Európai Parlament
2019-2024

Alkotmányügyi Bizottság

2022/0085(COD)

31.1.2023

VÉLEMÉNY

az Alkotmányügyi Bizottság részéről

az Ipari, Kutatási és Energiaügyi Bizottság részére

az uniós intézmények, szervek, hivatalok és ügynökségek egységesen magas szintű kiberbiztonságát biztosító intézkedések meghatározásáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatról
(COM(2022)0122 – C9-0122/2022 – 2022/0085(COD))

A vélemény előadója: Markéta Gregorová

PA_Legam

RÖVID INDOKOLÁS

Az Európai Unió intézményei, szervei és hivatalai az elmúlt években az állandó technológiai fejlődés és az ebből következő, folyamatosan változó kiberfenyegetettségi szintek miatt egyre digitalizáltabb környezetben működnek. Ezt a helyzetet tovább súlyosbította a Covid19-járvány okozta egészségügyi válság és többek között a távmunka elterjedése, miközben tovább nőtt a különböző forrásokból érkező kifinomult támadások száma.

Jelenleg a kiberbiztonsági környezet – többek között az irányítás, a kiberhigiénia, az általános képességek és az érettség – jelentősen eltér az uniós intézmények, szervek és hivatalok között, ami további akadályt gördít a nyitott, hatékony és független európai közigazgatás elé.

Az előadó ezért egyetért azzal, hogy a közös kiberbiztonsági rendszerek és követelmények kialakítása érdekében az uniós intézmények, szervek és hivatalok közötti alapmegközelítésre lenne szükség annak biztosítása érdekében, hogy a kiberbiztonság ugyanebbe az irányba fejlődjön, hozzájárulva ezáltal az európai közigazgatás hatékonyságához és függetlenségéhez.

Az előadó továbbá úgy véli, hogy egy szilárd és következetes biztonsági keret rendkívül fontos az uniós alkalmazottak, az adatok, a kommunikációs hálózatok, az információs rendszerek és a döntéshozatali folyamatok védelme érdekében, hozzájárulva ezáltal az Európai Unió demokratikus működéséhez is. Az uniós intézmények, szervek és hivatalok megerősített biztonsági kultúrája felkészítené Európát a digitális korra is, és időtálló gazdaságot építene az emberek szolgálatában.

MÓDOSÍTÁSOK

Az Alkotmányügyi Bizottság felkéri az Ipari, Kutatási és Energiaügyi Bizottságot mint illetékes bizottságot, hogy vegye figyelembe az alábbi módosításokat:

Módosítás 1

Rendeletre irányuló javaslat
1 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(1) A digitális korban az információs és kommunikációs technológia a nyitott, hatékony és független uniós közigazgatás sarokköve. A fejlődő technológia és a digitális rendszerek fokozódó összetettsége és összeköttetése növeli a kiberbiztonsági kockázatokat, ami az uniós közigazgatást még sérülékenyebbé teszi a kiberfenyegetésekkel és biztonsági	(1) A digitális korban az információs és kommunikációs technológia a nyitott, hatékony és független uniós közigazgatás sarokköve. A fejlődő technológia és a digitális rendszerek fokozódó összetettsége és összeköttetése növeli a kiberbiztonsági kockázatokat, ami az uniós közigazgatást még sérülékenyebbé teszi a kiberfenyegetésekkel és biztonsági

eseményekkel szemben, ami végeredményben veszélyezteti a közigazgatás ügymenet-folytonosságát és az adatai biztosítására irányuló képességét. Míg a felhőalapú szolgáltatások fokozott használata, az ***informatika*** mindenütt elterjedt használata, a nagyarányú digitalizáció, a távmunka, valamint a fejlődő technológia és konnektivitás manapság az uniós igazgatási szervek valamennyi tevékenységének alapvető jellemzői, a digitális rezilienciát még nem építették be kellőképpen munkájukba.	eseményekkel szemben, ami végeredményben veszélyezteti a közigazgatás ügymenet-folytonosságát és az adatai biztosítására irányuló képességét. Míg a felhőalapú szolgáltatások fokozott használata, az ***információs és kommunikációs technológia (IKT)*** mindenütt elterjedt használata, a nagyarányú digitalizáció, a távmunka, valamint a fejlődő technológia és konnektivitás manapság az uniós igazgatási szervek valamennyi tevékenységének alapvető jellemzői, a digitális rezilienciát még nem építették be kellőképpen munkájukba.

Indokolás

A Bizottság javaslatában szereplő „informatika” kifejezés helyett az „IKT”-t kellene használni, amely a NIS 2 irányelvben és az uniós kiberbiztonsági jogszabályban használt kifejezés.

Módosítás 2

Rendeletre irányuló javaslat
2 preambulumbekezdés

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

sebezhetőségeket.

Módosítás 3

Rendeletre irányuló javaslat
3 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(3) Az uniós intézmények, szervek és ügynökségek ***informatikai környezetében*** kölcsönös függőségek és integrált adatáramlások fordulnak elő, felhasználóik pedig szorosan együttműködnek. Ez az összekapcsoltság azt jelenti, hogy bármilyen zavarnak – akkor is, ha eredetileg csak egy uniós intézményre, szervre vagy ügynökségre korlátozódik – szélesebb körben lépcsőzetes hatásai lehetnek, ami messzemenő és hosszú távú negatív hatásokat eredményezhet a többire nézve. Emellett egyes intézmények, szervek és ügynökségek ***informatikai környezete*** összekapcsolódik a tagállamok ***informatikai környezetével***, ami az egyik uniós szervezetnél felmerülő biztonsági esemény miatt kockázatot jelenthet a tagállamok ***informatikai környezeteinek*** kiberbiztonságára nézve, és fordítva.	(3) Az uniós intézmények, szervek***, hivatalok*** és ügynökségek ***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 egy uniós intézményre, szervre***, hivatalra*** vagy ügynökségre korlátozódik – szélesebb körben lépcsőzetes hatásai lehetnek, ami messzemenő és hosszú távú negatív hatásokat eredményezhet a többire nézve. Emellett egyes intézmények, szervek***, hivatalok*** és ügynökségek ***IKT-környezete*** összekapcsolódik a tagállamok ***IKT-környezetével***, ami az egyik uniós szervezetnél felmerülő biztonsági esemény miatt kockázatot jelenthet a tagállamok ***IKT-környezeteinek*** kiberbiztonságára nézve, és fordítva.

Módosítás 4
Rendeletre irányuló javaslat
4 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(4) Az uniós intézmények, szervek és ügynökségek vonzó célpontok, akik magasan képzett és megfelelő erőforrásokkal rendelkező fenyegető szereplőkkel, valamint egyéb fenyegetésekkel szembesülnek. A kibertámadásokkal szembeni ellenálló képesség szintje és érettsége és a rossz szándékú kibertevékenységek felderítésére és az azokra való reagálásra irányuló	(4) Az uniós intézmények, szervek***, hivatalok*** és ügynökségek vonzó célpontok, akik magasan képzett és megfelelő erőforrásokkal rendelkező fenyegető szereplőkkel, valamint egyéb fenyegetésekkel szembesülnek. A kibertámadásokkal szembeni ellenálló képesség szintje és érettsége és a rossz szándékú kibertevékenységek felderítésére és az azokra való reagálásra irányuló

képesség ugyanakkor jelentős mértékben eltér a szervezetek között. Ezért az európai közigazgatás működéséhez szükséges, hogy az uniós intézmények, szervek és ügynökségek egységesen magas szintű kiberbiztonságot érjenek el olyan kiberbiztonsági minimumszabályok („kiberbiztonsági alapkövetelmények”) révén, amelyeknek a hálózati és információs rendszereknek, valamint üzemeltetőiknek és felhasználóiknak meg kell felelniük a kiberbiztonsági kockázatok ***minimalizálása***, valamint ***az*** információcsere és ***az együttműködés érdekében***.	képesség ugyanakkor jelentős mértékben eltér a szervezetek között. Ezért az európai közigazgatás működéséhez szükséges, hogy az uniós intézmények, szervek***, hivatalok*** és ügynökségek egységesen magas szintű kiberbiztonságot érjenek el olyan ***közös*** kiberbiztonsági minimumszabályok („kiberbiztonsági alapkövetelmények”) révén, amelyeknek a hálózati és információs rendszereknek, valamint üzemeltetőiknek és felhasználóiknak meg kell felelniük a kiberbiztonsági kockázatok ***korlátozása érdekében***, valamint ***rendszeres és hatékony*** információcsere és ***együttműködés, illetve kiberbiztonsági oktatás révén***.

