AZ EURÓPAI BIZOTTSÁG VÁLASZAI

AZ EURÓPAI SZÁMVEVŐSZÉK KÜLÖNJELENTÉSÉRE

Az uniós intézmények, szervek és ügynökségek kiberbiztonsága: a felkészültség szintje nem áll arányban a fenyegetésekkel

HU

HU

Tartalom

Ez a dokumentum az Európai Bizottság által a költségvetési rendelet 259. cikkével összhangban az Európai Számvevőszék különjelentésében foglalt észrevételekre adott válaszokat mutatja be, amelyeket a különjelentéssel együtt kell közzétenni.

I. A BIZOTTSÁG VÁLASZAI RÖVIDEN

a) Általános bevezetés

A kiberbiztonság az Európai Bizottság egyik legfontosabb politikai és operatív prioritásává vált. A Covid-válság fokozta a digitális szolgáltatásoktól (felhőalapú számítástechnika, mobileszközök, mesterséges intelligencia) való függőségünket. Az elmúlt két évben jelentős elmozdulás történt az otthoni munkavégzés felé. Ez azt jelenti, hogy mind a kiberbűnözés, mind a kiberkémkedés – az Európai Unió intézményeit, szerveit és ügynökségeit érintő két fő fenyegetés – szintén jelentős mértékben terjedtek el az interneten. A Bizottság felismeri ezt a tendenciát. Következetes és határozott vezető szerepet tölt be a kiberbiztonság terén. A kiberbiztonsági jogszabály 2019-ben lépett hatályba, és többek között kibővítette és állandóvá tette az ENISA megbízatását. Ez a jogi aktus hivatalos együttműködést is létrehozott az ENISA és a CERT-EU (az európai intézmények, szervek és hivatalok számítógépes vészhelyzeteket elhárító csoportja) között. 2020-ban a Bizottság javaslatot tett a hálózat- és információbiztonságról szóló irányelv megerősítésére, amelynek a jogalkotók általi elfogadása a közeljövőben esedékes.

A 2020. évi kiberbiztonsági stratégia három olyan intézkedést is tartalmazott, amelyek az uniós intézmények, szervek és ügynökségek kiberbiztonságával kapcsolatosak. Bejelentette az uniós intézmények, szervek és ügynökségek információbiztonságáról szóló rendeletet, az uniós intézményekre, szervekre és ügynökségekre vonatkozó közös kiberbiztonsági szabályokról szóló rendeletet, valamint azon szándékát, hogy új jogalapot biztosítson a CERT-EU számára, hogy megerősítse megbízatását és finanszírozását annak érdekében, hogy a növekvő fenyegetések, kockázatok és biztonsági események kezelése érdekében biztosítsa a megfelelő erőforrásokat.

Az e javaslatok előkészítésével kapcsolatos munka jól halad. Bár e javaslatokat a biztosi testület még nem fogadta el, erre várhatóan 2022 első negyedévében sor kerül. Ebben az előkészítő szakaszban az intézmények között megvitatott fontos kérdések a javaslat jogalapját, valamint az összes uniós intézmény, szerv és ügynökség azon költségvetési kapacitását érintik, hogy mind saját kiberbiztonsági szükségleteik finanszírozása, mind pedig a CERT-EU, a költségvetés és különösen az álláshelyek támogatásához szükséges források megtalálása tekintetében megfeleljenek a követelményeknek.

