, hogy a jelenlegi finanszírozási modell a stabil és optimális szolgáltatási szint biztosításának szempontjából nem ideális.

93 Tekintettel a kiberbiztonsági fenyegetések gyorsan változó környezetére (lásd: ***06***. és ***80***. bekezdés), a CERT-EU irányítóbizottsága 2020. február 19-i ülésén jóváhagyta az arra irányuló stratégiai javaslatot, hogy a CERT-EU bővítse kiberbiztonsági szolgáltatásait és fejlesszen ki „teljes körű operatív képességeket”. A javaslathoz csatoltak egy elemzést, amely a CERT-EU személyzeti és finanszírozási igényeit vizsgálta. Az elemzés megállapította, hogy CERT-EU-nak további 14 állandó tisztviselőre lenne szüksége, mely álláshelyeket 2021 és 2023 között fokozatosan kellene kialakítani. A CERT-EU így 2023-tól kezdődően teljes kapacitással tudna működni.
A javaslat a finanszírozás tekintetében azt fogalmazza meg, hogy a CERT-EU-nak a 2021 és 2023 közötti időszakban 7,6 millió euróval kellene megnövelni a költségvetését, hogy az 2024-re elérje a 11,3 millió eurót.

94 A uniós szervek azonban – bár jóváhagyták a stratégiai javaslatot, amely szerint a CERT-EU számára többletforrások biztosítandók – ezidáig nem jutottak megállapodásra a gyakorlati részletekről sem a 2021 és 2023 közötti átmeneti időszakra nézve, sem pedig hosszú távra, vagyis a jövőbeni kiberbiztonsági rendelet hatálybalépését követő időszakra vonatkozóan (lásd: ***12***. bekezdés).

Következtetések és ajánlások

95 Megállapítottuk, hogy az uniós intézmények, szervek és ügynökségek (röviden: „uniós szervek”) közösségének kiberfelkészültsége összességében nem arányos a fenyegetések mértékével. Ellenőrzésünkből kiderült, hogy az uniós szervek kiberbiztonsági fejlettségi szintje eltérő, és mivel mind az uniós szervek között, mind azok és a tagállami köz- és magánszervezetek között sok a kapcsolódási pont, az egyik uniós szerv kiberbiztonsági gyengeségei több más szervet is kiberfenyegetésnek tehetnek ki.

96 Úgy találtuk, hogy a legfontosabb bevált kiberbiztonsági gyakorlatok (ideértve bizonyos alapvető kontrollokat is) végrehajtására nem minden esetben került sor. A megbízható kiberbiztonsági irányítás kulcsfontosságú az információbiztonság és az informatikai rendszerek biztonsága szempontjából, azonban több uniós szerv esetében még nem valósult meg: az informatikai biztonsági stratégiák és tervek sok esetben hiányoznak vagy azokat a felsővezetés nem hagyta jóvá, a biztonsági szabályzatok nem minden esetben öltenek hivatalos formát, a kockázatértékelések pedig nem vizsgálják a teljes informatikai környezetet. A kiberbiztonsági kiadások eltérőek: egyes uniós szervek hasonló méretű társaikhoz képest egyértelműen túlságosan keveset költenek e célra (lásd: ***21***–***33***. és ***37***–***38***. bekezdés).

97 A kiberbiztonsággal kapcsolatos tudatosság növelését célzó, illetve képzési programok az eredményes kiberbiztonsági keretrendszer kulcsfontosságú elemei. Azonban az uniós szervek csupán 29%-a nyújt kötelező kiberbiztonsági képzést az érzékeny információkat tartalmazó informatikai rendszerekért felelős vezetők számára, és e képzés sok esetben informális jellegű. Az utóbbi öt évben az uniós szervek 55%-a szervezett szimulált adathalászati kampányt (vagy hasonló gyakorlatot). Ezek a gyakorlatok a személyzet képzésének és a figyelemfelkeltésnek fontos eszközei, azonban az uniós szervek nem élnek szisztematikusan ezzel a lehetőséggel (lásd: ***34***–***36***. bekezdés). Emellett nem mindegyik uniós szerv veti alá kiberbiztonsági intézkedéseit rendszeres független ellenőrzésnek (lásd: ***39***–***44***. bekezdés).

