EURÓPAI
BIZOTTSÁG

Brüsszel, 2017.10.4.
COM(2017) 476 final

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 476 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 476 final/2 of 4.10.2017

A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK

A kiberbiztonsági irányelv maximális kihasználása – a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló 1148/2016/EU irányelv hatékony végrehajtása felé

Bevezetés

A 2016. július 6-án elfogadott, a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló (EU) 2016/1148 irányelv[1] (a továbbiakban: kiberbiztonsági irányelv vagy irányelv) az első olyan uniós horizontális jogszabály, amely a kiberbiztonsági kihívásokkal foglalkozik, és valódi változást hozott Európában a kiberbiztonsági ellenálló képesség és együttműködés tekintetében.

Az irányelvnek három fő célja van:

- a nemzeti kiberbiztonsági képességek fejlesztése,
- az uniós szintű együttműködés kiépítése, valamint
- a kockázatkezelésnek és a biztonsági események jelentésének előmozdítása a kulcsfontosságú gazdasági szereplők, nevezetesen a gazdasági és társadalmi tevékenységek fenntartásához alapvető szolgáltatásokat nyújtó szereplők (OES), valamint a digitális szolgáltatók (DSP-k) körében.

A kiberbiztonsági irányelv a gazdasági és társadalmi életünk digitalizálásával együttjáró, fokozódó kiberfenyegetésekre és kihívásokra adott uniós válasz egyik sarokköve, ezért végrehajtása a 2017. szeptember 13-án előterjesztett kiberbiztonsági csomag lényeges részét képezi. Az uniós válasz eredményessége mindaddig sérül, amíg a kiberbiztonsági irányelvet nem ültetik át teljes mértékben valamennyi uniós tagállamban. Ezt az „Európa kibertámadásokkal szembeni ellenálló képességének erősítéséről” szóló 2016. évi bizottsági közlemény[2] is kritikus pontként ismerte el.

A kiberbiztonsági irányelv újszerűsége és a gyorsan változó kiberfenyegetések kezelésének sürgőssége okán különös figyelmet kell fordítani az összes olyan kihívásra, amelyekkel a szereplőknek szembe kell nézniük az irányelv időben történő és sikeres átültetésének biztosítása érdekében. A 2018. május 9-i átültetési határidőre, valamint az alapvető szolgáltatásokat nyújtó szereplők azonosítására vonatkozó 2018. november 9-i határidőre tekintettel a Bizottság támogatja a tagállamok átültetési folyamatát és a Kiberbiztonsági Együttműködési Csoportban e célból végzett munkáját.

Ez a közlemény és melléklete a Bizottságnak a kiberbiztonsági irányelv végrehajtásával kapcsolatos eddigi előkészítő munkáján és elemzésén, az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) közreműködésén, valamint a tagállamokkal az irányelv átültetésének szakaszában, különösen az együttműködési csoporton[3] belül folytatott megbeszéléseken alapul. Ez a közlemény kiegészíti az eddigi, különösen a következők révén tett jelentős erőfeszítéseket:

[1] 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. Az irányelv 2016. augusztus 8-án lépett hatályba.
[2] COM(2016) 410 final.
[3] A tagállamok közötti stratégiai együttműködésre szolgáló mechanizmus a kiberbiztonsági irányelv 11. cikke alapján.

- az együttműködési csoport intenzív munkája; a csoport olyan munkatervet fogadott el, amely elsősorban a kiberbiztonsági irányelv átültetésére, valamint különösen az alapvető szolgáltatásokat nyújtó szereplők azonosításának kérdésére, továbbá e szereplők biztonsági követelményekkel és a biztonsági események bejelentésével kapcsolatos kötelezettségeire összpontosít. Noha az irányelv mérlegelési jogkört biztosít az alapvető szolgáltatásokat nyújtó szereplőkre vonatkozó rendelkezések átültetése terén, a tagállamok felismerték, hogy e tekintetben fontos az összehangolt megközelítés[4],
- a számítógép-biztonsági eseményekre reagáló csoportokból (CSIRT-ekből) álló hálózat létrehozása és gyors működtetése az irányelv 12. cikkének (1) bekezdésével összhangban. A hálózat azóta elkezdte lefektetni az európai szintű strukturált operatív együttműködés alapjait.

