EURÓPAI
BIZOTTSÁG

Brüsszel, 2017.10.4.
COM(2017) 476 final

ANNEX 1

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

MELLÉKLET

a következőhöz:

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

TARTALOMJEGYZÉK

MELLÉKLET 4
1. Bevezetés 4
2. A hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégia 5
2.1. A nemzeti stratégia hatálya 5
2.2. A nemzeti stratégiák tartalma és az elfogadásukra szolgáló eljárás 6
2.3. A folyamat és a megoldandó kérdések 7
2.4. Konkrét lépések, amelyeket a tagállamoknak az átültetési határidő előtt el kell végezniük. . 9
3. A kiberbiztonsági irányelv: Az illetékes nemzeti hatóságok, az egyedüli kapcsolattartó pontok és a számítógép-biztonsági eseményekre reagáló csoportok (CSIRT-ek) 11
3.1. A hatóságok típusa 12
3.2. Nyilvánosság és további lényeges szempontok 13
3.3. A kiberbiztonsági irányelv 9. cikke: Számítógép-biztonsági eseményekre reagáló csoportok (CSIRT-ek) 18
3.4. Feladatok és követelmények 18
3.5. Segítségnyújtás a CSIRT-ek fejlesztéséhez 19
3.6. Az egyedüli kapcsolattartó pont szerepe 20
3.7. Szankciók 21
4.1. Az alapvető szolgáltatásokat nyújtó szereplők 22
4.1.1. A kiberbiztonsági irányelv II. mellékletében felsorolt szervezetek típusai 22
4.1.2. Az alapvető szolgáltatásokat nyújtó szereplők azonosítása 24
4.1.3. További ágazatok bevonása a jogszabályok hatálya alá 25
4.1.4. Joghatóság 26
4.1.5. A Bizottságnak benyújtandó információk 26
4.1.7. Határon átnyúló egyeztetési eljárás 33
4.2. Biztonsági követelmények 33
4.3. Bejelentési követelmények 34
4.4. A kiberbiztonsági irányelv III. melléklete: Digitális szolgáltatók 34
4.4.1. A digitális szolgáltatók kategóriái 35
4.4.2. Biztonsági követelmények. 38
4.4.3. Bejelentési követelmények. 38
4.4.4. Kockázatalapú szabályozási megközelítés. 38
4.4.5. Joghatóság. 39

4.4.6. A korlátozott méretű digitális szolgáltatók mentessége a biztonsági követelmények és a bejelentési kötelezettség hatálya alól. 39
5. A kiberbiztonsági irányelv és más jogszabályok közötti kapcsolat. 40
5.1. A kiberbiztonsági irányelv 1. cikkének (7) bekezdése: A *lex specialis* rendelkezése. 40
5.2. A kiberbiztonsági irányelv 1. cikkének (3) bekezdése: távközlési szolgáltatók és bizalmi szolgáltatók 44
6. Közzétett nemzeti kiberbiztonsági stratégiai dokumentumok 45
7. Az ENISA által kiadott ajánlások és bevált gyakorlatok jegyzéke 49

MELLÉKLET

1. Bevezetés

E melléklet célja, hogy elősegítse a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló (EU) 2016/1148 irányelv (a továbbiakban: kiberbiztonsági irányelv vagy irányelv)[1] hatékony alkalmazását, végrehajtását és érvényesítését, valamint hogy segítséget nyújtson a tagállamoknak, hogy biztosítani tudják az uniós jog hatékony alkalmazását. Közelebbről hármas célkitűzést szolgál: a) egyértelműbbé tenni a nemzeti hatóságok számára az irányelvben foglalt, rájuk vonatkozó kötelezettségeket, b) biztosítani az irányelvből fakadó, olyan jogalanyokra vonatkozó kötelezettségek hatékony érvényesítését, amelyekre a biztonsági követelményekkel és a biztonsági események bejelentésével kapcsolatos kötelezettségek hárulnak, valamint c) összességében hozzájárulni a jogbiztonság valamennyi érintett szereplő számára való megteremtéséhez.

Mindezek érdekében e melléklet iránymutatást nyújt az alábbiak tekintetében, amelyek kulcsfontosságúak a kiberbiztonsági irányelv céljának elérése szempontjából, azaz ahhoz, hogy a társadalmunk és gazdaságunk működésének alapját képező hálózati és információs rendszerek biztonságát az egész Unióban egységesen magas szint jellemezze:

- a tagállamok arra vonatkozó kötelezettsége, hogy a hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégiát fogadjanak el (2. pont),
- az illetékes nemzeti hatóságok, az egyedüli kapcsolattartó pontok és a számítógép-biztonsági eseményekre reagáló csoportok felállítása (3. pont),
- az alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók biztonsági követelményekkel és biztonsági események bejelentésével kapcsolatos kötelezettségei (4. pont), valamint
- a kiberbiztonsági irányelv és más jogszabályok közötti kapcsolat (5. pont).

Ezen iránymutatás kidolgozásához a Bizottság felhasználta az irányelv előkészítése során összegyűjtött információkat és elemzéseket, valamint az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) és az együttműködési csoport által szolgáltatott információkat. Ezenkívül egyes tagállamok tapasztalatait is felhasználta. A Bizottság értelemszerűen figyelembe vette az uniós jog értelmezésére vonatkozó alapelveket: a kiberbiztonsági irányelv szövegét, összefüggéseit és célkitűzéseit. Mivel az irányelvet még nem ültették át, az Európai Unió Bíróságán (EUB) és a nemzeti bíróságokon még nem született ítélet. Ezért az ítélkezési gyakorlatot nem lehet iránymutatásként használni.

[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.

Egyetlen dokumentumba foglalva ezen információk megfelelő áttekintést adhatnak a tagállamoknak az irányelvről, és lehetővé tehetik számukra, hogy nemzeti jogszabályaik kidolgozásakor figyelembe vegyék ezeket az információkat. A Bizottság ugyanakkor hangsúlyozza, hogy ez a melléklet nem kötelező érvényű, és nem szolgál új szabályok alkotására. Az uniós jog értelmezésére az EUB rendelkezik végső hatáskörrel.

2. A hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégia

A kiberbiztonsági irányelv 7. cikke értelmében a tagállamok kötelesek olyan nemzeti stratégiát elfogadni a hálózati és információs rendszerek biztonságára vonatkozóan, amely egyenértékűnek tekinthető a nemzeti kiberbiztonsági stratégiával (a továbbiakban: „NKBS"). A nemzeti stratégia feladata, hogy meghatározza a kiberbiztonsággal kapcsolatos stratégiai célkitűzéseket és a megfelelő szakpolitikai és szabályozási intézkedéseket. Az NKBS fogalmát széles körben alkalmazzák nemzetközi és európai szinten, különösen az ENISA által a tagállamokkal a nemzeti stratégiákkal kapcsolatban folytatott együttműködéssel összefüggésben, amelynek eredményeként a közelmúltban naprakésszé tette az „NKBS-sel kapcsolatos bevált gyakorlatra vonatkozó útmutatót"[2].

Ebben a pontban a Bizottság kifejti, hogy a kiberbiztonsági irányelv miként fokozza a tagállamok felkészültségét azáltal, hogy előírja a hálózati és információs rendszerek biztonságára vonatkozó kiforrott nemzeti stratégiák alkalmazását (7. cikk). Ez a pont a következő szempontokkal foglalkozik: a) a stratégia hatálya és b) a stratégia tartalma, valamint az elfogadási eljárás.

Az alábbiakban részletesebben is kifejtésre kerül, hogy a kiberbiztonsági irányelv 7. cikkének helyes átültetése alapvető fontosságú az irányelv céljainak eléréséhez, és e célból megfelelő pénzügyi és emberi erőforrások biztosítását igényli.

2.1. A nemzeti stratégia hatálya

A 7. cikk szövege értelmében az NKBS elfogadásának kötelezettsége csak a II. mellékletben említett ágazatokra (azaz az energiaágazatra, a közlekedési ágazatra, a banki szolgáltatásokra, a pénzügyi piacra, az egészségügyre, az ivóvízellátásra és -elosztásra, valamint a digitális infrastruktúrára) és a III. mellékletben említett szolgáltatásokra (az online piacterekre, az online keresőprogramokra és a felhőalapú számítástechnikai szolgáltatásokra) vonatkozik.

Az irányelv 3. cikke konkrétan meghatározza a harmonizáció minimumának elvét, amelynek értelmében a tagállamok a hálózati és információs rendszerek magasabb szintű biztonságának megvalósítása érdekében rendelkezéseket fogadhatnak el vagy tarthatnak fenn. Ezt az elvet az „NKBS" elfogadására vonatkozó kötelezettség tekintetében is követve a tagállamok több ágazatot és szolgáltatást felvehetnének a kötelezettség hatálya alá, mint amennyit az irányelv II. és III. melléklete magában foglal.

[2] ENISA, *National Cyber-Security Strategy Good Practice* (A nemzeti kiberbiztonsági stratégiával kapcsolatos bevált gyakorlat) (2016). Elérhető a következő címen: https://www.enisa.europa.eu/publications/ncss-good-practice-guide

A Bizottság álláspontja szerint és tekintettel a kiberbiztonsági irányelv céljára, nevezetesen a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjének elérésére[3], célszerű lenne olyan nemzeti stratégiát kidolgozni, amely a társadalom és a gazdaság valamennyi vonatkozó dimenzióját felöleli, nem csupán a kiberbiztonsági irányelv II. és III. mellékletében foglalt ágazatokat és digitális szolgáltatásokat. Ez összhangban van a nemzetközi szinten bevált gyakorlatokkal (az ITU útmutatására és az OECD elemzésére vonatkozó hivatkozásokat lásd az alábbiakban), valamint a kiberbiztonsági irányelvvel.

Amint az az alábbiakban bővebben kifejtésre kerül, ez különösen érvényes az irányelv II. és III. mellékletében felsoroltaktól eltérő ágazatokért és szolgáltatásokért felelős közigazgatási szervekre. Előfordulhat, hogy a közigazgatási szervek olyan érzékeny adatokat dolgoznak fel, amelyek miatt az adatok kiszivárgását megelőző és a szóban forgó információk védelmét biztosító NKBS és irányítási tervek hatálya alá kell tartozniuk.

2.2. A nemzeti stratégiák tartalma és az elfogadásukra szolgáló eljárás

A kiberbiztonsági irányelv 7. cikke értelmében az NKBS-nek legalább a következőket kell tartalmaznia:

i. a hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégia céljai és prioritásai;
ii. a nemzeti stratégia céljainak és prioritásainak teljesítését szolgáló irányítási keretrendszer;
iii. a felkészültségre, a reagálásra és a helyreállításra vonatkozó intézkedések azonosítása, ideértve a köz- és a magánszféra közötti együttműködést is;
iv. a vonatkozó oktatási, tájékoztató és képzési programok megjelölése;
v. a kutatási és fejlesztési tervek megjelölése;
vi. a kockázatok feltárására szolgáló kockázatértékelési terv; valamint
vii. a stratégia végrehajtásába bevont szereplők jegyzéke.

Sem a 7. cikk, sem a megfelelő (29) preambulumbekezdés nem határozza meg az NKBS elfogadására vonatkozó követelményeket vagy nagyobb részletességgel az NKBS tartalmát. Ami a folyamatot, valamint az NKBS tartalmával kapcsolatos további elemeket illeti, a Bizottság az alábbiakban ismertetett megközelítést az NKBS elfogadásának egyik megfelelő módjának tekinti. Ez a megközelítés a tagállamok és a harmadik országok azon tapasztalatainak elemzésén alapul, amelyeket a tagállamok saját stratégiáik kidolgozása során szereztek. További információs forrás az ENISA NKBS-re vonatkozó képzési eszköze, amely a honlapján[4] videó és letölthető média formájában is elérhető.

[3] Lásd az 1. cikk (1) bekezdését.
[4] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-training-tool

2.3. A folyamat és a megoldandó kérdések

A nemzeti stratégia kidolgozása és azt követő elfogadása összetett és sokrétű folyamat, amely tartós együttműködést igényel a kiberbiztonsággal foglalkozó szakértőkkel, a civil társadalommal és a nemzeti politikai folyamatokkal ahhoz, hogy hatékony és sikeres legyen. Elengedhetetlen feltétel a magas szintű közigazgatási támogatás a vezető minisztérium legalább államtitkári vagy azzal egyenértékű szintjén, valamint a politikai támogatás. Az NKBS sikeres elfogadása érdekében fontolóra lehet venni a következő öt lépésből álló folyamat követését (lásd az 1. ábrát):

Első lépés – **A stratégiából fakadó alapelvek és stratégiai célok meghatározása.**

Először is az illetékes nemzeti hatóságoknak meg kell határozniuk egyes kulcsfontosságú elemeket, amelyeket bele kell foglalni a NKBS-be, nevezetesen a kívánt eredményeket, vagy ahogy az irányelv 7. cikke (1) bekezdésének a) pontja fogalmaz, a *„célokat és prioritásokat”*, azt, hogy ezek az eredmények miként egészítik ki a nemzeti szociális és gazdaságpolitikákat, és azt, hogy ezek összeegyeztethetők-e az Európai Unió tagállamának jogállásából fakadó kiváltságokkal és kötelezettségekkel. A céloknak konkrétnak, mérhetőnek, teljesíthetőnek, reálisnak és határidőhöz kötöttnek (SMART) kell lenniük. Ezt szemlélteti a következő példa: „*Gondoskodni fogunk arról, hogy ez a [határidőhöz kötött] stratégia szigorú és átfogó mérőszámokon alapuljon, amelyekkel mérni fogjuk az elérendő eredmények elérése irányába elért előrelépést*”[5].

A fentiek politikai értékelést is magukban foglalnak arra vonatkozóan, hogy lehet-e jelentős költségvetési forrásokat biztosítani a stratégia végrehajtására. Szükségessé teszik továbbá a stratégia tervezett hatályának, valamint a köz- és a magánszférába tartozó érdekelt felek különböző kategóriáinak a leírását is, amelyeket be kell vonni a különböző célkitűzések és intézkedések kidolgozásába.

Ez az első lépés elérhető magas beosztású minisztériumi tisztviselőkkel és politikusokkal tartott célzott munkaértekezletek révén, amelyeken a moderátor szerepét olyan, professzionális kommunikációs készségekkel rendelkező kiberbiztonsági szakemberek töltik be, akik rá tudnak világítani arra, hogy egy modern digitális gazdaság és társadalom számára milyen következményekkel jár, ha nincs, vagy gyenge a kiberbiztonság.

Második lépés – **A stratégia tartalmának kidolgozása.**

A stratégiának tartalmaznia kell támogató intézkedéseket, határidőkön alapuló intézkedéseket, valamint fő teljesítménymutatókat, amelyek a meghatározott végrehajtási időszakot követő értékelést, pontosítást és továbbfejlesztést szolgálják. Ezeknek az intézkedéseknek támogatniuk kell az alapelvként meghatározott célkitűzést, prioritásokat és eredményeket. A támogató intézkedések szükségességét a kiberbiztonsági irányelv 7. cikke (1) bekezdésének c) pontja írja elő.

[5] Kivonat az Egyesült Királyság nemzeti kiberbiztonsági stratégiájából (2016–2021), 67. oldal.

Ajánlott, hogy a szövegezési folyamat irányítása és az előkészületekben való részvétel megkönnyítése érdekében hozzanak létre irányítóbizottságot, amelynek az elnökségét a vezető minisztérium biztosítja. Ezt több, az érintett tisztviselőkből és szakértőkből álló szerkesztői csoport révén lehetne elérni, amelyek olyan kiemelt általános témákkal foglalkoznának, mint például a kockázatértékelés, a vészhelyzeti tervezés, a biztonsági események kezelése, a készségfejlesztés, a tudatosság növelése, valamint a kutatás és az ipari fejlesztés stb. Minden egyes ágazatot (például az energiaipart, a közlekedési ágazatot stb.) külön-külön felkérnének arra, hogy értékeljék a felvételük következményeit, beleértve az erőforrások biztosítását, és vonják be a kijelölt, alapvető szolgáltatásokat nyújtó szereplőket és a kulcsfontosságú digitális szolgáltatókat a prioritások meghatározásába és a szövegezési folyamattal összefüggésben a javaslatok benyújtásába. Az ágazati szereplők bevonása azt figyelembe véve is alapvető fontosságú, hogy biztosítani kell az irányelvnek a különböző ágazatok között összehangolt végrehajtását, ugyanakkor az ágazatspecifikus sajátosságokra is tekintettel kell lenni.

Harmadik lépés – **Az irányítási keretrendszer kidolgozása.**

A hatékonyság és eredményesség érdekében az irányítási keretnek a kiemelt érdekelt feleken, a szövegezési folyamat során meghatározott prioritásokon, valamint a nemzeti közigazgatási és politikai struktúrák korlátain és összefüggésein kell alapulnia. Kívánatos, hogy a keretrendszer közvetlenül számoljon be a politikai szintnek, rendelkezzen döntéshozatali és erőforrás-elosztási hatáskörrel, valamint használja fel a kiberbiztonsági szakértők és az ágazati érdekelt felek által biztosított információkat. A kiberbiztonsági irányelv 7. cikke (1) bekezdésének b) pontja utal az irányítási keretrendszerre, és kifejezetten előírja „a kormányzati szervek és egyéb érintett szereplők [...] felelősségét”.