98 A CERT-EU-t nagyra becsülik a szolgáltatásait igénybe vevő uniós szervek, azonban kapacitása túlságosan ki van használva. A fenyegetettségi információk és a biztonsági események kezelésével kapcsolatos munkaterhelése 2018 óta gyors ütemben nő. A jelentős kiberbiztonsági események száma több mint tízszeresére emelkedett. Ugyanakkor az uniós szervek nem minden esetben osztják meg kellő időben a jelentős biztonsági eseményekkel, a sebezhetőségekkel és az informatikai infrastruktúrájukban beállt fontos változásokkal kapcsolatos információkat. Ez rontja a

CERT-EU eredményességét, mivel így nem tudja riasztani a többi, potenciálisan érintett uniós szervet, és előfordulhat, hogy jelentős események maradnak felderítetlenül. Ezenfelül a CERT-EU erőforrásai bizonytalanok, és jelenleg nem arányosak az aktuális fenyegetettségi szinttel és az uniós szervek szükségleteivel. A CERT-EU irányítóbizottsága 2020-ban jóváhagyta a CERT-EU által igényelt további források biztosításáról szóló stratégiai javaslatot, azonban a védett szervezetek ezidáig még nem jutottak megállapodásra a források biztosításának gyakorlati részleteivel kapcsolatban. Emiatt a CERT-EU személyi állománya nem képes megfelelni a vele szemben támasztott követelményeknek, így a csoport kénytelen leszűkíteni tevékenységeit (lásd: ***74–93***. bekezdés).

1. ajánlás. Valamennyi uniós szerv kiberbiztonsági felkészültségének javítása, kötelező, közös kiberbiztonsági szabályok és a CERT-EU forrásainak növelése révén

A Bizottság a következő elveket építse be a valamennyi uniós szerv közös, magas szintű kiberbiztonsági védelmét célzó intézkedéseket megállapító rendeletre irányuló jövőbeni javaslatába:

a) A felsővezetésnek a kiberbiztonsági stratégiák és a kulcsfontosságú biztonsági szabályzatok jóváhagyásával, valamint egy független információbiztonsági főtisztviselő (vagy azzal egyenértékű szerepet betöltő személy) kinevezésével felelősséget kell vállalnia a kiberbiztonsági irányításért.

b) Az uniós szerveknek rendelkezniük kell egy olyan informatikai biztonsági kockázatkezelési keretrendszerrel, amely informatikai infrastruktúrájuk egészére kiterjed, továbbá rendszeres kockázatértékeléseket kell végezniük.

c) Az uniós szerveknek a tudatosság növelését célzó rendszeres képzéseket kell biztosítaniuk a személyi állomány valamennyi tagja számára, beleértve a vezetőséget is.

d) Az uniós szerveknek gondoskodniuk kell kibervédelmi rendszerük rendszeres ellenőrzéséről és teszteléséről. Az ellenőrzéseknek ki kell terjedniük a kiberbiztonságra fordított források megfelelőségére is.

e) Az uniós szervek haladéktalanul tegyenek jelentést a CERT-EU felé a jelentős kiberbiztonsági eseményekről, valamint az informatikai infrastruktúrájukkal kapcsolatos releváns változásokról és sebezhetőségekről.

f) Az uniós szervek – az igazgatótanácsuk által jóváhagyott stratégiai javaslatban meghatározott szükségletekkel összhangban – növeljék és költségvetésükben különítsék el a CERT-EU részére előirányzott forrásokat.

g) A rendelet írjon elő rendelkezéseket arra nézve is, hogy ki kell jelölni egy, valamennyi uniós szervet képviselő testületet, amely megfelelő felhatalmazással és eszközökkel bír annak nyomon követésére, hogy minden uniós szerv betartja-e a közös kiberbiztonsági szabályokat, továbbá iránymutatást, ajánlásokat és intézkedésekre való felszólításokat tesz közzé.

