Az Európai Unió
Tanácsa

Brüsszel, 2022. március 22.
(OR. en)

7474/22

Intézményközi referenciaszám:
2022/0085(COD)

CYBER 93
TELECOM 116
JAI 383
INST 89
INF 32
CSC 119
CSCI 39
DATAPROTECT 81
FIN 353
BUDGET 2
CODEC 349
IA 30

JAVASLAT

Küldi:	az Európai Bizottság főtitkára részéről Martine DEPREZ igazgató
Az átvétel dátuma:	2022. március 22.
Címzett:	Jeppe TRANHOLM-MIKKELSEN, az Európai Unió Tanácsának főtitkára
Biz. dok. sz.:	COM(2022) 122 final
Tárgy:	Javaslat – AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE az uniós intézmények, szervek, hivatalok és ügynökségek egységesen magas szintű kiberbiztonságát biztosító intézkedések meghatározásáról

Mellékelten továbbítjuk a delegációknak a COM(2022) 122 final számú dokumentumot.

Melléklet: COM(2022) 122 final

EURÓPAI
BIZOTTSÁG

Brüsszel, 2022.3.22.
COM(2022) 122 final

2022/0085 (COD)

Javaslat

AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE

az uniós intézmények, szervek, hivatalok és ügynökségek egységesen magas szintű kiberbiztonságát biztosító intézkedések meghatározásáról

{SWD(2022) 67 final} - {SWD(2022) 68 final}

INDOKOLÁS

1. A JAVASLAT HÁTTERE

• A javaslat indokai és céljai

Ez a javaslat keretrendszert hoz létre az uniós intézmények, szervek és ügynökségek közös kiberbiztonsági szabályainak és intézkedéseinek biztosítására. Célja, hogy tovább javítsa valamennyi szervezet ellenálló képességét és biztonsági eseményekre való reagálási képességét. Összhangban áll a Bizottság azon prioritásaival, amelyek célja egyfelől Európának a digitális kor kihívásaira való felkészítése, másfelől a jövő kihívásaira felkészült, az emberek javát szolgáló gazdaság kiépítése. Emellett a biztonságos és reziliens közigazgatás biztosítása az egész társadalom digitális átalakulásának egyik sarokköve is.

Ez a javaslat a biztonsági unióra vonatkozó uniós stratégiára (COM(2020) 605 final) és a digitális évtizedre vonatkozó uniós kiberbiztonsági stratégiára (JOIN(2020) 18 final) épül.

A javaslat korszerűsíti a CERT-EU meglévő jogi keretét, és figyelembe veszi az intézmények, szervek és ügynökségek elmúlt években bekövetkezett megváltozott és fokozott digitalizálását, valamint a kiberbiztonsági fenyegetések változó helyzetét. Mindkét fejlemény tovább erősödött a Covid19-válság kezdete óta, miközben a biztonsági események száma továbbra is nő, és a támadások egyre kifinomultabbak, számos forrásból származnak.

A javaslat a CERT-EU-t „hálózatbiztonsági vészhelyzeteket elhárító csoportról” az uniós intézményeknek, szerveknek és ügynökségeknek szóló „kiberbiztonsági központra” nevezi át, összhangban a tagállamokban és világszerte bekövetkezett fejleményekkel, ahol számos CERT-et kiberbiztonsági központnak neveznek át, de a névfelismerés miatt megtartja a „CERT-EU” rövid nevet.

• Összhang a szabályozási terület jelenlegi rendelkezéseivel

E javaslat célja, hogy növelje az uniós intézmények, szervek és ügynökségek kiberbiztonsági ellenálló képességét a kiberfenyegetésekkel szemben, ugyanakkor igazodjon a meglévő jogszabályokhoz:

- (EU) 2016/1148 irányelv a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről. Összhangban van továbbá az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről szóló (EU) XXXX/XXXX irányelvjavaslattal [NIS 2-javaslat].
- (EU) 2019/881 rendelet az Európai Uniós Kiberbiztonsági Ügynökségről és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról (kiberbiztonsági jogszabály).
- Javaslat – (EU) XXXX/XXXX rendelet az uniós intézmények, szervek, hivatalok és ügynökségek információbiztonságáról.
- A Bizottság ajánlása (2021. június 23.) a közös kiberbiztonsági egység létrehozásáról.
- A Bizottság (EU) 2017/1584 ajánlása (2017. szeptember 13.) a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról.

A nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról szóló, 2017. szeptember 13-i (EU) 2017/1584 bizottsági ajánlás melléklete

meghatározza a nagyszabású, határokon átnyúló kiberbiztonsági eseményekre és válsághelyzetekre való koordinált reagálás tervét.

Az Európai Unió Tanácsa 2021. március 9-i állásfoglalásában hangsúlyozta, hogy a kiberbiztonság mind nemzeti, mind uniós szinten létfontosságú a közigazgatás működése, valamint a társadalom és a gazdaság egésze szempontjából, hangsúlyozva egy szilárd és következetes biztonsági keret fontosságát az uniós személyzet, az adatok, a kommunikációs hálózatok, az információs rendszerek és a döntéshozatali folyamatok védelme érdekében. Ezt különösen az uniós intézmények, szervek és ügynökségek fokozott ellenálló képességének és biztonsági kultúrájának javítása révén kell elérni. Elegendő erőforrást és képességet kell rendelkezésre bocsátani, többek között a CERT-EU megbízatásának megerősítésével összefüggésben.

2. JOGALAP, SZUBSZIDIARITÁS ÉS ARÁNYOSSÁG

• Jogalap

E rendelet jogalapja az Európai Unió működéséről szóló szerződés (EUMSZ) 298. cikke, amely előírja, hogy feladataik ellátása során az Unió intézményei, szervei, hivatalai és ügynökségei nyitott, hatékony és független európai igazgatásra támaszkodnak. A 336. cikk alapján elfogadott szabályzat és alkalmazási feltételek tiszteletben tartásával az Európai Parlament és a Tanács – rendes jogalkotási eljárás keretében elfogadott rendeletekben – rendelkezéseket állapít meg ennek érdekében.

Az információs technológia új lehetőségeket kínált az uniós intézmények, szervek és ügynökségek számára a munkavégzésre, a polgárokkal való kapcsolattartásra és az általános műveletek javítására. Ahogy a technológia egyre fejlődik, a kiberfenyegetés-környezet ezzel párhuzamosan szintén folyamatosan változik. Az uniós intézmények, szervek és ügynökségek a kifinomult kibertámadások rendkívül vonzó célpontjai. A kiberbiztonságot biztosító rendszerek és követelmények létrehozása hozzájárulhat az európai közigazgatás hatékonyságához és függetlenségéhez, hogy az uniós intézmények, szervek, hivatalok és ügynökségek feladataik ellátása során hatékonyabban tudjanak működni a digitális világban.

Emellett a kiberbiztonság területén az uniós intézmények, szervek és ügynökségek kiberbiztonsági helyzete és megközelítése közötti jelenlegi különbségek – amint azt az alábbi 3. szakasz kifejti – további akadályt jelentenek a nyitott, hatékony és független európai közigazgatás előtt. Közös megközelítés nélkül az uniós intézmények, szervek és ügynökségek kiberbiztonsági helyzete továbbra is eltérő irányokba fejlődne. Ez a jogalap ezért megfelelő, mivel a rendelet célja a kiberbiztonság közös jogi keretének létrehozása az uniós intézményeken, szerveken, hivatalokon és ügynökségeken belül.

• Szubszidiaritás

Az uniós intézmények, szervek, hivatalok és ügynökségek egységesen magas szintű kiberbiztonságát biztosító intézkedések megállapításáról szóló rendelet az Unió kizárólagos hatáskörébe tartozik.

• Arányosság

Az e rendeletben javasolt szabályok nem lépik túl a konkrét célkitűzések kielégítő eléréséhez szükséges mértéket. A tervezett intézkedések hozzá fognak járulni a kiberbiztonság egységesen magas szintjének eléréséhez anélkül, hogy túllépnék a célkitűzés eléréséhez szükséges mértéket, tekintettel az őket érintő egyre nagyobb kockázatokra.

- **A jogi aktus típusának megválasztása**

A közvetlenül alkalmazandó rendelet a megfelelő jogi eszköz az uniós intézményekre, szervekre és ügynökségekre rótt kötelezettségek meghatározására és észszerűsítésére. A célzott javítások lehetővé tétele érdekében a rendelet a legmegfelelőbb jogi eszköz.

3. AZ ELŐZETES ÉRTÉKELÉSEK, AZ ÉRDEKELT FELEKKEL FOLYTATOTT KONZULTÁCIÓK ÉS A HATÁSVIZSGÁLATOK EREDMÉNYEI

- **Előzetes értékelések**

A CERT-EU elvégezte azon főbb kiberfenyegetések értékelését, amelyeknek az uniós intézmények, szervek és ügynökségek jelenleg ki vannak téve vagy valószínűleg ki lesznek téve a belátható jövőben.

Az elemzés során a megfigyelések három kategóriáját alkalmazták:

- Az uniós intézmények, szervek és ügynökségek informatikai infrastruktúrájának megsértésére irányuló kísérletek (ha sikeresek, biztonsági eseményként kezelik őket, a többi esetben pedig továbbra is felderített kísérletként kerülnek rögzítésre).
- Az uniós intézmények, szervek és ügynökségek közelében (pl. kapcsolódó ágazataikban, érdekelt közösségeikben vagy Európában) észlelt fenyegetések.
- Globálisan megfigyelt főbb fenyegetettségi tendenciák.

Az elemzés továbbá megvizsgálta, hogy a folyamatban lévő jelentős változások hogyan befolyásolják az uniós intézmények informatikai infrastruktúrájának és szolgáltatásainak kezelését és használatát. Az ilyen változások közé tartoznak a következők:

- megnövekedett mértékű távmunka;
- a rendszerek migrációja a felhőbe;
- az informatikai szolgáltatások megnövekedett mértékű kiszervezése.

2019 és 2021 között drámai mértékben megugrott az uniós intézményeket, szerveket és ügynökségeket érintő, fejlett, folyamatos fenyegetést (APT) jelentő szereplők által okozott jelentős biztonsági események[1] száma. 2021 első felében a jelentős biztonsági események száma a 2020-ban mérttel azonos volt. Ezt tükrözi a CERT-EU által 2020-ban elemzett kriminalisztikai képek (az érintett rendszerek vagy eszközök tartalmának pillanatképei) száma is, amely 2019-hez képest megháromszorozódott, míg a jelentős biztonsági események száma 2018 óta több mint tízszeresére nőtt.

2020-ban a CERT-EU irányítóbizottsága új stratégiai célt tűzött ki a CERT-EU számára, hogy átfogó szintű kibervédelmet biztosítson valamennyi intézmény, szerv és ügynökség számára, megfelelő kiterjedéssel és mélységgel, valamint folyamatosan alkalmazkodva a jelenlegi vagy jövőbeli fenyegetésekhez, többek között a mobil eszközök, a felhőalapú környezet és a dolgok internete elleni támadásokhoz.

A CERT-EU fenyegetettségelemzését kiegészítve a Bizottság elvégezte 20 uniós intézmény, szerv és ügynökség kiberbiztonsági működésének értékelését. Ez betekintést nyújtott a bevált

[1] „Jelentős biztonsági esemény”: bármely váratlan esemény, kivéve, ha hatása korlátozott, és a módszer vagy technológia tekintetében valószínűleg már jól ismert.

kiberbiztonsági gyakorlatokba és a kiberbiztonsági irányítási képességekbe, egyes technikai védelmi ellenőrzések külső összehasonlító értékelésével.

Ez az értékelés az intézmények, szervek és ügynökségek által megválaszolt kérdőíveken, a nyilvánosan hozzáférhető adatokon, valamint a közvetlenül az uniós intézmények, szervek és ügynökségek által szolgáltatott adatokon alapult. Elegendő betekintést nyújt a jelenlegi helyzetbe ahhoz, hogy meg lehessen állapítani a következőt:

- A kiberbiztonsági érettség, az IT-infrastruktúra mérete és a képességek szintjei jelentősen eltérnek az értékelés tárgyát képező uniós intézmények, szervek és ügynökségek között.
- Mivel általában véve számos uniós intézmény, szerv és ügynökség fejlett felderítési és reagálási képességgel rendelkezik, kiberbiztonsági irányítási képességeikben eltérő szintű integrált kockázatkezelést alkalmaznak.
- Míg az értékelt uniós intézmények, szervek és ügynökségek kiberbiztonsági keretrendszerei (stratégia, szakpolitika és szabályalap) általánosságban jól megalapozottak a rendelet I. mellékletében felsorolt kulcsfontosságú kiberbiztonsági területeken, egyes uniós intézmények, szervek és ügynökségek nem rendelkeznek kiforrott ügymenet-folytonossági irányítással, megfeleléssel, ellenőrzéssel és folyamatos fejlesztéssel.
- Megállapítást nyert, hogy az értékelt uniós intézmények, szervek és ügynökségek egyenlőtlenül alkalmazzák a bevált gyakorlatoknak tekintett technikai intézkedéseket.

Összefoglalva, a 20 uniós intézmény, szerv és ügynökség elemzése azt mutatja, hogy irányításuk, kiberhigiéniájuk, általános képességük és érettségük széles spektrumban változik. Ezért alapvető fontosságú, hogy valamennyi uniós intézmény, szerv és ügynökség számára előírják a kiberbiztonsági intézkedésekkel kapcsolatos alapkövetelmények végrehajtását, hogy kezelni lehessen ezt az érettségi egyenlőtlenséget, és hogy valamennyi uniós intézmény, szerv és ügynökség egységesen magas kiberbiztonsági szintet érjen el.

Eddig egyetlen uniós jogszabály sem összpontosított az uniós intézmények, szervek és ügynökségek kiberbiztonságára, és átfogóan kezelte a kiberbiztonsági fenyegetések körét és a digitalizáció által előidézett, újonnan felmerülő informatikai kockázatokat.

- **Az érdekelt felekkel folytatott konzultációk**

A Bizottság konzultált az érdekelt felekkel valamennyi uniós intézményben, szervben és ügynökségben, valamint a tagállamok képviselőivel a Tanácsban és az érdekelt felekkel az Európai Parlamentben. 2021. június 25-én a tagállamok képviselői és az uniós intézmények, szervek és ügynökségek érintett érdekelt felei részt vettek a Bizottság által szervezett munkaértekezleten, amelynek célja a jövőbeli rendeletjavaslat tartalmának megvitatása volt.

- **Hatásvizsgálat**

E javaslat az uniós intézményekre, szervekre és ügynökségekre fog kihatni. Emiatt nincs szükség külön hatásvizsgálatra, mivel a javaslat nem fogja érinteni a tagállamokat.

- **Alapvető jogok**

Az Európai Unió elkötelezett amellett, hogy biztosítsa az alapjogok magas szintű védelmét. Az e rendeleten alapuló minden információmegosztásra megbízható környezetben kerülne sor, teljes mértékben tiszteletben tartva a személyes adatok védelméhez való jogot, amelyet az Európai Unió Alapjogi Chartájának 8. cikke és a vonatkozó adatvédelmi jogszabályok, nevezetesen az (EU) 2018/1725 európai parlamenti és tanácsi rendelet rögzít.