Az uniós intézmények, szervek és ügynökségek kiberbiztonsági felkészültségi szintje eltérő fejlettségű. Számos uniós intézmény, szerv és ügynökség jelentős teljesítményt nyújt a kiberbiztonsági felkészültség terén, és továbbra is vezető szerepet kell betölteniük, ösztönözve és inspirálva az előrelépést és a további javulást a teljes kiberbiztonsági környezetben. A mérhető haladás elérése érdekében fontos elismerni, hogy az uniós intézmények, szervek és ügynökségek eltérő fejlettségi szintet érnek el, és prioritásokat kell meghatározni azáltal, hogy a javító intézkedéseket elsősorban azon uniós intézmények, szervek és ügynökségek felé irányítják, ahol az azonosított hiányosságok a legmagasabb kockázati kitettséget eredményezik.

b) A Bizottság álláspontja a Számvevőszék legfontosabb észrevételeiről és ajánlásairól

A Bizottság üdvözli a Számvevőszék jelentését az uniós intézmények, szervek és ügynökségek kiberbiztonságáról. Tudomásul veszi, hogy a jelentés hangsúlyozza annak fontosságát, hogy valamennyi uniós intézmény, szerv és ügynökség számára közös jogi keretek álljanak rendelkezésre

az információbiztonsággal és a kiberbiztonsággal kapcsolatban a kiberbiztonság általános szintjének növelése érdekében. A Bizottság megjegyzi, hogy a Számvevőszék fő észrevételei és ajánlásai nem a Bizottság saját operatív kiberbiztonságára irányulnak, hanem a Bizottság szakpolitikai szerepére az uniós intézmények, szervek és ügynökségek kiberbiztonsági fejlettségének növelésére irányuló jogalkotási javaslatok előterjesztésében.

Az uniós intézmények, szervek és ügynökségek információbiztonságáról szóló jövőbeli rendeletek és az uniós intézményekre, szervekre és ügynökségekre vonatkozó közös kiberbiztonsági szabályok közös szabályokat fognak meghatározni az információbiztonság és a kiberbiztonság magas szintjének elérése érdekében, de végrehajtásuk az egyes uniós intézmények, szervek és ügynökségek szervezeti és működési keretein (különösen azok fenyegetettségi és kockázati profilján) belül továbbra is az uniós intézmények, szervek és ügynökségek önálló hatáskörébe tartozik. A kiberbiztonságról szóló javasolt rendelet olyan megfelelési mechanizmusokat fog tartalmazni, amelyek megfelelőek és arányosak az új szabályok célkitűzésével és hatályával, az intézmények, szervek és ügynökségek autonómiájának sérelme nélkül.

A Bizottság jelenleg a digitális transzformációval foglalkozó intézményközi bizottság (ICDT) kiberbiztonsági alcsoportjának elnöki tisztét tölti be, amely rotációs rendszerű (legfeljebb két évre szól). Meg kell jegyezni, hogy nem különítettek el forrásokat az alcsoport munkájához: valamennyi intézkedés a résztvevők önkéntes alapon tett erőfeszítésein alapul.

A Bizottság egyetért azzal az általános elképzeléssel, hogy meg kell erősíteni a CERT-EU erőforrásait és megbízatását.

Ennek jegyében a Bizottság támogatja a jelentés főbb megállapításait és ajánlásait. Részletes álláspontunkat a III. szakasz kiegészítő megjegyzéseiben fejtjük ki. Az ajánlások tekintetében a Bizottság elfogadja az 1. ajánlás a), b), c), d), e), f) és g) pontját, valamint a 2. ajánlás a), b) és c) pontját.

c) A vonatkozó legújabb fejlemények és a következő lépések

Az uniós intézmények, szervek és ügynökségek főigazgatóinak szintjén lezárult a két rendelet (információbiztonság, kiberbiztonság) egységes szerkezetbe foglalt tervezetéről folytatott hivatalos konzultáció, és folyamatban van a kapott visszajelzések értékelése, mielőtt a csomag elkészülne, és a biztosi testület 2022 első negyedévében elfogadná azt.

II. A BIZOTTSÁG VÁLASZAI A SZÁMVEVŐSZÉK FŐBB ÉSZREVÉTELEIRE

1. Az uniós intézmények, szervek és ügynökségek kiberbiztonsági fejlettségi szintje

A Bizottság egyetért azzal, hogy az uniós intézmények, szervek és ügynökségek által a kiberbiztonságra fordított kiadások szintjének megfigyelésekor fontos figyelembe venni a fenyegetéseket és a kockázatokat.

