Az Európai Unió
Tanácsa

Brüsszel, 2026. január 22.
(OR. en)

Intézményközi referenciaszámok:
2026/0011 (COD)
2026/0012 (COD)

5611/26
ADD 2

CYBER 29
JAI 85
DATAPROTECT 22
TELECOM 29
MI 58
IND 48
CADREFIN 26
FIN 100
BUDGET 3
CODEC 90

FEDŐLAP

Küldi:	az Európai Bizottság főtitkára részéről Martine DEPREZ igazgató
Az átvétel dátuma:	2026. január 21.
Címzett:	Thérèse BLANCHET, az Európai Unió Tanácsának főtitkára
Biz. dok. sz.:	SWD(2026) 12 final
Tárgy:	BIZOTTSÁGI SZOLGÁLATI MUNKADOKUMENTUM A HATÁSVIZSGÁLATI JELENTÉS VEZETŐI ÖSSZEFOGLALÓJA amely a következő dokumentumot kíséri Javaslat – Az Európai Parlament és a Tanács rendelete az Európai Uniós Kiberbiztonsági Ügynökségről (ENISA), az európai kiberbiztonsági tanúsítási keretrendszerről és az IKT-ellátási lánc biztonságáról, valamint az (EU) 2019/881 rendelet hatályon kívül helyezéséről (2. kiberbiztonsági jogszabály) valamint Javaslat – Az Európai Parlament és a Tanács irányelve az (EU) 2022/2555 irányelvnek az egyszerűsítési intézkedések és [a 2. kiberbiztonsági jogszabályra irányuló javaslattal] való összehangolás tekintetében történő módosításáról

Mellékelten továbbítjuk a delegációknak a következő dokumentumot: SWD(2026) 12 final.

Melléklet: SWD(2026) 12 final

EURÓPAI
BIZOTTSÁG

Strasbourg, 2026.1.20.
SWD(2026) 12 final

BIZOTTSÁGI SZOLGÁLATI MUNKADOKUMENTUM

A HATÁSVIZSGÁLATI JELENTÉS VEZETŐI ÖSSZEFOGLALÓJA

amely a következő dokumentumot kíséri

Javaslat – Az Európai Parlament és a Tanács rendelete az Európai Uniós Kiberbiztonsági Ügynökségről (ENISA), az európai kiberbiztonsági tanúsítási keretrendszerről és az IKT-ellátási lánc biztonságáról, valamint az (EU) 2019/881 rendelet hatályon kívül helyezéséről (2. kiberbiztonsági jogszabály)

valamint

Javaslat – Az Európai Parlament és a Tanács irányelve az (EU) 2022/2555 irányelvnek az egyszerűsítési intézkedések és [a 2. kiberbiztonsági jogszabályra irányuló javaslattal] való összehangolás tekintetében történő módosításáról

{COM(2026) 11 final} - {SEC(2026) 11 final} - {SWD(2026) 11 final}

A hatásvizsgálat összefoglalója

Célkitűzés

E hatásvizsgálat elsődleges célja annak értékelése, hogy a jelenlegi szabályozások megfelelőek-e a folyamatosan változó kiberbiztonsági fenyegetések Unió-szerte történő kezeléséhez. Integrált szakpolitikai alternatívákat javasol, amelyek célja az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) megerősítése, az európai kiberbiztonsági tanúsítási keretrendszer reformja, valamint a hatályos kiberbiztonsági jogszabályi keretnek való megfelelés egyszerűsítése. Ez az értékelés hangsúlyozza a kiberbiztonsági irányítás finomhangolásának fontosságát a technológiai fejlődéssel és a piaci igényekkel való harmonizáció érdekében, a versenyképesség biztosítása és a környezeti hatások figyelembevétele mellett.

A probléma ismertetése

A meglévő erőfeszítések ellenére, az egyre összetettebb fenyegetésekkel összefüggésben az EU kiberbiztonsági környezete továbbra is jelentős kihívásokkal szembesül. A tagállamok és más uniós szintű szereplők közötti elégtelen koordináció, a szakpolitikai eszközök végrehajtásának elakadása, valamint a szabályozás által jelentett akadályok és a szabályozás összetettsége akadályozzák a kiberbiztonság hatékony kezelését. Ezek a problémák magasabb költségeket eredményeznek a vállalkozások és a hatóságok számára, növelik a kiberbiztonsági incidensek kockázatát, és a védelem nem következetes szintjét biztosítják a polgárok számára.