Az e két struktúra által képviselt szakpolitikai és operatív szintekre egyaránt igaz, hogy valamennyi tagállamnak teljes mértékben el kell köteleznie magát a hálózati és információs rendszerek Unió-szerte egységesen magas szintű biztonságának mint célnak az elérése érdekében.

Ez a közlemény és melléklete megerősítik ezeket az erőfeszítéseket azzal, hogy összegyűjtik és összehasonlítják a tagállamoknak az irányelv végrehajtása szempontjából lényeges legjobb gyakorlatait, további iránymutatást nyújtanak az irányelv végrehajtásának módjával kapcsolatban, továbbá részletesebb magyarázattal szolgálnak egyes konkrét rendelkezésekkel kapcsolatban. Az átfogó cél a tagállamok támogatása a kiberbiztonsági irányelv EU-szerte eredményes és összehangolt végrehajtásában.

Ezt a közleményt a kiberbiztonsági irányelv 16. cikkének (8) bekezdése értelmében a digitális szolgáltatók biztonsági követelményekkel és a biztonsági események bejelentésével kapcsolatos kötelezettségeihez kapcsolódó elemek és paraméterek további meghatározásáról szóló, hamarosan elkészülő bizottsági végrehajtási rendelet fogja kiegészíteni. A végrehajtási rendelet megkönnyíti az irányelvnek a digitális szolgáltatókra vonatkozó kötelezettségek tekintetében történő végrehajtását[5].

A közlemény bemutatja a nemzeti jogba való átültetés szempontjából lényeges hivatkozási pontoknak és potenciálisan inspirációnak tekintett kérdések elemzéséből levont legfontosabb következtetéseket. Az elsődleges hangsúly itt a tagállamoknak az irányelv hatálya alá tartozó szervezetekre vonatkozó képességeivel és kötelezettségeivel kapcsolatos rendelkezésekre összpontosul. A melléklet részletesebben vizsgálja azokat a területeket, amelyeken a

[4] Az együttműködési csoport jelenleg olyan referencia-útmutatókon dolgozik, amelyek többek között a következőkre vonatkoznak: a gazdasági szereplőknek az irányelv 5. cikkének (2) bekezdése értelmében kritikus jellegét meghatározó kritériumok; azon körülmények, amelyek fennállása esetén az alapvető szolgáltatásokat nyújtó szereplőknek az irányelv 14. cikkének (7) bekezdése alapján a biztonsági eseményeket be kell jelenteniük; valamint a 14. cikk (1) és (2) bekezdésével összhangban az alapvető szolgáltatásokat nyújtó szereplőkre vonatkozó biztonsági követelmények.

[5] A végrehajtási rendelet tervezete nyilvános konzultáció céljából a következő weboldalon hozzáférhető: https://ec.europa.eu/info/law/better-regulation/have-your-say_hu

Bizottság szerint a legnagyobb többletértéket jelentené, ha az irányelv egyes rendelkezéseinek magyarázata és értelmezése, valamint az irányelvvel kapcsolatban eddig kialakult legjobb gyakorlatok és összegyűjtött tapasztalatok bemutatása révén gyakorlati iránymutatást nyújtana az irányelv átültetéséhez.

A kiberbiztonsági irányelv hatékony végrehajtására törekedve

A kiberbiztonsági irányelv célja a hálózati és információs rendszerek Unió-szerte egységesen magas szintű biztonságának a biztosítása. Ez azt jelenti, hogy meg kell erősíteni a társadalmunk és gazdaságunk működésének alapját képező internet, magánhálózatok és információs rendszerek biztonságát. E tekintetben az első fontos elem a tagállamok felkészültsége, amelyet a nemzeti kiberbiztonsági stratégiáknak az irányelvben leírt módon való megvalósításával, valamint a CSIRT-ek és az illetékes nemzeti hatóságok működésével kell biztosítani.

