NÉMETH GYULA

# A NIS irányelv és Magyarország kiberstratégiája

## Bevezetés

A NIS irányelvek (Az Európai Parlament és a Tanács (EU) 2016/1148 Irányelvének (2016. III. 6.) a hálózati és információs rendszerek biztonságának az egész unióban egységesen magas szintjét biztosító intézkedésekről) megalkotását megelőzte egy olyan széles körű társadalmi párbeszéd és konzultáció, amelynek az volt a célja és fő kérdése, hogy a tagállamok együttes erővel hogyan tudják felvenni a harcot a kibertér elleni, de a társadalmat és a gazdaságot is érintő rosszindulatú támadások ellen. Tekintettel arra, hogy a létesítmények többsége be van kapcsolva a kibertér hálózatának vérkeringésébe, az onnan érkező támadások nemcsak az érintett objektumot veszélyeztetik, hanem nemzetbiztonsági kockázatot is jelentenek. Ezek a támadások veszélyeztetik a létfontosságú szolgáltatásokat, jelentős veszteséget okozva ezzel a tagállamok gazdaságainak és negatív hatást gyakorolnak.

Az Európai Unión belül a határokon átnyúló kommunikációs szolgáltatások révén a tagállamok összeköttetésben vannak, így a digitális rendszerek nagy szerepet játszanak az áruk, a szolgáltatások, a személyek határon átnyúló szabad mozgásának elősegítésében. A hálózati rendszerek esetleges sikeres támadása az egész unión belül digitális katasztrófához vezethet.

A NIS irányelv (hálózati és információs rendszerek biztonságáról szóló dokumentum, amely geopolitikai alapon határoz szabályokat és együttműködést egyes intézmények számára)[1] megjelenése előtt az uniós tagállamok esetében önkéntes megközelítést alkalmaztak, amely azt jelentette, hogy az

[1] Nemzeti Kibervédelmi Intézet: http://www.cert-hungary.hu/nis_directive

egyes tagállamok saját hatáskörben alkalmaztak információ- és hálózatbiztonsági lépéseket. A hálózatok és a rendszerek egymáshoz kapcsolódása, így azok az országok, ahol a védelem nem megfelelő, részben és egészében is gyengíti az Európai Unió rendszer- és hálózatbiztonsági szintjét. Ez kihatással volt a piaci szereplők egymás iránti bizalmára, amely elengedhetetlen az együttműködéshez. Az irányelvek kialakítása előtt nem létezett olyan hatékony intézkedés és mechanizmus, amely lehetővé tette a tagállamok koordinált fellépését és együttműködését a kibertér fenyegetései ellen. Ma már az információ és hálózatvédelem nemcsak a vállalkozások versenyképességét csökkentheti, de azok teljes tönkretételéhez is elvezethet. A gazdasági károkon kívül jelentősek a társadalomra mért negatív hatások is, melyek mértéke ma nehezen mérhető számokban. Ezeket a veszélyeket az Európai Unió tagállamai már korán felismerték, ezért olyan mechanizmusokat és célkitűzéseket dolgoztak ki, amelyek hozzájárultak a NIS irányelvek egységes elfogadásához.

## A NIS irányelv megalkotásának előzményei

A NIS megalkotását megelőzte egy nemzeti illetékes hatóság felállítására irányuló elképzelés, amely a hálózat- és információbiztonság területén jelentős előrelépés volt. Ezen túl a NIS javaslata tartalmazza hálózatbiztonsági veszélyhelyzetet elhárító csoportok (CERT-ek) felállítását is [NIS irányelv (34)].

A tagállamok közigazgatásának és a magánszférájának szereplői az irányelvek mentén kötelesek lesznek az illetékes hatóságoknak jelentést tenni a hálózati rendszereiket veszélyeztető eseményekről, az összehangolt információcserére, a fenyegetések és támadások elleni küzdelem és a közös kockázatkezelés érdekében. Így az irányelv biztosítja azt a közös kockázatkezelési struktúra kialakulását a tagállamokon belül, ami korábban nem volt jellemző a tagállamokon belül, a közszféra és a magánszféra vonatkozásában [NIS irányelv, IV. fejezet. 14. cikk].

