NEMZETBIZTONSÁGI SZEMLE
12. évfolyam (2024) 3. szám 18–35. | DOI: 10.32561/nsz.2024.3.2

Vásárhelyi Örs[1]

Magyarország kiberbiztonságának jövője az európai uniós NIS2 irányelv tükrében

The Future of Cybersecurity in Hungary in the Light of the EU NIS2 Directive

Európát és az Európai Uniót az elmúlt években számos válság és megoldandó problémák érték. Talán a második világháború óta még sosem volt ennyire kiszámíthatatlan Európa biztonsága. Az orosz–ukrán háború és az azt megelőző konfliktusok rámutattak arra, hogy a kibertérben nemcsak az egymással ellenségeskedő felek számíthatnak fokozott támadásokra, de harmadik felek is, leginkább azon országok, amelyek valamelyik háborús fél ellátási láncának részét képezik. Ezért Európa és az Unió védelmi képességét folyamatosan fejleszteni kell, és valamennyi tagállam közreműködésével egységes, magas szintű rezilienciát kell megvalósítani több területen is. Elsődlegesen a kritikus infrastruktúrák tekintetében, amelynek védelmével a CER EU-s irányelv foglalkozik, valamint a kiberbiztonság területén kell egységes magas védelmi képességet létrehozni, amelynek alapjait a NIS2 irányelv hivatott megteremteni.

Kulcsszavak: *Európai Unió, kiberbiztonság, Magyarország, NIS2, NBSZ NKI, SZTFH*

Europe and the European Union have faced many crises and problems in recent years. Perhaps never since the World War II has Europe's security been so unpredictable. Russia's war in Ukraine and the conflicts that preceded it have shown that in cyberspace it is not only the warring parties that face increased attacks but also third parties, most notably countries that are part of the supply chain of one of the warring parties. Europe's and the EU's defence capabilities must therefore be continuously improved, and a high level of unified resilience must be achieved in several areas, with the cooperation of all Member States. First and foremost, there

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: vasarhelyi.ors.laszo@stud.uni-nke.hu

is a need to establish a common high level of defence capability in the area of critical infrastructure, which is addressed by the EU CER Directive, and in the area of cybersecurity, the basis for which is laid by the NIS2 Directive.

Keywords: *European Union, cybersecurity, Hungary, NIS2, SSNS NCSC, SZTFH*

Bevezető

A 21. század olyan kihívások elé állította társadalmunkat, amelyek korábban ismeretlenek voltak. Ezek a veszélyek elsődlegesen a kibertérben jelentkeztek. Ilyen jellegű biztonsági esemény volt a 2007-es észt kormány elleni DDoS-támadássorozat, amely ideiglenesen megbénította az észt kormányzat működőképességét. Az ukrán–orosz háború óta megnőtt a kibertámadások száma, elég a nemrég bekövetkezett francia kormányzati szerveket célpontba vevő támadássorozatra gondolni, amelyekért oroszbarát hackercsoportok vállalták a felelősséget. A kérdéssel már csak azért is szükséges foglalkoznunk, mivel az Európai Unióban a legtöbb állami és piaci szervezet digitalizációs folyamatokat kezdett el alkalmazni, ami egyrészt dicséretes és támogatandó, másrészt viszont számos kockázattal jár. Annak érdekében, hogy az ilyen jellegű fenyegetés hatásai a jövőben minimalizálhatók és a sikeresen végrehajtott támadások hatásai mérsékelhetők legyenek, megfelelő védelmi képességet kell kialakítani az állam, társadalom, valamint egyéb gazdasági szempontból fontos, nélkülözhetetlen rendszereken és azok szervezeteiben. Annak érdekében, hogy ezek a rendszerek megfelelő védelmi intézkedésekkel legyenek ellátva, az Unió 2022 decemberében elfogadta a NIS2 direktívát.

Az Európai Unió elektronikus információs rendszereit és ipari kiberfizikai rendszereit ért támadások száma az elmúlt években folyamatosan növekvő tendenciát mutatnak, és ez a világ régiói között is kiemelkedő méretű. Hazánkban fel kell készülnünk a 21. század egyik legnagyobb kihívásának, a kibertér fenyegetéseinek leküzdésére. Az új uniós irányelv ebben segítségünkre van, azonban Magyarország implementációs tevékenységének megfelelő végrehajtása kiemelten fontos, hiszen az elkövetkezendő években ez fogja meghatározni a hazai kibervédelem alapjait.

Jelen tanulmány célul tűzte ki, hogy felhívja a figyelmet Európa kiberbiztonsági helyzetére a legújabb nemzetközi kiberbiztonsági tanulmányok segítségével, továbbá bemutatja azon uniós direktívákat, különös tekintettel a NIS2-re, amelyek az elkövetkezendő években meg fogják határozni a térség kiberbiztonsági politikáját, valamint bemutatja a hazai implementáció eddig megvalósult folyamatait, és rávilágít a megvalósítási nehézségekre.

Kutatási módszertan

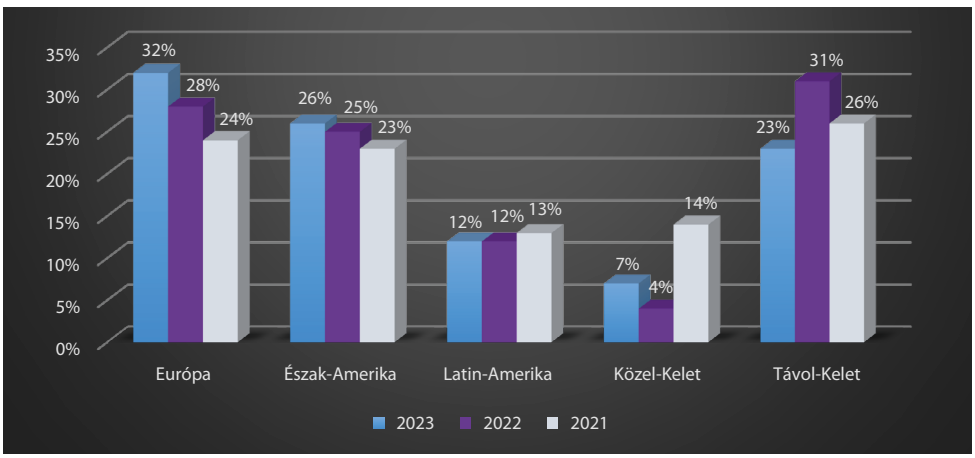
Jelen tudományos munka elkészítése során a szerző szekunder adatokat dolgozott fel, valamint a már megjelent hazai jogszabályokat és a friss NIS2 implementációs tevékenységből fakadó új jogszabályokat összehasonlító elemzés alá vetette a NIS2 uniós irányelvvel, valamint analitikai elemzését végezte el a témában megjelent releváns irodalomnak. Ennek keretében a szerző azonosította a megfelelő forrásokat, adatintegrációt végzett a különböző

forrásokból származó adatok egyesítése végett, összefüggéseket vont le az adatokban rejlő trendekkel kapcsolatban, és a jövőre vonatkozóan következtetéseket fogalmazott meg. A szerző rendszerezte az Európát ért kiberbiztonsági fenyegetéseket – annak bekövetkezési éve, a támadás típusa, illetve az érintett szektor szempontjai alapján.

A szerző empirikus kutatást is végzett, amelynek célja az volt, hogy közvetlen információkat gyűjtsön a NIS2 irányelv gyakorlati alkalmazásáról és kihívásairól, különböző munkaprojektek keretében. A szerző többéves munkatapasztalattal rendelkezik a kiberbiztonság területén, ami nagyban hozzájárult a kutatás hatékonyságához. Tapasztalatai révén mélyebb megértést és releváns kérdéseket tudott megfogalmazni, amelyek rávilágítanak a NIS2 hazai implementációjából fakadó nehézségekre, esetleges ellentmondásokra.

