NEMZETBIZTONSÁGI SZEMLE
13. évfolyam (2025) 2. szám 74–93. | DOI: 10.32561/nsz.2025.2.6

Ambrusz József,[1] Vásárhelyi Örs[2]

A kritikus szervezeti reziliencia és a lakosságfelkészítés nemzetbiztonsági jelentősége a modern fenyegetésekkel szemben

The National Security Importance of Critical Entities Resilience and Citizen Preparedness Against Modern Threats

Napjaink modern hibrid fenyegetései egyre összetettebb kihívások elé állítják a kritikus infrastruktúrákat és az alapvető szolgáltatást nyújtó szervezeteket. Az infrastruktúrák elleni kibertámadások nemcsak gazdasági és politikai instabilitást idézhetnek elő, hanem közvetlen hatással lehetnek a lakosság mindennapi életére is. Jelen tanulmány vizsgálja a kritikus szervezetek és infrastruktúrák védelmének nemzetbiztonsági dimenzióit, és rámutat a CER és a NIS2 uniós irányelvek szerepére az érintett szervezetek védelmének megerősítésében. A tudományos munka emellett párhuzamot von a lakossági felkészültség fokozásának szükségességével, amely az aktív felkészítés és a digitális tájékoztatás révén csökkentheti a krízishelyzetek kialakulását, és elősegítheti a hatékony eseménykezelést. Az esettanulmányokon alapuló kutatás konkrét példákkal mutatja be a hibrid fenyegetések hatásait, különös tekintettel a kritikus szolgáltatások működésére gyakorolt következményekre. A szerzők javaslatokat fogalmaznak meg a katasztrófavédelem digitális eszközökkel való támogatására, beleértve a lakosság katasztrófavédelmi felkészítésének eszközrendszerét is.

Kulcsszavak: *kritikus infrastruktúra, CER és NIS2 irányelvek, hibrid hadviselés, lakosságfelkészítés*

Today's modern hybrid threats pose increasingly complex challenges to critical infrastructure and essential service providers. Cyber and sabotage attacks against infrastructures can not only cause economic and political instability but can also

[1] Egyetemi docens, intézetigazgató-helyettes, tanszékvezető, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Katasztrófavédelmi Intézet, e-mail: ambrusz.jozsef@uni-nke.hu
[2] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: vasarhelyi.ors.laszlo@stud.uni-nke.hu

have a direct impact on the daily lives of citizens. This paper explores the national security dimensions of the protection of critical organisations and infrastructures and highlights the role of the EU CER and NIS2 Directives in strengthening the protection of these organisations. The academic draws parallels with the need to increase citizen preparedness, which through active preparation and digital information can reduce the occurrence of crisis situations and facilitate effective incident management. The case study-based research illustrates the impact of hybrid threats through concrete examples, with a particular focus on the consequences for the functioning of critical services. The authors make suggestions for supporting disaster management with digital tools, including tools for citizen preparedness.

Keywords: *critical infrastructure, CER and NIS2 directives, hybrid warfare, citizen preparedness*

Bevezetés

A modern társadalmak nagymértékben függenek az alapvető szolgáltatásokat nyújtó szervezetektől és a kritikus infrastruktúráktól – legyen szó energiaszolgáltatásról, kommunikációs hálózatokról, közlekedési rendszerekről vagy pénzügyi szolgáltatásokról. *Magyarország Nemzeti Kiberbiztonsági Stratégiája* is hangsúlyozza, hogy az elsődleges cél a megelőzésre épülő hatékony védelmi intézkedések révén a kibertérből érkező fenyegetések és azok kockázatainak kezelése. Ez napjainkban talán aktuálisabb, mint a stratégia megalkotásakor volt, hiszen egyre több konfliktus bontakozik ki világszerte, ezért hazánknak kiemelt figyelmet kell fordítania a biztonságra, így elkerülhetetlen az alapvető szolgálatást nyújtó szervezetek védelmének fokozása. A modern hadviselésben egyre nagyobb szerepet kapnak a hagyományos katonai erők mellett megjelenő aszimmetrikus eszközök és technikák is, mint például a kibertámadások és a dezinformációs kampányok. A kritikus infrastruktúrák és az alapvető szolgáltatást nyújtó szervezetek célpontként történő kiválasztása vonzó, mert ezen szervezetek rendszereinek a kompromittálódása vagy kiesése nemcsak gazdasági károkat okozhat, hanem társadalmi-politikai instabilitást és lakosságvédelmi problémákat is előidézhet. A 2024-es *Microsoft Defense Report* rámutatott annak tényére, hogy a modern hibrid konfliktusok során a kritikus infrastruktúra a fizikai csapások és a kibertámadások egyik fő célpontja. A Microsoft megfigyelte az alapvető szolgáltatást nyújtó szervezetek kritikus folyamatait vezérlő OT-rendszerek elleni támadások növekedését.[3]