Az uniós fellépés indokolása

A kiberbiztonsági fenyegetések túlmutatnak a nemzeti határokon, ezért a határozott reagáláshoz elengedhetetlen az egységes megközelítés. Az uniós szintű beavatkozás következetes védelmet biztosít, egyenlő versenyfeltételek biztosítása révén fokozza a versenyképességet, valamint megkönnyíti a digitális szolgáltatások és termékek szabad mozgását az európai egységes piacon belül. Az uniós szintű harmonizáció továbbá az egyszerűsített megfelelési követelmények és az észszerűbbé tett eljárások révén az adminisztratív terheket is csökkenti.

Szakpolitikai alternatívák és az előnyben részesített alternatíva

Ez a jelentés négy beavatkozási területet elemzését tartalmazza, amelyek mindegyike az elérendő konkrét célkitűzésekre tekintettel mérlegelt szakpolitikai alternatívákat foglal magában: 1. az ENISA megbízatása (amely egyúttal a jelenleg hatályos kiberbiztonsági jogszabálynak is a részét képezi), 2. az európai kiberbiztonsági tanúsítási keretrendszer (amely szintén részét képezi a jelenleg hatályos kiberbiztonsági jogszabálynak), és 3. a NIS 2 irányelv célzott módosításai, valamint az egyszerűsítés mint cél megfogalmazása, amely ugyanakkor kölcsönösen összekapcsolódik az ENISA megbízatásával és az európai kiberbiztonsági tanúsítási keretrendszerrel is. Ezen alternatívák mindegyike önmagában is beavatkozást igénylő terület, ugyanakkor kölcsönösen összefüggenek és kapcsolódnak egymáshoz.

Lehetőségek az uniós kiberbiztonsági szakpolitikai keret és az érdekelt felek igényei közötti összhang hiányának kezelésére az egyre ellenségesebbé váló környezetben

A.1. alternatíva: *Az ENISA megbízatásának pontosítása és a prioritások meghatározása* – Ez az alternatíva a más jogszabályokban meghatározott feladatok beépítése révén egyértelmű és stabil keretet biztosítana az ENISA feladatai tekintetében.

A.2. alternatíva: *Az ENISA megbízatásának reformja* – Ez az alternatíva hatályon kívül helyezné és felváltaná a kiberbiztonsági jogszabályt, és az Ügynökség megbízatásának teljes átalakítását jelentené.

A.3. alternatíva: *Az ENISA megbízatásának reformja az operatív támogatásra való erőteljes összpontosítással* – Ez az alternatíva az A.2. alternatívára építene. Emellett az ENISA a tagállamok kérésére olyan képességeket fejlesztene ki, amelyek közvetlenül támogatnák a NIS 2 irányelv hatálya alá tartozó szervezeteket a kiberbiztonsági incidensekre való reagálásban és az azt követő helyreállításban.

Az európai kiberbiztonsági tanúsítási keretrendszerrel kapcsolatos alternatívák

B.1. alternatíva: *Az európai kiberbiztonsági tanúsítási keretrendszer hatályának, elemeinek és célkitűzéseinek pontosítása, valamint egy karbantartási mechanizmus bevezetése* – Ez az alternatíva új karbantartási mechanizmust ír elő az egyes rendszerek tekintetében, amelyet azok elfogadását követően az ENISA-nak kell elvégeznie.

B.2. alternatíva: *Az európai kiberbiztonsági tanúsítási keretrendszer reformja eljárásainak felülvizsgálata és hatályának kiterjesztése révén, a szabályozásnak való megfelelés egyszerűsítésének előmozdítása érdekében* – E szerint az alternatíva szerint a kiberbiztonsági jogszabályt hatályon kívül helyeznék, és egy új rendelettel váltanák fel. A B.1. alternatíva mellett a rendszerek kérelmezésére, kifejlesztésére és elfogadására vonatkozó eljárást is módosítanák az elszámoltathatóság javítása és a hatékonyság növelése érdekében.

B.3. alternatíva: *Az európai kiberbiztonsági tanúsítási keretrendszernek a B.2. alternatíva szerint előirányzott reformja, valamint a kiberbiztonsági helyzet kötelező tanúsításának bevezetése* – Ez az alternatíva a B.2. alternatívára építene, de célja a keret hatásának további erősítése azáltal, hogy a NIS 2 irányelv hatálya alá tartozó alapvető szervezetek számára – konkrét kockázati forgatókönyvek mérlegelése alapján – kötelező tanúsítást vezetne be ahelyett, hogy kizárólag a szervezetek önkéntes tanúsítására támaszkodna.