Megvalósítás céldátuma: 2023. első negyedév

99 Az uniós szervek bevezettek a kiberbiztonsággal kapcsolatos együttműködést szolgáló mechanizmusokat, azonban megállapítottuk, hogy a lehetséges szinergiákat nem használják ki teljes mértékben. Az információcsere formalizált struktúrában zajlik, amelyben a szereplők és a bizottságok egymást kiegészítő szerepet töltenek be. Azonban a kisebb uniós szervek intézményközi fórumokon való részvételét akadályozzák a korlátozott erőforrások. A decentralizált ügynökségek és közös vállalkozások képviselete a CERT-EU irányítóbizottságában nem optimális. Azt is megállapítottuk, hogy az uniós szervek nem osztják meg egymással szisztematikusan a kiberbiztonsági projektekre, biztonsági értékelésekre és más szolgáltatási szerződésekre vonatkozó információkat, ami az erőfeszítések megkettőződéséhez és megnövekedett költségekhez vezethet. Működési nehézségeket tapasztaltunk a nem minősített érzékeny információk titkosított e-mailekben vagy videokonferenciákon keresztül történő cseréje kapcsán, amelyek oka az informatikai megoldások interoperabilitásának, az engedélyezett használatukra vonatkozó egységes iránymutatásoknak, valamint a közös információjelöléseknek és kezelési szabályoknak a hiánya (lásd: ***45–63***. bekezdés).

2. ajánlás. További szinergiák előmozdítása az uniós szervek között bizonyos kiválasztott területeken

A Bizottság a digitális transzformációval foglalkozó intézményközi bizottságon keresztül mozdítsa elő az alábbi tevékenységeket az uniós szervek között:

a) a biztonságos kommunikációs csatornák (például a titkosított e-mailek és a videokonferenciák) interoperabilitását célzó megoldások elfogadása, valamint a közös jelölések és kezelési szabályok alkalmazásának ösztönzése a nem minősített érzékeny információk tekintetében;

b) a kiberbiztonsághoz kapcsolódó, potenciálisan intézményközi hatással bíró projektekre, a szoftvereken elvégzett biztonsági értékelésekre és a külső beszállítókkal érvényben lévő szerződésekre vonatkozó információk szisztematikus megosztása;

c) olyan kiberbiztonsági szolgáltatásokra vonatkozó közös közbeszerzési szerződések és keretszerződések előírásainak meghatározása, amelyekben a méretgazdaságosság elősegítése céljából valamennyi uniós szerv részt vehet.

Megvalósítás céldátuma: 2023. negyedik negyedév

100 Az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) és a CERT-EU az uniós szervek kiberbiztonság terén való támogatásával megbízott két legfontosabb szereplő. Az erőforrások korlátozottsága és más területek előnyben részesítése miatt azonban nem voltak képesek az uniós szerveknek megadni mindazt a támogatást, amelyre azoknak szüksége lenne, különös tekintettel a kiberbiztonság terén kevésbé fejlett uniós szervek kapacitásépítésére (lásd: ***64–93***. bekezdés).

3. ajánlás. A CERT-EU és az ENISA fordítson több figyelmet a kevésbé fejlett uniós szervekre

A CERT-EU és az ENISA:

a) azonosítsa (például fejlettségi értékelések révén) azokat a prioritási területeket, amelyeken az uniós szerveknek a legtöbb támogatásra van szükségük;

b) az egyetértési megállapodásnak megfelelően hajtson végre kapacitásbővítési intézkedéseket.

