2023/2841

2023.12.18.

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU, Euratom) 2023/2841 RENDELETE

(2023. december 13.)

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 tervezete nemzeti parlamenteknek való megküldését követően,

rendes jogalkotási eljárás keretében ([1]),

mivel:

(1) A digitális korban az információs és kommunikációs technológia a nyitott, hatékony és független európai igazgatás sarokköve. A fejlődő technológia és a digitális rendszerek fokozódó összetettsége és összeköttetése növeli a kiberbiztonsági kockázatokat, ami az uniós szervezeteket még sérülékenyebbé teszi a kiberfenyegetésekkel és biztonsági eseményekkel szemben, ami veszélyezteti ügymeneteik folytonosságát és az adataik biztosítására irányuló képességüket. Míg a felhőalapú szolgáltatások fokozott használata, az információs és kommunikációs technológiák (IKT) mindenütt elterjedt használata, a nagyarányú digitalizáció, a távmunka, valamint a fejlődő technológia és konnektivitás az uniós szervezetek valamennyi tevékenységének alapvető jellemzői, a digitális rezilienciát még nem építették be kellőképpen munkájukba.

(2) Az uniós szervezeteket érintő kiberfenyegetettségi helyzet 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. A fenyegető szereplők egyre gyorsabb ütemben hajtanak végre kibertámadásokat, miközben kampányaik egyre kifinomultabbak és automatizáltabbak, a fenyegetéseknek kitett támadási felületeket célozzák, egyre bővülnek és gyorsan kihasználják a sérülékenységeket.

(3) Az uniós szervezetek IKT-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 egyetlen uniós szervezetre korlátozódik – szélesebb körben lépcsőzetes hatásai lehetnek, ami messzemenő és hosszú távú negatív hatásokat eredményezhet más uniós szervezetekre nézve. Emellett egyes uniós szervezetek IKT-környezete összekapcsolódik a tagállamok IKT-környezetével, ami az egyik uniós szervezetnél felmerülő biztonsági esemény miatt kiberbiztonsági kockázatot jelenthet a tagállamok IKT-környezeteire nézve, és fordítva. A konkrét biztonsági eseményekre vonatkozó információk megosztása emellett megkönnyítheti a tagállamokat érintő hasonló kiberfenyegetések, illetve biztonsági események észlelését is.

(4) Az uniós szervezetek vonzó célpontok, amelyek magasan képzett és megfelelő erőforrásokkal rendelkező fenyegető szereplőkkel, valamint egyéb fenyegetésekkel szembesülnek. A kiberbiztonsági ellenállóképesség 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 uniós szervezetek működéséhez szükséges, hogy az azonosított kiberbiztonsági kockázatokkal arányos kiberbiztonsági intézkedések végrehajtása, az információcsere és az együttműködés révén egységesen magas szintű kiberbiztonságot érjenek el.

([1]) Az Európai Parlament 2023. november 21-i álláspontja (a Hivatalos Lapban még nem tették közzé) és a Tanács 2023. december 8-i határozata.

(5) Az (EU) 2022/2555 európai parlamenti és tanácsi irányelv ([2]) célja az állami és magánszervezetek, az illetékes hatóságok és szervek, valamint az egész Unió kiberbiztonsági ellenállóképességének és biztonsági eseményekre való reagálási képességének további javítása. Ezért szükséges biztosítani, hogy az uniós szervezetek hasonló szellemben cselekedjenek azáltal, hogy olyan szabályokról gondoskodnak, amelyek összhangban vannak az (EU) 2022/2555 irányelvvel, és tükrözik annak ambíciószintjét.

(6) A kiberbiztonság egységesen magas szintjének elérése érdekében minden uniós szervezetnek olyan belső kiberbiztonsági kockázatkezelési, -irányítási és -ellenőrzési keretrendszert (a továbbiakban: a keretrendszer) kell létrehoznia, amely biztosítja az összes kiberbiztonsági kockázat hatékony és prudens kezelését, és figyelembe veszi az ügymenet-folytonosságot és a válságkezelést. A keretrendszernek meg kell határoznia a hálózati és információs rendszerek biztonságára vonatkozó kiberbiztonsági politikákat, beleértve a célokat és prioritásokat, a nem minősített IKT-környezet egészére kiterjedően. A keretrendszernek minden veszélyre kiterjedő megközelítésen kell alapulnia, amelynek célja a hálózati és információs rendszereknek és azok fizikai környezetének a védelme minden olyan eseménytől, mint például a lopás, a tűz, az árvíz, a távközlési és áramellátási zavarok, vagy a szervezet információs és információfeldolgozó létesítményeihez való jogosulatlan fizikai hozzáférés, az azokban keletkezett kár és az azokon végrehajtott beavatkozás, amely veszélyeztetheti a tárolt, továbbított vagy kezelt adatok vagy a hálózati és információs rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, hitelességét, integritását vagy bizalmas jellegét.

(7) A keretrendszerben azonosított kiberbiztonsági kockázatok kezelése érdekében minden uniós szervezetnek meg kell hoznia a megfelelő és arányos technikai, működési és szervezeti intézkedéseket. Ezeknek az intézkedéseknek az egyes uniós szervezetek kiberbiztonságának megerősítése céljából az e rendeletben meghatározott területekre kell kiterjedniük, ideértve a kiberbiztonsági kockázatkezelési intézkedéseket is.

(8) A keretrendszerben azonosított eszközöknek és kiberbiztonsági kockázatoknak, valamint a rendszeres kiberbiztonsági érettségi értékelésekből levont következtetéseknek tükröződniük kell az egyes uniós szervezetek által létrehozott kiberbiztonsági tervekben. A kiberbiztonsági tervnek tartalmaznia kell az elfogadott kiberbiztonsági kockázatkezelési intézkedéseket.

(9) Mivel a kiberbiztonság garantálása állandó folyamat, az e rendelet értelmében meghozott intézkedések alkalmasságát és hatékonyságát rendszeresen felül kell vizsgálni az uniós szervezetek változó kiberbiztonsági kockázatainak, eszközeinek és kiberbiztonsági érettségének fényében. A keretrendszert rendszeresen, de legalább négyévente, a kiberbiztonsági tervet pedig kétévente – vagy szükség esetén gyakrabban – a keretrendszer kiberbiztonsági érettségi értékelését vagy jelentős felülvizsgálatát követően felül kell vizsgálni.

(10) Az uniós szervezetek által bevezetett kiberbiztonsági kockázatkezelési intézkedéseknek olyan politikákat kell magukban foglalniuk, amelyek lehetőség szerint a forráskód átláthatóvá tételére irányulnak, figyelembe véve a harmadik felek vagy az uniós szervezetek jogaira vonatkozó biztosítékokat. Ezeknek a politikáknak arányosnak kell lenniük a kiberbiztonsági kockázattal, és céljuk a kiberfenyegetések elemzésének megkönnyítése, ugyanakkor nem keletkeztetnek az alkalmazandó szerződéses feltételeken túlmenő, harmadik felek kódjának közzétételére vonatkozó kötelezettségeket vagy az ahhoz való hozzáférésre vonatkozó jogokat.

(11) A nyílt forráskódú kiberbiztonsági eszközök és alkalmazások nagyobb fokú nyitottságot biztosíthatnak. A nyílt szabványok elősegítik a biztonsági eszközök közötti interoperabilitást, ami az érdekelt felek biztonságát is szolgálja. A nyílt forráskódú kiberbiztonsági eszközök és alkalmazások ösztönözhetik a szélesebb fejlesztői közösséget, lehetővé téve a beszállítók diverzifikálását. A nyílt forráskód a kiberbiztonsággal kapcsolatos eszközök átláthatóbb ellenőrzési folyamatához és a sérülékenységek közösségi alapú felderítéséhez vezethet. Az uniós szervezeteknek ezért képesnek kell lenniük arra, hogy előmozdítsák a nyílt forráskódú szoftverek és nyílt szabványok használatát a nyílt hozzáférésű adatok és a nyílt forráskódok – az átláthatóságon alapuló biztonság részeként történő – felhasználásával kapcsolatos szakpolitikák folytatása révén.

([2]) Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről, a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv) (HL L 333., 2022.12.27., 80. o.).

(12) Az uniós szervezetek közötti különbségek rugalmasságot tesznek szükségessé e rendelet végrehajtása terén. Az e rendeletben előírt, a kiberbiztonság egységesen magas szintjére vonatkozó intézkedések nem tartalmazhatnak olyan kötelezettségeket, amelyek közvetlenül ütköznek az uniós szervezetek feladatainak ellátásával, vagy beavatkoznak intézményi autonómiájukba. Ezért ezeknek a szervezeteknek létre kell hozniuk saját keretrendszereiket, és el kell fogadniuk saját kiberbiztonsági kockázatkezelési intézkedéseiket és kiberbiztonsági terveiket. Ezen intézkedések végrehajtása során – az erőforrások megfelelő kezelése és a költségoptimalizálás érdekében – kellően figyelembe kell venni az uniós szervezetek között fennálló szinergiákat. Kellő körültekintéssel biztosítani kell azt is, hogy az intézkedések ne befolyásolják hátrányosan az uniós szervezetek egymás között folytatott hatékony információcseréjét és együttműködését, valamint az uniós szervezetek és a tagállami partnerek között folytatott hatékony információcserét és együttműködést.

(13) Az erőforrások felhasználásának optimalizálása érdekében e rendeletnek lehetővé kell tennie, hogy két vagy több, hasonló struktúrákkal rendelkező uniós szervezet együttműködjön saját szervezeteik kiberbiztonsági érettségi értékelésének elvégzésében.

(14) Annak elkerülése érdekében, hogy az uniós szervezetekre aránytalanul nagy pénzügyi és adminisztratív terhek háruljanak, a kiberbiztonsági kockázatok kezelésére vonatkozó követelményeknek – a legújabb technikai lehetőségekre figyelemmel – arányosaknak kell lenniük a hálózati és információs rendszereket fenyegető kockázatokkal. Minden uniós szervezetnek törekednie kell arra, hogy IKT-költségvetésének megfelelő százalékát a kiberbiztonsági szintjének javítására fordítsa. Hosszabb távon legalább 10 %-os nagyságrendű indikatív célkitűzés elérésére kell törekedni. A kiberbiztonsági érettségi értékelésben fel kell mérni, hogy az uniós szervezet kiberbiztonsági kiadásai arányosak-e az előtte álló kiberbiztonsági kockázatokkal. A Szerződések szerint az Unió éves költségvetésére vonatkozó szabályok sérelme nélkül a Bizottságnak az e rendelet hatálybalépését követően elfogadandó első éves költségvetésre vonatkozó javaslatában figyelembe kell vennie az e rendeletből eredő kötelezettségeket, amikor értékeli az uniós szervezeteknél a tervezett kiadásaikból eredően felmerülő költségvetési és személyzeti igényeket.

(15) A kiberbiztonság egységesen magas szintje megköveteli, hogy a kiberbiztonság minden egyes uniós szervezetben a legmagasabb vezetői szint felügyelete alá tartozzon. E rendelet végrehajtásáért, többek között a keretrendszer létrehozásáért, a kiberbiztonsági kockázatkezelési intézkedések meghozataláért és a kiberbiztonsági terv jóváhagyásáért az uniós szervezet legmagasabb vezetői szintjének kell felelnie. A kiberbiztonsági kultúra, azaz a kiberbiztonság napi gyakorlatának kezelése szerves részét képezi a keretrendszernek, valamint a kapcsolódó kiberbiztonsági kockázatkezelési intézkedéseknek valamennyi uniós szervezetben.

(16) Alapvető fontosságú az EU-minősített adatokat kezelő hálózati és információs rendszerek biztonsága. Az EU-minősített adatokat kezelő uniós szervezeteknek kötelező alkalmazniuk az ilyen információk védelmét szolgáló átfogó szabályozási keretrendszereket, többek között konkrét irányítási, szakpolitikai és kockázatkezelési eljárásokat. Az EU-minősített adatokat kezelő hálózati és információs rendszereknek szigorúbb biztonsági előírásoknak kell megfelelniük, mint a nem minősített hálózati és információs rendszereknek. Ezért az EU-minősített adatokat kezelő hálózati és információs rendszerek reziliensebbek a kiberfenyegetésekkel és a biztonsági eseményekkel szemben. Következésképpen, elismerve, hogy e tekintetben közös keretrendszerre van szükség, ez a rendelet nem alkalmazandó az EU-minősített adatokat kezelő hálózati és információs rendszerekre. Amennyiben azonban valamely uniós szervezet ezt kifejezetten kéri, az uniós intézmények, szervek és hivatalok hálózatbiztonsági vészhelyzeteket elhárító csoportja (a továbbiakban: a CERT-EU) számára lehetővé kell tenni, hogy segítséget nyújtson az adott uniós szervezetnek a minősített IKT-környezetekben bekövetkező biztonsági eseményekkel kapcsolatban.

(17) Az uniós szervezeteknek fel kell mérniük a beszállítókkal és szolgáltatókkal – többek között az adattárolási és -kezelési szolgáltatások nyújtóival vagy az irányított biztonsági szolgáltatásokkal – fenntartott kapcsolatokból eredő kiberbiztonsági kockázatokat, és megfelelő intézkedéseket kell hozniuk azok kezelésére. A kiberbiztonsági intézkedéseket a CERT-EU által kiadott iránymutatásokban vagy ajánlásokban részletesebben meg kell határozni. Az intézkedések és iránymutatások meghatározásakor megfelelően figyelembe kell venni a technika állását, továbbá adott esetben a vonatkozó európai és nemzetközi szabványokat, valamint az idevágó uniós jogszabályokat és szakpolitikákat, többek között az (EU) 2022/2555 irányelv 14. cikke alapján létrehozott együttműködési csoport által kiadott kiberbiztonsági kockázatértékeléseket és ajánlásokat, például az 5G-hálózatok kiberbiztonságának összehangolt uniós kockázatértékelését és az 5G kiberbiztonsággal kapcsolatos uniós eszköztárat. Emellett a

kiberfenyegetettségi helyzetet és az uniós szervezetek kiberbiztonsági ellenállóképessége kialakításának fontosságát figyelembe véve az (EU) 2019/881 európai parlamenti és tanácsi rendelet ([3]) 49. cikke alapján elfogadott konkrét európai kiberbiztonsági tanúsítási rendszerek keretében szükség lehet az IKT-termékek, -szolgáltatások és -folyamatok tanúsítására.