Egyszerűsítéssel kapcsolatos alternatívák

C.1. alternatíva: *„Puha” jogi és nem jogalkotási eszközökön alapuló megközelítés alkalmazása, beleértve a meglévő felhatalmazások alkalmazását (végrehajtási jogi aktusok elfogadása a NIS 2 irányelv 21. cikkének (5) bekezdése és 23. cikkének (11) bekezdése alapján)* – Ez az alternatíva végrehajtási jogi aktusok elfogadását irányozza elő a NIS 2 irányelv szerinti, meglévő felhatalmazások alapján a kiberbiztonsági kockázatkezelési intézkedések, az incidensek bejelentésére vonatkozó küszöbértékek, valamint az értesítésekre vonatkozó információk, formátumok és eljárások nagyobb fokú harmonizációjának biztosítása

érdekében, valamint iránymutatások elfogadását a jogbiztonság elmélyítése és a fokozottabban harmonizált végrehajtás érdekében.

C.2. alternatíva: *Célzott beavatkozás – a vonatkozó uniós kiberbiztonsági jogszabályi keretnek való megfelelés további egyszerűsítése* – Ez az alternatíva korlátozott beavatkozást foglal magában a kiberbiztonsági jogszabály és a NIS 2 irányelv módosítása révén, amelynek célja a kiberbiztonsági keret egyes konkrét vonatkozásainak egyszerűsítése, beleértve a hatály kiigazítását, a végrehajtási jogi aktusok maximális mértékű harmonizációját, a megfelelés tanúsítás révén történő igazolását és a C.1. alternatíva szerint előirányzott iránymutatások elfogadását.

C.3. alternatíva: *Az uniós jogszabályokban a kiberbiztonsággal kapcsolatban meghatározott intézkedések harmonizációja* – Ez az alternatíva a C.2. alternatívára építve eltávolítana minden olyan, a kiberbiztonsági kockázatok kezelésére vonatkozó intézkedést, illetve felhatalmazást, amely az ágazati jogszabályokban már szerepel. Ehelyett a NIS 2 irányelv ökoszisztémáját módosítaná annak érdekében, hogy valamennyi típusú szervezetre vonatkozóan észszerűbb követelmények kerüljenek előírásra, ezáltal biztosítva a nagyobb fokú harmonizációt.

Az IKT-ellátási lánc biztonságával kapcsolatos alternatívák

D.1. alternatíva: *„Puha" jogi megközelítés alkalmazása az IKT-ellátási láncokat érintő kiberbiztonsági kockázatok kezelésére* – Ez az alternatíva nem írna elő uniós szintű szabályozási beavatkozást. Ehelyett a Bizottság növelné az összehangolt kockázatértékelések és az önkéntes eszköztárak számát.

D.2. alternatíva: *Ad hoc szabályozási beavatkozás az 5G eszköztár kodifikálására* – Ez az alternatíva kodifikálná az 5G eszköztárhoz kapcsolódó intézkedéseket. Kötelezővé tenné a tagállamok számára annak biztosítását, hogy magas kockázatú beszállítóktól származó összetevőket nem használnak fel a hálózat kulcsfontosságú eszközeiben.

D.3. alternatíva: *Átfogó és horizontális keret az IKT-ellátási láncokat érintő kiberbiztonsági kockázatok kezelésére* – Ez az alternatíva horizontális, technológiai és ágazatsemleges szabályozási keretet hozna létre az IKT-ellátási láncokat érintő nem technikai kiberbiztonsági kockázatok kezelésére.

Kiterjedt elemzéseket követően az előnyben részesített szakpolitikai csomag a következőket foglalja magában: A.2. alternatíva –Az ENISA megbízatásának reformja; B.2. alternatíva – Az európai kiberbiztonsági tanúsítási keretrendszer reformja az eljárás felülvizsgálata és a hatály kiterjesztése révén, a szabályozásnak való megfelelés egyszerűsítésének előmozdítása érdekében, valamint a C.2. alternatíva – Célzott beavatkozás – a vonatkozó uniós kiberbiztonsági jogszabályi keretnek való megfelelés további egyszerűsítése, továbbá a D.3. alternatíva – Átfogó és horizontális keret az IKT-ellátási láncok kiberbiztonsági kockázatainak kezelésére.