Megvalósítás céldátuma: 2022. negyedik negyedév

A jelentést 2022. február 22-i luxembourgi ülésén fogadta el a Bettina Jakobsen számvevőszéki tag elnökölte III. Kamara.

A Számvevőszék nevében

Klaus-Heiner LEHNE
elnök

Mellékletek

I. melléklet. A felmérésben közreműködő uniós szervek

Az uniós szerv neve	Típus
Európai Parlament (EP)	Intézmény (az EUSZ 13. cikkének (1) bekezdése)
Az Európai Unió Tanácsa és az Európai Tanács (a Tanács Főtitkársága)	Intézmény (az EUSZ 13. cikkének (1) bekezdése)
Európai Bizottság (EB)	Intézmény (az EUSZ 13. cikkének (1) bekezdése)
Az Európai Unió Bírósága (EUB)	Intézmény (az EUSZ 13. cikkének (1) bekezdése)
Európai Központi Bank (EKB)	Intézmény (az EUSZ 13. cikkének (1) bekezdése)
Európai Számvevőszék	Intézmény (az EUSZ 13. cikkének (1) bekezdése)
Európai Külügyi Szolgálat (EKSZ)	Szerv (az EUSZ 27. cikkének (3) bekezdése)
Európai Gazdasági és Szociális Bizottság (EGSZB) és Régiók Bizottsága (RB)[37]	Szervek (az EUSZ 13. cikkének (4) bekezdése)
Európai Beruházási Bank (EBB)	Szerv (az EUMSZ 308. cikke)
Európai Munkaügyi Hatóság (ELA)	Decentralizált ügynökség
Energiaszabályozók Európai Uniós Együttműködési Ügynöksége (ACER)	Decentralizált ügynökség
Európai Elektronikus Hírközlési Szabályozók Testületének Hivatala (BEREC Hivatal)	Decentralizált ügynökség
Közösségi Növényfajta-hivatal (CPVO)	Decentralizált ügynökség
Európai Munkahelyi Biztonsági és Egészségvédelmi Ügynökség (EU-OSHA)	Decentralizált ügynökség
Európai Határ- és Partvédelmi Ügynökség (Frontex/EBCGA)	Decentralizált ügynökség
A szabadságon, a biztonságon és a jog érvényesülésén alapuló térség nagyméretű IT-rendszereinek üzemeltetési igazgatását végző európai uniós ügynökség (eu-LISA)	Decentralizált ügynökség
Az Európai Unió Menekültügyi Ügynöksége (EUAA)	Decentralizált ügynökség
Az Európai Unió Repülésbiztonsági Ügynöksége (EASA)	Decentralizált ügynökség
Európai Bankhatóság (EBH)	Decentralizált ügynökség
Európai Betegségmegelőzési és Járványvédelmi Központ (ECDC)	Decentralizált ügynökség

[37] Az EGSZB és az RB egy uniós szervnek tekintendő.