Negyedik lépés – **A stratégiatervezet összeállítása és felülvizsgálata.**

Ebben a szakaszban a stratégiatervezetet össze kell állítani, és a gyengeségek, erősségek, lehetőségek és veszélyek (GYELV) elemzése alapján felül kell vizsgálni, ami segíthet eldönteni, hogy szükség van-e a tartalom felülvizsgálatára. A belső felülvizsgálatot követően az érdekelt felekkel való konzultációra kerül sor. Fontos, hogy nyilvános konzultációra is sor kerüljön annak érdekében, hogy felhívják a közvélemény figyelmét a javasolt stratégia jelentőségére, minden lehetséges forrásból érkezzen információ, és támogatást kapjanak a stratégia későbbi végrehajtásához szükséges erőforrások biztosításához.

Ötödik lépés – **Hivatalos elfogadás.**

Ez az utolsó lépés politikai szintű hivatalos elfogadást foglal magában az érintett tagállam által a kiberbiztonságnak tulajdonított fontosságot tükröző támogató költségvetéssel együtt. A kiberbiztonsági irányelv céljainak elérése érdekében, valamint a nemzeti stratégiai dokumentumnak a 7. cikk (3) bekezdése szerint a Bizottsággal való közlése kapcsán a Bizottság arra ösztönzi a tagállamokat, hogy nyújtsanak tájékoztatást a költségvetésről. A költségvetésre és a szükséges humánerőforrásokra vonatkozó kötelezettségvállalások

elengedhetetlenek a stratégia és az irányelv hatékony végrehajtásához. Mivel a kiberbiztonság még mindig meglehetősen 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.

A nemzeti stratégiák kidolgozásának folyamatára és tartalmára vonatkozó tanácsadás különböző nyilvános és tudományos forrásokból, például az ENISA-tól[6], az ITU-tól[7], az OECD-től[8], a számítástechnikai szakértők világfórumától (GFCE) és az Oxfordi Egyetemtől[9] is elérhető.

2.4. Konkrét lépések, amelyeket a tagállamoknak az átültetési határidő előtt el kell végezniük.

Az irányelv elfogadását megelőzően szinte már valamennyi tagállam[10] közzétette az NKBS-ként megjelölt dokumentumokat. E melléklet 6. pontja felsorolja az egyes tagállamokban jelenleg alkalmazott stratégiákat[11]. Ezek általában stratégiai elveket, iránymutatásokat és célokat foglalnak magukban, egyes esetekben pedig a kiberbiztonsághoz kapcsolódó kockázatok csökkentésére irányuló konkrét intézkedéseket.

Mivel e stratégiák némelyikét a kiberbiztonsági irányelv elfogadását megelőzően fogadták el, ezek nem feltétlenül tartalmazzák a 7. cikk által előírt valamennyi elemet. A helyes átültetés biztosítása érdekében a tagállamoknak hiányelemzést kell végezniük, ehhez pedig az NKBS-ük tartalmát össze kell vetniük a 7. cikkben felsorolt hét különböző követelménnyel az irányelv II. mellékletében felsorolt ágazatok és III. mellékletében felsorolt szolgáltatások körén belül. Az azonosított hiányosságokat a meglévő NKBS felülvizsgálatával, illetve a nemzeti hálózat- és információbiztonsági stratégia elveinek teljes körű felülvizsgálatáról szóló

---

[6] ENISA, *National Cyber-Security Strategy Good Practice* (A nemzeti kiberbiztonsági stratégiával kapcsolatos bevált gyakorlat) (2016). Elérhető a következő címen: https://www.enisa.europa.eu/publications/ncss-good-practice-guide

[7] ITU, *National Cybersecurity Strategy Guide* (A nemzeti kiberbiztonsági stratégiával kapcsolatos iránymutatás) (2011). Elérhető a következő címen: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf
Az ITU 2017 folyamán nemzeti kiberbiztonsági stratégiai eszköztárat is közzé fog tenni (lásd a prezentációt a következő címen: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National%20Strategy%20Toolkit%20introduction.pdf).

[8] OECD, *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies* (A kiberbiztonsági szakpolitikai döntéshozatal fordulóponthoz érkezett: A nemzeti kiberbiztonsági stratégiák új generációjának elemzése) (2012). Elérhető a következő címen: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

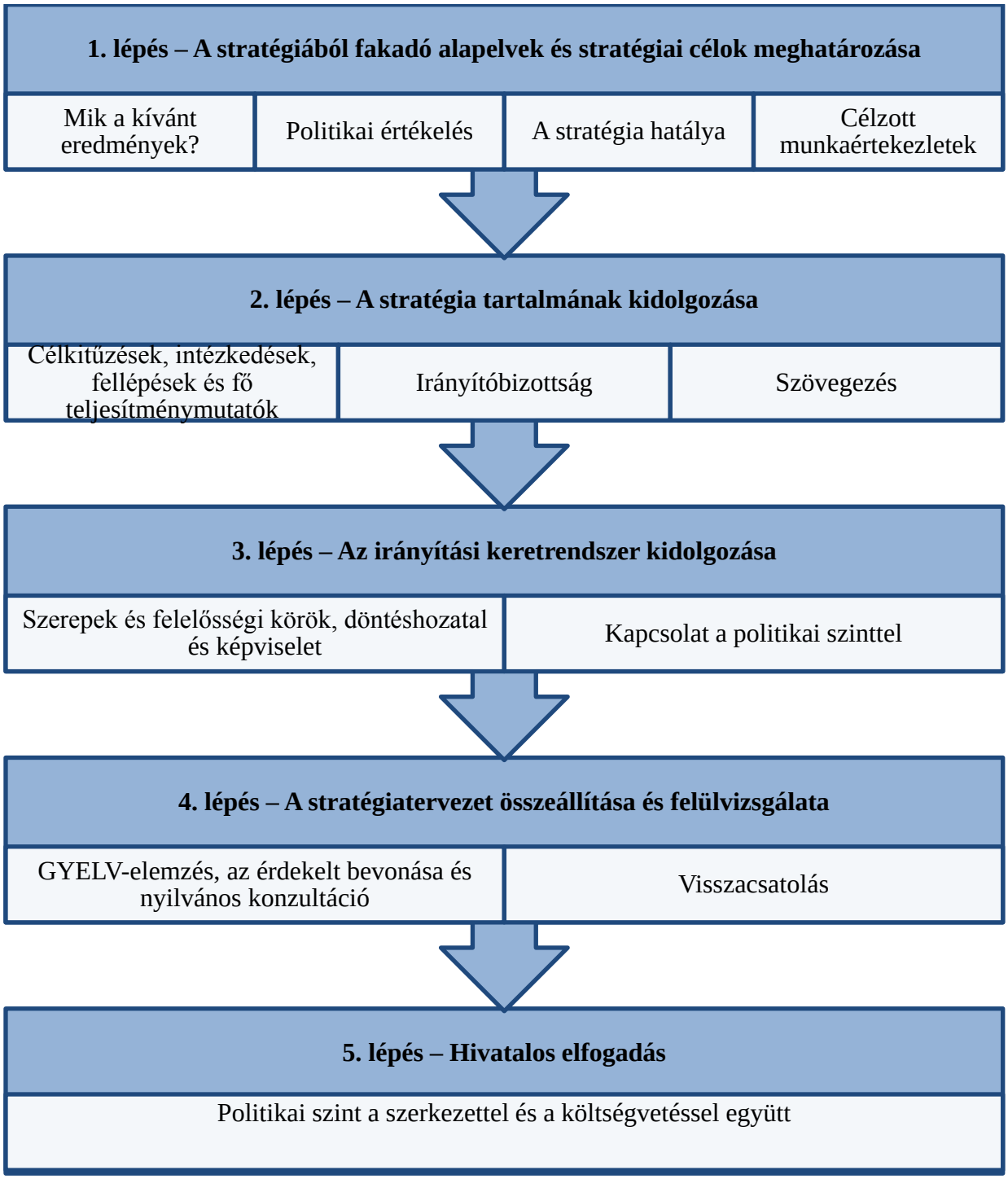
[9] Global Cyber Security Capacity Centre (Globális kiberbiztonsági kapacitásépítési központ) és Oxfordi Egyetem, *Cybersecurity Capacity Maturity Model for Nations (A kiberbiztonsági kapacitás kiforrottságának modellje a nemzetek számára), javított kiadás* (2016). Elérhető a következő címen: https://www.thegfce.com/binaries/gfce/documents/publications/2017/02/13/cybersecurity-cmm-for-nations/CMM+revised+edition.pdf

[10] Görögország kivételével, ahol 2014 óta dolgoznak a nemzeti kiberbiztonsági stratégián (lásd: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-greece/view).

[11] Ez az információ az NKBS-eknek az ENISA által készített áttekintésén alapul, lásd: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

döntéssel lehet megoldani. Az NKBS elfogadására szolgáló folyamatra vonatkozó, fent említett iránymutatások a meglévő NKBS felülvizsgálatára és aktualizálására is vonatkoznak.

1. ábra: Az NKBS elfogadásának 5 lépésből álló folyamata



3. A kiberbiztonsági irányelv: Az illetékes nemzeti hatóságok, az egyedüli kapcsolattartó pontok és a számítógép-biztonsági eseményekre reagáló csoportok (CSIRT-ek).

A 8. cikk (1) bekezdése értelmében a tagállamoknak ki kell jelölniük az irányelv alkalmazásának nyomon követésére egy vagy több illetékes nemzeti hatóságot, amelyek legalább az irányelv II. mellékletében említett ágazatokkal és az irányelv III. mellékletében

említett szolgáltatásokkal foglalkoznak. A tagállamok már létező hatóságot vagy hatóságokat is megbízhatnak ezzel a feladattal.

Ez a pont arra összpontosít, hogy a kiberbiztonsági irányelv miként erősíti a tagállamok felkészültségét azáltal, hogy előírja számukra, hogy rendelkezniük kell hatékonyan működő nemzeti illetékes hatóságokkal és számítógép-biztonsági eseményekre reagáló csoportokkal (CSIRT-ekkel). Pontosabban fogalmazva ez a pont foglalkozik a nemzeti illetékes hatóságok kijelölésének kötelezettségével, beleértve az egyedüli kapcsolattartó pont szerepét. Három témát tárgyal: a) a lehetséges nemzeti irányítási struktúrákat (pl. centralizált, decentralizált modellek stb.) és egyéb követelményeket; b) az egyedüli kapcsolattartó pont szerepét és c) a számítógép-biztonsági eseményekre reagáló csoportokat.

3.1. A hatóságok típusa

A kiberbiztonsági irányelv 8. cikke előírja a tagállamok számára, hogy jelöljenek ki a hálózati és információs rendszerek biztonságáért felelős nemzeti illetékes hatóságot, ugyanakkor kifejezetten elismerik annak lehetőségét, hogy „egy vagy több [...] nemzeti illetékes hatóságot” jelöljenek ki. Az irányelv (30) preambulumbekezdése fejti ki ezt a szakpolitikai döntést: „*Tekintettel a nemzeti kormányzási struktúrák közötti különbségekre, valamint a meglévő ágazati intézkedések vagy az uniós felügyeleti és szabályozó szervek megőrzése és az átfedések elkerülése érdekében a tagállamoknak lehetőséget kell kapniuk arra, hogy az ezen irányelv hatálya alá tartozó alapvető szolgáltatásokat nyújtó szereplők és digitális szolgáltatók hálózati és információs rendszereinek biztonságával összefüggő feladatok ellátására egynél több nemzeti illetékes hatóságot jelöljenek ki.*”

Ennek megfelelően a tagállamok szabadon dönthetnek úgy, hogy egy központi hatóságot jelölnek ki, amely az irányelv hatálya alá tartozó valamennyi ágazattal és szolgáltatással foglalkozik, vagy több hatóságot, például az ágazat típusától függően.

A megközelítésre vonatkozó döntés meghozatalakor a tagállamok felhasználhatják a kritikus információs infrastruktúrák védelemére vonatkozó meglévő jogszabályok keretében alkalmazott nemzeti megközelítésekkel kapcsolatban szerzett tapasztalatokat. Amint az 1. táblázatból kiderül, a kritikus információs infrastruktúrák védelme esetében a tagállamok, amikor a hatásköröket nemzeti szinten kijelölték, centralizált vagy decentralizált megközelítést fogadtak el. A tagállami példák itt csak tájékoztató jelleggel szerepelnek azzal a céllal, hogy felhívják a tagállamok figyelmét a meglévő szervezeti keretekre. A Bizottság tehát nem akarja azt sugallni, hogy az egyes országok által a kritikus információs infrastruktúrák védelme tekintetében használt modellt kell szükségképpen használni a kiberbiztonsági irányelv átültetéséhez.

A tagállamok különböző hibrid megoldásokat is választhatnak, amelyek mind a centralizált, mind a decentralizált megközelítések elemeit magukban foglalják. A döntéseket meg lehet hozni az irányelv hatálya alá tartozó különböző ágazatokra és szolgáltatásokra vonatkozó meglévő nemzeti irányítási intézkedésekkel összhangban, vagy meghozhatják azokat újonnan az érintett hatóságok, valamint az alapvető szolgáltatásokat nyújtó szereplőként vagy digitális szolgáltatóként azonosított érintett érdekelt felek. A kiberbiztonsággal, az erőforrások

biztosításával összefüggő megfontolásokkal, valamint az érdekelt felek és a nemzeti érdekek (például a gazdasági fejlődés, a közbiztonság stb.) közötti kapcsolatokkal kapcsolatos szakértelem megléte szintén fontos tényező lehet a tagállamok döntéseinek meghozatalában.

3.2. Nyilvánosság és további lényeges szempontok

A 8. cikk (7) bekezdésének értelmében a tagállamoknak tájékoztatniuk kell a Bizottságot az illetékes nemzeti hatóságok kijelöléséről és feladataikról. Ezt az átültetés határidejéig meg kell tenni.

A kiberbiztonsági irányelv 15. és 17. cikke előírja a tagállamok számára, hogy gondoskodjanak arról, hogy az illetékes hatóságok rendelkezzenek az e cikkekben meghatározott feladatok elvégzéséhez szükséges konkrét hatáskörökkel és eszközökkel.

Ezenkívül nyilvánosságra kell hozni az egyes jogalanyok nemzeti illetékes hatóságként való kijelölését. Az irányelv nem határozza meg, hogy a nyilvánosságra hozatal milyen módon történjék. Tekintettel arra, hogy ennek a követelménynek az a célja, hogy a kiberbiztonsági irányelv hatálya alá tartozó szereplők és a közvélemény tájékozottsága magas szintet érjen el, valamint a más ágazatokban (távközlés, banki szolgáltatások, gyógyszerek) szerzett tapasztalatok alapján a Bizottság úgy véli, hogy ez megvalósítható például egy jól meghirdetett portál segítségével.

A kiberbiztonsági irányelv 8. cikkének (5) bekezdése előírja, hogy az ilyen hatóságoknak „elegendő erőforrással” kell rendelkezniük az irányelv által kijelölt feladatok elvégzéséhez.

1. táblázat: A kritikus információs infrastruktúrák védelmére vonatkozó nemzeti megközelítések

2016-ban az ENISA tanulmányt[12] tett közzé a tagállamok által a kritikus információs infrastruktúrák védelme érdekében alkalmazott különböző megközelítésekről. A kritikus információs infrastruktúrák védelmének tagállami irányítására vonatkozóan két profil létezik, amelyek a kiberbiztonsági irányelv átültetésével összefüggésben is használhatók.

1. profil: Decentralizált megközelítés – több, az irányelv II. és III. mellékletében említett meghatározott egyes ágazatok és szolgáltatások tekintetében illetékes ágazati hatóság

A decentralizált megközelítést a következők jellemzik:

i. a szubszidiaritás elve;
ii. az állami ügynökségek közötti szoros együttműködés;
iii. ágazatspecifikus jogszabályok.

A szubszidiaritás elve

A decentralizált megközelítés egyetlen, átfogó felelősséggel bíró ügynökség létrehozása vagy kijelölése helyett a szubszidiaritás elvét követi. Ez azt jelenti, hogy a végrehajtás felelőssége olyan ágazati hatóság kezében van, amely a legjobban érti a helyi ágazatot, és már kialakult kapcsolatokkal rendelkezik az érdekeltekkel. Ezen elv értelmében a döntéseket azok hozzák, akik a legközelebb állnak azokhoz, akikre a döntések hatást gyakorolnak.

Az állami ügynökségek közötti szoros együttműködés

A kritikus információs infrastruktúrák védelmével foglalkozó állami ügynökségek sokfélesége miatt számos tagállam együttműködési rendszereket dolgozott ki a különböző hatóságok munkájának és erőfeszítéseinek koordinálása érdekében. Ezek az együttműködési rendszerek informális hálózatok vagy fokozottabb mértékben intézményesített fórumok vagy megállapodások formáját ölthetik. Ezek az együttműködési rendszerek azonban csak a különböző állami ügynökségek közötti információcserére és koordinációra szolgálnak, de nem rendelkeznek felettük hatáskörrel.

Ágazatspecifikus jogszabályok

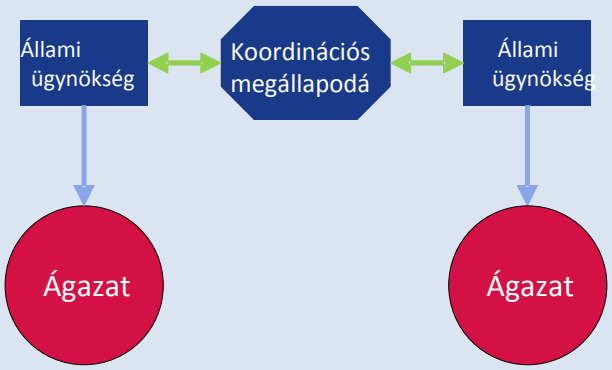
A kritikus ágazatokban a decentralizált megközelítést alkalmazó országok gyakran tartózkodnak a kritikus információs infrastruktúrák védelmére irányuló jogalkotástól. Ehelyett továbbra is ágazatspecifikus törvényeket és rendeleteket fogadnak el, amelyek nagy eltéréseket mutathatnak az ágazatok között. Ez a megközelítés azzal az előnnyel jár, hogy a hálózat- és információbiztonsággal kapcsolatos intézkedéseket összehangolja a meglévő ágazati szabályozásokkal, és ezáltal javítja mind az ágazat általi elfogadást, mind pedig az érintett

[12] ENISA, *Stocktaking, Analysis and Recommendations on the protection of CIIs* (A kritikus információs infrastruktúrák védelmével kapcsolatos helyzetfelmérés, elemzés és ajánlások) (2016). Elérhető a következő címen: https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis

hatóság általi végrehajtás hatékonyságát.