A nemzeti stratégiák átfogó jellege

Fontos, hogy a tagállamok felhasználják a kiberbiztonsági irányelv átültetése nyújtotta lehetőséget arra, hogy a hiányosságok, a bevált módszerek és a mellékletben szereplő új kihívások fényében felülvizsgálják nemzeti kiberbiztonsági stratégiájukat.

Bár az irányelv érthető módon a kiemelt jelentőségű vállalatokra és szolgáltatásokra összpontosít, a gazdaság és a társadalom egészének kiberbiztonságát kell holisztikus és következetes módon kezelni, tekintettel arra, hogy egyre nagyobb mértékben hagyatkozunk az információs és kommunikációs technológiákra. Ezért a kiberbiztonsági irányelv minimumkövetelményeit túllépő (azaz az irányelv II. és III. mellékletében felsorolt ágazatoknál és szolgáltatásoknál többre is kiterjedő) átfogó nemzeti stratégiák elfogadása növelné a hálózati és információs rendszerek biztonságának általános szintjét.

Mivel a kiberbiztonság még mindig viszonylag új és gyorsan bővülő közpolitikai terület, a legtöbb esetben új beruházásokra van szükség, még akkor is, ha az államháztartás általános helyzete megszorításokat és megtakarításokat igényel. Az irányelv céljainak elérése szempontjából ezért alapvetően fontos, hogy a nemzeti stratégiák hatékony végrehajtásához elengedhetetlen, megfelelő pénzügyi és emberi erőforrások, ezen belül az illetékes nemzeti hatóságok és a CSIRT-ek elegendő erőforrásainak biztosítása érdekében ambiciózus döntéseket hozzanak.

A végrehajtás és az érvényesítés hatékonysága

Az irányelv 8. cikke körvonalazza a nemzeti illetékes hatóságok és az egyedüli kapcsolattartó pontok kijelölésének szükségességét, ami a kiberbiztonsági irányelv eredményes végrehajtása és a határokon átnyúló együttműködés kulcsfontosságú eleme. Ezen a területen a tagállamok centralizáltabb és decentralizáltabb megközelítéseket egyaránt alkalmaznak. Bebizonyosodott, hogy amennyiben a tagállamok decentralizáltabb megközelítést alkalmaznak az illetékes nemzeti hatóságok kijelölése tekintetében, lényeges biztosítani a számos hatóság és az

egyedüli kapcsolattartó pont közötti szoros együttműködést (*lásd az 1. táblázatot a melléklet 3.2. pontjában*). Ez növeli a végrehajtás hatékonyságát és megkönnyíti az érvényesítést.

A kritikus információs infrastruktúrák védelemével kapcsolatos korábbi tapasztalatok hasznosítása segítséget jelenthet a tagállamok optimális irányítási modelljének kialakításában, ami a kiberbiztonsági irányelv hatékony ágazati végrehajtását és a koherens horizontális megközelítést egyaránt biztosítaná (*lásd a melléklet 3.1. pontját*).

A nemzeti CSIRT-ek kapacitásainak fokozása

A kiberbiztonsági irányelv 9. cikkében foglaltaknak megfelelően EU-szerte létrehozott, hatékony és elegendő erőforrással ellátott nemzeti CSIRT-ek nélkül az EU továbbra is ki lesz szolgáltatva a határokon átnyúló számítógépes fenyegetéseknek. A tagállamok ezért mérlegelhetnék a CSIRT-ek hatáskörének kiterjesztését az irányelv hatályán kívül eső ágazatokra és szolgáltatásokra (*lásd a melléklet 3.3. pontját*). Ez lehetővé tenné a nemzeti CSIRT-ek számára, hogy kiberbiztonsági események bekövetkezése esetén olyan vállalatoknak és szervezeteknek is nyújtsanak operatív támogatást, amelyek nem tartoznak az irányelv hatálya alá, de fontosak a társadalom és a gazdaság számára. Emellett a tagállamok teljes mértékben ki tudnák használni az Európai Hálózatfinanszírozási Eszköz (CEF) kiberbiztonsági digitális szolgáltatási infrastruktúrák (DSI) programja által kínált további finanszírozási lehetőségeket, amelyek célja a nemzeti CSIRT-ek képességeinek és együttműködésének fejlesztése (*lásd a melléklet 3.5. pontját*).

