Védelem Tudomány 2024. különszám
„VIII. Rendvédelmi Adatvédelmi és Adatbiztonsági Szakmai Napok”
Konferenciaközlemény

A NIS2 irányelv kihívásai és gyakorlati alkalmazása

Challenges and Practical Application of the NIS2 Directive

Dr. Krasznay Csaba
Nemzeti Közszolgálati Egyetem, Államtudományi és Nemzetközi Tanulmányok Kar,
Kiberbiztonsági Tanszék
egyetemi docens
Email: krasznay.csaba@uni-nke.hu
ORCID: 0000-0003-3216-2592

Bevezetés

A NIS2 irányelv az Európai Unió kritikus infrastruktúrák kibervédelmét célozza, erősítve a szervezetek rezilienciáját a kiberbiztonsági fenyegetésekkel szemben. A jogszabály egy egységes európai keretrendszert alakít ki, amely 2024-ben vált hatályossá. Az előadás a 21. cikk által előírt követelményeket, például a kockázatelemzést, az eseménykezelést és a tudatosságnövelést részletezi. Emellett Magyarország úttörő szerepét is bemutatja, amely az európai szabályozás egyik legszigorúbb implementációját valósította meg. Az összefoglaló célja, hogy rámutasson a NIS2 irányelv jelentőségére, valamint az európai és magyar kontextusban jelentkező kihívásokra. Az irányelv sikeres alkalmazása nemcsak a megfelelőséget, hanem a kontinens kibervédelmi szintjének növekedését is eredményezheti.

Introduction

The NIS2 Directive aims to enhance the cybersecurity resilience of critical infrastructures in the European Union, strengthening organizations' preparedness against cybersecurity threats. The legislation establishes a unified European framework, which came into force in 2024. The presentation elaborates on the requirements set forth by Article 21, such as risk analysis, incident management, and awareness-building. Additionally, it highlights Hungary's pioneering role, which implemented one of the strictest adaptations of the European regulation. The summary seeks to underline the significance of the NIS2 Directive and the challenges arising in the European and Hungarian contexts. The successful application of the directive may not only ensure compliance but also lead to a higher level of cybersecurity across the continent.

Kulcsszavak: kiberbiztonság, kritikus infrastruktúra, reziliencia, NIS2

Keywords: cybersecurity, critical infrastructure, resilience, NIS2

Kiberreziliencia Európában

A NIS2 irányelv, amely 2024-ben vált hatályossá, jelentős lépés az Európai Unió kritikus infrastruktúráinak védelme érdekében. Az irányelv célja, hogy javítsa az ellenállóképességet, kiberrezilienciát a kiberbiztonsági fenyegetésekkel szemben, miközben harmonizálja a tagállamok szabályozását.

Az előadás elsősorban a NIS2 irányelv részleteire fókuszált, különösen a 21. cikk által meghatározott követelményekre, Magyarország szerepére az implementációban, valamint a nemzetközi kiberbiztonsági kihívásokra.

A NIS2 irányelv előzményei

A NIS2 irányelv az Európai Unió első, 2016-ban életbe lépett NIS irányelvének továbbfejlesztése. Az eredeti NIS irányelv célja az volt, hogy a kritikus infrastruktúrák védelmének első uniós szintű szabályozási keretét biztosítsa. Az irányelv többek között az energetikai, közlekedési, egészségügyi és pénzügyi szektorokban működő szolgáltatókra, valamint a digitális infrastruktúra egyes részeire terjedt ki. Azonban az első NIS irányelv hatékonysága korlátozott volt, mivel a tagállamok eltérő módon értelmezték és hajtották végre a szabályozásokat. Ez a különbség nemcsak a szabályok alkalmazásában, hanem az érintett szektorok körének meghatározásában is megnyilvánult, ami a jogi harmonizáció hiányát eredményezte. [1]

Egy másik kihívás az volt, hogy a kiberfenyegetések fejlődése gyorsabbnak bizonyult, mint a jogszabályi környezet alkalmazkodóképessége. Az elmúlt években jelentősen megszaporodtak a zsarolóvírusok és az ellátási láncokban jelentkező támadások, valamint a kritikus infrastruktúrákat célzó államilag támogatott kiberműveletek. Az első NIS irányelv nem tudta megfelelően kezelni ezeket a kihívásokat, így szükségessé vált egy átfogóbb és modernebb szabályozás.

A NIS2 irányelv létrehozása és céljai

A NIS2 irányelvet azért hozták létre, hogy az elődjénél hatékonyabb és egységesebb jogi keretet biztosítson a kibervédelem terén. Az irányelv egyik fő célkitűzése a kritikus infrastruktúrák védelmének erősítése, különösen a digitalizáció által átalakított ágazatokban. Az irányelv kiterjesztette az érintett szektorok körét, és például az egészségügy, a közlekedés, az energiaipar, valamint a vízgazdálkodás mellett a gyártásra, digitális szolgáltatásokra és a távközlési szektorra is kiterjed. Így már olyan szektorokat is érint, amelyek nem hagyományos értelemben vett kritikus infrastruktúrák, de működésük alapvető fontosságú a társadalom és a gazdaság szempontjából.

