Az Európai Unió
Tanácsa

Brüsszel, 2022. március 22.
(OR. en)

**7474/22**
**ADD 3**

**Intézményközi referenciaszám:**
**2022/0085(COD)**

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

**FEDŐLAP**

| | |
|---|---|
| Küldi: | az Európai Bizottság főtitkára részéről Martine DEPREZ igazgató |
| Az átvétel dátuma: | 2022. március 22. |
| Címzett: | Jeppe TRANHOLM-MIKKELSEN, az Európai Unió Tanácsának főtitkára |
| Biz. dok. sz.: | SWD(2022) 68 final |
| Tárgy: | BIZOTTSÁGI SZOLGÁLATI MUNKADOKUMENTUM A HATÁSVIZSGÁLATI JELENTÉS ÖSSZEFOGLALÓJA amely a következő dokumentumot kíséri Javaslat – AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE az uniós intézmények, szervek, hivatalok és ügynökségek egységesen magas szintű kiberbiztonságát biztosító intézkedések meghatározásáról |

Mellékelten továbbítjuk a delegációknak a SWD(2022) 68 final számú dokumentumot.

Melléklet: SWD(2022) 68 final

EURÓPAI
BIZOTTSÁG

Brüsszel, 2022.3.22.
SWD(2022) 68 final

# BIZOTTSÁGI SZOLGÁLATI MUNKADOKUMENTUM

# A HATÁSVIZSGÁLATI JELENTÉS ÖSSZEFOGLALÓJA

***amely a következő dokumentumot kíséri***

**Javaslat**
**AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE**

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

{COM(2022) 122 final} - {SWD(2022) 67 final}

## 1. Bevezetés

2020-ban megugrott az uniós intézményeket, szerveket és ügynökségeket érintő, fejlett, folyamatos fenyegetést (APT, advanced persistent threat) jelentő szereplők által okozott jelentős biztonsági események száma. Ezt tükrözi a CERT-EU által 2020-ban elemzett kriminalisztikai képek száma is, amely 2019-hez képest megháromszorozódott, míg a jelentős biztonsági események száma 2018 óta több mint tízszeresére nőtt.

Az uniós intézmények, szervek és ügynökségek kiberbiztonsági képességei és informatikai biztonsági kiadásai azonban egyes esetekben szembetűnően egyenlőtlenek, ami a kiberbiztonsági érettségi szintek széles skálájának kialakulásához vezetettaz uniós intézmények, szervek és ügynökségek között. Emellett a fenyegetettségi helyzet elemzése és az informatikai biztonsági eseményekre vonatkozó statisztikák azt mutatják, hogy az uniós intézmények, szervek és ügynökségek kiberbiztonsági kitettsége csak fokozódik.

## 2. Célkitűzések

A feltárt hiányosságok végső soron az uniós intézmények, szervek és ügynökségek nem megfelelő szintű kiberrezilienciájához, az informatikai biztonsági erőforrások széttagoltságához és kiegyensúlyozatlan informatikai biztonsági helyzethez vezetnek.

A jogalkotási aktus célja az uniós intézmények, szervek és ügynökségek egységesen magas szintű kiberbiztonságát biztosító intézkedések előírása. Ez elősegítené és biztosítaná, hogy a kiberbiztonság érettségi szintje lépést tartson az uniós intézmények, szervek és ügynökségek felgyorsuló digitalizációjával.

## 3. Intézményközi Kiberbiztonsági Testület és kiberbiztonsági keretrendszer

Az Intézményközi Kiberbiztonsági Testületre és a kiberbiztonsági keretrendszerre irányuló javaslat olyan intézkedéseket vezet be az uniós intézmények, szervek és ügynökségek egységesen magas szintű kiberbiztonsága érdekében, amelyek lehetővé teszik egy olyan kerethez való igazodást, amely kezeli az összes uniós intézmény, szerv és ügynökség kiberbiztonsági fenyegetéseit, és bevezeti a nyomon követést és az intézményközi kiberbiztonsági testületnek való jelentéstételt.

A javaslat korszerűsíti a CERT-EU küldetését és feladatait, és figyelembe veszi az intézmények, szervek és ügynökségek elmúlt években bekövetkezett, megváltozott és fokozott digitalizálását, valamint a kiberbiztonsági fenyegetések változó helyzetét.

A tagállamokra vagy az uniós polgárokra nézve nincsenek közvetlen hatások vagy költségvetési vonzatok.

E rendeletjavaslat jogalapja az Európai Unió működéséről szóló szerződés 298. cikke, amely előírja, hogy feladataik ellátása során az Unió intézményei, szervei, hivatalai és ügynökségei nyitott, hatékony és független európai igazgatásra támaszkodnak.

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

## 4. Következtetés

Az Intézményközi Kiberbiztonsági Testület és a kiberbiztonsági keretrendszer létrehozása más alternatívákkal összehasonlítva eredményes, hatékony és más uniós szakpolitikákkal koherens módon valósítja meg a kitűzött célok többségét, az érdekelt felek legszélesebb körű támogatásával. Ez a választott alternatíva a legéletképesebb megoldás, tekintettel azokra a

jogi korlátokra, amelyek mellett a fellépést meg kell valósítani, továbbá tekintettel arra, hogy az „egyenmegoldásra” irányuló megközelítés nem felelne meg az uniós intézmények, szervek és ügynökségek jelenlegi heterogén érettségi szintjének, valamint a technológiai kockázatok és összetettség terén fennálló különbségeknek.