Az Európai Unió
Tanácsa

Brüsszel, 2019. március 20.
(OR. en)

7737/19

CYBER 101	**RELEX 287**
COPEN 118	**TELECOM 141**
COPS 92	**DAPIX 109**
COSI 52	**CATS 43**
DATAPROTECT 98	**CSC 111**
IND 102	**CSCI 47**
JAI 313	**IA 106**
JAIEX 44	**EJUSTICE 44**
POLMIL 31	

AZ ELJÁRÁS EREDMÉNYE

Küldi:	a Tanács Főtitkársága
Dátum:	2019. március 19.
Címzett:	a delegációk
Előző dok. sz.:	6866/19
Tárgy:	A Tanács következtetései az uniós kiberbiztonsági kapacitás és képességek megerősítéséről

Mellékelten továbbítjuk a delegációknak az uniós kiberbiztonsági kapacitás és képességek megerősítéséről szóló tanácsi következtetéseket, amelyeket az Általános Ügyek Tanácsa a 2019. március 19-i ülésén elfogadott.

MELLÉKLET

A Tanács következtetései az uniós kiberbiztonsági kapacitás és képességek megerősítéséről

Az Európai Unió Tanácsa,

1. EMLÉKEZTETVE az „Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése” című közös közleményről szóló következtetéseire[1];

2. EMLÉKEZTETVE a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt uniós reagálásról szóló következtetéseire[2];

3. EMLÉKEZTETVE a külső kiberkapacitás-építésről szóló következtetéseire[3];

4. ÚJÓLAG HANGSÚLYOZVA, hogy a hálózati és információs rendszerek biztonságának magas szintjét a tagállamok, továbbá az uniós intézmények, ügynökségek és szervek kiberbiztonsági kapacitásainak és képességeinek fokozása, majd kiberrezilienciájuk ezt követő megerősítése révén lehet biztosítani;

5. ÜDVÖZÖLVE a tagállamok által elért eredményeket a számítógép-biztonsági eseményekre reagáló csoportok (CSIRT) megerősítése terén;

6. ELISMERÉSÉT KIFEJEZVE annak kapcsán, hogy a tagállamok munkájának, valamint a Bizottság és az ENISA aktív támogatásának eredményeképp kiépült a CSIRT-hálózat, továbbá hogy erősödött az a stratégiai együttműködés, amely a tagállamok, a Bizottság és az ENISA részvételével működő Kiberbiztonsági Együttműködési Csoport keretében zajlik;

---

1 14435/17 (A Tanács következtetései az „Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése” című, az Európai Parlamenthez és a Tanácshoz intézett közös közleményről, 2017. november 20.).

2 10086/18 (A Tanács következtetései a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt uniós reagálásról, 2018. június 26.).

3 10496/18 (A Tanács következtetései a külső kiberkapacitás-építésre vonatkozó uniós iránymutatásokról, 2018. június 26.).

7. HANGSÚLYOZVA, hogy a Kiberbiztonsági Együttműködési Csoportnak meghatározó szerepe van egyrészt az annak biztosításához szükséges iránymutatás nyújtásában, hogy a kiberbiztonsági irányelv[4] átültetése során az EU egészében a lehető legnagyobb mértékben összehangolt megközelítés érvényesüljön, másrészt pedig a releváns kiberbiztonsági problémák kezelésében;

8. ELISMERVE a jelenlegi támogatást, amelyet a Bizottság az Európai Hálózatfinanszírozási Eszközön keresztül nyújt a tagállamok számára a számítógép-biztonsági eseményekre reagáló csoportok kapacitásépítéséhez;

9. ELISMERVE a Belső Biztonsági Alapon és a CEPOL-on keresztül a bűnüldöző hatóságok részére nyújtott támogatást a kiberbűnözés elleni küzdelemre irányuló kapacitásépítéshez;

10. ÜDVÖZÖLVE az uniós kibervédelmi szakpolitikai keret naprakésszé tételét, amely további támogatást irányoz elő a tagállamok kibervédelmi képességeinek fejlesztéséhez;

11. NAGYRA ÉRTÉKELVE a kiberbiztonsági irányelv végrehajtása terén a tagállamok által elért eredményeket;

12. MEGÁLLAPÍTVA, hogy a kiberbiztonság összetett, egyéb területekkel összefonódó és folyamatosan változó terület, amely szükségessé teszi a politikai és jogi keret hozzáigazítását az új technológiai trendekhez és az olyan kialakulóban lévő technológiákhoz, mint például a mesterséges intelligencia, a blokklánc vagy a kvantuminformatika;

---

[4] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (HL L 194., 2016.7.19., 1. o.).

13. HANGSÚLYOZVA, hogy a kiberbiztonsággal kapcsolatos oktatási és képzési programoknak, valamint a biztonsági fenyegetések témájában a végfelhasználókat célzó tájékoztatásnak, illetve figyelemfelhívásnak meghatározó szerepe van a kiberbiztonsági kockázatok csökkentésében;

14. KIEMELVE, hogy a kiberbiztonsági gyakorlatok hatékony eszközei a nagyszabású kiberbiztonsági eseményekkel és válsághelyzetekkel szembeni uniós és tagállami felkészültség szintjének értékelésében és további javításában;

15. ÚJÓLAG HANGSÚLYOZVA, hogy a kibertérben nincsenek határok, amiből az következik, hogy a kiberkapacitás-építési tevékenységek és kezdeményezések vonatkozásában a határokon átnyúló és az ágazatokon átívelő dimenzió és együttműködés megingathatatlan alapelv;