(18) 2011 májusában az uniós intézmények és szervek főtitkárai úgy határoztak, hogy létrehozzák a CERT-EU előzetes szervezési 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 a 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 ([4]). E rendeletnek átfogó szabályokat kell előírnia a CERT-EU szervezetére, működésére és működtetésére vonatkozóan. E rendelet rendelkezései elsőbbséget élveznek a CERT-EU szervezetéről és működéséről szóló, 2017 decemberében megkötött intézményközi megállapodás rendelkezéseivel szemben.

(19) A CERT-EU-t az uniós intézményeket, szerveket, hivatalokat és ügynökségeket támogató „Kiberbiztonsági Szolgálatra" kell átnevezni, de a névfelismerés céljából meg kell tartani a „CERT-EU" rövid nevet.

(20) A CERT-EU több feladattal és kibővített szereppel való felruházása mellett e rendelet – az egységesen magas szintű kiberbiztonság uniós szervezetek körében való biztosításának megkönnyítése érdekében – létrehozza az Intézményközi Kiberbiztonsági Testületet (a továbbiakban: az IICB). Az IICB-nek kizárólagos szerepet kell kapnia e rendelet uniós szervezetek általi végrehajtásának nyomon követésében és támogatásában, az általános prioritások és célkitűzések CERT-EU általi végrehajtásának felügyeletében, és a CERT-EU-nak nyújtott stratégiai iránymutatásban. Az IICB-nek ennélfogva biztosítania kell az uniós intézmények képviseletét, és magában kell foglalnia az uniós szervek, hivatalok és ügynökségek képviselőit az uniós ügynökségek hálózatán (a továbbiakban: az EUAN) keresztül. Az IICB szervezetét és működését tovább kell szabályozni belső eljárási szabályzattal, amely magában foglalhat további pontosításokat az IICB rendszeres ülései tekintetében, beleértve azokat az éves politikai szintű találkozókat is, amelyeken az IICB valamennyi tagja legmagasabb vezetői szintjének képviselői jelenlétében az IICB stratégiai megbeszéléseket folytathatna, és stratégiai iránymutatást kaphatna. Ezen túlmenően az IICB végrehajtó bizottságot hozhat létre, amelytől munkájához segítséget kaphat és amelyre átruházhatja egyes feladatait és hatásköreit, különösen a tagjaitól különleges szakértelmet igénylő olyan feladatok tekintetében, mint például a szolgáltatási katalógus jóváhagyása és későbbi frissítései, a szolgáltatási szintre vonatkozó megállapodásokra vonatkozó szabályok, az uniós szervezetek által az IICB-nek e rendelet szerint benyújtott dokumentumok és jelentések értékelése, illetve az IICB által kibocsátott, megfelelőségi intézkedésekről szóló határozatok kidolgozásával és azok végrehajtásának nyomon követésével kapcsolatos teendők. Az IICB-nek meg kell állapítania a végrehajtó bizottság eljárási szabályzatát, beleértve annak feladatait és hatásköreit.

(21) Az IICB célja, hogy e rendelet végrehajtásán keresztül támogassa az uniós szervezeteket saját kiberbiztonsági helyzetük javításában. Az uniós szervezetek támogatása érdekében az IICB-nek iránymutatást kell nyújtania a CERT-EU vezetője számára, többéves stratégiát kell elfogadnia az uniós szervezetek kiberbiztonsági szintjének emelésére vonatkozóan, meg kell határoznia az önkéntes szakértői értékelések módszertanát és egyéb szempontjait, valamint elő kell segítenie a helyi kiberbiztonsági tisztviselők informális csoportjának létrehozását az Európai Uniós Kiberbiztonsági Ügynökség (a továbbiakban: az ENISA) támogatásával, az e rendelet végrehajtásával kapcsolatos bevált gyakorlatok és információk cseréje céljából.

([3]) 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.).

([4]) Megállapodás az Európai Parlament, az Európai Tanács, az Európai Unió Tanácsa, az Európai Bizottság, az Európai Unió Bírósága, az Európai Központi Bank, az Európai Számvevőszék, az Európai Külügyi Szolgálat, az Európai Gazdasági és Szociális Bizottság, a Régiók Európai Bizottsága és az Európai Beruházási Bank között az uniós intézmények, szervek és ügynökségek hálózatbiztonsági vészhelyzeteket elhárító csoportjának (CERT-EU) szervezetéről és működéséről (HL C 12., 2018.1.13., 1. o.).

(22) Az összes uniós szervezet magas szintű kiberbiztonságának elérése érdekében a saját IKT-környezetüket működtető uniós szervek, hivatalok és ügynökségek érdekeit az EUAN által kijelölt három képviselőnek kell képviselnie az IICB-ben. A személyes adatok kezelésének biztonsága, és ezért annak kiberbiztonsága is az adatvédelem sarokköve. Az adatvédelem és a kiberbiztonság közötti szinergiák fényében az európai adatvédelmi biztosnak az e rendelet hatálya alá tartozó, az adatvédelem, többek között az elektronikus hírközlő hálózatok biztonsága területén is különleges szakértelemmel rendelkező uniós szervezetként képviseltetnie kell magát az IICB-ben. Tekintettel az innováció és a versenyképesség fontosságára a kiberbiztonság terén, az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontnak képviseltetnie kell magát az IICB-ben. Tekintettel az ENISA kiberbiztonsági szakértői központként betöltött szerepére és az ENISA által nyújtott támogatásra, valamint az uniós űrinfrastruktúra és -szolgáltatások kiberbiztonságának fontosságára, az ENISA-nak és az Európai Unió Űrprogramügynökségének képviseltetnie kell magát az IICB-ben. Tekintettel az e rendelet értelmében a CERT-EU-ra ruházott szerepre, az IICB elnökének meg kell hívnia a CERT-EU vezetőjét az IICB valamennyi ülésére, kivéve, ha az IICB közvetlenül a CERT-EU vezetőjéhez kapcsolódó kérdéseket vitat meg.

(23) Az IICB-nek ellenőriznie kell az e rendeletnek való megfelelést, továbbá nyomon kell követnie az iránymutatások és az ajánlások végrehajtását, valamint a cselekvési felhívásokat. Az IICB-t technikai kérdésekben az IICB által megfelelőnek tartott technikai tanácsadó csoportoknak kell támogatniuk. E technikai tanácsadó csoportoknak szükség esetén szorosan együtt kell működniük a CERT-EU-val, az uniós szervezetekkel, valamint más érdekelt felekkel.

(24) Amennyiben az IICB megállapítja, hogy egy uniós szervezet nem alkalmazta hatékonyan ezt a rendeletet vagy az annak alapján kiadott iránymutatásokat, ajánlásokat és cselekvési felhívásokat, az IICB az érintett uniós szervezet belső eljárásainak sérelme nélkül megfelelési intézkedéseket alkalmazhat. Az IICB-nek fokozatosan kell alkalmaznia a megfelelési intézkedéseket – más szóval az IICB-nek először a legkevésbé szigorú intézkedést, azaz indokolással ellátott véleményt kell elfogadnia, és csak szükség esetén egyre szigorúbb intézkedéseket, amelyek a legszigorúbb intézkedéshez, azaz az érintett uniós szervezet felé irányuló adatáramlás ideiglenes felfüggesztésére vonatkozó ajánláshoz vezetnek. Ilyen ajánlás csak abban a kivételes esetben alkalmazható, ha az érintett uniós szervezet hosszú távon, szándékosan, ismétlődően vagy súlyosan megsérti e rendeletet.

(25) Az indokolással ellátott vélemény a legkevésbé szigorú megfelelési intézkedés az e rendelet végrehajtásában észlelt hiányosságok orvoslására. Az IICB számára lehetővé kell tenni, hogy nyomon kövesse az indokolással ellátott véleményt, iránymutatással segítve az uniós szervezetet annak biztosításában, hogy keretrendszere, kiberbiztonsági kockázatkezelési intézkedései, kiberbiztonsági terve és jelentéstétele megfeleljen e rendeletnek, majd figyelmeztetést adjon ki az uniós szervezet azonosított hiányosságainak meghatározott időn belüli kezelésére. Amennyiben a figyelmeztetésben feltárt hiányosságokat nem orvosolják megfelelően, az IICB számára lehetővé kell tenni, hogy indokolással ellátott értesítést adjon ki.

(26) A IICB számára lehetővé kell tenni, hogy audit végzését ajánlja az uniós szervezetnél. Az uniós szervezet számára lehetővé kell tenni, hogy e célból igénybe vegye belső ellenőrzési részlegét. Az IICB számára azt is lehetővé kell tenni, hogy kérje, hogy az auditot harmadik fél ellenőrzési szolgálata, például egy kölcsönösen elfogadott magánszektorbeli szolgáltató végezze.

(27) Amennyiben egy uniós szervezet kivételes esetekben hosszú távon, szándékosan, ismétlődően vagy súlyosan megsérti e rendeletet, az IICB számára lehetővé kell tenni, hogy végső megoldásként valamennyi tagállamnak és uniós szervezetnek ajánlja az uniós szervezet felé irányuló adatáramlás ideiglenes felfüggesztését, amelyet addig kell alkalmazni, amíg az uniós szervezet véget nem vet a jogsértésnek. Ezt az ajánlást megfelelő és biztonságos kommunikációs csatornákon keresztül kell közölni.

(28) E rendelet helyes végrehajtásának biztosítása érdekében az IICB-nek – amennyiben úgy ítéli meg, hogy e rendeletnek valamely uniós szervezet általi tartós megsértését közvetlenül a személyzete valamely tagjának cselekményei vagy mulasztásai okozták, többek között a legmagasabb vezetői szinten – fel kell kérnie az érintett uniós szervezetet, hogy tegye meg a megfelelő intézkedéseket, beleértve a fegyelmi eljárás kezdeményezésének megfontolását is, a 259/68/EGK, Euratom, ESZAK tanácsi rendelettel ([5]) megállapított, az Európai Unió tisztviselőinek személyzeti szabályzatában és az Unió egyéb alkalmazottaira vonatkozó alkalmazási feltételekben (a továbbiakban: a személyzeti szabályzat) megállapított szabályokkal és eljárásokkal, valamint bármely más alkalmazandó szabállyal és eljárással összhangban.

(29) A CERT-EU-nak hozzá kell járulnia valamennyi uniós szervezet IKT-környezetének biztonságához. Annak mérlegelésekor, hogy valamely uniós szervezet kérésére adjon-e technikai tanácsot vagy nyilvánítson-e technikai véleményt releváns szakpolitikai kérdésekben, a CERT-EU-nak biztosítania kell, hogy az ne akadályozza az e rendelet értelmében rá bízott egyéb feladatok teljesítését. A CERT-EU-nak az uniós szervezetek részéről az (EU) 2022/2555 irányelv 12. cikkének (1) bekezdése szerint a sérülékenységek összehangolt közzététele céljából kijelölt koordinátorral egyenértékűként kell eljárnia.

(30) A CERT-EU-nak támogatnia kell a kiberbiztonság egységesen magas szintjét célzó intézkedések végrehajtását az IICB-nek szóló iránymutatásokra és ajánlásokra irányuló javaslatok vagy cselekvési felhívások közzététele révén. Az ilyen iránymutatásokat 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 szervezeteknek meghatározott időn belül meg kell hozniuk. Az IICB-nek utasítania kell a CERT-EU-t, hogy adjon ki, vonjon vissza vagy módosítson iránymutatásokra vagy ajánlásokra vonatkozó javaslatokat, illetve cselekvési felhívásokat.

(31) A CERT-EU-nak az (EU) 2022/2555 irányelvben meghatározott további, a számítógép-biztonsági eseményekre reagáló csoportok (a továbbiakban: a CSIRT-ek) említett irányelv 15. cikke értelmében létrehozott hálózatával való együttműködésre és információcserére irányuló szerepét is be kell töltenie. Emellett az (EU) 2017/1584 bizottsági ajánlással ([6]) 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 tagállami partnerekkel. A CERT-EU-nak más állami és magánpartnerekkel is együtt kell működnie, többek között az Észak-atlanti Szerződés Szervezetében, az IICB előzetes jóváhagyásával.

(32) Az operatív kiberbiztonság támogatása során a CERT-EU-nak az (EU) 2019/881 rendeletben előírt strukturált együttműködés révén igénybe kell vennie az ENISA rendelkezésre álló szakértelmét. Adott esetben a két szervezet között külön megállapodásokat kell kötni az együttműködés gyakorlati megvalósításának meghatározása és a párhuzamos tevékenységek elkerülése érdekében. A CERT-EU-nak együtt kell működnie az ENISA-val a kiberfenyegetettségi elemzés terén, és rendszeresen meg kell osztania az ENISA-val a fenyegetettségi helyzetjelentését.

(33) A CERT-EU számára lehetővé kell tenni, hogy együttműködjön és információkat osszon meg az Unión és tagállamain belüli releváns kiberbiztonsági közösségekkel az operatív együttműködés előmozdítása és annak lehetővé tétele érdekében, hogy a meglévő hálózatok teljes mértékben kiaknázhassák az Unió védelme terén bennük rejlő lehetőségeket.

(34) Mivel a CERT-EU szolgáltatásai és feladatai az uniós szervezetek érdekét szolgálják, az IKT-kiadásokkal rendelkező valamennyi uniós szervezetnek méltányos részt kell vállalnia e szolgáltatások és feladatok finanszírozásából. Ezek a hozzájárulások nem érintik az uniós szervezetek költségvetési autonómiáját.

([5]) A Tanács 259/68/EGK, Euratom, ESZAK rendelete (1968. február 29.) az Európai Közösségek tisztviselőinek személyzeti szabályzatáról, egyéb alkalmazottainak alkalmazási feltételeiről, valamint a Bizottság tisztviselőire ideiglenesen alkalmazandó különleges intézkedések bevezetéséről (HL L 56., 1968.3.4., 1. o.).

([6]) 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.).