Európa helyzete napjainkban

Számos kiberbiztonsággal foglalkozó szervezet és ügynökség adatai azt mutatják, hogy globálisan a kibertámadások száma évről évre nő, azonban az elmúlt években Európát ért kibertámadások száma a többi régióhoz képest is kiemelkedő. Már az izraeli, amerikai Check Point Software Technologies Ltd. kutatórészlege a Check Point Research 2022-es kiberbiztonsági jelentésében felhívta a figyelmet az Európai Unió ágazatai ellen elkövetett kibertámadások számának jelentős növekedésére.[2] Jelen tudományos munka elsősorban az Európai Uniós Kiberbiztonsági Ügynökségnek (ENISA) 2023-as évre kiadott fenyegetésekkel kapcsolatos tanulmányát, valamint az amerikai IBM X-Force legújabb, 2024-ben kiadott, fenyegetésekkel foglalkozó éves tanulmányát vette alapul.



1. ábra: Az elmúlt években regisztrált támadások arányai régiónként
Forrás: a szerző szerkesztése IBM X-Force 2024: 18. alapján

Az amerikai székhellyel rendelkező IBM X-Force kiberbiztonsági kutatási és tanácsadó csoport éves jelentésében Európát találta a leginkább kibertámadásoknak kitett régiónak

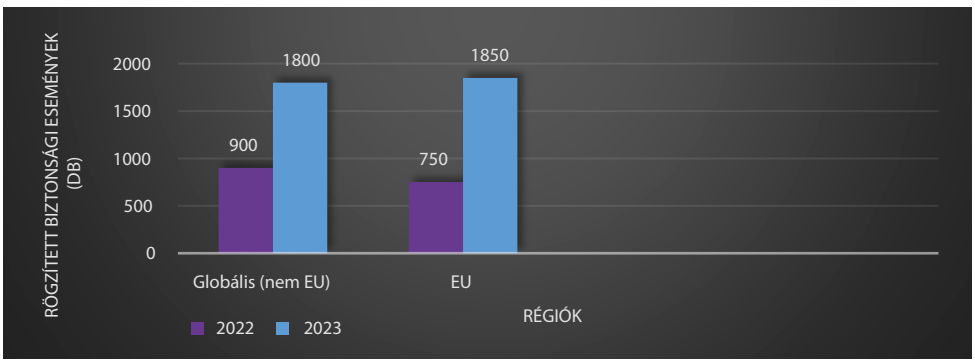
[2] Checkpoint Research Team 2023.

globálisan. A szervezet által megfigyelt biztonsági események 44%-áért a rosszindulatú kódok *(malware)* voltak felelősök. 2023-ban Európában volt a legtöbb ransomware támadás globálisan, 26% (az ENISA ennél is nagyobb mértékű ransomware fenyegetést figyelt meg). Ez hozzájárult ahhoz, hogy az IBM X-Force listáján Európa legyen 2023-ban az első helyen. A 2023 februárjában ESXiArgs néven futó nagyszabású zsarolóvírus-kampány Európa-szerte érintett szervezeteket, ez a vírus a VMware ESXi szerverek sebezhetőségét célozta (CVE-2021-21974).

Más régiókhoz képest a felhőplatformok magas használata Európában potenciálisan nagyobb támadási felületet is eredményez, különösen, ha a támadók képesek érvényes felhőfelhasználó fiókokat szerezni a kezdeti hozzáférés megszerzéséhez. A bekövetkezett biztonsági események 30%-ában a támadók érvényes fiókokat használtak.

Az európai székhelyű szervezeteket érő három legnagyobb kedvezőtlen hatás a hitelesítő adatok megszerzése volt 28%-kal, a zsarolás 24%-kal és az adatszivárgás 16%-kal.

A tanulmány kitér az európai szektorok helyzetére is, ahol ismerteti, hogy a feldolgozóipar a 2022-es második helyről a leginkább támadott iparággá vált, az incidensek 28%-a érintette ezt az ágazatot. A második helyen az üzleti és fogyasztói szolgáltatások állnak az esetek 25%-ával, a harmadik helyen pedig a pénzügyi és biztosítási szektor áll 16%-kal, megelőzve az energiaipart, amely 14%-kal a negyedik helyen áll. Európában az Egyesült Királyság volt a leginkább támadott ország, az esetek 27%-ával, amit Németország követett 15%-kal.[3]



2. ábra: Az EU-t ért támadások száma, a világ többi részén történt támadásokéval összevetve
Forrás: a szerző szerkesztése a European Union Agency for Cybersecurity 2023: 11. alapján

A Európai Uniós Kiberbiztonsági Ügynökség (ENISA) arról számolt be, hogy a jelentéstételi időszak során (2022. július – 2023. június) az EU tagállamaira nagy hatással van a jelenlegi geopolitikai válság, és egyre több ellenséges szereplő vette célba az állami és magánszervezeteket. Az ilyen jellegű események gyakrabban tartoznak a DDoS-fenyegetés körébe, és az OSINT[4] által feltárt bejelentett esetek többségében nem, vagy csak minimálisan

[3] IBM 2024.

[4] Az OSINT (Open Source Intelligence) az a folyamat és gyakorlat, amely során nyilvánosan elérhető forrásokat, információkat és adatokat gyűjtenek, elemeznek és értékelnek személyekkel, szervezetekkel vagy eseményekkel kapcsolatos információk felderítéséhez és értelmezéséhez.

voltak hatásosak ezek a támadások. A jelentés későbbi fejezetében kifejti, hogy az EU-ban a zsarolóvírus-támadások megszaporodtak.

Az ENISA körülbelül 2580 incidenst figyelt meg, további 220 incidens pedig kifejezetten két vagy több uniós tagállamot célzott meg. Az ENISA a tanulmányban kitér arra is, hogy a zsarolóvírusok és a DDoS a két fő fenyegetés jelenleg az EU számára.

Az ENISA a szektorokat a NIS2 irányelvben meghatározottak szerint csoportosította, valamint azon túlmenően még egyéb szektorokat is meghatározott, mint például a védelmi, a média- és szórakoztatóipari ágazatok. A leginkább támadott szektor a jelentés alapján a közigazgatás volt az esetek 19%-val, ezt követte az egészségügy, a harmadik helyen pedig holtversenyben a gyártás és a digitális infrastruktúra-ágazatok álltak.[5]

Az ilyen jellegű kiberfenyegetettségi elemzések következtetései körültekintést igényelnek, mert valamennyi publikáló szervezet a saját adatbázisából dolgozik és von le következtetéseket. Viszont az elmondható ezek alapján, hogy Európa fokozottan ki van téve a kibertér fenyegetéseinek, így a 2022 decemberében elfogadott uniós irányelv, amely az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedéseket kíván megteremteni, időszerű és pozitív döntés volt a Bizottság részéről.

Az Európai Parlament és a Tanács (EU) 2022/2555 (NIS2) irányelvének ismertetése

A NIS2, vagy más néven a Network and Information Security Directive 2 (Hálózati és Információbiztonsági Irányelv 2) az Európai Unió egyik jelentős kezdeményezése a digitális biztonság terén. Az előző, eredeti NIS irányelvet (NIS1) 2016-ban fogadták el, amely a tagállamokat arra kötelezte, hogy javítsák és erősítsék meg az információbiztonságot a kritikus infrastruktúrák és szolgáltatások terén. A NIS2 az első irányelv hatékonyságának értékelése és az új kihívásokra való válaszadás alapján született, célja a digitális fenyegetésekkel szembeni felkészültség további javítása és az EU-s kritikus infrastruktúrák biztonságának megerősítése.