Tisztán decentralizált megközelítést követve jelentős a kockázata annak, hogy az irányelv alkalmazása kevésbé egységesen valósul meg a különféle ágazatok és szolgáltatások esetében. Erre az esetre az irányelv egyedüli nemzeti kapcsolattartó pontról rendelkezik a határokon átnyúló ügyekben való kapcsolattartás céljából, és ezt a szervet az érintett tagállam az irányelv 10. cikkével összhangban azzal is megbízhatja, hogy belső koordinációt és együttműködést folytasson több nemzeti illetékes hatósággal.

2. ábra – decentralizált megközelítés



Példák a decentralizált megközelítésre.

Svédország jó példa az olyan országokra, amelyek a kritikus információs infrastruktúrák védelme tekintetében decentralizált megközelítést követnek. Az ország „rendszerszempontú” megközelítést alkalmaz, ami azt jelenti, hogy a kritikus információs infrastruktúrák védelmének fő feladatai, mint például a létfontosságú szolgáltatások és a kritikus infrastruktúrák azonosítása, a szolgáltatók koordinációja és támogatása, a szabályozási feladatok, valamint a veszélyhelyzeti felkészültségre vonatkozó intézkedések különböző ügynökségek és települések hatáskörébe tartoznak. Ezen ügynökségek között szerepel a svéd polgári védelmi ügynökség (MSB), a svéd postai és távközlési ügynökség (PTS), valamint több svéd védelmi, katonai és bűnüldöző szerv.

A különböző ügynökségek és közigazgatási intézmények tevékenységeinek összehangolása érdekében a svéd kormány együttműködési hálózatot hozott létre a „sajátos társadalmi információbiztonsági feladatokkal” megbízott hatóságokból. Ez az információbiztonsági együttműködési munkacsoport (SAMFI) a különböző hatóságok képviselőiből áll, és évente többször ülésezik a nemzeti információbiztonsággal kapcsolatos kérdések megvitatása céljából. A SAMFI által tárgyalt témakörök főként a politikai-stratégiai területekhez tartoznak, és olyan témákat érintenek, mint a technikai kérdések és a szabványosítás, a nemzeti és nemzetközi fejlesztés az információbiztonság területén, illetve az informatikai események kezelése és megelőzése. (Svéd polgári védelmi ügynökség (MSB) 2015)

Svédország nem tett közzé olyan, a kritikus információs infrastruktúrák védelméről szóló központi törvényt, amely az ágazatokon átívelve vonatkozna a kritikus információs infrastruktúrák üzemeltetőire. Ehelyett az egyes ágazatokba tartozó vállalatokra vonatkozó jogszabályok kidolgozása az illetékes közigazgatási szervek hatáskörébe tartozik. Például az MSB-nek jogában áll szabályozást kiadni a kormányzati hatóságok számára az információbiztonság területén, a PTS pedig másodlagos jogszabályok alapján előírhatja a szolgáltatók számára, hogy egyes műszaki vagy szervezési biztonsági intézkedéseket meghozzanak.

Írország is azokra az országokra példa, amelyek e profil jellemzőit mutatják. Írország a „szubszidiaritás elvét” követi, amelynek értelmében minden minisztérium maga felelős a saját ágazatán belüli kritikus információs infrastruktúrák azonosításáért és a kockázatértékelésért. Ezenkívül nemzeti szinten nem hoztak külön rendelkezéseket a kritikus információs infrastruktúrák védelmére vonatkozóan. A jogalkotás továbbra is ágazati jellegű, és főleg az energia- és a távközlési ágazat tekintetében léteznek jogszabályok (2015). További példa Ausztria, Ciprus és Finnország.

2. profil: Centralizált megközelítés – az irányelv II. és III. mellékletében említett valamennyi ágazat és szolgáltatás tekintetében illetékes egyetlen központi hatóság

A centralizált megközelítést a következők jellemzik:

i. az ágazatokon átívelő központi hatóság;
ii. átfogó jogszabályok.

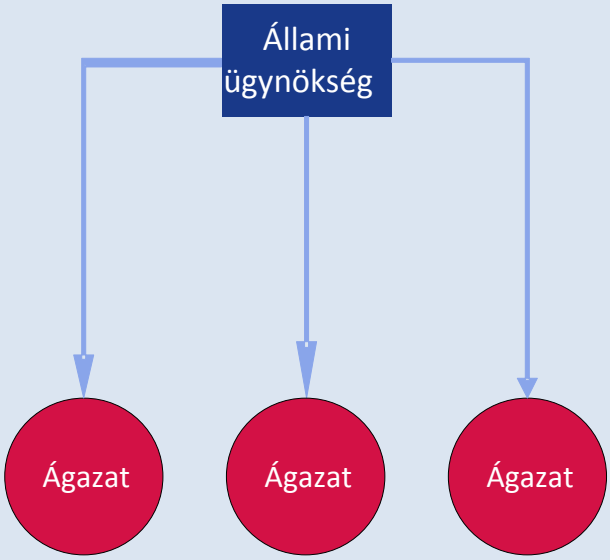
Az ágazatokon átívelő központi hatóság.

Azok a tagállamok, amelyek centralizált megközelítést követnek, olyan hatóságokat hoztak létre, amelyek több vagy valamennyi kritikus ágazat tekintetében feladatkörrel és széles hatáskörrel rendelkeznek, vagy a meglévő hatóságok hatáskörét terjesztették ki. A kritikus információs infrastruktúrák védelméért felelős fő hatóságok több feladatért – például a vészhelyzeti tervezésért, a vészhelyzetkezelésért, a szabályozási feladatokért és a magánszolgáltatók támogatásáért – is felelősek. Számos esetben a nemzeti vagy kormányzati CSIRT része a kritikus információs infrastruktúrák védelméért felelős fő hatóságnak. Tekintettel a kiberbiztonsági szakértelem általános hiányára, egy központi hatóság valószínűleg több kiberbiztonsági szakértőt képes összegyűjteni, mint több ágazati hatóság együtt.

Átfogó jogszabályok.

Egy átfogó jogszabály minden ágazatban kötelezettségeket és követelményeket keletkeztet a kritikus információs infrastruktúrák valamennyi szolgáltatója számára. Ez új átfogó jogszabályok vagy a meglévő ágazatspecifikus rendeletek kiegészítése révén érhető el. Ez a megközelítés elősegítené a kiberbiztonsági irányelv következetes alkalmazását az összes érintett ágazatban és szolgáltatásban. Ezzel kiküszöbölhető lenne a végrehajtás terén kialakuló hiányosságok kockázata, amelyek több, egyedi hatáskörrel rendelkező hatóság léte esetén merülhetnének fel.

3. ábra – Centralizált megközelítés



Példák a centralizált megközelítésre

Franciaország jó példa a centralizált megközelítést alkalmazó uniós tagállamokra. Az információs rendszerek biztonságáért felelős francia állami ügynökséget (Agence Nationale de la Sécurité des Systèmes d'Information, ANSSI) 2011-ben nyilvánították az információs rendszerek védelméért felelős fő nemzeti hatóságnak. Az ANSSI erős felügyeleti szerepet tölt be a „létfontosságú gazdasági szereplők" (OIV-k) tekintetében: az ügynökség utasíthatja az OIV-ket a biztonsági intézkedéseknek való megfelelésre, és jogosult biztonsági ellenőrzéseknek alávetni azokat. Ezenkívül az ügynökség az egyedüli kapcsolattartó pont az OIV-k számára, amelyek kötelesek jelenteni a biztonsági eseményeket az ügynökségnek.

Biztonsági események esetén az ANSSI a kritikus információs infrastruktúrák védelméért felelős ügynökségként jár el, és dönt arról, hogy a szereplőknek milyen intézkedéseket kell megtenniük a válság kezelése érdekében. A kormány tevékenységeit is az ANSSI műveleti

központjában koordinálják. A veszélyek felderítését és a biztonsági eseményekre való operatív szintű reagálást az CERT-FR végzi, amely az ANSSI része.

Franciaország átfogó jogi keretet hozott létre a kritikus információs infrastruktúrák védelmére. A miniszterelnök 2006-ban elrendelte a kritikus fontosságú infrastrukturális ágazatok jegyzékének összeállítását. E jegyzék alapján, amely tizenkét létfontosságú ágazatot azonosított, a kormány mintegy 250 OIV-t határozott meg. 2013-ban kihirdetésre került a katonai programozási törvény (LPM)[13]. A szóban forgó törvény különböző kötelezettségeket határoz meg az OIV-k számára, például a biztonsági események jelentésére és a biztonsági intézkedések végrehajtására vonatkozóan. Ezek a követelmények minden ágazatban valamennyi OIV számára kötelező erejűek (Francia szenátus, 2013).

3.3. A kiberbiztonsági irányelv 9. cikke: Számítógép-biztonsági eseményekre reagáló csoportok (CSIRT-ek)

A 9. cikk értelmében a tagállamoknak ki kell jelölniük egy vagy több CSIRT-et, amely(ek) megbízást kap(nak) a kiberbiztonsági irányelv II. mellékletében felsorolt ágazatokkal és III. mellékletében felsorolt szolgáltatásokkal kapcsolatos kockázatok és biztonsági események kezelésére. Figyelembe véve az irányelv 3. cikkében foglalt, a harmonizáció minimumára vonatkozó követelményt, a tagállamok szabadon alkalmazhatják a CSIRT-eket más, az irányelv hatálya alá nem tartozó ágazatok, például a közigazgatás tekintetében is.

A tagállamok dönthetnek úgy is, hogy a nemzeti illetékes hatóságon belül hoznak létre CSIRT-et[14].

3.4. Feladatok és követelmények

A kijelölt CSIRT-eknek a kiberbiztonsági irányelv I. mellékletében meghatározott feladatai a következőket foglalják magukban:

- a biztonsági események nemzeti szintű monitoringja,
- a kockázatokkal és biztonsági eseményekkel kapcsolatos korai előrejelzés, riasztás, bejelentéstétel és információterjesztés a releváns érdekeltek számára,
- reagálás a biztonsági eseményekre,
- dinamikus kockázat- és eseményelemzés, valamint helyzetkép nyújtása, valamint
- részvétel a nemzeti CSIRT-ek 12. cikk szerint létrehozott hálózatában (CSIRT-hálózat).

[13] La loi de programmation militaire.
[14] Lásd a 9. cikk (1) bekezdésének utolsó mondatát.

További feladatokat ír elő a 14. cikk (3), (5) és (6) bekezdése, valamint a 16. cikk (3), (6) és (7) bekezdése a biztonsági események bejelentésével kapcsolatban arra az esetre, ha egy tagállam úgy határoz, hogy a nemzeti illetékes hatóságok mellett vagy helyett a CSIRT-ek is betölthetnek ilyen szerepeket.

A tagállamoknak az irányelv átültetése során a biztonsági események bejelentésére vonatkozó követelményekkel összefüggésben választási lehetőségeik vannak arra vonatkozóan, hogy a CSIRT-ek milyen szerepet játsszanak. Lehetséges az, hogy a kötelező jelentéstétel közvetlenül a CSIRT-eknek történjen, ami az adminisztratív hatékonyság szempontjából jár előnyökkel, vagy ehelyett a tagállamok dönthetnek úgy is, hogy a jelentéstétel közvetlenül a nemzeti illetékes hatóságoknak történjen, a CSIRT-ek pedig hozzáférési joggal rendelkezzenek a bejelentett információkhoz. A CSIRT-ek végső soron az érdekelt felekkel együtt a kiberbiztonsági események (ezen belül a kötelező jelentéstétel szempontjából nem kritikus fontosságú események) megakadályozásához, felderítéséhez, az azokra való reagáláshoz és azok hatásának enyhítéséhez kapcsolódó problémamegoldásban érdekeltek, míg a szabályozásnak való megfelelés a nemzeti illetékes hatóságok hatáskörébe tartozik.

Az irányelv 9. cikkének (3) bekezdése értelmében a tagállamoknak gondoskodniuk kell arról, hogy a CSIRT-ek biztonságos és ellenállóképes IKT-infrastruktúrát használhassanak.

Az irányelv 9. cikkének (4) bekezdése előírja a tagállamok számára, hogy tájékoztassák a Bizottságot a kijelölt CSIRT-ek hatásköréről, valamint a biztonsági események kezelésére szolgáló eljárás főbb elemeiről.

A tagállamok által kijelölt CSIRT-ekre vonatkozó követelményeket a kiberbiztonsági irányelv I. melléklete tartalmazza. A CSIRT-eknek biztosítaniuk kell hírközlési szolgáltatásaik magas szintű elérhetőségét. Hivatali helyiségeiket és a támogató információs rendszereket biztonságos helyszíneken kell elhelyezni, és tudniuk kell biztosítani az üzletmenet folytonosságát. Emellett a CSIRT-ek számára lehetővé kell tenni, hogy nemzetközi együttműködési hálózatokban vegyenek részt.

3.5. Segítségnyújtás a CSIRT-ek fejlesztéséhez

Az Európai Hálózatfinanszírozási Eszköz (CEF) kiberbiztonsággal foglalkozó digitális szolgáltatási infrastruktúra (DSI) programja jelentős mértékű uniós finanszírozást biztosíthat a tagállami CSIRT-ek számára annak érdekében, hogy javítsák képességeiket és információcsere-együttműködési mechanizmus révén együttműködjenek egymással. A SMART 2015/1089 projekt keretében kidolgozás alatt álló együttműködési mechanizmus célja az önkéntes alapon működő, gyors és hatékony operatív együttműködés elősegítése a tagállami CSIRT-ek között, nevezetesen az irányelv 12. cikke alapján a CSIRT-ek hálózatára bízott feladatok támogatása érdekében.

A tagállami CSIRT-ek kapacitásépítésére vonatkozó pályázati felhívások részletei az Európai Bizottság Innovációs és Hálózati Projektek Végrehajtó Ügynökségének (INEA) honlapján érhetők el[15].

A CEF kiberbiztonsági digitális szolgáltatási infrastruktúrával foglalkozó irányító testülete a tagállami CSIRT-eknek nyújtott szakpolitikai szintű iránymutatás és segítségnyújtás érdekében informális struktúrát biztosít a kapacitásépítéshez és az önkéntes együttműködési mechanizmus végrehajtásához.

Az újonnan létrehozott vagy a kiberbiztonsági irányelv I. mellékletében meghatározott feladatok ellátására kijelölt CSIRT-ek teljesítményük javítása és munkájuk hatékony elvégzése érdekében az ENISA tanácsadására és szakértelmére is támaszkodhat[16]. E tekintetben meg kell jegyezni, hogy a tagállami CSIRT-ek hivatkozási alapul vehetik az ENISA által a közelmúltban elvégzett munka egyes részeit. Közelebbről nézve az ügynökség az e melléklet 7. pontjában felsoroltak szerint több olyan dokumentumot és tanulmányt is közzétett, amelyek a CSIRT-ek különböző képességeire és szolgáltatásaira vonatkozóan bevált gyakorlatokat, valamint technikai szintű ajánlásokat írnak le, beleértve a CSIRT-ek kiforrottságának mértékére vonatkozó értékeléseket. Emellett a CSIRT-ek hálózatai világszinten (FIRST[17]) és európai szinten (Trusted Introducer, TI[18]) egyaránt megosztják egymással az iránymutatásokat és a legjobb gyakorlatokat.

3.6. Az egyedüli kapcsolattartó pont szerepe

A kiberbiztonsági irányelv 8. cikkének (3) bekezdése értelmében minden tagállamnak ki kell jelölnie egy egyedüli kapcsolattartó pontot, amely ellátja az összekötő szerepét a többi tagállam illetékes hatóságaival, valamint az együttműködési csoporttal és az irányelv által létrehozott CSIRT-hálózattal[19] való, határokon átnyúló együttműködés biztosítása érdekében. A (31) preambulumbekezdés és a 8. cikk (4) bekezdése kifejti, hogy e követelményt mi indokolja, nevezetesen a határokon átnyúló együttműködés és kommunikáció megkönnyítése. Erre különösen azért van szükség, mert a tagállamok dönthetnek úgy, hogy egynél több nemzeti hatóságot hoznak létre. Így az egyedüli kapcsolattartó pont megkönnyítené a különböző tagállamok hatóságainak azonosítását és együttműködését.

Az egyedüli kapcsolattartó pont összekötő szerepe valószínűleg olyan esetekben jár együtt az együttműködési csoport és a CSIRT-hálózat titkárságaival való együttműködéssel, amikor a nemzeti egyedüli kapcsolattartó pont nem CSIRT és nem is tagja az együttműködési csoportnak. Emellett a tagállamoknak biztosítaniuk kell, hogy az egyedüli kapcsolattartó pont tájékoztatást kapjon az alapvető szolgáltatásokat nyújtó szereplőktől és a digitális szolgáltatóktól kapott bejelentésekről[20].