(35) Számos kibertámadás olyan szélesebb körű kampányok részét képezi, amelyek az uniós szervezetek csoportjait, illetve az uniós szervezeteket is magukban foglaló érdekközösségeket célozzák. A proaktív felderítés, a biztonsági eseményekre való reagálás vagy a mérséklő intézkedések és a biztonsági események utáni helyreállítás lehetővé tétele érdekében az uniós szervezetek számára lehetővé kell tenni, hogy értesítsék a CERT-EU-t a biztonsági eseményekről, a kiberfenyegetésekről, a sérülékenységekről és a majdnem bekövetkezett (near miss) eseményekről, és megosszák azokat a megfelelő technikai részleteket, amelyek lehetővé teszik a más uniós szervezeteknél előforduló, hasonló biztonsági események, kiberfenyegetések, sérülékenységek és majdnem bekövetkezett (near miss) események észlelését vagy mérséklését, valamint az azokra való reagálást. Az (EU) 2022/2555 irányelvben szereplővel megegyező megközelítést követve, az uniós szervezeteknek a jelentős biztonsági eseményről való tudomásszerzéstől számított 24 órán belül korai előrejelzést kell benyújtaniuk a CERT-EU-nak. Az ilyen információcserének lehetővé kell tennie a CERT-EU számára, hogy továbbítsa az információkat más uniós szervezeteknek, valamint a megfelelő partnereknek, hogy segítsen megvédeni az uniós szervezetek IKT-környezetét és az uniós szervezetek partnereinek IKT-környezetét a hasonló biztonsági eseményekkel szemben.

(36) Ez a rendelet többlépcsős megközelítést állapít meg a jelentős biztonsági események bejelentésével kapcsolatban annak érdekében, hogy megtalálja a megfelelő egyensúlyt egyrészt a gyors bejelentések között, amelyek segítenek mérsékelni a jelentős biztonsági események potenciális terjedését, és lehetővé teszik az uniós szervezetek számára, hogy segítséget kérjenek, másrészt pedig az olyan mélyreható jelentéstétel érdekében, amely értékes tanulságokat von le az egyes biztonsági eseményekből, és idővel javítja az uniós szervezetek kiberbiztonsági ellenállóképességét, továbbá hozzájárul az általános kiberbiztonsági helyzetük javításához. E tekintetben e rendeletnek ki kell terjednie azon biztonsági események bejelentésére is, amelyek – az érintett uniós szervezet által végzett kezdeti értékelés alapján – jelentős működési zavart eredményezhetnek az uniós szervezet működésében, vagy pénzügyi veszteséggel járhatnak az érintett uniós szervezet számára, vagy jelentős vagyoni vagy nem vagyoni kár okozásával érinthetnek más természetes vagy jogi személyeket. E kezdeti értékelésnek figyelembe kell vennie többek között az érintett hálózati és információs rendszereket, különösen azok jelentőségét az uniós szervezet működése szempontjából, a kiberfenyegetés súlyosságát és technikai jellemzőit, minden kihasznált mögöttes sérülékenységet, valamint az uniós szervezet hasonló biztonsági eseményekkel kapcsolatos tapasztalatait. Annak meghatározásában, hogy a működési zavar súlyos-e, fontos szerepet játszhatnak olyan mutatók, mint például az uniós szervezet működési érintettségének mértéke, a biztonsági esemény időtartama, illetve az érintett természetes vagy jogi személyek száma.

(37) Mivel az érintett uniós szervezet infrastruktúrája és hálózati és információs rendszerei, valamint az uniós szervezet székhelye szerinti tagállam infrastruktúrája és hálózatai összekapcsolódnak, alapvető fontosságú, hogy a szóban forgó tagállamot indokolatlan késedelem nélkül tájékoztassák az adott uniós szervezeten belüli jelentős biztonsági eseményről. E célból az érintett uniós szervezetnek tájékoztatnia kell az (EU) 2022/2555 irányelv 8. és 10. cikke alapján kijelölt vagy létrehozott érintett tagállami partnereket az olyan jelentős biztonsági események bekövetkezéséről, amelyekről a CERT-EU-nak jelentést tesz. Amennyiben a CERT-EU valamely tagállamban bekövetkező jelentős biztonsági eseményről szerez tudomást, értesítenie kell az érintett partnert az adott tagállamban.

(38) Olyan mechanizmust kell bevezetni, amely súlyos biztonsági események esetén biztosítja az uniós szervezetek közötti hatékony információcserét, koordinációt és együttműködést, beleértve az érintett uniós szervezetek szerepének és felelősségi körének egyértelmű meghatározását. A Bizottság IICB-ben részt vevő képviselőjének – a kiberbiztonsági válságkezelési tervtől függően – kapcsolattartó pontként kell szolgálnia, hogy megkönnyítse az IICB számára a súlyos biztonsági eseményekkel kapcsolatos lényeges információk megosztását az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatával (a továbbiakban: az EU-CyCLONe), hozzájárulva ezzel a közös helyzetismerethez. A Bizottság IICB-ben részt vevő képviselőjének kapcsolattartó pontként betöltött szerepe nem sértheti a Bizottságnak az EU-CyCLONe-ban az (EU) 2022/2555 irányelv 16. cikkének (2) bekezdése szerint betöltött különálló és elkülönülő szerepét.

(39) A személyes adatok e rendelet alapján történő kezelésére az (EU) 2018/1725 európai parlamenti és tanácsi rendelet ([7]) alkalmazandó. A személyes adatok kezelésére a kiberbiztonsági kockázatkezelés, a sérülékenységek és a biztonsági események kezelése, a biztonsági eseményekkel, kiberfenyegetésekkel és sérülékenységekkel kapcsolatos információk megosztása, valamint a biztonsági eseményekre való reagálás koordinációja és az ezzel kapcsolatos együttműködés keretében elfogadott intézkedésekkel összefüggésben kerülhet sor. Az ilyen intézkedések szükségessé tehetik a személyes adatok bizonyos kategóriáinak – például IP-címek, egységes forrás-helymeghatározók (URL), doménnevek, e-mail-címek, az érintett szervezeti szerepe, időbélyegzők, e-mailek tárgya

([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.).

vagy fájlnevek – kezelését. Az e rendelet alapján hozott valamennyi intézkedésnek meg kell felelnie az adatvédelmi és a magánélet védelmére vonatkozó keretnek, és az uniós szervezeteknek, a CERT-EU-nak és adott esetben az IICB-nek minden releváns technikai és szervezeti biztosítékot rendelkezésre kell bocsátaniuk a megfelelés elszámoltatható módon történő biztosítása érdekében.

(40) Ez a rendelet az (EU) 2018/1725 rendelet 5. cikke (1) bekezdésének b) pontjával összhangban megteremti a jogalapot a személyes adatoknak az uniós szervezetek, a CERT-EU és adott esetben az IICB által az e rendelet szerinti feladataik ellátása és kötelezettségeik teljesítése céljából végzett kezelésére. A CERT-EU az (EU) 2018/1725 rendelet szerint végzett feladatától függően adatfeldolgozóként vagy adatkezelőként járhat el.

(41) Bizonyos esetekben az e rendelet szerinti, a kiberbiztonság magas szintjének biztosítására irányuló kötelezettségeik teljesítése céljából és különösen a sérülékenységek és a biztonsági események kezelésével összefüggésben szükségessé válhat, hogy az uniós szervezetek és a CERT-EU a személyes adatok (EU) 2018/1725 rendelet 10. cikkének (1) bekezdésében említett különleges kategóriáit kezeljék. Ez a rendelet megteremti a jogalapot a személyes adatok különleges kategóriáinak az uniós szervezetek és a CERT-EU általi kezelésére az (EU) 2018/1725 rendelet 10. cikke (2) bekezdésének g) pontjával összhangban. A személyes adatok különleges kategóriái e rendelet szerinti kezelésének szigorúan arányosnak kell lennie az elérni kívánt céllal. Az említett rendelet 10. cikke (2) bekezdésének g) pontjában meghatározott feltételekre is figyelemmel az uniós szervezetek és a CERT-EU csak a szükséges mértékben és abban az esetben kezelhetik ezeket az adatokat, ha azt e rendelet kifejezetten előírja. A személyes adatok különleges kategóriáinak kezelése során az uniós szervezeteknek és a CERT-EU-nak tiszteletben kell tartaniuk a személyes adatok védeleméhez való jog lényeges tartalmát, és megfelelő és konkrét intézkedéseket kell előírniuk az érintettek alapvető jogainak és érdekeinek biztosítására.

(42) Az (EU) 2018/1725 rendelet 33. cikke értelmében az uniós szervezeteknek és a CERT-EU-nak a tudomány és a technológia állása, a megvalósítás költségei, valamint az adatkezelés jellege, hatóköre, körülményei és céljai, továbbá a természetes személyek jogait és szabadságait érintő, változó valószínűségű és súlyosságú kockázatok figyelembevételével megfelelő technikai és szervezési intézkedéseket kell végrehajtania annak érdekében, hogy biztosítsa a személyes adatok megfelelő szintű biztonságát, mint például korlátozott hozzáférési jogok biztosítása a szükséges ismeret elve alapján, az ellenőrzési nyomvonal elveinek alkalmazása, felügyeleti lánc elfogadása, az inaktív adatok ellenőrzött és ellenőrizhető környezetben való tárolása, szabványosított működési eljárások és a magánélet védelmét biztosító intézkedések, például az álnevesítés vagy a titkosítás. Ezeket az intézkedéseket nem szabad olyan módon végrehajtani, hogy az befolyásolja a biztonsági események kezelésének és a bizonyítékok sértetlenségének célját. Amennyiben egy uniós szervezet vagy a CERT-EU e rendelet alkalmazásában egy biztonsági eseményhez kapcsolódó személyes adatokat – többek között személyes adatok különleges kategóriáit – továbbít egy partnernek, az ilyen adattovábbításnak meg kell felelnie az (EU) 2018/1725 rendeletnek. Amennyiben a személyes adatok különleges kategóriáit harmadik félnek továbbítják, az uniós szervezeteknek és a CERT-EU-nak biztosítaniuk kell, hogy a harmadik fél az (EU) 2018/1725 rendelettel egyenértékű szintű intézkedéseket alkalmazzon a személyes adatok védelmére vonatkozóan.

(43) Az e rendelet alkalmazásában kezelt személyes adatok az (EU) 2018/1725 rendelettel összhangban csak a szükséges ideig őrizhetők meg. Az adatkezelőként eljáró uniós szervezeteknek és adott esetben a CERT-EU-nak olyan adattárolási időtartamokat kell meghatározniuk, amelyek a meghatározott célok eléréséhez szükséges mértékre korlátozódnak. Különösen a biztonsági események kezelése céljából gyűjtött személyes adatok tekintetében az uniós szervezeteknek és a CERT-EU-nak különbséget kell tenniük az IKT-környezetükben előforduló kiberfenyegetés észlelése céljából a biztonsági események megelőzése érdekében gyűjtött személyes adatok és a biztonsági események mérséklése, az azokra való reagálás és az azokat követő helyreállítás céljából gyűjtött személyes adatok között. A kiberfenyegetés észleléséhez fontos figyelembe venni azt az időt, amely alatt a fenyegető szereplő észrevétlenül maradhat egy rendszerben. A biztonsági események mérséklése, az azokra való reagálás és az azokat követő helyreállítás érdekében fontos mérlegelni, hogy a személyes adatokra visszatérő biztonsági események vagy hasonló jellegű olyan biztonsági események nyomon követéséhez és kezeléséhez van-e szükség, amelyekkel kapcsolatban bizonyítható az eseménnyel való összefüggés.

(44) Az uniós szervezetek és a CERT-EU általi információkezelésnek meg kell felelnie az információbiztonság tekintetében alkalmazandó szabályoknak. A humánerőforrás-biztonság kiberbiztonsági kockázatkezelési intézkedések közé való bevonásának az alkalmazandó szabályoknak is meg kell felelnie.

(45) Az információk megosztása céljára látható jelölések használatosak annak jelzésére, hogy az információk címzettjeinek be kell tartaniuk bizonyos korlátokat a megosztást illetően, különösen titoktartási megállapodások, illetve olyan informális titoktartási megállapodások, mint például a jelzőlámpa-protokoll alapján, vagy a forrás általi egyéb egyértelmű megjelölés alapján. A jelzőlámpa-protokollt olyan eszközként kell értelmezni, amely arra szolgál, hogy tájékoztatást nyújtson az információk további terjesztésének korlátairól. Használják szinte valamennyi CSIRT-ben, valamint egyes információelemző és -megosztó központokban.

(46) E rendeletet rendszeresen értékelni kell a többéves pénzügyi keretekről szóló jövőbeli tárgyalások fényében, lehetővé téve a CERT-EU működésével és intézményi szerepével kapcsolatos további döntések meghozatalát, beleértve a CERT-EU uniós hivatalként történő esetleges létrehozását is.

(47) 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. E jelentésnek az IICB közreműködésével értékelnie kell, hogy helyénvaló-e az EU-minősített adatokat kezelő hálózati és információs rendszerek bevonása e rendelet hatálya alá, különösen az uniós szervezetekre vonatkozó közös információbiztonsági szabályok hiányában.

(48) Az arányosság elvével összhangban szükséges és célszerű az uniós szervezeteken belül az egységesen magas szintű kiberbiztonság elérése alapvető céljának megvalósításához az uniós szervezetek kiberbiztonságáról szóló szabályok megállapítása. E rendelet az Európai Unióról szóló szerződés 5. cikkének (4) bekezdésével összhangban nem lépi túl a cél eléréséhez szükséges mértéket.

(49) Ez a rendelet tükrözi azt, hogy az uniós szervezetek mérete és kapacitása eltérő, többek között a pénzügyi és emberi erőforrások tekintetében is.

(50) Az európai adatvédelmi biztossal az (EU) 2018/1725 rendelet 42. cikkének (1) bekezdésével összhangban konzultációra került sor, és a biztos 2022. május 17-én véleményt ([8]) nyilvánított,

ELFOGADTA EZT A RENDELETET:

I. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. cikk

Tárgy

Ez a rendelet olyan intézkedéseket állapít meg, amelyek célja a kiberbiztonság egységesen magas szintjének elérése az uniós szervezeteken belül az alábbiakra való tekintettel:

a) az egyes uniós szervezetek belső kiberbiztonsági kockázatkezelési, -irányítási és -ellenőrzési keretrendszerének létrehozása a 6. cikk szerint;

b) kiberbiztonsági kockázatok kezelése, jelentéstétel és információmegosztás;

c) a 10. cikk alapján létrehozott Intézményközi Kiberbiztonsági Testület szervezete, működése és működtetése, valamint az uniós intézmények, szervek, hivatalok és ügynökségek Kiberbiztonsági Szolgálatának (CERT-EU) szervezete, működése és működtetése;

d) e rendelet végrehajtásának nyomon követése;

([8]) HL C 258., 2022.7.5., 10. o.