Az irányelv elsődleges célja továbbra is az EU tagállamainak kritikus infrastruktúráinak és digitális szolgáltatásainak megerősítése a digitális fenyegetésekkel szemben. Azonban számos új ágazat került az irányelv hatálya alá, aminek köszönhetően az eddig még nem érintett, új ágazatok szereplőinek is meg kell valósítaniuk az elvárt biztonsági követelményeket. Vélhetően az újonnan bekerült szervezetek, amelyekre korábban nem vonatkoztak információbiztonsággal kapcsolatos követelmények, nagyobb energia és erőforrás befektetése révén tudnak elérni egy, az irányelv követelményeit megjelenítő jogszabálynak való megfelelést, mint azon szereplők, akik a NIS1 direktíva szerint érintettek voltak. Az új szabályozás által érintett ágazatok két nagy csoportba sorolódnak, amelyek a kiemelten kritikus ágazatok és az egyéb kritikus ágazatok. Az egyéb kritikus ágazatok közé jellemzően olyan szektorok tartoznak, amelyek nem létfontosságúak,

[5] European Union Agency for Cybersecurity 2023.

azonban nemzetgazdasági és államigazgatási szempontból kiesésük jelentős negatív hatással járna. Az ágazatok a következők:

- postai és futárszolgáltatások;
- hulladékgazdálkodás;
- vegyszerek gyártása, előállítása és forgalmazása;
- élelmiszer-termelés, -feldolgozás és -forgalmazás;
- gyártás;
- digitális szolgáltatók;
- kutatás.

Fontos felhívni a figyelmet, hogy a „kiemelten kockázatos ágazatok" nem azonos a „kritikus infrastruktúrákkal", amelyek védelmével külön direktíva, a CER foglalkozik. A direktíva által meghatározott auditra való kötelezettséget nem lehet kiváltani más kiberbiztonsági megfelelőséget igazoló tanúsítvány meglétével, például ISO 27001 információbiztonsági irányítási rendszer meglétét igazoló tanúsítvánnyal.

A direktíva hatálya alá azon ágazatok szervezetei tartoznak, amelyek legalább 50 főt foglalkoztatnak, és/vagy éves nettó árbevételük meghaladja a 10 millió eurót (körülbelül 3,9 milliárd forint). Kivételt képeznek ebből például a minősített bizalmi szolgáltatást nyújtó szervezetek, DNS-szolgáltatók, legfelső szintű domainnév-nyilvántartók, valamint a digitális infrastruktúrák alapvető szolgáltatói. Ennek megfelelően főként közép- és nagyvállalatok érintettek.

A szervezetek általános kitettségére, valamint az ebből fakadó negatív hatásokra számos dokumentum rávilágít, jelen tudományos munka az IBM 2023-as adatvédelmi incidensek *(data breach)* költségeiről szóló jelentést és a Sophos *The State of Ransomware* 2024-es dokumentumát vette alapul. Az IBM jelentésében részletesen leírják a szervezeteket ért adatkompromittálódások költségeit. A jelentés számos fontos dologra és összefüggésre hívja fel a figyelmet. Az adatvédelmi incidensek átlagos költsége 2023-ban minden idők legmagasabb szintjére, 4,45 millió amerikai dollárra emelkedett. Ez 2,3%-os növekedést jelent a 2022-es 4,35 millió dolláros költséghez képest. Az adatvédelmi incidensekben érintett szervezetek 51%-a tervezte növelni a biztonsági befektetéseit az esemény bekövetkezését követően. Az adatvédelmi incidensek 67%-át egy harmadik fél vagy maga a támadó jelentette, ami kiemeli a jobb fenyegetésfelismerés szükségességét. Az olyan incidensek, amelyeket a támadók jelentettek, közel 1 millió dollárral többe kerültek a szervezeteknek, mint a belső észlelésű incidensek. Azok a szervezetek, amelyek nem vonták be az illetékes bűnüldöző szervet egy ransomware támadás során, 470 ezer dollárral többet fizettek, és 33 nappal hosszabb ideig tartott a probléma megoldása, mint azoknak, akik bevonták az illetékes hatóságot. A Sophos legfrissebb jelentése szerint a zsarolóprogramok által érintett szervezetek átlagosan 2,73 millió dollárt költenek el a helyreállításra, valamint kitér arra is, hogy a helyreállítási idők is növekedtek az elmúlt évekhez képest. Üdvözlendő azonban, hogy a Sophos adatai azt mutatják, a ransomware támadást elszenvedő szervezetek 97%-a igénybe vette az illetékes szervek segítségét.[6]

Az IBM jelentése kitér azon megoldásokra, amelyek csökkentik az adatvédelmi incidensek kialakulását, valamint az incidens bekövetkezése esetén felmerülő költségeket.

[6] Sophos 2024.

Az integrált biztonsági fejlesztés és üzemeltetés (DevSecOps) alkalmazása jelentős megtakarítást eredményez. Azok a szervezetek, amelyek a biztonságot a szoftverfejlesztési életciklus minden fázisába integrálták, 1,68 millió dollárral alacsonyabb adatvédelmi incidenssel kapcsolatos költséget jelentettek, mint azok, amelyek nem alkalmazták ezt a megközelítést.

Az incidenskezelési tervek és tesztelések magas szintű alkalmazása szintén hatékony költségcsökkentő tényező volt, 1,49 millió dollár megtakarítást eredményezve.

Az egészségügyi ágazat 13. éve egymás után a legdrágább adatvédelmi incidenseket jelentette, az átlagos költség 10,93 millió dollár volt 2023-ban. Bár a dokumentum 16 ország adatait vette alapul, köztük számos európait is, az jól látható, hogy a NIS2 irányelv segíti a szervezeteket az adatvédelmi incidensekből fakadó költségek csökkentésében azáltal, hogy kötelezővé teszi a kiberbiztonsági intézkedések bevezetését és a gyors reagálást, javítva így az incidensek észlelését és kezelését, csökkentve az adatvédelmi incidensek bekövetkezésének kockázatát.[7]

Az irányelv a kockázatalapú megközelítést alkalmazza, a fókusz nem az egyes információs rendszereken van, hanem a teljes üzleti folyamatra kiterjed, valamint a beszállítói láncok biztonságára is. Az együttműködési csoport az IKT-rendszerek, IKT-termékek és IKT-szolgáltatások ellátási láncainak vonatkozásában összehangolt biztonsági kockázatértékeléseket végez, együttműködve az ENISA-val.

A NIS1-hez képest az új irányelv a humán erőforrás biztonsági kockázatára jelentős figyelmet fordít, ennek keretében a biztonságtudatossági képzések létrehozása, megtartása, számonkérése, frissítése prioritást élvez. Az irányelv a vezetőkre is kiterjeszti a biztonságtudatossági képzéseken való részvételt.

A *zero trust* kiberbiztonsági szemléletnek az alkalmazását szorgalmazza a NIS2, ennek köszönhetően az érintett szervezetek, többek között az alapvető szolgáltatást nyújtó szervezetek kiberrezilienciájukat jelentősen képesek lesznek fokozni. A *zero trust* megközelítés azt vallja, hogy a fenyegetések mindenütt jelen lehetnek, még a belső hálózaton belül is, így minden kommunikációt és hozzáférést alaposan és rendszeresen ellenőrizni kell. Ennek köszönhetően biztosítani lehet, hogy csak azok a felhasználók és eszközök férjenek hozzá a szervezeti adatokhoz és erőforrásokhoz, akiknek ehhez valóban jogosultságuk van. Ide tartozik a legkisebb jogosultság elve is, miszerint csak azokat a hozzáféréseket és jogosultságokat kell biztosítani a felhasználóknak és eszközöknek, amelyek elengedhetetlenek az adott feladat vagy munkafolyamat elvégzéséhez.

