



Az Európai Unió
Tanácsa

Brüsszel, 2020. december 2.
(OR. en)

13629/20

CYBER 263
TELECOM 248
COPEN 362
CODEC 1266
COPS 441
COSI 235
CSC 344
CSCI 86
IND 248
RECH 493
SPACE 77

AZ ELJÁRÁS EREDMÉNYE

Küldi:	a Tanács Főtitkársága
Dátum:	2020. december 2.
Címzett:	a delegációk
Tárgy:	A Tanács következtetései a csatlakoztatott eszközök kiberbiztonságáról – Írásbeli eljárás keretében jóváhagyott tanácsi következtetések

Mellékelten továbbítjuk a delegációknak a csatlakoztatott eszközök kiberbiztonságáról szóló, a Tanács által 2020. december 2-án írásbeli eljárás keretében jóváhagyott tanácsi következtetéseket.

A Tanács következtetései a csatlakoztatott eszközök kiberbiztonságáról

Az Európai Unió Tanácsa,

EMLÉKEZTETVE

- az „Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése” című, az Európai Parlamenthez és a Tanácshoz intézett közös közleményről szóló tanácsi következtetésekre,
 - az uniós kiberbiztonsági kapacitás és képességek megerősítéséről szóló tanácsi következtetésekre,
 - „Az 5G jelentősége az európai gazdaság számára és az 5G-hez kapcsolódó biztonsági kockázatok enyhítésének szükségessége” című tanácsi következtetésekre,
 - a nagymértékben digitalizált Európa jövőjéről 2020 után: „A digitális és gazdasági versenyképesség fokozása Unió-szerte és a digitális kohézió” című tanácsi következtetésekre,
 - az Európa digitális jövőjének alakításáról szóló tanácsi következtetésekre,
 - a Covid19-ről, az egységes piacról, az iparpolitikáról, a digitális vonatkozásokról és a külkapcsolatokról szóló európai tanácsi következtetésekre,
 - az Európai Bizottság Európa digitális jövőjének megtervezéséről szóló közleményére,
1. KIEMELI, hogy az Európai Uniónak és tagállamainak a nyitott gazdaság megőrzésével együtt biztosítaniuk kell digitális szuverenitásukat és stratégiai autonómiájukat. Ez magában foglalja azon képesség megerősítését, hogy autonóm technológiai döntéseket hozzanak, az egyik fő pillérként pedig reziliens és biztonságos infrastruktúrákat, termékeket és szolgáltatásokat hozzanak létre annak érdekében, hogy bizalom alakuljon ki a digitális egységes piac iránt és az európai társadalmon belül. Az Európai Unió alapvető értékei védik különösen a magánéletet, a biztonságot, az egyenlőséget, az emberi méltóságot, a jogállamiságot és a nyílt internetet, amelyek a digitális dimenzió által vezérelt, emberközpontú társadalom, gazdaság és ipar megvalósításának előfeltételei;

2. ELISMERI, hogy a csatlakoztatott eszközöknek – többek között a dolgok internetét alkotó gépeknek, érzékelőknek és hálózatoknak – és azok biztonságának egyre nagyobb a jelentősége. A csatlakoztatott eszközök ipari és üzleti szempontból kulcsfontosságú szerepet fognak játszani Európa digitális jövőjének további alakításában, valamint az újgenerációs technológiák fogyasztóinak mindennapi életében. Az 5G-n kívül a mesterséges intelligencia, a kvantum-számítástechnika, a nagy teljesítményű számítástechnika, a felhőalapú számítástechnika, a megosztott főkönyvi technológiák, nevezetesen a blokklánc és minden olyan egyéb új alkalmazás és lehetőség, amely támogatja a fenntartható gazdasági növekedést és társadalmunk magasabb szintű digitalizációját, csak kiberbiztonsági szempontból megbízható csatlakoztatott eszközökkel valósítható meg;
3. NYUGTÁZZA, hogy az internetre csatlakoztatott fogyasztási cikkek és ipari eszközök megnövekedett használata a magánéletre, valamint az információ- és kiberbiztonságra nézve szintén új kockázatokat fog keletkeztetni, ideértve azt is, hogy egyre több potenciális hatás érheti a termékek és az adatok integritását és elérhetőségét, ami közvetlenül érintheti a biztonságot. A fogyasztók védelme, Európa általános kiberrezilienciájának megerősítése, valamint a polgárok digitális megoldásokba és technológiákba vetett bizalmának növelése érdekében alapvető fontosságú az ilyen kockázatok minimálisra csökkentése. Ez elő fogja mozdítani a szóban forgó eszközök európai szolgáltatóinak versenyképességét és innovációs képességeit is. A kiberbiztonságot és a magánélet tiszteletben tartását alapvető követelményként kell elismerni a termékinnovációban, a gyártási és a fejlesztési folyamatokban, beleértve a tervezési szakaszt is (beépített biztonság), és azokat a termékek teljes életciklusa és ellátási lánc során biztosítani kell;
4. HANGSÚLYOZZA, hogy a csatlakoztatott eszközök magas szintű biztonságának biztosítása mellett ugyanilyen fontos növelni a fogyasztók azzal kapcsolatos tudatosságát, hogy a magánélet védelme és a biztonság terén milyen esetleges kockázatoknak vannak kitéve. Ez segítene abban, hogy a minimálisra csökkenjenek a csatlakoztatott eszközök megnövekedett használatából eredő veszélyek, nőjön a digitális egységes piacba vetett bizalom, és a lehető legjobban ki lehessen használni a csatlakoztatott eszközökkel kapcsolatos technológiák kínálta gazdasági és társadalmi előnyöket;