2. cikk

Hatály

(1) Ez a rendelet az uniós szervezetekre, a 10. cikk alapján létrehozott Intézményközi Kiberbiztonsági Testületre és a CERT-EU-ra alkalmazandó.

(2) Ez a rendelet a Szerződések szerinti intézményi autonómia sérelme nélkül alkalmazandó.

(3) A 13. cikk (8) bekezdésének kivételével ez a rendelet nem alkalmazandó az EU-minősített adatokat kezelő hálózati és információs rendszerekre.

3. cikk

Fogalommeghatározások

E rendelet alkalmazásában:

1. „uniós szervezetek”: az Európai Unióról szóló szerződés, az Európai Unió működéséről szóló szerződés (EUMSZ) vagy az Európai Atomenergia-közösséget létrehozó szerződés által vagy ezek szerint létrehozott uniós intézmények, szervek, hivatalok és ügynökségek;

2. „hálózati és információs rendszer”: az (EU) 2022/2555 irányelv 6. cikkének 1. pontjában meghatározott hálózati és információs rendszer;

3. „hálózati és információs rendszerek biztonsága”: az (EU) 2022/2555 irányelv 6. cikkének 2. pontjában meghatározott hálózati és információs rendszerek biztonsága;

4. „kiberbiztonság”: az (EU) 2019/881 rendelet 2. cikkének 1. pontjában meghatározott kiberbiztonság;

5. „legmagasabb vezetői szint”: az uniós szervezet működéséért felelős vezető személy, vezető testület vagy koordináló és felügyeleti testület a legmagasabb igazgatási szinten, aki vagy amely az említett uniós szervezet magas szintű irányítására vonatkozó szabályoknak megfelelően felhatalmazással rendelkezik döntések meghozatalára vagy engedélyezésére, az egyéb vezetői szintek saját felelősségi körükbe tartozó megfelelési és kiberbiztonsági kockázatkezelési formális kötelezettségeinek sérelme nélkül;

6. „majdnem bekövetkezett (near miss) esemény”: az (EU) 2022/2555 irányelv 6. cikkének 5. pontjában meghatározott majdnem bekövetkezett (near miss) esemény;

7. „biztonsági esemény”: az (EU) 2022/2555 irányelv 6. cikkének 6. pontjában meghatározott esemény;

8. „súlyos biztonsági esemény”: olyan biztonsági esemény, amely olyan szintű zavart okoz, amely meghaladja az adott uniós szervezet és a CERT-EU reagálási képességeit, vagy amely legalább két uniós szervezetre jelentős hatást gyakorol;

9. „nagyszabású kiberbiztonsági esemény”: az (EU) 2022/2555 irányelv 6. cikkének 7. pontjában meghatározott nagyszabású kiberbiztonsági esemény;

10. „biztonsági esemény kezelése”: az (EU) 2022/2555 irányelv 6. cikkének 8. pontjában meghatározott eseménykezelés;

11. „kiberfenyegetés”: az (EU) 2019/881 rendelet 2. cikkének 8. pontjában meghatározott kiberfenyegetés;

12. „jelentős kiberfenyegetés”: az (EU) 2022/2555 irányelv 6. cikkének 11. pontjában meghatározott jelentős kiberfenyegetés;

13. „sérülékenység”: az (EU) 2022/2555 irányelv 6. cikkének 15. pontjában meghatározott sérülékenység;

14. „kiberbiztonsági kockázat”: az (EU) 2022/2555 irányelv 6. cikkének 9. pontjában meghatározott kockázat;

15. „felhőszolgáltatás”: az (EU) 2022/2555 irányelv 6. cikkének 30. pontjában meghatározott felhőszolgáltatás;

4. cikk

A személyes adatok kezelése

(1) A személyes adatok e rendelet szerinti, a CERT-EU, a 10. cikk alapján létrehozott Intézményközi Kiberbiztonsági Testület és az uniós szervezetek általi kezelését az (EU) 2018/1725 rendelettel összhangban kell végezni.

(2) Amennyiben az e rendelet szerinti feladatokat látnak el vagy kötelezettségeket teljesítenek, a CERT-EU, a 10. cikk alapján létrehozott Intézményközi Kiberbiztonsági Testület és az uniós szervezetek csak az említett feladatok ellátásához vagy kötelezettségek teljesítéséhez szükséges mértékben és kizárólag abból a célból kezelhetnek és cserélhetnek személyes adatokat.

(3) A személyes adatok különleges kategóriáinak az (EU) 2018/1725 rendelet 10. cikkének (1) bekezdésében említett kezelését az említett rendelet 10. cikke (2) bekezdésének g) pontja értelmében jelentős közérdek miatt szükségesnek kell tekinteni. Ezeket az adatokat csak a 6. és a 8. cikkben említett kiberbiztonsági kockázatkezelési intézkedések végrehajtásához, a CERT-EU által a 13. cikk alapján nyújtott szolgáltatásokhoz, a biztonsági eseményekre vonatkozó információknak a 17. cikk (3) bekezdése és a 18. cikk (3) bekezdése szerinti megosztásához, a 20. cikk szerinti információ-megosztáshoz, a 21. cikk szerinti jelentéstételi kötelezettségekhez, a biztonsági eseményekre való reagálás 22. cikk szerinti koordinálásához és az ezzel kapcsolatos együttműködéshez, valamint a súlyos biztonsági események e rendelet 23. cikke szerinti kezeléséhez szükséges mértékben lehet kezelni. Az uniós szervezeteknek és a CERT-EU-nak, amikor adatkezelőként járnak el, technikai intézkedéseket kell alkalmazniuk a személyes adatok különleges kategóriái más célból történő kezelésének megelőzése érdekében, és megfelelő és konkrét intézkedésekről kell rendelkezniük az érintettek alapvető jogainak és érdekeinek védelme érdekében.

II. FEJEZET

A KIBERBIZTONSÁG EGYSÉGESEN MAGAS SZINTJÉRE IRÁNYULÓ INTÉZKEDÉSEK

5. cikk

Az intézkedések végrehajtása

(1) 2024. szeptember 8-ig a 10. cikk alapján létrehozott Intézményközi Kiberbiztonsági Testület az Európai Uniós Kiberbiztonsági Ügynökséggel (ENISA) folytatott konzultációt és a CERT-EU iránymutatásának kézhezvételét követően iránymutatásokat ad ki az uniós szervezeteknek a kezdeti kiberbiztonsági felülvizsgálat elvégzése és a 6. cikk szerinti belső kiberbiztonsági kockázatkezelési, -irányítási és -ellenőrzési keretrendszer létrehozása, a 7. cikk szerinti kiberbiztonsági érettségi értékelések elvégzése, a 8. cikk szerinti kiberbiztonsági kockázatkezelési intézkedések meghozatala, valamint a 9. cikk szerinti kiberbiztonsági terv elfogadása céljából.

(2) A 6–9. cikk végrehajtása során az uniós szervezeteknek figyelembe kell venniük az e cikk (1) bekezdésében említett iránymutatásokat, valamint a 11. és a 14. cikk alapján elfogadott vonatkozó iránymutatásokat és ajánlásokat.

6. cikk

Kiberbiztonsági kockázatkezelési, -irányítási és -ellenőrzési keretrendszer

(1) 2025. április 8-ig minden uniós szervezet a kezdeti kiberbiztonsági felülvizsgálat, például audit elvégzését követően belső kiberbiztonsági kockázatkezelési, -irányítási és -ellenőrzési keretrendszert (a továbbiakban: a keretrendszer) hoz létre. A keretrendszer létrehozását az uniós szervezet legmagasabb vezetői szintje felügyeli és annak felelősségi körébe tartozik.

(2) A keretrendszernek ki kell terjednie az érintett uniós szervezet teljes nem minősített IKT-környezetére, beleértve a helyszíni IKT-környezetet, a helyszíni működő technológiai hálózatot (OT-rendszer), 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 e környezetekhez (a továbbiakban: az IKT-környezet) kapcsolódó eszközöket. A keretrendszernek minden veszélyre kiterjedő megközelítésen kell alapulnia.

(3) A keretrendszernek magas szintű kiberbiztonságot kell biztosítania. A keretrendszer meghatározza a hálózati és információs rendszerek biztonságára vonatkozó belső kiberbiztonsági politikákat, beleértve a célkitűzéseket és prioritásokat, valamint az uniós szervezet e rendelet hatékony végrehajtásának biztosításával megbízott személyzetének szerepét és felelősségi körét. A keretrendszernek tartalmaznia kell a végrehajtás hatékonyságának mérésére szolgáló mechanizmusokat is.

(4) A keretrendszert a változó kiberbiztonsági kockázatok fényében rendszeresen, de legalább négyévente felül kell vizsgálni. Adott esetben és a 10. cikk alapján létrehozott Intézményközi Kiberbiztonsági Testület kérését követően az uniós szervezet keretrendszerét frissíteni lehet a CERT-EU-nak az e rendelet rendelkezéseinek végrehajtása során azonosított biztonsági eseményekre vagy esetleges hiányosságokra vonatkozó iránymutatása alapján.

(5) Az egyes uniós szervezetek legmagasabb vezetői szintje felel e rendelet végrehajtásáért, és felügyeli, hogy szervezete megfeleljen a keretrendszerrel kapcsolatos kötelezettségeknek.

(6) Adott esetben és az e rendelet végrehajtásával kapcsolatos felelősségének sérelme nélkül, az egyes uniós szervezetek legmagasabb vezetői szintje az e rendelet szerinti konkrét kötelezettségeket átruházhatja a személyzeti szabályzat 29. cikkének (2) bekezdése értelmében vett rangidős tisztviselőkre vagy az érintett uniós szervezeten belüli egyéb azonos szintű tisztviselőkre. Az ilyen átruházástól függetlenül a legmagasabb vezetői szint felelősségre vonható e rendeletnek az érintett uniós szervezet általi megsértéséért.

(7) Minden uniós szervezetnek hatékony mechanizmusokkal kell rendelkeznie annak biztosítására, hogy az IKT-költségvetés megfelelő százalékát a kiberbiztonságra fordítsák. Az említett százalékos arány meghatározásakor kellően figyelembe kell venni a keretrendszert.

(8) Minden uniós szervezet helyi kiberbiztonsági tisztviselőt vagy azzal egyenértékű funkciót nevez ki, aki a kiberbiztonság valamennyi vonatkozása tekintetében egyedüli kapcsolattartó pontjaként jár el. A helyi kiberbiztonsági tisztviselő elősegíti e rendelet végrehajtását, és rendszeresen beszámol közvetlenül a legmagasabb vezetői szintnek a végrehajtás állásáról. Annak sérelme nélkül, hogy a helyi kiberbiztonsági tisztviselő az egyes uniós szervezeteken belül az egyedüli kapcsolattartó pont, az uniós szervezetek a köztük és a CERT-EU között létrejött, szolgáltatási szintre vonatkozó megállapodás alapján átruházhatják a CERT-EU-ra a helyi kiberbiztonsági tisztviselő e rendelet végrehajtásával kapcsolatos bizonyos feladatait, vagy ezeket a feladatokat több uniós szervezet megoszthatja. Amennyiben ezeket a feladatokat a CERT-EU-ra ruházzák, a 10. cikk alapján létrehozott Intézményközi Kiberbiztonsági Testületnek kell döntenie arról, hogy e szolgáltatás nyújtása részét képezi-e a CERT-EU alapszolgáltatásainak, figyelembe véve az érintett uniós szervezet emberi és pénzügyi erőforrásait. Az egyes uniós szervezeteknek indokolatlan késedelem nélkül értesíteniük kell a CERT-EU-t a kinevezett helyi kiberbiztonsági tisztviselőkről és a személyükben történő minden későbbi változásról.

A CERT-EU-nak létre kell hoznia és naprakészen kell tartania a kinevezett helyi kiberbiztonsági tisztviselők jegyzékét.

(9) Az egyes uniós szervezeteknek a személyzeti szabályzat 29. cikkének (2) bekezdése értelmében vett rangidős tisztviselői vagy egyéb azonos szintű tisztviselői, valamint a személyzetnek az e rendeletben meghatározott kiberbiztonsági kockázatkezelési intézkedések végrehajtásával és kötelezettségek betartásával megbízott tagjai rendszeresen külön képzéseken vesznek részt azon ismeretek és készségek elsajátítása érdekében, amelyek a kiberbiztonsági kockázatok és irányítási gyakorlatok, valamint az azok által az uniós szervezet működésére gyakorolt hatások megismeréséhez és értékeléséhez szükségesek.

7. cikk

Kiberbiztonsági érettségi értékelések

(1) 2025. július 8-ig és azt követően legalább kétévente minden uniós szervezet kiberbiztonsági érettségi értékelést végez, amelynek ki kell terjednie IKT-környezetének valamennyi elemére.

(2) A kiberbiztonsági érettségi értékeléseket adott esetben szakosodott harmadik fél segítségével kell elvégezni.

(3) A hasonló struktúrákkal rendelkező uniós szervezetek együttműködhetnek saját szervezeteik kiberbiztonsági érettségi értékelésének elvégzésében.

(4) A 10. cikk alapján létrehozott Intézményközi Kiberbiztonsági Testület kérésére és az érintett uniós szervezet kifejezett beleegyezésével a kiberbiztonsági érettségi értékelés eredményei megvitathatók az említett Testületen belül vagy a helyi kiberbiztonsági tisztviselők nem hivatalos csoportjában a tapasztalatokból való tanulás, valamint a bevált gyakorlatok megosztása céljából.