Módosítás 5

Rendeletre irányuló javaslat
7 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(7) Az uniós intézmények, szervek és ügynökségek közötti különbségek rugalmasságot tesznek szükségessé a végrehajtás terén, mivel az egységes megközelítés nem illik minden szervezetre. A kiberbiztonság egységesen magas szintjére vonatkozó ***intézkedések nem tartalmazhatnak olyan kötelezettségeket, amelyek közvetlenül ütköznek*** az uniós intézmények, szervek és ügynökségek feladatainak ***ellátásával***, ***vagy beavatkoznak*** intézményi ***autonómiájukba***. Ezért ezeknek az intézményeknek, szerveknek és ügynökségeknek létre kell hozniuk a kiberbiztonsági kockázatkezelésre, -irányításra és -ellenőrzésre vonatkozó saját keretrendszereiket, és el kell fogadniuk saját alapkövetelményeiket és kiberbiztonsági terveiket.	(7) Az uniós intézmények, szervek***, hivatalok*** és ügynökségek közötti különbségek rugalmasságot tesznek szükségessé a végrehajtás terén, mivel az egységes megközelítés nem illik minden szervezetre. A kiberbiztonság egységesen magas szintjére vonatkozó ***intézkedéseknek támogatniuk kell*** az uniós intézmények, szervek***, hivatalok*** és ügynökségek feladatainak ***ellátását***, ***és figyelembe kell venniük azok*** intézményi ***autonómiáját***. Ezért ezeknek az intézményeknek, szerveknek***, hivataloknak*** és ügynökségeknek ***figyelembe véve saját keretrendszerük koherenciáját és interoperabilitását, valamint az e rendelet által megállapított közös keretrendszer alapján*** létre kell hozniuk a kiberbiztonsági kockázatkezelésre, -irányításra és -ellenőrzésre vonatkozó saját keretrendszereiket, és el kell fogadniuk saját alapkövetelményeiket és

kiberbiztonsági terveiket.

Módosítás 6
Rendeletre irányuló javaslat
8 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(8) Annak elkerülése érdekében, hogy az uniós intézményekre, szervekre és ügynökségekre aránytalanul nagy pénzügyi és adminisztratív terhek háruljanak, a kiberbiztonsági kockázatok kezelésére vonatkozó követelményeknek – a legújabb technikai lehetőségekre figyelemmel – ***arányosaknak*** kell ***lenniük*** az adott hálózati és információs rendszert érintő ***kockázatokkal***. Minden uniós intézménynek, szervnek és ügynökségnek törekednie kell arra, hogy ***informatikai költségvetésének megfelelő százalékát*** a kiberbiztonság szintjének javítására fordítsa***; hosszabb távon 10 %-os nagyságrendű célkitűzés elérésére törekedve.***	(8) Annak elkerülése érdekében, hogy az uniós intézményekre, szervekre***, hivatalokra*** és ügynökségekre aránytalanul nagy pénzügyi és adminisztratív terhek háruljanak, a kiberbiztonsági kockázatok kezelésére vonatkozó követelményeknek – a legújabb technikai lehetőségekre figyelemmel – ***meg*** kell ***felelniük*** az adott hálózati és információs rendszert érintő ***kockázatoknak***. Minden uniós intézménynek, szervnek***, hivatalnak*** és ügynökségnek törekednie kell arra, hogy ***IKT-költségvetésének legalább 10%-át*** a kiberbiztonság szintjének javítására fordítsa ***középtávon, hosszú távon pedig szükség esetén többet;***

Módosítás 7

Rendeletre irányuló javaslat
9 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(9) A kiberbiztonság egységesen magas szintje megköveteli, hogy a kiberbiztonság az egyes uniós intézmények, ***szervek*** és ügynökségek legmagasabb szintű ***vezetésének*** felügyelete alá tartozzon, amelynek jóvá kell hagynia az egyes intézmények, szervek és ügynökségek által létrehozandó keretrendszerben azonosított kockázatok kezelésére szolgáló kiberbiztonsági alapkövetelményeket. A kiberbiztonsági ***kultúra***, azaz a kiberbiztonság napi gyakorlatának ***kezelése*** valamennyi uniós intézmény, szerv és	(9) A kiberbiztonság egységesen magas szintje megköveteli, hogy a kiberbiztonság az egyes uniós intézmények, ***hivatalok*** és ügynökségek legmagasabb szintű ***vezetését magában foglaló közös uniós testület*** felügyelete alá tartozzon, amelynek jóvá kell hagynia az egyes intézmények, szervek***, hivatalok*** és ügynökségek által létrehozandó keretrendszerben azonosított kockázatok kezelésére szolgáló kiberbiztonsági alapkövetelményeket. A kiberbiztonsági ***kultúrának***, azaz a kiberbiztonság napi gyakorlatának

ügynökség kiberbiztonsági alapkövetelményeinek szerves ***részét képezi***.

kezelésének valamennyi uniós intézmény, szerv***, hivatal*** és ügynökség kiberbiztonsági alapkövetelményeinek szerves ***részévé kell válnia***.

Módosítás 8

Rendeletre irányuló javaslat
10 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(10) Az uniós intézményeknek, szerveknek és ügynökségeknek fel kell mérniük a beszállítókkal és szolgáltatókkal – többek között az adattárolási és -kezelési szolgáltatások nyújtóival vagy az irányított biztonsági szolgáltatásokkal – fenntartott kapcsolatokból eredő kockázatokat, és megfelelő intézkedéseket kell hozniuk azok kezelésére. Ezeknek az intézkedéseknek a kiberbiztonsági alapkövetelmények részét kell képezniük, és azokat a CERT-EU által kiadott útmutatókban vagy ajánlásokban részletesebben meg kell határozni. Az intézkedések és iránymutatások meghatározásakor megfelelően figyelembe kell venni a vonatkozó uniós jogszabályokat és szakpolitikákat, többek között a Kiberbiztonsági Együttműködési Csoport által kiadott kockázatértékeléseket és ajánlásokat, például az összehangolt uniós kockázatértékelést és az 5G kiberbiztonságra vonatkozó uniós eszköztárat. Emellett az (EU) 2019/881 rendelet 49. cikke alapján elfogadott konkrét uniós kiberbiztonsági tanúsítási rendszerek keretében ***szükség lehet a*** releváns IKT-termékek, -szolgáltatások és -folyamatok ***tanúsítására***.	(10) Az uniós intézményeknek, szerveknek***, hivataloknak*** és ügynökségeknek fel kell mérniük a beszállítókkal és szolgáltatókkal – többek között az adattárolási és -kezelési szolgáltatások nyújtóival vagy az irányított biztonsági szolgáltatásokkal – fenntartott kapcsolatokból eredő kockázatokat, és megfelelő intézkedéseket kell hozniuk azok kezelésére. ***Ezeket a beszállítókat és szolgáltatókat alaposan át kell vizsgálni, figyelembe véve a teljes ellátási láncot, valamint azt a gazdasági és politikai környezetet, amelyben működnek. Amennyiben az ilyen beszállítókkal és szolgáltatókkal fennálló kapcsolatok kockázatot jelentenek az Unió demokratikus folyamatainak integritására nézve, azokat indokolatlan késedelem nélkül meg kell szüntetni.*** Ezeknek az intézkedéseknek a kiberbiztonsági alapkövetelmények részét kell képezniük, és azokat a CERT-EU által kiadott útmutatókban vagy ajánlásokban részletesebben meg kell határozni. Az intézkedések és iránymutatások meghatározásakor megfelelően figyelembe kell venni a vonatkozó uniós jogszabályokat és szakpolitikákat, többek között a Kiberbiztonsági Együttműködési Csoport által kiadott kockázatértékeléseket és ajánlásokat, például az összehangolt uniós kockázatértékelést és az 5G kiberbiztonságra vonatkozó uniós eszköztárat. Emellett ***a fenyegetettségi helyzetet és az ellenálló képesség***

	kialakításának fontosságát figyelembe véve az (EU) 2019/881 rendelet 49. cikke alapján elfogadott konkrét uniós kiberbiztonsági tanúsítási rendszerek keretében ***elő kell írni az uniós intézményeknél, szerveknél, hivataloknál és ügynökségeknél használt*** releváns IKT-termékek, -szolgáltatások és -folyamatok ***tanúsítását***.