Hasonlóképpen, ami az emberi erőforrásokat illeti, az uniós intézmények, szervek és ügynökségek személyi állományának stabilitását számos tényező befolyásolja. A szakosodott kiberbiztonsági szakértők toborzásának piaca egyre összetettebb. Az emberi erőforrásokra vonatkozó szabályok sok esetben nem igazodnak a speciális profilokhoz (felvétel, szakmai előmenetel, képzés). Ezen túlmenően a költségvetési hatóság által az uniós intézményekre, szervekre és ügynökségekre a személyzeti állomány létszáma tekintetében gyakorolt általános nyomás azt jelenti, hogy az újonnan megjelenő, kiemelt fontosságú területeken, például a kiberbiztonság terén továbbra is túl kevés az álláshely, különösen a belső operatív szolgálatoknál.

Az irányítás és a kockázatkezelés terén elért haladásra való hivatkozásnak figyelembe kell vennie azt a tényt, hogy a megfelelés nyomon követése jelenleg a kísérleti szakaszból a teljes körű bevezetés felé mozdul el. Ezért normális, hogy a lefedettség eddig meglehetősen alacsony volt. Ez a megfelelési projekt egy hosszú távú, a kiberbiztonság fejlettségének javítására irányuló folyamat következő szakasza, amely a közös kockázati módszertan meghatározásával, a közös eszköztár kialakításával, a sebezhetőségkezelés bevezetésével, valamint az eszközök leltárának nyomon követésével, tesztelésével és validálásával kezdődött. A Bizottság eszközalapjának összetettsége ellenére előrelépés történt ezen a hosszú pályán, mivel több mint 50 főigazgatóság és végrehajtó ügynökség több mint 1 000 információs rendszert működtet.

2. Az uniós intézmények, szervek és ügynökségek együttműködési mechanizmusai

A CERT-EU olyan jelentős sikertörténet, amely nemcsak az uniós intézmények, szervek és ügynökségek közötti, hanem európai szinten is előmozdítja az együttműködést azáltal, hogy teljes jogú tagként részt vesz a kiberbiztonsági irányelv alapján létrehozott CSIRT-hálózatban. Ily módon a CERT-EU példaértékű eset arra, hogy miként lehet fokozni az együttműködést és a kiberbiztonsági szolgáltatásokat. A Számvevőszék CERT-EU-val kapcsolatos észrevételei nagyon világosan szemléltetik a CERT-EU által az egyre ellenségesebb kiberfenyegetések és a tartós forráshiány közepette végzett kiemelkedő munkát.

Ezen intézményközi megállapodás értelmében az uniós decentralizált ügynökségeket és közös vállalkozásokat hivatalosan az ENISA képviseli a CERT-EU irányítóbizottságában. Ezen túlmenően az irányítóbizottság ülésein az IKT tanácsadó bizottság (ICTAC) képviselője fejti ki nézeteiket, aki az ügynökségeket képviselő szerepében részt vehet az ENISA-nak való segítségnyújtásban, de nem rendelkezik hivatalos képviselői hellyel vagy szavazati joggal. Az ügynökségek CERT-EU irányítóbizottságban való megfelelő képviseletének kérdésével a javasolt rendelet foglalkozik majd azáltal, hogy az uniós ügynökségek hálózata (EUAN) által kijelölt legfeljebb három képviselővel egészíti ki az irányítóbizottság összetételét, az IKT tanácsadó bizottságának javaslata alapján.

Az ICDT kiberbiztonsággal foglalkozó alcsoportjában való részvétel a legnagyobb gondosság elve alapján, az egyes uniós intézmények, szervek és ügynökségek által meghatározott szerepvállalási szinten történik. Az új kiberbiztonsági keretszerződés előkészítése során jelenleg foglalkoznak a közbeszerzéssel kapcsolatos információmegosztás javításával, amely a kiberbiztonsággal foglalkozó alcsoport 2. munkacsoportjának egyik fontos témája.