Az uniós szerv neve	Típus
Európai Szakképzésfejlesztési Központ (Cedefop)	Decentralizált ügynökség
Európai Vegyianyag-ügynökség (ECHA)	Decentralizált ügynökség
Európai Környezetvédelmi Ügynökség (EEA)	Decentralizált ügynökség
Európai Halászati Ellenőrző Hivatal (EFCA)	Decentralizált ügynökség
Európai Élelmiszerbiztonsági Hatóság (EFSA)	Decentralizált ügynökség
Európai Alapítvány az Élet- és Munkakörülmények Javításáért (Eurofound)	Decentralizált ügynökség
Az Európai Unió Űrprogramügynöksége (EUSPA) [az Európai GNSS Ügynökség helyébe lép]	Decentralizált ügynökség
A Nemek Közötti Egyenlőség Európai Intézete (EIGE)	Decentralizált ügynökség
Európai Biztosítás- és Foglalkoztatóinyugdíj-hatóság (EIOPA)	Decentralizált ügynökség
Európai Tengerészeti Biztonsági Ügynökség (EMSA)	Decentralizált ügynökség
Európai Gyógyszerügynökség (EMA)	Decentralizált ügynökség
A Kábítószer és a Kábítószer-függőség Európai Megfigyelőközpontja (EMCDDA)	Decentralizált ügynökség
Európai Uniós Kiberbiztonsági Ügynökség (ENISA)	Decentralizált ügynökség
Az Európai Unió Bűnüldözési Képzési Ügynöksége (CEPOL)	Decentralizált ügynökség
Európai Rendőrségi Hivatal (Europol)	Decentralizált ügynökség
Az Európai Unió Vasúti Ügynöksége (ERA)	Decentralizált ügynökség
Európai Értékpapírpiaci Hatóság (ESMA)	Decentralizált ügynökség
Európai Képzési Alapítvány (ETF)	Decentralizált ügynökség
Az Európai Unió Alapjogi Ügynöksége (FRA)	Decentralizált ügynökség
Az Európai Unió Szellemi Tulajdoni Hivatala [2016. március 23-ig BPHH néven] (EUIPO)	Decentralizált ügynökség
Egységes Szanálási Testület (ESZT)	Decentralizált ügynökség
Az Európai Unió Büntető Igazságügyi Együttműködési Ügynöksége (Eurojust)	Decentralizált ügynökség
Az Európai Unió Szerveinek Fordítóközpontja (CdT)	Decentralizált ügynökség
Európai Ügyészség (EPPO)	Decentralizált ügynökség
Európai Innovációs és Technológiai Intézet (EIT)	A K+I keretében létrehozott szervek
„Egységes európai égbolt” légiforgalmi szolgáltatási kutatás (SESAR)	Az EUMSZ szerinti közös vállalkozás
Kiváló Európai Elektronikai Alkatrészek és Rendszerek közös vállalkozás (ECSEL)	Az EUMSZ szerinti közös vállalkozás
Második Üzemanyagcella- és Hidrogéntechnológiai Közös Vállalkozás (FCH2)	Az EUMSZ szerinti közös vállalkozás

Az uniós szerv neve	Típus
Innovatív Gyógyszerek Kezdeményezés 2 Közös Vállalkozás (IMI2)	Az EUMSZ szerinti közös vállalkozás
Tiszta Égbolt 2 Közös Vállalkozás (Clean Sky 2)	Az EUMSZ szerinti közös vállalkozás
Bioalapú Iparágak Közös Vállalkozás (BBI)	Az EUMSZ szerinti közös vállalkozás
Shift2Rail Közös Technológiai Kezdeményezés Közös Vállalkozás (S2R)	Az EUMSZ szerinti közös vállalkozás
Európai Nagy Teljesítményű Számítástechnika Közös Vállalkozás (EuroHPC)	Az EUMSZ szerinti közös vállalkozás
ITER Európai Közös Vállalkozás – Fusion for Energy (F4E)	Az EUMSZ szerinti közös vállalkozás
Az Európai Unió ukrajnai tanácsadó missziója (EUAM Ukrajna)	Polgári misszió (KBVP)
Az EU líbiai integrált határigazgatást segítő missziója (EUBAM Líbia)	Polgári misszió (KBVP)
Az EU nigeri kapacitásépítő missziója (EUCAP Száhel Niger)	Polgári misszió (KBVP)
Az EU grúziai megfigyelő missziója (EUMM Georgia)	Polgári misszió (KBVP)
Az EU Palesztin Rendőrség Támogatására létrejött Koordinációs Irodája (EUPOL COPPS)	Polgári misszió (KBVP)
Az EU közép-afrikai köztársasági tanácsadó missziója (EUAM Közép-Afrikai Köztársaság)	Polgári misszió (KBVP)
Az EU iraki tanácsadó missziója (EUAM Irak)	Polgári misszió (KBVP)
A rafahi átkelőhelyen működő határőrizeti európai uniós misszió (EUBAM Rafah)	Polgári misszió (KBVP)
Az EU mali kapacitásépítő missziója (EUCAP Száhel Mali)	Polgári misszió (KBVP)
A szomáliai kapacitásépítést célzó európai uniós misszió (EUCAP Szomália)	Polgári misszió (KBVP)
Az EU koszovói jogállamiság-missziója (EULEX Koszovó)	Polgári misszió (KBVP)