---

[15] Elérhető a következő címen: https://ec.europa.eu/inea/en/connecting-europe-facility
[16] Lásd a kiberbiztonsági irányelv 9. cikkének (5) bekezdését.
[17] Forum of Incident Response and Security Teams (számítógép-biztonsági eseményekre reagáló és biztonsági csoportok fóruma) (https://www.first.org/)
[18] https://www.trusted-introducer.org/
[19] A nemzeti CSIRT-ek 12. cikk szerinti, a tagállamok közötti operatív együttműködést szolgáló hálózata.
[20] Lásd a 10. cikk (3) bekezdését.

Az irányelv 8. cikkének (3) bekezdése előírja, hogy amennyiben valamely tagállam centralizált megközelítést alkalmaz, azaz csak egy illetékes hatóságot jelöl ki, ez a hatóság fogja egyúttal az egyedüli kapcsolattartó pont szerepét is betölteni. Ha egy tagállam decentralizált megközelítést választ, akkor a különböző illetékes hatóságok közül kiválaszthatja az egyiket, hogy az járjon el egyedüli kapcsolattartó pontként. A választott intézményi modelltől függetlenül, amennyiben az illetékes hatóság, a CSIRT és az egyedüli kapcsolattartó különálló szervezetek, a tagállamok kötelesek az irányelvben meghatározott kötelezettségek teljesítése érdekében biztosítani közöttük a hatékony együttműködést[21].

Az egyedüli kapcsolattartó pontnak legkésőbb 2018. augusztus 9-ig, majd azt követően évente összefoglaló jelentést kell benyújtania az együttműködési csoporthoz a beérkezett bejelentésekről, amelynek tartalmaznia kell a bejelentések számát, a biztonsági események jellegét, valamint a hatóságok által hozott intézkedéseket, mint például más érintett tagállamok tájékoztatása az eseményről vagy megfelelő információk biztosítása a bejelentő vállalat számára az esemény kezeléséhez[22]. Az illetékes hatóság vagy a CSIRT kérésére az egyedüli kapcsolattartó pontnak továbbítania kell az alapvető szolgáltatásokat nyújtó szereplők bejelentéseit az események által érintett többi tagállam egyedüli kapcsolattartó pontjainak[23].

A tagállamoknak az átültetés határidejéig tájékoztatniuk kell a Bizottságot az egyedüli kapcsolattartó pont kijelöléséről és feladatairól. Az egyedüli kapcsolattartó pont kijelölését a nemzeti illetékes hatóságokéval megegyező módon közzé kell tenni. A Bizottság közzéteszi a kijelölt egyedüli kapcsolattartó pontok jegyzékét.

3.7. Szankciók

A 21. cikk lehetővé teszi a tagállamok számára, hogy döntsenek az alkalmazandó szankciók típusáról és jellegéről, azonban azoknak mindenképpen hatékonynak, arányosnak és visszatartó erejűnek kell lenniük. Más szóval a tagállamok elvileg szabadon dönthetnek a nemzeti jogszabályaikban megállapított szankciók maximális összegéről, de az összeget vagy százalékot úgy kell meghatározni, hogy a nemzeti hatóságok minden konkrét esetben hatékony, arányos és visszatartó erejű szankciókat tudjanak kiszabni, figyelembe véve a különböző tényezőket, mint például a jogsértés súlyosságát vagy gyakoriságát.

4. A biztonsági intézkedésekre és a biztonsági események bejelentésére vonatkozó kötelezettségek hatálya alá tartozó jogalanyok

Az irányelv 4. cikkének (4) bekezdésében és 4. cikkének (5) bekezdésében alapvető szolgáltatásokat nyújtó szereplőkként és digitális szolgáltatókként említett, a társadalom és a gazdaság szempontjából fontos szerepet betöltő jogalanyok kötelesek megfelelő biztonsági intézkedéseket tenni, és a súlyos biztonsági eseményeket az illetékes nemzeti hatóságoknak bejelenteni. Ennek az az oka, hogy a biztonsági események e szolgáltatásokra gyakorolt

[21] Lásd a 10. cikk (1) bekezdését.
[22] Ugyanott.
[23] Lásd a 14. cikk (5) bekezdését.

hatásai komoly veszélyt jelenthetnek a szóban forgó szolgáltatások működésére, ami jelentős fennakadásokat okozhat a gazdasági tevékenységekben és egészében véve a társadalomban, potenciálisan alááshatja a fogyasztói bizalmat, és jelentős kárt okozhat az Unió gazdaságának[24].

Ez a pont áttekintést nyújt a kiberbiztonsági irányelv II. és III. mellékletének hatálya alá tartozó szervezetekről, és felsorolja azok kötelezettségeit. A szöveg részletesen foglalkozik az alapvető szolgáltatásokat nyújtó szereplők azonosításával, tekintettel arra, hogy e folyamat rendkívül fontos a kiberbiztonsági irányelv EU-szerte történő összehangolt végrehajtása szempontjából. Ez a rész emellett részletes magyarázattal szolgál a digitális infrastruktúrákra és a digitális szolgáltatókra vonatkozó fogalommeghatározásokkal kapcsolatban. Végül megvizsgálja további ágazatok bevonásának lehetőségét, és további részleteket tartalmaz a digitális szolgáltatókra vonatkozó konkrét megközelítésről.

4.1. Az alapvető szolgáltatásokat nyújtó szereplők

A kiberbiztonsági irányelv nem határozza meg konkrétan, hogy hatálya alatt mely jogalanyok minősülnek alapvető szolgáltatásokat nyújtó szereplőknek. Ehelyett olyan kritériumokat tartalmaz, amelyeket a tagállamoknak az azonosítási eljárás lefolytatásához alkalmazniuk kell, amely eljárás során végül meghatározásra kerül, hogy a II. mellékletben felsorolt szervezetek közé tartozó vállalatok közül melyek azok, amelyek alapvető szolgáltatásokat nyújtó szereplőknek minősülnek, és ily módon az irányelv szerinti kötelezettségek hatálya alá tartoznak.

4.1.1. A kiberbiztonsági irányelv II. mellékletében felsorolt szervezetek típusai

A 4. cikk (4) bekezdésében szereplő meghatározás szerint alapvető szolgáltatásokat nyújtó szereplő az irányelv II. mellékletében felsorolt, az 5. cikk (2) bekezdésében foglalt követelményeknek megfelelő közjogi vagy magánjogi szervezet. A II. melléklet felsorolja azokat az ágazatokat, alágazatokat és szervezettípusokat, amelyek esetében minden tagállamnak el kell végeznie az 5. cikk (2) bekezdése szerinti azonosítási eljárást[25]. Ezen ágazatok közé tartozik az energia, a közlekedés, a banki szolgáltatások, az egészségügy, a vízellátás és a digitális infrastruktúra.

A „hagyományos ágazatokhoz” tartozó legtöbb szervezetre vonatkozóan az uniós jogszabályok jól kidolgozott fogalommeghatározásokat tartalmaznak, és a II. melléklet ezekre hivatkozik. A digitális infrastruktúra ágazatában azonban – amely a II. melléklet 7. pontjában szerepel –, beleértve az internetes exchange pontokat, a doménnévrendszereket és a legfelső szintű doménnév-nyilvántartókat, nem ez a helyzet. Ezért a fogalommeghatározások egyértelművé tétele érdekében az alábbi pontok részletes magyarázattal szolgálnak ezekről.

[24] Lásd a (2) preambulumbekezdést.
[25] Az azonosítási eljárás további részletei a 4.1.6. pontban olvashatók.

1) Internetes exchange pont (IXP)

Az internetes exchange pont fogalmát a 4. cikk (13) bekezdése határozza meg, és a (18) preambulumbekezdés pontosítja tovább, és olyan hálózati létesítményt jelent, amely elsősorban az internetes forgalomcsere megkönnyítése érdekében lehetővé teszi kettőnél több, egymástól független, autonóm rendszer összekapcsolását. Az internetes exchange pont egy olyan fizikai helyszínként is meghatározható, ahol több hálózat egy kapcsoló révén meg tudja osztani egymással az internetes forgalmat. Az IXP elsődleges célja, hogy a megosztáson keresztül lehetővé tegye a hálózatok közvetlen, nem pedig egy vagy több harmadik fél hálózatán keresztüli összekapcsolását. Az IXP biztosítója általában nem felelős az internetes forgalom irányításáért. A forgalom irányítását a hálózati szolgáltatók végzik. A közvetlen összekapcsolásnak számos előnye van, de a legfontosabbak a költségekkel, a várakozási idővel és a sávszélességgel kapcsolatosak. Az exchange ponton áthaladó forgalmat általában egyik fél sem számlázza ki, míg a hálózatban következő internetszolgáltató felé irányuló forgalmat kiszámlázzák. A közvetlen összekapcsolással – amely gyakran ugyanabban a városban található, mint a két hálózat – elkerülhető, hogy az adatoknak nagy távolságot kelljen megtenniük ahhoz, hogy egyik hálózatból egy másikba jussanak, és ily módon csökken a várakozási idő.

Meg kell jegyezni, hogy az IXP meghatározása nem terjed ki az olyan fizikai pontokra, amelyeknél csak két fizikai hálózat (azaz a hálózati szolgáltatók, mint például a BASE és a Proximus) kapcsolódik egymáshoz. Ezért az irányelv átültetése során a tagállamoknak különbséget kell tenniük az olyan szereplők között, amelyek több hálózatüzemeltető között segítik elő az összesített internetes forgalom cseréjét, és azok között, amelyek egyetlen hálózatüzemeltetőnek minősülnek, és összekapcsolásra vonatkozó megállapodás alapján fizikailag kapcsolják össze hálózatukat. Ez utóbbi esetben a hálózati szolgáltatók nem tartoznak a 4. cikk (13) bekezdésének meghatározása alá. Ezt a kérdést a (18) preambulumbekezdés tisztázza, amely kimondja, hogy az IXP-k nem biztosítanak hálózati hozzáférést, és nem működnek tranzitszolgáltatóként vagy adattovábbítóként sem. A szolgáltatók utolsó kategóriájába az olyan nyilvános hírközlő hálózatokat és/vagy szolgáltatásokat biztosító vállalkozások tartoznak, amelyekre a 2002/21/EK irányelv 13a. és 13b. cikkében foglalt biztonsági és bejelentési követelmények alkalmazandók, és amelyek ezért nem tartoznak a kiberbiztonsági irányelv hatálya alá[26].

2) Doménnévrendszer

A doménnévrendszer (DNS) a 4. cikk 14. pontja szerint „*olyan hierarchikusan felépülő elnevezési rendszer, amely a hálózatban doménnév lekérdezéseket szolgál ki*”. A DNS tulajdonképpen leírható úgy is, mint számítógépek, szolgáltatások vagy az internethez kapcsolódó bármely más forrás hierarchikusan felépülő elnevezési rendszere, amely lehetővé teszi a doménnnevek IP (internetprotokoll) -címekre történő kódolását. A rendszer fő feladata az, hogy a kijelölt doménneveket IP-címekre fordítsa. Ebből a célból a DNS adatbázist

[26] A kiberbiztonsági irányelv és a 2002/21/EK irányelv közötti kapcsolatról további részletek az 5.2. pontban olvashatók.

működtet, és névszervereket, illetve rezolvert használ annak érdekében, hogy lehetővé tegye a doménnevek IP-címekre történő „lefordítását”. A doménnevek kódolása a DNS-nek nem az egyetlen, de az egyik legfőbb feladata. A 4. cikk 14. pontjában szereplő jogi meghatározás a rendszernek a felhasználó szempontjából betöltött legfőbb szerepére összpontosít anélkül, hogy további műszaki részletekbe bocsátkozna például a domménnév-rendszer, a névszerverek, illetve a rezolverek működéséről. Végül a 4. cikk 15. pontja tisztázza, hogy kit kell a DNS-szolgáltatások nyújtójának tekinteni.

3) Legfelső szintű doménnév-nyilvántartó (TLD név-nyilvántartó).

A legfelső szintű doménnév-nyilvántartó a 4. cikk 16. pontjában szereplő meghatározás szerint olyan szervezet, amely egy konkrét legfelső szintű domén (TLD) alatti internetes doménnevek regisztrációját irányítja és működteti. A doménnevek irányítása és kezelése magában foglalja a TLD nevek IP-címekre történő kódolását.

Az IANA (internetes számkiosztó hatóság) felelős a DNS-gyökérzóna, az internetprotokoll-kezelés és más internetprotokoll-források globális koordinálásért. Az IANA feladata különösen az általános legfelső szintű doménnevek („gTLD”), például a „.com”, illetve az országkód szerinti legfelső szintű doménnevek (ccTLD), pl. a „.be” kiosztása az érintett szereplők (nyilvántartók) számára, valamint e doménnevek technikai és adminisztratív adatainak kezelése. Az IANA a kiosztott TLD-kről globális nyilvántartást vezet, és szerepet játszik a listának az internetes felhasználók részére világszerte történő megismertetésében, valamint az új TLD-k bevezetésében.

A nyilvántartások egyik fontos feladata, hogy a második szintű neveket hozzárendeljék TLD-jük keretében az úgynevezett regisztrálókhoz. Ezek a regisztrálók arra is jogosultak, hogy – amennyiben úgy döntenek – saját maguk osszanak ki harmadik szintű doménneveket. Az országkód szerinti legfelső szintű doménnevek az ISO 3166-1 szabvány szerint egy adott országot vagy területet jelölnek. Az „általános” TLD-k általában nem kapcsolódnak földrajzi helyhez vagy országhoz.

Meg kell jegyezni, hogy a felső szintű doménnév-nyilvántartó működése magában foglalhatja DNS rendelkezésre bocsátását. Például az IANA hatáskör-átruházási szabályai értelmében az országkód szerinti legfelső szintű doménnevekkel foglalkozó kijelölt szervezetnek többek között az is feladata, hogy felügyelje a doménneveket és működtesse az adott ország DNS-ét[27]. Ezeket a körülményeket a tagállamoknak figyelembe kell venniük az 5. cikk (2) bekezdése szerinti, alapvető szolgáltatásokat nyújtó szereplők azonosítási eljárása során.

4.1.2. Az alapvető szolgáltatásokat nyújtó szereplők azonosítása

Az irányelv 5. cikkének követelményeivel összhangban minden tagállamnak azonosítási eljárást kell végeznie a II. mellékletben felsorolt típusokba tartozó összes olyan szervezet vonatkozásában, amely az adott tagállam területén jogszerűen le van telepedve. Ennek az értékelésnek az eredményeként az 5. cikk (2) bekezdésében meghatározott kritériumokat

[27] További információk: https://www.icann.org/resources/pages/delegation-2012-02-25-en

teljesítő valamennyi jogalanyt alapvető szolgáltatásokat nyújtó szereplőként kell azonosítani, és a 14. cikkben előírt biztonsági és bejelentési kötelezettségek hatálya alá kell vonni.

A tagállamoknak 2018. november 9-ig kell azonosítaniuk a gazdasági szereplőket minden ágazatban és alágazatban. Annak érdekében, hogy a tagállamokat e folyamat során támogassa, az együttműködési csoport jelenleg olyan iránymutatásokat tartalmazó dokumentáció összeállításán dolgozik, amely releváns információkat fog tartalmazni az alapvető szolgáltatásokat nyújtó szereplők azonosításához szükséges lépésekről és bevált módszerekről.

Továbbá a 24. cikk (2) bekezdésével összhangban az együttműködési csoportnak meg kell vitatnia az egyes ágazatokban az alapvető szolgáltatásokat nyújtó szereplők azonosítására szolgáló nemzeti intézkedéseket alkotó folyamatot, az intézkedések lényegi jellemzőit és típusát. A tagállamok 2018. november 9. előtt kérhetik, hogy az együttműködési csoport vitassa meg az alapvető szolgáltatásokat nyújtó szereplők azonosítására szolgáló nemzeti intézkedéseik tervezetét.

4.1.3. További ágazatok bevonása a jogszabályok hatálya alá

Figyelembe véve a 3. cikkben foglalt minimális harmonizációs követelményt, a tagállamok jogszabályokat fogadhatnak el vagy tarthatnak fenn a hálózati és információs rendszerek magasabb szintű biztonságának garantálása érdekében. E tekintetben a tagállamok a 14. cikk szerinti biztonsági és bejelentési kötelezettségeket általában szabadon kiterjeszthetik a kiberbiztonsági irányelv II. mellékletében felsoroltaktól eltérő ágazatokba és alágazatokba tartozó jogalanyokra is. Több tagállam is úgy döntött, hogy az alábbi ágazatok közül némelyeket bevon a kötelezettségek hatálya alá, vagy jelenleg mérlegeli ezt:

i. Közigazgatási szervek

A közigazgatási szervek nyújthatnak az irányelv II. mellékletében szereplő olyan alapvető szolgáltatásokat, amelyek megfelelnek az 5. cikk (2) bekezdésében meghatározott követelményeknek. Ilyen esetekben az ilyen szolgáltatásokat nyújtó közigazgatási szervekre a vonatkozó biztonsági követelmények és bejelentési kötelezettségek vonatkoznának. Ellenkező esetben, vagyis ha a közigazgatási szervek olyan szolgáltatásokat kínálnak, amelyek nem tartoznak a fenti hatály alá, e szolgáltatások nem tartoznának a vonatkozó kötelezettségek hatálya alá.