Ami az olyan szolgáltatásokhoz kapcsolódó közös eszköztárat illeti, mint az e-mail és a videokonferencia, a Bizottság által valamennyi uniós intézmény, szerv és ügynökség esetében alkalmazott SECEM-2 rendszer már használható a titkosított e-mailekhez, a titkosítási kulcsok és tanúsítványok hatékony kezelésétől függően. Ehhez járul még a SECABC, az e-mailek intézmények

közötti titkosítását lehetővé tevő eszköz fejlesztése, azzal a szándékkal, hogy 2022-től minden érdeklődő uniós intézmény, szerv és ügynökség számára hozzáférést biztosítsanak. A nem minősített érzékeny adatokkal kapcsolatos szolgáltatások esetében már megvalósult a biztonságos videokonferencia, és az eseti alapon más uniós intézményekre, szervekre és ügynökségekre is kiterjeszthető az ülésen részt vevők személyazonosságának kezelésével. Az érzékeny információk megosztásával az információbiztonságról szóló rendeletjavaslat is foglalkozik majd (pl. közös címkézés és jelölések révén).

3. A jelentős eseményekre vagy sebezhetőségekre vonatkozó információk megosztása

A NIS-2 irányelvben foglalt bizottsági javaslattal összhangban a kiberbiztonsági rendelettervezet foglalkozik azzal a ténnyel, hogy nem minden uniós intézmény, szerv és ügynökség értesíti a CERT-EU-t a jelentős eseményekről vagy sebezhetőségekről[1]. A végrehajtás szintje az önálló uniós intézmények, szervek és ügynökségek által erre szánt többletforrásoktól függ. Az ilyen értesítések végrehajtásának hatóköre továbbra is korlátozott, többek között a javasolt rendelet szerinti jelenlegi tervek szerint, az uniós intézmények, szervek és ügynökségek intézményi autonómiája miatt. A kiberbiztonságról szóló javasolt rendelet olyan megfelelési mechanizmusokat fog tartalmazni, amelyek megfelelőek és arányosak az új szabályok célkitűzésével és hatályával, az intézmények, szervek és ügynökségek autonómiájának sérelme nélkül.

III. A BIZOTTSÁG VÁLASZAI A SZÁMVEVŐSZÉK KÖVETKEZTETÉSEIRE ÉS AJÁNLÁSAIRA

1. ajánlás – Az uniós szervek kiberfelkészültségének fejlesztése közös szabványok útján

A rendelet javasolt szövege olyan konkrét intézkedéseket tartalmaz majd, amelyek célja a kiberbiztonság közös szintjének további növelése. Az említett intézkedéseket kiberbiztonsági tervekbe fogják átültetni, amelyeket az uniós intézmények, szervek és ügynökségek szintjén határoznak meg és hajtanak végre saját kiberbiztonsági irányítási keretüknek megfelelően.

A Bizottság elfogadja ezt az ajánlást. Az ajánlások konkrét pontjaival kapcsolatban a Bizottság a következőket állapítja meg:

a) A Bizottság elfogadja az 1. ajánlás a) pontját. A rendelettervezet rendelkezéseket fog tartalmazni az egyes uniós intézmények, szervek és ügynökségek felsővezetésének szintjén létrehozott irányítási és kontrollkeretekre vonatkozóan, az összes kiberbiztonsági kockázat hatékony és prudens kezelésének biztosítása érdekében.