Az Európai Bizottság 2012. július 23. és október 15. között egy online nyilvános konzultációt tartott „A hálózat- és információbiztonság javítás az EU-ban” címmel. A konzultáció legfontosabb tapasztalata az volt, hogy a

válaszadók nagy többsége (82 %-a) egyet értett azzal a felvetéssel, hogy az információbiztonság területén nagyobb együttműködésre van szükség az Európai Unión belül. A válaszadók a bankszektorban, az internetes szolgáltatások, valamint a közigazgatás területén is fontosnak tartották bevezetni szabályozási és hálózat- és információbiztonsági követelményeket. A konzultációt számos fórum, illetve egyes tagállamok közötti kétoldalú találkozó követte, ahol szintén a tagállamok véleményét kérték ki az ügyben. Az Európai Bizottság és az Európai Külügyi Szolgálat 2012. július 6-án összehívott egy kiberbiztonsági konferenciát, ahol szintén a tagállamok információcseréje volt a cél a témát érintően.

Az irányelv jogalapját az Európai Unió működéséről szóló szerződés adja, amely szerint az Európai Unió hatáskörrel rendelkezik a belső piac működésének biztosítása érdekében. A hálózati- és információs rendszerek az áruk, a szolgáltatások és a személyek szabad mozgásának érdekében fontos szerepet játszanak, mivel a hálózatok azon túl, hogy egymáshoz kapcsolódnak, a fizikális határokon átívelő, globális természetűek. Vagyis egy, a hálózatot érintő fenyegetés vagy zavar a belső piac működésére is hatással lehet. A NIS irányelv a szubszidiaritás elvén nyugszik vagyis, hogy a tagállamok közötti koordináció és közös fellépés érdekében egyeztetni kell, a kormányok által elfogadott hálózat- és információbiztonsági intézkedéseket össze kell hangolni, hogy a közös szakpolitikai fellépés kellő mértékben segítse elő a személyes adatok és a magánélet védelméhez fűződő jog hatékony érvényesülését. A nyilvános konzultáció során egyértelművé vált, hogy a kiemelkedő létesítmények védelme elengedhetetlen. Továbbá az is napirendre került, hogy a mikrovállalkozások esetében a hálózati- és információs rendszerek biztonsági követelményeit nem szabad alkalmazni, mert azokra aránytalanul nagy terhet jelentene az új rendszer bevezetése. Tehát azok a piaci és közigazgatási szereplők állapítják meg a kockázati tényezőket, akik a kockázatok enyhítésére alkalmas intézkedés kidolgozását is vállalni tudják [NIS irányelv (75)].

## A NIS irányelvek hálózatbiztonsági intézkedéseket elősegítő célkitűzései

A NIS irányelvek célja egy olyan egységesen magas szintű hálózatbiztonság megteremtése, amely képes megfelelő szintű védelmet nyújtani az EU vállalkozásai és állampolgárai részére is. Ehhez meg kell erősíteni az egyes tagállamok társadalmi és gazdasági rendszereinek védelmét és biztonságát, különös tekintettel az internet és az információs rendszerek és hálózatok védelmére. Elő kell írni a tagállamok számára, az együttműködést és a védelmi felkészültség fokozását, az állandó nyomon követési mechanizmusok alkalmazását. A gazdaságon belül a kritikus szektorok (energiaügy, bankszektor) bevonásával olyan intézkedéseket kell elfogadni, amely letéteményül szolgál a magas szintű védelemhez. Ezen túlmenően nagy gondot kell fordítani a kockázatkezelésre, illetve a rendkívüli események egy, az illetékes hatóságnak való jelentési kötelezettségre is. [NIS irányelv, II. sz. melléklet]