8. cikk

Kiberbiztonsági kockázatkezelési intézkedések

(1) Indokolatlan késedelem nélkül, de legkésőbb 2025. szeptember 8-ig az egyes uniós szervezeteknek – a legmagasabb vezetői szintjük felügyelete mellett – meg kell hozniuk a keretrendszer keretében azonosított kiberbiztonsági kockázatok kezeléséhez, valamint a biztonsági események megelőzéséhez vagy hatásuk minimálisra csökkentéséhez szükséges megfelelő és arányos technikai, működési és szervezeti intézkedéseket. Figyelembe véve a legkorszerűbb és adott esetben a vonatkozó európai és nemzetközi szabványokat, ezeknek az intézkedéseknek biztosítaniuk kell a hálózati és információs rendszerek biztonságának a felmerülő kiberbiztonsági kockázatokkal arányos szintjét az IKT-környezet egészében. Az említett intézkedések arányosságának értékelésekor kellően figyelembe kell venni az uniós szervezet kiberbiztonsági kockázatoknak való kitettségének mértékét, a szervezet méretét, a biztonsági események bekövetkeztének valószínűségét és azok súlyosságát, beleértve társadalmi, gazdasági és intézményközi hatásukat is.

(2) Az uniós szervezeteknek a kiberbiztonsági kockázatkezelési intézkedések végrehajtása során legalább a következő területekkel foglalkozniuk kell:

a) kiberbiztonsági szakpolitika, beleértve a 6. cikkben és az e cikk (3) bekezdésében említett célok és prioritások eléréséhez szükséges intézkedéseket;

b) kiberbiztonsági kockázatelemzési és az informatikai rendszerek biztonságára vonatkozó szakpolitikák;

c) a felhőszolgáltatások használatára vonatkozó szakpolitikai célok;

d) adott esetben kiberbiztonsági audit, amely magában foglalhatja a kiberbiztonsági kockázat, a sérülékenység és a kiberfenyegetések értékelését, valamint egy megbízható magánszolgáltató által rendszeresen végzett behatolási tesztelést;

e) a d) pontban említett kiberbiztonsági auditokból eredő ajánlások végrehajtása kiberbiztonsági frissítések és a szakpolitikák frissítése révén;

f) a kiberbiztonság megszervezése, beleértve a szerepek és feladatkörök meghatározását is;

g) eszközkezelés, beleértve az IKT-eszközök leltárát és az IKT-hálózatok feltérképezését;

h) az emberi erőforrások biztonsága és a hozzáférés ellenőrzése;

i) üzembiztonság;

j) kommunikációs biztonság;

k) a rendszerek beszerzése, fejlesztése és karbantartása, beleértve a sérülékenységkezelésre és -feltárásra vonatkozó politikákat;

l) ahol lehetséges, a forráskód átláthatóságára vonatkozó politikák;

m) az ellátási lánc biztonsága, beleértve az egyes uniós szervezetek és közvetlen beszállítóik vagy szolgáltatóik közötti kapcsolatok biztonsági vonatkozásait is;

n) biztonsági események kezelése és együttműködés a CERT-EU-val, például a biztonsági nyomonkövetés és a naplózás fenntartása;

o) az üzletmenet-folytonosság kezelése, például tartalékrendszerek kezelése, valamint katasztrófa utáni helyreállítás és válságkezelés; valamint

p) a kiberbiztonsággal kapcsolatos oktatási, készségfejlesztő, tudatosságnövelő, gyakorlati és képzési programok előmozdítása és kidolgozása.

Az első albekezdés m) pontjának alkalmazásában az uniós szervezeteknek figyelembe kell venniük az egyes közvetlen beszállítókra és szolgáltatókra jellemző sérülékenységeket, valamint a beszállítóik és szolgáltatóik termékeinek és kiberbiztonsági gyakorlatainak – többek között biztonságos fejlesztési eljárásaiknak – az általános minőségét.

(3) Az uniós szervezeteknek meg kell hozniuk legalább a következő konkrét kiberbiztonsági kockázatkezelési intézkedéseket:

a) a távmunka lehetővé tételét és fenntartását szolgáló műszaki intézkedések;

b) konkrét lépések a zéró bizalom alapelvei felé történő elmozdulás érdekében;

c) a többtényezős hitelesítés mint norma használata a hálózati és információs rendszerekben;

d) kriptográfia és titkosítás, különösen végponttól végpontig terjedő titkosítás, valamint biztonságos digitális aláírás használata;

e) adott esetben biztonságos hang-, video- és szöveges kommunikáció, valamint biztonságos vészhelyzeti kommunikációs rendszerek használata az uniós szervezeten belül;

f) a rosszindulatú szoftverek és kémszoftverek felderítésére és eltávolítására irányuló proaktív intézkedések;

g) a szoftverellátási lánc biztonságának megteremtése a biztonságos szoftverfejlesztésre és -értékelésre vonatkozó kritériumok révén;

h) az uniós szervezet legmagasabb vezetői szintje és az e rendelet hatékony végrehajtásának biztosításával megbízott személyzete tagjai számára a számukra előírt feladatoknak és a tőlük elvárt képességeknek megfelelő kiberbiztonsági képzési tantervek kidolgozása és elfogadása;

i) a személyzet tagjainak rendszeres kiberbiztonsági képzése;

j) adott esetben részvétel az uniós szervezetek összekapcsoltságával összefüggő kockázatok elemzésében;

k) a közbeszerzési szabályok javítása a kiberbiztonság egységesen magas szintjének elősegítése érdekében a következők révén:

   i. az informatikai szolgáltatók biztonsági eseményekkel, sérülékenységekkel és kiberfenyegetésekkel kapcsolatos információinak a CERT-EU-val való megosztását korlátozó szerződéses akadályok felszámolása;

   ii. a biztonsági események, sérülékenységek és kiberfenyegetések bejelentésére, valamint a biztonsági eseményekre való reagálási és nyomon követési mechanizmusok bevezetésére vonatkozó szerződéses kötelezettségek.

9. cikk

Kiberbiztonsági tervek

(1) A 7. cikk szerint elvégzett kiberbiztonsági érettségi értékelésből levont következtetések nyomán, valamint figyelembe véve a keretrendszerben azonosított eszközöket és kiberbiztonsági kockázatokat, továbbá a 8. cikk alapján hozott kiberbiztonsági kockázatkezelési intézkedéseket, az egyes uniós szervezetek legfelsőbb vezetői szintjének indokolatlan késedelem nélkül, de legkésőbb 2026. január 8-ig jóvá kell hagynia a kiberbiztonsági tervet. A kiberbiztonsági tervnek az uniós szervezet általános kiberbiztonságának növelésére kell irányulnia, és ezáltal hozzá kell járulnia az uniós szervezeteken belüli egységesen magas szintű kiberbiztonság javításához. A kiberbiztonsági tervnek tartalmaznia kell legalább a 8. cikk alapján hozott kiberbiztonsági kockázatkezelési intézkedéseket. A kiberbiztonsági tervet kétévente, vagy szükség esetén gyakrabban, a 7. cikk szerint elvégzett kiberbiztonsági érettségi értékeléseket vagy a keretrendszer bármely jelentős felülvizsgálatát követően felül kell vizsgálni.

(2) A kiberbiztonsági tervnek tartalmaznia kell az uniós szervezetnek a súlyos biztonsági eseményekre vonatkozó kiberbiztonsági válságkezelési tervét.

(3) Az uniós szervezet benyújtja elkészített kiberbiztonsági tervét a 10. cikk alapján létrehozott Intézményközi Kiberbiztonsági Testületnek.

III. FEJEZET

INTÉZMÉNYKÖZI KIBERBIZTONSÁGI TESTÜLET

10. cikk

Intézményközi Kiberbiztonsági Testület

(1) Létrejön az Intézményközi Kiberbiztonsági Testület (a továbbiakban: az IICB).

(2) Az IICB felelős az alábbiakért:

a) e rendelet uniós szervezetek általi végrehajtásának nyomon követése és támogatása;

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:

a) az alábbiak mindegyike által kinevezett egy-egy képviselő:

i. az Európai Parlament;

ii. az Európai Tanács;

iii. az Európai Unió Tanácsa;

iv. a Bizottság;

v. az Európai Unió Bírósága;

vi. az Európai Központi Bank;

vii. a Számvevőszék;

viii. az Európai Külügyi Szolgálat;

ix. az Európai Gazdasági és Szociális Bizottság;

x. a Régiók Európai Bizottsága;

xi. az Európai Beruházási Bank;

xii. az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont;

xiii. az ENISA;

xiv. az európai adatvédelmi biztos;

xv. az Európai Unió Űrprogramügynöksége;

b) három képviselő, akiket az uniós ügynökségek hálózata (a továbbiakban: az EUAN) jelöl ki IKT-tanácsadó bizottságának javaslata alapján az a) pontban említettektől eltérő, saját IKT-környezetüket működtető uniós szervek, hivatalok és ügynökségek érdekeinek képviseletére.

Az IICB-ben képviselt uniós szervezetek törekednek arra, hogy a kijelölt képviselők körében megvalósuljon a nemek közötti egyensúly.

(4) Az IICB tagjainak munkáját póttag segítheti. Az elnök meghívhatja a (3) bekezdésben említett uniós szervezetek vagy más uniós szervezetek egyéb képviselőit, hogy szavazati jog nélkül részt vegyenek az IICB ülésein.

(5) A CERT-EU vezetője, valamint az (EU) 2022/2555 irányelv 14., 15. és 16. cikke alapján létrehozott együttműködési csoport, a CSIRT-ek hálózata és az EU-CyCLONe elnökei vagy az őket helyettesítő póttagok megfigyelőként részt vehetnek az IICB ülésein. Kivételes esetekben és az IICB – belső eljárási szabályzatával összhangban – másként határozhat.

(6) Az IICB elfogadja saját belső eljárási szabályzatát.

(7) Az IICB – belső eljárási szabályzatával összhangban – a tagjai közül hároméves időtartamra elnököt jelöl ki. Az elnököt helyettesítő póttag ugyanezen időtartamra az IICB teljes jogú tagjává válik.

(8) Az IICB az elnök kezdeményezésére, illetve a CERT-EU-nak vagy bármely tagjának kérésére évente legalább háromszor ülésezik.

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

(10) Az IICB a 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.

(11) Az IICB titkárságát a Bizottság biztosítja, és az az IICB elnökének tartozik felelősséggel.

(12) Az EUAN által kijelölt képviselők továbbítják az IICB határozatait az EUAN tagjainak. Az EUAN bármely tagja jogosult az említett képviselők vagy az IICB elnöke elé terjeszteni minden olyan ügyet, amelyet megítélése szerint az IICB tudomására kell hozni.

(13) Az IICB létrehozhat egy végrehajtó bizottságot, amely segíti 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.

(14) Az IICB 2025. január 8-ig, majd azt követően évente jelentést nyújt be az Európai Parlamentnek és a Tanácsnak, amelyben részletezi az e rendelet végrehajtása terén elért eredményeket, és különösen a CERT-EU és az egyes tagállamokban található tagállami partnerei közötti együttműködés mértékét. A jelentés hozzájárul az uniós kiberbiztonsági helyzetről az (EU) 2022/2555 irányelv 18. cikke alapján elfogadott, kétévente kiadandó jelentéshez.

11. cikk

Az IICB feladatai

Feladatainak ellátása során az IICB különösen:

a) iránymutatást nyújt a CERT-EU vezetője számára;

b) hatékonyan nyomon követi és felügyeli e rendelet végrehajtását, valamint támogatja az uniós szervezeteket kiberbiztonságuk megerősítésében, beleértve adott esetben eseti jelentések kérését az uniós szervezetektől és a CERT-EU-tól;

c) stratégiai megbeszélést követően többéves stratégiát fogad el az uniós szervezetek kiberbiztonsági szintjének növelésére, és azt rendszeresen, de legalább ötévente értékeli és szükség esetén módosítja;

d) meghatározza az uniós szervezetek által végzett önkéntes szakértői értékelések módszertanát és szervezeti vonatkozásait a közös tapasztalatokból való tanulás, a kölcsönös bizalom megerősítése, az egységesen magas szintű kiberbiztonság elérése, valamint az uniós szervezetek kiberbiztonsági képességeinek javítása érdekében, biztosítva, hogy az ilyen szakértői értékeléseket a felülvizsgálat tárgyát képező uniós szervezettől eltérő uniós szervezet által kijelölt kiberbiztonsági szakértők végezzék, és hogy a módszertan az (EU) 2022/2555 irányelv 19. cikkén alapuljon, és adott esetben igazodjon az uniós szervezetekhez;

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

f) a CERT-EU vezetőjének javaslata alapján jóváhagyja a CERT-EU szolgáltatási katalógusát és annak frissítéseit;

g) a CERT-EU vezetőjének javaslata alapján jóváhagyja a CERT-EU tevékenységeinek bevételeire és kiadásaira vonatkozó éves pénzügyi tervet, beleértve a személyzetre vonatkozót is;

h) a CERT-EU vezetőjének javaslata alapján jóváhagyja a szolgáltatási szintre vonatkozó megállapodásokra vonatkozó szabályokat;

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

j) jóváhagyja és nyomon követi a CERT-EU vezetőjének javaslata alapján a CERT-EU-ra vonatkozóan meghatározott fő teljesítménymutatókat (KPI-k);

k) jóváhagyja a CERT-EU és más szervezetek közötti, a 18. cikk szerinti együttműködési megállapodásokat, szolgáltatási szintre vonatkozó megállapodásokat vagy szerződéseket;

l) a CERT-EU javaslata alapján a 14. cikkel összhangban iránymutatásokat és ajánlásokat fogad el, és utasítja a CERT-EU-t, hogy adjon ki, vonjon vissza vagy módosítson valamely, iránymutatásokra vagy ajánlásokra irányuló javaslatot, illetve cselekvési felhívást;

m) az IICB munkájának támogatásához technikai tanácsadó csoportokat hoz létre konkrét feladatokkal, jóváhagyja azok megbízatását, és kinevezi azok elnökeit;

n) fogadja és értékeli az uniós szervezetek által e rendelet alapján benyújtott dokumentumokat és jelentéseket, például a kiberbiztonsági érettségi értékeléseket;

o) az e rendelet végrehajtásával kapcsolatos bevált gyakorlatok és információk cseréje céljából az ENISA támogatásával elősegíti az uniós szervezetek helyi kiberbiztonsági tisztviselőiből álló informális csoport létrehozását;

p) figyelembe véve a CERT-EU által az azonosított kiberbiztonsági kockázatokra és levont tanulságokra vonatkozóan szolgáltatott információkat, nyomon követi az uniós szervezetek IKT-környezete közötti összekapcsolhatósági megállapodások megfelelőségét, és tanácsot ad a lehetséges fejlesztésekre vonatkozóan;

q) kiberbiztonsági válságkezelési tervet hoz létre az uniós szervezeteket érintő súlyos biztonsági események koordinált kezelésének operatív szintű támogatása, valamint a releváns információk rendszeres cseréjéhez való hozzájárulás céljából, különös tekintettel a súlyos biztonsági események hatásaira és súlyosságára, valamint hatásai mérséklésének lehetséges módjaira;

r) koordinálja az egyes uniós szervezetek 9. cikk (2) bekezdésében említett kiberbiztonsági válságkezelési terveinek elfogadását;

s) az (EU) 2022/2555 irányelv 22. cikkében említett, a kritikus ellátási láncokra vonatkozó összehangolt uniós szintű biztonsági kockázatértékelések eredményeit figyelembe véve a 8. cikk (2) bekezdése első albekezdésének m) pontjában említett, az ellátási lánc biztonságára vonatkozó ajánlásokat fogad el annak érdekében, hogy támogassa az uniós szervezeteket a hatékony és arányos kiberbiztonsági kockázatkezelési intézkedések elfogadásában.