Módosítás 9

Rendeletre irányuló javaslat
13 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(13) Számos kibertámadás olyan szélesebb körű kampányok részét képezi, amelyek az uniós intézmények, szervek és ügynökségek csoportjait, illetve az uniós intézményeket, szerveket és ügynökségeket is magukban foglaló érdekközösségeket célozzák. A proaktív felderítés, a biztonsági eseményekre való reagálás vagy az enyhítő intézkedések lehetővé tétele érdekében az uniós intézményeknek, szerveknek és ügynökségeknek értesíteniük kell a CERT-EU-t a jelentős kiberfenyegetésekről, a jelentős sebezhetőségekről és a jelentős biztonsági eseményekről, és meg kell osztaniuk azokat a megfelelő technikai részleteket, amelyek lehetővé teszik a más uniós intézményekben, szervekben és ügynökségekben előforduló, hasonló kiberfenyegetések, sebezhetőségek és biztonsági események észlelését vagy enyhítését, valamint az azokra való reagálást. Az irányelvben [a NIS 2-javaslatban] tervezettel megegyező megközelítést követve, amennyiben a szervezetek jelentős biztonsági eseményről szereznek tudomást, elő kell írni számukra, hogy 24 órán belül nyújtsanak be ***kezdeti értesítést*** a CERT-EU-nak. Az ilyen információcserének lehetővé kell tennie a	(13) Számos kibertámadás olyan szélesebb körű kampányok részét képezi, amelyek az uniós intézmények, szervek***, hivatalok*** és ügynökségek csoportjait, illetve az uniós intézményeket, szerveket***, hivatalokat*** és ügynökségeket is magukban foglaló érdekközösségeket célozzák. A proaktív felderítés, a biztonsági eseményekre való reagálás vagy az enyhítő intézkedések lehetővé tétele érdekében az uniós intézményeknek, szerveknek***, hivataloknak*** és ügynökségeknek értesíteniük kell a CERT-EU-t a jelentős kiberfenyegetésekről, a jelentős sebezhetőségekről és a jelentős biztonsági eseményekről, és meg kell osztaniuk azokat a megfelelő technikai részleteket, amelyek lehetővé teszik a más uniós intézményekben, szervekben***, hivatalokban*** és ügynökségekben előforduló, hasonló kiberfenyegetések, sebezhetőségek és biztonsági események észlelését vagy enyhítését, valamint az azokra való reagálást. Az irányelvben [a NIS 2-javaslatban] tervezettel megegyező megközelítést követve, amennyiben a szervezetek jelentős biztonsági eseményről szereznek tudomást, elő kell írni számukra, hogy ***indokolatlan késedelem nélkül és minden esetben legfeljebb*** 24 órán belül

CERT-EU számára, hogy továbbítsa az információkat más uniós intézményeknek, szerveknek és ügynökségeknek, valamint a megfelelő partnereknek, hogy segítsen megvédeni az uniós ***informatikai környezetet*** és az uniós partnerek ***informatikai környezetét*** a hasonló eseményekkel, fenyegetésekkel és sebezhetőségekkel szemben.	nyújtsanak be ***korai előrejelzést*** a CERT-EU-nak. Az ***uniós intézmények, szervek, hivatalok és ügynökségek számára elegendő forrást kell biztosítani jelentéstételi kötelezettségeik gyors és hatékony teljesítéséhez annak biztosítása érdekében, hogy a kialakított rendszer megfelelően működjön.*** Az ilyen információcserének lehetővé kell tennie a CERT-EU számára, hogy továbbítsa az információkat más uniós intézményeknek, szerveknek***, hivataloknak*** és ügynökségeknek, valamint a megfelelő partnereknek, hogy segítsen megvédeni az uniós ***IKT-környezetet*** és az uniós partnerek ***IKT-környezetét*** a hasonló eseményekkel, fenyegetésekkel és sebezhetőségekkel szemben.

Módosítás 10

Rendeletre irányuló javaslat
14 preambulumbekezdés

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

Módosítás 11

Rendeletre irányuló javaslat
16 preambulumbekezdés

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

Módosítás 12

Rendeletre irányuló javaslat
17 preambulumbekezdés

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

Módosítás 13

Rendeletre irányuló javaslat
18 preambulumbekezdés

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

Módosítás 14

Rendeletre irányuló javaslat
19 a preambulumbekezdés (új)

A Bizottság által javasolt szöveg	*Módosítás*
	(19a) Az uniós intézmények, szervek, hivatalok és ügynökségek kiberbiztonsági intézkedéseinek és iránymutatásainak jobb végrehajtása, valamint a kiberbiztonsági kultúrájuk megszilárdítása érdekében a CERT-EU-nak fokoznia kell az európai kiberbiztonsági kompetenciahálózattal és kompetenciaközponttal folytatott együttműködést is.

Módosítás 15

Rendeletre irányuló javaslat
20 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(20) Az operatív kiberbiztonság támogatása során a CERT-EU-nak az (EU) 2019/881 európai parlamenti és tanácsi rendeletben[5] előírt strukturált együttműködés révén fel kell használnia az Európai Uniós Kiberbiztonsági Ügynökség rendelkezésre álló szakértelmét. ***Adott esetben*** a két szervezet között külön megállapodásokat kell kialakítani az együttműködés gyakorlati megvalósításának meghatározása és a párhuzamos tevékenységek elkerülése érdekében. A CERT-EU-nak együtt kell működnie az Európai Uniós Kiberbiztonsági Ügynökséggel a fenyegetettségelemzés terén, és rendszeresen meg kell osztania az Ügynökséggel a fenyegetettségi helyzetjelentését.	(20) Az operatív kiberbiztonság támogatása során a CERT-EU-nak az (EU) 2019/881 európai parlamenti és tanácsi rendeletben[5] előírt strukturált együttműködés révén fel kell használnia az Európai Uniós Kiberbiztonsági Ügynökség rendelkezésre álló szakértelmét. A két szervezet között külön megállapodásokat kell kialakítani az együttműködés gyakorlati megvalósításának meghatározása és a párhuzamos tevékenységek elkerülése érdekében. A CERT-EU-nak együtt kell működnie az Európai Uniós Kiberbiztonsági Ügynökséggel a fenyegetettségelemzés terén, és rendszeresen meg kell osztania az Ügynökséggel a fenyegetettségi helyzetjelentését.
[5] Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) (HL L 151., 2019.6.7., 15. o.).	[5] Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) (HL L 151., 2019.6.7., 15. o.).

Módosítás 16
Rendeletre irányuló javaslat
24 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(24) Mivel a CERT-EU szolgáltatásai és feladatai valamennyi uniós intézmény,	(24) Mivel a CERT-EU szolgáltatásai és feladatai valamennyi uniós intézmény,

szerv és ügynökség érdekét szolgálják, az ***informatikai kiadásokkal*** rendelkező valamennyi uniós intézménynek, szervnek és ügynökségnek ***méltányos részt*** kell ***vállalnia*** e szolgáltatások és feladatok ***finanszírozásából***. Ezek a hozzájárulások nem érintik az uniós intézmények, szervek és ügynökségek költségvetési ***autonómiáját***.

szerv***, hivatal*** és ügynökség érdekét szolgálják, az ***IKT-kiadásokkal*** rendelkező valamennyi uniós intézménynek, szervnek***, hivatalnak*** és ügynökségnek ***arányosan hozzá*** kell ***járulnia*** e szolgáltatások és feladatok ***finanszírozásához***. Ezek a hozzájárulások nem érintik az uniós intézmények, szervek***, hivatalok*** és ügynökségek költségvetési ***kapacitását***.

Módosítás 17

Rendeletre irányuló javaslat
25 preambulumbekezdés

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

Módosítás 18

Rendeletre irányuló javaslat
1 cikk – 1 bekezdés – a pont

A Bizottság által javasolt szöveg	*Módosítás*
a) az uniós intézmények, szervek és ügynökségek kötelezettségei a belső kiberbiztonságikockázat-kezelési, -irányítási és -ellenőrzési keretrendszerük létrehozása kapcsán;	a) az uniós intézmények, szervek***, hivatalok*** és ügynökségek kötelezettségei a belső kiberbiztonságikockázat-kezelési, -irányítási és -ellenőrzési keretrendszerük létrehozása kapcsán;

Módosítás 19

Rendeletre irányuló javaslat
1 cikk – 1 bekezdés – c pont

A Bizottság által javasolt szöveg	*Módosítás*
c) az uniós intézmények, szervek és ügynökségek kiberbiztonsági központjának (CERT-EU) szervezetére és működésére, valamint az Intézményközi Kiberbiztonsági Testület szervezetére és működésére vonatkozó szabályok.	c) az uniós intézmények, szervek***,*** ***hivatalok*** és ügynökségek kiberbiztonsági központjának (CERT-EU) szervezetére és működésére, valamint az Intézményközi Kiberbiztonsági Testület ***(IICB) működtetésére,*** szervezetére és működésére vonatkozó szabályok.

Módosítás 20

Rendeletre irányuló javaslat
2 a cikk (új)

A Bizottság által javasolt szöveg	*Módosítás*
	2a. cikk
	A személyes adatok kezelése
	A személyes adatoknak a CERT-EU, az IICB és valamennyi uniós intézmény, szerv, hivatal és ügynökség általi, e rendelet alapján történő kezelését az (EU) 2018/1725 európai parlamenti és tanácsi rendelettel összhangban kell végezni.

Módosítás 21

Rendeletre irányuló javaslat
3 cikk – 1 bekezdés – 2 pont

A Bizottság által javasolt szöveg	*Módosítás*
2. „hálózati és információs rendszer”: az irányelv [a NIS 2-javaslat] ***4***. cikkének 1. pontjában ***meghatározott*** hálózati és információs rendszer;	2. „hálózati és információs rendszer”: az irányelv [a NIS 2-javaslat] ***6***. cikkének 1. pontjában ***meghatározottak szerinti*** hálózati és információs rendszer;

Módosítás 22

Rendeletre irányuló javaslat
3 cikk – 1 bekezdés – 4 pont

A Bizottság által javasolt szöveg	*Módosítás*

4. „kiberbiztonság”: az ***irányelv [a NIS*** 2***-javaslat] 4***. cikkének ***3***. ***pontja értelmében vett*** kiberbiztonság;	4. „kiberbiztonság”: az ***(EU) 2019/881 európai parlamenti és tanácsi rendelet[1a]2.***cikkének 1. ***pontjában meghatározott*** kiberbiztonság;
	[1a] 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.).