4. KÖLTSÉGVETÉSI VONZATOK

A piaci referenciaértékek és tanulmányok[2] azt mutatják, hogy a közvetlen kiberbiztonsági kiadások általában a szervezetek összesített informatikai kiadásainak 4–7 %-át teszik ki. A CERT-EU által e jogalkotási javaslat alátámasztására végzett fenyegetettségelemzés azonban azt mutatja, hogy a nemzetközi szerveknek és a politikai szervezeteknek fokozott kockázatokkal kell szembenézniük, ezért a kiberbiztonságra fordított informatikai kiadások 10 %-os szintje megfelelőbb célnak tűnik. Az ilyen erőfeszítések pontos költsége nem határozható meg, mivel nem állnak rendelkezésre részletes információk az uniós intézmények, szervek és ügynökségek informatikai kiadásairól, valamint a kiberbiztonsági kiadások vonatkozó arányáról.

Bár ezért valószínű, hogy számos uniós intézmény, szerv és ügynökség kevesebbet költ a kiberbiztonságra, mint amennyit kellene, ez a rendelet önmagában nem fogja az aktuális kiadások növekedését okozni. Még a rendelet nélkül is minden szervezetnek biztosítania kellene a kiberbiztonság megfelelő szintjét. A rendelet folytatja a CERT-EU irányítóbizottságában folytatott korábbi együttműködést, és formalizálja az információcsere azon szintjét, amely részben már ma is létezik. A pénzügyi kimutatásban foglaltaknak megfelelően a CERT-EU-nak további forrásokra lesz szüksége kibővített szerepének betöltéséhez, és ezeket a forrásokat a CERT-EU szolgáltatásait igénybe vevő uniós intézményektől, szervektől és ügynökségektől kell átcsoportosítani.

5. EGYÉB ELEMEK

- **Végrehajtási, nyomonkövetési, értékelési és jelentéstételi intézkedések**

Az Intézményközi Kiberbiztonsági Testületnek (IICB) a CERT-EU segítségével felül kell vizsgálnia e rendelet működését, értékeléseket kell végeznie, és a megállapításait tartalmazó jelentést be kell nyújtania a Bizottságnak. A Bizottságnak biztosítania kell az Európai Parlament, a Tanács, az Európai Gazdasági és Szociális Bizottság és a Régiók Bizottsága részére történő rendszeres jelentéstételt.

A CERT-EU útmutatóra vagy ajánlásra vonatkozó javaslatot dolgozhat ki, amelyet az IICB elfogadhat. Az útmutató az uniós intézmények, szervek és ügynökségek egészére vagy egy részhalmazára irányuló tanácsadó dokumentum, míg az ajánlás az egyes uniós intézményekre, szervekre és ügynökségekre vonatkozik. A cselekvési felhívás egy CERT-EU tanácsadó dokumentum, amely ismerteti azokat a sürgős biztonsági intézkedéseket, amelyeket az uniós intézményeknek, szerveknek és ügynökségeknek meghatározott időn belül meg kell hozniuk.

- **A rendelet konkrét rendelkezéseinek részletes ismertetése**

Általános rendelkezések

A rendelet intézkedéseket állapít meg a kiberbiztonság egységesen magas szintjének biztosítása érdekében, és az uniós intézményekre, szervekre és ügynökségekre alkalmazandó annak érdekében, hogy azok nyílt, hatékony és független módon végezhessék feladataikat. (1–3. cikk és 23–25. cikk)

[2] Forrás: Gartner: Identifying the Real Information Security Budget (A valós információbiztonsági költségvetés azonosítása), 2016. Ez kiegészíti az informatikai biztonságra fordított közvetett kiadásokat, többek közt a hálózatbiztonságra, például a tűzfalakra, a vírusirtókra és a rendszertulajdonosi feladatokra, például a kockázatértékelésre és a védelmi ellenőrzések végrehajtására fordított kiadásokat. Egy 2020. évi dokumentum szerint a pénzügyi intézmények kiberbiztonsági kiadásai az informatikai kiadások 10–11 %-át teszik ki, forrás: DI_2020-FS-ISAC-Cybersecurity.pdf (deloitte.com).

A kiberbiztonság egységesen magas szintjére irányuló intézkedések

Az uniós intézmények, szervek és ügynökségek kötelesek létrehozni egy olyan belső kiberbiztonsági kockázatkezelési, -irányítási és -ellenőrzési keretrendszert, amely biztosítja az összes kiberbiztonsági kockázat hatékony és prudens kezelését. Az intézményeknek, szerveknek és ügynökségeknek továbbá kiberbiztonsági alapkövetelményeket kell elfogadniuk a keretrendszerben azonosított kockázatok kezelésére, rendszeres kiberbiztonsági érettségi értékeléseket kell végezniük, és kiberbiztonsági tervet kell elfogadniuk. (4–8. cikk)

Intézményközi Kiberbiztonsági Testület

Létrejön az Intézményközi Kiberbiztonsági Testület, amely felelős e rendelet uniós intézmények, szervek és ügynökségek általi végrehajtásának nyomon követéséért, az általános prioritások és célkitűzések CERT-EU általi végrehajtásának felügyeletéért, valamint a CERT-EU stratégiai irányításáért. (9–11. cikk)

CERT-EU

A CERT-EU hozzájárul valamennyi uniós intézmény, szerv és ügynökség informatikai környezetének biztonságához azáltal, hogy tanácsadást nyújt számukra, segíti a biztonsági események megelőzését, észlelését, enyhítését és az azokra való reagálást, valamint azáltal, hogy kiberbiztonsági információcserére és eseményreagálási koordinációra szolgáló központként működik. (12–17. cikk)

Együttműködési és jelentéstételi kötelezettségek

A rendelet biztosítja a CERT-EU, valamint az uniós intézmények, szervek és ügynökségek közötti együttműködést és információcserét a bizalom növelése érdekében. E célból a CERT-EU felkérheti az uniós intézményeket, szerveket és ügynökségeket, hogy bocsássák rendelkezésére a vonatkozó információkat, továbbá az érintett védett szervezet beleegyezése nélkül biztonsági eseményekre vonatkozó információkat cserélhet az uniós intézményekkel, szervekkel és ügynökségekkel annak érdekében, hogy megkönnyítse a hasonló kiberfenyegetések vagy -események felderítését. A CERT-EU csak az érintett védett szervezet beleegyezésével cserélhet olyan biztonságiesemény-specifikus információkat, amelyek feltárják a kiberbiztonsági esemény célpontját.

Nevezetesen valamennyi uniós intézménynek, szervnek és ügynökségnek indokolatlan késedelem nélkül, de legkésőbb 24 órával azt követően, hogy tudomást szerzett róla, értesítenie kell a CERT-EU-t a jelentős kiberfenyegetésekről, a jelentős sebezhetőségekről és a jelentős biztonsági eseményekről. (18–22. cikk)

2022/0085 (COD)

Javaslat

AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE

az uniós intézmények, szervek, hivatalok és ügynökségek egységesen magas szintű kiberbiztonságát biztosító intézkedések meghatározásáról

AZ EURÓPAI PARLAMENT ÉS AZ EURÓPAI UNIÓ TANÁCSA,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 298. cikkére,

tekintettel az Európai Atomenergia-közösséget létrehozó szerződésre és különösen annak 106a. cikkére,

tekintettel az Európai Bizottság javaslatára,

a jogalkotási aktus tervezetének a nemzeti parlamenteknek való továbbítását követően,

rendes jogalkotási eljárás keretében,

mivel:

(1) A digitális korban az információs és kommunikációs technológia a nyitott, hatékony és független uniós közigazgatás sarokköve. A fejlődő technológia és a digitális rendszerek fokozódó összetettsége és összeköttetése növeli a kiberbiztonsági kockázatokat, ami az uniós közigazgatást még sérülékenyebbé teszi a kiberfenyegetésekkel és biztonsági eseményekkel szemben, ami végeredményben veszélyezteti a közigazgatás ügymenet-folytonosságát és az adatai biztosítására irányuló képességét. Míg a felhőalapú szolgáltatások fokozott használata, az informatika mindenütt elterjedt használata, a nagyarányú digitalizáció, a távmunka, valamint a fejlődő technológia és konnektivitás manapság az uniós igazgatási szervek valamennyi tevékenységének alapvető jellemzői, a digitális rezilienciát még nem építették be kellőképpen munkájukba.

(2) Az uniós intézményeket, szerveket és ügynökségeket érintő kiberfenyegetések helyzete folyamatosan változik. A fenyegető szereplők által alkalmazott taktikák, technikák és eljárások folyamatosan változnak, míg az ilyen támadások elsőrendű indítékai az értékes, nyilvánosságra nem hozott információk ellopásától kezdve a pénzszerzésig, a közvélemény manipulálásáig vagy a digitális infrastruktúra aláásásáig változatlanok. Egyre gyorsabb ütemben hajtanak végre kibertámadásokat, miközben kampányaik egyre kifinomultabbak és automatizáltabbak, a fenyegetéseknek kitett támadási felületeket célozzák, egyre bővülnek és gyorsan kihasználják a sebezhetőségeket.

(3) Az uniós intézmények, szervek és ügynökségek informatikai környezetében kölcsönös függőségek és integrált adatáramlások fordulnak elő, felhasználóik pedig szorosan együttműködnek. Ez az összekapcsoltság azt jelenti, hogy bármilyen zavarnak – akkor is, ha eredetileg csak egy uniós intézményre, szervre vagy ügynökségre korlátozódik – szélesebb körben lépcsőzetes hatásai lehetnek, ami messzemenő és hosszú távú negatív hatásokat eredményezhet a többire nézve. Emellett egyes intézmények, szervek és ügynökségek informatikai környezete összekapcsolódik a tagállamok informatikai környezetével, ami az egyik uniós szervezetnél felmerülő biztonsági

esemény miatt kockázatot jelenthet a tagállamok informatikai környezeteinek kiberbiztonságára nézve, és fordítva.

(4) Az uniós intézmények, szervek és ügynökségek vonzó célpontok, akik magasan képzett és megfelelő erőforrásokkal rendelkező fenyegető szereplőkkel, valamint egyéb fenyegetésekkel szembesülnek. A kibertámadásokkal szembeni ellenálló képesség szintje és érettsége és a rossz szándékú kibertevékenységek felderítésére és az azokra való reagálásra irányuló képesség ugyanakkor jelentős mértékben eltér a szervezetek között. Ezért az európai közigazgatás működéséhez szükséges, hogy az uniós intézmények, szervek és ügynökségek egységesen magas szintű kiberbiztonságot érjenek el olyan kiberbiztonsági minimumszabályok („kiberbiztonsági alapkövetelmények”) révén, amelyeknek a hálózati és információs rendszereknek, valamint üzemeltetőiknek és felhasználóiknak meg kell felelniük a kiberbiztonsági kockázatok minimalizálása, valamint az információcsere és az együttműködés érdekében.

(5) A kiberbiztonság Unió-szerte egységesen magas szintjét biztosító intézkedésekről szóló irányelv [NIS 2-javaslat] célja az állami és magánszervezetek, az illetékes nemzeti hatóságok és szervek, valamint az egész Unió kiberbiztonsági ellenálló képességének és biztonsági eseményekre való reagálási képességének további javítása. Ezért szükséges, hogy az uniós intézmények, szervek és ügynökségek hasonló szellemben cselekedjenek azáltal, hogy olyan szabályokat biztosítanak, amelyek összhangban vannak az irányelvvel [a NIS 2-javaslattal], és tükrözik annak ambíciószintjét.

(6) A kiberbiztonság egységesen magas szintjének elérése érdekében minden uniós intézménynek, szervnek és ügynökségnek olyan belső kiberbiztonsági kockázatkezelési, -irányítási és -ellenőrzési keretrendszert kell létrehoznia, amely biztosítja az összes kiberbiztonsági kockázat hatékony és prudens kezelését, és figyelembe veszi az ügymenet-folytonosságot és a válságkezelést.

(7) Az uniós intézmények, szervek és ügynökségek közötti különbségek rugalmasságot tesznek szükségessé a végrehajtás terén, mivel az egységes megközelítés nem illik minden szervezetre. A kiberbiztonság egységesen magas szintjére vonatkozó intézkedések nem tartalmazhatnak olyan kötelezettségeket, amelyek közvetlenül ütköznek az uniós intézmények, szervek és ügynökségek feladatainak ellátásával, vagy beavatkoznak intézményi autonómiájukba. Ezért ezeknek az intézményeknek, szerveknek és ügynökségeknek létre kell hozniuk a kiberbiztonsági kockázatkezelésre, -irányításra és -ellenőrzésre vonatkozó saját keretrendszereiket, és el kell fogadniuk saját alapkövetelményeiket és kiberbiztonsági terveiket.

(8) Annak elkerülése érdekében, hogy az uniós intézményekre, szervekre és ügynökségekre aránytalanul nagy pénzügyi és adminisztratív terhek háruljanak, a kiberbiztonsági kockázatok kezelésére vonatkozó követelményeknek – a legújabb technikai lehetőségekre figyelemmel – arányosaknak kell lenniük az adott hálózati és információs rendszert érintő kockázatokkal. Minden uniós intézménynek, szervnek és ügynökségnek törekednie kell arra, hogy informatikai költségvetésének megfelelő százalékát a kiberbiztonság szintjének javítására fordítsa; hosszabb távon 10 %-os nagyságrendű célkitűzés elérésére törekedve.

(9) A kiberbiztonság egységesen magas szintje megköveteli, hogy a kiberbiztonság az egyes uniós intézmények, szervek és ügynökségek legmagasabb szintű vezetésének felügyelete alá tartozzon, amelynek jóvá kell hagynia az egyes intézmények, szervek és ügynökségek által létrehozandó keretrendszerben azonosított kockázatok kezelésére

szolgáló kiberbiztonsági alapkövetelményeket. A kiberbiztonsági kultúra, azaz a kiberbiztonság napi gyakorlatának kezelése valamennyi uniós intézmény, szerv és ügynökség kiberbiztonsági alapkövetelményeinek szerves részét képezi.

(10) Az uniós intézményeknek, szerveknek és ügynökségeknek fel kell mérniük a beszállítókkal és szolgáltatókkal – többek között az adattárolási és -kezelési szolgáltatások nyújtóival vagy az irányított biztonsági szolgáltatásokkal – fenntartott kapcsolatokból eredő kockázatokat, és megfelelő intézkedéseket kell hozniuk azok kezelésére. Ezeknek az intézkedéseknek a kiberbiztonsági alapkövetelmények részét kell képezniük, és azokat a CERT-EU által kiadott útmutatókban vagy ajánlásokban részletesebben meg kell határozni. Az intézkedések és iránymutatások meghatározásakor megfelelően figyelembe kell venni a vonatkozó uniós jogszabályokat és szakpolitikákat, többek között a Kiberbiztonsági Együttműködési Csoport által kiadott kockázatértékeléseket és ajánlásokat, például az összehangolt uniós kockázatértékelést és az 5G kiberbiztonságra vonatkozó uniós eszköztárat. Emellett az (EU) 2019/881 rendelet 49. cikke alapján elfogadott konkrét uniós kiberbiztonsági tanúsítási rendszerek keretében szükség lehet a releváns IKT-termékek, -szolgáltatások és -folyamatok tanúsítására.