12. cikk

Megfelelés

(1) Az IICB a 10. cikk (2) bekezdése és a 11. cikk alapján hatékonyan nyomon követi e rendelet, valamint az elfogadott iránymutatások, ajánlások és cselekvési felhívások uniós szervezetek általi végrehajtását. Az IICB az e célból szükséges információkat vagy dokumentumokat kérhet az uniós szervezetektől. Az e cikk szerinti megfelelési intézkedések elfogadása céljából, ha az érintett uniós szervezet közvetlenül képviselteti magát az IICB-ben, az említett uniós szervezet nem rendelkezik szavazati joggal.

(2) Amennyiben az IICB megállapítja, hogy egy uniós szervezet nem alkalmazta hatékonyan ezt a rendeletet vagy az annak alapján kiadott iránymutatásokat, ajánlásokat vagy cselekvési felhívásokat, az érintett uniós szervezet belső eljárásainak sérelme nélkül, és miután lehetőséget biztosított az érintett uniós szervezet számára észrevételei megtételére:

a) indokolással ellátott véleményt küldhet az e rendelet végrehajtásában észlelt hiányosságok által érintett uniós szervezetnek;

b) a CERT-EU-val folytatott konzultációt követően iránymutatásokat nyújthat az érintett uniós szervezet számára annak biztosítása érdekében, hogy annak keretrendszere, kiberbiztonsági kockázatkezelési intézkedései, kiberbiztonsági terve és jelentéstétele meghatározott időn belül megfeleljen e rendeletnek;

c) figyelmeztetést adhat ki a feltárt hiányosságok meghatározott határidőn belüli kezelésére, így többek között ajánlásokat adhat ki az érintett uniós szervezet által e rendelet alapján elfogadott intézkedések módosítására vonatkozóan;

d) indokolással ellátott értesítést adhat ki az érintett uniós szervezetnek abban az esetben, ha a c) pont szerint kiadott figyelmeztetésben feltárt hiányosságokat a meghatározott határidőn belül nem orvosolják megfelelően;

e) kiadhatja az alábbiakat:

i. audit elvégzésére vonatkozó ajánlást; vagy

ii. arra irányuló kérelmet, hogy az auditot harmadik fél ellenőrzési szolgálata végezze el;

f) adott esetben a hatáskörén belül tájékoztathatja a Számvevőszéket a feltételezett meg nem felelésről;

g) ajánlást adhat ki arra vonatkozóan, hogy valamennyi tagállam és uniós szervezet ideiglenesen függessze fel az adott uniós szervezet felé irányuló adatáramlást.

Az első albekezdés c) pontjának alkalmazásában a figyelmeztetés célközönségét megfelelően korlátozni kell, amennyiben ez a kiberbiztonsági kockázat miatt szükséges.

Az első albekezdés alapján kiadott valamennyi figyelmeztetést és ajánlást az érintett uniós szervezet legmagasabb vezetői szintjének kell címezni.

(3) Amennyiben az IICB a (2) bekezdés első albekezdésének a)–g) pontja szerinti intézkedéseket fogadott el, az érintett uniós szervezetnek részletesen be kell számolnia az IICB által feltárt állítólagos hiányosságok kezelése érdekében hozott intézkedésekről és lépésekről. Az uniós szervezetnek ezeket az információkat az IICB-vel egyeztetett észszerű határidőn belül kell benyújtania.

(4) Amennyiben az IICB úgy ítéli meg, hogy egy uniós szervezet közvetlenül az Unió valamely tisztviselőjének vagy egyéb alkalmazottjának – beleértve a legmagasabb vezetői szintet is – intézkedéseiből vagy mulasztásaiból eredően tartósan megsérti e rendeletet, az IICB felkéri az érintett uniós szervezetet a megfelelő intézkedések megtételére, többek között arra, hogy a személyzeti szabályzatban megállapított szabályokkal és eljárásokkal, valamint az egyéb alkalmazandó szabályokkal és eljárásokkal összhangban fontolja meg fegyelmi intézkedés meghozatalát. E célból az IICB átadja a szükséges információkat az érintett uniós szervezetnek.

(5) Amennyiben az uniós szervezetek bejelentik, hogy nem tudják betartani a 6. cikk (1) bekezdésében és a 8. cikk (1) bekezdésében meghatározott határidőket, az IICB kellően indokolt esetekben, figyelembe véve az uniós szervezet méretét, engedélyezheti e határidők meghosszabbítását.

IV. FEJEZET

CERT-EU

13. cikk

A CERT-EU küldetése és feladatai

(1) A CERT-EU küldetése, hogy hozzájáruljon az uniós szervezetek nem minősített IKT-környezetének biztonságához azáltal, hogy kiberbiztonsági tanácsadást nyújt számukra, segíti a biztonsági események megelőzését, észlelését, kezelését, mérséklését, az azokra való reagálást és az azokat követő helyreállítást, valamint azáltal, hogy a kiberbiztonsági információcsere és a biztonsági eseményekre való reagálás koordinációs központjaként működik.

(2) A CERT-EU információkat gyűjt a nem minősített IKT-infrastruktúrát érintő kiberfenyegetésekről, sérülékenységekről és biztonsági eseményekről, ezeket az információkat kezeli és elemzi, valamint megosztja az uniós szervezetekkel. Intézményközi szinten és az uniós szervezetek szintjén koordinálja a biztonsági eseményekre való reagálást, ideértve konkrét operatív segítségnyújtás biztosítását vagy koordinálását is.

(3) A CERT-EU a következő feladatokat látja el az uniós szervezetek támogatása érdekében:

a) támogatja őket e rendelet végrehajtásában, és a 14. cikk (1) bekezdésében felsorolt intézkedések vagy az IICB által kért eseti jelentések révén hozzájárul e rendelet végrehajtásának koordinálásához;

b) az uniós szervezetek számára szabványos CSIRT-szolgáltatásokat kínál a szolgáltatási katalógusában ismertetett kiberbiztonsági szolgáltatáscsomag eszközei által (a továbbiakban: alapszolgáltatások);

c) hálózatot tart fenn a hasonló szervezetekkel és partnerekkel a 17. és 18. cikkben vázolt szolgáltatások támogatása érdekében;

d) felhívja az IICB figyelmét az e rendelet végrehajtásával, valamint az iránymutatások, ajánlások és cselekvési felhívások végrehajtásával kapcsolatos bármely problémára;

e) a (2) bekezdésben említett információk alapján az ENISA-val szorosan együttműködve hozzájárul az Unió kiberbiztonsági helyzetismeretéhez;

f) koordinálja a súlyos biztonsági események kezelését;

g) az (EU) 2022/2555 irányelv 12. cikkének (1) bekezdése szerint a sérülékenységek összehangolt közzététele céljából kijelölt koordinátorral egyenértékűként eljár az uniós szervezetek részéről;

h) valamely uniós szervezet kérésére proaktív, behatolásmentes átvilágítást végez az adott uniós szervezet nyilvánosan hozzáférhető hálózati és információs rendszerein.

Az első albekezdés e) pontjában említett információkat adott esetben, megfelelő titoktartási feltételek mellett kell megosztani az IICB-vel, a CSIRT-ek hálózatával és az Európai Unió Helyzetelemző Központjával (EU INTCEN).

(4) A CERT-EU a 17. vagy adott esetben a 18. cikkel összhangban együttműködhet az Unión és tagállamain belüli releváns kiberbiztonsági közösségekkel, többek között a következő területeken:

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

b) operatív együttműködés a CSIRT-ek hálózatával, többek között a kölcsönös segítségnyújtással kapcsolatban;

c) kiberfenyegetettségi információk, beleértve a helyzetismeretet;

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

(5) Hatáskörén belül a CERT-EU az (EU) 2019/881 rendelettel összhangban strukturált együttműködést folytat az ENISA-val a kapacitásépítés, az operatív együttműködés és a kiberfenyegetések hosszú távú stratégiai elemzése terén. A CERT-EU együttműködhet és információt cserélhet az Europol Kiberbűnözés Elleni Európai Központjával.

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

a) a (3) bekezdésben említettektől eltérő, az uniós szervezetek IKT-környezetének kiberbiztonságát támogató szolgáltatások, a szolgáltatási szintre vonatkozó megállapodások alapján és a rendelkezésre álló erőforrások függvényében, különösen a hálózatok széles spektrumú nyomon követése, beleértve a súlyos kiberfenyegetések a hét minden napján, napi 24 órában történő közvetlen nyomon követését is;

b) olyan szolgáltatások, amelyek írásbeli megállapodások alapján és az IICB előzetes jóváhagyásával támogatják az uniós szervezetek kiberbiztonsági műveleteit vagy projektjeit, kivéve azokat, amelyek IKT-környezetük védelmét szolgálják;

c) kérésre az érintett uniós szervezet hálózati és információs rendszereinek proaktív átvilágítása a potenciálisan jelentős hatással bíró sérülékenységek felderítése érdekében;

d) írásbeli megállapodások alapján és az IICB előzetes jóváhagyásával az uniós szervezetektől eltérő olyan szervezetek számára nyújtott, IKT-környezetük biztonságát támogató szolgáltatások, amelyek szorosan együttműködnek az uniós szervezetekkel, például az uniós jog által rájuk ruházott feladatok vagy felelősségi körök teljesítése révén.

Az első albekezdés d) pontja tekintetében a CERT-EU kivételes esetben, az IICB előzetes jóváhagyásával az uniós szervezeteken kívüli egyéb szervezetekkel is köthet szolgáltatási szintre vonatkozó megállapodásokat.

(7) A CERT-EU – adott esetben az ENISA-val szoros együttműködésben – kiberbiztonsági gyakorlatokat szervez, és részt vehet azokban, vagy ajánlhatja a meglévő gyakorlatokban való részvételt az uniós szervezetek kiberbiztonsági szintjének tesztelése céljából.

(8) A CERT-EU segítséget nyújthat az uniós szervezeteknek az EU-minősített adatokat kezelő hálózati és információs rendszerekben előforduló biztonsági események tekintetében, amennyiben az érintett uniós szervezetek erre saját eljárásaikkal összhangban kifejezetten felkérik. A CERT-EU által e bekezdés alapján nyújtott segítség nem érinti a minősített adatok védelmére vonatkozó alkalmazandó szabályokat.

(9) A CERT-EU tájékoztatja az uniós szervezeteket a biztonsági események kezelésére szolgáló eljárásairól és folyamatairól.

(10) A CERT-EU a megfelelő együttműködési mechanizmusokon és jelentési útvonalakon keresztül magas szintű titoktartás és megbízhatóság mellett szolgáltat releváns és anonimizált információkat a súlyos biztonsági eseményekről és azok kezelésének módjáról. Ezeket az információkat bele kell foglalni a 10. cikk (14) bekezdésében említett jelentésbe.

(11) A CERT-EU az európai adatvédelmi biztossal együttműködve támogatja az érintett uniós szervezeteket a személyes adatok megsértéséhez vezető biztonsági események kezelésében, az európai adatvédelmi biztosnak az (EU) 2018/1725 rendelet szerinti felügyeleti hatóságként fennálló hatáskörének és feladatainak sérelme nélkül.

(12) Ha az uniós szervezetek szakpolitikai részlegei azt kifejezetten kérik, a CERT-EU technikai tanácsot adhat vagy technikai véleményt nyilváníthat releváns szakpolitikai kérdésekben.

14. cikk

Iránymutatások, 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 szervezeteknek meghatározott időn belül meg kell hozniuk;

b) javaslatok az IICB számára az uniós szervezetek összességének vagy egy részhalmazának szóló iránymutatásokra vonatkozóan;

c) javaslatok az IICB számára az egyes uniós szervezeteknek címzett ajánlásokra vonatkozóan.

Az első albekezdés a) pontja tekintetében az érintett uniós szervezet a cselekvési felhívás kézhezvételét követően indokolatlan késedelem nélkül tájékoztatja a CERT-EU-t arról, hogy hogyan alkalmazta a sürgős biztonsági intézkedéseket.

(2) Az iránymutatások és ajánlások a következőket foglalhatják magukban:

a) az uniós szervezetek kiberbiztonsági érettségének értékelésére szolgáló közös módszertanok és modell, beleértve a megfelelő léptékeket vagy fő teljesítménymutatókat is, amelyek referenciaként szolgálnak az uniós szervezetek folyamatos kiberbiztonsági fejlődésének támogatásához, és megkönnyítik a kiberbiztonsági területek és intézkedések rangsorolását, figyelembe véve a szervezetek kiberbiztonsági helyzetét;

b) a kiberbiztonsági kockázatkezelésre és a kiberbiztonsági kockázatkezelési intézkedésekre vonatkozó szabályok vagy javítások;

c) a kiberbiztonsági érettségi értékelésekre és kiberbiztonsági tervekre vonatkozó szabályok;

d) adott esetben a közös technológia, az architektúra, a nyílt forráskód és a kapcsolódó legjobb gyakorlatok alkalmazása az interoperabilitás és az egységes szabványok megvalósítása céljából, beleértve az ellátási lánc biztonságára vonatkozó koordinált megközelítést;

e) adott esetben olyan információk, amelyek megkönnyítik a releváns kiberbiztonsági szolgáltatások és termékek harmadik fél beszállítóktól történő beszerzésére szolgáló közös közbeszerzési eszközök használatát;

f) a 20. cikk szerinti információmegosztási megállapodások.