A stratégia biztosítja a megbízható digitális környezetet úgy, hogy közben figyelembe veszi az Európai Unió alapvető értékeinek megőrzését és védelmét. Az irányelv kiegészülve a tagállamok saját nemzeti kibertér biztonságára irányuló intézkedéseivel tudatos és határozott fellépést biztosítanak a számítástechnikai bűnözés elleni védekezésben. A hálózat- és információbiztonság jelentős mértékben a közigazgatási rendszerek felelőssége is. Ezért az irányelv kiemeli azt, hogy kizárólag közigazgatás ágazataira gyakorolt célzott motivációval lehet eredményt elérni a kockázatkezelésben, figyelembe véve az egyenlő versenyfeltételeket is. Ez a célzott motiváció pedig nem más, mint egy központi szabályozás kialakítása, ami az egyes tagállamokra lebontva épülhet be a közigazgatási rendszerekbe mint védelmi stratégia és kockázatkezelési gyakorlat. Kiemeli annak jelentőségét is, hogy a védelem megfelelően magas szintre emelése érdekében a magán- és az állami szektor között, az eddiginél jóval erősebb együttműködés szükséges. Ösztönözni szükséges tehát a piaci szereplőket arra, hogy együttműködjenek az állami szereplőkkel és a sikeres kooperáció érdekében osszák meg egymással információikat és kockázatkezelési gyakorlatu-

kat. Az így kialakuló információcsere alapja egy biztonságos infrastruktúra. A kockázatos vagy támadó jellegű eseményeket pedig egy központi hatóságnak kell jelenteniük. A tagállamoknak rendelkezni kell tehát egy kiválóan működő, a vészjeleket korai szakaszban prognosztizáló és elhárító csoportnak, amely az együttműködést a különböző csoportok között megfelelő szintre hozva a lehető legerősebb védelmi mechanizmust tudja kidolgozni [NIS irányelv, (34)]. Ennek érdekében valamennyi tagállam az irányelvek mentén egy nemzeti stratégiát fogad el, amely tartalmazza a konkrét intézkedéseket a hálózat- és információbiztonság elérése és megtartása érdekében.

A tagállamok stratégiáinak tartalmaznia szükséges a kormányzati szervek és az egyéb érintettek konkrét feladatainak meghatározását, a veszélyhelyzetekre való felkészülést, a reagálás intézkedéseit, valamint a társadalom szegmensei közti együttműködés lépéseit is. Ennek érdekében minden tagállam stratégiájának tartalmaznia kell oktatási és képzési terveket, amely a társadalom tudatosságra ösztönzését szolgálja. Fontos eleme továbbá egy olyan kockázatkezelő és kockázatértékelő terv is, amelynek része a veszélyek azonosítása, illetve az érintett szereplők feladatainak a meghatározása. A tagállamok stratégiáinak ki kell térnie a megelőzést és reagálást szolgáló kommunikációs folyamatokra is, és rendelkezni szükséges a megfelelő hálózat és információbiztonsági gyakorlatokra irányuló elképzelésekkel, amelyek tesztelése után az eredményeket dokumentálás után be lehet építeni a kockázatkezelési tervekbe.

Minden tagállamnak ki kell jelölnie egy nemzeti illetékes hatóságot, amely az információs rendszerek biztonságáért lesz felelős, mégpedig úgy, hogy ezek a hatóságok az irányelvek betartását hivatottak nyomon követni az egyes tagállamokban [NIS irányelv, (34)]. A tagállamoknak biztosítaniuk szükséges, hogy a hatóságoknak a célok teljesítéséhez megfelelő műszaki, pénzügyi és emberi erőforrás álljon rendelkezésre [NIS irányelv, (31)]. Az illetékes hatóságok és a bizottság együttműködési hálózatot hoznak létre az információs rendszereket érintő támadások megelőzése és leküzdése érdekében. Az együttműködés keretében előrejelzéseket tesznek közzé a kockázatokról, gondoskodnak a megfelelő intézkedések kidolgo-

zásáról és végrehajtásáról. Közös honlapot üzemeltetnek, ahol nem bizalmas információkat tesznek közzé a válaszintézkedésekről és az előrejelzésekről. Fontos, hogy a NIS alapján együttműködnek a Számítástechnikai Bűnözés Elleni Európai Központtal, illetve más olyan szervezettel, amely az energiaszolgáltatást, a közlekedést, a banki szférát és valamely kulcsfontosságú szektort érint.[2]

