Az Európai Unió
Tanácsa

Brüsszel, 2016. április 21.
(OR. en)

Intézményközi referenciaszám:
2013/0027 (COD)

5581/16
ADD 1

TELECOM 7
DATAPROTECT 6
CYBER 4
MI 37
CSC 15
CODEC 84

TERVEZET – A TANÁCS INDOKOLÁSA

Tárgy:	A Tanács álláspontja első olvasatban a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló EURÓPAI PARLAMENTI ÉS TANÁCSI IRÁNYELV elfogadása céljából – Tervezet – A Tanács indokolása

I. BEVEZETÉS

1. A Bizottság 2013. február 12-én benyújtotta *a hálózat- és információbiztonságnak az egész Unióban egységesen magas szintjére vonatkozó intézkedésekről* szóló európai parlamenti és tanácsi irányelvre (a továbbiakban: az irányelv) vonatkozó javaslatát, melynek jogalapjaként az EUMSZ 114. cikkét jelölte meg.

2. Az Európai Gazdasági és Szociális Bizottság 2013. május 22-én, a Régiók Bizottsága pedig 2013. július 3–4-én szavazta meg a véleményét.

3. Az Európai Parlament 2014. március 13-án szavazta meg az első olvasat során kialakított jogalkotási állásfoglalását[1], és 138 módosítást fogadott el.

4. A Tanács és az Európai Parlament 2014 októberében tárgyalásokat kezdett annak érdekében, hogy a második olvasatban mielőbb megállapodás szülessen. A tárgyalások 2015. december 7-én sikeresen lezárultak, amikor is az Európai Parlament és a Tanács ideiglenes megállapodásra jutott a kompromisszumos szövegről.

5. Az Állandó Képviselők Bizottsága 2015. december 18-án megerősítette az irányelvnek a két intézmény által közösen jóváhagyott kompromisszumos szövegét.

6. Az Európai Parlament Belső Piaci és Fogyasztóvédelmi Bizottságának (IMCO) elnöke 2016. január 28-án levelet intézett az Állandó Képviselők Bizottságának elnökéhez, amelyben jelezte, hogy amennyiben a Tanács hivatalosan is továbbítja az Európai Parlament részére az elfogadott álláspontját, ő ajánlani fogja a plenáris ülésnek, hogy a Parlament – a jogász-nyelvészi ellenőrzést követően – a második olvasat során módosítás nélkül fogadja el a tanácsi álláspontot.

7. A Tanács 2016. február 29-én megerősítette az irányelv kompromisszumos szövegére vonatkozóan elért politikai megállapodását.

---

[1] Az Európai Parlament 2014. március 13-i jogalkotási állásfoglalása a hálózat- és információbiztonságnak az egész Unióban egységesen magas szintjére vonatkozó intézkedésekről szóló európai parlamenti és tanácsi irányelvre irányuló javaslatról.

II. CÉL

8. A tárgyalások eredményéből következik, hogy az irányelv a belső piac működésének javítása érdekében intézkedéseket állapít meg a hálózatok és információs rendszerek egységesen magas szintű biztonságának az Európai Unión belüli megvalósítása céljából.

III. A TANÁCS ELSŐ OLVASATBAN ELFOGADOTT ÁLLÁSPONTJÁNAK ELEMZÉSE

A. Általános információk

9. A plenáris ülésen történt szavazást követően az Európai Parlament és a Tanács tárgyalásokat folytatott azzal a céllal, hogy a második olvasatban megállapodás születhessen a Tanács első olvasatban kialakított álláspontja alapján, amelyet a Parlament módosítások nélkül hagyna jóvá. A Tanács első olvasatban kialakított álláspontjának szövege teljes mértékben tükrözi a társjogalkotók között létrejött kompromisszumot.