Az új típusú szürkezónás hadviselési forma – amely a béke és a háború közötti határon mozgó katonai, gazdasági, politikai és kiberműveletek összessége, célja pedig egy állam vagy egy szervezet destabilizációja nyílt háborús konfliktus kockázata nélkül – relatív alacsony erőforrás-befektetés mellett is súlyos hatásokat képes elérni, ezért a modern társadalom biztonsága szempontjából elengedhetetlenül fontos a kritikus infrastruktúrák és a kritikus szervezetek megfelelő védelme, valamint a lakosság felkészítése a kedvezőtlen események hatásaira.[4] Hazánk nemzetbiztonsági érdeke ezen szervezetek és infrastruktúrák védelme

[3] *Microsoft Digital Defense Report 2024:* 20.
[4] Kiss 2019: 17–37.

és az ezzel összefüggő lakosságvédelem, hiszen ezek biztosítják a társadalom és a gazdaság alapvető működését és stabilitását konfliktushelyzetekben is.

Jelen tudományos munka célul tűzte ki, hogy rávilágítson a lakosság és a kritikus szervezetek rezilienciájának nemzetbiztonsági jelentőségére egy összehangolt hibrid támadással vagy kibertámadással szemben. Továbbá a szerzők célja, hogy bemutassák a CER és a NIS2 irányelv szerepét a kritikus szervezetek és infrastruktúrák 21. századi kihívásokkal szembeni védelmi képességének erősítésében, valamint a lakosság felkészítését az új évszázad kihívásaival szemben, annak technológiai előnyeit felhasználva.

Kutatási módszertan

Jelen tudományos munka elkészítése során a szerzők elsődlegesen szekunder adatokat dolgoztak fel, valamint a CER és a NIS2 irányelv implementációs tevékenységből fakadó új jogszabályok összehasonlító elemzését végezték el, emellett analitikai szempontból vizsgálták a témában megjelent releváns irodalmat. A szerzők azonosították a releváns forrásokat, majd a különböző forrásokból származó adatok egyesítésével összefüggéseket vontak le az adatokban lévő mintázatokból, és következtetéseket fogalmaztak meg. Esettanulmányokon keresztül mutatják be a kritikus szervezetek kitettségét a 21. századi kihívásoknak, valamint górcső alá kerültek a támadásokat követő hatások. A nemzetközi színtér esettanulmányaiból levont következtetések hazai viszonylatban is értelmezhetők. Emellett a szerzők empirikus kutatást is végeztek, amelynek célja az volt, hogy közvetlen információkat szerezzenek a kritikus infrastruktúrák és az alapvető szolgáltatást nyújtó szervezetek rezilienciáját célzó intézkedések gyakorlati alkalmazásáról és kihívásairól, különböző munkaprojektek keretében, valamint az iparági jógyakorlatok vizsgálatával. A szerzők a Shodan keresőmotort alkalmazták annak érdekében, hogy magyarországi sérülékeny ipari rendszerelemeket keressenek a hazai szervezetek potenciális kitettségének alátámasztására.

A kritikus infrastruktúrák sérülékenysége

A kritikus infrastruktúrák, valamint a kritikus szervezetek stabil üzemfolytonos működése alapvető nemzetbiztonsági érdek és érték, mivel azok meghibásodása vagy kompromittálódása a lakosság ellátásának összeomlásához, társadalmi zavarokhoz és gazdasági károkhoz vezethet. Magyarország földrajzi helyzete és energiafüggősége[5] különösen érzékennyé teszi az országot a hibrid és kiberfenyegetésekre, ilyen például az energiaellátási láncok megszakadása, ami gazdasági és társadalmi feszültségeket kelthet.[6] Törekedni kell arra, hogy a hazai kritikus infrastruktúrák a kockázatokkal arányos védelmi képességet alakítsanak ki, és ne rendelkezzenek olyan támadási felületekkel, amelyek célzott fenyegetések látókörébe helyezhetik.

[5] Brucker–Jóna–Szemerédi 2024: 155–182.
[6] Ambrusz–Beke 2023: 638–639.

Hibrid hadviselés keretében a kritikus infrastruktúrák elleni támadások stratégiai eszközzé váltak:

- Fizikai támadások (például energiaellátó hálózatok szabotálása vagy katonai műveletek keretében történő támadása).
- Kibertámadások, amelyek adatvesztéssel járhatnak, továbbá megbéníthatják az üzemfolytonosságot, illetve az ügy- és üzletmenet-folytonosságot.