II. melléklet. További információk a kulcsfontosságú intézményközi bizottságokról

A digitális transzformációval foglalkozó intézményközi bizottság (ICDT)

Az ICDT az információcsere és az informatikai együttműködés előmozdítását szolgáló fórum. 2020 májusában hozták létre a korábbi Comité Interinstitutionnel de l'Informatique (CII) felváltására. Az ICDT az uniós szervek informatikai osztályainak vezetőiből áll. Az ICDT kiberbiztonsági alcsoportja az ICDT CSSG, amelynek feladata az uniós szervek közötti kiberbiztonsági együttműködés előmozdítása, továbbá az információcsere fórumaként működik.

Az ICDT döntéshozatali jogköre olyan kérdésekre korlátozódik, amelyek nem befolyásolják „azt, ahogy az intézmények teljesítik feladataikat” és nem „érintik az irányítást az egyes intézményeken belül”. A hatáskörét meghaladó döntések esetében az ICDT ajánlásokat fogalmazhat meg az uniós intézmények és szervek főtitkárainak kollégiuma számára.

Az ICDT megbízatása értelmében tagjai az egyes uniós intézmények és szervek képviselői, valamint az uniós ügynökségek (ICTAC) által kijelölt egy képviselő. Az ICDT elnöki tisztét jelenleg a Tanács Főtitkársága tölti be.

Az ICDT kiberbiztonsági alcsoportja (ICDT CSSG)

A jelenlegi összetételű ICDT CSSG-t 2020 szeptemberében hozták létre. Az ICDT CSSG a korábbi CII állandó biztonsági alcsoportjának helyébe lépett. Elődjéhez képest az ICDT CSSG strukturáltabb, ambiciózusabb és eredményorientáltabb megközelítéssel dolgozik. Tevékenységét munkacsoportok végzik, amelyek rendszeresen üléseznek és a legfontosabb közös kérdésekre összpontosítják figyelmüket:

- 1. munkacsoport: „Közös szabványok, referenciaértékek és fejlettség”
- 2. munkacsoport: „A megosztási platformokhoz kapcsolódó módszerek, eszközök, szerződések”
- 3. munkacsoport: „Felhőbiztonság”
- 4. munkacsoport: „Tehetségfejlesztés a kiberkészségek terén”
- 5. munkacsoport: „A kiberbiztonsággal kapcsolatos tudatosság”
- 6. munkacsoport: „Videokonferenciák biztonsága”

A CSSG megbízatása szerint a titkárság feladata a munkacsoportok tevékenységének rendszeres ellenőrzése és az előrehaladásról való beszámolás. A titkárság rendszeresen jelentést készít az ICDT kiberbiztonsági alcsoportja elnökének és elnökhelyettesének a részére, rendszeresen összegyűjtve a munkacsoportok koordinátorainak észrevételeit. A CSSG összefoglaló tevékenységi jelentést is köteles benyújtani minden év végén.

Az ICDT CSSG elnöki tisztét jelenleg a Bizottság, elnökhelyettesi tisztét pedig az ICTAC tölti be. Jóllehet a CSSG nem rendelkezik döntéshozatali hatáskörrel, a releváns kérdésekben javasolhat döntéseket a ICDT-nek.