Módosítás 23

Rendeletre irányuló javaslat
3 cikk – 1 bekezdés – 5 pont

A Bizottság által javasolt szöveg	*Módosítás*
5. „legmagasabb vezetői szint”: vezető személy, vezető vagy koordináló és felügyeleti testület a legmagasabb közigazgatási szinten, figyelembe véve az egyes uniós intézmények, szervek vagy ügynökségek magas szintű irányításának felépítését;	5. „legmagasabb vezetői szint”: ***döntések meghozatalára vagy engedélyezésére vonatkozó felhatalmazással rendelkező*** vezető személy, vezető vagy koordináló és felügyeleti testület a legmagasabb közigazgatási szinten, figyelembe véve az egyes uniós intézmények, szervek***, hivatalok*** vagy ügynökségek magas szintű irányításának felépítését;

Módosítás 24

Rendeletre irányuló javaslat
3 cikk – 1 bekezdés – 7 pont

A Bizottság által javasolt szöveg	*Módosítás*
7. „jelentős biztonsági esemény”: bármely ***váratlan*** esemény, ***kivéve, ha hatása korlátozott, és a módszer vagy technológia tekintetében valószínűleg már jól ismert;***	7. „jelentős biztonsági esemény”: bármely ***olyan*** esemény, ***amely súlyos működési zavart eredményezett, illetve eredményezhet az uniós szervezet működésében***, ***vagy pénzügyi veszteséggel járt, illetve járhat az érintett uniós***

	szervezet számára, ***vagy amely jelentős vagyoni*** vagy ***nem vagyoni kárt okozott vagy okozhat egyéb természetes vagy jogi személyeknek;***

Módosítás 25

Rendeletre irányuló javaslat
3 cikk – 1 bekezdés – 11 pont

A Bizottság által javasolt szöveg	*Módosítás*
11. „jelentős kiberfenyegetés”: ***jelentős biztonsági esemény előidézésére irányuló szándékkal, lehetőséggel és képességgel rendelkező*** kiberfenyegetés;	11. „jelentős kiberfenyegetés”: ***az irányelv [a NIS 2-javaslat] 6. cikkének 11. pontjában meghatározottak szerinti*** kiberfenyegetés;

Módosítás 26

Rendeletre irányuló javaslat
3 cikk – 1 bekezdés – 14 pont

A Bizottság által javasolt szöveg	*Módosítás*
14. ***„kiberbiztonsági kockázat”***: ***minden olyan észszerűen azonosítható körülmény vagy esemény, amely kedvezőtlen hatást gyakorolhat a hálózati és információs rendszerek biztonságára***;	14. ***„kockázat”***: ***az irányelv [a NIS 2-javaslat] 6. cikkének 9. pontjában meghatározott bármilyen kockázat***;

Módosítás 27

Rendeletre irányuló javaslat
3 cikk – 1 bekezdés – 14 a pont (új)

A Bizottság által javasolt szöveg	*Módosítás*
	14a. „IKT-környezet”: az (EU) 2019/881 rendelet 2. cikkének 12., 13. és 14. pontjában meghatározott bármely helyszíni vagy virtuális IKT-termék, IKT-szolgáltatás és IKT-folyamat, valamint bármely hálózati és információs rendszer, függetlenül attól, hogy uniós intézmény, szerv, hivatal vagy ügynökség tulajdonában van-e vagy működteti, vagy

	harmadik fél biztosítja a tárhelyet vagy üzemelteti, beleértve a mobil eszközöket, vállalati hálózatokat és az internethez nem kapcsolódó üzleti hálózatokat, valamint az IKT-környezethez kapcsolódó eszközöket;

Indokolás

A kifejezés átkerült e javaslat 4. cikkének (2) bekezdéséből a fogalommeghatározásokról szóló cikkbe, mivel a szövegben következetesen ezt a kifejezést használják. A kifejezés javasolt meghatározása a kiberbiztonsági jogszabály (az (EU) 2019/881 rendelet) 2. cikkében szereplő elemek fogalommeghatározásain alapul.

Módosítás 28

Rendeletre irányuló javaslat
3 cikk – 1 bekezdés – 15 pont

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

Módosítás 29
Rendeletre irányuló javaslat
4 cikk – 1 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(1) A szervezet küldetésének támogatása érdekében, saját intézményi autonómiáját gyakorolva minden uniós intézmény, szerv és ügynökség létrehozza saját belső kiberbiztonsági kockázatkezelési, -irányítási és -ellenőrzési keretrendszerét (a továbbiakban: keretrendszer). Ezt a munkát a szervezet legmagasabb szintű vezetése felügyeli az összes kiberbiztonsági kockázat hatékony és prudens kezelésének ***biztosítása***	(1) A szervezet küldetésének támogatása érdekében, saját intézményi autonómiáját gyakorolva***, figyelembe véve saját keretének a többi érintett uniós intézmény, szerv, hivatal és ügynökség keretével való koherenciáját és interoperabilitását, teljes körű biztonsági ellenőrzés alapján*** minden uniós intézmény, szerv***, hivatal*** és ügynökség létrehozza saját belső kiberbiztonsági kockázatkezelési, -irányítási és -ellenőrzési

érdekében. E keretrendszert legkésőbb [15 hónappal e rendelet ***hatálybalépését*** követően]-ig be kell vezetni.

keretrendszerét (a továbbiakban: keretrendszer). Ezt a munkát a szervezet legmagasabb szintű vezetése felügyeli**,** ***amely felel*** az összes kiberbiztonsági kockázat hatékony és prudens kezelésének ***biztosításáért***. E keretrendszert legkésőbb [15 hónappal e rendelet ***hatálybalépésének dátumát*** követően]-ig be kell vezetni.

Módosítás 30

Rendeletre irányuló javaslat
4 cikk – 2 bekezdés

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

Módosítás 31
Rendeletre irányuló javaslat
4 cikk – 4 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(4) Minden uniós intézménynek, szervnek és ügynökségnek hatékony mechanizmusokkal kell rendelkeznie annak biztosítására, hogy az ***informatikai költségvetés megfelelő százalékát*** a	(4) Minden uniós intézménynek, szervnek**,** ***hivatalnak*** és ügynökségnek hatékony mechanizmusokkal kell rendelkeznie annak biztosítására, hogy ***középtávon*** az ***összesített IKT-költségvetés***

kiberbiztonságra fordítsák.	***legalább 10%-át*** a kiberbiztonságra fordítsák.

Módosítás 32

Rendeletre irányuló javaslat
4 cikk – 5 a bekezdés (új)

A Bizottság által javasolt szöveg	*Módosítás*
	(5a) A helyi kiberbiztonsági tisztviselő együttműködik az (EU) 2018/1725 rendelet 43. cikkében említett adatvédelmi tisztviselővel az egymást átfedő tevékenységek során, a beépített és alapértelmezett adatvédelmet alkalmazva a kiberbiztonsági intézkedésekre, valamint a személyes adatok védelmét, az integrált kockázatkezelést és a biztonsági események integrált kezelését magukban foglaló kiberbiztonsági intézkedések kiválasztása során.

Módosítás 33

Rendeletre irányuló javaslat
5 cikk – 1 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(1) Az egyes uniós intézmények, szervek és ügynökségek legmagasabb vezetői szintje jóváhagyja a szervezet saját kiberbiztonsági alapkövetelményeit, melyek a 4. cikk (1) bekezdésében említett keretrendszerben azonosított kockázatok kezelésére szolgálnak. Mindezt a szervezet küldetésének támogatása érdekében és a szervezet intézményi ***autonómiájának*** gyakorolva kell végrehajtani. A kiberbiztonsági alapkövetelményeket legkésőbb [18 hónappal e rendelet ***hatálybalépését*** követően]-ig ki kell dolgozni, és a követelményeknek ki kell terjedniük az I. mellékletben felsorolt területekre és a II. mellékletben felsorolt	(1) Az egyes uniós intézmények, szervek***, hivatalok*** és ügynökségek legmagasabb vezetői szintje jóváhagyja a szervezet saját kiberbiztonsági alapkövetelményeit, melyek a 4. cikk (1) bekezdésében említett keretrendszerben azonosított kockázatok kezelésére szolgálnak. Mindezt a szervezet küldetésének támogatása érdekében és a szervezet intézményi ***autonómiáját*** gyakorolva kell végrehajtani***, teljes összhangban e rendelet követelményeivel, figyelembe véve a keretrendszere és az egyéb érintett intézmények, szervek, hivatalok és ügynökségek keretrendszere közötti koherenciát és interoperabilitást,***

intézkedésekre.	***továbbá az IICB által a CERT-EU javaslatára elfogadott iránymutatásokat és ajánlásokat, valamint az alkalmazandó uniós kiberbiztonsági tanúsítási rendszereket***. A kiberbiztonsági alapkövetelményeket legkésőbb [18 hónappal e rendelet ***hatálybalépésének dátumát*** követően]-ig ki kell dolgozni, és a követelményeknek ki kell terjedniük az I. mellékletben felsorolt területekre és a II. mellékletben felsorolt intézkedésekre.