5. KIEMELI, hogy a kutatásba és innovációba – különösen az Európai horizont és a Digitális Európa program keretében – történő közberuházások, valamint a magánberuházások értékes ösztönzőket teremthetnek ahhoz, hogy a csatlakoztatott eszközök biztonságosabbá és védettebbé, az intelligens kommunikációs hálózatok pedig ezáltal reziliensebbé váljanak. Az ipari és digitális vezető szerep elérése, valamint a stratégiai autonómia biztosítása érdekében, a nyitott gazdaság megőrzésével együtt fel kell gyorsítani a csatlakoztatott eszközökkel kapcsolatos legújabb technológiák alkalmazásához szükséges digitális infrastruktúrába és technológiába történő beruházásokat is;
6. HANGSÚLYOZZA, hogy biztosítani kell a digitális egységes piac számos különböző ágazatában használt IKT-rendszerek és IKT-komponensek biztonsági funkcióinak nagy fokú komplementaritását és összehasonlíthatóságát;
7. MÉLTÁNYOLJA a csatlakoztatott eszközök kiberbiztonsági szintjének növelésére irányuló jelenlegi uniós szintű fejleményeket, különös tekintettel a Bizottság azon közelmúltbeli kezdeményezéseire, amelyek a vonatkozó jogi aktusokban, például az új jogszabályi keretbe tartozó jogi aktusokban, különösen a 2014/53/EU irányelvben (a rádióberendezésekről szóló irányelv) a kiberbiztonsági vonatkozások rövid távú kezelését szolgálják.
HANGSÚLYOZZA, hogy fontos felmérni, hogy hosszú távon szükség van-e a nélkülözhetetlen forgalomba hozatali feltételek meghatározására is kiterjedő horizontális jogszabályra annak érdekében, hogy szabályozva legyen a csatlakoztatott eszközök összes releváns kiberbiztonsági szempontja, például az elérhetőség, az integritás és a bizalmas jelleg. ÜDVÖZLI e tekintetben azt a megbeszélést, amelynek keretében feltérképezik majd az említett jogszabály hatályát és a kiberbiztonsági jogszabályban meghatározott kiberbiztonsági tanúsítási keretrendszerrel való kapcsolatait abból a célból, hogy növelni lehessen a biztonság szintjét a digitális egységes piacon;
8. HANGSÚLYOZZA, hogy a kiberbiztonsági követelményeket a vonatkozó uniós jogszabályokkal, többek között a kiberbiztonsági jogszabállyal, az új jogszabályi kerettel, az európai szabványosításról szóló rendelettel és egy esetleges jövőbeli horizontális jogszabállyal összhangban kell meghatározni annak érdekében, hogy biztosítani lehessen az egyértelmű és egységes jogi szabályozást;

9. TISZTÁBAN VAN azzal, hogy valamennyi érdekelt fél – különösen a gyártók – fontos szerepet játszanak abban, hogy a csatlakoztatott eszközök kiberbiztonsági szintjét növelni lehessen a digitális egységes piacon, ezért koordinációt és szoros együttműködést SZORGALMAZ valamennyi érintett köz- és magánszférabeli érdekelt féllel, tekintettel az esetleges jövőbeli horizontális jogszabályra is;
- 9a. ÜDVÖZLI az ENISA vezetésével jelenleg folyó munkát, amely az első uniós kiberbiztonsági tanúsítási rendszerek – nevezetesen a javasolt európai uniós közös kritériumok és a javasolt felhőszolgáltatási rendszerek – kidolgozására irányul. E rendszerek releváns alapként szolgálnak majd a csatlakoztatott eszközök tanúsításához;
10. HANGSÚLYOZZA, hogy a csatlakoztatott eszközökre és a kapcsolódó szolgáltatásokra vonatkozó, az uniós gördülő munkaprogramban és a kiberbiztonsági jogszabály értelmében meghatározandó minden további tanúsítási rendszer tekintetében fel kell tüntetni egyrészt azt, hogy a vonatkozó megbízhatósági szinten alkalmazandó biztonsági követelményeket hogyan kell teljesíteni a konkrét európai és nemzetközileg elismert szabványok alapján, függetlenül attól, hogy a terméket mely ágazatban használják majd, másrészt azt, hogy milyen tesztelési előírásokat, tanúsítványokat stb. kell alkalmazni;
11. ELISMERI, hogy a csatlakoztatott eszközök tanúsításához a kiberbiztonsági jogszabály szerinti kiberbiztonsági értékelésekre vonatkozó normákra, szabványokra, illetve műszaki előírásokra lenne szükség. Ezért HANGSÚLYOZZA, hogy kiberbiztonsági normákat, szabványokat, illetve műszaki előírásokat kell megállapítani a csatlakoztatott eszközökre vonatkozóan, és AJÁNLIJA, hogy az európai szabványügyi szervezetek erősítsék meg az ennek érdekében tett erőfeszítéseiket. Ugyanakkor MEGÁLLAPÍTJA, hogy a dolgok internetével kapcsolatos fogyasztói eszközökre vonatkozó ETSI EN 303 645 kiberbiztonsági szabvány fontos előrelépés ebben az irányban;