A Bizottság a tagállamok közti stratégiai együttműködés és információcsere támogatása és megkönnyítése, valamint a bizalom erősítése érdekében együttműködési csoportot hozott létre. A csoportnak számos feladata van, többek között az illetékes hatóságoknak az irányelv átültetésével és végrehajtásával kapcsolatban iránymutatást ad.

A NIS2 direktíva előírja a tagállamoknak, hogy hozzanak létre nemzeti CSIRT-ket, amelyek felelősek az országos szintű informatikai biztonsági események kezeléséért és a kritikus infrastruktúrák védelméért. Emellett a direktíva ösztönzi a tagállamokat a regionális és nemzetközi együttműködésre a CSIRT-k között, hogy hatékonyabban kezeljék a határokon átnyúló kiberbiztonsági fenyegetéseket és incidenseket. A hálózat

[7] IBM 2023.

alapvetően információcserét és közös tapasztalatok levonását valósítja meg a tagállamok között, de a határokon átnyúló események kezelésében aktív segítségnyújtást is biztosít.

Az irányelv kapcsán létrehozták az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatát, amelynek neve EU CyCLONe. Ez a hálózat a tagállamok kiberválságok kezelésével foglalkozó hatóságainak képviselőiből, valamint, amikor egy potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági esemény jelentős hatással van, vagy valószínűleg jelentős hatást gyakorolhat az ezen irányelv hatálya alá tartozó szolgáltatásokra és tevékenységekre, a Bizottság képviselőiből áll. Az EU CyCLONe alapvető feladata, hogy a nagyszabású kiberbiztonsági események összehangolt kezelését támogassa, valamint az Unió intézményei, szervei, hivatalai és ügynökségei és a tagállamok között a rendszeres információcserét biztosítsa.

A sérülékenységeket egy összehangolt európai sérülékenység-adatbázisba gyűjtik. Így valamennyi tagállamnak kötelessége segítenie azt a természetes vagy jogi személyt, aki bejelentést tesz valamely IKT-termék vagy -szolgáltatás sérülékenységére vonatkozóan. Ezt követően a kijelölt CSIRT felveszi a kapcsolatot a gyártóval és a munkacsoporttal, amely az ENISA-val együtt kezeli az adatbázist. Minden érdekelt fél számára hozzáférést kell biztosítani az európai sérülékenység-adatbázisban található sérülékenységekre vonatkozó információkhoz, ezzel segítve valamennyi szervezetet és beszállítót.

Az alapvető és fontos szervezetek jelentéstételi kötelezettséggel vannak az eseménybejelentés tekintetében, ideértve az esemény jelentését és értékelését, az esemény kezelésével kapcsolatos tájékoztatást, valamint az információk továbbítását a CSIRT-nek és az illetékes hatóságoknak. Emellett a direktíva kitér az érintett szervezetek és a CSIRT közötti kommunikációra, a határokon átnyúló eseményekre vonatkozó együttműködésre és az információk összegyűjtésére és megosztására vonatkozó rendelkezésekre.

A tagállamoknak biztosítaniuk kell, hogy az alapvető és fontos szervezetekre vonatkozó felügyeleti és végrehajtási intézkedések hatékonyak, arányosak és visszatartó erejűek legyenek, figyelembe véve az egyes esetek körülményeit. Az illetékes hatóságoknak széles hatáskörrel kell rendelkezniük a szervezetek ellenőrzésével kapcsolatban, beleértve a helyszíni ellenőrzéseket, a rendszeres biztonsági ellenőrzéseket és az objektív kockázatértékeléseket. Amennyiben szükséges, az illetékes hatóságoknak joguk van különféle intézkedéseket hozni, beleértve a figyelmeztetéseket, kötelező utasításokat, vagy akár a bírság kiszabását az irányelv megsértése esetén. Az illetékes hatóságoknak indokolniuk kell az intézkedéseiket, és mérlegelniük kell a szabálysértőkkel szembeni hatósági szankcionálási eszközök használatát, figyelembe kell venniük az elkövetett jogsértés súlyát és az érintett szervezetek együttműködését.

Az alapvető szervezetek esetén, amennyiben elmulasztják a kiberbiztonsági kockázatkezelési intézkedések megtételét, vagy nem tesznek eleget jelentéstételi kötelezettségüknek, legalább 10 millió euró vagy a szervezet előző évi bevételének akár a 2%-a is lehet közigazgatási bírság mértéke. A fontos szervezetek (nem alapvető szervezetnek minősülő szervezetek) esetén ez az összeg némileg alacsonyabb, mint a fenti értékhatárok.[8]

[8] Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete.

Holisztikus megközelítés

A NIS2 direktíva mellett a CER direktíva is megjelent, amely a kritikus infrastruktúrák teljes körű rezilienciáját tűzte ki célul, és a két irányelv számos ponton kimutat a másikra, vagy behivatkozza azt, így fontos, hogy tagállami és uniós szinten is a két irányelv által megjelölt hatóságok között fokozottan jó és magas szintű együttműködés alakuljon ki. A CER-t implementáló hazai jogszabály, a jelenleg hatályos 2012. évi CLXVI. törvényt (Lrtv.) hatályon kívül fogja helyezni, és megteremti az új EU-s irányelv szabályozási kereteit. 2024 októberéig ezt a jogszabályt is ki fogják hirdetni. Az irányelv célja a dinamikusan változó fenyegetések, például a hibrid hadviselés és a terrorizmus, valamint az infrastruktúra és az ágazatok közötti növekvő kölcsönös függőségek és a szélsőséges időjárás okozta kihívások kezelése. Az irányelv meghatározza a kritikus szolgáltatókat az EU-ban és azok kötelezettségeit a teljes körű reziliencia megvalósítása érdekében. A dokumentum hangsúlyozza a harmonizált minimumszabályok fontosságát az alapvető belső piaci szolgáltatásokban és az illetékes hatóságok közötti határokon átnyúló együttműködés javítása érdekében. A Covid–19-járványt is figyelembe véve az irányelv kockázatalapú megközelítést alkalmaz a kritikus szervezetek azonosítására és rezilienciájuk biztosítására. A dokumentum számos ponton kimutat a NIS2 irányelvre, különösen a nemzeti hatóságok és a CER irányelv szerint kijelölt hatóságok közötti együttműködést támogatja.[9]

A CER irányelv mellett fontos megemlíteni a nemrég elfogadott dokumentumot [Commission Delegated Regulation (EU) 2024/1366 of 11 March 2024 supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows], amely kiegészítése a 2019/943 európai parlamenti és tanácsi rendeletnek (EU) a villamos energia belső piacáról, amely az Európai Unió energiapiacának működését és fejlődését szabályozza. A rendelet célja a közös energiapiac létrehozása és a hatékony energiatermelés, -elosztás és -fogyasztás biztosítása az EU-ban. A „sector-specific rules for cybersecurity aspects of cross-border electricity flows" a kibervédelmi szabályokra utal, amelyek a határokon átnyúló áramlásokat érintik az energiaiparban. Ez a rendeletkiegészítés kiberbiztonsági szempontokat vezet be a határokon átnyúló áramlások területén, vagyis a kereskedelmi áramlásoknál figyelembe kell venni a kiberbiztonsági kockázatokat.[10]

Ez a rendeletkiegészítés ágazatspecifikus szabályokat állapít meg a határokon átnyúló villamosenergia-áramlás kiberbiztonsági szempontjaira vonatkozóan, beleértve a közös minimumkövetelményekre, a tervezésre, a nyomon követésre, a jelentéstételre és a válságkezelésre vonatkozó szabályokat. Továbbá a meglévő jogi kiberbiztonsági követelményekre fog építeni, és arra törekszik, hogy kiegészítse azokat annak érdekében, hogy növelje a kiberbiztonságot az Európai Unió villamosenergia-ágazatában. A hálózati kódex különösen a hálózati és információs rendszerek biztonságára vonatkozó, az (EU) 2022/2555 irányelvben (NIS2 irányelv) meghatározott általános szabályokat egészíti ki.[11]