Módosítás 34

Rendeletre irányuló javaslat
5 cikk – 2 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(2) Az egyes uniós intézmények, szervek és ügynökségek felső vezetése rendszeresen képzéseken vesz részt azon ismeretek és készségek elsajátítása érdekében, amelyek a kiberbiztonsági kockázatok és irányítási gyakorlatok, valamint az azok által a szervezet működésére gyakorolt hatások megismeréséhez és értékeléséhez szükségesek.	(2) Az egyes uniós intézmények, szervek***, hivatalok*** és ügynökségek felső vezetése rendszeresen***, megfelelő erőforrással ellátott*** képzéseken vesz részt azon ismeretek és készségek elsajátítása érdekében, amelyek a kiberbiztonsági kockázatok és irányítási gyakorlatok, valamint az azok által a szervezet működésére gyakorolt hatások megismeréséhez és értékeléséhez szükségesek. ***Az ilyen speciális képzések mellett, valamint a kiberbiztonsági kultúra kiépítése és megszilárdítása céljából a kiberbiztonsági tervbe bele kell foglalni a személyzet tagjainak rendszeres kiberbiztonsági képzését, és azt legalább kétévente naprakésszé kell tenni. Elegendő erőforrást kell biztosítani a minőségi képzés biztosításához.***

Módosítás 35

Rendeletre irányuló javaslat
6 cikk – 1 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
Minden uniós intézmény, szerv és ügynökség legalább ***háromévente*** kiberbiztonsági érettségi értékelést végez, amelynek ki kell terjednie ***informatikai környezetük*** 4. cikkben leírt valamennyi elemére, figyelembe véve a 13. cikkel összhangban elfogadott vonatkozó iránymutatásokat és ajánlásokat.	Minden uniós intézmény, szerv***, hivatal*** és ügynökség ***[6 hónappal e rendelet hatálybalépését követően] ...-ig, és azt követően*** legalább ***kétévente*** kiberbiztonsági érettségi értékelést végez, amelynek ki kell terjednie ***IKT-környezetük*** 4. cikkben leírt valamennyi elemére, figyelembe véve a 13. cikkel összhangban elfogadott vonatkozó iránymutatásokat és ajánlásokat. ***Az érettségi értékelés ellenőrzött szolgáltatók által végzett független kiberbiztonsági ellenőrzéseken alapul.***

Módosítás 36

Rendeletre irányuló javaslat
7 cikk – 1 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(1) Az érettségi értékelésből levont következtetéseket követően, valamint a 4. cikk szerint azonosított eszközök és kockázatok figyelembevételével az egyes uniós intézmények, szervek és ügynökségek legmagasabb szintű vezetése a kockázatkezelési, -irányítási és -ellenőrzési keretrendszer, valamint a kiberbiztonsági alapkövetelmények kidolgozását követően indokolatlan késedelem nélkül jóváhagyja a kiberbiztonsági tervet. A terv az érintett szervezet általános kiberbiztonságának növelésére irányul, és ezáltal hozzájárul az összes uniós intézmény, szerv és ügynökség egységesen magas szintű kiberbiztonságának eléréséhez vagy javításához. A szervezet intézményi autonómiájára építve és a szervezet küldetésének támogatása érdekében a tervnek tartalmaznia kell legalább az I. mellékletben felsorolt területeket, a II. mellékletben felsorolt intézkedéseket, valamint a biztonsági eseményekre való	(1) Az érettségi értékelésből levont következtetéseket követően, valamint a 4. cikk szerint azonosított eszközök és kockázatok figyelembevételével az egyes uniós intézmények, szervek***, hivatalok*** és ügynökségek legmagasabb szintű vezetése a kockázatkezelési, -irányítási és -ellenőrzési keretrendszer, valamint a kiberbiztonsági alapkövetelmények kidolgozását követően indokolatlan késedelem nélkül jóváhagyja a kiberbiztonsági tervet. A terv az érintett szervezet általános kiberbiztonságának növelésére irányul, és ezáltal hozzájárul az összes uniós intézmény, szerv***, hivatal*** és ügynökség egységesen magas szintű kiberbiztonságának eléréséhez vagy javításához. A szervezet intézményi autonómiájára építve és a szervezet küldetésének támogatása érdekében a tervnek tartalmaznia kell legalább az I. mellékletben felsorolt területeket, a II. mellékletben felsorolt intézkedéseket, valamint a biztonsági eseményekre való

felkészültséggel, reagálással és helyreállítással kapcsolatos intézkedéseket, például a biztonsági megfigyelést és naplózást. A terv felülvizsgálatára a 6. cikk szerint elvégzett érettségi értékeléseket követően legalább ***háromévente*** kerül sor.	felkészültséggel, reagálással és helyreállítással kapcsolatos intézkedéseket, például a ***szállítók és szolgáltatások*** biztonsági ***értékelését, a*** megfigyelést és ***a*** naplózást. A terv felülvizsgálatára a 6. cikk szerint elvégzett érettségi értékeléseket követően legalább ***kétévente*** kerül sor.

Módosítás 37

Rendeletre irányuló javaslat
7 cikk – 2 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(2) A kiberbiztonsági tervek tartalmaznia kell a személyzet tagjainak a terv végrehajtásával kapcsolatos szerepét és felelősségi körét.	(2) A kiberbiztonsági tervek tartalmaznia kell a személyzet tagjainak a terv végrehajtásával kapcsolatos szerepét***, arra való felkészültségét*** és ***azzal kapcsolatos*** felelősségi körét.

Módosítás 38

Rendeletre irányuló javaslat
7 cikk – 3 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(3) A kiberbiztonsági terv ***figyelembe veszi*** a CERT-EU által kiadott alkalmazandó ***iránymutatásokat*** és ***ajánlásokat***.	(3) A kiberbiztonsági terv ***magában foglalja*** a CERT-EU által kiadott alkalmazandó ***iránymutatásokban*** és ***ajánlásokban szereplő valamennyi javasolt intézkedést***.

Módosítás 39

Rendeletre irányuló javaslat
7 cikk – 3 a bekezdés (új)

A Bizottság által javasolt szöveg	*Módosítás*
	(3a) Az uniós intézmények, szervek, hivatalok és ügynökségek benyújtják kiberbiztonsági terveiket az IICB-nek. Ezeket a terveket a lehető legnagyobb

	mértékben meg kell osztani anélkül, hogy fennállna annak kockázata, hogy az uniós szervezet konkrét technikai kiberbiztonsági intézkedéseire és képességeire vonatkozó érzékeny vagy bizalmas információkat jogosulatlan harmadik felek számára feltárják vagy nyilvánosságra hozzák.

Módosítás 40

Rendeletre irányuló javaslat
9 cikk – 2 bekezdés – a pont

A Bizottság által javasolt szöveg	*Módosítás*
a) e rendelet uniós intézmények, szervek és ügynökségek általi végrehajtásának nyomon követése;	a) e rendelet uniós intézmények, szervek***, hivatalok*** és ügynökségek általi végrehajtásának nyomon követése***, valamint ajánlások megfogalmazása a kiberbiztonság egységesen magas szintjének elérése érdekében***;

Módosítás 41

Rendeletre irányuló javaslat
9 cikk – 3 bekezdés – 1 albekezdés – bevezető rész

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

Módosítás 42

Rendeletre irányuló javaslat
9 cikk – 3 bekezdés – 1 albekezdés – k a pont (új)

A Bizottság által javasolt szöveg	*Módosítás*
	ka) az európai adatvédelmi biztos.

Módosítás 43

Rendeletre irányuló javaslat
10 cikk – 1 bekezdés – a a pont (új)

A Bizottság által javasolt szöveg	*Módosítás*
	aa) a CERT-EU vezetőjének javaslata alapján jóváhagyja a kiberbiztonság egységesen magas szintjének elérésére vonatkozó, egy vagy valamennyi uniós intézményre, szervre, hivatalra és ügynökségre irányuló ajánlásokat;

Módosítás 44

Rendeletre irányuló javaslat
11 cikk – 1 bekezdés – a pont

A Bizottság által javasolt szöveg	*Módosítás*
a) figyelmeztetést ad ki; amennyiben egy jelentős kiberbiztonsági kockázat miatt szükséges, a figyelmeztetés célközönségét megfelelően korlátozza;	a) figyelmeztetést ad ki; amennyiben egy jelentős kiberbiztonsági kockázat miatt szükséges, a figyelmeztetés célközönségét ***egy közösen elfogadott módszertan segítségével*** megfelelően korlátozza;

Módosítás 45

Rendeletre irányuló javaslat
11 cikk – 1 bekezdés – b pont

A Bizottság által javasolt szöveg	*Módosítás*
b) ***javaslatot tesz*** a megfelelő ellenőrzési ***szolgálat számára*** az ellenőrzés elvégzésére.	b) ***utasítja*** a megfelelő ellenőrzési ***szolgálatot*** az ellenőrzés elvégzésére.