A NIS2 célja a kiberreziliencia növelése, vagyis annak biztosítása, hogy a szervezetek képesek legyenek ellenállni a kibertámadásoknak, és gyorsan helyreállítani működésüket egy esetleges incidens után. Az irányelv kiemelt hangsúlyt helyez a tagállamok közötti együttműködésre, beleértve a kiberbiztonsági incidensekről szóló információk megosztását és az európai szintű fenyegetéskezelési stratégiák kidolgozását.

Az irányelv másik fontos célja a jogharmonizáció előmozdítása. A NIS2 szigorúbb követelményeket támaszt az érintett szervezetekkel szemben, például kötelezővé teszi a kockázatelemzést és az incidenskezelési folyamatok bevezetését. Ezen kívül az irányelv egyértelműbb szabályokat határoz meg a hatósági ellenőrzésekre, beleértve az auditok rendszerét és a nem megfelelőség esetén alkalmazható szankciókat. Ez jelentős előrelépés az első NIS irányelvhez képest, amely sok esetben nem rendelkezett konkrét követelményekről. [2]

A NIS2 irányelv jelentősége

A NIS2 irányelv hatása messze túlmutat a jogi megfelelésen. Az irányelv bevezetése nemcsak a szervezetek működését teszi biztonságosabbá, hanem hozzájárul az uniós szintű kiberbiztonsági kultúra kialakításához is. A tagállamok szorosabb együttműködése lehetővé teszi, hogy az egyes országok ne csak saját tapasztalataikra, hanem más tagállamok sikereire és hibáira is támaszkodjanak. Az egységes európai szabályozás révén a NIS2 irányelv hozzájárul ahhoz, hogy az unió hatékonyabban kezelje a globális kiberfenyegetéseket, miközben megőrzi gazdasági és társadalmi stabilitását.

A NIS2 irányelv emellett elősegíti a szervezeti szintű kiberbiztonsági intézkedések standardizálását. Az irányelv alapján a szervezetek kötelesek kidolgozni olyan belső politikákat és eljárásokat, amelyek biztosítják a folyamatos kiberbiztonsági megfelelést. Ezek az intézkedések nemcsak a támadások megelőzésére, hanem az incidensek utáni helyreállításra is kiterjednek, így átfogóbb védelmet nyújtanak, mint az első NIS irányelv.

A NIS2 irányelv létrehozása tehát világosan tükrözi az Európai Unió elkötelezettségét a kritikus infrastruktúrák és a digitális gazdaság védelme iránt. Az irányelv nemcsak a kiberbiztonság jelenlegi kihívásaira nyújt választ, hanem hosszú távon is elősegíti a fenyegetések kezelésére képes európai kiberbiztonsági ökoszisztéma kialakítását. A szabályozás hatása különösen fontos az egyre digitalizálódó világban, ahol a kiberbiztonság többé nem csupán technológiai kérdés, hanem alapvető gazdasági és társadalmi érdek.

A 21. cikk részletezése és jelentősége

A 21. cikk az irányelv központi eleme, amely világos követelményeket fogalmaz meg az érintett szervezetek számára. Elsőként a kockázatelemzés jelentőségét emeli ki, amely az alapját képezi minden hatékony kiberbiztonsági stratégiának. A kockázatelemzés célja az infrastruktúrákat fenyegető veszélyek azonosítása és a potenciális károk csökkentése érdekében szükséges intézkedések meghatározása. Például egy kritikus adatközpont esetében a fenyegetések azonosítása magában foglalja a fizikai és digitális támadások lehetőségét is, mint például a zsarolóvírus-támadások vagy a belső fenyegetések. A cikk követelményei közé tartozik továbbá az eseménykezelési folyamatok létrehozása, amelyek biztosítják, hogy az érintett szervezetek gyorsan és hatékonyan tudjanak reagálni a biztonsági eseményekre. Az események kezelése során például kiemelt jelentőséggel bír a pontos nyomonkövetés, a támadások dokumentálása és a gyors helyreállítás.

Az oktatás és tudatosságnövelés a 21. cikk további kulcselemei. Az emberi tényező a kiberbiztonság egyik leggyengébb pontja lehet, hiszen a felhasználók tudatlansága vagy hibái jelentős veszélyforrást jelenthetnek. Az oktatási programok célja, hogy felkészítsék a munkavállalókat az alapvető kiberbiztonsági szabályok betartására, mint például az erős jelszavak használata, az adathalász e-mailek felismerése vagy a biztonságos adatkezelési gyakorlatok.