(11) 2011 májusában az uniós intézmények és szervek főtitkárai úgy határoztak, hogy létrehozzák az uniós intézmények, szervek és ügynökségek számítógépes vészhelyzeteket elhárító csoportjának (CERT-EU) előkészítő csoportját, amelyet egy intézményközi irányítóbizottság felügyel. 2012 júliusában a főtitkárok megerősítették a gyakorlati intézkedéseket, és megállapodtak abban, hogy a CERT-EU-t megtartják állandó szervezetként annak érdekében, hogy továbbra is segítsen javítani az uniós intézmények, szervek és ügynökségek információtechnológiai biztonságának általános szintjét, a kiberbiztonság terén folytatott, látható intézményközi együttműködés példájaként. 2012 szeptemberében az Európai Bizottság intézményközi megbízatással rendelkező munkacsoportjaként létrehozták a CERT-EU-t. 2017 decemberében az uniós intézmények és szervek intézményközi megállapodást kötöttek a CERT-EU szervezetéről és működéséről[3]. E megállapodást tovább kell fejleszteni e rendelet végrehajtásának támogatása érdekében.

(12) A CERT-EU-t a „számítógépes vészhelyzeteket elhárító csoportról” az uniós intézményeket, szerveket és ügynökségeket támogató „kiberbiztonsági központra” kell átnevezni, összhangban a tagállamokban és világszerte bekövetkezett fejleményekkel, ahol számos CERT-et kiberbiztonsági központnak neveznek át, de a névfelismerés céljából meg kell tartani a „CERT-EU” rövid nevet.

(13) Számos kibertámadás olyan szélesebb körű kampányok részét képezi, amelyek az uniós intézmények, szervek és ügynökségek csoportjait, illetve az uniós intézményeket, szerveket és ügynökségeket is magukban foglaló érdekközösségeket célozzák. A proaktív felderítés, a biztonsági eseményekre való reagálás vagy az enyhítő intézkedések lehetővé tétele érdekében az uniós intézményeknek, szerveknek és ügynökségeknek értesíteniük kell a CERT-EU-t a jelentős kiberfenyegetésekről, a jelentős sebezhetőségekről és a jelentős biztonsági eseményekről, és meg kell osztaniuk azokat a megfelelő technikai részleteket, amelyek lehetővé teszik a más uniós intézményekben, szervekben és ügynökségekben előforduló, hasonló kiberfenyegetések, sebezhetőségek és biztonsági események észlelését vagy enyhítését, valamint az azokra való reagálást. Az irányelvben [a NIS 2-javaslatban]

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

tervezettel megegyező megközelítést követve, amennyiben a szervezetek jelentős biztonsági eseményről szereznek tudomást, elő kell írni számukra, hogy 24 órán belül nyújtsanak be kezdeti értesítést a CERT-EU-nak. Az ilyen információcserének lehetővé kell tennie a CERT-EU számára, hogy továbbítsa az információkat más uniós intézményeknek, szerveknek és ügynökségeknek, valamint a megfelelő partnereknek, hogy segítsen megvédeni az uniós informatikai környezetet és az uniós partnerek informatikai környezetét a hasonló eseményekkel, fenyegetésekkel és sebezhetőségekkel szemben.

(14) A CERT-EU több feladattal és kibővített szereppel való felruházása mellett létre kell hozni egy intézményközi kiberbiztonsági testületet (IICB), amelynek elő kell segítenie a kiberbiztonság egységesen magas szintjének megteremtését az uniós intézmények, szervek és ügynökségek körében azáltal, hogy nyomon követi e rendelet uniós intézmények, szervek és ügynökségek általi végrehajtását, felügyeli az általános prioritások és célkitűzések CERT-EU általi végrehajtását, és stratégiai iránymutatást nyújt a CERT-EU számára. Az IICB-nek biztosítania kell az intézmények képviseletét, és magában kell foglalnia az ügynökségek és szervek képviselőit az uniós ügynökségek hálózatán keresztül.

(15) A CERT-EU-nak támogatnia kell a kiberbiztonság egységesen magas szintjét célzó intézkedések végrehajtását az IICB-nek szóló útmutató dokumentumokra és ajánlásokra irányuló javaslatok vagy cselekvési felhívások közzététele révén. Az ilyen iránymutatásokat tartalmazó dokumentumokat és ajánlásokat az IICB-nek jóvá kell hagynia. Szükség esetén a CERT-EU-nak cselekvési felhívásokat kell közzétennie, amelyek ismertetik azokat a sürgős biztonsági intézkedéseket, amelyeket az uniós intézményeknek, szerveknek és ügynökségeknek meghatározott időn belül meg kell hozniuk.

(16) Az IICB-nek nyomon kell követnie az e rendeletnek való megfelelést, továbbá nyomon kell követnie az iránymutatásokat tartalmazó dokumentumokat és ajánlásokat, valamint a CERT-EU által kiadott cselekvési felhívásokat. Az IICB-t technikai kérdésekben az IICB által megfelelőnek tartott technikai tanácsadó csoportoknak kell támogatniuk, amelyeknek szükség esetén szorosan együtt kell működniük a CERT-EU-val, az uniós intézményekkel, szervekkel és ügynökségekkel, valamint más érdekelt felekkel. Szükség esetén az IICB-nek nem kötelező erejű figyelmeztetéseket kell kiadnia, és ellenőrzéseket kell javasolnia.

(17) A CERT-EU feladata, hogy hozzájáruljon valamennyi uniós intézmény, szerv és ügynökség informatikai környezetének biztonságához. A CERT-EU-nak az uniós intézmények, szervek és ügynökségek kijelölt koordinátoraként kell eljárnia, az irányelv [a NIS 2-javaslat] 6. cikkében említett, az európai biztonságirés-nyilvántartásban való összehangolt sebezhetőségfeltárás céljából.

(18) 2020-ban a CERT-EU irányítóbizottsága új stratégiai célt tűzött ki a CERT-EU számára, miszerint átfogó szintű kibervédelmet kell biztosítania valamennyi uniós intézmény, szerv és ügynökség számára, megfelelő kiterjedéssel és mélységgel, valamint folyamatosan alkalmazkodva a jelenlegi vagy jövőbeli fenyegetésekhez, többek között a mobil eszközök, a felhőalapú környezet és a dolgok internete elleni támadásokhoz. A stratégiai cél magában foglalja továbbá a hálózatokat nyomon követő, széles spektrumú biztonsági műveleti központokat (SOC-ok), valamint a súlyos fenyegetések napi 24 órában történő nyomon követését. A nagyobb uniós intézmények, szervek és ügynökségek esetében a CERT-EU-nak támogatnia kell az informatikai biztonsági csoportjaikat, többek között a hét minden napján, napi 24

órában végzett nyomon követés révén. A kisebb és egyes közepes méretű uniós intézmények, szervek és ügynökségek számára a CERT-EU-nak valamennyi szolgáltatást biztosítania kell.

(19) A CERT-EU-nak az irányelvben [a NIS 2-javaslatban] meghatározott további, a számítógép-biztonsági eseményekre reagáló csoportok (CSIRT-ek) hálózatával való együttműködésre és információcserére irányuló szerepét is be kell töltenie. Emellett az (EU) 2017/1584 bizottsági ajánlással[4] összhangban a CERT-EU-nak együtt kell működnie és koordinálnia kell a reagálást az érintett érdekelt felekkel. Annak érdekében, hogy Unió-szerte hozzá tudjon járulni a magas szintű kiberbiztonsághoz, a CERT-EU-nak meg kell osztania a biztonsági eseményekre vonatkozó információkat a nemzeti partnerekkel. A CERT-EU-nak más állami és magánpartnerekkel is együtt kell működnie, többek között a NATO-ban, az IICB előzetes jóváhagyásával.

(20) Az operatív kiberbiztonság támogatása során a CERT-EU-nak az (EU) 2019/881 európai parlamenti és tanácsi rendeletben[5] előírt strukturált együttműködés révén fel kell használnia az Európai Uniós Kiberbiztonsági Ügynökség rendelkezésre álló szakértelmét. Adott esetben a két szervezet között külön megállapodásokat kell kialakítani az együttműködés gyakorlati megvalósításának meghatározása és a párhuzamos tevékenységek elkerülése érdekében. A CERT-EU-nak együtt kell működnie az Európai Uniós Kiberbiztonsági Ügynökséggel a fenyegetettségelemzés terén, és rendszeresen meg kell osztania az Ügynökséggel a fenyegetettségi helyzetjelentését.

(21) A 2021. június 23-i bizottsági ajánlással[6] összhangban létrehozott közös kiberbiztonsági egység támogatása céljából a CERT-EU-nak együtt kell működnie és információkat kell megosztania az érdekelt felekkel az operatív együttműködés előmozdítása és annak lehetővé tétele érdekében, hogy a meglévő hálózatok teljes mértékben kiaknázhassák az Unió védelme terén bennük rejlő lehetőségeket.

(22) Az e rendelet alapján kezelt személyes adatok kezelését az (EU) 2018/1725 európai parlamenti és tanácsi rendeletnek[7] megfelelően kell végezni.

(23) A CERT-EU és az uniós intézmények, szervek és ügynökségek általi információkezelésnek összhangban kell lennie a rendeletben [az információbiztonságról szóló rendeletjavaslatban] meghatározott szabályokkal. A biztonsági kérdésekkel kapcsolatos koordináció biztosítása érdekében a nemzeti biztonsági és hírszerző szolgálatok által a CERT-EU-val kezdeményezett vagy kért kapcsolattartásról indokolatlan késedelem nélkül tájékoztatni kell a Bizottság Biztonsági Igazgatóságát és az IICB elnökét.

(24) Mivel a CERT-EU szolgáltatásai és feladatai valamennyi uniós intézmény, szerv és ügynökség érdekét szolgálják, az informatikai kiadásokkal rendelkező valamennyi

---

4 A Bizottság (EU) 2017/1584 ajánlása (2017. szeptember 13.) a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról (HL L 239., 2017.9.19., 36. o.).

5 Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) (HL L 151., 2019.6.7., 15. o.).

6 A Bizottság C(2021) 4520 ajánlása (2021. június 23.) a közös kiberbiztonsági egység létrehozásáról.

7 Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről (HL L 295., 2018.11.21., 39. o.).

uniós intézménynek, szervnek és ügynökségnek méltányos részt kell vállalnia e szolgáltatások és feladatok finanszírozásából. Ezek a hozzájárulások nem érintik az uniós intézmények, szervek és ügynökségek költségvetési autonómiáját.

(25) Az IICB-nek a CERT-EU segítségével felül kell vizsgálnia és értékelnie kell e rendelet végrehajtását, és megállapításairól jelentést kell tennie a Bizottságnak. Erre a hozzájárulásra építve a Bizottságnak jelentést kell tennie az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának,

ELFOGADTA EZT A RENDELETET:

I. fejezet
ÁLTALÁNOS RENDELKEZÉSEK

1. cikk
Tárgy

Ez a rendelet meghatározza az alábbiakat:

a) az uniós intézmények, szervek és ügynökségek kötelezettségei a belső kiberbiztonságikockázat-kezelési, -irányítási és -ellenőrzési keretrendszerük létrehozása kapcsán;

b) az uniós intézmények, szervek és ügynökségek kötelezettségei a kiberbiztonsági kockázatok kezelése és jelentése kapcsán;

c) az uniós intézmények, szervek és ügynökségek kiberbiztonsági központjának (CERT-EU) szervezetére és működésére, valamint az Intézményközi Kiberbiztonsági Testület szervezetére és működésére vonatkozó szabályok.

2. cikk
Hatály

Ez a rendelet a kiberbiztonsági kockázatok valamennyi uniós intézmény, szerv és ügynökség általi kezelésére, irányítására és ellenőrzésére, valamint a CERT-EU és az Intézményközi Kiberbiztonsági Testület szervezetére és működésére alkalmazandó.

3. cikk
Fogalommeghatározások

E rendelet alkalmazásában:

1. „uniós intézmények, szervek és ügynökségek”: az Európai Unióról szóló szerződés, az Európai Unió működéséről szóló szerződés vagy az Európai Atomenergia-közösséget létrehozó szerződés által vagy ezek alapján létrehozott uniós intézmények, szervek és ügynökségek;

2. „hálózati és információs rendszer”: az irányelv [a NIS 2-javaslat] 4. cikkének 1. pontjában meghatározott hálózati és információs rendszer;

3. „hálózati és információs rendszerek biztonsága”: az irányelv [a NIS 2-javaslat] 4. cikkének 2. pontjában meghatározott hálózati és információs rendszerek biztonsága;

4. „kiberbiztonság”: az irányelv [a NIS 2-javaslat] 4. cikkének 3. pontja értelmében vett kiberbiztonság;

5. „legmagasabb vezetői szint”: vezető személy, vezető vagy koordináló és felügyeleti testület a legmagasabb közigazgatási szinten, figyelembe véve az egyes uniós intézmények, szervek vagy ügynökségek magas szintű irányításának felépítését;

6. „biztonsági esemény”: az irányelv [a NIS 2-javaslat] 4. cikkének 5. pontja értelmében vett biztonsági esemény;

7. „jelentős biztonsági esemény”: bármely váratlan esemény, kivéve, ha hatása korlátozott, és módszer vagy technológia tekintetében valószínűleg már jól érthető;

8. „súlyos támadás”: minden olyan esemény, amely az érintett uniós intézménynél, szervnél vagy ügynökségnél és a CERT-EU-nál rendelkezésre állónál több erőforrást igényel;

9. „biztonsági esemény kezelése”: az irányelv [a NIS 2-javaslat] 4. cikkének 6. pontja értelmében vett eseménykezelés;

10. „kiberfenyegetés”: az (EU) 2019/881 rendelet 2. cikkének 8. pontja értelmében vett kiberfenyegetés;

11. „jelentős kiberfenyegetés”: jelentős biztonsági esemény előidézésére irányuló szándékkal, lehetőséggel és képességgel rendelkező kiberfenyegetés;

12. „sebezhetőség”: az irányelv [a NIS 2-javaslat] 4. cikkének 8. pontja értelmében vett biztonsági rés;

13. „jelentős sebezhetőség”: olyan sebezhetőség, amely kihasználása esetén valószínűsíthetően jelentős biztonsági eseményhez vezet;

14. „kiberbiztonsági kockázat”: minden olyan észszerűen azonosítható körülmény vagy esemény, amely kedvezőtlen hatást gyakorolhat a hálózati és információs rendszerek biztonságára;

15. „közös kiberbiztonsági egység”: az Unió különböző kiberbiztonsági közösségei közötti együttműködés virtuális és fizikai platformja, amely a 2021. június 23-i bizottsági ajánlás szerinti, határokon átnyúló jelentős kiberfenyegetések és biztonsági események elleni operatív és technikai koordinációra összpontosít;

16. „kiberbiztonsági alapkövetelmények”: kiberbiztonsági minimumszabályok, amelyeknek a hálózati és információs rendszereknek, valamint üzemeltetőiknek és felhasználóiknak meg kell felelniük a kiberbiztonsági kockázatok minimalizálása érdekében.