16. NYOMATÉKOSÍTVA a közszektor, a magánszektor és a tudományos világ közötti, különösen együttműködési projektek révén megvalósuló együttműködés fontosságát;

17. NYOMATÉKOSÍTVA a polgári-katonai együttműködés fontosságát, amely a kiberkérdésekkel kapcsolatos közös célok elérésére irányul, a kiberfenyegetésekre való koherens és hatékony reagálás érdekében;

18. NYUGTÁZZA, hogy a tagállamok egy csoportja a kiberterületet érintő kölcsönös segítségnyújtáson alapuló önkéntes együttműködés elmélyítése céljából előrelépést tett a kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportok létrehozása terén;

19. ÜDVÖZLI a Tanácsban folyó megbeszéléseket az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a nemzeti koordinációs központok hálózatának létrehozásáról szóló európai parlamenti és tanácsi rendeletre irányuló bizottsági javaslatról;

20. SZORGALMAZZA a Kiberbiztonsági Együttműködési Csoport munkájában való aktív részvételt, különösen a kiberkapacitás-építés tekintetében;

21. ÖSZTÖNZI a Kiberbiztonsági Együttműködési Csoportban a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt uniós reagálással kapcsolatban végzett, folyamatban lévő munkát;

22. FELKÉRI a tagállamokat, hogy nemzeti kiberbiztonsági stratégiájukra építve, az ágazatspecifikus követelményeket figyelembe véve általánosságban érvényesítsék a kiberbiztonság szempontját;

23. FELKÉRI a tagállamokat, hogy folyamatosan kövessék nyomon, értékeljék/vizsgálják meg a kiberreziliencia, valamint a kiberbiztonsági kapacitás és képességek megerősítése céljából hozott nemzeti intézkedések hatását;

24. FELKÉRI a tagállamokat, hogy az oktatás valamennyi szintjén (alapfokú, középfokú és felsőoktatás, egész életen át tartó tanulás) érvényesítsék a kiberbiztonság és a digitális jártasság szempontját a tantervekben, adott esetben meglévő és jövőbeli munkakörök tükrében;

25. FELKÉRI a tagállamokat, hogy indítsanak a közszférában dolgozókat célzó, a nagyközönség és a végfelhasználók kiberbiztonsággal és kiberhigiéniával kapcsolatos tudatosságának növelésére irányuló kezdeményezéseket;

26. ÖSZTÖNZI a tagállamokat, hogy végezzenek nemzeti szintű kiberbiztonsági gyakorlatokat és uniós szinten is vezessenek ilyen gyakorlatokat, illetve vegyenek részt bennük, egyrészt a stratégiai és technológiai szempontok tesztelése és az azokkal kapcsolatos képzés céljából, másrészt pedig a szükséges készségek hatékony és gyakorlati szempontú fejlesztése érdekében;

27. FELKÉRI a tagállamokat, hogy fejlesszék tovább a számítógép-biztonsági eseményekre reagáló csoportok kiberbiztonsággal kapcsolatos technikai és operatív képességeit a kiberbiztonsági események megelőzése, hatásaik mérséklése és a reagálás területén;

28. FELSZÓLÍTJA a Bizottságot és az ENISA-t, hogy továbbra is támogassák a CSIRT-hálózat kapacitásainak és képességeinek tagállamok általi fejlesztését az együttműködés javítása, a kiberbiztonsági eseményekkel kapcsolatos információcsere hatékonyabbá tétele, valamint a nagy léptékű, határokon átnyúló kiberbiztonsági eseményekre való hatékony reagálás lehetővé tétele érdekében;

29. FELKÉRI a tagállamokat, hogy az illetékes európai hatóságokkal koordinálva továbbra is nyújtsanak segítséget a bűnüldöző hatóságoknak a konkrét kompetenciák fejlesztéséhez annak érdekében, hogy uniós szinten hatékonyan lehessen fellépni a kiberbűnözés ellen;

30. FELKÉRI a tagállamokat, hogy növeljék a kiberkapacitás-építésbe való beruházásokat;

31. FELHÍVJA a Bizottságot és az ENISA-t, hogy indítsanak az uniós intézmények, ügynökségek és szervek alkalmazottait célzó, a kiberbiztonsággal kapcsolatos tudatosság növelésére irányuló programokat és képzéseket;

32. FELSZÓLÍTJA az EU-t és tagállamait, hogy információcserével és a bevált gyakorlatok megosztásával önkéntes alapon járuljanak hozzá a nemzeti és uniós szintű fő kiberkapacitás-építési igények meghatározásához és kezeléséhez;

33. FELKÉRI az EU-t és tagállamait, hogy támogassák a kiberbiztonság területére vonatkozó kutatást és érvényesítsék a kiberbiztonság szempontját az egyéb tanulmányi területeken, egyetlen átfogó egészben összefogva a kiberbiztonságra irányuló különféle kutatási és fejlesztési ágakat és ösztönözve a kiválóságot a kiberbiztonsági kutatás terén;

34. FELKÉRI az EU-t és tagállamait, hogy fejlesszék tovább a kiberbiztonsági kutatást oly módon, hogy az társadalmi szükségletekre adjon választ, és eredményei beépüljenek a piacba;

35. FELSZÓLÍTJA az EU-t és tagállamait, hogy az ikt-vel kapcsolatos közbeszerzési felhívásokban adott esetben vegyék figyelembe a kiberbiztonság szempontját.