[1] Javaslat – Az Európai Parlament és a Tanács irányelve az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről, COM(2020) 823 final.

b) A Bizottság elfogadja az 1. ajánlás b) pontját. A rendelettervezet megerősíti a kiberbiztonság kezelésére vonatkozó kockázatalapú megközelítés megemlítését azáltal, hogy egyértelművé teszi, hogy az értékeléseket az intézkedéseknek, az informatikai biztonsági terveknek és az alapvető ellenőrzések tényleges végrehajtásának kell követnie.

c) A Bizottság elfogadja az 1. ajánlás c) pontját. A kiberbiztonsági oktatási, tájékoztatási és képzési programokat a kiberbiztonsági alapkövetelmények részeként említik a rendelettervezetben.

d) A Bizottság elfogadja az 1. ajánlás d) pontját. Tapasztalataink szerint, bár a rendszeres ellenőrzések és tesztelések alapvető fontosságúak, ezek nem elegendőek az előrehaladás biztosításához. Ezért az a) pontban szereplő kiberbiztonsági irányítási keret részeként rendszeres jelentéstételre és átláthatóságra van szükség.

e) A Bizottság elfogadja az 1. ajánlás e) pontját. A rendelettervezet rendelkezéseket fog tartalmazni a jelentős kiberfenyegetéseknek, sebezhetőségeknek és biztonsági eseményeknek a CERT-EU-nak történő, az uniós intézmények, szervek és ügynökségek általi bejelentésére vonatkozóan.

f) A Bizottság elfogadja az 1. ajánlás f) pontját. A Bizottság támogatja a CERT-EU forrásainak megerősítését. A rendelettervezet szövege tartalmazni fogja az uniós intézményektől, szervektől és ügynökségektől származó személyzeti és pénzügyi hozzájárulásokkal kapcsolatos rendelkezéseket.

g) A Bizottság elfogadja az 1. ajánlás g) pontját. A javasolt rendelet olyan megfelelési mechanizmusokat fog tartalmazni, amelyek arányosak a rendelkezések célkitűzésével és hatályával, és tiszteletben tartják az uniós intézmények, szervek és ügynökségek intézményi autonómiáját. A jövőbeli rendelet tartalma a jogalkotási eljárás eredményétől függ, és az uniós jogalkotó által a Bizottság javaslatával kapcsolatban hozott határozat eredménye.

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

A Bizottság, amely jelenleg a digitális átalakulással foglalkozó intézményközi bizottság (ICDT) kiberbiztonsági alcsoportjának elnöki tisztét tölti be, egyetért azokkal az ajánlásokkal, amelyek az érzékeny információk következetes és biztonságos megosztására, a kiberbiztonsági projektekre vonatkozó információk szisztematikus megosztására, valamint a kiberbiztonsági szolgáltatásokkal kapcsolatos közös közbeszerzési keretekre és szerződésekre vonatkozó megoldások előmozdítására irányulnak.

A Bizottság elfogadja ezt az ajánlást. Az ajánlások konkrét pontjaival kapcsolatban a Bizottság a következőket állapítja meg:

a) A Bizottság elfogadja a 2. ajánlás a) pontját. A Bizottság technikai kezdeményezéseket és szolgáltatásokat vezet be az ICDT kiberbiztonsági alcsoportjában annak érdekében, hogy előmozdítsa és támogassa az érzékeny információk megosztására szolgáló közös eszköztárat, lehetővé téve az olyan szolgáltatásokat, mint az e-mail és a videokonferencia. Megjegyezzük továbbá, hogy az információbiztonságról szóló rendeletjavaslat foglalkozni fog a nem minősített érzékeny adatok közös jelöléseivel és közös kezelési szabályaival.

b) A Bizottság elfogadja a 2. ajánlás b) pontját. Az ICDT kiberbiztonsági alcsoportján belül működő munkacsoportok foglalkoznak ezzel a ponttal, és azt tovább fogják fejleszteni. Az új kiberbiztonsági keretszerződés előkészítése során foglalkoznak a közbeszerzéssel kapcsolatos információmegosztás javításával.

c) A Bizottság elfogadja a 2. ajánlás c) pontját. Az uniós intézmények, szervek és ügynökségek már most is hozzáférnek a Bizottság által kezelt, az IKT területére vonatkozó intézményközi keretszerződésekhez. Az új kiberbiztonsági keretszerződés előkészítését összehangolják az ICDT kiberbiztonsági alcsoportjával.

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

Ennek az ajánlásnak a CERT-EU és az ENISA a címzettje.