II. fejezet
A KIBERBIZTONSÁG EGYSÉGESEN MAGAS SZINTJÉRE IRÁNYULÓ INTÉZKEDÉSEK

4. cikk
Kockázatkezelés, -irányítás és -ellenőrzés

(1) A szervezet küldetésének támogatása érdekében, saját intézményi autonómiáját gyakorolva minden uniós intézmény, szerv és ügynökség létrehozza saját belső kiberbiztonsági kockázatkezelési, -irányítási és -ellenőrzési keretrendszerét (a továbbiakban: keretrendszer). Ezt a munkát a szervezet legmagasabb szintű vezetése

felügyeli az összes kiberbiztonsági kockázat hatékony és prudens kezelésének biztosítása érdekében. E keretrendszert legkésőbb [15 hónappal e rendelet hatálybalépését követően]-ig be kell vezetni.

(2) A keretrendszernek ki kell terjednie az érintett intézmény, szerv vagy ügynökség teljes informatikai környezetére, beleértve a helyszíni informatikai környezetet, a felhőalapú számítástechnikai környezetben működő vagy harmadik felek által üzemeltetett, kiszervezett eszközöket és szolgáltatásokat, a mobil eszközöket, a vállalati hálózatokat, az internethez nem kapcsolódó üzleti hálózatokat és az informatikai környezethez kapcsolódó eszközöket. A keretrendszernek figyelembe kell vennie az ügymenet-folytonosságot, a válságkezelést és az ellátási lánc biztonságát, valamint az olyan emberi kockázatok kezelését, amelyek hatással lehetnek az érintett uniós intézmény, szerv vagy ügynökség kiberbiztonságára.

(3) Az egyes uniós intézmények, szervek és ügynökségek legmagasabb szintű vezetése felügyeli, hogy szervezetük megfelel-e a kiberbiztonsági kockázatkezeléssel, -irányítással és -ellenőrzéssel kapcsolatos kötelezettségeknek, ami nem érinti a vezetés más szintjeinek a megfeleléssel és a kockázatkezeléssel kapcsolatos formális felelősségét a felelősségi körükbe tartozó területeken.

(4) Minden uniós intézménynek, szervnek és ügynökségnek hatékony mechanizmusokkal kell rendelkeznie annak biztosítására, hogy az informatikai költségvetés megfelelő százalékát a kiberbiztonságra fordítsák.

(5) Minden uniós intézmény, szerv és ügynökség helyi kiberbiztonsági tisztviselőt vagy azzal egyenértékű funkciót nevez ki, aki a kiberbiztonság valamennyi vonatkozása tekintetében egyedüli kapcsolattartó pontként jár el.

5. cikk
Kiberbiztonsági alapkövetelmények

(1) Az egyes uniós intézmények, szervek és ügynökségek legmagasabb vezetői szintje jóváhagyja a szervezet saját kiberbiztonsági alapkövetelményeit, melyek a 4. cikk (1) bekezdésében említett keretrendszerben azonosított kockázatok kezelésére szolgálnak. Mindezt a szervezet küldetésének támogatása érdekében és a szervezet intézményi autonómiájának gyakorolva kell végrehajtani. A kiberbiztonsági alapkövetelményeket legkésőbb [18 hónappal e rendelet hatálybalépését követően]-ig ki kell dolgozni, és a követelményeknek ki kell terjedniük az I. mellékletben felsorolt területekre és a II. mellékletben felsorolt intézkedésekre.

(2) Az egyes uniós intézmények, szervek és ügynökségek felső vezetése rendszeresen képzéseken vesz részt azon ismeretek és készségek elsajátítása érdekében, amelyek a kiberbiztonsági kockázatok és irányítási gyakorlatok, valamint az azok által a szervezet működésére gyakorolt hatások megismeréséhez és értékeléséhez szükségesek.

6. cikk
Érettségi értékelések

Minden uniós intézmény, szerv és ügynökség legalább háromévente kiberbiztonsági érettségi értékelést végez, amelynek ki kell terjednie informatikai környezetük 4. cikkben leírt valamennyi elemére, figyelembe véve a 13. cikkel összhangban elfogadott vonatkozó iránymutatásokat és ajánlásokat.

7. cikk

Kiberbiztonsági tervek

(1) Az érettségi értékelésből levont következtetéseket követően, valamint a 4. cikk szerint azonosított eszközök és kockázatok figyelembevételével az egyes uniós intézmények, szervek és ügynökségek legmagasabb szintű vezetése a kockázatkezelési, -irányítási és -ellenőrzési keretrendszer, valamint a kiberbiztonsági alapkövetelmények kidolgozását követően indokolatlan késedelem nélkül jóváhagyja a kiberbiztonsági tervet. A terv az érintett szervezet általános kiberbiztonságának növelésére irányul, és ezáltal hozzájárul az összes uniós intézmény, szerv és ügynökség egységesen magas szintű kiberbiztonságának eléréséhez vagy javításához. A szervezet intézményi autonómiájára építve és a szervezet küldetésének támogatása érdekében a tervnek tartalmaznia kell legalább az I. mellékletben felsorolt területeket, a II. mellékletben felsorolt intézkedéseket, valamint a biztonsági eseményekre való felkészültséggel, reagálással és helyreállítással kapcsolatos intézkedéseket, például a biztonsági megfigyelést és naplózást. A terv felülvizsgálatára a 6. cikk szerint elvégzett érettségi értékeléseket követően legalább háromévente kerül sor.

(2) A kiberbiztonsági tervek tartalmaznia kell a személyzet tagjainak a terv végrehajtásával kapcsolatos szerepét és felelősségi körét.

(3) A kiberbiztonsági terv figyelembe veszi a CERT-EU által kiadott alkalmazandó iránymutatásokat és ajánlásokat.

8. cikk

Végrehajtás

(1) Az érettségi értékelések elvégzését követően az uniós intézmények, szervek és ügynökségek benyújtják ezeket az Intézményközi Kiberbiztonsági Testületnek. A biztonsági tervek elkészítését követően az uniós intézmények, szervek és ügynökségek értesítik az Intézményközi Kiberbiztonsági Testületet azok befejezéséről. A Testület kérésére jelentést tesznek e fejezet egyes vonatkozásairól.

(2) Az e fejezetben megállapított rendelkezések végrehajtását a 13. cikkel összhangban kiadott iránymutatásokat tartalmazó dokumentumokkal és ajánlásokkal kell támogatni.

III. fejezet
INTÉZMÉNYKÖZI KIBERBIZTONSÁGI TESTÜLET

9. cikk

Intézményközi Kiberbiztonsági Testület

(1) Létrejön az Intézményközi Kiberbiztonsági Testület (IICB).

(2) Az IICB felelős az alábbiakért:

a) e rendelet uniós intézmények, szervek és ügynökségek általi végrehajtásának nyomon követése;

b) az általános prioritások és célkitűzések CERT-EU általi végrehajtásának felügyelete és stratégiai irányítás biztosítása a CERT-EU számára.

(3) Az IICB tagjai a következők: három képviselő, akiket az uniós ügynökségek hálózata (EUAN) nevez ki IKT-tanácsadó bizottságának javaslata alapján a saját informatikai környezetüket működtető ügynökségek és szervek érdekeinek képviseletére, valamint az alábbiak mindegyike által kinevezett egy-egy képviselő:

a) az Európai Parlament;

b) az Európai Unió Tanácsa;

c) az Európai Bizottság;

d) az Európai Unió Bírósága;

e) az Európai Központi Bank;

f) az Európai Számvevőszék;

g) az Európai Külügyi Szolgálat;

h) az Európai Gazdasági és Szociális Bizottság;

i) a Régiók Európai Bizottsága;

j) az Európai Beruházási Bank;

k) az Európai Uniós Kiberbiztonsági Ügynökség.

A tagok munkáját egy-egy póttag is segítheti. Az elnök meghívhatja a fent felsorolt szervezetek vagy más uniós intézmények, szervek és ügynökségek egyéb képviselőit, hogy szavazati jog nélkül részt vegyenek az IICB ülésein.

(4) Az IICB elfogadja saját eljárási szabályzatát.

(5) Az IICB – belső eljárási szabályzatával összhangban – a tagjai közül négyéves időtartamra elnököt jelöl ki. Póttagja ugyanezen időtartamra az IICB teljes jogú tagjává válik.

(6) Az IICB az elnök kezdeményezésére, a CERT-EU kérésére vagy bármely tagjának kérésére ül össze.

(7) Az IICB minden tagja egy szavazattal rendelkezik. Amennyiben e rendelet másként nem rendelkezik, az IICB határozatait egyszerű többséggel hozza meg. Az elnök csak szavazategyenlőség esetén szavazhat, amelynek során döntő szavazatot adhat le.

(8) Az IICB az IICB belső eljárási szabályzatával összhangban kezdeményezett egyszerűsített írásbeli eljárás keretében járhat el. Ezen eljárás szerint a vonatkozó határozatot az elnök által meghatározott határidőn belül elfogadottnak kell tekinteni, kivéve, ha valamely tag kifogást emel ellene.

(9) A CERT-EU vezetője vagy helyettese részt vesz az IICB ülésein, kivéve, ha az IICB másként határoz.

(10) Az IICB titkárságát a Bizottság biztosítja.

(11) Az IKT-tanácsadó bizottság javaslata alapján az EUAN által kijelölt képviselők továbbítják az IICB határozatait az uniós ügynökségeknek és közös vállalkozásoknak. Bármely uniós ügynökség és szerv jogosult az IICB képviselői vagy elnöke elé terjeszteni minden olyan ügyet, amelyet megítélése szerint az IICB tudomására kell hozni.

(12) Az IICB az elnök által kezdeményezett egyszerűsített írásbeli eljárás keretében is eljárhat, amelynek értelmében a vonatkozó határozatot az elnök által meghatározott

határidőn belül jóváhagyottnak kell tekinteni, kivéve, ha valamely tag kifogást emel ellene.

(13) Az IICB kijelölhet egy végrehajtó bizottságot, amely segíti annak munkáját, és bizonyos feladatait és hatásköreit átruházhatja rá. Az IICB megállapítja a végrehajtó bizottság eljárási szabályzatát, beleértve annak feladatait és hatásköreit, valamint tagjainak hivatali idejét.

10. cikk
Az IICB feladatai

Feladatainak ellátása során az IICB különösen:

a) felülvizsgálja a CERT-EU-tól az e rendelet uniós intézmények, szervek és ügynökségek általi végrehajtásának állapotáról kért jelentéseket;

b) a CERT-EU vezetőjének javaslata alapján jóváhagyja a CERT-EU éves munkaprogramját és nyomon követi annak végrehajtását;

c) a CERT-EU vezetőjének javaslata alapján jóváhagyja a CERT-EU szolgáltatási katalógusát;

d) a CERT-EU vezetője által benyújtott javaslat alapján jóváhagyja a CERT-EU tevékenységeinek bevételeire és kiadásaira vonatkozó éves pénzügyi tervet, beleértve a személyzetre vonatkozót is;

e) a CERT-EU vezetőjének javaslata alapján jóváhagyja a szolgáltatási szintre vonatkozó megállapodások szabályait;

f) megvizsgálja és jóváhagyja a CERT-EU vezetője által készített, a CERT-EU tevékenységeiről és pénzeszközeinek kezeléséről szóló éves jelentést;

g) jóváhagyja és nyomon követi a CERT-EU vezetőjének javaslata alapján meghatározott fő teljesítménymutatókat;

h) jóváhagyja a CERT-EU és más szervezetek közötti, a 17. cikk szerinti együttműködési megállapodásokat, szolgáltatási szintre vonatkozó megállapodásokat vagy szerződéseket;

i) az IICB munkájának támogatásához szükséges számú technikai tanácsadó csoportot hoz létre, jóváhagyja azok feladatkörét, és kijelöli azok elnökeit.

11. cikk
Megfelelés

Az IICB nyomon követi e rendelet, valamint az elfogadott iránymutatásokat tartalmazó dokumentumok, ajánlások és az uniós intézmények, szervek és ügynökségek cselekvési felhívásainak végrehajtását. Amennyiben az IICB megállapítja, hogy az uniós intézmények, szervek vagy ügynökségek nem alkalmazták vagy nem hajtották végre hatékonyan ezt a rendeletet vagy az e rendelet alapján kiadott iránymutatásokat tartalmazó dokumentumokat, ajánlásokat és cselekvési felhívásokat, az érintett uniós intézmény, szerv vagy ügynökség belső eljárásainak sérelme nélkül:

a) figyelmeztetést ad ki; amennyiben egy jelentős kiberbiztonsági kockázat miatt szükséges, a figyelmeztetés célközönségét megfelelően korlátozza;

b) javaslatot tesz a megfelelő ellenőrzési szolgálat számára az ellenőrzés elvégzésére.

IV. fejezet
CERT-EU

12. cikk
A CERT-EU küldetése és feladatai

(1) A CERT-EU, az európai intézmények, szervek és hivatalok számítógépes vészhelyzeteket elhárító önálló csoportjának küldetése, hogy hozzájáruljon valamennyi uniós intézmény, szerv és ügynökség nem minősített informatikai környezetének biztonságához azáltal, hogy tanácsadást nyújt számukra a kiberbiztonsággal kapcsolatban, segíti őket a biztonsági események megelőzésében, észlelésében, enyhítésében és az azokra való reagálásban, valamint azáltal, hogy kiberbiztonsági információcsere- és eseményreagálási koordinációs központként működik.

(2) A CERT-EU a következő feladatokat látja el az uniós intézmények, szervek és ügynökségek számára:

a) támogatja pket e rendelet végrehajtásában, és a 13. cikk (1) bekezdésében felsorolt intézkedések vagy az IICB által kért eseti jelentések révén hozzájárul e rendelet alkalmazásának összehangolásához;

b) támogatja őket a szolgáltatási katalógusában leírt kiberbiztonsági szolgáltatások csomagja révén („alapszolgáltatások”);

c) hálózatot alakít ki a hasonló szervezetekkel és partnerekkel fenntartása a 16. és 17. cikkben vázolt szolgáltatások támogatása érdekében;

d) felhívja az IICB figyelmét az e rendelet végrehajtásával, valamint az iránymutató dokumentumok, ajánlások és cselekvési felhívások végrehajtásával kapcsolatos bármely kérdésre;

e) jelentést tesz az uniós intézményeket, szerveket és ügynökségeket érintő kiberfenyegetésekről és hozzájárul az EU kiberbiztonsággal kapcsolatos helyzetismeretéhez.

(3) A CERT-EU hozzájárul a 2021. június 23-i bizottsági ajánlással összhangban létrehozott közös kiberbiztonsági egység munkájához, többek között a következő területeken:

a) felkészültség, biztonsági események koordinálása, információcsere és válságreagálás technikai szinten az uniós intézményekkel, szervekkel és ügynökségekkel kapcsolatos ügyekben;

b) operatív együttműködés a számítógép-biztonsági eseményekre reagáló csoportok (CSIRT-ek) hálózatával – többek között a kölcsönös segítségnyújtással – és a tágabb kiberbiztonsági közösséggel kapcsolatban;

c) kiberfenyegetettségi információk, beleértve a helyzetismeretet;

d) a CERT-EU technikai kiberbiztonsági szakértelmét igénylő bármely téma.