Az Ügynökségek Hálózata

Az Európai Unió Ügynökségeinek Hálózata (EUAN) informális hálózat, amelyet az uniós ügynökségek vezetői 2012-ben hoztak létre. Az EUAN jelenleg 48 decentralizált uniós ügynökségből és közös vállalkozásból áll. Célja, hogy a hálózat tagjai számára közös érdeklődésre számot tartó területeken a cserét és az együttműködést lehetővé tevő platformot biztosítson. Az Információs és Kommunikációs Technológiai Tanácsadó Bizottság (ICTAC) az EUAN alcsoportja, amelynek feladata az együttműködés előmozdítása az IKT (többek között a kiberbiztonság) terén.

Információs és Kommunikációs Technológiai Tanácsadó Bizottság (ICTAC)

Az ICTAC az ügynökségek és a közös vállalkozások közötti együttműködést mozdítja elő az infokommunikációs technológiák terén. Célja, hogy megvalósítható és gazdaságos megoldásokat találjon a közös problémákra, információkat cseréljen és szükség esetén közös álláspontokat fogadjon el. Az ICTAC megbízatása szerint évente kétszer kerül sor közgyűlésre, amelyre az összes tag hivatalos. Emellett havonta rendszeres ülésekre kerül sor az ICTAC-nak a CSSG munkacsoportokban részt vevő képviselői, az ICTAC-nak a CSSG-be delegált képviselője és az ICTAC „trojkája” között. A trojka az ICTAC hivatalban lévő, korábbi és jövőbeni elnökeiből áll (az elnök megbízatása egy évre szól). A trojka feladata, hogy támogatást nyújtson a hivatalban lévő elnöknek a feladatkörével kapcsolatos minden kérdésben (ideértve a helyettesítését is, ha a körülmények szükségessé teszik).

Betűszavak és rövidítések

APT: Magas szintű állandó fenyegetés

CERT-EU: Az uniós szervek hálózatbiztonsági vészhelyzeteket elhárító csoportja

CIS: Kommunikációs és információs rendszer

CISO: Információbiztonsági főtisztviselő

CSA: Kiberbiztonsági jogszabály

CSIRT: Számítógép-biztonsági eseményekre reagáló csoport

DG DIGIT: Informatikai Főigazgatóság

DG HR: Humánerőforrásügyi és Biztonsági Főigazgatóság

ENISA: Európai Uniós Kiberbiztonsági Ügynökség

EUAN: Az Európai Unió Ügynökségeinek Hálózata

eu-LISA: A szabadságon, a biztonságon és a jog érvényesülésén alapuló térség nagyméretű IT-rendszereinek üzemeltetési igazgatását végző európai ügynökség

ICDT CSSG: A digitális transzformációval foglalkozó intézményközi bizottság kiberbiztonsági alcsoportja

ICDT: A digitális transzformációval foglalkozó intézményközi bizottság

ICTAC: Információs és Kommunikációs Technológiai Tanácsadó Bizottság

IIA: Intézményközi megállapodás

IKT: Információs és kommunikációs technológiák

ISACA: Információrendszer-ellenőrök Egyesülete

ITCB: Informatikai és Kiberbiztonsági Tanács

MoU: Egyetértési megállapodás

NIS: Hálózat- és információbiztonság

SLA: Szolgáltatási szintre vonatkozó megállapodás

TME: Teljes munkaidős egyenérték

Uniós szervek: Az Európai Unió intézményei, szervei és ügynökségei

Glosszárium

Adathalászat (phishing): Megbízható forrásból érkezőnek feltüntetett e-mailek küldése, amelyek a címzetteket csellel rosszindulatú linkek megnyitására vagy személyes adatok megosztására bírják rá.

Az európai intézmények, szervek és hivatalok hálózatbiztonsági vészhelyzeteket elhárító csoportja: Az információcserét és a biztonsági eseményekre való reagálás koordinációját szolgáló központ, amelynek ügyfelei (az úgynevezett „védett szervezetek”) az uniós intézmények, szervek és ügynökségek.