Módosítás 46

Rendeletre irányuló javaslat
12 cikk – 1 bekezdés

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

Módosítás 47

Rendeletre irányuló javaslat
12 cikk – 2 bekezdés – d pont

A Bizottság által javasolt szöveg	*Módosítás*
d) felhívja az IICB figyelmét az e rendelet végrehajtásával, valamint az iránymutató dokumentumok, ajánlások és cselekvési felhívások végrehajtásával kapcsolatos bármely kérdésre;	d) felhívja az IICB figyelmét az e rendelet végrehajtásával, valamint az iránymutató dokumentumok, ajánlások és cselekvési felhívások végrehajtásával kapcsolatos bármely kérdésre***, és jogorvoslatra tesz javaslatot***;

Módosítás 48

Rendeletre irányuló javaslat
12 cikk – 4 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(4) A CERT-EU az (EU) 2019/881 európai parlamenti és tanácsi rendelettel összhangban strukturált együttműködést folytat az Európai Uniós Kiberbiztonsági Ügynökséggel a kapacitásépítés, az operatív együttműködés és a kiberfenyegetések hosszú távú stratégiai elemzése terén.	(4) A CERT-EU az (EU) 2019/881 európai parlamenti és tanácsi rendelettel összhangban strukturált együttműködést folytat az Európai Uniós Kiberbiztonsági Ügynökséggel a kapacitásépítés, az operatív együttműködés és a kiberfenyegetések hosszú távú stratégiai elemzése terén. ***Emellett a CERT-EU együttműködhet és információt cserélhet a Kiberbűnözés Elleni Európai Központtal.***

Módosítás 49

Rendeletre irányuló javaslat
12 cikk – 5 bekezdés – bevezető rész

A Bizottság által javasolt szöveg	*Módosítás*
(5) A CERT-EU a szolgáltatáskatalógusában nem szereplő következő szolgáltatásokat (a továbbiakban: díjköteles szolgáltatások) nyújthatja:	(5) A CERT-EU ***az uniós intézményeknek, szerveknek, hivataloknak és ügynökségeknek*** a szolgáltatáskatalógusában nem szereplő következő szolgáltatásokat (a továbbiakban: díjköteles szolgáltatások) nyújthatja:

Módosítás 50

Rendeletre irányuló javaslat
12 cikk – 5 bekezdés – a pont

A Bizottság által javasolt szöveg	*Módosítás*
a) a (2) bekezdésben említettektől eltérő, az uniós intézmények, szervek és ügynökségek ***informatikai környezetének*** kiberbiztonságát támogató szolgáltatások, a szolgáltatási szintre vonatkozó megállapodások alapján és a rendelkezésre álló erőforrások függvényében;	a) a (2) bekezdésben említettektől eltérő, az uniós intézmények, szervek***,*** ***hivatalok*** és ügynökségek ***IKT-környezetének*** kiberbiztonságát támogató szolgáltatások, a szolgáltatási szintre vonatkozó megállapodások alapján és a rendelkezésre álló erőforrások függvényében;

Módosítás 51

Rendeletre irányuló javaslat
12 cikk – 5 bekezdés – b pont

A Bizottság által javasolt szöveg	*Módosítás*
b) olyan szolgáltatások, amelyek írásbeli megállapodások alapján és az IICB előzetes jóváhagyásával támogatják az uniós intézmények, szervek és ügynökségek kiberbiztonsági műveleteit vagy projektjeit, kivéve azokat, amelyek ***informatikai környezetük*** védelmét szolgálják;	b) olyan szolgáltatások, amelyek írásbeli megállapodások alapján és az IICB előzetes jóváhagyásával támogatják az uniós intézmények, szervek***, hivatalok*** és ügynökségek kiberbiztonsági műveleteit vagy projektjeit, kivéve azokat, amelyek ***IKT-környezetük*** védelmét szolgálják;

Módosítás 52
Rendeletre irányuló javaslat
12 cikk – 5 bekezdés – c pont

A Bizottság által javasolt szöveg	*Módosítás*
c) írásbeli megállapodások alapján és az IICB előzetes jóváhagyásával az uniós intézményektől, szervektől és ügynökségektől eltérő olyan szervezetek számára nyújtott, ***informatikai környezetük*** biztonságát támogató szolgáltatások, amelyek szorosan együttműködnek az uniós intézményekkel, szervekkel és ügynökségekkel, például az uniós jog szerinti feladatok vagy felelősségi körök teljesítése révén.	c) írásbeli megállapodások alapján és az IICB előzetes jóváhagyásával az uniós intézményektől, szervektől***, hivataloktól*** és ügynökségektől eltérő olyan szervezetek számára nyújtott, ***IKT-környezetük*** biztonságát támogató szolgáltatások, amelyek szorosan együttműködnek az uniós intézményekkel, szervekkel***,*** ***hivatalokkal*** és ügynökségekkel, például az uniós jog szerinti feladatok vagy felelősségi körök teljesítése révén.

Módosítás 53

Rendeletre irányuló javaslat
12 cikk – 6 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(6) A CERT-EU – adott esetben az Európai Uniós Kiberbiztonsági Ügynökséggel szoros együttműködésben – kiberbiztonsági gyakorlatokat szervezhet	(6) A CERT-EU – adott esetben az Európai Uniós Kiberbiztonsági Ügynökséggel szoros együttműködésben – kiberbiztonsági gyakorlatokat szervezhet

vagy ajánlhatja a meglévő gyakorlatokban való részvételt az uniós intézmények, szervek és ügynökségek kiberbiztonsági szintjének tesztelése céljából.	vagy ajánlhatja a meglévő gyakorlatokban való részvételt az uniós intézmények, szervek***, hivatalok*** és ügynökségek kiberbiztonsági szintjének ***rendszeres*** tesztelése céljából. ***Emellett az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközponttal folytatott megerősített együttműködés és közös programok révén a CERT-EU támogathatja a kutatást és az innovációt, valamint segítheti az uniós intézmények, szervek, hivatalok és ügynökségek kiberbiztonsági képességeinek megerősítését.***

Módosítás 54

Rendeletre irányuló javaslat
12 cikk – 7 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(7) A CERT-EU segítséget ***nyújthat*** az uniós intézményeknek, szerveknek és ügynökségeknek a minősített ***informatikai környezetben*** bekövetkező biztonsági eseményekkel kapcsolatban, amennyiben erre az érintett ***védett szervezet*** kifejezetten ***felkéri***.	(7) A CERT-EU segítséget ***nyújt*** az uniós intézményeknek, szerveknek***, hivataloknak*** és ügynökségeknek a minősített ***IKT-környezetben*** bekövetkező biztonsági eseményekkel kapcsolatban, amennyiben erre az érintett ***uniós intézmények, szervek, hivatalok vagy ügynökségek*** kifejezetten ***felkérik, és amennyiben a CERT-EU rendelkezik az ehhez szükséges erőforrásokkal, vagy ha az érintett szervezettől ilyen erőforrásokat kap***.

Módosítás 55

Rendeletre irányuló javaslat
14 cikk – 1 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
A CERT-EU vezetője ***rendszeresen*** jelentést nyújt be az IICB-nek és az IICB elnökének a CERT-EU teljesítményéről, a pénzügyi tervezésről, a bevételekről, a költségvetés végrehajtásáról, a szolgáltatási	A CERT-EU vezetője ***évente legalább egyszer*** jelentést nyújt be az IICB-nek és az IICB elnökének a CERT-EU teljesítményéről, a pénzügyi tervezésről, a bevételekről, a költségvetés

szintre vonatkozó megállapodásokról és a megkötött írásbeli megállapodásokról, a hasonló szervezetekkel és partnerekkel folytatott együttműködésről, valamint a személyzet által végzett küldetésekről, beleértve a 10. cikk (1) bekezdésében említett jelentéseket is.

végrehajtásáról, a szolgáltatási szintre vonatkozó megállapodásokról és a megkötött írásbeli megállapodásokról, a hasonló szervezetekkel és partnerekkel folytatott együttműködésről, valamint a személyzet által végzett küldetésekről, beleértve a 10. cikk (1) bekezdésében említett jelentéseket is.

Módosítás 56

Rendeletre irányuló javaslat
16 cikk – 1 bekezdés

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

Módosítás 57

Rendeletre irányuló javaslat
16 cikk – 2 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(2) A CERT-EU a hasonló kiberfenyegetések vagy -események felderítésének megkönnyítése érdekében az érintett ***védett szervezet*** beleegyezése nélkül megoszthatja a biztonsági eseményekkel kapcsolatos információkat a tagállami partnerekkel. A CERT-EU csak	(2) A CERT-EU a hasonló kiberfenyegetések vagy -események felderítésének megkönnyítése érdekében az érintett ***uniós intézmények, szervek, hivatalok vagy ügynökségek*** beleegyezése nélkül megoszthatja a biztonsági eseményekkel kapcsolatos információkat a

az érintett ***védett szervezet*** beleegyezésével cserélhet olyan biztonságiesemény-specifikus információkat, amelyek feltárják a kiberbiztonsági esemény célpontját.	tagállami partnerekkel***, amennyiben a személyes adatok kezelése megfelel az (EU) 2018/1725 rendelet alkalmazandó rendelkezéseinek***. A CERT-EU csak az érintett ***uniós intézmények, szervek, hivatalok vagy ügynökségek*** beleegyezésével cserélhet olyan biztonságiesemény-specifikus információkat, amelyek feltárják a kiberbiztonsági esemény célpontját.