(4) A CERT-EU az (EU) 2019/881 európai parlamenti és tanácsi rendelettel összhangban strukturált együttműködést folytat az Európai Uniós Kiberbiztonsági Ügynökséggel a kapacitásépítés, az operatív együttműködés és a kiberfenyegetések hosszú távú stratégiai elemzése terén.

(5) A CERT-EU a szolgáltatáskatalógusában nem szereplő következő szolgáltatásokat (a továbbiakban: díjköteles szolgáltatások) nyújthatja:

a) a (2) bekezdésben említettektől eltérő, az uniós intézmények, szervek és ügynökségek informatikai környezetének kiberbiztonságát támogató szolgáltatások, a szolgáltatási szintre vonatkozó megállapodások alapján és a rendelkezésre álló erőforrások függvényében;

b) olyan szolgáltatások, amelyek írásbeli megállapodások alapján és az IICB előzetes jóváhagyásával támogatják az uniós intézmények, szervek és ügynökségek kiberbiztonsági műveleteit vagy projektjeit, kivéve azokat, amelyek informatikai környezetük védelmét szolgálják;

c) írásbeli megállapodások alapján és az IICB előzetes jóváhagyásával az uniós intézményektől, szervektől és ügynökségektől eltérő olyan szervezetek számára nyújtott, informatikai környezetük biztonságát támogató szolgáltatások, amelyek szorosan együttműködnek az uniós intézményekkel, szervekkel és ügynökségekkel, például az uniós jog szerinti feladatok vagy felelősségi körök teljesítése révén.

(6) A CERT-EU – adott esetben az Európai Uniós Kiberbiztonsági Ügynökséggel szoros együttműködésben – kiberbiztonsági gyakorlatokat szervezhet vagy ajánlhatja a meglévő gyakorlatokban való részvételt az uniós intézmények, szervek és ügynökségek kiberbiztonsági szintjének tesztelése céljából.

(7) A CERT-EU segítséget nyújthat az uniós intézményeknek, szerveknek és ügynökségeknek a minősített informatikai környezetben bekövetkező biztonsági eseményekkel kapcsolatban, amennyiben erre az érintett védett szervezet kifejezetten felkéri.

13. cikk

Útmutató dokumentumok, ajánlások és cselekvési felhívások

(1) A CERT-EU e rendelet végrehajtását a következők kibocsátásával támogatja:

a) cselekvési felhívások, amelyek ismertetik azokat a sürgős biztonsági intézkedéseket, amelyeket az uniós intézményeknek, szerveknek és ügynökségeknek meghatározott időn belül meg kell hozniuk;

b) javaslatok az IICB számára az uniós intézmények, szervek és ügynökségek összességének vagy egy részhalmazának szóló útmutató dokumentumokra vonatkozóan;

c) ajánlások az IICB számára az egyes uniós intézményeknek, szerveknek és ügynökségeknek címzett útmutató dokumentumokra vonatkozóan.

(2) Az útmutató dokumentumok és ajánlások a következőket foglalhatják magukban:

a) a kiberbiztonsági kockázatkezelésre és a kiberbiztonsági alapkövetelményekre vonatkozó szabályok vagy javítások;

b) az érettségi értékelésekre és kiberbiztonsági tervekre vonatkozó szabályok; és

c) adott esetben a közös technológia, architektúra és a kapcsolódó bevált gyakorlatok alkalmazása az interoperabilitás és az egységes, az irányelv [a NIS 2-javaslat] 4. cikkének 10. pontja szerinti szabványok megvalósítása céljából.

(3) Az IICB a CERT-EU javaslata alapján útmutató dokumentumokat vagy ajánlásokat fogadhat el.

(4) Az IICB utasíthatja a CERT-EU-t, hogy adjon ki, vonjon vissza vagy módosítson útmutató dokumentumokra vagy ajánlásokra vonatkozó javaslatokat, illetve cselekvési felhívásokat.

14. cikk
A CERT-EU vezetője

A CERT-EU vezetője rendszeresen jelentést nyújt be az IICB-nek és az IICB elnökének a CERT-EU teljesítményéről, a pénzügyi tervezésről, a bevételekről, a költségvetés végrehajtásáról, a szolgáltatási szintre vonatkozó megállapodásokról és a megkötött írásbeli megállapodásokról, a hasonló szervezetekkel és partnerekkel folytatott együttműködésről, valamint a személyzet által végzett küldetésekről, beleértve a 10. cikk (1) bekezdésében említett jelentéseket is.

15. cikk
Pénzügyi és személyzeti kérdések

(1) A Bizottság az IICB egyhangú jóváhagyását követően kinevezi a CERT-EU vezetőjét. A CERT-EU vezetőjének kinevezését megelőzően az eljárás minden szakaszában konzultálni kell az IICB-vel, különösen az álláshirdetések megszövegezése, a pályázatok vizsgálata és a felvételi bizottságok kinevezése során.

(2) Az adminisztratív és pénzügyi eljárások tekintetében a CERT-EU vezetője a Bizottság felügyelete alatt jár el.

(3) A CERT-EU feladatait és tevékenységeit, beleértve a CERT-EU által a 12. cikk (2), (3), (4) és (6) bekezdése, valamint a 13. cikk (1) bekezdése alapján az uniós intézményeknek, szerveknek és ügynökségeknek nyújtott, a többéves pénzügyi keret európai közigazgatásra vonatkozó fejezetéből finanszírozott szolgáltatásokat a Bizottság költségvetésének külön költségvetési sorából kell finanszírozni. A CERT-EU számára elkülönített álláshelyeket a Bizottság létszámtervéhez fűzött lábjegyzetben kell részletezni.

(4) A (3) bekezdésben említettektől eltérő uniós intézmények, szervek és ügynökségek éves pénzügyi hozzájárulást nyújtanak a CERT-EU-nak a CERT-EU által az említett (3) bekezdés értelmében nyújtott szolgáltatások fedezésére. A vonatkozó hozzájárulások az IICB által adott iránymutatásokon alapulnak, amelyekről az egyes szervezetek és a CERT-EU szolgáltatási szintre vonatkozó megállapodásokban állapodnak meg. A hozzájárulások méltányos és arányos részt képviselnek a nyújtott szolgáltatások teljes költségéből. Az összegeket az (EU, Euratom) 2018/1046 európai parlamenti és tanácsi rendelet[8] 21. cikke (3) bekezdésének c) pontja szerinti címzett bevételként a (3) bekezdésben említett külön költségvetési sorból kell beszedni.

[8] Az Európai Parlament és a Tanács (EU, Euratom) 2018/1046 rendelete (2018. július 18.) az Unió általános költségvetésére alkalmazandó pénzügyi szabályokról, az 1296/2013/EU, az 1301/2013/EU, az 1303/2013/EU, az 1304/2013/EU, az 1309/2013/EU, az 1316/2013/EU, a 223/2014/EU és a 283/2014/EU rendelet és az 541/2014/EU határozat módosításáról, valamint a 966/2012/EU, Euratom rendelet hatályon kívül helyezéséről (HL L 193., 2018.7.30., 1. o.).

(5) A 12. cikk (5) bekezdésében meghatározott feladatok költségeit a CERT-EU szolgáltatásait igénybe vevő uniós intézmények, szervek és ügynökségek térítik meg. A bevételeket a költségeket támogató költségvetési sorokhoz kell rendelni.

16. cikk

A CERT-EU és a tagállami partnerek közötti együttműködés

(1) A CERT-EU együttműködik és információt cserél a tagállami partnerekkel, többek között a CERT-ekkel, a nemzeti kiberbiztonsági központokkal, a CSIRT-ekkel és az irányelv [a NIS 2-javaslat] 8. cikkében említett egyedüli kapcsolattartó pontokkal a kiberfenyegetésekről, a sebezhetőségekről és a biztonsági eseményekről, a lehetséges ellenintézkedésekről, valamint az uniós intézmények, szervek és ügynökségek informatikai környezete védelmének javítása szempontjából releváns valamennyi kérdésről, többek között az irányelv [a NIS 2-javaslat] 13. cikkében említett CSIRT-hálózaton keresztül.

(2) A CERT-EU a hasonló kiberfenyegetések vagy -események felderítésének megkönnyítése érdekében az érintett védett szervezet beleegyezése nélkül megoszthatja a biztonsági eseményekkel kapcsolatos információkat a tagállami partnerekkel. A CERT-EU csak az érintett védett szervezet beleegyezésével cserélhet olyan biztonságiesemény-specifikus információkat, amelyek feltárják a kiberbiztonsági esemény célpontját.

17. cikk

A CERT-EU és a nem tagállami partnerek közötti együttműködés

(1) A CERT-EU együttműködhet nem tagállami partnerekkel, többek között ágazatspecifikus partnerekkel az eszközök és módszerek, például a technikák, taktikák, eljárások és bevált gyakorlatok, valamint a kiberfenyegetések és -sebezhetőségek terén. A CERT-EU-nak az ilyen partnerekkel folytatott minden együttműködéshez – ideértve azokat a kereteket is, amelyekben a nem uniós partnerek együttműködnek a tagállamok nemzeti partnereivel – az IICB előzetes jóváhagyását kell kérnie.

(2) A CERT-EU együttműködhet más partnerekkel, például kereskedelmi szervezetekkel, nemzetközi szervezetekkel, nem európai uniós nemzeti szervezetekkel vagy egyéni szakértőkkel annak érdekében, hogy információkat gyűjtsön az általános és konkrét kiberfenyegetésekről, sebezhetőségekről és a lehetséges ellenintézkedésekről. Az ilyen partnerekkel való szélesebb körű együttműködéshez a CERT-EU-nak előzetes jóváhagyást kell kérnie az IICB-től.

(3) A CERT-EU a biztonsági esemény által érintett védett szervezet beleegyezésével információkat szolgáltathat a biztonsági eseményről azoknak a partnereknek, akik hozzájárulhatnak annak elemzéséhez.

V. fejezet
EGYÜTTMŰKÖDÉSI ÉS JELENTÉSTÉTELI KÖTELEZETTSÉGEK

18. cikk
Információkezelés

(1) A CERT-EU és az uniós intézmények, szervek és ügynökségek tiszteletben tartják az Európai Unió működéséről szóló szerződés 339. cikke vagy az azzal egyenértékű alkalmazandó keretrendszerek szerinti szakmai titoktartási kötelezettséget.

(2) Az 1049/2001/EK európai parlamenti és tanácsi rendelet[9] rendelkezései alkalmazandók a CERT-EU birtokában lévő dokumentumokhoz való nyilvános hozzáférés iránti kérelmekre, beleértve az említett rendelet szerinti azon kötelezettséget is, hogy minden olyan esetben, amikor a kérelem azok dokumentumaira vonatkozik, konzultálni kell más uniós intézményekkel, szervekkel és ügynökségekkel.

(3) A személyes adatok e rendelet szerinti kezelése tekintetében az (EU) 2018/1725 európai parlamenti és tanácsi rendelet irányadó.

(4) A CERT-EU és az uniós intézmények, szervek és ügynökségek általi információkezelés összhangban van az [információbiztonságról szóló rendeletjavaslatban] meghatározott szabályokkal.

(5) A nemzeti biztonsági és hírszerző szolgálatok által a CERT-EU-val kezdeményezett vagy kért kapcsolattartásról indokolatlan késedelem nélkül tájékoztatni kell a Bizottság Biztonsági Igazgatóságát és az IICB elnökét.

19. cikk
Megosztási kötelezettségek

(1) Annak érdekében, hogy a CERT-EU koordinálhassa a sebezhetőségek kezelését és a biztonsági eseményekre való reagálást, felkérheti az uniós intézményeket, szerveket és ügynökségeket, hogy a CERT-EU támogatása szempontjából releváns információkat szolgáltassanak számára informatikai rendszereik jegyzékéből. A megkeresett intézmény, szerv vagy ügynökség indokolatlan késedelem nélkül továbbítja a kért információt és annak minden későbbi frissítését.

(2) Az uniós intézmények, szervek és ügynökségek a CERT-EU kérésére indokolatlan késedelem nélkül átadják a biztonsági eseményekben érintett elektronikus eszközök használatával létrehozott digitális információkat. A CERT-EU tovább pontosíthatja, hogy az ilyen digitális információk mely típusaira van szüksége a helyzetismerethez és a biztonsági eseményekre való reagáláshoz.

(3) A CERT-EU csak az érintett szervezet beleegyezésével cserélhet olyan biztonságiesemény-specifikus információkat, amelyek feltárják a kiberbiztonsági eseménnyel érintett uniós intézményt, szervet vagy ügynökséget. A CERT-EU csak a biztonsági esemény által érintett szervezet beleegyezésével cserélhet olyan biztonságiesemény-specifikus információkat, amelyek feltárják a kiberbiztonsági esemény célpontját.

---

[9] Az Európai Parlament és a Tanács 1049/2001/EK rendelete (2001. május 30.) az Európai Parlament, a Tanács és a Bizottság dokumentumaihoz való nyilvános hozzáférésről (HL L 145., 2001.5.31., 43. o.).

(4) A megosztási kötelezettségek nem terjednek ki az EU-minősített adatokra és azokra az információkra, amelyeket valamely uniós intézmény, szerv vagy ügynökség valamely tagállam biztonsági vagy hírszerző szolgálatától vagy bűnüldöző hatóságától kapott azzal a kifejezett feltétellel, hogy azokat nem oszthatja meg a CERT-EU-val.

20. cikk

Értesítési kötelezettségek

(1) Valamennyi uniós intézmény, szerv és ügynökség indokolatlan késedelem nélkül, de legkésőbb 24 órával azt követően, hogy tudomást szerzett róla, kezdeti értesítést nyújt be a CERT-EU-nak a jelentős kiberfenyegetésekről, a jelentős sebezhetőségekről és a jelentős biztonsági eseményekről.

Kellően indokolt esetekben és a CERT-EU-val egyetértésben az érintett uniós intézmény, szerv vagy ügynökség eltérhet az előző bekezdésben meghatározott határidőtől.

(2) Az uniós intézmények, szervek és ügynökségek indokolatlan késedelem nélkül értesítik a CERT-EU-t a kiberfenyegetések, sebezhetőségek és biztonsági események megfelelő technikai részleteiről, amelyek lehetővé teszik a felderítést, a biztonsági eseményekre való reagálást vagy a kockázatcsökkentő intézkedéseket. Az értesítésnek tartalmaznia kell a következőket, amennyiben rendelkezésre állnak:

a) a vonatkozó fertőzöttségi mutatók;

b) a vonatkozó felderítési mechanizmusok;

c) a potenciális hatás;

d) a vonatkozó kockázatcsökkentő intézkedések.

(3) A CERT-EU havonta összefoglaló jelentést nyújt be az ENISA-nak, amely anonimizált és összesített adatokat tartalmaz az (1) bekezdéssel összhangban bejelentett jelentős kiberfenyegetésekről, jelentős sebezhetőségekről és jelentős biztonsági eseményekről.