Az alapvető szolgáltatásokat nyújtó szereplők következetes azonosítási folyamata

A kiberbiztonsági irányelv 5. cikkével összhangban a tagállamoknak 2018. november 9-ig azonosítaniuk kell azokat a szervezeteket, amelyek alapvető szolgáltatásokat nyújtó szereplőnek minősülnek. E feladattal kapcsolatban a tagállamok fontolóra vehetik az e közleményben foglalt fogalommeghatározások és iránymutatások következetes alkalmazását annak biztosítása érdekében, hogy a belső piacon hasonló szerepet betöltő, hasonló típusú szervezetek más tagállamokban is következetesen alapvető szolgáltatásokat nyújtó szereplőnek minősüljenek. A tagállamok mérlegelhetik továbbá a kiberbiztonsági irányelv hatályának a közigazgatásra való kiterjesztését, tekintettel arra, hogy az milyen szerepet tölt be a társadalom és a gazdaság egésze szempontjából (*lásd a melléklet 2.1. és 4.1.3. pontját*).

Az alapvető szolgáltatásokat nyújtó szereplők azonosítására vonatkozó nemzeti megközelítéseknek – az együttműködési csoport által kidolgozott útmutatást követve (*lásd a melléklet 4.1.2. pontját*) – a lehető legnagyobb mértékben való összehangolása nagyon hasznos lenne, mivel az irányelv rendelkezéseinek összehangoltabb alkalmazásához vezetne, és ezáltal csökkentené a piac széttagoltságának kockázatát. Olyan esetekben, amikor az alapvető szolgáltatásokat nyújtó szereplők két vagy több tagállamban is nyújtanak alapvető

szolgáltatásokat, elengedhetetlen, hogy a tagállamok törekedjenek megállapodásra (az 5. cikk (4) bekezdése szerinti egyeztetési eljárás keretében) a szervezetek egységes azonosításáról (*lásd a melléklet 4.1.7. pontját*), mivel ezzel elkerülhető, hogy ugyanazon szervezet különböző tagállami joghatóságok alatt eltérő szabályozási bánásmódban részesüljön.

Az alapvető szolgáltatásokat nyújtó szereplők azonosítására vonatkozó információk benyújtása a Bizottság számára

A tagállamoknak az 5. cikk (7) bekezdésével összhangban be kell nyújtaniuk a Bizottsághoz az alapvető szolgáltatásokat nyújtó szereplők azonosítását lehetővé tevő nemzeti intézkedésekre vonatkozó információkat, az alapvető szolgáltatások jegyzékét, az azonosított, alapvető szolgáltatásokat nyújtó szereplők számát, valamint az érintett szereplők jelentőségét a gazdasági ágazat számára. Ezen túlmenően a Bizottság felkéri a tagállamokat arra, hogy adják meg az azonosítási eljárás során a megfelelő ellátási szintnek vagy a megfelelő ellátási szint fenntartása szempontjából egy adott szereplő jelentőségének meghatározására használt küszöbértékeket, amennyiben létezik ilyen küszöbérték. A tagállamok mérlegelhetik továbbá, hogy – amennyiben szükséges, bizalmasan – megosszák a Bizottsággal az azonosított, alapvető szolgáltatásokat nyújtó szereplők jegyzékét, mivel ez segítséget jelentene a bizottsági értékelés pontosságának és minőségének javításában (*lásd a melléklet 4.1.5. és 4.1.6. pontját*).
Összehangolt megközelítések az alapvető szolgáltatásokat nyújtó szereplők biztonsági követelményekkel és a biztonsági események bejelentésével kapcsolatos kötelezettségei tekintetében