A közigazgatási szervek felelősek a kormányzati szervek, regionális és helyi hatóságok, ügynökségek és kapcsolt vállalkozások által nyújtott közszolgáltatások megfelelő biztosításáért. Ezeknek a szolgáltatásoknak gyakran része az egyénekre és szervezetekre vonatkozó olyan személyes és vállalati adatok létrehozása és kezelése, amelyek később több állami szervvel is megoszthatók, és azok rendelkezésére bocsáthatók. Tágabb értelemben véve a társadalom és a gazdaság egésze számára fontos, hogy a közigazgatási szervek által használt hálózati és információs rendszerek biztonsági szintje magas legyen. A Bizottság ezért úgy véli, hogy észszerű volna, ha a tagállamok megfontolnák, hogy a II. mellékletben és az 5. cikk (2) bekezdésében meghatározott alapvető szolgáltatásokon túlmenően a közigazgatást is bevonják az irányelvet átültető nemzeti jogszabályok hatálya alá.

ii. Postai ágazat

A postai ágazat különféle postai szolgáltatások nyújtását foglalja magában, például a postai küldemények összegyűjtését, válogatását, szállítását és kihordását.

iii. Élelmiszerágazat

Az élelmiszerágazat a mezőgazdasági és egyéb élelmiszerek előállításával foglalkozik, és olyan alapvető szolgáltatásokat is magában foglalhat, mint az élelmezésbiztonság biztosítása, valamint az élelmiszerek minőségének és biztonságának biztosítása.

iv. Vegyipar és nukleáris ipar

A vegyipar és a nukleáris ipar különösen a vegyi és petrolkémiai termékek, illetve nukleáris anyagok tárolásával, előállításával és feldolgozásával foglalkozik.

v. Környezetvédelmi ágazat

A környezetvédelmi tevékenységek magukban foglalják a környezet védeleméhez és az erőforrások kezeléséhez szükséges áruk és szolgáltatások nyújtását. Ezért a tevékenységek célja a szennyezés megelőzése, csökkentése és megszüntetése, valamint a rendelkezésre álló természeti erőforrások készleteinek megőrzése. Ezen ágazat keretében az alapvető szolgáltatások között említhetjük a szennyezés (pl. levegő- és vízszennyezés) és az időjárási jelenségek nyomon követését és ellenőrzését.

vi. Polgári védelem

A polgári védelmi ágazat célja a természeti és ember okozta katasztrófák megelőzése, valamint az azokra való felkészülés és reagálás. Az e célból nyújtott szolgáltatások közé tartozhat a sürgősségi számok aktiválása és a vészhelyzetekkel kapcsolatos tájékoztatást, a veszélyhelyzetek hatásainak enyhítését és azok elhárítását célzó intézkedések végrehajtása.

4.1.4. Joghatóság

Az 5. cikk (1) bekezdése értelmében minden tagállamnak azonosítania kell a területén telephellyel rendelkező, alapvető szolgáltatásokat nyújtó szereplőket. A rendelkezés nem határozza meg pontosabban a telephely típusát, de a (21) preambulumbekezdés egyértelművé teszi, hogy a letelepedés a tevékenység tényleges és valós, állandó keretek között történő végzését jelenti, e keretek jogi formája azonban nem meghatározó tényező. Ez azt jelenti, hogy egy alapvető szolgáltatásokat nyújtó szereplő felett a tagállamok nem csak akkor rendelkezhetnek joghatósággal, ha a szereplő székhelye van a tagállam területén, hanem olyan esetekben is, amikor a szereplőnek például fióktelepe vagy más típusú jogi telephelye van.

Ez azzal a következménnyel jár, hogy ugyanazon jogalany felett több tagállam is joghatósággal rendelkezhet.

4.1.5. A Bizottságnak benyújtandó információk

Azon felülvizsgálat céljából, amelyet a Bizottságnak a kiberbiztonsági irányelv 23. cikkének (1) bekezdésével összhangban el kell végeznie, a tagállamoknak 2018. november 9-ig, illetve azt követően kétévente be kell nyújtaniuk a Bizottságnak a következő információkat:

- az alapvető szolgáltatásokat nyújtó szereplők azonosítását lehetővé tevő nemzeti intézkedések,

- az alapvető szolgáltatások jegyzéke,
- a II. mellékletben említett minden egyes ágazatra vonatkozóan az alapvető szolgáltatásokat nyújtó szereplőkként azonosított szervezetek száma, és az adott szereplők jelentősége az ágazat szempontjából, valamint
- adott esetben azon küszöbértékek, amelyek alapján meghatározásra került a szolgáltatási szint az érintett szervezet által nyújtott szolgáltatásra támaszkodó felhasználók számára (a 6. cikk (1) bekezdésének a) pontja) vagy a szervezet jelentőségére (a 6. cikk (1) bekezdése f) pontja) való tekintettel.

Az, hogy az irányelv átfogó felülvizsgálatát megelőzően az irányelv 23. cikkének (1) bekezdése értelmében a Bizottságnak jelentést kell készítenie, jelzi, hogy a piac széttöredezettségének elkerülése érdekében a társjogalkotók mennyire fontosnak tartják az irányelv helyes átültetését az alapvető szolgáltatásokat nyújtó szereplők azonosítása tekintetében.

E folyamat lehető legeredményesebb lebonyolítása érdekében a Bizottság arra biztatja a tagállamokat, hogy az együttműködési csoport keretében vitassák meg e kérdést, valamint osszák meg egymással a vonatkozó tapasztalatokat. A Bizottság továbbá arra biztatja a tagállamokat, hogy mindazon információkon túlmenően, amelyeket a tagállamoknak az irányelv alapján a Bizottság rendelkezésére kell bocsátaniuk, osszák meg a Bizottsággal – szükség esetén az információk bizalmas kezelése mellett – az alapvető szolgáltatásokat nyújtóként azonosított szereplők (végső soron kiválasztott) listáját. Az ilyen jegyzékek rendelkezésre állása megkönnyítené a Bizottság által az azonosítási folyamat következetességére vonatkozóan végzett értékelést, javítaná annak minőségét, valamint lehetővé tenné a tagállamok által alkalmazott megközelítések összehasonlítását, ami elősegítené az irányelv céljainak gyorsabb elérését.

4.1.6. Hogyan kell elvégezni az azonosítási folyamatot?

Amint a 4. ábra mutatja, hat olyan kulcsfontosságú kérdés van, amelyet a nemzeti hatóságnak az adott szervezetre vonatkozó azonosítási eljárás során meg kell vizsgálnia. A következő bekezdésben az egyes kérdések a 6. cikkel összefüggésben értelmezett 5. cikk szerinti lépéseknek felelnek meg, figyelembe véve az 1. cikk (7) bekezdésének alkalmazhatóságát is.

1. lépés – **A szervezet az irányelv II. mellékletének hatálya alá tartozó ágazatok/alágazatok és típusok valamelyikébe tartozik?**

A nemzeti hatóságnak értékelnie kell, hogy a területén letelepedett adott szervezet az irányelv II. mellékletében felsorolt ágazatokhoz és alágazatokhoz tartozik-e. A II. melléklet olyan különböző gazdasági ágazatokat foglal magában, amelyek a belső piac megfelelő működése szempontjából meghatározónak minősülnek. A II. melléklet különösen a következő ágazatokra és alágazatokra vonatkozik:

- energia: villamos energia, kőolaj és földgáz,
- közlekedés: légi, vasúti, vízi és közúti közlekedés,
- banki szolgáltatások: hitelintézetek,

- pénzügyi piaci infrastruktúrák: kereskedési helyszínek, központi szerződő felek,
- egészségügy: egészségügyi ellátó létesítmények (beleértve a kórházakat és a magánklinikákat is),
- víz: ivóvízellátás és -elosztás,
- digitális infrastruktúra: IXP-k, DNS-szolgáltatók, TLD név-nyilvántartók[28].

2. lépés – **Alkalmazandó-e *lex specialis* az adott helyzetre?**

Következő lépésként a nemzeti hatóságnak azt kell értékelnie, hogy az 1. cikk (7) bekezdésében foglalt *lex specialis* alkalmazandó-e. A rendelkezés különösen azt mondja ki, hogy amennyiben egy uniós jogi aktus olyan biztonsági és/vagy bejelentési követelményeket ír elő a digitális szolgáltatók vagy az alapvető szolgáltatásokat nyújtó szereplők számára, amelyek hatása legalább egyenértékű a kiberbiztonsági irányelvben foglalt vonatkozó követelményekkel, akkor a különös jogi aktus rendelkezéseit kell alkalmazni. A (9) preambulumbekezdés továbbá egyértelművé teszi, hogy amennyiben az 1. cikk (7) bekezdésében foglalt követelmények teljesülnek, a tagállamoknak az ágazatspecifikus uniós jogi aktus rendelkezéseit kell alkalmazniuk, a joghatósággal kapcsolatos rendelkezéseket is beleértve. Ezzel ellentétben a kiberbiztonsági irányelv vonatkozó rendelkezései nem alkalmazandók. Ilyen esetben az illetékes hatóságnak fel kell függesztenie az 5. cikk (2) bekezdése szerinti azonosítási eljárást[29].

3. lépés – **Az irányelv értelmében vett alapvető szolgáltatást nyújt-e az adott szereplő?**

Ahhoz, hogy az azonosítás tárgyát képező szervezet alapvető szolgáltatásokat nyújtó szereplőnek minősüljön, az 5. cikk (2) bekezdésének a) pontja értelmében olyan szolgáltatást kell nyújtania, amely alapvető a kritikus társadalmi és/vagy gazdasági tevékenységek fenntartásához. Ezen értékelés lefolytatása során a tagállamoknak figyelembe kell venniük, hogy a szervezetek egyszerre alapvető és nem alapvető szolgáltatásokat is nyújthatnak. Ez azt jelenti, hogy a kiberbiztonsági irányelv biztonsági és bejelentési követelményei csak annyiban alkalmazandók egy adott szereplőre, amennyiben az alapvető szolgáltatásokat nyújt.

Az 5. cikk (3) bekezdésével összhangban mindegyik tagállamnak össze kell állítania egy jegyzéket azokról az alapvető szolgáltatásokról, amelyeket az alapvető szolgáltatásokat nyújtó szereplők az adott tagállam területén nyújtanak. Ezt a jegyzéket 2018. november 9-ig, majd azt követően kétévente kell benyújtani a Bizottságnak[30].

4. lépés – **A szolgáltatás függ-e valamilyen hálózati és információs rendszertől?**

A fentieken túl tisztázni kell, hogy a szolgáltatás teljesíti-e az 5. cikk (2) bekezdésének b) pontjában foglalt második feltételt, és különösen azt, hogy az alapvető szolgáltatás nyújtása a 4. cikk 1. pontjában meghatározott hálózati és információs rendszerektől függ-e.

[28]Ezekről a szervezetekről a 4.1.1. pont tovább részletekkel szolgál.

[29] A *lex specialis* alkalmazásával kapcsolatos további részletek az 5.1. pontban találhatók.
[30] Lásd az 5. cikk (7) bekezdésének b) pontját.

5. lépés – **Egy biztonsági esemény jelentős zavart okozna-e?**

Az 5. cikk (2) bekezdésének c) pontja előírja a nemzeti hatóság számára annak értékelését, hogy egy biztonsági esemény jelentős zavart okozna-e a szolgáltatás nyújtásában. Ebben az összefüggésben a 6. cikk (1) bekezdése több olyan ágazatközi tényezőt határoz meg, amelyet figyelembe kell venni az értékelés során. Továbbá a 6. cikk (2) bekezdése szerint az értékelésnek adott esetben ágazatspecifikus tényezőket is figyelembe kell vennie.

A 6. cikk (1) bekezdésében felsorolt **ágazatközi tényezők** a következők:

- az érintett szervezet által nyújtott szolgáltatásra támaszkodó felhasználók száma,
- a II. mellékletben említett más ágazatok függése az említett szervezet által nyújtott szolgáltatástól,
- az, hogy a biztonsági események – mértéküket és időtartamukat tekintve – milyen hatást gyakorolnának a gazdasági és társadalmi tevékenységekre vagy a közbiztonságra,
- az említett szervezet piaci részesedése,
- az adott biztonsági esemény által esetlegesen érintett terület földrajzi kiterjedése,
- az, hogy a szervezetnek mekkora jelentősége van a szolgáltatás elégséges szintjének fenntartásában, figyelembe véve az adott szolgáltatás nyújtásához rendelkezésre álló egyéb lehetőségeket is.

Az **ágazatspecifikus tényezőkkel** kapcsolatban a (28) preambulumbekezdés tartalmaz néhány példát (lásd a 4. táblázatot), amelyek hasznos iránymutatással szolgálhatnak a nemzeti hatóságok számára.

4. táblázat: Példák olyan ágazatspecifikus tényezőkre, amelyeket figyelembe kell venni annak meghatározása során, hogy egy biztonsági esemény jelentős zavart okozna-e.

Ágazat	Ágazatspecifikus tényezők
Energiaszolgáltatók	a tagállamban előállított energia volumene vagy aránya
Olajszállítók	a naponta szállított olaj mennyisége
Légi közlekedés (beleértve a repülőtereket és a légi fuvarozókat is) **Vasúti közlekedés** **Tengeri kikötők**	a tagállambeli szállítás volumenének aránya; az utasok vagy a teherszállítási műveletek éves száma
Banki vagy pénzügyi piaci infrastruktúrák	a teljes vagyonon alapuló rendszerszintű jelentőség; a teljes vagyonnak a GDP-hez viszonyított aránya
Egészségügy	a szolgáltató által évente ellátott betegek száma
Víztermelés, -feldolgozás és -szolgáltatás	a mennyiség, valamint a szolgáltatást igénybe vevő felhasználók száma és típusa (például hogy kórházakról, közszolgálatokról vagy egyénekről van-e szó); olyan alternatív források megléte, amelyekkel ugyanazt a

földrajzi területet el lehet látni

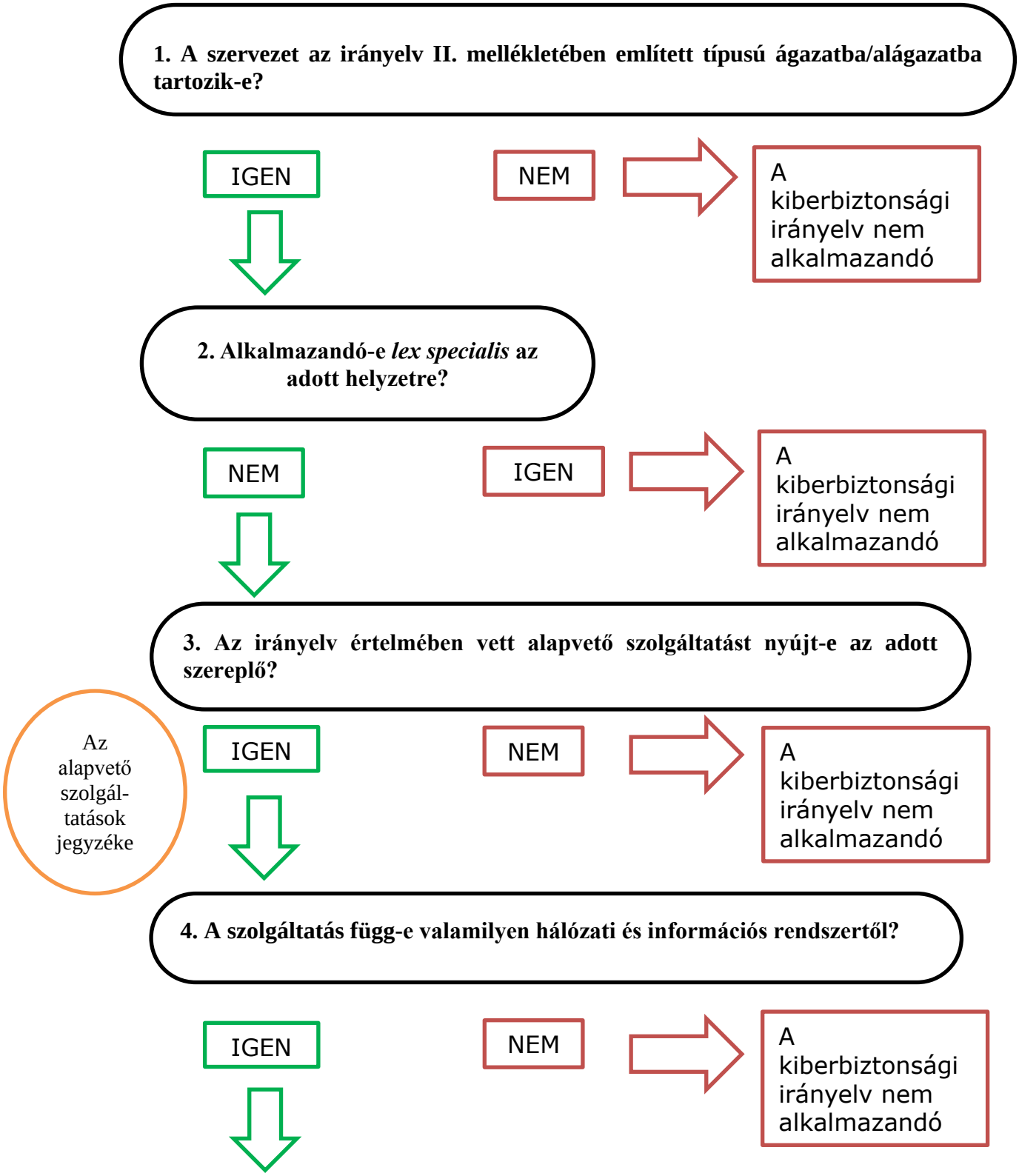
Le kell szögezni, hogy az 5. cikk (2) bekezdése szerinti értékelés során a tagállamok nem egészíthetik ki újabb kritériumokkal az említett rendelkezésben felsoroltakat, mivel az csökkentené az alapvető szolgáltatásokat nyújtó, azonosított szereplők számát és veszélyeztetné a harmonizációnak az irányelv 3. cikke szerinti minimumát az alapvető szolgáltatásokat nyújtó szereplők vonatkozásában.