(4) Az IICB útmutató dokumentumokat vagy ajánlásokat bocsáthat ki az értesítés szabályaira és tartalmára vonatkozóan. A CERT-EU megosztja a megfelelő technikai részleteket annak érdekében, hogy lehetővé tegye az uniós intézmények, szervek és ügynökségek általi proaktív felderítést, biztonsági eseményekre való reagálást vagy a kockázatcsökkentő intézkedések meghozatalát.

(5) Az értesítési kötelezettségek nem terjednek ki az EU-minősített adatokra és azokra az információkra, amelyeket valamely uniós intézmény, szerv vagy ügynökség valamely tagállam biztonsági vagy hírszerző szolgálatától vagy bűnüldöző hatóságától kapott azzal a kifejezett feltétellel, hogy azokat nem oszthatja meg a CERT-EU-val.

21. cikk

A biztonsági eseményekre való reagálás koordinációja és együttműködés a jelentős biztonsági eseményekkel kapcsolatban

(1) Kiberbiztonsági információcsere- és eseményreagálási koordinációs központként eljárva a CERT-EU elősegíti a kiberfenyegetésekre, sebezhetőségekre és biztonsági eseményekre vonatkozó információcserét az alábbiak között:

a) az uniós intézmények, szervek és ügynökségek;

b) a 16. és a 17. cikkben említett partnerek.

(2) A CERT-EU elősegíti az uniós intézmények, szervek és ügynökségek közötti koordinációt a biztonsági eseményekre való reagálás terén, beleértve a következőket:

a) hozzájárulás az egységes külső kommunikációhoz;

b) kölcsönös segítségnyújtás;

c) az operatív erőforrások optimális felhasználása;

d) koordináció más uniós szintű válságreagálási mechanizmusokkal.

(3) A CERT-EU támogatja az uniós intézményeket, szerveket és ügynökségeket a kiberfenyegetésekkel, sebezhetőségekkel és biztonsági eseményekkel kapcsolatos helyzetismeret kialakításában.

(4) Az IICB iránymutatást ad ki a jelentős biztonsági eseményekre való reagálás koordinálásáról és együttműködéséről. Amennyiben egy biztonsági esemény büntetőjogi jellege gyanítható, a CERT-EU tanácsot ad arra vonatkozóan, hogy miként kell bejelenteni az eseményt a bűnüldöző hatóságoknak.

22. cikk
Súlyos támadások

(1) A CERT-EU koordinálja az uniós intézmények, szervek és ügynökségek által a súlyos támadások esetén adandó válaszlépéseket. Nyilvántartást vezet arról a technikai szakértelemről, amelyre ilyen támadások esetén a biztonsági események elhárításához szükség lehet.

(2) Az uniós intézmények, szervek és ügynökségek hozzájárulnak a technikai szakértelem nyilvántartásához azáltal, hogy a szervezetükön belül rendelkezésre álló szakértőkről évente frissített jegyzéket állítanak össze, amely részletezi sajátos technikai készségeiket.

(3) Az érintett uniós intézmények, szervek és ügynökségek jóváhagyásával a CERT-EU a (2) bekezdésben említett jegyzékben szereplő szakértőkhöz fordulhat, hogy a közös kiberbiztonsági egységgel és annak működési eljárásaival összhangban hozzájáruljanak a valamely tagállamban elkövetett súlyos támadásra való reagáláshoz.

VI. fejezet
ZÁRÓ RENDELKEZÉSEK

23. cikk
Kezdeti költségvetési átcsoportosítás

A Bizottság javaslatot tesz az érintett uniós intézményektől, szervektől és ügynökségektől származó személyzeti és pénzügyi forrásoknak a Bizottság költségvetésébe történő átcsoportosítására. Az átcsoportosítás az e rendelet hatálybalépését követően elfogadott első költségvetéssel egy időben lép hatályba.

24. cikk

Felülvizsgálat

(1) A IICB a CERT-EU segítségével rendszeresen jelentést tesz a Bizottságnak e rendelet végrehajtásáról. Az IICB ezenkívül ajánlásokat tehet a Bizottságnak e rendelet módosítására.

(2) A Bizottság legkésőbb 48 hónappal e rendelet hatálybalépését követően, majd azt követően háromévente jelentést tesz az Európai Parlamentnek és a Tanácsnak e rendelet végrehajtásáról.

(3) A Bizottság legkorábban öt évvel e rendelet hatálybalépését követően értékeli a rendelet működését, és jelentést tesz az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának.

25. cikk

Hatálybalépés

Ez a rendelet az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

Ez a rendelet teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban.

Kelt Brüsszelben, -án/-én.

az Európai Parlament részéről	*a Tanács részéről*
az elnök	*az elnök*

PÉNZÜGYI KIMUTATÁS

1. A JAVASLAT/KEZDEMÉNYEZÉS FŐBB ADATAI

1.1. A javaslat/kezdeményezés címe

1.2. Érintett szakpolitikai terület(ek)

1.3. A javaslat/kezdeményezés a következőre irányul:

1.4. Célkitűzés(ek)

1.4.1. Általános célkitűzés(ek)

1.4.2. Egyedi célkitűzés(ek)

1.4.3. Várható eredmény(ek) és hatás

1.4.4. Teljesítménymutatók

1.5. A javaslat/kezdeményezés indoklása

1.5.1. Rövid vagy hosszú távon kielégítendő szükséglet(ek) a kezdeményezés végrehajtásának részletes ütemtervével.

1.5.2. Az uniós részvételből adódó többletérték (ez különböző tényezőkből származhat, például a koordináció jelentette előnyökből, a jogbiztonságból, a fokozott hatékonyságból vagy a kiegészítő jellegből). E pont értelmében „az uniós részvételből adódó többletérték” az az uniós részvételből adódó érték, amely többletként jelentkezik ahhoz az értékhez képest, amely a tagállamok egyedüli fellépése esetén jött volna létre.

1.5.3. Hasonló korábbi tapasztalatok tanulsága

1.5.4. A többéves pénzügyi kerettel való összeegyeztethetőség és egyéb megfelelő eszközökkel való lehetséges szinergiák

1.5.5. A rendelkezésre álló különböző finanszírozási lehetőségek értékelése, ideértve az átcsoportosítási lehetőségeket is

1.6. A javaslat/kezdeményezés időtartama és pénzügyi hatása

1.7. Tervezett irányítási módszer(ek)

2. IRÁNYÍTÁSI INTÉZKEDÉSEK

2.1. A nyomon követésre és a jelentéstételre vonatkozó rendelkezések

2.2. Irányítási és kontrollrendszer(ek)

2.2.1. Az irányítási módszer(ek), a finanszírozás végrehajtási mechanizmusai, a kifizetési módok és a javasolt kontrollstratégia indokolása

2.2.2. A felismert kockázatokkal és a csökkentésükre létrehozott belső kontrollrendszerekkel kapcsolatos információk

2.2.3. A kontroll költséghatékonyságának becslése és indokolása (a „kontroll költségei ÷ a kezelt kapcsolódó források értéke” hányados) és a hibakockázat várható szintjeinek értékelése (kifizetéskor és záráskor)

2.3. A csalások és a szabálytalanságok megelőzésére vonatkozó intézkedések

3. A JAVASLAT/KEZDEMÉNYEZÉS BECSÜLT PÉNZÜGYI HATÁSA

3.1. A többéves pénzügyi keret érintett fejezete/fejezetei és a költségvetés érintett kiadási sora/sorai

3.2. A javaslat előirányzatokra gyakorolt becsült pénzügyi hatása

3.2.1. Az operatív előirányzatokra gyakorolt becsült hatás összegzése

3.2.2. Operatív előirányzatokból finanszírozott becsült kimenet

3.2.3. Az igazgatási előirányzatokra gyakorolt becsült hatás összegzése

3.2.4. A jelenlegi többéves pénzügyi kerettel való összeegyeztethetőség

3.2.5. Harmadik felek hozzájárulásai

3.3. A bevételre gyakorolt becsült pénzügyi hatás

PÉNZÜGYI KIMUTATÁS

1. A JAVASLAT/KEZDEMÉNYEZÉS FŐBB ADATAI

1.1. A javaslat/kezdeményezés címe

Javaslat – Az Európai Parlament és a Tanács rendelete az uniós intézmények, szervek, hivatalok és ügynökségek egységesen magas szintű kiberbiztonságát biztosító intézkedések meghatározásáról

1.2. Érintett szakpolitikai terület(ek)

Európai közigazgatás

A javaslat az uniós intézmények, szervek és ügynökségek egységesen magas szintű kiberbiztonságát biztosító intézkedéseket érinti

1.3. A javaslat/kezdeményezés a következőre irányul:

☑új intézkedés

☐ kísérleti projektet/előkészítő intézkedést követő új intézkedés[10]

☐ jelenlegi intézkedés meghosszabbítása

☑ egy vagy több intézkedés összevonása vagy átcsoportosítása egy másik/új intézkedésre

1.4. Célkitűzés(ek)

1.4.1. Általános célkitűzés(ek)

– Az uniós intézmények, szervek és ügynökségek egységesen magas szintű kiberbiztonságát biztosító keretrendszer létrehozása

– Új jogalap biztosítása a CERT-EU számára megbízatásának és finanszírozásának megerősítése érdekében

1.4.2. Egyedi célkitűzés(ek)

1. Az uniós intézmények, szervek és ügynökségek belső kiberbiztonságikockázat-kezelési, -irányítási és -ellenőrzési keretrendszer létrehozására vonatkozó kötelezettségének meghatározása
2. Kötelezettségek megállapítása az uniós intézmények, szervek és ügynökségek számára a kiberbiztonsági kockázatkezelési, -irányítási és -ellenőrzési keretrendszereikre, valamint a kiberbiztonsági eseményekre vonatkozó jelentéstétel tekintetében
3. Az uniós intézmények, szervek és ügynökségek kiberbiztonsági központjának (CERT-EU) szervezetére és működésére, valamint az Intézményközi Kiberbiztonsági Testület (IICB) szervezetére és működésére vonatkozó szabályok meghatározása
4. Hozzájárulás a közös kiberbiztonsági egységhez

[10] A költségvetési rendelet 58. cikke (2) bekezdésének a) vagy b) pontja szerint.

1.4.3. Várható eredmény(ek) és hatás

Tüntesse fel, milyen hatásokat gyakorolhat a javaslat/kezdeményezés a kedvezményezettekre/célcsoportokra.

- Belső kiberbiztonsági kockázatkezelési, -irányítási és -ellenőrzési keretrendszerek, kiberbiztonsági alapkövetelmények, rendszeres érettségi értékelések és kiberbiztonsági tervek az uniós intézményeknél, szerveknél és ügynökségeknél
- A kiberbiztonsági ellenálló képesség és a biztonsági eseményekre való reagálási képességek fejlesztése az uniós intézményeknél, szerveknél és ügynökségeknél
- A CERT-EU modernizálása
- Hozzájárulás a közös kiberbiztonsági egységhez

1.4.4. Teljesítménymutatók

Határozza meg az előrehaladás és az eredmények nyomon követésére szolgáló mutatókat.

- Meglévő keretrendszerek és alapkövetelmények, az uniós intézményeknél, szerveknél és ügynökségeknél végzett rendszeres érettségi értékelések és kiberbiztonsági tervek
- A biztonsági események jobb kezelése
- A kiberbiztonsági kockázatok fokozott tudatosítása az uniós intézmények, szervek és ügynökségek felső vezetői szintjén
- Az IKT-biztonsági kiadások kiegyenlítése a teljes IKT-kiadások százalékában
- Az IICB és a CERT-EU erős vezetése
- Fokozott információmegosztás az uniós intézmények, szervek és ügynökségek, valamint az érintett uniós szervek és érdekelt felek között
- Fokozott kiberbiztonsági együttműködés az érintett uniós szervekkel és érdekelt felekkel a CERT-EU-n és az ENISA-n keresztül

1.5. A javaslat/kezdeményezés indoklása

1.5.1. Rövid vagy hosszú távon kielégítendő szükséglet(ek) a kezdeményezés végrehajtásának részletes ütemtervével.

A javaslat célja, hogy növelje az uniós intézmények, szervek és ügynökségek kiberrezilienciáját, csökkentse az e szervek rezilienciájában mutatkozó következetlenségeket, valamint javítsa a közös helyzetismeret szintjét és a közös felkészülési és reagálási képességet.

A javaslat teljes mértékben összhangban áll és koherens más kapcsolódó kezdeményezésekkel, különösen az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről szóló irányelvre irányuló javaslattal [a NIS 2-javaslattal].

A javaslat alapvető részét képezi a biztonsági unióra vonatkozó uniós stratégiának és a digitális évtizedre vonatkozó uniós kiberbiztonsági stratégiának.

A rendeletre az Európai Bizottság a tervek szerint 2021 októberében tesz javaslatot, az Európai Parlament és a Tanács várhatóan 2022-ben fogadja el a rendeletet, és a rendelkezések a rendelet hatálybalépésétől alkalmazandók. Az e pénzügyi

kimutatásban felvázolt pénzügyi és HR-hatás a tervek szerint 2023-ban jelenik meg először. Az előkészítő időszak 2021-ben már megkezdődött, de a 2021-es és 2022-es előkészítő tevékenységek nem érintik a javaslat pénzügyi hatását.

1.5.2. Az uniós részvételből adódó többletérték (ez különböző tényezőkből származhat, például a koordináció jelentette előnyökből, a jogbiztonságból, a fokozott hatékonyságból vagy a kiegészítő jellegből). E pont értelmében „az uniós részvételből adódó többletérték" az az uniós részvételből adódó érték, amely többletként jelentkezik ahhoz az értékhez képest, amely a tagállamok egyedüli fellépése esetén jött volna létre.

Az európai szintű fellépés indokai (előzetes)

2019 és 2021 között drámai mértékben megugrott az uniós intézményeket, szerveket és ügynökségeket érintő, fejlett, folyamatos fenyegetést jelentő szereplők által okozott jelentős biztonsági események száma. 2021 első felében a jelentős biztonsági események száma a 2020-ban mérttel azonos volt. Ezt tükrözi a CERT-EU által 2020-ban elemzett kriminalisztikai képek (az érintett rendszerek vagy eszközök tartalmának pillanatképei) száma is, amely 2019-hez képest megháromszorozódott, míg a jelentős biztonsági események száma 2018 óta több mint tízszeresére nőtt.

A kiberbiztonsági érettség szintje szervezetenként jelentősen eltér[11]. Ez a rendelet biztosítja, hogy valamennyi uniós intézmény, szerv és ügynökség végrehajtsa a biztonsági intézkedések alapkövetelményeit, és együttműködjön egymással az uniós igazgatás nyitott és hatékony működése érdekében.

A megőrzendő rendszerek az uniós intézmények, szervek és ügynökségek autonómiája alá tartoznak, és azokat az uniós intézmények, szervek és ügynökségek működtetik; a javasolt intézkedéseket a tagállamok nem tudnák létrehozni.

1.5.3. Hasonló korábbi tapasztalatok tanulsága

A kiberbiztonsági irányelv volt az első horizontális belső piaci eszköz, amelynek célja az uniós hálózatok és rendszerek kiberbiztonsági kockázatokkal szembeni ellenálló képességének javítása. 2016-os hatálybalépése óta nagymértékben hozzájárult a kiberbiztonság közös szintjének emeléséhez a tagállamokban. A NIS2 irányelvre irányuló javaslat ezen intézkedések további javítására törekszik.