Módosítás 58

Rendeletre irányuló javaslat
17 cikk – 1 bekezdés

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

Módosítás 59

Rendeletre irányuló javaslat
17 cikk – 2 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(2) A CERT-EU együttműködhet más partnerekkel, például kereskedelmi szervezetekkel, nemzetközi szervezetekkel, nem európai uniós nemzeti szervezetekkel vagy egyéni szakértőkkel annak érdekében, hogy információkat gyűjtsön az általános	(2) A CERT-EU együttműködhet más partnerekkel, például kereskedelmi szervezetekkel, nemzetközi szervezetekkel, nem európai uniós nemzeti szervezetekkel vagy egyéni szakértőkkel annak érdekében, hogy információkat gyűjtsön az általános

és konkrét kiberfenyegetésekről, sebezhetőségekről és a lehetséges ellenintézkedésekről. Az ilyen partnerekkel való szélesebb körű együttműködéshez a CERT-EU-nak előzetes jóváhagyást kell kérnie az IICB-től.	és konkrét kiberfenyegetésekről, sebezhetőségekről és a lehetséges ellenintézkedésekről. Az ilyen partnerekkel való szélesebb körű együttműködéshez a CERT-EU-nak előzetes jóváhagyást kell kérnie az IICB-től. ***Minden ilyen együttműködésnek tiszteletben kell tartania az EU demokratikus integritását.***

Módosítás 60

Rendeletre irányuló javaslat
17 cikk – 3 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(3) A CERT-EU a biztonsági esemény által érintett ***védett szervezet*** beleegyezésével információkat szolgáltathat a biztonsági eseményről azoknak a partnereknek, akik hozzájárulhatnak annak elemzéséhez.	(3) A CERT-EU a biztonsági esemény által érintett ***uniós intézmények, szervek, hivatalok vagy ügynökségek*** beleegyezésével információkat szolgáltathat a biztonsági eseményről azoknak a partnereknek, akik hozzájárulhatnak annak elemzéséhez.

Módosítás 61

Rendeletre irányuló javaslat
19 cikk – -1 bekezdés (új)

A Bizottság által javasolt szöveg	*Módosítás*
	(-1) Az uniós intézmények, szervek, hivatalok vagy ügynökségek önkéntesen információt szolgáltathatnak a CERT-EU-nak az őket érintő kiberfenyegetésekre, biztonsági eseményekre, majdnem bekövetkezett (near miss) eseményekre és sebezhetőségekre vonatkozóan. A CERT-EU-nak biztosítania kell azt, hogy az uniós szervezetekkel való információmegosztás megkönnyítése érdekében hatékony kommunikációs eszközök álljanak rendelkezésre. A CERT-EU előnyben részesítheti a kötelező bejelentések feldolgozását az önkéntes

bejelentésekkel szemben.

Módosítás 62

Rendeletre irányuló javaslat
19 cikk – 1 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(1) Annak érdekében, hogy ***a CERT-EU koordinálhassa*** a ***sebezhetőségek kezelését és a biztonsági eseményekre való reagálást,*** felkérheti az uniós intézményeket, szerveket és ügynökségeket, hogy ***a CERT-EU támogatása szempontjából releváns információkat szolgáltassanak számára informatikai rendszereik jegyzékéből.*** A ***megkeresett intézmény***, ***szerv vagy ügynökség*** indokolatlan késedelem nélkül továbbítja a kért információt és annak minden későbbi frissítését.	(1) Annak érdekében, hogy ***teljesítse*** a ***12. cikkben meghatározott küldetését és feladatait, a CERT-EU*** felkérheti az uniós intézményeket, szerveket***, hivatalokat*** és ügynökségeket, hogy ***információkat szolgáltassanak számára IKT-rendszereik nyilvántartásaiból, ideértve a kiberfenyegetésekre, a majdnem bekövetkezett (near miss) eseményekre,*** a ***sebezhetőségekre, a fertőzöttségi mutatókra***, ***a kiberbiztonsági figyelmeztetésekre és a kiberbiztonsági események észlelésére szolgáló kiberbiztonsági eszközök konfigurációjára vonatkozó ajánlásokkal kapcsolatos információkat is. A megkeresett szervezet*** indokolatlan késedelem nélkül továbbítja a kért információt és annak minden későbbi frissítését.

Módosítás 63

Rendeletre irányuló javaslat
19 cikk – 2 bekezdés

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

Módosítás 64
Rendeletre irányuló javaslat
20 cikk – cím

A Bizottság által javasolt szöveg	*Módosítás*
Értesítési kötelezettségek	***Jelentéstételi*** kötelezettségek

Módosítás 65

Rendeletre irányuló javaslat
20 cikk – 1 bekezdés – 1 albekezdés

A Bizottság által javasolt szöveg	*Módosítás*
Valamennyi uniós intézmény, szerv és ügynökség indokolatlan késedelem nélkül, de legkésőbb 24 órával azt követően, hogy tudomást szerzett róla, ***kezdeti értesítést nyújt be*** a CERT-EU-nak a jelentős kiberfenyegetésekről, a jelentős sebezhetőségekről és a jelentős biztonsági eseményekről.	Valamennyi uniós intézmény, szerv***, hivatal*** és ügynökség indokolatlan késedelem nélkül, de legkésőbb 24 órával azt követően, hogy tudomást szerzett róla, ***korai előrejelzést ad*** a CERT-EU-nak a jelentős kiberfenyegetésekről, a jelentős sebezhetőségekről és a jelentős biztonsági eseményekről. ***Ez a korai előrejelzés adott esetben jelzi, hogy a jelentős biztonsági eseményt feltehetően jogellenes vagy rosszhiszemű cselekmény okozta-e, és hogy van-e vagy lehet-e határokon átnyúló hatása.***

Módosítás 66

Rendeletre irányuló javaslat
20 cikk – 1 bekezdés – 2 albekezdés

A Bizottság által javasolt szöveg	*Módosítás*
Kellően indokolt esetekben és a CERT-EU-val egyetértésben az érintett uniós intézmény, szerv vagy ügynökség eltérhet ***az előző bekezdésben meghatározott*** határidőtől.	Kellően indokolt esetekben és a CERT-EU-val egyetértésben az érintett uniós intézmény, szerv***, hivatal*** vagy ügynökség eltérhet ***ettől a*** határidőtől.

Módosítás 67

Rendeletre irányuló javaslat
20 cikk – 2 bekezdés – bevezető rész

A Bizottság által javasolt szöveg	*Módosítás*
(2) Az uniós intézmények, szervek és ügynökségek indokolatlan késedelem nélkül ***értesítik*** a ***CERT-EU-t*** a kiberfenyegetések, sebezhetőségek és biztonsági események megfelelő technikai ***részleteiről***, amelyek lehetővé teszik a felderítést, a biztonsági eseményekre való reagálást vagy a kockázatcsökkentő intézkedéseket. Az értesítésnek tartalmaznia kell a következőket, amennyiben rendelkezésre állnak:	(2) Az uniós intézmények, szervek és ügynökségek indokolatlan késedelem nélkül***, de legkésőbb a jelentős biztonsági eseményről való tudomásszerzést követő 72 órán belül értesítést küldenek a CERT-EU-nak, frissítik a korai előrejelzést és kezdeti értékelést nyújtanak be*** a ***jelentős biztonsági eseményről, annak súlyosságáról és hatásáról*** a kiberfenyegetések, sebezhetőségek és biztonsági események megfelelő technikai ***részleteivel együtt***, amelyek lehetővé teszik a felderítést, a biztonsági eseményekre való reagálást vagy a kockázatcsökkentő intézkedéseket. Az értesítésnek tartalmaznia kell a következőket, amennyiben rendelkezésre állnak:

Módosítás 68
Rendeletre irányuló javaslat
20 cikk – 2 bekezdés – 1 a albekezdés (új)

A Bizottság által javasolt szöveg	*Módosítás*
	Kellően indokolt esetekben és a CERT-EU-val egyetértésben az érintett uniós intézmény, szerv, hivatal vagy ügynökség eltérhet ettől a határidőtől.

Módosítás 69

Rendeletre irányuló javaslat
20 cikk – 2 a bekezdés (új)

A Bizottság által javasolt szöveg	*Módosítás*
	(2a) Az uniós intézmények, szervek, hivatalok és ügynökségek legkésőbb a jelentős biztonsági eseményre vonatkozó

	bejelentés benyújtását követő egy hónapon belül zárójelentést nyújtanak be a CERT-EU-nak, amely legalább a következőket tartalmazza:
	a) a jelentős biztonsági eseménynek, súlyosságának és hatásának részletes leírása;
	b) a jelentős biztonsági eseményt valószínűleg kiváltó fenyegetés típusa vagy valószínű kiváltó oka;
	c) az alkalmazott és folyamatban lévő mérséklési intézkedések;
	d) adott esetben a jelentős biztonsági esemény határokon átnyúló hatása.
	Ha a jelentős biztonsági esemény az első albekezdésben említett zárójelentés benyújtásának időpontjában még folyamatban van, ebben az időpontban az elért eredményekről szóló jelentést, a biztonsági eseményt követő egy hónapon belül pedig zárójelentést kell benyújtani.