6. lépés – **Az érintett szereplő nyújt-e alapvető szolgáltatásokat más tagállamban?**

A 6. lépés olyan esetekre vonatkozik, amikor az érintett szereplő két vagy több tagállamban is nyújt alapvető szolgáltatásokat. Az 5. cikk (4) bekezdése előírja az érintett tagállamok számára, hogy az azonosítási eljárás befejezése előtt egyeztessenek egymással[31].

[31] Az egyeztetési eljárás részleteit lásd a 4.1.7. pontban.

4. ábra: Az azonosítási eljárás 6 lépése



5. Egy biztonsági esemény jelentős zavart okozna-e?

Ágazatközi tényezők (6. cikk (1) bekezdés)

- A szolgáltatásra támaszkodó **felhasználók száma**
- Más alapvető ágazatok **függése** a szolgáltatástól
- A biztonsági események által a **gazdasági és társadalmi tevékenységekre** vagy a **közbiztonságra** gyakorolt lehetséges hatás
- Az esetlegesen érintett terület **földrajzi kiterjedése**

Ágazatspecifikus tényezők (a (28) preambulumbekezdésben említett példák)

- **Energiaipar**: a tagállamban előállított energia volumene vagy aránya
- **Közlekedés**: a tagállambeli szállítás volumenének aránya és a szállítási műveletek éves száma
- **Egészségügy**: a szolgáltató által évente ellátott betegek száma

IGEN

NEM → A kiberbiztonsági irányelv nem alkalmazandó

6. Az érintett szereplő nyújt-e alapvető szolgáltatásokat más tagállamban?

IGEN

NEM → A kiberbiztonsági irányelv nem alkalmazandó

Kötelező egyeztetés az érintett tagállammal/tagállamokkal

Nemzeti intézkedések elfogadása (pl. az alapvető szolgáltatásokat nyújtó szereplők jegyzéke, szakpolitikai és jogi intézkedések)

4.1.7. Határon átnyúló egyeztetési eljárás

Amennyiben egy szereplő két vagy több tagállamban nyújt alapvető szolgáltatásokat, az 5. cikk (4) bekezdése előírja, hogy e tagállamoknak az azonosítási eljárás befejezése előtt egyeztetniük kell egymással. Az egyeztetés célja, hogy elősegítse a szereplő kritikus jellegének a határokon átnyúló hatások tekintetében történő értékelését.

Az egyeztetés lehetővé teszi a részt vevő nemzeti hatóságok számára, hogy megosszák egymással érveiket és álláspontjaikat, ezt követően ideális esetben azonos eredményre jutnak az érintett szereplő azonosításával kapcsolatban. A kiberbiztonsági irányelv azonban nem zárja ki azt a lehetőséget sem, hogy a tagállamok eltérő következtetésre jutnak a tekintetben, hogy egy adott szervezet alapvető szolgáltatásokat nyújtó szereplőnek minősül-e vagy sem. A (24) preambulumbekezdés megemlíti, hogy a tagállamok ilyen esetekben az együttműködési csoport segítségét kérhetik.

A Bizottság álláspontja szerint a tagállamoknak törekedniük kell arra, hogy konszenzust érjenek el ezekben a kérdésekben, és ily módon elkerüljék azt, hogy ugyanazon vállalat eltérő jogállással rendelkezzen a különböző tagállamokban. Ilyen eltérések csak valóban kivételes esetekben fordulhatnak elő, például ha egy szervezet, amely az egyik tagállamban alapvető szolgáltatásokat nyújtó szereplőnek számít, egy másik tagállamban csak marginális és elhanyagolható mértékű tevékenységet folytat.

4.2. Biztonsági követelmények

A 14. cikk (1) bekezdése értelmében a tagállamoknak biztosítaniuk kell, hogy az alapvető szolgáltatásokat nyújtó szereplők – tekintettel a tudomány és a technika mindenkori állására – megfelelő és arányos műszaki és szervezési intézkedéseket tegyenek a szolgáltatásuk nyújtása során általuk használt hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése érdekében. A 14. cikk (2) bekezdésével összhangban a megfelelő intézkedéseknek meg kell akadályozniuk a biztonsági eseményeket és csökkenteniük kell azok hatását.

Az együttműködési csoport egy erre a célra létrehozott munkafolyamat keretében jelenleg a biztonsági intézkedésekkel kapcsolatos, az alapvető szolgáltatásokat nyújtó szereplőknek szóló nem kötelező erejű iránymutatások összeállításán dolgozik[32]. A csoportnak 2017 negyedik negyedévére kell véglegesítenie az iránymutatásokat tartalmazó dokumentációt. A Bizottság arra ösztönzi a tagállamokat, hogy pontosan kövessék az együttműködési csoport által kidolgozott iránymutatásokat tartalmazó dokumentációt annak érdekében, hogy a biztonsági követelményekre vonatkozó nemzeti rendelkezések a lehető legnagyobb mértékben összhangban legyenek. E követelmények harmonizálása nagyban elősegítené, hogy a gyakran több tagállamban is alapvető szolgáltatásokat nyújtó szereplők meg tudjanak felelni az

[32] E munkafolyamat elősegítése céljából a kiberbiztonsági irányelv hatálya alá tartozó valamennyi ágazatra vonatkozóan nemzetközi szabványok, bevált gyakorlatok és kockázatelemzési módszerek jegyzéke került megosztásra és felhasználásra alapanyagként a javasolt biztonsági területekhez és biztonsági intézkedésekhez.

említett követelményeknek, továbbá megkönnyítené a nemzeti illetékes hatóságok és a CSIRT-ek felügyeleti munkáját is.

4.3. Bejelentési követelmények

A 14. cikk (3) bekezdése értelmében a tagállamok biztosítják, hogy az alapvető szolgáltatásokat nyújtó szereplők „*bejelentik [...] az általuk nyújtott alapvető szolgáltatások folytonosságára jelentős hatást gyakorló biztonsági eseményeket*". Következésképpen az alapvető szolgáltatásokat nyújtó szereplőknek a kisebb biztonsági eseményekről nem kell jelentést tenniük, csak az alapvető szolgáltatás folytonosságát befolyásoló, súlyos eseményeket kell bejelenteni. A 4. cikk 7. pontja alapján biztonsági esemény „*minden olyan esemény, amely ténylegesen kedvezőtlen hatást gyakorol a hálózati és információs rendszerek biztonságára*". A „hálózati és információs rendszerek biztonsága" kifejezést a 4. cikk 2. pontja határozza meg pontosabban: „*a hálózati és információs rendszer arra való képessége, hogy adott bizonyossággal ellenálljon az olyan cselekményeknek, amelyek veszélyeztetik a rajtuk tárolt, továbbított vagy kezelt adatok vagy az említett hálózati és információs rendszeren nyújtott vagy rajta keresztül elérhető kapcsolódó szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét és bizalmasságát*". Ebből következően nemcsak az adatok vagy a kapcsolódó szolgáltatások rendelkezésre állására, hanem azok hitelességére, sértetlenségére vagy bizalmasságára kedvezőtlen hatást gyakoroló események is bejelentési kötelezettséget keletkeztethetnek. A szolgáltatásnak a 14. cikk (3) bekezdésében említett folytonosságát ugyanis nemcsak a fizikai rendelkezésre állást érintő esetek, hanem a szolgáltatás megfelelő nyújtását befolyásoló bármilyen egyéb biztonsági esemény is veszélyeztetheti[33].

Az együttműködési csoporton belül külön munkacsoport foglalkozik az azon körülményekre vonatkozó, nem kötelező erejű eseménybejelentési iránymutatások (és a nemzeti bejelentések formátumának és eljárásának) kidolgozásával, amelyek fennállása esetén az alapvető szolgáltatásokat nyújtó szereplőknek a 14. cikk (7) bekezdése alapján be kell jelenteniük a biztonsági eseményeket. Az iránymutatások a tervek szerint 2017 negyedik negyedévére készülnek el.

A bejelentések tekintetében fennálló különféle nemzeti követelmények jogbizonytalansághoz, bonyolultabb és nehézkesebb eljárásokhoz, valamint a több tagállamban is tevékenykedő szolgáltatók számára jelentős adminisztratív költségekhez vezethetnek. A Bizottság ezért üdvözli az együttműködési csoport munkáját. A biztonsági követelményekhez hasonlóan a Bizottság e téren is arra ösztönzi a tagállamokat, hogy pontosan kövessék az együttműködési csoport által kidolgozott iránymutatásokat tartalmazó dokumentációt annak érdekében, hogy a biztonsági események bejelentésére vonatkozó nemzeti rendelkezések a lehető legnagyobb mértékben összhangban legyenek.

4.4. A kiberbiztonsági irányelv III. melléklete: Digitális szolgáltatók

[33] Ugyanez vonatkozik a digitális szolgáltatókra is.

A digitális szolgáltatók alkotják a kiberbiztonsági irányelv hatálya alá tartozó szervezetek második kategóriáját. Ezek a szervezetek fontos gazdasági szereplőknek minősülnek, mivel számos vállalkozás veszi igénybe szolgáltatásaikat a saját szolgáltatásai nyújtása céljából, ezért a digitális szolgáltatásokban bekövetkező zavar hatással lehet az alapvető gazdasági és társadalmi tevékenységekre

4.4.1. A digitális szolgáltatók kategóriái

A 4. cikknek a digitális szolgáltatás fogalmát meghatározó 5. pontja az (EU) 2015/1535 európai parlamenti és tanácsi irányelv 1. cikke (1) bekezdésének b) pontjában foglalt fogalommeghatározásra hivatkozva az alkalmazási kört leszűkíti a III. mellékletben felsorolt szolgáltatástípusokra. Pontosabban az (EU) 2015/1535 irányelv 1. cikke (1) bekezdésének b) pontja e szolgáltatásokat a következőképpen határozza meg: „*bármely, általában térítés ellenében, távolról, elektronikus úton és a szolgáltatást igénybe vevő egyéni kérelmére nyújtott szolgáltatás”*, az irányelv III. melléklete pedig a szolgáltatások három konkrét típusát sorolja fel: online piactér, online keresőprogram és felhőalapú számítástechnikai szolgáltatás. Az alapvető szolgáltatásokat nyújtó szereplőktől eltérően az irányelv nem írja elő a tagállamok számára, hogy azonosítsák azokat a digitális szolgáltatókat, amelyekre ezt követően a releváns kötelezettségek vonatkoznának. Ezért az irányelv vonatkozó kötelezettségeit, nevezetesen a 16. cikkben meghatározott biztonsági és bejelentési követelményeket az irányelv hatálya alá tartozó valamennyi digitális szolgáltató esetében alkalmazni kell.

A következő pontok további magyarázattal szolgálnak a digitális szolgáltatásoknak az irányelv hatálya alá tartozó három típusa tekintetében.

1. Online piacterekkel foglalkozó szolgáltatók

Az online piacterek számos különféle vállalkozás számára teszik lehetővé, hogy a fogyasztókkal való kereskedelmi tevékenységüket és a vállalkozásokkal való kapcsolataikat e piactereken folytassák. E rendszerek az online és a határokon átnyúló kereskedelemhez szükséges alapvető infrastruktúrát biztosítják a vállalkozások számára. Jelentős szerepet játszanak a gazdaságban, elsősorban azáltal, hogy a kkv-k számára hozzáférést kínálnak a szélesebb körű uniós digitális egységes piachoz. Az ügyfél gazdasági tevékenységét elősegítő távoli számítástechnikai szolgáltatások nyújtása, beleértve az ügyletek feldolgozását, valamint a vevőkre, szállítókra és termékekre vonatkozó információk összesítését is, szintén beletartozhat az online piacterek tevékenységeibe, ahogy a megfelelő termékek felkutatásának elősegítése, a termékek forgalmazása, az ügyleti szakértelem, valamint a vevők és az eladók párosítása is.

Az online piactér fogalmának meghatározása a 4. cikk 17. pontjában, további pontosítása a (15) preambulumbekezdésben található. A meghatározás szerint az online piacterek lehetővé teszik, hogy a fogyasztók és a kereskedők online adás-vételi és szolgáltatási szerződéseket kössenek kereskedőkkel, emellett ezek a piacterek az említett szerződések megkötésének végpontjai. Az *E-bayhez* hasonló szolgáltatók például online piactérnek tekinthetők, mivel lehetővé teszik, hogy a platformjukon mások saját üzletet nyissanak, és így online kínálják

termékeiket és szolgáltatásaikat a fogyasztóknak vagy a vállalkozásoknak. Az alkalmazásokat és szoftvereket kínáló online alkalmazás-áruházak szintén online piactereknek minősülnek, mivel az alkalmazásfejlesztők ezen áruházak segítségével értékesíthetik vagy terjeszthetik szolgáltatásaikat a fogyasztók vagy más vállalkozások számára. Ezzel szemben a 4. cikk 17. pontja szerinti meghatározás nem terjed ki a harmadik felek szolgáltatásait köztes szereplőként kínáló szolgáltatókra (például a *Skyscannerre* és az ár-összehasonlító portálokra), amelyek továbbirányítják a felhasználót a kereskedő honlapjára, és a szolgáltatásra vagy a termékre vonatkozó tényleges szerződés megkötésére már itt kerül sor.

2. Online keresőprogramokkal foglalkozó szolgáltatók

Az online keresőprogram fogalmának meghatározása a 4. cikk 18. pontjában, további pontosítása pedig a (16) preambulumbekezdésben található. Az online keresőprogram olyan digitális szolgáltatás, amelynek segítségével a felhasználók elvben valamennyi weboldalon, illetve konkrét nyelvű weboldalakon megadott lekérdezés alapján bármilyen témában kereséseket végezhetnek. Az adott weboldalon belüli keresési funkciók és az ár-összehasonlító weboldalak nem tartoznak ebbe a körbe. Az EUR LEX portál[34] által kínált keresőmotor például nem minősül az irányelv értelmében vett keresőprogramnak, mivel a keresési funkció kizárólag ennek a konkrét weboldalnak a tartalmára korlátozódik.

3. Felhőalapú számítástechnikai szolgáltatásokkal foglalkozó szolgáltatók

A 4. cikk 19. pontja szerint a felhőalapú számítástechnikai szolgáltatás „olyan digitális szolgáltatás, amely megosztható számítástechnikai erőforrások méretezhető és rugalmas pooljához enged hozzáférést” – a számítástechnikai erőforrások, a méretezhetőség és a rugalmas pool pontosabb magyarázata a (17) preambulumbekezdésben található.

Röviden összefoglalva a felhőalapú számítástechnika az informatikai szolgáltatások olyan típusának tekinthető, amely megosztott erőforrásokat alkalmaz az igényalapú adatfeldolgozáshoz, ahol a megosztott erőforrások olyan hardver- vagy szoftverelemeket (pl. hálózatokat, szervereket vagy más infrastruktúrát, tárolóhelyet, alkalmazásokat és szolgáltatásokat) jelentenek, amelyek igény szerint állnak a felhasználók rendelkezésére az adatfeldolgozáshoz. A „megosztható” kifejezés olyan számítástechnikai erőforrásokat jelöl, amelyek esetében sok felhasználó veszi igénybe ugyanazt a fizikai infrastruktúrát az adatok feldolgozásához. A számítástechnikai erőforrások akkor minősülnek megoszthatónak, ha a szolgáltató által használt erőforrások poolja bármikor bővíthető vagy szűkíthető a felhasználói igényeknek megfelelően. Ily módon adatközpontok vagy egy adatközponton belüli elemek hozzáadására vagy eltávolítására van lehetőség, ha a számítási vagy tárolási kapacitás teljes mennyiségének módosítása szükséges. A rugalmas pool az erőforrások automatikus rendelkezésre bocsátásával vagy leépítésével történő terhelésmódosításokra utal, melyek révén a rendelkezésre álló erőforrások minden egyes időpontban a lehető legnagyobb mértékben megfelelnek az aktuális keresletnek[35].

[34] Elérhető a következő címen: http://eur-lex.europa.eu/homepage.html

[35] Nikolas Roman Herbst, Samuel Kounev, Ralf Reussner, Karlsruhe Institute of Technology: „Elasticity in Cloud Computing: What It Is, and What It Is Not”, hozzáférhető a következő címen:

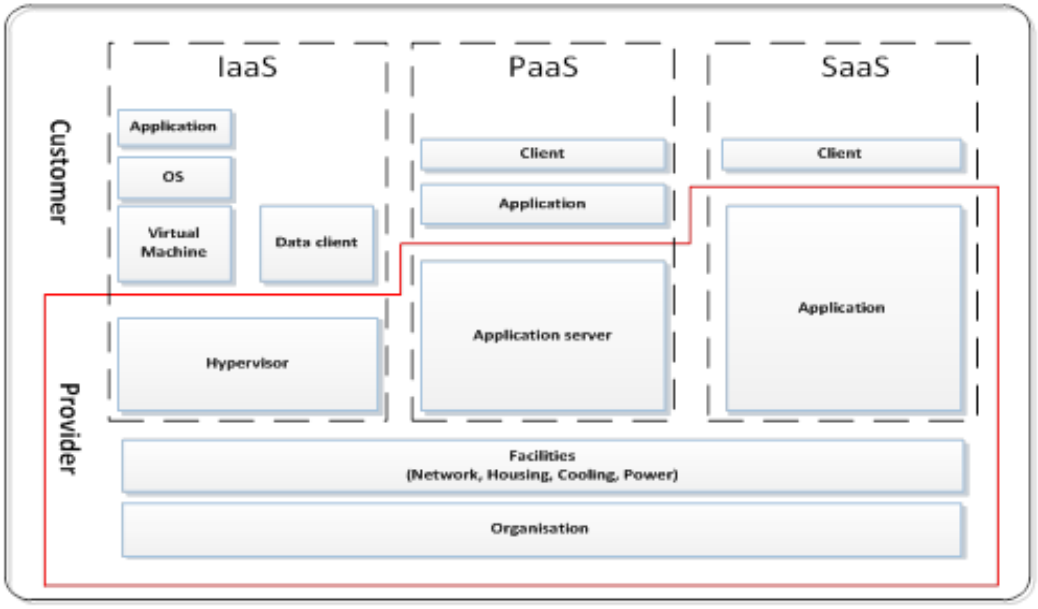
Jelenleg a felhőalapú szolgáltatási modell három típusát kínálhatják a szolgáltatók:

- Infrastruktúra-szolgáltatás (IaaS): A felhőalapú szolgáltatások azon kategóriája, ahol a felhőalapú kapacitást infrastruktúra formájában kínálják az ügyfél számára. Magában foglalja a számítástechnikai erőforrások hardver, illetve hálózati és tárolási szolgáltatások formájában történő virtuális biztosítását. Az IaaS-re épülve működhetnek szerverek, valamint tárolási, hálózati és operációs rendszerek. Olyan vállalati infrastruktúrát biztosít, ahol a vállalkozások adatokat tárolhatnak és amelyen a napi működésükhöz szükséges alkalmazásokat futtathatják.