A rendelet célja, hogy hasonló intézkedéseket írjon elő az uniós intézmények, szervek és ügynökségek számára.

1.5.4. A többéves pénzügyi kerettel való összeegyeztethetőség és egyéb megfelelő eszközökkel való lehetséges szinergiák

A javaslat összhangban van a többéves pénzügyi kerettel, és alapvető részét képezi a biztonsági unióra vonatkozó uniós stratégiának, valamint a digitális évtizedre vonatkozó uniós kiberbiztonsági stratégiának.

A javaslat az uniós intézmények, szervek és ügynökségek egységesen magas szintű kiberbiztonságát biztosító intézkedések alkalmazását tervezi. A javaslat összhangban áll az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről,

[11] Hivatkozás: [Az Európai Számvevőszék különjelentése az uniós intézmények, szervek és ügynökségek kiberbiztonságáról].

valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről szóló irányelvre irányuló javaslattal [NIS 2 javaslat].

1.5.5. A rendelkezésre álló különböző finanszírozási lehetőségek értékelése, ideértve az átcsoportosítási lehetőségeket is

A feladatok CERT-EU általi irányítása olyan speciális profilokat és kiegészítő munkaterhet igényel, amelyeknek az emberi és pénzügyi erőforrások növelése nélkül nem lehet eleget tenni.

1.6. A javaslat/kezdeményezés időtartama és pénzügyi hatása

☐ **határozott időtartam**

– ☐ időtartam: ÉÉÉÉ [HH/NN]-tól/-től ÉÉÉÉ [HH/NN]-ig

– ☐ pénzügyi hatás: ÉÉÉÉ-tól/-től ÉÉÉÉ-ig a kötelezettségvállalási előirányzatok esetében és ÉÉÉÉ-tól/-től ÉÉÉÉ-ig a kifizetési előirányzatok esetében

☑ **határozatlan időtartam**

– A pénzügyi hatásnak a rendelet hatálybalépését követően elfogadott első költségvetéssel kell kezdődnie. A forrásoknak az uniós intézményektől és a fő szervektől a Bizottsághoz történő átcsoportosítására az első évben kerülne sor, amely átmeneti évnek tekinthető; erre és a források egyéb (át)csoportosítására az éves költségvetések keretében kerül sor. Amennyiben a rendeletet 2022-ben elfogadják, a 2023-as pénzügyi év lesz az átmeneti időszak, 2024 pedig teljes mértékben fog működni.

1.7. Tervezett irányítási módszer(ek)[12]

☑ **Közvetlen irányítás** a Bizottság és az egyes uniós intézmények, szervek és ügynökségek által

– ☑ a Bizottság szervezeti egységein keresztül, ideértve az uniós küldöttségek személyzetét;

– ☐ végrehajtó ügynökségen keresztül

☐ **Megosztott irányítás** a tagállamokkal

☐ **Közvetett irányítás** a költségvetés végrehajtásával kapcsolatos feladatoknak a következőkre történő átruházásával:

– ☐ harmadik országok vagy az általuk kijelölt szervek;

– ☐ nemzetközi szervezetek és ügynökségeik (nevezze meg);

– ☐ az EBB és az Európai Beruházási Alap;

– ☐ a költségvetési rendelet 70. és 71. cikkében említett szervek;

– ☐ közjogi szervek;

– ☐ magánjog alapján működő, közfeladatot ellátó szervek, amennyiben megfelelő pénzügyi garanciákat nyújtanak;

– ☐ valamely tagállam magánjoga alapján működő, köz- és magánszféra közötti partnerség végrehajtásával megbízott és megfelelő pénzügyi garanciákat nyújtó szervek;

– ☐ az EUSZ V. címének értelmében a KKBP terén konkrét fellépések végrehajtásával megbízott, és a vonatkozó alap-jogiaktusban meghatározott személyek.

– *Egynél több irányítási módszer feltüntetése esetén kérjük, adjon részletes felvilágosítást a „Megjegyzések” rovatban.*

[12] Az egyes irányítási módszerek ismertetése, valamint a költségvetési rendeletre való megfelelő hivatkozások megtalálhatók a BudgWeb oldalon: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

Megjegyzések

Az adminisztratív és pénzügyi eljárások tekintetében a CERT-EU a Bizottság felügyelete alatt jár el.

A rendelettervezetből származó további források:

A rendelettervezet 12. és 13. cikkének végrehajtása további alapszolgáltatásokkal bővített szolgáltatási katalógust eredményez. Teljes körű működés esetén a következő kiegészítő forrásokra lesz szükség (a többéves pénzügyi keret végéig, 2027 végén): 21 teljes munkaidős egyenérték és 14,05 millió EUR.

A költségvetés kiegészítő forrásainak megoszlása a különböző feladatok között a következő:

a) az uniós intézmények, szervek és ügynökségek számára a 12. cikk (2) bekezdésének a), b), c) és e) pontjában részletezett feladatok ellátása tekintetében: 13,75 teljes munkaidős egyenérték és 11,275 millió EUR;

b) a 12. cikk (3) bekezdésében részletezett feladatok (a közös kiberbiztonsági egységhez való hozzájárulás) ellátása tekintetében: 2 teljes munkaidős egyenérték és 381 000 EUR;

c) a 12. cikk (4) bekezdésében részletezett feladatok (az ENISA-val folytatott strukturált együttműködés) ellátása tekintetében: 0,25 teljes munkaidős egyenérték és 236 000 EUR;

d) a 12. cikk (6) bekezdésében részletezett feladatok (kiberbiztonsági gyakorlatok) ellátása tekintetében: 0,25 teljes munkaidős egyenérték és 79 000 EUR;

e) a 12. cikk (2) bekezdésének d) pontjában és a 13. cikkben részletezett feladatok (a rendelet végrehajtásának elemzése és jelentése, útmutató dokumentumok, ajánlások és cselekvési felhívások elkészítése) ellátása tekintetében: 3,75 teljes munkaidős egyenérték és 2,079 millió EUR.

f) az Intézményközi Kiberbiztonsági Testület (IICB) titkárságát támogató feladatok ellátása tekintetében: 1 teljes munkaidős egyenérték.

A jelenlegi erőforrások és a teljes körű működésre való áttérés áttekintése:

2021 szeptemberében a CERT-EU a következő erőforrásokkal működött:

– állandó és kirendelt álláshelyek: 14 teljes munkaidős egyenérték,

– a szolgáltatási szintre vonatkozó megállapodások alapján finanszírozott szerződéses alkalmazottak: 24 teljes munkaidős egyenérték,

– összesen 38 teljes munkaidős egyenérték.

A CERT-EU költségvetése 2020-ban: 250 000 EUR a Bizottság költségvetésében, 3,5 millió EUR a szolgáltatási szintre vonatkozó megállapodásokból származó címzett bevételekből. Összesen: 3,75 millió EUR. Ez képezte a CERT-EU teljes költségvetését, amely a képzésre, a hardverekre, a szoftverekre, a kiküldetésekre, a támogatásra, a szerződéses alkalmazottakra és a konferenciákra terjedt ki.

A rendelet hatálybalépését követően a CERT-EU jövőbeli erőforrásai a tervek szerint a következők lesznek:

– állandó álláshelyek: 34 teljes munkaidős egyenérték,

– szerződéses alkalmazottak: 15 teljes munkaidős egyenérték,

– összesen 49 teljes munkaidős egyenérték, ami 11 teljes munkaidős egyenértéknyi nettó növekedést jelent.

Az állandó álláshelyek és a szerződéses alkalmazottak arányának változása orvosolja a vezető kiberbiztonsági szakemberek felvételének és megtartásának munkaerőpiaci hiányuk miatti jelentős akadályát.

Emellett a Bizottság Informatikai Főigazgatóságán belül 1 teljes munkaidős egyenértékben kifejezett szerződéses alkalmazottra lesz szükség az IICB (Intézményközi Kiberbiztonsági Testület) támogatásához.

Így összesen 21 teljes munkaidős egyenértékre lesz szükség a rendelet végrehajtásához (20 teljes munkaidős egyenérték a CERT-EU és 1 teljes munkaidős egyenérték a Bizottság Informatikai Főigazgatósága esetében). Ezt ellensúlyozza a CERT-EU 9 teljes munkaidős egyenértékben kifejezett szerződéses alkalmazottjával való párhuzamos csökkentés, akiket korábban a szolgáltatási szintre vonatkozó megállapodásokból származó címzett bevételekből finanszíroztak.

A CERT-EU nem emberi erőforrásokra vonatkozó, 2024-ben, az átmeneti időszakot követően rendelkezésre álló költségvetése a fenti a)–e) pontban felsorolt feladatokat fogja fedezni, és a tervek szerint az alábbiak szerint kerül finanszírozásra:

– évi 8,921 millió EUR az uniós intézményektől az uniós költségvetés 7. fejezetéből,

– 2,459 millió EUR az uniós intézményektől, szervektől és ügynökségektől, amelyeket az uniós költségvetés 1–6. fejezetéből finanszíroznak,

– 2,670 millió EUR az önfinanszírozó uniós intézményektől, szervektől és ügynökségektől,

– a CERT-EU teljes költségvetése: 14,05 millió EUR.

A 12. cikk (5) bekezdésében felsorolt feladatok nem szerepelnek a szolgáltatáskatalógusban, ezek díjköteles szolgáltatások. Ezek kiegészítő jellegűek, viszonylag alacsony összegeket képviselnek, többnyire ideiglenesek, és e szolgáltatások költségeit szolgáltatási szintre vonatkozó megállapodások vagy írásbeli megállapodások révén térítik meg a szolgáltatások kedvezményezettjei.

A CERT-EU személyzetének nyújtott hozzájárulások tekintetében: az uniós intézmények és a fő szervek méltányos részt vállalnak, amely arányos a szervezet állandó adminisztrátori álláshelyeinek arányával. Meg kell vizsgálni, hogy az EKB és az EBB is képes-e méltányos részt vállalni az állandó személyzet kirendelése révén.

2. IRÁNYÍTÁSI INTÉZKEDÉSEK

2.1. A nyomon követésre és a jelentéstételre vonatkozó rendelkezések

Adja meg a gyakoriságot és a feltételeket.

A Bizottság az IICB és a CERT-EU segítségével rendszeresen felülvizsgálja a rendelet működését, és jelentést tesz az Európai Parlamentnek és a Tanácsnak, először legkésőbb e rendelet hatálybalépésétől számított 48 hónapon belül, majd azt követően háromévente.

A felülvizsgálatokhoz használt adatforrások többnyire az IICB-től és a CERT-EU-tól származnának. Emellett szükség esetén konkrét adatgyűjtési eszközök is alkalmazhatók, például az uniós intézmények, szervek és ügynökségek, az ENISA vagy a CSIRT-ek hálózata körében végzett felmérések.

2.2. Irányítási és kontrollrendszer(ek)

2.2.1. Az irányítási módszer(ek), a finanszírozás végrehajtási mechanizmusai, a kifizetési módok és a javasolt kontrollstratégia indokolása

A rendeletből eredő intézkedéseket az egyes uniós intézményeken, szerveken és ügynökségeken belül a vonatkozó, alkalmazandó szabályokkal és rendeletekkel összhangban kell irányítani.

A CERT-EU tevékenységeinek adminisztratív és pénzügyi irányítása be van ágyazva a bizottsági igazgatásba, és követi az alkalmazandó irányítási és végrehajtási mechanizmusait, fizetési módszereit és kontrolljait.

A Bizottság belső ellenőre ugyanazokkal a hatáskörökkel rendelkezik a CERT-EU felett, mint a Bizottság szervezeti egységei felett.

2.2.2. A felismert kockázatokkal és a csökkentésükre létrehozott belső kontrollrendszerekkel kapcsolatos információk

Nagyon alacsony kockázat, mivel a CERT-EU adminisztratív szempontból már bizottsági munkacsoportként kapcsolódik az Informatikai Főigazgatóság főigazgatójához, és az IICB a jelenlegi CERT-EU irányítóbizottság mintájára működik. A pénzügyi irányítás és a belső ellenőrzés ökoszisztémája így már működik.

2.2.3. A kontroll költséghatékonyságának becslése és indokolása (a „kontroll költségei ÷ a kezelt kapcsolódó források értéke” hányados) és a hibakockázat várható szintjeinek értékelése (kifizetéskor és záráskor)

A közbeszerzésre, a pénzgazdálkodásra és a kontrollra vonatkozó eljárások már érvényben vannak, és megfelelően tesztelték őket. A kontrollok költséghatékonysága és a hibakockázat szintje megfelel az egyes uniós intézmények, szervek vagy ügynökségek, valamint a Bizottság által a CERT-EU tevékenységei tekintetében alkalmazott kontrolloknak.

2.3. A csalások és a szabálytalanságok megelőzésére vonatkozó intézkedések

Tüntesse fel a meglévő vagy tervezett megelőző és védintézkedéseket, pl. a csalás elleni stratégiából.

A CERT-EU tevékenységeire a Bizottság pénzgazdálkodási és belső kontrollrendszerei alkalmazandók.

A csalás, korrupció és más jogellenes tevékenységek elleni küzdelmet illetően az Európai Csaláselleni Hivatal (OLAF) által lefolytatott vizsgálatokról szóló, 2013. szeptember 11-i 883/2013/EU, Euratom európai parlamenti és tanácsi rendelet rendelkezései korlátozás nélkül alkalmazandók.

3. A JAVASLAT/KEZDEMÉNYEZÉS BECSÜLT PÉNZÜGYI HATÁSA

3.1. A többéves pénzügyi keret érintett fejezete/fejezetei és a költségvetés érintett kiadási sora/sorai

- Jelenlegi költségvetési sorok

A többéves pénzügyi keret fejezetei, azon belül pedig a költségvetési sorok sorrendjében.

A többéves pénzügyi keret fejezete	Költségvetési sor	Kiadás típusa	Hozzájárulás			
	Szám	Diff./Nem diff.[13]	EFTA-országok-tól[14]	tagjelölt országok-tól[15]	harmadik országok-tól	a költségvetési rendelet 21. cikke (2) bekezdésének b) pontja értelmében
1–6.	A decentralizált ügynökségeknek és szerveknek nyújtott uniós hozzájárulásokat fedező költségvetési sorok	Diff.	NEM	NEM	NEM	NEM
7.	Az uniós költségvetés különböző szakaszainak személyzeti javadalmazását, informatikai kiadásait és egyéb igazgatási kiadásait fedező költségvetési sorok	Nem diff.	NEM	NEM	NEM	NEM

- Létrehozandó új költségvetési sorok

A többéves pénzügyi keret fejezetei, azon belül pedig a költségvetési sorok sorrendjében.

A többéves pénzügyi keret fejezete	Költségvetési sor	Kiadás típusa	Hozzájárulás			
	Szám	diff./nem diff.	EFTA-országok-tól	tagjelölt országoktól	harmadik országok-tól	a költségvetési rendelet 21. cikke (2) bekezdésének b) pontja értelmében
	is ke		IGEN/ NEM	IGEN/ NEM	IGEN/ NEM	IGEN/NEM

[13] Diff. = differenciált előirányzatok/nem diff. = nem differenciált előirányzatok.
[14] EFTA: Európai Szabadkereskedelmi Társulás.
[15] Tagjelölt országok és adott esetben a nyugat-balkáni potenciális tagjelöltek.