Az alapvető szolgáltatásokat nyújtó szereplők biztonsági követelményekkel és a biztonsági események bejelentésével kapcsolatos kötelezettségei tekintetében (lásd a 14. cikk (1), (2) és (3) bekezdését) az uniós tagállamok határain átnyúló alapvető szolgáltatásokat nyújtó szereplők megfelelésének megkönnyítését szolgáló, a biztonsági követelményekkel és a biztonsági események bejelentésével kapcsolatos kötelezettségekre vonatkozó összehangolt megközelítés mozdítaná elő a lehető legnagyobb mértékben az egységes piac hatását. Itt továbbra is az együttműködési csoporton belül az iránymutatásokat tartalmazó dokumentummal kapcsolatosan végzett munka szerepel hivatkozásként (*lásd a melléklet 4.2. és 4.3. pontját*).

Több tagállamot érintő, nagyszabású kiberbiztonsági esemény bekövetkezése esetén nagyon valószínű, hogy egy alapvető szolgáltatásokat nyújtó szereplő vagy egy digitális szolgáltató a 14. cikk (3) bekezdése és a 16. cikk (3) bekezdése értelmében kötelezően, vagy egy másik, az irányelv hatálya alá nem tartozó szervezet a 20. cikk (1) bekezdése értelmében önként bejelenti az eseményt. A tagállamok a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról szóló bizottsági ajánlással összhangban fontolóra vehetik, hogy nemzeti megközelítéseiket összehangolják annak érdekében, hogy az említett bejelentéseken alapuló lényeges információkat a lehető leghamarabb a többi érintett tagállam illetékes hatóságai vagy CSIRT-jei rendelkezésre tudják bocsátani. A pontos és intézkedést lehetővé tevő információk elengedhetetlenek a fertőzések számának csökkentéséhez és ahhoz, hogy a sebezhetőségeket még az előtt kezelni lehessen, mielőtt kihasználják azokat.

A kiberbiztonsági irányelv lehető legnagyobb mértékű kiaknázására törekvő partnerség szellemében a Bizottságnak az a szándéka, hogy a jogszabály értelmében valamennyi érdekelt félre kiterjessze az Európai Hálózatfinanszírozási Eszköz keretében nyújtott támogatást. Míg eddig a CSIRT-ek kapacitásépítése, valamint egy gyors és hatékony operatív együttműködést lehetővé tevő platform kialakítása és ezáltal a CSIRT-hálózat megerősítése kapott hangsúlyt, a Bizottság most megvizsgálja, hogy az Európai Hálózatfinanszírozási Eszköz keretében nyújtott finanszírozás milyen előnyökkel járhat a nemzeti illetékes hatóságok, valamint az alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók számára.

Következtetés

Tekintettel a kiberbiztonsági irányelv nemzeti jogba való átültetésének 2018. május 9-i, küszöbönálló határidejére, valamint az alapvető szolgáltatásokat nyújtó szereplők azonosítására vonatkozó 2018. november 9-i határidőre, a tagállamoknak megfelelő intézkedéseket kell tenniük annak érdekében, hogy a kiberbiztonsági irányelv rendelkezései és együttműködési modelljei a lehető legjobb uniós szintű eszközöket biztosíthassák a hálózati és információs rendszerek Unió-szerte egységesen magas szintű biztonságának a biztosításához. A Bizottság felkéri a tagállamokat, hogy mindezek során vegyék figyelembe az e közleményben foglalt lényeges információkat, iránymutatást és ajánlásokat.

E közleményt kiegészíthetik más, többek között az együttműködési csoport keretében folyó munkából eredő intézkedések is.