B. A legfontosabb kérdések

10. Az Európai Parlamenttel kialakított kompromisszum főbb elemei a következőképpen foglalhatók össze:

a) *Nemzeti képességek*

11. A kompromisszum értelmében a tagállamokat bizonyos kötelezettségek terhelik nemzeti kiberbiztonsági képességeik vonatkozásában. Először is, a tagállamoknak nemzeti stratégiát kell elfogadniuk, amelyben meghatározzák a stratégiai célokat, valamint a hálózatok és információs rendszerek magas szintű biztonságának megteremtéséhez és fenntartásához szükséges megfelelő szakpolitikai és szabályozási intézkedéseket.

12. Másodszor, minden tagállamnak ki kell jelölnie egy vagy több, a hálózati és információs rendszerek biztonságáért felelős illetékes nemzeti hatóságot, amelynek feladata, hogy nemzeti szinten figyelemmel kísérje az irányelv alkalmazását.

13. Harmadszor, minden tagállamnak ki kell jelölnie egy, a hálózatok és információs rendszerek biztonságáért felelős nemzeti kapcsolattartó pontot is (a továbbiakban: egyetlen kapcsolattartó pont). Ez az egyetlen kapcsolattartó pont összekötő feladatokat fog ellátni a tagállami hatóságok közötti és a többi tagállam érintett hatóságaival folytatott, határokon átnyúló együttműködés, valamint az együttműködési csoporttal és a CSIRT-hálózattal folytatott együttműködés biztosítása céljából. Az egyetlen kapcsolattartó pont ezen túlmenően évente jelentést nyújt majd be az együttműködési csoportnak a beérkezett bejelentésekről.

14. Végezetül, minden tagállamnak ki kell jelölnie egy vagy több hálózatbiztonsági incidenselhárító csoportot (CSIRT), amelynek feladata a biztonsági események és kockázatok kezelése. A hálózatbiztonsági incidenselhárító csoportok kötelezettségeit és feladatait a kompromisszumos szöveg I. melléklete tartalmazza.

b) *Együttműködés*

15. A kompromisszumos szöveg értelmében együttműködési csoport jön létre a tagállamok közötti stratégiai együttműködés támogatása és megkönnyítése, a bizalom megteremtése, valamint az uniós hálózatok és információs rendszerek egységesen magas szintű biztonságának a megvalósítása érdekében. Az együttműködési csoport a tagállamok, a Bizottság és az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) képviselőiből áll majd, és a kompromisszumos szövegben felsorolt konkrét feladatokat fogja ellátni. Ezek közé tartozik a bevált gyakorlatok és különböző kérdésekkel kapcsolatos információk cseréje, valamint a tagállamok képességeinek és felkészültségének a megvitatása.

16. Ezen túlmenően, a tagállamok közötti bizalom erősítése és a gyors és hatékony operatív együttműködés előmozdítása érdekében a kompromisszum értelmében létrejön a nemzeti CSIRT-ek hálózata. A CSIRT-hálózat a tagállamok CSIRT-jeinek és a hálózatbiztonsági vészhelyzeteket elhárító csoportnak (CERT-EU) a képviselőiből áll majd, és abban megfigyelőként a Bizottság is részt vesz. Az ENISA biztosítja a titkárságot, és aktívan támogatja a CSIRT-ek közötti együttműködést. A kompromisszumos szöveg meghatározza a hálózat által elvégzendő feladatokat. Ezek közé tartozik a CSIRT-ek szolgáltatásaival, tevékenységeivel és együttműködési képességeivel kapcsolatos információk megosztása; a tagállamok segítése a határon átnyúló biztonsági események kezelésében; valamint – bizonyos feltételek mellett – a biztonsági eseményekre és a kapcsolódó kockázatokra vonatkozó információk cseréje és megvitatása.

c) *Biztonsági és bejelentési követelmények*

17. Az irányelv a piaci szereplők két csoportja – nevezetesen az alapvető szolgáltatásokat nyújtó gazdasági szereplők és a digitális szolgáltatók – vonatkozásában bizonyos kötelezettségeket állapít meg a biztonsági és bejelentési követelményeket illetően.