A DORA (Digital Operational Resilience Act) egy európai uniós rendelet, amely 2023. január 16-án lépett hatályba és 2025. január 17-től alkalmazandó a NIS2 és a CER

[9] Ambrusz et al. 2024: 16.
[10] Az Európai Parlament és a Tanács (EU) 2019/943 rendelete.
[11] European Commision Directorate-General for Energy 2024.

irányelv mellett, amelynek célja a pénzügyi szektor digitális működési ellenálló képességének megerősítése. Ha nem kezelik megfelelően, az IKT-kockázatok a határokon átnyúló pénzügyi szolgáltatások megszakadásához vezethetnek. Ez pedig hatással lehet más vállalatokra, ágazatokra, sőt a gazdaság többi részére is, ezért kiemelt fontosságú a pénzügyi szektor digitális működési rezilienciájának megerősítése. Az uniós rendelet hatálya alá tartoznak a pénzügyi intézmények, például bankok és biztosítók, valamint az olyan szolgáltatók, amelyek fontos infrastruktúrát biztosítanak a pénzügyi rendszer számára. Magyarországon az MNB (Magyar Nemzeti Bank) a DORA rendelet kapcsán felügyeleti hatósági tevékenységet fog ellátni. Az MNB felelős lesz a pénzügyi intézmények, valamint a kulcsfontosságú infrastruktúrát biztosító szolgáltatók felügyeletéért és a DORA irányelv hazai jogszabályában foglalt követelmények betartásáért.[12]

A súlyos vagy nagy kiterjedésű kiberbiztonsági események és krízisek kezelésére valamennyi tagállam egy vagy több illetékességgel rendelkező hatóságot jelöl ki. Továbbá a számítógép-biztonsági események kezelésére létre kell hozni egy vagy több nemzeti CSIRT-t.

Hazánk implementációs tevékenysége

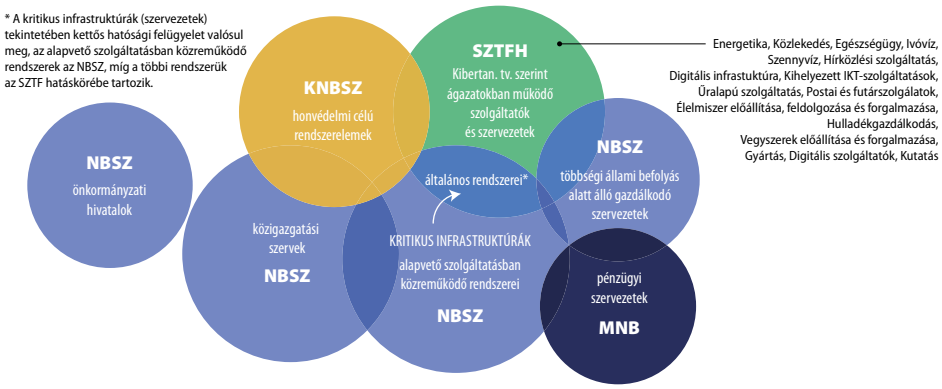
Valamennyi tagállam legkésőbb 2024. október 17-ig elfogadja és kihirdeti azokat a rendelkezéseket, amelyek szükségesek ahhoz, hogy ennek az irányelvnek megfeleljen, majd erről haladéktalanul tájékoztatja a Bizottságot. Magyarország a NIS2 direktíva megjelenését követően megalkotta a 2023. évi XXIII. törvényt, amely nagy vonalakban a NIS2 irányelv által elvártakat foglalja keretbe. Elsődlegesen, az irányelv által elvárt felügyeleti hatóság feladat- és hatásköre lett kijelölve, valamint az érintett ágazatok, amelyek a NIS2 által meghatározottak.

Hazánkban a NIS2 végrehajtásának hatósági felügyeletét alapvetően négy hatósági szerv fogja végrehajtani, amelyek a következők: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI), Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH), Magyar Nemzeti Bank (MNB) és a Katonai Nemzetbiztonsági Szakszolgálat (KNBSZ) (3. ábra).

Az SZTFH egy újonnan létrehozott kiberbiztonsági hatósági feladatot is ellátó szervezet. Működése jogszabályi hátterét a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény biztosítja. A szervezet mérete korlátozott, és a német mintát követve, külső szervezet auditorjai fogják az ellenőrzéseket végrehajtani. Azonban a NIS2 hazai megvalósításában és a későbbi hatósági munkában jelentős szerepük van és lesz. Az SZTFH alapvetően a NIS2-ből fakadó nyilvántartóhatóság szerepkörét is ellátja, valamint a piaci alapokon működő szervezetek esetén ő az elsődleges felügyeleti hatóság. Magyarországon az eddigiek fényében megállapítható, hogy nem egy kiberbiztonsági „szuper" hatóságot hoztak létre, hanem több, saját hatás- és illetékességi körrel rendelkező kiberbiztonsági hatóságokat, amelyeknek vannak közös

[12] Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve.

metszéspontjaik. Az eseménykezelést azonban a piaci alapon működő szervezeteknél, az érintett államigazgatási szervezeteknél, valamint a kritikus infrastruktúrák esetén az NBSZ NKI látja majd el.[13]



3. ábra: Hazai kiberbiztonsági felügyeletet ellátó hatóságok
Forrás: Orosházi 2024: 7.

A honvédség, a korábbi gyakorlatoknak megfelelően, önálló kiberbiztonsági felügyeletet valósít meg a honvédelmi célú zárt elektronikus információs rendszerek biztonsági felügyelete esetén, amelyet a KNBSZ lát el.

Az NBSZ NKI feladatkörét tekintve eseménykezelő központként, nemzeti kapcsolattartó pontként is fog funkcionálni, hatósági feladatot is el fog látni az állami és önkormányzati szervek esetén, valamint az állami tulajdonban lévő kritikus infrastruktúrák tekintetében, továbbá az SZTFH felügyelete alá tartozó azon szervezetek esetén, ahol valamely rendszert vagy rendszerelemet kritikus infrastruktúraként jelöltek ki. Mint eseménykezelő központ, valamennyi NIS2 hatálya alá tartozó szervezet esetén ők látják el ezt a feladat- és szerepkört.

Az MNB a pénzügyi szervezetek információbiztonságának felügyeletét és irányítását fogja végezni, a pénzügyi ágazat digitális működési rezilienciájáról szóló 2022/2554 (EU) rendelet (DORA rendelet) alapján. A rendelet hatálya húszféle pénzügyi szervezetre és nekik IT-szolgáltatást nyújtó külső szolgáltatókra terjed ki, függetlenül attól, hogy kiszervezés keretében vagy egyéb módon nyújtják e szolgáltatásaikat. A rendelet fő célja, hogy a NIS2 irányelv „lex specialis”-aként, a teljes pénzügyi szektorra vonatkozó, uniós szintű, egységes rezilienciára vonatkozó előírásokat fogalmazzon meg.

Az új EU-s direktíva hatálya alá tartozik számos olyan szervezet, amely korábban nem volt köteles kiberbiztonsági tanúsítvánnyal rendelkezni. Ennek megfelelően a magyar hatóság felkészülési időt biztosít minden érintett szervezet számára. Becslések szerint Magyarországon körülbelül 2500-3000 szervezet esik ennek hatálya alá (az SZTFH 2546 érintett szervezetet azonosított). Az irányelv alá tartozó szervezeteknek legkésőbb

[13] NBSZ NKI 2024a; 2023. évi XXIII. törvény (Kibertan. tv.).

2025 végéig át kell esniük egy olyan auditon, amely az új jogszabályoknak megfelelően történik, és az esetleges hiányosságokat 120 napon belül ki kell javítaniuk.