Ez a kombináció kiegyensúlyozott választ kínál az azonosított szakpolitikai kihívásokra, jelentősen növelve az eredményességet, a hatékonyságot és a koherenciát az egész EU-ban.

Fő hatások

Költség-haszon elemzés: A javasolt szabályozási keretre való átállás költségekkel fog járni mind az ENISA számára, amelyek esetében az új feladatok ellátásával kapcsolatban a becslések szerint öt év alatt legfeljebb 161,3 millió EUR összeget fognak kitenni, mind pedig EU-szerte a hatóságok számára, az általuk végzett felügyeleti tevékenységekre öt év alatt legfeljebb 80 millió EUR összeget kitéve (figyelembe véve a releváns költségmegtakarításokat). Ami a vállalkozásokat illeti, egy hároméves átmeneti időszak alatt bizonyos magas kockázatú berendezések fokozatos kivezetése 3,4–4,3 milliárd EUR éves költséget eredményezhet a mobilhálózat-üzemeltetők számára, míg a megbízható szolgáltatókba történő beruházások egyidejűleg akár évi 2 milliárd EUR-val is növekedhetnek. Emellett az észszerűsített és csökkentett megfelelési kötelezettségek várhatóan akár 14,6 milliárd EUR költségmegtakarítást is eredményezhetnek a vállalkozások számára. Ezenfelül a polgárok, a hatóságok és a vállalkozások számára jelentős előnyök származnának az EU általános kiberbiztonsági helyzetének és technológiai szuverenitásának javításából, valamint az innováció és a versenyképesség ösztönzéséből, amelyek hosszú távon várhatóan nagyrészt ellensúlyozzák a kezdeti kiadásokat.

Versenyképesség: Az előnyben részesített alternatívák a piac széttagoltságának csökkentése és a szabályozás harmonizációja révén Unió-szerte fokozzák a versenyképes egyenlőséget, és egyértelműbb pályákat biztosítanak a vállalkozások számára a megfeleléshez és az innovációhoz.

Az éghajlatvédelmi következetesség ellenőrzése: Az értékelés során figyelembe vettük az egyes alternatívák lehetséges környezeti hatásait. Különös figyelmet fordítottunk az energiahatékonyságra, az utazással kapcsolatos kibocsátásokra és az infrastruktúra egységesítésére. Az előnyben részesített A.2., B.2. és C.2. alternatíva korlátozott környezeti hatással jár, míg a D.3. alternatíva környezeti semlegességet biztosít, figyelembe véve a termékek életciklusát és a kulcsfontosságú eszközök helyettesítéséhez szükséges átmeneti időszakokat. Ez összhangban van az EU fenntarthatóság iránti elkötelezettségével.

Alapértelmezésben digitális: A digitális folyamatok észszerűsítésének középpontba helyezése azt mutatja, hogy az EU elkötelezett a digitális megoldásokat priorizáló megközelítés mellett, amely gyorsabb és megbízhatóbb adatcserét és döntéshozatalt biztosít. A D.3. alternatíva jelentős hatást gyakorolhat a digitalizációra is, mivel a kiberbiztonsági aggályokat felvető harmadik országokban letelepedett vagy ilyen harmadik országbeli szervezetek által ellenőrzött szervezetektől származó alkotóelemek lecserélésével járna.

Egyszerűsítés és tehercsökkentés: Az előnyben részesített alternatívák a hatály pontosítása, valamint a megfelelés és a felügyelet észszerűsítésére és az adminisztratív terhek csökkentésére irányuló intézkedések bevezetése révén járulnak hozzá az egyszerűsítéshez. Az „egy be, egy ki” elvet annak biztosítása révén veszik figyelembe, hogy az új kötelezettségeket máshol bevezetett csökkentések ellensúlyozzák.

Összefoglalás

Ez a hatásvizsgálat az EU kiberbiztonságának megerősítésére, a szabályozással kapcsolatos hatékonysági problémák kezelésére és a digitális környezetnek a jövőbeli kihívásokra való felkészítésére irányuló átfogó stratégiát ismerteti. Együttműködésen alapuló és koherens megközelítést javasol, amely a szakpolitikai reformokat a meglévő keretekre alapozza, miközben alkalmazkodik az új technológiai realitásokhoz. Az EU ezen intézkedések révén kíván reziliens, versenyképes és fenntartható digitális gazdaságot biztosítani.