Behatolási tesztelés: Az informatikai rendszerek biztonságának értékelésére szolgáló módszer, amelynek alkalmazása során arra tesznek kísérletet, hogy a biztonsági biztosítékokat olyan eszközökkel és technikákkal törjék át, amelyeket jellemzően a támadók használnak.

Kiberbiztonság: Az informatikai hálózatok és infrastruktúrák, illetve az azokban tárolt információk külső fenyegetésekkel szembeni védelmét szolgáló intézkedések.

Kiberkémkedés: Az a cselekmény vagy gyakorlat, amelynek során az információ birtokosának engedélye és tudta nélkül titkokat és információkat szereznek meg az internetről, hálózatokról vagy egyéni számítógépekről.

Kibertér: a globális online környezet, ahol az emberek, szoftverek és szolgáltatások számítógépek, illetve egyéb csatlakoztatott eszközök hálózatán keresztül kommunikálnak egymással.

Magas szintű állandó fenyegetés: Olyan támadás, amely során jogosultság nélküli felhasználó érzékeny adatok ellopása céljából behatol egy rendszerbe vagy hálózatba, és hosszabb időn keresztül ott marad.

Pszichológiai manipuláció (social engineering): Az információbiztonsági területen olyan pszichológiai manipuláció, amelynek célja, hogy az embereket rávegye valamilyen cselekvés elvégzésére vagy bizalmas információk megosztására.

Red teaming (valósághű támadásszimulációs gyakorlatok): Kibertámadások valósághű szimulációja, amely a meglepetés eszközét és a közelmúltban megfigyelt, ténylegesen használt technikákat alkalmazza, és több támadási vonallal konkrét célokra összpontosít.

A Bizottság válaszai

https://www.eca.europa.eu/hu/Pages/DocItem.aspx?did=60922

A CERT-EU és az ENISA válaszai

https://www.eca.europa.eu/hu/Pages/DocItem.aspx?did=60922

Időrendi áttekintés

https://www.eca.europa.eu/hu/Pages/DocItem.aspx?did=60922

SZERZŐI JOGOK

PDF	ISBN 978-92-847-7584-2	1977-5733	doi:10.2865/58919	QJ-AB-22-003-HU-N
HTML	ISBN 978-92-847-7615-3	1977-5733	doi:10.2865/384396	QJ-AB-22-003-HU-Q

Meredeken nő az uniós intézmények, szervek és ügynökségek (a továbbiakban együttesen: uniós szervek) ellen elkövetett kibertámadások száma. Mivel az uniós szervek szorosan kapcsolódnak egymáshoz, egyikük gyengeségei másokat is biztonsági kockázatoknak tehetnek ki. Megvizsgáltuk, hogy az uniós szervek megfelelő intézkedésekkel védekeznek-e a kiberfenyegetések ellen. Megállapítottuk, hogy az uniós szervek felkészültségi szintje összességében nem áll arányban a fenyegetésekkel, és kiberbiztonsági fejlettségük igen eltérő. Javasoljuk, hogy a Bizottság javítsa az uniós szervek felkészültségét: ennek érdekében tegyen javaslatot kötelező kiberbiztonsági szabályok bevezetésére, valamint növelje a hálózatbiztonsági vészhelyzeteket elhárító csoport (CERT-EU) forrásait. A Bizottság emellett mozdítsa elő az uniós szervek közötti szinergiák jobb kihasználását, a CERT-EU és az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) pedig elsődlegesen a kevésbé fejlett uniós szerveket támogassa.

A Számvevőszék különjelentése az EUMSZ 287. cikke (4) bekezdésének második albekezdése alapján.

EURÓPAI SZÁMVEVŐSZÉK

Az Európai Unió Kiadóhivatala

EURÓPAI SZÁMVEVŐSZÉK
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBOURG

Telefon: +352 4398-1

Megkeresés: eca.europa.eu/hu/Pages/ContactForm.aspx
Weboldal: eca.europa.eu
Twitter: @EUAuditors