## A hálózatbiztonsági elhárító csoportok

A tagállamoknak a nemzeti stratégián túl fel kell állítaniuk úgynevezett hálózatbiztonsági veszélyeket elhárító csoportokat (CERT). Ezeknek a csoportoknak az a feladatuk, hogy biztosítsák a hírközlési szolgáltatások elérhetőségét a kapcsolattartás és az együttműködés érdekében. A CERT a hozzá érkező információkat bizalmasan kezeli, az információk sérthetetlensége érdekében pedig fokozott biztonsági intézkedéseket hoz létre [NIS irányelv, IV. fejezet, 14. cikk]. Éppen ezért a CERT irodáit biztonságos helyszíneken szükséges felállítani, ahol adott a megfelelő rendszer és az infrastruktúra folytonossága, védelme, valamint a megfelelő számú és felkészültségű személyzet.

A CERT legfontosabb feladatai közé tartozik az események nyomon követése, a veszélyek előrejelzése, a riasztás, a bejelentések megtétele és az információ terjesztése az érintett csoportok vonatkozásában. Tevékenységi körükhöz tartozik még a rendkívüli eseményekkel szembeni válaszintézkedések megtétele, a helyzetmegfigyelés és a kockázatkezelés. Az oktatási kampányok megszervezésére és a széles körű ismeretterjesztésre is kiemelt figyelmet kell fordítaniuk.

A CERT-ek együttműködést alakítanak ki a magánszféra szereplőivel, méghozzá olyan szabványosított gyakorlatokon mint a kockázatkezelési eljárások, a kockázatok mérésére vonatkozó ismeretek, illetve az információcseréhez használatos formátumok [NIS irányelv, II. fejezet, 7. cikk].

[2] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve: http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.HUN&toc=OJ:L:2016:194:TOC

A CERT-ek tevékenységét az illetékes hatóság felügyeli és a tagállamok tájékoztatást nyújtanak a biztosságnak a CERT rendelkezésre álló forrásairól.[3]

## A NIS és Magyarország nemzeti kiberbiztonsági stratégiájának összehasonlítása

Magyarország nemzeti kiberbiztonsági stratégiája a fent említett vonulatok mentén született, érvényesítve azokat a stratégiai alapelveket, amelyek az irányelv szabott az uniós tagállamok részére. Ezen kívül azokat a speciális feladatokat is, amelyek a NIS, illetve a kormányhatározat összevetése által célkitűzésként jelentek meg, mivel a NIS rendelkezései részben tükröződnek Magyarország nemzeti kiberbiztonsági stratégiájában.

Az irányelv öt fejezetben tárgyalja a hálózat- és információbiztonságnak az egész unióban egységesen magas szintjére vonatkozó intézkedéseket. Az érdekelt felekkel folytatott konzultációk és a hatásvizsgálatok eredményei alapján az „Irányelv" olyan intézkedéseket állapít meg a tagállamok részére, amelyek biztosítják a hálózat- és információbiztonság magas szintjét. Valamennyi tagállamra, így Magyarországra is olyan kötelezettségeket ír elő, mint például a hálózati és információs rendszereket érintő kockázatok és biztonsági események megelőzése, kezelése, valamint az azokra való reagálás.