3.2. A javaslat előirányzatokra gyakorolt becsült pénzügyi hatása

3.2.1. Az operatív előirányzatokra gyakorolt becsült hatás összegzése

– ☐ A javaslat/kezdeményezés nem vonja maga után operatív előirányzatok felhasználását

– ☑ A javaslat/kezdeményezés az alábbi operatív előirányzatok felhasználását vonja maga után:

millió EUR (három tizedesjegyig)

A többéves pénzügyi keret fejezete	1–6.	A decentralizált ügynökségeknek és szerveknek nyújtott uniós hozzájárulásokat fedező fejezetek

Főigazgatóság: Számos			**2023**	**2024**	**2025**	**2026**	**2027**	**ÖSSZESEN**
○ Operatív előirányzatok								
A decentralizált ügynökségeknek és szerveknek nyújtott uniós hozzájárulásokat fedező költségvetési sorok (xx 10 xx xx)[16]	Kötelezettség-vállalások	(1a)	2,459	2,459	2,459	2,459	2,459	12,293
	Kifizetési előirányzatok	(2a)	2,459	2,459	2,459	2,459	2,459	12,293
Bizonyos egyedi programok keretéből finanszírozott igazgatási jellegű előirányzatok[17]								
Költségvetési sor		(3)						
TELJES pénzügyi előirányzat a következő Főigazgatóság esetében: Számos	Kötelezettség-vállalások	= 1a + 1b + 3	2,459	2,459	2,459	2,459	2,459	12,293
	Kifizetési előirányzatok	= 2a + 2b +3	2,459	2,459	2,459	2,459	2,459	12,293

[16] A hivatalos költségvetési nómenklatúra szerint.

[17] Technikai és/vagy igazgatási segítségnyújtás, valamint uniós programok és/vagy intézkedések végrehajtásához biztosított támogatási kiadások (korábban: BA-tételek), közvetett kutatás, közvetlen kutatás.

○ Operatív előirányzatok ÖSSZESEN	Kötelezettség-vállalások	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Kifizetési előirányzatok	(5)	2,459	2,459	2,459	2,459	2,459	12,293
○ Bizonyos egyedi programok keretéből finanszírozott igazgatási jellegű előirányzatok ÖSSZESEN		(6)						
A többéves pénzügyi keret 1–6. FEJEZETÉHEZ tartozó előirányzatok ÖSSZESEN	Kötelezettség-vállalások	= 4 + 6	2,459	2,459	2,459	2,459	2,459	12,293
	Kifizetési előirányzatok	= 5 + 6	2,459	2,459	2,459	2,459	2,459	12,293

Ha a javaslat/kezdeményezés egynél több operatív fejezetet is érint, ismételje meg a fenti szakaszt:

○ működési előirányzatok ÖSSZESEN (összes operatív fejezet)	Kötelezettség-vállalások	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Kifizetési előirányzatok	(5)	2,459	2,459	2,459	2,459	2,459	12,293
Bizonyos egyedi programok keretéből finanszírozott igazgatási jellegű előirányzatok ÖSSZESEN (összes operatív fejezet)		(6)						
A többéves pénzügyi keret 1–6. FEJEZETÉHEZ tartozó előirányzatok ÖSSZESEN (Referenciaösszeg)	Kötelezettség-vállalások	= 4 + 6	2,459	2,459	2,459	2,459	2,459	12,293
	Kifizetési előirányzatok	= 5 + 6	2,459	2,459	2,459	2,459	2,459	12,293

A többéves pénzügyi keret fejezete	7.	„Igazgatási kiadások”

Ezt a részt az igazgatási jellegű költségvetési adatok táblázatában kell kitölteni, melyet először a pénzügyi kimutatás mellékletébe (a belső szabályzat V. melléklete) kell bevezetni; a mellékletet a szolgálatközi konzultációhoz fel kell tölteni a DECIDE rendszerbe.

millió EUR (három tizedesjegyig)

		2023	2024	2025	2026	2027	ÖSSZESEN
Főigazgatóság: DIGIT (CERT-EU)							
○ Humán erőforrás		1,184	2,126	2,754	3,225	3,225	12,514
○ Egyéb igazgatási kiadások		7,938	8,921	8,921	8,921	8,921	43,622
ÖSSZESEN DG DIGIT (CERT-EU)	Költségvetési előirányzatok	9,122	11,047	11,675	12,146	12,146	56,136

A többéves pénzügyi keret **7. FEJEZETÉHEZ tartozó előirányzatok ÖSSZESEN**	(Összes kötelezettségvállalási előirányzat = Összes kifizetési előirányzat)	9,122	11,047	11,675	12,146	12,146	**56,136**

millió EUR (három tizedesjegyig)

		2023	2024	2025	2026	2027	ÖSSZESEN
A többéves pénzügyi keret 1–7. FEJEZETÉHEZ tartozó előirányzatok ÖSSZESEN (*)	Kötelezettségvállalások	11,581	13,506	14,134	14,605	14,605	68,429
	Kifizetési előirányzatok	11,581	13,506	14,134	14,605	14,605	68,429

(*) Az uniós intézmények, szervek és ügynökségek önfinanszírozó hozzájárulásai a becslések szerint évi 2,670 millió EUR-t tesznek ki (az öt évre összesen 13,350 millió EUR-t). A hozzájárulások címzett bevételt képeznek a CERT-EU számára. A fenti táblázatok csak az uniós költségvetésre gyakorolt becsült teljes hatást tartalmazzák, ezeket a hozzájárulásokat nem.

3.2.2. Operatív előirányzatokból finanszírozott becsült kimenet

Kötelezettségvállalási előirányzat millió EUR-ban (három tizedesjegyig)

Tüntesse fel a célkitűzéseket és a teljesítéseket ⇩			**N. év**		**N+1. év**		**N+2. év**		**N+3. év**		A táblázat a hatás időtartamának megfelelően (vö. 1.6. pont) további évekkel bővíthető						**TELJESÍTÉSEK**	
	ÖSSZESEN																	
	Típus [18]	Átlagos költség	Szám	Költség	Szám	Költség	Szám	Költség	Szám	Költség	Szám	Költség	Szám	Költség	Szám	Költség	Összesített szám	Összköltség
1. EGYEDI CÉLKITŰZÉS[19]…																		
– Teljesítés																		
– Teljesítés																		
– Teljesítés																		
1. egyedi célkitűzés részösszege																		
2. EGYEDI CÉLKITŰZÉS…																		
– Teljesítés																		
A 2. egyedi célkitűzés részösszege																		
ÖSSZESEN																		

[18] A teljesítés a nyújtandó termékekre és szolgáltatásokra vonatkozik (például: a finanszírozott diákcserék száma, épített utak hossza kilométerben stb.).

[19] Az 1.4.2. pontban ismertetettek szerint „Egyedi célkitűzés(ek)…”.

3.2.3. Az igazgatási előirányzatokra gyakorolt becsült hatás összegzése

– ☐ A javaslat/kezdeményezés nem vonja maga után igazgatási jellegű előirányzatok felhasználását

– ☑ A javaslat/kezdeményezés az alábbi igazgatási jellegű előirányzatok felhasználását vonja maga után:

millió EUR (három tizedesjegyig)

	2023	2024	2025	2026	2027	**ÖSSZESEN**
A többéves pénzügyi keret 7. FEJEZETE						
Humán erőforrás						
Állandó alkalmazottak (AD besorolási fokozat)	1,099	2,041	2,669	3,14	3,14	12,089
Szerződéses alkalmazottak	0,085	0,085	0,085	0,085	0,085	0,425
Egyéb igazgatási kiadások	7,938	8,921	8,921	8,921	8,921	43,622
A többéves pénzügyi keret 7. FEJEZETÉNEK részösszege	9,122	11,047	11,675	12,146	12,146	56,136

A többéves pénzügyi keret 7. FEJEZETÉBE bele nem tartozó előirányzatok[20]						
Humán erőforrás						
Egyéb igazgatási jellegű kiadások						
A többéves pénzügyi keret 7. FEJEZETÉBE bele nem tartozó előirányzatok részösszege						

ÖSSZESEN	9,122	11,047	11,675	12,146	12,146	56,136

A humán erőforrással és más igazgatási jellegű kiadásokkal kapcsolatos előirányzat-igényeket az adott főigazgatóság rendelkezésére álló, az intézkedés irányításához rendelt előirányzatokkal és/vagy az adott főigazgatóságon belüli

[20] Technikai és/vagy igazgatási segítségnyújtás, valamint uniós programok és/vagy intézkedések végrehajtásához biztosított támogatási kiadások (korábban: BA-tételek), közvetett kutatás, közvetlen kutatás.

átcsoportosítással kell teljesíteni. A források adott esetben a költségvetési korlátok betartása mellett kiegészíthetők az éves elosztási eljárás keretében az irányító főigazgatósághoz rendelt további allokációkkal.

3.2.3.1. Becsült humánerőforrás-szükségletek

– ☐ A javaslat/kezdeményezés nem igényel humán erőforrást.

– ☑ A javaslat/kezdeményezés az alábbi humánerőforrás-igénnyel jár:

A becsléseket teljes munkaidős egyenértékben kell kifejezni

		2023	2024	2025	2026	2027		
O A létszámtervben szereplő álláshelyek (tisztviselők és ideiglenes alkalmazottak)								
20 01 02 01 (a központban és a bizottsági képviseleteken)		7	13	17	20	20		
20 01 02 03 (a küldöttségeknél)								
01 01 01 01 (közvetett kutatás)								
01 01 01 11 (közvetlen kutatás)								
Egyéb költségvetési sorok (kérjük megnevezni)								
O Külső munkatársak (teljes munkaidős egyenértékben, azaz FTE-ben kifejezve)[21]								
20 02 01 (AC, END, INT a teljes keretből)		1	1	1	1	1		
20 02 03 (AC, AL, END, INT és JPD a küldöttségeknél)								
XX 01 xx **yy zz** [22]	– a központban							
	– a küldöttségeknél							
01 01 01 02 (AC, END, INT – közvetett kutatás)								
01 01 01 12 (AC, END, INT – közvetlen kutatás)								
Egyéb költségvetési sorok (kérjük megnevezni)								
ÖSSZESEN		**8**	**14**	**18**	**21**	**21**		

XX az érintett szakpolitikai terület vagy költségvetési cím.

A humánerőforrás-igényeknek az adott főigazgatóság rendelkezésére álló, az intézkedés irányításához rendelt és/vagy az adott főigazgatóságon belül átcsoportosított személyzettel kell eleget tenni. A források adott esetben a meglévő költségvetési korlátok betartása mellett kiegészíthetők az éves elosztási eljárás keretében az irányító főigazgatósághoz rendelt további allokációkkal.

Az elvégzendő feladatok leírása:

Tisztviselők és ideiglenes alkalmazottak	A CERT-EU feladatait és tevékenységeit a rendelet, különösen a IV. és V. fejezet szerint a tisztviselők hajtják végre.
Külső munkatársak	A szerződéses alkalmazott segíti az Intézményközi Kiberbiztonsági Testület titkársági feladatait.

[21] AC = szerződéses alkalmazott; AL = helyi alkalmazott; END = kirendelt nemzeti szakértő; INT = kölcsönmunkaerő; JPD = küldöttségi pályakezdő szakértő.

[22] Az operatív előirányzatokból finanszírozott külső munkatársakra vonatkozó részleges felső határérték (korábban: BA-tételek).

3.2.4. A jelenlegi többéves pénzügyi kerettel való összeegyeztethetőség

A javaslat/kezdeményezés:

– ☑ teljes mértékben finanszírozható a többéves pénzügyi keret érintett fejezetén belüli átcsoportosítás révén.

Fejtse ki, miként kell átprogramozni a pénzügyi keretet: tüntesse fel az érintett költségvetési tételeket és a megfelelő összegeket. Jelentős átprogramozás esetén mellékeljen Excel-táblát.

– ☐ a többéves pénzügyi keret lekötetlen mozgásterének és/vagy a többéves pénzügyi keretről szóló rendeletben meghatározott különleges eszközök felhasználását teszi szükségessé.

Fejtse ki, mire van szükség, meghatározva az érintett fejezeteket és költségvetési sorokat, a megfelelő összegeket és a felhasználni javasolt eszközöket.

– ☐ a többéves pénzügyi keret módosítását teszi szükségessé.

Fejtse ki a szükségleteket: tüntesse fel az érintett fejezeteket és költségvetési tételeket és a megfelelő összegeket.

3.2.5. Harmadik felek hozzájárulásai

A javaslat/kezdeményezés:

– ☑ nem irányoz elő harmadik felek általi társfinanszírozást[23]

– ☐ előirányoz harmadik felek általi társfinanszírozást az alábbi becslések szerint:

Előirányzatok, millió EUR (három tizedesjegyig)

	N. év[24]	**N+1. év**	**N+2. év**	**N+3. év**	A táblázat a hatás időtartamának megfelelően (vö. 1.6. pont) további évekkel bővíthető			Összesen
Tüntesse fel a társfinanszírozó szervet								
Társfinanszírozott előirányzatok ÖSSZESEN								

[23] A 12. cikk (5) bekezdésének c) pontjában említett, nem védett szervezeteknek nyújtott szolgáltatások szórványos nyújtásából származó címzett bevételek becslése nem történt meg, mivel a címzett bevételek elhanyagolhatóak.

[24] Az N. év a javaslat/kezdeményezés végrehajtásának első éve. Az „N” helyére a végrehajtás várható első évét kell beírni (például: 2021). A következő évek esetében ugyanígy kell eljárni.

3.3. A bevételre gyakorolt becsült pénzügyi hatás

– ☑ A javaslatnak/kezdeményezésnek nincs pénzügyi hatása a bevételre.

– ☐ A javaslatnak/kezdeményezésnek van pénzügyi hatása – a bevételre gyakorolt hatása a következő:

  – ☐ a javaslat a saját forrásokra gyakorol hatást

  – ☐ a javaslat az egyéb bevételekre gyakorol hatást

  – kérjük adja meg, hogy a bevétel kiadási sorhoz van-e rendelve ☐

millió EUR (három tizedesjegyig)

Bevételi költségvetési sor:	Az aktuális költségvetési évben rendelkezésre álló előirányzatok	A javaslat/kezdeményezés hatása[25]						
		N. év	**N+1. év**	**N+2. év**	**N+3. év**	A táblázat a hatás időtartamának megfelelően (vö. 1.6. pont) további évekkel bővíthető		
… jogcímcsoport								

A címzett bevételek esetében tüntesse fel az érintett költségvetési kiadási sor(oka)t.

Egyéb megjegyzések (pl. a bevételre gyakorolt hatás számítására használt módszer/képlet vagy egyéb más információ).

[25] A tradicionális saját források (vámok, cukorilletékek) tekintetében nettó összeget kell megadni, amely a 20 %-kal (beszedési költségek) csökkentett bruttó összegnek felel meg.