- Platformszolgáltatás (PaaS): A felhőalapú szolgáltatások azon kategóriája, ahol a felhőalapú kapacitást platform formájában kínálják az ügyfél számára. Olyan online számítástechnikai platformokat foglal magában, amelyek lehetővé teszik a vállalatok számára a meglévő alkalmazásaik futtatását, illetve újak kifejlesztését és tesztelését.

- Szoftverszolgáltatás (SaaS): A felhőalapú szolgáltatások azon kategóriája, ahol a felhőalapú kapacitást az interneten működő alkalmazás vagy szoftver formájában kínálják az ügyfél számára. A felhőalapú szolgáltatások e típusánál a végfelhasználónak nem kell megvásárolnia, telepítenie vagy kezelnie a szoftvereket, és azzal az előnnyel jár, hogy azok internetkapcsolattal bárhonnan elérhetők.

5. ábra: Szolgáltatási modellek és eszközök a felhőalapú számítástechnika területén



https://sdqweb.ipd.kit.edu/publications/pdfs/HeKoRe2013-ICAC-Elasticity.pdf. Lásd még a COM(2012) 529 számú dokumentum 2–5. oldalát.

Az ENISA átfogó iránymutatásokat állított össze a felhőalapú számítástechnikával kapcsolatos konkrét témákról[36], valamint egy iránymutatásokat tartalmazó dokumentációt a felhőalapú számítástechnika alapjairól[37].

4.4.2. Biztonsági követelmények.

A 16. cikk (1) bekezdése értelmében a tagállamoknak biztosítaniuk kell, hogy a digitális szolgáltatók a szolgáltatásaik nyújtása során általuk használt hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése érdekében megfelelő és arányos műszaki és szervezési intézkedéseket tegyenek. Ezeknek a biztonsági intézkedéseknek figyelembe kell venniük a tudomány és a technika mindenkori állását, valamint a következő öt elemet: i. a rendszerek és létesítmények biztonsága; ii. a biztonsági események kezelése; iii. üzletmenetfolytonosság-menedzsment; iv. monitoring, ellenőrzés és vizsgálat; valamint v. a nemzetközi szabványoknak való megfelelés.

E tekintetben a Bizottság a 16. cikk (8) bekezdése alapján felhatalmazást kap arra, hogy végrehajtási jogi aktusokat fogadjon el, amelyek pontosabban meghatározzák a szóban forgó elemeket, és magas szintű harmonizációt biztosítanak e szolgáltatók számára. A Bizottság várhatóan 2017 őszén fogadja el a végrehajtási aktust. Továbbá a tagállamoknak biztosítaniuk kell, hogy a digitális szolgáltatók megtegyék a szükséges intézkedéseket annak érdekében, hogy a szolgáltatásaik folyamatosságának biztosítása érdekében megelőzzék és minimalizálják a biztonsági események hatását.

4.4.3. Bejelentési követelmények.

A digitális szolgáltatókat kötelezni kell arra, hogy a súlyos biztonsági eseményeket jelentsék be az illetékes hatóságoknak vagy a CSIRT-eknek. A kiberbiztonsági irányelv 16. cikkének (3) bekezdésével összhangban a digitális szolgáltatókra vonatkozó bejelentési kötelezettség olyan esetekben merül fel, amikor a biztonsági esemény jelentős hatást gyakorol a szolgáltatásnyújtásra. A hatás meghatározásához a 16. cikk (4) bekezdése különösen öt olyan paramétert sorol fel, amelyeket a digitális szolgáltatóknak figyelembe kell venniük. E tekintetben a Bizottság a 16. cikk (8) bekezdése alapján felhatalmazást kap arra, hogy végrehajtási jogi aktusokat fogadjon el, amelyek pontosabban leírják a paramétereket. A szóban forgó paraméterek pontosabb meghatározása a 4.4.2. pontban említett biztonsági elemeket meghatározó azon végrehajtási aktus részét fogja képezni, amelyet a Bizottság a tervek szerint ősszel fogad el.

4.4.4. Kockázatalapú szabályozási megközelítés.

A 17. cikk előírja, hogy a nemzeti illetékes hatóságok lássák el a digitális szolgáltatók utólagos felügyeleti ellenőrzését. A tagállamoknak gondoskodniuk kell arról, hogy az illetékes hatóságok lépéseket tegyenek, amennyiben bizonyítékokat tárnak eléjük arra vonatkozóan, hogy valamely digitális szolgáltató nem teljesíti az irányelv 16. cikkében meghatározott követelményeket.

---

[36] Elérhető a következő címen: https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security

[37] ENISA, *Cloud Security Guide for SMEs* (2015). Elérhető a következő címen: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

Továbbá a 16. cikk (8) és (9) bekezdése értelmében a Bizottság felhatalmazást kap arra, hogy olyan végrehajtási jogi aktusokat fogadjon el a bejelentési és a biztonsági követelmények tekintetében, amelyek javítják a digitális szolgáltatókra vonatkozó harmonizáció szintjét. Továbbá a 16. cikk (10) bekezdése értelmében a tagállamok az irányelvben foglaltakon kívül nem írhatnak elő további biztonsági és bejelentési követelményeket a digitális szolgáltatók számára, kivéve olyan esetekben, amikor az ilyen intézkedések az alapvető állami funkciók védelméhez, különösen a nemzetbiztonság védelméhez, valamint a bűncselekmények kivizsgálásának, felderítésének és büntetőeljárás alá vonásának lehetővé tétele érdekében szükségesek.

Végül pedig figyelembe véve a digitális szolgáltatók határokon átnyúló jellegét, az irányelv nem a több párhuzamos joghatóság modelljét, hanem az azon a kritériumon alapuló megközelítést követi, hogy a vállalat központi ügyvezetésének helye az EU-ban legyen[38]. Ez a megközelítés lehetővé teszi, hogy valamennyi digitális szolgáltatóra ugyanaz az egységes szabályrendszer vonatkozzon, a felügyelet pedig egy illetékes hatóság felelőssége legyen, ami különösen fontos, mivel számos digitális szolgáltató egyidejűleg több tagállamban is kínálja szolgáltatásait. E megközelítés alkalmazása minimálisra csökkenti a digitális szolgáltatók megfeleléssel kapcsolatos terhét, és biztosítja a digitális egységes piac megfelelő működését.

4.4.5. Joghatóság.

A fent kifejtettek szerint a kiberbiztonsági irányelv 18. cikkének (1) bekezdése értelmében a digitális szolgáltató felett az a tagállam rendelkezik joghatósággal, amelyben a vállalat központi ügyvezetésének helye található. Azon esetekben, amikor a konkrét digitális szolgáltató szolgáltatásokat kínál az EU-ban, de az EU területén nincs letelepedve, a 18. cikk (2) bekezdése arra kötelezi a digitális szolgáltatót, hogy képviselőt jelöljön ki az Unióban. Ebben az esetben a képviselő székhelye szerinti tagállam rendelkezik joghatósággal a társaság felett. Olyan esetekben, amikor egy digitális szolgáltató szolgáltatásokat nyújt egy tagállamban, de nem jelölt ki képviselőt az EU-ban, a tagállam elvben eljárhat a digitális szolgáltatóval szemben, mivel a szolgáltató megsérti az irányelvből eredő kötelezettségeit.

4.4.6. A korlátozott méretű digitális szolgáltatók mentessége a biztonsági követelmények és a bejelentési kötelezettség hatálya alól.

A 16. cikk (11) bekezdése értelmében a 2003/361/EK bizottsági ajánlás39 szerint mikro- vagy kisvállalkozásnak minősülő digitális szolgáltatók nem tartoznak a 16. cikkben meghatározott biztonsági követelmények és bejelentési kötelezettség hatálya alá. Ez azt jelenti, hogy azok a vállalkozások, amelyek kevesebb mint 50 személyt foglalkoztatnak, és amelyek éves forgalma és/vagy éves mérlegfőösszege nem haladja meg a 10 millió eurót, nem tartoznak e követelmény hatálya alá. A gazdálkodó egység méretének meghatározásakor nem releváns, hogy az érintett vállalat csak a kiberbiztonsági irányelv értelmében vett digitális szolgáltatásokat vagy más szolgáltatásokat is nyújt.

[38] Lásd különösen az irányelv 18. cikkét.
[39] HL L 24., 2003.5.20., 36. o.

5. A kiberbiztonsági irányelv és más jogszabályok közötti kapcsolat.

Ez a pont a kiberbiztonsági irányelv 1. cikkének (7) bekezdésében foglalt, a *lex specialis*-ra vonatkozó rendelkezésekre összpontosít, bemutatja a *lex specialis* Bizottság által eddig értékelt három példáját, valamint pontosítja a távközlési és a bizalmi szolgáltatókra vonatkozó biztonsági és bejelentési követelményeket.

5.1. A kiberbiztonsági irányelv 1. cikkének (7) bekezdése: A *lex specialis* rendelkezése.

A kiberbiztonsági irányelv 1. cikkének (7) bekezdése értelmében az irányelv szerint a digitális szolgáltatókra vagy az alapvető szolgáltatásokat nyújtó szereplőkre vonatkozó biztonsági és/vagy bejelentési követelményekről szóló rendelkezéseket nem kell alkalmazni, amennyiben egy uniós ágazatspecifikus jogszabály olyan biztonsági és/vagy bejelentési követelményeket ír elő, amelyek hatása legalább egyenértékű a kiberbiztonsági irányelvben foglalt vonatkozó kötelezettségekkel. A tagállamoknak az irányelv teljes átültetése során figyelembe kell venniük az 1. cikk (7) bekezdését, és tájékoztatniuk kell a Bizottságot a *lex specialis*-ra vonatkozó rendelkezések alkalmazásáról.

Módszertan.

Egy uniós ágazatspecifikus jogszabálynak a kiberbiztonsági irányelv vonatkozó rendelkezéseivel való egyenértékűségére vonatkozó értékeléskor különös jelentőséget kell tulajdonítani annak a kérdésnek, hogy az ágazatspecifikus jogszabályban foglalt biztonsági kötelezettségek magukban foglalnak-e olyan intézkedéseket, amelyek garantálják az irányelv 4. cikkének 2. pontjában meghatározott hálózati és információs rendszerek biztonságát.

Ami a bejelentési követelményeket illeti, a kiberbiztonsági irányelv 14. cikkének (3) bekezdése és 16. cikkének (3) bekezdése előírja, hogy az alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók kötelesek indokolatlan késedelem nélkül bejelenteni az illetékes hatóságoknak vagy a CSIRT-nek minden olyan biztonsági eseményt, amely jelentős hatást gyakorol a szolgáltatás nyújtására. Itt különös figyelemet kell fordítani a szereplő/digitális szolgáltató azon kötelezettségére, hogy a bejelentésbe olyan információkat foglaljon, amelyek lehetővé teszik az illetékes hatóság vagy a CSIRT számára a biztonsági esemény határokon átnyúló hatásainak meghatározását.

Jelenleg nincs olyan ágazatspecifikus jogszabály a digitális szolgáltatók kategóriájára vonatkozóan, amely a kiberbiztonsági irányelv 16. cikkében foglaltakhoz hasonló biztonsági és bejelentési követelményeket írna elő, amelyeket a kiberbiztonsági irányelv 1. cikke (7) bekezdésének alkalmazása során figyelembe lehetne venni[40].

Az alapvető szolgáltatásokat nyújtó szereplőket illetően a pénzügyi szektorra, és különösen a II. melléklet 3. és 4. pontjában említett banki szolgáltatásokra és pénzügyi piaci infrastruktúrákra vonatkoznak jelenleg uniós ágazatspecifikus jogszabályokból eredő biztonsági és/vagy bejelentési követelmények. Ez annak köszönhető, hogy a pénzügyi

[40] Ez nem érinti az általános adatvédelmi rendelet 33. cikkének hatálya alatt személyes adatok megsértéséről a felügyeleti hatóságnak tett bejelentéseket.

intézmények által használt informatikai, hálózati és információs rendszerek biztonsága és megbízhatósága alapvető részét képezi az uniós jogszabályok értelmében a pénzügyi intézményekre rótt működési kockázati követelményeknek.

Példák.

i. A felülvizsgált pénzforgalmi irányelv (PSD2).

Ami a banki ágazatot és különösen az 575/2013/EU rendelet 4. cikkének 1. pontjában meghatározott hitelintézetek által nyújtott pénzforgalmi szolgáltatásokat illeti, az úgynevezett felülvizsgált pénzforgalmi irányelv (a továbbiakban: PSD2)[41] az említett irányelv 95. és 96. cikkében meghatározott biztonsági és bejelentési követelményeket ír elő.

Pontosabban a 95. cikk (1) bekezdése előírja a pénzforgalmi szolgáltatók számára, hogy olyan megfelelő kockázatmérséklési intézkedéseket és ellenőrzési mechanizmusokat fogadjanak el, amelyek lehetővé teszik az általuk nyújtott pénzforgalmi szolgáltatásokhoz kapcsolódó működési és biztonsági kockázatok kezelését. Ezen intézkedések részeként – a súlyosabb működési és biztonsági események felderítését és osztályozását is tartalmazó – hatékony eseménykezelési eljárásokat kell létrehozniuk és fenntartaniuk. A PSD2 (95) és (96) preambulumbekezdése tovább pontosítja az ilyen biztonsági intézkedések jellegét. E rendelkezésekből kitűnik, hogy az előírt intézkedések célja a pénzforgalmi szolgáltatások nyújtása során alkalmazott hálózati és információs rendszerekhez kapcsolódó biztonsági kockázatok kezelése. Ezért úgy lehet tekinteni, hogy ezek a biztonsági követelmények hatásukat tekintve legalább egyenértékűek a kiberbiztonsági irányelv 14. cikke (1) és (2) bekezdésének megfelelő rendelkezésével.

A bejelentési követelményeket illetően a PSD2 96. cikkének (1) bekezdése előírja a pénzforgalmi szolgáltatók számára, hogy a súlyos biztonsági eseményeket indokolatlan késedelem nélkül bejelentsék az illetékes hatóságnak. Továbbá a PSD2 96. cikkének (2) bekezdése a kiberbiztonsági irányelv 14. cikkének (5) bekezdéséhez hasonlóan előírja az illetékes hatóság számára, hogy tájékoztassa más tagállamok illetékes hatóságait, amennyiben egy biztonsági esemény számukra is releváns. Ez a kötelezettség ugyanakkor azt is jelenti, hogy a biztonsági események jelentésének tartalmaznia kell olyan információkat, amelyek lehetővé teszik a hatóságok számára az esemény határokon átnyúló hatásainak értékelését. A PSD2 96. cikke (3) bekezdésének a) pontja e tekintetben felhatalmazza az EBH-t, hogy az EKB-val együttműködésben iránymutatásokat dolgozzon ki a bejelentés pontos tartalmára és formátumára vonatkozóan.

Következésképpen megállapítható, hogy a kiberbiztonsági irányelv 1. cikkének (7) bekezdése értelmében a hitelintézetek által nyújtott pénzforgalmi szolgáltatások tekintetében a PSD2 95. és 96. cikkében foglalt biztonsági és bejelentési követelmények alkalmazandók a kiberbiztonsági irányelv 14. cikkének megfelelő rendelkezései helyett.

[41] (EU) 2015/2366 irányelv, HL L 337., 2015.12.23., 35. o.

ii. Az Európai Parlament és a Tanács 648/2012/EU rendelete (2012. július 4.) a tőzsdén kívüli származtatott ügyletekről, a központi szerződő felekről és a kereskedési adattárakról.

A pénzügyi piaci infrastruktúra tekintetében a 648/2012/EU rendelet és azzal összefüggésben a 153/2013/EU felhatalmazáson alapuló bizottsági rendelet tartalmaz rendelkezéseket a központi szerződő felekre vonatkozó biztonsági követelmények tekintetében, amelyet *lex specialis*-nak lehet tekinteni. Ezek a jogi aktusok különösen a hálózati és információs rendszerek biztonságával kapcsolatos műszaki és szervezeti intézkedésekről rendelkeznek, amelyek részletesség tekintetében túlmutatnak a kiberbiztonsági irányelv 14. cikkének (1) és (2) bekezdésében foglalt követelményeken, ezért a biztonsági követelmények tekintetében teljesítik a kiberbiztonsági irányelv 1. cikke (7) bekezdésének követelményeit.