Meg kell említeni, hogy más információbiztonsági tanúsítvány, például az ISO/IEC: 27001:2022 szabvány szerinti információbiztonsági irányítási rendszer tanúsítványa nem mentesíti a NIS2 irányelv hatálya alá tartozó szervezetet a magyar jogszabályokban előírt biztonsági követelmények teljesítése alól, valamint az a szerinti audit alól sem. A jelenleg ez év végéig hatályos 41/2015. (VII. 15.) BM rendelet várhatóan hatályát veszti legkésőbb ez év végén, és helyébe az új, a NIS2-nek megfelelő, korszerű követelményeket előíró 7/2024. (VI. 24.) KM rendelet fog hatályba lépni 2025. január 1-jével. A rendelet nyilvánosan elérhető, és jól kivehető, hogy az amerikai NIST 800-53 rev5-ös dokumentum képezi az alapját, viszont a hazai sajátosságok figyelembevételével, testre szabták az eredeti NIST követelménykatalógust. Az ötödik kiadás (rev5) sokkal korszerűbb (technológiai kontrollok tekintetében is), és tágabb hatókörrel rendelkezik, mint az NIST SP 800-53 rev4, amely a tudományos munka írásának pillanatában még hatályos hazai jogszabály alapját képezi. A frissen megjelent rendeletnek számos pozitív hozadéka lehet majd a későbbiekben, egyrészt a külföldi szervezetek esetén könnyebb és egyértelműbb lesz az átjárhatóság, hiszen az NIST kontrolljai széles körben ismertek és alkalmazottak, másrészt a három biztonsági osztállyal, a szervezeti szintbe sorolás mellőzésével, valamennyi üzemeltető feladata egyértelműbbé és egyszerűbbé válik. A 41/2015. (VII. 15.) BM rendeletben meghatározott öt biztonsági osztály helyett három új osztály fog létrejönni: alap, jelentős és magas az amerikai NIST SP 800-53 szabványnak megfelelően. A biztonsági osztályba soroláshoz szükséges irányelveket a jogszabály tartalmazza. A 7/2024. (VI. 24.) KM rendelet 1. mellékletének 2. fejezete rendelkezik az osztályba sorolás során alkalmazandó alapvető módszertanról, amit az elektronikus információs rendszerben kezelt adatok és az adott rendszer funkciói határoznak meg. Az érintett szervezetek a hatáselemzéshez felügyeleti hatóságuk által kiadott módszertani ajánlásokat is követhetnek, ha nincs az adott szervezetnek vonatkozó hatáselemzési módszertana.

Fontos még megemlíteni, hogy az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben, valamint annak végrehajtási rendeletében a meghatározott biztonsági követelmények adminisztratív, fizikai és logikai védelmi intézkedésekre való felosztása megszűnni látszik, az új követelményeket tartalmazó jogszabályban nem alkalmaz ilyen jellegű felosztást, ahogyan a követelményeknek és biztonsági osztályoknak BSR[14]-elv szerinti besorolása is megszűnik. Egyedül a kockázatelemzéshez határozza meg a jogszabály a 3. melléklet fenyegetés katalóguselemeit alkalmazni mint minimális elvárást. A melléklet az elektronikus információs rendszer bizalmassága, sértetlensége és rendelkezésre állása szempontjából értelmezhető fenyegetéseket gyűjti össze. Maga a 2013. évi L. törvény szintén átdolgozás alatt van, helyét egy új hazai törvényerejű jogszabály fogja átvenni, és ki fog térni a fejlesztések hatósági felügyeletére annak érdekében, hogy a biztonsági elvárások biztosan megvalósuljanak.

[14] A BSR az információbiztonság egyik alapelve, amelynek jelentése bizalmasság, sértetlenség és rendelkezésre állás. Az elektronikus információs rendszer biztonsága olyan állapot, amelyben az érintettek számára kielégítő módon biztosított a rendszer védelme. Ez magában foglalja a rendszerben tárolt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának garantálását, valamint a rendszer elemeinek sértetlenségét és rendelkezésre állását. A biztonsági intézkedések folyamatosak, átfogók, zártak és arányosak a fennálló kockázatokkal. Muha–Krasznay 2014.

A jogszabály rendelkezni fog az EU CyCLONe és a kiberválság-kezelés szabályait lefedő eljárásokról, valamint a kötelező gyakorlatok szabályairól is.[15]

Azoknak az érintett szervezeteknek, amelyek 2024. január 1. előtt kezdték meg tevékenységüket, ez év június 30-ig kell jelentkezniük a nyilvántartásba vétel végett. Azoknak a szervezeteknek, amelyek működése 2024. január 1. után kezdődött, a megkezdéstől számított 30 napon belül kell jelentkezniük a hatóságnál. A regisztrációval párhuzamosan a szervezeteknek az elektronikus információs rendszereiket be kell sorolniuk a megfelelő biztonsági osztályba. A nyilvántartásba vétellel kapcsolatos részleteket az az érintett szervezetek kiberbiztonsági felügyeleti hatósági nyilvántartásáról szóló 23/2023. (XII. 19.) SZTFH rendelet szabályozza.

A nyilvántartásba vételt követően a szervezeteknek 2024. október 18-tól be kell fizetnie a hatóság felé a felügyeleti díjat, amelynek mértéke az előző évi árbevétel maximum 0,015%-a, de maximum 10 millió forint. 2024. december 31-ig kell szerződést kötniük az érintett szervezeteknek egy SZTFH által nyilvántartásba vett auditorszervezettel (jelenleg négy szereplős a piac), és 2025. december 31-ig az első NIS2 követelmények szerinti auditot végre kell hajtani. A NIS2 hatókörébe sok szervezet beletartozik itthon is, így a hatóságnak vélhetően nem lesz kapacitása valamennyi szervezet ellenőrzésére, csak szúrópróbaszerű vizsgálatokat fognak végrehajtani. Hiányosságok feltárása esetén a hatóság vélhetően először figyelmeztet, majd tevékenységtől eltilt, és ha szükséges bírságot szab ki, amelynek nagysága igencsak jelentős, így nem érdemes a szervezeteknek megvárni ezt a lépést. Valamint itt minden félnek az az érdeke, hogy az érintett rendszerek biztonságosan tudjanak üzemelni, ezzel is biztosítva a folyamatos üzletmenetet és a szolgáltatások zavartalanságát.

A NIS2 irányelv adaptációs kihívásai

Az uniós irányelv hazai implementációja önmagában nagy kihívás, és Magyarország az első tagállamok között lépett az implementációs tevékenységet illetően, így született meg a 2023. évi XXIII. törvény. Azonban az eddig megjelent jogszabály, valamint a biztonsági követelménykatalógust tartalmazó 7/2024. (VI. 24.) KM rendelet felvet néhány kérdést.

A korábbi gyakorlattól eltérően, új felügyeleti hatóságok jelentek meg a hazai kiberbiztonsági színen, ami az ország méreteit tekintve elsőre indokolatlannak tűnhet. Ezt a heterogén struktúrát meg fogják őrizni hosszú távon is, vagy ezek a szervezetek elkezdenek konvergálni egymáshoz, aminek eredményeképp kiberbiztonsági csúcshatóság jöhet létre?