Módosítás 70

Rendeletre irányuló javaslat
20 cikk – 2 b bekezdés (új)

A Bizottság által javasolt szöveg	*Módosítás*
	(2b) Kellően indokolt esetekben és a CERT-EU-val egyetértésben az érintett uniós intézmény, szerv, hivatal vagy ügynökség eltérhet a (2a) bekezdésben meghatározott határidőtől.

Módosítás 71

Rendeletre irányuló javaslat
20 cikk – 3 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(3) A CERT-EU havonta összefoglaló jelentést nyújt be az ENISA-nak, amely	(3) A CERT-EU havonta összefoglaló jelentést nyújt be az ENISA-nak, amely

anonimizált és összesített adatokat tartalmaz az (1) bekezdéssel összhangban bejelentett jelentős kiberfenyegetésekről, jelentős sebezhetőségekről és jelentős biztonsági eseményekről.	anonimizált és összesített adatokat tartalmaz az (1) bekezdéssel összhangban bejelentett jelentős kiberfenyegetésekről, jelentős sebezhetőségekről és jelentős biztonsági eseményekről. ***Az említett jelentés hozzájárul az uniós kiberbiztonsági helyzetről a [NIS 2-javaslat] irányelv 18. cikkével összhangban kétévente kiadandó jelentéshez.***

Módosítás 72

Rendeletre irányuló javaslat
20 cikk – 4 bekezdés

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

Módosítás 73

Rendeletre irányuló javaslat
20 cikk – 5 bekezdés

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

Módosítás 74

Rendeletre irányuló javaslat
24 cikk – 2 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(2) A Bizottság legkésőbb ***48*** hónappal e rendelet hatálybalépését követően, majd azt követően ***háromévente*** jelentést tesz az Európai Parlamentnek és a Tanácsnak e rendelet végrehajtásáról.	(2) A Bizottság legkésőbb ***36*** hónappal e rendelet hatálybalépését követően, majd azt követően ***kétévente*** jelentést tesz az Európai Parlamentnek és a Tanácsnak e rendelet végrehajtásáról.

Módosítás 75

Rendeletre irányuló javaslat
24 cikk – 3 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(3) A Bizottság legkorábban ***öt*** évvel e rendelet hatálybalépését követően értékeli a rendelet működését, és jelentést tesz az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának.	(3) A Bizottság ***– tekintettel a kiberfenyegetettségek gyorsan változó környezetére –*** legkorábban ***három*** évvel e rendelet hatálybalépését követően értékeli a rendelet működését, és jelentést tesz az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának.

Módosítás 76

Rendeletre irányuló javaslat
I melléklet – 1 bekezdés – bevezető rész

A Bizottság által javasolt szöveg	*Módosítás*
A kiberbiztonsági alapkövetelményeknek a következő területekre kell kiterjedniük:	A kiberbiztonsági alapkövetelményeknek ***legalább*** a következő területekre kell kiterjedniük:

Módosítás 77

Rendeletre irányuló javaslat
I melléklet – 1 bekezdés – 1 a pont (új)

A Bizottság által javasolt szöveg	*Módosítás*
	1a. a személyzet tagjainak kiberbiztonsági képzése;

Módosítás 78

Rendeletre irányuló javaslat
I melléklet – 1 bekezdés – 3 pont

A Bizottság által javasolt szöveg	*Módosítás*
3. ***eszközkezelés***, beleértve az ***informatikai eszközök*** leltárát és az ***informatikai hálózati*** térképeket;	3. ***eszközbeszerzés és -kezelés***, beleértve az ***IKT-eszközök*** leltárát és az ***IKT-hálózati*** térképeket;

Módosítás 79

Rendeletre irányuló javaslat
I melléklet – 1 bekezdés – 7 pont

A Bizottság által javasolt szöveg	*Módosítás*
7. rendszerbeszerzés, -fejlesztés és -karbantartás;	7. rendszerbeszerzés, -fejlesztés és -karbantartás***, beleértve a nyílt forráskódú szoftverek házon belüli fejlesztését is***;

Módosítás 80

Rendeletre irányuló javaslat
I melléklet – 1 bekezdés – 7 a pont (új)

A Bizottság által javasolt szöveg	*Módosítás*
	7a. kiberbiztonsági ellenőrzések;

Módosítás 81

Rendeletre irányuló javaslat
I melléklet – 1 bekezdés – 9 pont

A Bizottság által javasolt szöveg	*Módosítás*
9. a biztonsági események kezelése,	9. a biztonsági események kezelése,

beleértve a biztonsági eseményekre való felkészültség, az azokra való reagálás és az azokat követő helyreállítás javítását célzó megközelítéseket, valamint a CERT-EU-val való együttműködést, például a biztonsági ellenőrzés és naplózás fenntartását;	beleértve a biztonsági eseményekre való felkészültség, az azokra való reagálás és az azokat követő helyreállítás javítását célzó megközelítéseket, ***a jelentéstételi kötelezettségeknek való megfelelést és a határidők lerövidítését,*** valamint a CERT-EU-val való együttműködést, például a biztonsági ellenőrzés és naplózás fenntartását;

Módosítás 82

Rendeletre irányuló javaslat
II melléklet – 1 bekezdés – 3 a pont (új)

A Bizottság által javasolt szöveg	*Módosítás*
	3a. a személyzet tagjainak rendszeres kiberbiztonsági képzése;

Módosítás 83

Rendeletre irányuló javaslat
II melléklet – 1 bekezdés – 4 pont – a pont

A Bizottság által javasolt szöveg	*Módosítás*
a) az ***informatikai szolgáltatók*** biztonsági eseményekkel, sebezhetőségekkel és kiberfenyegetésekkel kapcsolatos információinak a CERT-EU-val való megosztását korlátozó szerződéses akadályok felszámolása;	a) az ***IKT-szolgáltatók*** biztonsági eseményekkel, sebezhetőségekkel és kiberfenyegetésekkel kapcsolatos információinak a CERT-EU-val való megosztását korlátozó szerződéses akadályok felszámolása;

A VÉLEMÉNYNYILVÁNÍTÁSRA FELKÉRT BIZOTTSÁG ELJÁRÁSA

Cím	Az uniós intézmények, szervek, hivatalok és ügynökségek egységesen magas szintű kiberbiztonságát biztosító intézkedések meghatározása
Hivatkozások	COM(2022)0122 – C9-0122/2022 – 2022/0085(COD)
Illetékes bizottság A plenáris ülésen való bejelentés dátuma	ITRE 4.4.2022
Véleményt nyilvánított A plenáris ülésen való bejelentés dátuma	AFCO 4.4.2022
A vélemény előadója A kijelölés dátuma	Markéta Gregorová 20.6.2022
Vizsgálat a bizottságban	26.10.2022 1.12.2022
Az elfogadás dátuma	25.1.2023
A zárószavazás eredménye	+: 24 –: 0 0: 0
A zárószavazáson jelen lévő tagok	Gerolf Annemans, Gabriele Bischoff, Damian Boeselager, Gwendoline Delbos-Corfield, Salvatore De Meo, Daniel Freund, Charles Goerens, Esteban González Pons, Laura Huhtasaari, Victor Negrescu, Max Orville, Domènec Ruiz Devesa, Helmut Scholz, Pedro Silva Pereira, Sven Simon, Guy Verhofstadt, Loránt Vincze, Rainer Wieland
A zárószavazáson jelen lévő póttagok	Nathalie Colin-Oesterlé, Pascal Durand, Seán Kelly, Jaak Madison, Maite Pagazaurtundúa
A zárószavazáson jelen lévő póttagok (209. cikk, (7) bekezdés)	Leszek Miller

A VÉLEMÉNYNYILVÁNÍTÁSRA FELKÉRT BIZOTTSÁG

NÉV SZERINTI ZÁRÓSZAVAZÁSA

24	+
ID	Gerolf Annemans, Laura Huhtasaari, Jaak Madison
PPE	Nathalie Colin-Oesterlé, Salvatore De Meo, Esteban González Pons, Seán Kelly, Sven Simon, Loránt Vincze, Rainer Wieland
Renew	Charles Goerens, Max Orville, Maite Pagazaurtundúa, Guy Verhofstadt
S&D	Gabriele Bischoff, Pascal Durand, Leszek Miller, Victor Negrescu, Domènec Ruiz Devesa, Pedro Silva Pereira
The Left	Helmut Scholz
Verts/ALE	Damian Boeselager, Gwendoline Delbos-Corfield, Daniel Freund

0	-

0	0

Jelmagyarázat:
+ : mellette
- : ellene
0 : tartózkodás