12. FELKÉRI a Bizottságot, hogy mérlegelje a csatlakoztatott eszközökre és a kapcsolódó szolgáltatásokra irányuló, a jelenleg fejlesztés alatt álló uniós gördülő munkaprogramra épülő és a jelenleg fejlesztés alatt álló horizontális európai kiberbiztonsági tanúsítási rendszereket a lehető legnagyobb mértékben figyelembe vevő, javaslati európai kiberbiztonsági tanúsítási rendszerekre vonatkozó [...] felkérés lehetőségét. Egy ilyen rendszer önkéntes alapon lehetővé teszi majd az említett termékek gyártói számára a termékeknek az értékelés szerinti megbízhatósági szint megadásával történő promócióját;
13. megbeszélést SZORGALMAZ arról, hogy miként lenne rögzíthető a kiberbiztonsági cél egy olyan jövőbeli horizontális jogszabályban, amely kiterjed a csatlakoztatott eszközökkel kapcsolatos kiberbiztonsági kockázatokra is, továbbá ezzel egyidejűleg MEGÁLLAPÍTJA, hogy adott esetben mérlegelni kell az új jogszabályi keret vonatkozó irányelveiben foglalt alapkövetelmények kiigazítását is;
14. arra ÖSZTÖNZI a Bizottságot, hogy szükség esetén olyan ágazatspecifikus kiegészítő szabályozás lehetőségét is mérje fel, amelynek keretében meg kellene határozni a csatlakoztatott eszközök által teljesítendő kiberbiztonsági szintet, mégpedig annak szavatolása érdekében, hogy konkrét biztonsági és adatvédelmi követelmények legyenek megállapítva az említett nagyobb biztonsági kockázatú eszközökre vonatkozóan;
15. KIEMELI, hogy javítani kell az európai polgárok életminőségét és jóllétét, és erősíteni kell a digitális egységes piacba vetett bizalmat. Társadalmainkban a biztonság és a magánélet védelme alapvető fontosságú ahhoz, hogy megőrizzük az Unió alapvető értékeit. Ezért HANGSÚLYOZZA, hogy a kiberbiztonsági jogszabály által biztosított keretre szükséges építeni ahhoz, hogy – a különböző megbízhatósági szinteknek megfelelően – harmonizáljuk a biztonsági követelményeket az új jogszabályi keret valamennyi ágazatában annak érdekében, hogy el lehessen kerülni a széttagoltságot és az azonos követelmények többszörös ellenőrzését, valamint egyenlő innovációs és versenyfeltételeket lehessen biztosítani az Európai Unióban;

16. FELKÉRI a Bizottságot, az Európai Unió Kiberbiztonsági Ügynökséget (ENISA), a Távközlési Megfelelőségértékelési és Piacfelügyeleti Bizottságot, valamint az európai kiberbiztonsági tanúsítási csoportot, hogy egyrészt tevékenyen vegyen részt ebben a kezdeményezésben, amely a digitális egységes piacnak és a csatlakoztatott eszközökhöz kapcsolódó IKT-termékekbe, -szolgáltatásokba és -eljárásokba vetett bizalomnak a megerősítésére irányul a magánélet védelmének és a kiberbiztonságnak a szavatolása révén, másrészt pedig a lehető legmagasabb szintű reziliencia, biztonság és védelem biztosításával segítse elő a dolgok internetéhez kapcsolódó uniós ágazat globális versenyképességének fokozását;
17. ebben az összefüggésben KIEMELI, hogy támogatni kell a kkv-kat, mivel azok az európai kiberbiztonsági ökoszisztéma szerves részét képezik, és arra ÖSZTÖNZI a kkv-kat, hogy vegyenek részt valamennyi elindított nyilvános konzultációban, valamint a szabványosítási tevékenységekben annak érdekében, hogy figyelembe lehessen venni értékes és fontos hozzájárulásukat az arra irányuló folyamatban, hogy a kiberbiztonság teljesíthető célkitűzéssé, illetve versenyelőnyé váljon az európai piacon;
18. MEGÁLLAPÍTJA, hogy a kiberbiztonságnak és a magánélet védelmének a termék teljes életciklusa és ellátási lánc során való biztosítására vonatkozó kötelezettség pozitív hatással lehet a technológiai ágazat környezeti lábnyomára azáltal, hogy a gyártókat intelligens és fenntartható fejlesztési és gyártási folyamatok felé tereli, és ezáltal csökkenti a csatlakoztatott eszközök ártalmatlanításához kapcsolódó elektronikus hulladék mennyiségét.
-