Pontosabban a 648/2012/EU rendelet 26. cikkének (1) bekezdése kimondja, hogy a szervezetnek „*megbízható vállalatirányítási rendszerrel [kell] rendelkez[nie], amely magában foglalja a következőket: egymástól jól elhatárolt, átlátható és következetes felelősségi köröket előíró áttekinthető szervezeti felépítés, hatékony eljárások azoknak a kockázatoknak azonosítására, kezelésére, felügyeletére és jelentésére, amelyeknek [...] ki van [...] vagy ki lehet [...] téve, valamint megbízható adminisztratív és számviteli eljárásokat is tartalmazó megfelelő belső ellenőrzési mechanizmusok*”. A 26. cikk (3) bekezdése előírja, hogy a szervezeti struktúrának megfelelő és arányos rendszerek, erőforrások és eljárások alkalmazásával biztosítania kell a szolgáltatásnyújtás és a tevékenységvégzés folyamatosságát és rendes működését.

A 26. cikk (6) bekezdése továbbá egyértelművé teszi, hogy a központi szerződő félnek „*az általa nyújtott szolgáltatások és végzett tevékenységek komplexitásának, változatosságának és jellegének kezelésére alkalmas információtechnológiai rendszereket [kell fenntartania] a szigorú biztonsági standardok, valamint a kezelt információk integritásának és bizalmas jellegének biztosítása érdekében*”. Továbbá a 34. cikk (1) bekezdése olyan megfelelő üzletmenet-folytonossági politika és vészhelyzet esetére szóló helyreállítási terv kidolgozását, végrehajtását és fenntartását írja elő, amely biztosítja a műveletek kellő időben történő helyreállítását.

Ezeket a kötelezettségeket még pontosabban meghatározza a 648/2012/EU európai parlamenti és tanácsi rendeletnek a központi szerződő felekre vonatkozó követelményekről szóló szabályozási technikai standardok tekintetében történő kiegészítéséről szóló, 2012. december 19-i 153/2013/EU felhatalmazáson alapuló bizottsági rendelet[42]. Különösen annak 4. cikke arra kötelezi a központi szerződő felet, hogy annak érdekében, hogy képes legyen minden releváns kockázatot kezelni és azokról jelentést tenni, megfelelő kockázatkezelési eszközöket dolgozzon ki és szolgáljon részletekkel az intézkedések típusáról (pl. stabil információs és kockázatellenőrzési rendszer alkalmazása, az erőforrások és szakértelem rendelkezésre állása, és hozzáférés a kockázatkezelési funkcióval kapcsolatos valamennyi releváns információhoz, olyan megfelelő belső ellenőrzési mechanizmusok,

[42] HL L 52., 2013.2.3., 41. o.

például megbízható adminisztratív és számviteli eljárások rendelkezésre állása, amelyek segítséget nyújtanak a központi szerződő fél igazgatóságának kockázatkezelési politikái, eljárásai és rendszerei megfelelőségének és hatékonyságának nyomon követéséhez és értékeléséhez).

Továbbá a 9. cikk kifejezetten utal az információtechnológiai rendszerek biztonságára, és konkrét műszaki és szervezeti intézkedéseket ír elő az informatikai biztonsági kockázatok kezelésére szolgáló, nagy ellenálló képességű információbiztonsági keretrendszer fenntartásával összefüggésben. Ezen intézkedéseknek magukban kell foglalniuk olyan mechanizmusokat és eljárásokat, amelyek biztosítják a szolgáltatások rendelkezésre állását, valamint az adatok valódiságának, integritásának és bizalmas jellegének védelemét.

iii. Az Európai Parlament és a Tanács 2014/65/EU irányelve (2014. május 15.) a pénzügyi eszközök piacairól, valamint a 2002/92/EK irányelv és a 2011/61/EU irányelv módosításáról[43]

A kereskedési helyszínek tekintetében a 2014/65/EU irányelv 48. cikkének (1) bekezdése előírja a működtetők számára, hogy biztosítsák szolgáltatásaik folyamatosságát, amennyiben a kereskedési rendszerekben meghibásodás következne be. Ezt az általános kötelezettséget a közelmúltban pontosította és kiegészítette a 2014/65/EU európai parlamenti és tanácsi irányelvnek a kereskedési helyszínekre vonatkozó szervezeti követelményeket meghatározó szabályozástechnikai standardok tekintetében történő kiegészítéséről szóló, 2016. július 14-i (EU) 2017/584 felhatalmazáson alapuló bizottsági rendelet[44] [45]. Különösen e rendelet 23. cikkének (1) bekezdése előírja, hogy a kereskedési helyszíneknek fizikai és elektronikus biztonsági eljárásokat és mechanizmusokat kell kialakítaniuk a rendszereik rendellenes használattól vagy jogosulatlan hozzáféréstől való védelmének és az adatok integritásának biztosítása érdekében. Ezen intézkedéseknek lehetővé kell tenniük az információs rendszerek elleni támadások kockázatának megelőzését vagy minimálisra csökkentését.

A 23. cikk (2) bekezdése előírja továbbá, hogy a működtetők által hozott intézkedéseknek és mechanizmusoknak lehetővé kell tenniük a jogosulatlan hozzáféréssel, az információs rendszerek működését súlyosan akadályozó vagy megszakító rendszerzavarokkal, illetve az adatok rendelkezésre állását, integritását vagy hitelességét veszélyeztető adatzavarokkal kapcsolatos kockázatok haladéktalan azonosítását és kezelését. Emellett a rendelet 15. cikke arra kötelezi a kereskedési helyszíneket, hogy rendszereik kellő stabilitásának biztosítása és a rendszerzavarok kezelése érdekében hatékony üzletmenet-folytonossági intézkedésekkel rendelkezzenek. Ezeknek az intézkedéseknek különösen lehetővé kell tenniük az üzemeltető számára, hogy a kereskedés két órán belül vagy ahhoz közeli időtartamon belül helyreálljon, és hogy az elveszett adatmennyiség a nullához közelítsen.

[43] HL L 173., 2014.6.2., 349. o.
[44] HL L 87., 2017.3.31., 350. o.
[45] http://ec.europa.eu/finance/securities/docs/isd/mifid/rts/160714-rts-7_en.pdf

Továbbá a 16. cikk kimondja, hogy a rendszerzavarok kezelésére meghatározott intézkedéseknek a kereskedési helyszínek üzletmenet-folytonossági tervének részét kell képezniük, és meghatároz olyan konkrét elemeket, amelyeket a működtetőnek az üzletmenet-folytonossági terv elfogadásakor figyelembe kell vennie (pl. különleges biztonsági műveleti csoport létrehozása, a kockázatokat azonosító hatásvizsgálat elvégzése és annak időszakos felülvizsgálata).

A biztonsági intézkedések tartalmát figyelembe véve úgy tűnik, hogy azok az adatok vagy a nyújtott szolgáltatások rendelkezésre állásával, hitelességével, integritásával és bizalmas jellegével kapcsolatos kockázatok kezelésére és megoldására irányulnak, és ennek eredményeként megállapítható, hogy a fent említett ágazatspecifikus uniós jogszabály olyan biztonsági kötelezettségeket tartalmaz, amelyek hatása legalább egyenértékű a kiberbiztonsági irányelv 14. cikkének (1) és (2) bekezdésében foglalt vonatkozó kötelezettségekével.

5.2. A kiberbiztonsági irányelv 1. cikkének (3) bekezdése: távközlési szolgáltatók és bizalmi szolgáltatók

Az 1. cikk (3) bekezdése értelmében az irányelvben megállapított biztonsági és bejelentési követelmények nem alkalmazandók a 2002/21/EK irányelv 13a. és 13b. cikkében foglalt követelmények hatálya alá tartozó szolgáltatókra. A 2002/21/EK irányelv 13a. és 13b. cikke a nyilvános hírközlő hálózatokat szolgáltató és a nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó vállalkozásokra vonatkozik. Következésképpen a nyilvános hírközlő hálózatok vagy a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása tekintetében a vállalatnak teljesítenie kell a 2002/21/EK irányelv biztonsági és bejelentési követelményeit.

Ugyanakkor, ha ugyanaz a vállalat más szolgáltatásokat is biztosít, így például a kiberbiztonsági irányelv III. mellékletében felsorolt digitális szolgáltatásokat (pl. felhőalapú számítástechnika vagy online piactér) vagy olyan szolgáltatásokat, mint például a kiberbiztonsági irányelv II. mellékletének 7. pontja szerinti DNS vagy IXP, a vállalatra e szolgáltatások nyújtása tekintetében vonatkoznak a kiberbiztonsági irányelv biztonsági és bejelentési követelményei . Meg kell jegyezni, hogy mivel a II. melléklet 7. pontjában felsorolt szolgáltatások nyújtói az alapvető szolgáltatásokat nyújtó szereplő kategóriájába tartoznak, a tagállamok kötelesek az 5. cikk (2) bekezdése szerinti azonosítási eljárást lefolytatni, és meghatározni, hogy a DNS-, az IXP- vagy a TLD-szolgáltatásokat nyújtó egyes szolgáltatók közül melyeknek kell megfelelniük a kiberbiztonsági irányelv követelményeinek. Ez azt jelenti, hogy az ilyen értékelést követően kizárólag a kiberbiztonsági irányelv 5. cikkének (2) bekezdésében foglalt kritériumokat teljesítő DNS-, IXP- vagy TLD-szolgáltatók kötelesek teljesíteni a kiberbiztonsági irányelv követelményeit.

Az 1. cikk (3) bekezdése továbbá kimondja, hogy az irányelv biztonsági és bejelentési követelményei a 910/2014/EU rendelet 19. cikkében foglalt hasonló követelmények hatálya alá tartozó bizalmi szolgáltatókra sem alkalmazandók.

6. Közzétett nemzeti kiberbiztonsági stratégiai dokumentumok

	Tagállam	A stratégia címe és a rendelkezésre álló linkek
1.	Ausztria	*Austrian Cybersecurity Strategy (Osztrák kiberbiztonsági stratégia)* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf (EN)
2.	Belgium	*Securing Cyberspace (A kibertér biztosítása)* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ncss-be-fr (FR)
3.	Bulgária	*Cyber Resilient Bulgaria 2020 (Kiberreziliens Bulgária 2020)* (2016) http://www.cyberbg.eu/ (BG)
4.	Horvátország	*The national cyber security strategy of the republic of Croatia (A Horvát Köztársaság nemzeti kiberbiztonsági stratégiája)*(2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf (EN)
5.	Cseh Köztársaság	*National cyber security strategy of the Czech Republic for the period from 2015 to 2020 (A Cseh Köztársaság 2015 és 2020 közötti időszakra vonatkozó nemzeti kiberbiztonsági stratégiája)* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (EN)
6.	Ciprus	*A Ciprusi Köztársaság kiberbiztonsági stratégiája* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf (EN)
7.	Dánia	*The Danish Cyber and Information Security Strategy (A dán kiber- és információbiztonsági stratégia)* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/DK_NCSS.pdf (EN)
8.	Észtország	*Cyber Security Strategy (Kiberbiztonsági stratégia)* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf (EN)
9.	Finnország	*Finland´s Cyber security Strategy (Finnország kiberbiztonsági stratégiája)* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf (EN)

10.	Franciaország	*French national digital security strategy (Francia nemzeti digitális biztonsági stratégia)* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf (EN)
11.	Írország	*National Cyber Security Strategy 2015-2017 (A 2015–2017-es időszakra vonatkozó nemzeti kiberbiztonsági stratégia)* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf (EN)
12.	Olaszország	*National Strategic Framework for Cyberspace Security (A kibertér biztonságára vonatkozó nemzeti stratégiai keret)* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf (EN)
13.	Németország	*Cyber-security Strategy for Germany (Kiberbiztonsági stratégia Németország számára)* (2016) http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/ModerneVerwaltung-OeffentlicherDienst/Informationsgesellschaft/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile (DE)
14.	Magyarország	*National Cyber Security Strategy of Hungary (Magyarország nemzeti kiberbiztonsági stratégiája)* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf (EN)
15.	Lettország	*Cyber Security Strategy of Latvia 2014–2018 (Lettország 2014–2018 közötti kiberbiztonsági stratégiája)* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss (EN)
16.	Litvánia	*The programme for the development of electronic information security (cyber-security) for 2011–2019 (Az elektronikus információbiztonság [kiberbiztonság] fejlesztésének 2011–2019-re szóló programja)* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf (EN)
17.	Luxemburg	*National Cybersecurity Strategy II (II. nemzeti kiberbiztonsági stratégia) (2015)* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf (EN)
18.	Málta	*National Cyber Security Strategy Green Paper (A nemzeti kiberbiztonsági stratégiáról szóló zöld könyv)* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSSGreenPaper.pdf (EN)
19.	Hollandia	*National Cyber Security Strategy 2 (2. nemzeti kiberbiztonsági*

		stratégia) (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf (EN)
20.	Lengyelország	*Cyberspace Protection Policy of the Republic of Poland (A Lengyel Köztársaság kibertérvédelmi politikája*(2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf (EN)
21.	Románia	*Cybersecurity Strategy of Romania (Románia kiberbiztonsági stratégiája)* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf (RO)
22.	Portugália	*National Cyberspace Security Strategy (Nemzeti kibertérbiztonsági stratégia* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/portuguese-national-cyber-security-strategy/view (EN)
23.	Szlovák Köztársaság	*Cyber Security Concept of the Slovak Republic for 2015 – 2020 (A Szlovák Köztársaság kiberbiztonsági koncepciója a 2015–2020 közötti időszakra)* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1 (EN)
24.	Szlovénia	*Cyber Security Strategy establishing a system to ensure a high level of cyber security (A kiberbiztonság magas szintjét biztosító rendszert létrehozó kiberbiztonsági stratégia)* (2016) http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Cyber_Security_Strategy_Slovenia.pdf (EN)
25.	Spanyolország	*National Cyber Security Strategy (Nemzeti kiberbiztonsági stratégia)* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf (EN)
26.	Svédország	*The Swedish National Cybersecurity Strategy (A svéd nemzeti kiberbiztonsági stratégia)* (2017) http://www.government.se/49edf4/contentassets/b5f956be6c50412188fb4e1d72a5e501/fact-sheet-a-national-cyber-security-strategy.pdf (EN)
27.	Egyesült Királyság	*National Cyber Security Strategy (2016-2021) (Nemzeti kiberbiztonsági stratégia) (2016–2021)* (2016) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf (EN)

7. Az ENISA által kiadott ajánlások és bevált gyakorlatok jegyzéke

A biztonsági eseményekre való reagálásra vonatkozóan

- ✓ A biztonsági eseményekre való reagálásra és a kiberbiztonsági válsághelyzetekben folytatott együttműködésre vonatkozó stratégiák[46]

A biztonsági események kezelésére vonatkozóan

- ✓ A biztonsági események kezelésének automatizálására irányuló projekt[47]
- ✓ Iránymutatás a biztonsági események kezelésére vonatkozó bevált gyakorlatokról[48]

A biztonsági események osztályozására és taxonómiájára vonatkozóan

- ✓ A meglévő taxonómiák áttekintése[49]
- ✓ Iránymutatás a taxonómiáknak a biztonsági események megelőzése és felderítése terén történő használatára vonatkozó bevált gyakorlatokról[50]

A CSIRT-ek fejlettségi szintjére vonatkozóan

- ✓ A nemzeti CSIRT-ek előtt álló kihívások Európában 2016-ban: tanulmány a CSIRT-ek fejlettségi szintjéről[51]
- ✓ Tanulmány a CSIRT-ek fejlettségi szintjéről – értékelési eljárás[52]
- ✓ Útmutató a nemzeti és kormányzati CSIRT-ek számára a fejlettségi szint értékelésének módjáról[53]

A CSIRT-ek kapacitásépítésére és képzésére vonatkozóan

- ✓ Iránymutatás a képzési módszerekre vonatkozó bevált gyakorlatokról[54]

---

[46] ENISA, *Strategies for incident response and cyber crisis cooperation (Az eseményekre való reagálásra és a kiberbiztonsági válsághelyzetekben folytatott együttműködésre vonatkozó stratégiák)* (2016). A következő internetcímen érhető el:https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation

[47] További információk: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation

[48] ENISA, *Good Practice Guide for Incident Management (Iránymutatás a biztonsági események kezelésére vonatkozó bevált gyakorlatokról)* (2010). A következő internetcímen érhető el:https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

[49] További információk: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies

[50] ENISA, *A good practice guide of using taxonomies in incident prevention and detection (Iránymutatás a taxonómiáknak a biztonsági események megelőzése és felderítése terén történő használatára vonatkozó bevált gyakorlatokról)* (2017). A következő internetcímen érhető el:https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection

[51] ENISA, *Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity (A nemzeti CSIRT-ek előtt álló kihívások Európában 2016-ban: tanulmány a CSIRT-ek fejlettségi szintjéről)* (2017). A következő internetcímen érhető el:https://www.enisa.europa.eu/publications/study-on-csirt-maturity

[52] ENISA, *Study on CSIRT Maturity – Evaluation Process (Tanulmány a CSIRT-ek fejlettségi szintjéről – értékelési eljárás)* (2017). A következő internetcímen érhető el:https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process

[53] ENISA, CSIRT-képességek. *How to assess maturity? Guidelines for national and governmental CSIRTs (Hogyan értékeljük a fejlettségi szintet? Útmutató a nemzeti és kormányzati CSIRT-ek számára)* (2016). A következő internetcímen érhető el: https://www.enisa.europa.eu/publications/csirt-capabilities

Az Európában létező CSIRT-ekkel kapcsolatos tájékozódáshoz – A CSIRT-ek országonkénti áttekintése[55]

[54] ENISA, *Good Practice Guide on Training Methodologies (Iránymutatás a képzési módszerekre vonatkozó bevált gyakorlatokról)* (2014). A következő internetcímen érhető el:https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies

[55] További információk: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map