Az Európai Unió
Tanácsa

Brüsszel, 2022. március 22.
(OR. en)

Intézményközi referenciaszám:
2022/0085(COD)

7474/22
ADD 1

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

JAVASLAT

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.:	COM(2022) 122 final - Annexes
Tárgy:	MELLÉKLETEK a következőhöz: 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 COM(2022) 122 final számú dokumentum mellékleteit.

Melléklet: COM(2022) 122 final - Annexes

EURÓPAI
BIZOTTSÁG

Brüsszel, 2022.3.22.
COM(2022) 122 final

ANNEXES 1 to 2

MELLÉKLETEK

a következőhöz:

Javaslat
AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE

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

{SWD(2022) 67 final} - {SWD(2022) 68 final}

I. MELLÉKLET

A kiberbiztonsági alapkövetelményeknek a következő területekre kell kiterjedniük:

1. kiberbiztonsági politika, beleértve a hálózati és információs rendszerek biztonságára vonatkozó célkitűzéseket és prioritásokat, különös tekintettel a ([NIS 2-irányelvre vonatkozó javaslat] 4. cikkének 19. pontja szerinti) felhőszolgáltatások használatára és a távmunkát lehetővé tevő műszaki intézkedésekre;
2. a kiberbiztonság szervezete, beleértve a szerepek és feladatkörök meghatározását;
3. eszközkezelés, beleértve az informatikai eszközök leltárát és az informatikai hálózati térképeket;
4. a hozzáférés szabályozása;
5. üzembiztonság;
6. kommunikációs biztonság;
7. rendszerbeszerzés, -fejlesztés és -karbantartás;
8. kapcsolat a beszállítókkal;
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;
10. üzletmenetfolytonosság-menedzsment és válságkezelés; és
11. kiberbiztonsági oktatási, figyelemfelkeltő és képzési programok.

II. MELLÉKLET

Az uniós intézményeknek, szerveknek és ügynökségeknek a kiberbiztonsági alapkövetelmények végrehajtása során és kiberbiztonsági terveikben az IICB útmutató dokumentumaival és ajánlásaival összhangban legalább a következő konkrét kiberbiztonsági intézkedésekkel kell foglalkozniuk:

1. konkrét lépések a „zero trust architektúra” felé történő elmozdulás érdekében (ideértve a biztonsági modellt, a rendszertervezési elveket, valamint egy összehangolt kiberbiztonsági és rendszerirányítási stratégiát, amely annak elismerésén alapul, hogy a hagyományos hálózatok határain belül és kívül egyaránt számolni kell fenyegetésekkel);
2. a többtényezős hitelesítés mint norma elfogadása a hálózati és információs rendszerekben;
3. a szoftverellátási lánc biztonságának megteremtése a biztonságos szoftverfejlesztésre és -értékelésre vonatkozó kritériumok révén;
4. a közbeszerzési szabályok javítása a kiberbiztonság egységesen magas szintjének elősegítése érdekében a következők révén:
   a) az informatikai szolgáltatók biztonsági eseményekkel, sebezhetőségekkel és kiberfenyegetésekkel kapcsolatos információinak a CERT-EU-val való megosztását korlátozó szerződéses akadályok felszámolása;
   b) a biztonsági események, sebezhetőségek és kiberfenyegetések bejelentésére, valamint a biztonsági események megfelelő kezelésére és nyomon követésére vonatkozó szerződéses kötelezettség.