A 1139/2013. (III.21.) kormányhatározat az alaptörvénnyel összhangban határoz meg nemzeti célokat, stratégiai irányokat, feladatokat és olyan átfogó kormányzati eszközöket, amelyek alapján Magyarország érvényesíteni tudja nemzeti érdekeit a magyar kibertérben is. Az irányelv okai és céljai között szerepel az információbiztonság, illetve a szolgáltatásokhoz szükséges megbízható környezet megteremtése azért, mert az információs rendszerek olyan eseményeknek vannak kitéve, mint a műszaki meghibásodások, illetve a rosszindulatú támadások.

[3] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve: http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.HUN&toc=OJ:L:2016:194:TOC

A kormányhatározatban alapvetés, hogy Magyarország nemzeti kiberbiztonsági stratégiája hatékony védelmi intézkedések útján a megelőzésre épül. Az irányelv meghatározza a hálózati és információs rendszerek biztonságáért felelős nemzeti illetékes hatóság kijelölését, a kormányhatározat feladatként említi ebben a tekintetben a Miniszterelnökség keretében megvalósuló kormányzati koordinációt.

Az irányelv vészhelyzeteket elhárító csoportok (CERT) felállítását írja elő a tagállamok számára. A CERT által akkreditált tagszervezet működő kormányzati eseménykezelő központok végzik a kiberbiztonsági eseményekkel kapcsolatos feladatok ellátását. Az „Általános rendelkezései" között kitér arra, hogy a tagállamok piaci szereplőire és a közigazgatásokra biztonsági követelményeket állapít meg.[4]

A kormányhatározat „Szabályozás" pontja kimondja, hogy a civil, tudományos, és a gazdasági élet szereplőivel együttműködési megállapodásokat kell kötni, amelyek alapot, nyújtanak egy hatékony kiberbiztonsági rendszer működtetéséhez.

Magyarország nemzeti kiberbiztonsági stratégiája a „Tudatosság" ponton belül kitér a hazai és nemzetközi szakmai fórumok szervezésével kapcsolatos feladatokra, amely a javaslatnak nem képezi a részét.[5]

Szintén különbség a két dokumentum között, hogy a kormányhatározat külön kitér az „Oktatás, kutatás-fejlesztés" pontban a közép- és felsőoktatásban, valamint a kormányzati tisztviselők képzésében, illetve a szakmai továbbképzéseken a kiberbiztonság szakterületének integrálódására az informatikai oktatásba. A „Gyermekvédelem" pont alatt a kormányhatározat rögzíti, hogy a kiberbiztonság lényegi elemének tartja a gyermekek és fiatalok számára biztonságos online környezetet, illetve a tudatosságnövelő és felkészítő intézkedések támogatását. Az irányelv erre külön nem tér ki.

Az irányelv fontos eleme a gazdasági szereplők motiválása a legmagasabb szintű kiberbiztonsági intézkedések megtételére, a kormányhatározat ezt külön a „Gazdasági szereplők motiválása" pontban fejti ki, kiegészítve

[4] 1139/2013. (III.21.) Korm. határozat: http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK13047.pdf

[5] 1139/2013. (III.21.) Korm. határozat: http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK13047.pdf

a nemzetközi tanúsítványoknak való megfelelést, valamint a gazdasági élet szereplőivel való közös ösztönző intézkedések kidolgozását.

## Az Európai Parlament és a Tanács (EU) 2016/1148 Irányelvének legfontosabb célkitűzései

A NIS irányelv célja egy magas szintű és egységes hálózat- és információbiztonság kialakítása. A tagállamok számára tehát elő kell írni azt, hogy milyen módszerekkel tudják a biztonsági készültségüket fokozni, fenntartani, az ebbéli törekvéseiket támogatni szükséges [NIS irányelv, (36), (42), II. fejezet 7. cikk]. Az irányelv hangsúlyozza, hogy ennek érdekében a tagállamok közigazgatásainak a megfelelő intézkedések meghozatalán túl a biztonsági kockázatok kezelésére is gondot kell fordítani [NIS irányelv, (56), 25. cikk]. A rendkívüli támadásokat, eseményeket pedig az illetékes hatóságnak azonnal jelenteni.