A jogszabály által előírt auditok során vizsgált elektronikus információs rendszerek körének megállapítása kiemelten fontos kérdés. Az EU-s irányelv, valamint a hazai jogszabály az érintett szervezetek esetén valamennyi elektronikus információs rendszert a hatókörébe vesz. Azonban ez a gyakorlatban vélhetően másképp fog kinézni, hiszen a nagyvállalatok, akár több tíz elektronikus információs rendszert (EIR) is üzemeltethetnek, amelyek esetén a követelménykatalógusban szereplő védelmi intézkedések megvalósítása roppant költséges és erőforrás-igényes lehet, auditori szempontból kivitelezhetetlen egy

[15] Orosházi 2023.

szervezet tízes nagyságrendű rendszereit alaposan vizsgálni, adott időintervallum alatt. Például számlázórendszerek zártsági vizsgálata során, az auditorok a számlázási folyamattal kapcsolatos rendszereket vizsgálják, azonban a NIS2 hatókörébe valamennyi EIR beletartozik. A hatékonyság jegyében a szerző feltételezi, hogy bizonyos szempontok szerint ki fogják választani a vizsgálat hatókörébe tartozó rendszereket, például BIA- (üzletmenet szempontjából kritikus rendszerek) besorolás alapján, kezelt adatok mennyisége, minősége alapján, vagy egyéb horizontális kritériumok mentén. A teljes körű védelem megteremtése nagy erőfeszítéseket igényel, ha valamennyi EIR esetén biztosítani kell, hiszen ha csak valamilyen szempontrendszer által kiválasztott rendszerek védelmét biztosítjuk magas szinten, nem garantálható a teljes védelem, mert lehet, hogy más, kevésbé releváns rendszerekben maradtak sérülékenységek. Ezek révén a potenciális támadók bejuthatnak az adott szervezet belső hálózatába, annak rendszerelemeihez hozzáférhetnek, és súlyos károkat okozhatnak. Az észszerűség azonban azt diktálja, hogy azokat a rendszereket kell kiemelten védeni, amelyek valamely szempontrendszer szerint kiemeltnek minősülnek, és akkor még nem ejtettünk szót a felhőalapú rendszerekről és a hálózatba kapcsolt ipari vezérlőrendszerekről, amelyek szintén védelmi intézkedéseket igényelnek, a szervezet teljes körű kiberbiztonságának megvalósítása érdekében.

A NIS2 hatálya alá kerülő gazdálkodó szervezetek miatt megnövekedhet az igény az információs rendszer biztonságáért felelős személyek (IBF) iránt, mert azon szereplők akikre korábban nem vonatkozott kiberbiztonsági elvárás, sok esetben nem rendelkeznek IBF-fel, ezért ezeknek a szervezeteknek szükségük lesz egy megfelelő kompetenciával rendelkező egyénre, aki betöltheti ezt a fontos és felelősségteljes szerepkört. Az IBF-eket érintő elvárások nincsenek egyértelműen lefektetve. A Kibertan. tv. nem szab feltételt a gazdálkodó szervezetek IBF-ére vonatkozóan, azt az adott szervezet vezetőjére bízza, azonban a jelenleg hatályos, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.), valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendelet elvárásokat határoz meg az állami és önkormányzati szervezetek IBF-jeire vonatkozóan. A rendelet kitér arra, hogy 5 éves szakmai tapasztalat vagy a meghatározott nemzetközi szervezetek által létrehozott képzések elvégzését igazoló oklevelek mentesítik az egyént a Nemzeti Közszolgálati Egyetem által biztosított képzésen való részvételtől. Az állami és önkormányzati szervek esetén elfogadott oklevél az NKE elektronikus információbiztonsági vezető szakirányú továbbképzésén szerezhető. Ez a képzés két félévből áll, és évente mintegy 60-70 fő végez itt, azonban az itt végzettek egy része nem a civil szférában van állományban, vagy nem ott helyezkedik el a későbbiekben. Ezzel a végzett hallgatói mennyiséggel nem biztos, hogy minden, NIS2 irányelv hatálya alá tartozó újonnan csatlakozó szervezet megfelelő kvalitású és szakmaiságú felelőst fog tudni alkalmazni, ami komoly biztonsági kockázatot jelenthet. A 2013 óta hatályos jogszabályok, valamint a Kibertan. tv. között ellentmondás van az IBF-ekre vonatkozó követelmények tekintetében. A jogalkotónak javasolt törekednie az ilyen jellegű ellentmondások feloldására a jövőben, annak érdekében, hogy a Kibertan. tv. hatálya alá tartozó gazdálkodó szervezetek is hasonlóan magas

követelményeknek megfelelő felelőst alkalmazzanak, mint az állami és önkormányzati szervek esetén elvárt.[16]

Az új irányelvnek való megfelelést vizsgáló auditorokkal, valamint auditori szolgáltatást nyújtó szervezetekkel szemben a 7/2024. (VI. 24.) SZTFH rendelet ír elő követelményeket. Jelenleg NIS2 audit lefolytatására és tanúsításra az SZTFH által jóváhagyott és nyilvántartásba vett auditori szervezetek jogosultak. A kijelölt négy szervezet szakembergárdája nehezen lesz képes 2025 végéig leauditálni valamennyi érintett szervezetet és az általuk használt rendszereket. Legalábbis abban az esetben, ha alapos, valamennyi követelmény ellenőrzésére kiterjedő auditok megtartására törekednek, mivel a követelménykatalógus jelentős terjedelmű. Ebből kifolyólag javasolt lehet az érintett szervezeteknek minél előbb jelentkezniük és szerződést kötniük az audit miatt, hogy a vizsgálat ténylegesen megtartásra kerülhessen legkésőbb 2025. december végéig. A nemrég megjelent SZTFH rendelet szigorú elvárásokat támaszt az auditáló szervezetek részére, különösen azon szervezetek elé, akik nem csak az alap biztonsági osztályba sorolt rendszerekkel rendelkező szervezeteket akarják a későbbiekben vizsgálni. Ez egyik oldalról dicséretes, hiszen azon szervezetek, amelyek nem képviselnek magas szakmai színvonalat, nem válhatnak kiberbiztonsági audit végrehajtására jogosult gazdálkodó szervezetté, ugyanakkor a jelentős biztonsági osztályba sorolt rendszerekkel rendelkező szervezetek esetén jelentősen megszigorodnak az elvárások, ami miatt lehetséges, hogy nem lesz elegendő auditori szervezet, amely a magasabb biztonsági osztályba sorolt rendszereket leauditálja határidőre. Kérdés továbbá, hogy a Nemzeti Kiberbiztonsági Koordinációs Központ (Hun NCC) számára meg fognak-e határozni feladatot, akár a tanúsítást végző auditorok toborzásában, akár egyéb erőforrás-áramoltatási feladatok tekintetében.

Az auditorok rendelkezésre állásánál maradva, az NBSZ NKI Hatósági Főosztály megbízott vezetője 2024. március 19-i, „NIS2 aki bújt, aki nem, jövök!" című budapesti konferencia alkalmával elmondta, hogy a jövőben meg fog jelenni egy felhőplatformra és ipari vezérlőrendszerek védelmére vonatkozó követelménykatalógus, az utóbbi az NIST SP 800-82 rev3 alapjaira fog épülni. Erre vonatkozóan azonban több információ nem hangzott el. Ez viszont számos kérdést felvet, amennyiben ez is hatóköre lesz a hatósági és auditori vizsgálatoknak. A hatóság és a jelenleg kijelölt szervezetek rendelkeznek-e megfelelő szakértelemmel az ipari, valamint felhőkörnyezet ellenőrzésére vonatkozóan? Az ipari és felhőkörnyezet ellenőrzésében jártas auditorok, valamint hatósági szakemberek létszáma vajon elégséges méretű ahhoz, hogy valamennyi érintett ipari és felhőkörnyezet tanúsítása még időben megtörténhessen?