Magyarország szerepe az implementációban

Magyarország a NIS2 irányelv egyik korai és meglehetősen szigorú adaptálója az Európai Unión belül, mivel az ország nemcsak időben implementálta a szabályozást, hanem az amerikai NIST Special Publication 800-53 Rev. 5 ajánlásain alapuló, rendkívül részletes megfelelési követelményeket is meghatározott. Az ország jogszabályi keretei egyedülállóak, és a 7/2024-es Miniszterelnöki Kabinetiroda rendelet révén biztosítják, hogy a kritikus infrastruktúrák megfeleljenek az irányelv előírásainak. Ezen belül kiemelt szerepet kapott a hatósági ellenőrzések és auditok rendszere, amely folyamatos monitorozással és szigorú ellenőrzésekkel biztosítja az előírások betartását. A magyarországi implementáció további érdekessége, hogy az ország mintegy 4000 érintett szervezet helyzetét rendezte az új szabályozás bevezetésével. [3]

Nemzetközi kiberbiztonsági kihívások

Az ENISA, az Európai Unió Kiberbiztonsági Ügynökségének jelentései szerint a globális kiberfenyegetések egyre növekvő kihívást jelentenek. Ezek közé tartoznak a zsarolóvírusok, amelyek jelentős károkat okozhatnak azáltal, hogy titkosítják a szervezetek adatait, majd váltságdíjat követelnek azok visszafejtéséért. Az ellátási láncokat érintő támadások szintén kiemelt veszélyforrást jelentenek, mivel ezek révén a támadók a beszállítói kapcsolatokon keresztül tudnak hozzáférni a szervezetek rendszereihez. Az információmanipuláció és a dezinformáció terjedése további komoly fenyegetést jelent, különösen a kritikus infrastruktúrák működésének szabotálása szempontjából. [4]

Az előadás részletezte, hogy az ilyen típusú fenyegetések milyen hatással vannak az európai és magyar szervezetek működésére. Például egy nemrégiben Magyarországon történt zsarolóvírus-támadás során egy nagyvállalat rendszerei teljesen működésképtelenné váltak, ami több millió eurós kiesést eredményezett. [5] Az ilyen események rávilágítanak arra, hogy a NIS2 irányelv milyen fontos szerepet játszik a szervezetek ellenállóképességének növelésében.

Tagállamok közötti együttműködés

A tagállamok közötti együttműködés a NIS2 irányelv egyik legfontosabb célkitűzése, amelynek megvalósítása érdekében az Európai Unió harmonizált szabályozási keretet hozott létre. Ez az együttműködés nemcsak a szabályozási keret egységesítését jelenti, hanem a tapasztalatok megosztását és a közös fenyegetéskezelési stratégiák kidolgozását is. Az előadás példákat hozott arra, hogyan segíti a tagállamok közötti információmegosztás a kiberbiztonság javítását, valamint hogyan járul hozzá az együttműködés a szabályozás hatékonyságának növeléséhez.

Hosszú távú hatások

Az előadás végül azt is tárgyalja, hogy milyen hosszú távú hatásokkal járhat a NIS2 irányelv alkalmazása. A szabályozás célja nemcsak a kiberbiztonsági incidensek számának csökkentése, hanem az érintett szervezetek felkészültségének javítása is. Ez különösen fontos a kritikus infrastruktúrák esetében, amelyek megfelelő védelme elengedhetetlen a társadalom és a gazdaság zavartalan működéséhez. Az előadás hangsúlyozta, hogy a NIS2 irányelv hosszú távon hogyan járulhat hozzá az európai kiberbiztonsági környezet megerősítéséhez.

Végkövetkeztetés

Az előadás során részletesen bemutatásra került a NIS2 irányelv jelentősége, Magyarország úttörő szerepe és a nemzetközi kiberbiztonsági kihívások. A bemutatott példák és elemzések rámutatnak arra, hogy a szabályozás megfelelő végrehajtása nemcsak a megfelelőséget biztosítja, hanem hosszú távon hozzájárulhat az infrastruktúrák megerősítéséhez is.

Összefoglalás és következtetés

A NIS2 irányelv jelentős lépés az európai kiberbiztonsági stratégia megvalósítása felé. Magyarország példája kiemeli, hogy az időben történő implementáció és a szigorú megfelelési követelmények kulcsfontosságúak a hatékonyság szempontjából. Az előadás rámutatott a kihívásokra, különösen a 21. cikkben megfogalmazott szervezeti felkészültség és a hatósági ellenőrzések terén, de hangsúlyozta, hogy a NIS2 irányelv hosszú távon a reziliencia erősítését és a kontinens kibervédelmének fejlődését szolgálja.

Irodalomjegyzék

[1] Vásárhelyi Örs „Magyarország kiberbiztonságának jövője az európai uniós NIS2 irányelv tükrében”, *Nemzetbiztonsági Szemle* 12. évfolyam (2024) 3. szám 18–35. doi: 10.32561/nsz.2024.3.2

[2] Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)

[3] 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről

[4] ENISA, „ENISA Threat Landscape 2024” European Union Agency for Cybersecurity, 2024. https://www.enisa.europa.eu/topics/threat-landscape

[5] UNIX Autóalkatrészek, „Hackertámadás - 2021.03.30.”, 2021. https://www.unixauto.hu/hirlevel/hackertamadas