A NIS rávilágít, hogy nem elegendő az eddigi „önkéntes megközelítés" gyakorlata, mert ez nem nyújt megfelelő védelmet a támadások és a kockázatok ellen. A másik lényeges elem, amiért szükség volt egy egységes kockázatkezelési és védelmi arculat kialakítására, hogy a tagállamok különböző képességekkel és felkészültséggel rendelkeznek, ezért az Európai Unióban túl sokféle információbiztonsági megközelítés érvényesül. Ráadásul egyes tagállamokban gyengék a védelmi rendszerek, ami az együttműködésre és az információk áramlására és megosztására is hatással van, így kizárólag a magas szintű képességekkel rendelkező tagállamok tudnak hatékonyan együttműködni ebben a kérdésben.[6]

Fontos momentum továbbá, hogy a NIS irányelveket megelőző szabályozás kizárólag a távközlési vállalatok részére írta elő kockázatkezeséi intézkedések megalkotását és a támadások jelentését, holott a gazdaság többi ágazatát (például a bankszféra, tőzsde, energiatermelés) is indokolt lenne

[6] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve: http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.HUN&toc=OJ:L:2016:194:TOC

bevonni a hálózat- és információbiztonságba, mivel ezen ágazatok információbiztonsága kiemelkedő jelentőségű. Összességében a szakemberek jól érzékelték, hogy egységes szabályozás és új védelmi módszerek megosztása nélkül a fejletlen elhárító technológiával rendelkező tagállamok könnyű célpontjai lehetnek a kibertérből érkező támadásoknak.

## Összegzés

Jól látható, hogy a biztonságos és ellenálló hálózat, illetve az információs rendszerek feltétele a NIS irányelvekben meghatározott stratégiai lépések egymásutánisága, az egymásra épülő biztonsági lépések betartása. A biztonság kialakítása során a tagállamok különböző kormányzati intézkedésekkel biztosítják, hogy a közigazgatás és a piac szereplői az általuk használt hálózatok biztonságát veszélyeztető események ellen közösen lépjenek fel. Az illetékes hatóságoknak való bejelentési kötelezettség tovább növeli a tagállamok biztonságát, mivel a hatóság különböző utasításokat adhat a tagállam hálózatbiztonságának megerősítése érdekében. Tehát a rosszindulatú fenyegetések és támadások kivédése ellen egy hatékony és magas színvonalú védelem kialakítása biztosított.

A hálózatok kibertámadás elleni védelme költséges, és szükséges a kormányzati és piaci szereplők együttműködése is. Ennek hiánya veszélyezteti a társadalom különböző rétegeinek a biztonságérzetét, csökkenti az államba vetett bizalmat, de a gazdasági szereplők léte is függhet a megfelelő szintű biztonsági kritériumok elérésétől.

Megállapítható, hogy az irányelv és a kormányhatározat a kiberbiztonság fontosságának a hangsúlyozására épül, ennek összes elemét és célkitűzéseit számba veszi, de Magyarország nemzeti kiberbiztonsági stratégiája árnyaltabban részletezi a szabad és biztonságos kibertér fontosságát. Lényeges, hogy mindkét szabályozás alapos, és megfelelő védelmet nyújt azok számára, akik a rendelkezéseket betartják. Azt is fontos megjegyezni, hogy a védelem költséges, és a kisebb vállalkozásoknak irreálisan nagy terheket róna a teljes rendszer alkalmazása. A jövő egyik fontos feladata, hogy erre a kihívásra megfelelő választ keressenek a döntéshozók, továbbá a piac

szereplői is megértsék, hogy a XXI. század biztonságos gazdasági környezetének kialakítása elképzelhetetlen a kiberbiztonság folyamatos, magas szinten tartása, illetve az új védelmi mechanizmusok nélkül.