Ehhez kapcsolódva az üzemeltetői oldalon szintén fennáll ugyanez a kérdéskör. A megjelenő szabályozás alá tartozó hazai szervezeteknek lesz-e elegendő kompetenciájuk, erőforrásuk és idejük, hogy a felhővel és ipari vezérlőrendszerekkel kapcsolatos védelmi intézkedéseket megvalósítsák a meghatározott határidőre. A nemrég megjelent rendelethez kapcsolódóan már kiadtak egy EIR-ekre és szervezeti biztonsági követelményekre vonatkozó alkalmazási útmutatót, amely segíti az üzemeltetőket a biztonsági követelmények megvalósításában. Továbbá az NBSZ NKI hatósági főosztályvezetőjének elmondása alapján kiadnak még a felhő- és ipari rendszerek esetén is egy megvalósítási segédletet.[17]

16 Krasznay 2017.
17 NBSZ NKI 2024b.

Mióta a Bizottság elfogadta a NIS2 irányelvet, a hazai piacon sorra jelennek meg az erre való felkészítést mint szolgáltatást nyújtó ismert és kevésbé ismert szervezetek hirdetései. Kialakult egy piaci verseny a felkészítést illetően, ami az irányelv hatálya alá tartozó szervezeteknek egyfelől jó is lehet, hiszen az árversenynek köszönhetően nem feltétlen lesz drága a NIS2-re való felkészülés támogatása. Azonban másfelől kockázat, mert a szakmai minőség bizonyos esetekben kérdőjeles lehet, amivel nemcsak a szakma presztízsét ásnák alá, de végső soron az adott szervezet kiberrezilienciája sem tudna teljeskörűen megvalósulni, ami kockázati tényező lehet, akár nemzetbiztonsági szempontból is, amennyiben egy alapvető szolgáltatást nyújtó szervezet az érintett. Erre a problémára nem könnyű megoldást találni, de nem elképzelhetetlen, hogy a későbbiekben követelményeket határozhatnak meg a NIS2-re felkészítést kínáló szervezetekre vonatkozóan.

Számos hatósági eseményt rendeztek és rendeznek országszerte, ahol mind az SZTFH, mind az NBSZ NKI képviselői előadások keretében ismertetik a NIS2-vel és annak hazai implementációjával kapcsolatos információkat, a gyakorlatban végrehajtani szükséges teendőket. Ennek köszönhetően a június végi határidő közeledtével valamennyi érintett szervezet elvégezte az önazonosítását és bejelentkezett a hatóságnál. Az biztosan látszik már, hogy az EU-s irányelv által meghatározott szankcionálási eszközök és bírságtételek miatt sem érdemes trükköznie egyetlen szervezetnek sem, azoknak sem, amelyek a NIS2 hatálya alá tartozás küszöbén állnak (például azzal, hogy kijelentenek pár munkavállalót, mert a méretkorlátszabály gyakorlati megközelítése esetén a 2004. évi XXXIV. törvény szerint jár el a hatóság). A törvény szerint a szervezet átsorolásához az elmúlt 2 év adatait kell figyelembe venni. Továbbá az uniós irányelv felruházza a hatóságot azzal a jogkörrel, hogy kijelöljön olyan szervezeteket, amelyeknek megítélésük szerint meg kell felelniük a NIS2 irányelv által támasztott követelményeknek.[18]

Összegzés

Nemcsak Magyarország, de az egész Európai Unió komoly kihívások előtt áll, mióta az egységes és magas szintű kiberreziliencia megvalósítását tűzte ki célul. Ez egy szükségszerű lépés volt, amit számos kiberfenyegetésekkel kapcsolatos statisztika alátámaszt. A hazai implementáció jelen tudományos munka írásakor is zajlik. Az eddig nyilvánosságra hozott dokumentumok és megjelent jogszabályok alapján elmondható, hogy hazánk jó úton jár a megfelelő szintű és mélységű kiberbiztonság megvalósításában. A hazai jogszabályi környezet a nemzetközi átjárhatóságot és az átláthatóságot megfelelően biztosítja. Az irányelv implementálása számos kihívást és kérdést rejt. Azon szervezeteknek, amelyek most találkoznak először kiberbiztonsági követelményekkel, jelentős mennyiségű erőforrást kell biztosítaniuk a megfelelés érdekében. Azonban az eddigi, az NBSZ NKI és SZTFH által szervezett események, valamint a hatósági médiumok segítségével eljuttatott információk, valamint kiadott útmutató az irányelv hatálya alá tartozó szervezetek üzemeltetésének nyújtanak segítséget és mélyebb megértést. A hatóságoknak nem

[18] ICT Global 2024.

a szankcionálás a céljuk, hanem sokkal inkább az ország kiberbiztonságának előmozdítása és a megfelelő védelem kialakításának megkövetelése. A most kialakítás alatt álló hazai jogi környezet fogja meghatározni Magyarország kiberbiztonságát a következő években, ezért az egységességre, átláthatóságra, egyértelműségre és a nemzetközi szabványokkal való átjárhatóságra kell törekedni.

Felhasznált irodalom

Ambrusz József – Dobor József – Vásárhelyi Örs (2024): Létfontosságú rendszerek,-rendszerelemek rezilienciájának fejlesztési lehetőségei az Európai Unió direktíváinak tükrében. *Polgári Védelmi Szemle,* (különszám), 57–69. Online: https://mpvsz.hu/pv_szemlek/pvszemle2024/index.html

Checkpoint Research Team (2023): *Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks*. 2023. január 5. Online: https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/

European Commission Directorate-General for Energy (2024): *New Network Code on Cybersecurity for EU Electricity Sector.* 2024. március 11. Online: https://energy.ec.europa.eu/news/new-network-code-cybersecurity-eu-electricity-sector-2024-03-11_en

European Union Agency for Cybersecurity (2023): *ENISA Threat Landscape 2023*. ENISA. Online: https://doi.org/10.2824/782573

IBM (2023): *Cost of a Data Breach Report 2023*. Armonk, USA: IBM Corporation.

IBM (2024): *IBM X-Force Threat Intelligence Index 2024*. Armonk, NY: IBM Corporation.

ICT Global (2024): *Rám is vonatkozik a NIS2? Három részletes kritérium, ami segít eldönteni*. 2024. április 20. Online: https://ictglobal.hu/technologia/biztonsag/ram-is-vonatkozik-a-nis2-harom-reszletes-kriterium-ami-segit-eldonteni

IT Business (2024): *NIS2 – sikerkulcs lehet a megúszás helyett a megismerés*. Online: https://itbusiness.hu/technology/aktualis-lapszam/human/nis2-kiberbiztonsag-meguszas-megismeres/

Krasznay Csaba (2017): A kiberbiztonság stratégiai vetületeinek oktatási kérdései a közszolgálatban. *Nemzet és Biztonság,* 10(3), 38–53. Online: https://folyoirat.ludovika.hu/index.php/neb/article/view/3718/2997

Muha Lajos – Krasznay Csaba (2014): *Az elektronikus információs rendszerek biztonságának menedzselése*. Budapest: NKE.

NBSZ NKI (2024a): *NIS2 új követelmények [aktuális].* Podcast, 2024. április 9. Online: https://nki.gov.hu/podcast/

NBSZ NKI (2024b): *Indul a NIS2 tájékoztató kampány (2. rész).* Podcast, 2024. április 9. Online: https://nki.gov.hu/podcast/

Orosházi Dávid (2023): *A NIS2 közvetlen hatásai a kritikus infrastruktúrára és az állami szektorra*. IT Business Konferencia, 2023. mácius 19. Online: https://itbusiness.hu/wp-content/uploads/2024/03/6.-Oroshazi-David_prezi.pdf

Sophos (2024): *The State of Ransomware 2024*. Abingdon, UK: Sophos Ltd.

Jogi források

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

2023. évi XXIII. törvény a kiberbiztonsági tanusításról és a kiberbiztonsági felügyeletről. Online: https://net.jogtar.hu/jogszabaly?docid=a2300023.tv

Az Európai Parlament és a Tanács (EU) 2019/943 rendelete (2019. június 5.) a villamos energia belső piacáról (átdolgozás) (EGT-vonatkozású szöveg.) Online: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32019R0943

Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK rendelet, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32022R2554

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 (NIS2 irányelv). Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32022L2555&qid=1700772235586