15. cikk

A CERT-EU vezetője

(1) A Bizottság az IICB tagjai kétharmados többségének jóváhagyását követően kinevezi a CERT-EU vezetőjét. A kinevezési eljárás minden szakaszában konzultálni kell az IICB-vel, különösen az állással kapcsolatos álláshirdetések megszövegezése, a pályázatok vizsgálata és a felvételi bizottságok kinevezése során. A kiválasztási eljárásnak – beleértve azon előválogatott jelöltek végleges listáját is, akik közül a CERT-EU vezetőjét ki kell nevezni – biztosítania kell az egyes nemek méltányos képviseletét, figyelembe véve a benyújtott pályázatokat.

(2) A CERT-EU vezetője – hatáskörén belül, az IICB irányítása alapján eljárva – felelős a CERT-EU megfelelő működéséért. A CERT-EU vezetője rendszeresen jelentést tesz a IICB elnökének és kérésre ad hoc jelentéseket nyújt be az IICB-nek.

(3) A CERT-EU vezetőjének segítenie kell a megbízott, engedélyezésre jogosult felelős tisztviselőt abban, hogy az (EU, Euratom) 2018/1046 európai parlamenti és tanácsi rendelet ([9]) 74. cikke (9) bekezdésének megfelelően elkészítse a kontrollok eredményeit is magukban foglaló pénzügyi és igazgatási információkat tartalmazó éves tevékenységi jelentést, és rendszeresen be kell számolnia a megbízott, engedélyezésre jogosult tisztviselő számára azon intézkedések végrehajtásáról, amelyekre vonatkozóan hatásköröket ruháztak tovább a CERT-EU vezetőjére.

(4) A CERT-EU vezetője évente elkészíti a tevékenységeihez kapcsolódó igazgatási bevételek és kiadások pénzügyi tervezését, a javasolt éves munkaprogramot, a CERT-EU számára javasolt szolgáltatási katalógust, a szolgáltatási katalógus javasolt felülvizsgálatát, a szolgáltatási szintre vonatkozó megállapodások szabályaira vonatkozó javaslatot és a CERT-EU fő teljesítménymutatóira vonatkozó javaslatát, amelyeket a IICB a 11. cikkel összhangban hagy jóvá. A CERT-EU szolgáltatási katalógusában szereplő szolgáltatások jegyzékének felülvizsgálatakor a CERT-EU vezetőjének figyelembe kell vennie a CERT-EU számára allokált erőforrásokat.

(5) A CERT-EU vezetője legalább évente jelentést nyújt be az IICB-nek és az IICB elnökének a CERT-EU referencia-időszak alatti tevékenységeiről és teljesítményéről, többek között 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 11. cikkben említett jelentéseket is. E jelentések tartalmazzák a következő időszakra vonatkozó munkaprogramot, a bevételek és kiadások pénzügyi tervezését, beleértve a személyi állományt, a CERT-EU szolgáltatási katalógusának tervezett frissítéseit, valamint annak értékelését, hogy ezek a frissítések milyen várható hatást gyakorolhatnak a pénzügyi és emberi erőforrásokra.

16. cikk

Pénzügyi és személyzeti kérdések

(1) A CERT-EU-t integrálni kell a Bizottság valamely főigazgatóságának igazgatási struktúrájába annak érdekében, hogy igénybe vehesse a Bizottság igazgatási, pénzgazdálkodási és számviteli támogatási struktúráit, megőrizve ugyanakkor önálló intézményközi szolgáltatói státuszát valamennyi uniós szervezet számára. A Bizottság tájékoztatja az IICB-t a CERT-EU adminisztratív helyszínéről és annak bármely változásáról. A Bizottság a megfelelő intézkedések meghozatala érdekében rendszeresen, de minden esetben az EUMSZ 312. cikke szerinti többéves pénzügyi keret létrehozása előtt felülvizsgálja a CERT-EU-val kapcsolatos igazgatási megállapodásokat. A felülvizsgálatnak ki kell terjednie a CERT-EU uniós hivatalként történő létrehozásának lehetőségére is.

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

([9]) 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.).

(3) A CERT-EU feladatait és tevékenységeit, beleértve a CERT-EU által a 13. cikk (3), (4), (5) és (7) bekezdése, valamint a 14. cikk (1) bekezdése alapján az uniós szervezeteknek 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) Az e cikk (3) bekezdésében említettektől eltérő uniós szervezetek éves pénzügyi hozzájárulást nyújtanak a CERT-EU-nak a CERT-EU által az említett bekezdés értelmében nyújtott szolgáltatások fedezésére. A hozzájárulások az IICB által adott iránymutatásokon alapulnak, amelyekről az egyes uniós 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 rendelet 21. cikke (3) bekezdésének c) pontja szerinti belső címzett bevételként az e cikk (3) bekezdésében említett külön költségvetési sorba kell beszedni.

(5) A 13. cikk (6) bekezdésében meghatározott szolgáltatások költségeit a CERT-EU szolgáltatásait igénybe vevő uniós szervezetektől kell beszedni. A bevételeket a költségeket támogató költségvetési sorokhoz kell rendelni.

17. cikk

A CERT-EU és a tagállami partnerek közötti együttműködés

(1) A CERT-EU indokolatlan késedelem nélkül együttműködik és információcserét folytat a tagállami partnerekkel, különösen az (EU) 2022/2555 irányelv 10. cikke alapján kijelölt vagy létrehozott CSIRT-ekkel, vagy adott esetben az említett irányelv 8. cikke szerint kijelölt vagy létrehozott illetékes hatóságokkal és egyedüli kapcsolattartó pontokkal a biztonsági események, a kiberfenyegetések, a sérülékenységek, a majdnem bekövetkezett (near miss) események, a lehetséges ellenintézkedések és a bevált gyakorlatok, valamint az uniós szervezetek IKT-környezetei védelmének javítása szempontjából releváns valamennyi kérdés tekintetében, többek között az (EU) 2022/2555 irányelv 15. cikke alapján létrehozott CSIRT-hálózaton keresztül. A CERT-EU támogatja a Bizottságot a nagyszabású kiberbiztonsági események és válsághelyzetek összehangolt kezeléséről szóló (EU) 2022/2555 irányelv 16. cikke alapján létrehozott EU-CyCLONe-ban.

(2) Amennyiben a CERT-EU valamely tagállam területén bekövetkező jelentős biztonsági eseményről szerez tudomást, az (1) bekezdéssel összhangban haladéktalanul értesíti az érintett partnert az adott tagállamban.

(3) A CERT-EU – feltéve, hogy a személyes adatok az alkalmazandó uniós adatvédelmi joggal összhangban védelemben részesülnek – indokolatlan késedelem nélkül, az érintett uniós szervezet beleegyezése nélkül megosztja a releváns biztonságiesemény-specifikus információkat a hasonló kiberfenyegetések vagy biztonsági események felderítésének megkönnyítése vagy a biztonsági esemény elemzéséhez való hozzájárulás érdekében a tagállami partnerekkel. A CERT-EU az olyan biztonságiesemény-specifikus információkat, amelyek feltárják a biztonsági esemény célpontját csak az alábbiak egyikének fennállása esetén oszthatja meg:

a) az érintett uniós szervezet beleegyezését adja;

b) az érintett uniós szervezet nem adja beleegyezését az a) pontban előírtak szerint, de az érintett uniós szervezet kilétének közzététele növelné annak valószínűségét, hogy a máshol bekövetkező biztonsági eseményeket elkerülnék vagy mérsékelnék;

c) az érintett uniós szervezet már nyilvánosságra hozta, hogy érintett volt.

A biztonsági eseményre vonatkozó azon információk cseréjére vonatkozó határozatokat, amelyek az első albekezdés b) pontja alapján feltárják a biztonsági esemény célpontjának kilétét, a CERT-EU vezetőjének jóvá kell hagynia. Az ilyen határozat kibocsátása előtt a CERT-EU írásban felveszi a kapcsolatot az érintett uniós szervezettel, egyértelműen kifejtve, hogy kilétének nyilvánosságra hozatala hogyan segítené elő máshol a biztonsági események elkerülését vagy mérséklését. A CERT-EU vezetőjének magyarázatot kell adnia, és kifejezetten fel kell kérnie az uniós szervezetet, hogy meghatározott határidőn belül nyilatkozzon arról, hogy beleegyezik-e ebbe. A CERT-EU vezetője arról is tájékoztatja az uniós szervezetet, hogy az adott magyarázat fényében fenntartja magának a jogot arra, hogy még beleegyezés hiányában is közzétegye az információkat. Az érintett uniós szervezetet az információk közzététele előtt tájékoztatni kell.

18. cikk

A CERT-EU együttműködése más partnerekkel

(1) A CERT-EU együttműködhet az uniós kiberbiztonsági követelmények hatálya alá tartozó, a 17. cikkben említettektől eltérő uniós partnerekkel, többek között ágazatspecifikus partnerekkel az eszközök és módszerek – például a technikák, taktikák, eljárások és a legjobb gyakorlatok –, valamint a kiberfenyegetések és -sérülékenységek terén. Az ilyen partnerekkel való mindennemű együttműködéshez a CERT-EU-nak – eseti alapon – előzetes jóváhagyást kell kérnie az IICB-től. Amennyiben a CERT-EU ilyen partnerekkel alakít ki együttműködést, erről tájékoztatnia kell a partner székhelye szerinti tagállamban működő valamennyi, a 17. cikk (1) bekezdésében említett érintett tagállami partnert. Adott esetben az ilyen együttműködést és annak feltételeit – többek között a kiberbiztonság, az adatvédelem és az információkezelés tekintetében – egyedi titoktartási megállapodásokban, például szerződésekben vagy igazgatási megállapodásokban kell meghatározni. A titoktartási megállapodásokhoz nem kell kikérni az IICB előzetes jóváhagyását, de az IICB elnökét ezekről tájékoztatni kell. Abban az esetben, ha az uniós szervezetek vagy egy másik fél érdekében sürgős és azonnali kiberbiztonsági információcserére van szükség, a CERT-EU ezt megteheti egy olyan szervezettel, amelynek különleges kompetenciája, kapacitása és szakértelme indokoltan szükséges ahhoz, hogy segítséget nyújtson egy ilyen sürgős és azonnali szükséglet kielégítéséhez, még akkor is, ha a CERT-EU nem kötött titoktartási megállapodást az adott szervezettel. Ilyen esetekben a CERT-EU haladéktalanul tájékoztatja az IICB elnökét, és rendszeres jelentések vagy ülések útján jelentést tesz az IICB-nek.

(2) A CERT-EU együttműködhet más partnerekkel, például kereskedelmi szervezetekkel, köztük ágazatspecifikus ipari szervezetekkel, nemzetközi szervezetekkel, nem uniós nemzeti szervezetekkel vagy egyéni szakértőkkel annak érdekében, hogy információkat gyűjtsön az általános és konkrét kiberfenyegetésekről, a majdnem bekövetkezett (near miss) eseményekről, a sérülékenységekről és a lehetséges ellenintézkedésekről. Az ilyen partnerekkel való szélesebb körű együttműködéshez a CERT-EU-nak eseti alapon előzetes jóváhagyást kell kérnie az IICB-től.

(3) A CERT-EU – a biztonsági esemény által érintett uniós szervezet beleegyezésével, és feltéve, hogy az érintett partnerrel titoktartási megállapodás vagy szerződés van érvényben – az (1) és a (2) bekezdésben említett partnerek rendelkezésére bocsáthatja az adott biztonsági eseményre vonatkozó információkat, kizárólag az elemzéséhez való hozzájárulás céljából.

V. FEJEZET

EGYÜTTMŰKÖDÉSI ÉS JELENTÉSTÉTELI KÖTELEZETTSÉGEK

19. cikk

Információkezelés

(1) Az uniós szervezeteknek és a CERT-EU-nak tiszteletben kell tartaniuk az EUMSZ 339. cikke vagy az azzal egyenértékű alkalmazandó keretrendszerek szerinti szakmai titoktartási kötelezettséget.

(2) Az 1049/2001/EK európai parlamenti és tanácsi rendelet ([10]) alkalmazandó 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 szervezetekkel vagy adott esetben a tagállamokkal.

(3) Az uniós szervezetek és a CERT-EU általi információkezelésnek meg kell felelnie az információbiztonság tekintetében alkalmazandó szabályoknak.

([10]) 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.).

20. cikk

Kiberbiztonsági információmegosztási megállapodások

(1) Az uniós szervezetek önkéntes alapon értesíthetik a CERT-EU-t az őket érintő biztonsági eseményekről, kiberfenyegetésekről, majdnem bekövetkezett (near miss) eseményekről és sérülékenységekről, és azokról információkat szolgáltathatnak számára. A CERT-EU biztosítja, hogy az uniós szervezetekkel való információmegosztás megkönnyítése érdekében hatékony, magas szintű nyomon követhetőséget, titkosságot és megbízhatóságot biztosító kommunikációs eszközök álljanak rendelkezésre. Az értesítések feldolgozásakor a CERT-EU előnyben részesítheti a kötelező értesítések feldolgozását az önkéntes értesítésekkel szemben. A 12. cikk sérelme nélkül, az önkéntes értesítés nem eredményezhet olyan további kötelezettségeket az adatszolgáltató uniós szervezet számára, amelyek nem terhelték volna, ha nem nyújtotta volna be az értesítést.

(2) Annak érdekében, hogy teljesítse a 13. cikkben ráruházott küldetését és feladatait, a CERT-EU felkérheti az uniós szervezeteket, hogy információkat szolgáltassanak számára IKT rendszereik nyilvántartásaiból, ideértve a kiberfenyegetésekre, a majdnem bekövetkezett (near miss) eseményekre, a sérülékenységekre, a fertőzöttségi mutatókra (IoC), a kiberbiztonsági figyelmeztetésekre és a biztonsági események észlelésére szolgáló kiberbiztonsági eszközök konfigurációjára vonatkozó ajánlásokra vonatkozó információkat is. A megkeresett uniós szervezet indokolatlan késedelem nélkül továbbítja a kért információt és annak minden későbbi frissítését is.