18. Az irányelv II. melléklete egy sor olyan ágazatot felsorol, amelyek nagy jelentőséggel bírnak a társadalom és a gazdaság szempontjából. Ezek a következők: energia, közlekedés, banki szolgáltatások, pénzügyi piaci infrastruktúrák, egészségügy, ivóvízellátás és -elosztás, digitális infrastruktúra. A tagállamok az irányelvben meghatározott pontos kritériumok alapján megállapítják, hogy az említett ágazatokon belül melyek az alapvető szolgáltatásokat nyújtó gazdasági szereplők.

19. Az irányelv III. melléklete a digitális szolgáltatások három olyan típusát sorolja fel, amelyek esetében a szolgáltatóknak meg kell felelniük az irányelv követelményeinek. Ezek az online piacterek, az online keresőprogramok és a számításifelhő-szolgáltatások. A III. mellékletben felsorolt szolgáltatásokat nyújtó minden digitális szolgáltatónak meg kell felelnie az irányelv követelményeinek, a mikro- és a kisvállalkozások kivételével.

20. A piaci szereplők két csoportjának szervezési és műszaki intézkedéseket kell majd hoznia a hálózatok és információs rendszerek biztonságát fenyegető kockázatok kezelése, valamint annak érdekében, hogy meg lehessen előzni a szóban forgó rendszerek biztonságát érintő eseményeket vagy minimális szintre lehessen csökkenteni azok hatását. Ezen túlmenően, azokat a biztonsági eseményeket, amelyeknek a szóban forgó szolgáltatásokra gyakorolt hatása elér egy bizonyos szintet, be kell majd jelenteni az illetékes nemzeti hatóságok vagy a CSIRT-ek felé. A biztonsági események hatásainak szintjét az irányelvben meghatározott kritériumok alapján kell megállapítani.

21. Az irányelv a piaci szereplők két kategóriája esetében differenciált megközelítést alkalmaz. A digitális szolgáltatók esetében kevésbé szigorúak a biztonsági és bejelentési követelmények, mint az alapvető szolgáltatásokat nyújtó gazdasági szereplők esetében, ami azt tükrözi, hogy a digitális szolgáltatók által nyújtott szolgáltatásokban bekövetkező zavarok kisebb kockázatot jelenthetnek a társadalomra és a gazdaságra nézve, mint az alapvető szolgáltatások nyújtásában támadt zavarok. Ezen túlmenően, az irányelv nem teszi lehetővé, hogy a tagállamok további biztonsági vagy bejelentési követelményeket rójanak a digitális szolgáltatókra, egyrészt a magas szintű harmonizáció biztosítása érdekében, másrészt pedig arra tekintettel, hogy e szolgáltatók gyakran egyszerre több tagállamban folytatják tevékenységüket.

22. A kompromisszumos szöveg azt is kimondja, hogy azok a szervezetek, amelyeket nem azonosítottak alapvető szolgáltatásokat nyújtó gazdasági szereplőként és amelyek nem digitális szolgáltatók, önkéntes alapon bejelenthetnek bizonyos biztonsági eseményeket.

d) *Átültetés*

23. A tagállamoknak legkésőbb az irányelv hatálybalépésétől számított 21 hónapon belül át kell ültetniük az irányelvet. Az alapvető szolgáltatásokat nyújtó gazdasági szereplők azonosítására az átültetési határidőn túl további hat hónap áll a rendelkezésükre.

IV. ÖSSZEGZÉS

24. A Tanács álláspontja maradéktalanul tükrözi az Európai Parlament és a Tanács közötti tárgyalások során a Bizottság egyetértésével kialakított kompromisszumot. Ezt a kompromisszumot megerősíti az a levél is, amelyet a Belső Piaci és Fogyasztóvédelmi Bizottság elnöke 2016. január 28-án küldött az Állandó Képviselők Bizottsága elnökének.