(3) A CERT-EU akkor cserélhet az uniós szervezetekkel olyan biztonságiesemény-specifikus információkat, amelyek felfedik a biztonsági eseménnyel érintett uniós szervezet kilétét, ha az érintett uniós szervezet abba beleegyezik. Amennyiben egy uniós szervezet megtagadja a beleegyezését, a CERT-EU rendelkezésére kell bocsátania a döntését alátámasztó indokokat.

(4) Az uniós szervezeteknek kérésre meg kell osztaniuk az Európai Parlamenttel és a Tanáccsal a kiberbiztonsági tervek teljesítésére vonatkozó információkat.

(5) Az IICB vagy adott esetben a CERT-EU kérésre iránymutatásokat, ajánlásokat és cselekvési felhívásokat oszt meg az Európai Parlamenttel és a Tanáccsal.

(6) Az e cikkben meghatározott megosztási kötelezettségek nem terjednek ki a következőkre:

a) EU-minősített adatok;

b) olyan információk, amelyek további terjesztését egy látható jelöléssel kizárták, kivéve, ha kifejezetten engedélyezték azok CERT-EU-val való megosztását.

21. cikk

Jelentéstételi kötelezettségek

(1) Egy biztonsági esemény akkor tekintendő jelentősnek, ha:

a) súlyos működési zavart eredményezett, illetve eredményezhet az uniós szervezet működésében, vagy pénzügyi veszteséggel járt, illetve járhat az érintett uniós szervezet számára;

b) a biztonsági esemény jelentős vagyoni vagy nem vagyoni kár okozásával más természetes vagy jogi személyeket érintett vagy érinthet.

(2) Az uniós szervezeteknek be kell nyújtaniuk a CERT-EU-nak a következőket:

a) indokolatlan késedelem nélkül, de minden esetben a jelentős biztonsági eseményről való tudomásszerzéstől számított 24 órán belül egy első figyelmeztetést, amelyben adott esetben fel kell tüntetni, hogy a jelentős biztonsági eseményt gyaníthatóan jogellenes vagy rosszindulatú cselekmény okozta-e és hogy lehet-e több szervezetre kiterjedő vagy határokon átnyúló hatása;

b) indokolatlan késedelem nélkül, de minden esetben a jelentős biztonsági eseményről való tudomásszerzéstől számított 72 órán belül a biztonsági eseményről szóló értesítést, amely adott esetben aktualizálja az a) pontban említett információkat, és tartalmazza a jelentős biztonsági esemény, illetve annak súlyossága és hatása kezdeti értékelését, valamint – amennyiben rendelkezésre állnak – a fertőzöttségi mutatókat;

c) a CERT-EU kérésére a releváns állapotfrissítésekről szóló időközi jelentést.

d) zárójelentést, legkésőbb a b) pont szerinti, a biztonsági eseményről való értesítés benyújtását követő egy hónapon belül, amely tartalmazza a következőket:

i. a biztonsági esemény részletes leírása, beleértve annak súlyosságát és hatását;

ii. a biztonsági eseményt valószínűsíthetően előidéző fenyegetés vagy kiváltó ok típusa;

iii. az alkalmazott és folyamatban lévő mérséklő intézkedések;

iv. adott esetben a biztonsági esemény határokon átnyúló vagy intézmények közötti hatása;

e) a d) pontban említett zárójelentés benyújtásának időpontjában folyamatban lévő biztonsági esemény esetén az említett időpontban eredményjelentés, a biztonsági esemény kezelését követő egy hónapon belül pedig zárójelentés.

(3) Az uniós szervezet indokolatlan késedelem nélkül, de minden esetben a jelentős biztonsági eseményről való tudomásszerzéstől számított 24 órán belül tájékoztatja a 17. cikk (1) bekezdésében említett, a székhelye szerinti tagállamban működő érintett tagállami partnereket a jelentős biztonsági esemény bekövetkezéséről.

(4) Az uniós szervezeteknek be kell jelenteniük többek között minden olyan információt, amely lehetővé teszi a CERT-EU számára, hogy a jelentős biztonsági eseményt követően azonosítsa a szervezetek közötti, a fogadó tagállamra gyakorolt vagy határokon átnyúló hatást. A 12. cikk sérelme nélkül, pusztán az értesítés következtében az uniós szervezetet többletfelelősség nem terhelheti.

(5) Adott esetben az uniós szervezetek indokolatlan késedelem nélkül tájékoztatják az érintett hálózati és információs rendszerek vagy az IKT-környezet más elemei azon felhasználóit, akiket jelentős biztonsági esemény vagy jelentős kiberfenyegetés érinthet, és adott esetben tájékoztatják őket a biztonsági eseményre vagy fenyegetésre válaszul általuk hozható mérséklő intézkedésekről, egyéb intézkedésekről vagy korrekciós intézkedésekről is. Adott esetben az uniós szervezetek tájékoztatják a felhasználókat magáról a jelentős kiberfenyegetésről.

(6) Amennyiben egy jelentős biztonsági esemény vagy jelentős kiberfenyegetés egy hálózati és információs rendszert, vagy egy uniós szervezet IKT-környezetének valamely olyan elemét érinti, amely köztudottan kapcsolódik egy másik uniós szervezet IKT-környezetéhez, a CERT-EU megfelelő kiberbiztonsági riasztást ad ki.

(7) Az uniós szervezetek a CERT-EU kérésére indokolatlan késedelem nélkül átadják a CERT-EU részére a biztonsági eseményekben érintett elektronikus eszközök használatával létrehozott digitális információkat. A CERT-EU további részletekkel szolgálhat a helyzetismerethez és a biztonsági eseményre való reagáláshoz szükséges információtípusokról.

(8) A CERT-EU háromhavonta összefoglaló jelentést nyújt be az IICB-nek, az ENISA-nak, az EU INTCEN-nek és a CSIRT-hálózatnak, amely anonimizált és összesített adatokat tartalmaz a 20. cikk szerinti jelentős biztonsági eseményekről, biztonsági eseményekről, kiberfenyegetésekről, majdnem bekövetkezett (near miss) eseményekről és sérülékenységekről, valamint az e cikk (2) bekezdése szerint bejelentett jelentős biztonsági eseményekről. Az összefoglaló jelentés hozzájárul az uniós kiberbiztonsági helyzetről az (EU) 2022/2555 irányelv 18. cikke alapján elfogadott, kétévente kiadandó jelentéshez.

(9) Az IICB-nek 2024. július 8-ig iránymutatásokat vagy ajánlásokat kell ki bocsátania, amelyekben tovább pontosítja az e cikk szerinti jelentéstétel szabályait, formátumát és tartalmát. Az ilyen iránymutatások vagy ajánlások kidolgozása során az IICB figyelembe veszi az (EU) 2022/2555 irányelv 23. cikkének (11) bekezdése alapján elfogadott, az információk típusát, formátumát és az értesítésekre vonatkozó eljárást meghatározó végrehajtási jogi aktusokat. A CERT-EU megosztja a megfelelő technikai részleteket annak érdekében, hogy lehetővé tegye az uniós szervezetek általi proaktív felderítést, biztonsági eseményekre való reagálást vagy a mérséklő intézkedések meghozatalát.

(10) Az e cikkben meghatározott jelentéstételi kötelezettségek nem terjednek ki a következőkre:

a) EU-minősített adatok;

b) olyan információk, amelyek további terjesztését egy látható jelöléssel kizárták, kivéve, ha kifejezetten engedélyezték azok CERT-EU-val való megosztását.

22. cikk

A biztonsági eseményekre való reagálás koordinálása és az azokkal kapcsolatos együttműködés

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

a) az uniós szervezetek;

b) a 17. és a 18. cikkben említett partnerek.

(2) A CERT-EU-nak – adott esetben az ENISA-val szorosan együttműködve – elő kell segítenie az uniós szervezetek közötti koordinációt a biztonsági eseményekre való reagálás terén, beleértve a következőket:

a) hozzájárulás az egységes külső kommunikációhoz;

b) kölcsönös támogatás, például az uniós szervezetek számára releváns információk megosztása vagy adott esetben közvetlen helyszíni segítségnyújtás;

c) az operatív erőforrások optimális felhasználása;

d) koordináció más uniós szintű válságreagálási mechanizmusokkal.

(3) A CERT-EU az ENISA-val szorosan együttműködve támogatja az uniós szervezeteket a biztonsági eseményekkel, kiberfenyegetésekkel, sérülékenységekkel és majdnem bekövetkezett (near miss) eseményekkel kapcsolatos helyzetismeret kialakításában, valamint a kiberbiztonság területén bekövetkezett fontos fejlemények megosztásában.

(4) Az IICB-nek 2025. január 8-ig, a CERT-EU ajánlása alapján iránymutatásokat vagy ajánlásokat kell elfogadnia a jelentős biztonsági eseményekre való reagálás koordinálásáról és az azokkal kapcsolatos együttműködésről. Amennyiben egy biztonsági esemény büntetőjogi jellege gyanítható, a CERT-EU tanácsot ad arra vonatkozóan, hogy miként kell indokolatlan késedelem nélkül bejelenteni a biztonsági eseményt a bűnüldöző hatóságoknak.

(5) Valamely tagállam egyedi kérésére és az érintett uniós szervezetek jóváhagyásával a CERT-EU az (EU) 2022/2555 irányelv 15. cikke (3) bekezdésének g) pontjával összhangban felkérheti a 23. cikk (4) bekezdésében említett jegyzékben szereplő szakértőket, hogy járuljanak hozzá az adott tagállamban hatást gyakorló súlyos biztonsági eseményre vagy egy nagyszabású kiberbiztonsági eseményre való reagáláshoz. Az IICB a CERT EU javaslatára egyedi szabályokat hagy jóvá az uniós szervezetek technikai szakértőihez való hozzáférésre és azok igénybevételére vonatkozóan.

23. cikk

A súlyos biztonsági események kezelése

(1) Az uniós szervezeteket érintő súlyos biztonsági események koordinált operatív szintű kezelésének támogatása, továbbá a releváns információknak az uniós szervezetek közötti és a tagállamokkal való rendszeres cseréjéhez való hozzájárulás érdekében az IICB a 11. cikk q) pontja értelmében a 22. cikk (2) bekezdésében részletezett tevékenységek alapján, a CERT-EU-val és az ENISA-val szoros együttműködésben kiberbiztonsági válságkezelési tervet hoz létre. A kiberbiztonsági válságkezelési tervnek legalább a következő elemeket kell tartalmaznia:

a) az uniós szervezetek közötti, a súlyos biztonsági események operatív szintű kezelésére vonatkozó koordinációra és információáramlásra vonatkozó szabályok;

b) közös eljárási standardok;

c) a súlyos biztonsági események súlyossági fokaira és a válságot kiváltó tényezőkre vonatkozó egységes taxonómia;

d) rendszeres gyakorlatok;

e) az igénybe veendő biztonságos kommunikációs csatornák.

(2) Az e cikk (1) bekezdése alapján létrehozott kiberbiztonsági válságkezelési tervre figyelemmel és az (EU) 2022/2555 irányelv 16. cikke (2) bekezdése első albekezdésének sérelme nélkül a Bizottságnak az IICB-ben részt vevő képviselője a kapcsolattartó pont a súlyos biztonsági eseményekkel kapcsolatos releváns információknak az EU-CyCLONe-val való megosztása tekintetében.

(3) A CERT-EU koordinálja az uniós szervezetek között a súlyos biztonsági események kezelését. Nyilvántartást vezet arról a rendelkezésre álló technikai szakértelemről, amelyre ilyen súlyos biztonsági események esetén az eseményekre való reagáláshoz szükség lehet, és segíti az IICB-t az uniós szervezetek 9. cikk (2) bekezdésében említett súlyos biztonsági eseményekre vonatkozó kiberbiztonsági válságkezelési terveinek koordinálásában.

(4) Az uniós szervezetek hozzájárulnak a technikai szakértelem nyilvántartásához azáltal, hogy a szervezetükön belül rendelkezésre álló szakértőkről évente frissített jegyzéket állítanak össze, amely részletezi sajátos technikai készségeiket.

VI. FEJEZET

ZÁRÓ RENDELKEZÉSEK

24. cikk

Kezdeti költségvetési átcsoportosítás

A CERT-EU megfelelő és stabil működésének biztosítása érdekében a Bizottság javasolhatja a személyzeti és pénzügyi erőforrások átcsoportosítását a Bizottság költségvetésébe a CERT-EU műveleteiben való felhasználás céljából. Az átcsoportosítás az e rendelet hatálybalépését követően elfogadott első uniós éves költségvetéssel egy időben lép hatályba.

25. cikk

Felülvizsgálat

(1) 2025. január 8-ig, majd azt követően évente az IICB a CERT-EU segítségével jelentést tesz a Bizottságnak e rendelet végrehajtásáról. Az IICB ajánlásokat tehet a Bizottságnak e rendelet felülvizsgálatára.

(2) A Bizottság 2027. január 8-ig és azt követően kétévente értékeli e rendelet végrehajtását, valamint a stratégiai és operatív szinten szerzett tapasztalatokat, és jelentést nyújt be az Európai Parlamentnek és a Tanácsnak.

Az e bekezdés első albekezdésében említett jelentés tartalmazza a 16. cikk (1) bekezdésében említett felülvizsgálatot a CERT-EU uniós hivatalként való létrehozásának lehetőségéről.

(3) A Bizottság 2029. január 8-ig értékeli e rendelet működését, és jelentést nyújt be az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. A Bizottság azt is értékeli, hogy helyénvaló-e e rendelet hatálya alá vonni az EU-minősített adatokat kezelő hálózati és információs rendszereket, figyelembe véve az e rendszerekre alkalmazandó egyéb uniós jogalkotási aktusokat is. A jelentéshez szükség esetén jogalkotási javaslatot kell csatolni.

26. 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 Strasbourgban, 2023. december 13-án.

az Európai Parlament részéről	*a Tanács részéről*
az elnök	*az elnök*
R. METSOLA	P. NAVARRO RÍOS