A kritikus szervezetek az általuk nyújtott szolgáltatástól függően, de jellemzően IT-rendszerek mellett kiberfizikai (OT-) rendszereket is alkalmaznak. Ezeknek a kiberfizikai rendszereknek a szerepe, hogy az egyes ipari folyamatokat irányítsák. Az ipari vezérlőrendszerek segítségével megfelelő felügyeleti kontrollt képesek ezen szervezetek biztosítani folyamataikra. Ugyanakkor fontos megemlíteni, hogy ezen ipari rendszerek jellemzően kevesebb védelmi képességgel rendelkeznek, mint az IT-rendszerek, így amennyiben hálózatra vannak kapcsolva, sérülékenyek lehetnek a kibertérből érkező támadási kísérletekkel szemben. Ezek az ipari vezérlőrendszereket ért sikeres kibertámadások már képesek lehetnek az ipari folyamatokba beavatkozni és akár negatív hatást gyakorolni fizikai világunkra.

Sérülékenységi statisztika

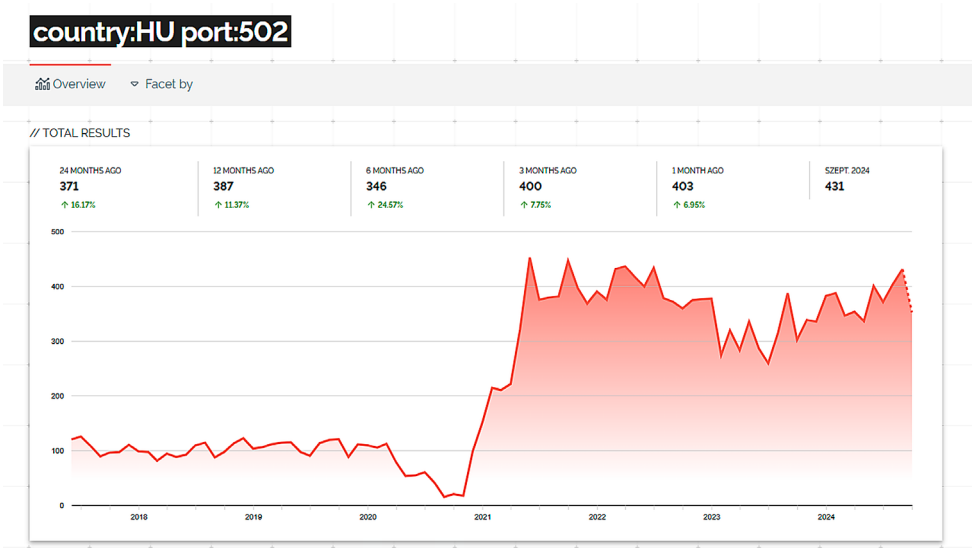
Eltérően a hagyományos keresőktől, a Shodan nem weboldalakra, hanem olyan hálózati eszközökre koncentrál, mint az Internet of Things (IoT) eszközök, szerverek, ipari vezérlőrendszerek, webkamerák és routerek. A keresőmotor az internetre csatlakozó eszközök nyitott portjait és egyéb alapinformációit gyűjti össze, így a biztonsági szakemberek számára értékes adatforrás lehet. Lehetőség van IP-cím, nyitott portok, használt protokollok, szoftververziók és geolokációs adatok alapján keresni.[7]

A Shodan elsősorban etikus hackerek és kiberbiztonsági szakemberek eszköze, amelyet az internetre csatlakozó eszközök biztonsági állapotának vizsgálatára használnak. A nyitott portokon keresztül elérhető eszközök adatai érzékenyek lehetnek, és a jogosulatlan hozzáférés büntetőjogi felelősséggel járhat. A platform segítségével olyan portokat is lehet keresni, amelyek ipari vezérlőrendszerekhez tartoznak, és nyitva vannak az internet felé.

Az ipari hálózatok több olyan portot használnak, amelyek rendszerelemekhez biztosítanak hozzáférést, például vezérlőkhöz, szenzorokhoz és egyéb hálózati eszközökhöz. A tanulmány három olyan nyitva lévő portot mutat be, amely potenciálisan veszélyeztetheti az ipari rendszereket; az adatok anonimizáltak. Az 1., a 2. és a 3. ábra az internet felé nyitott magyarországi portok számát és az elmúlt évek trendjeit (növekedés vagy csökkenés) szemléltetik.

A Modbus TCP/IP egy elterjedt ipari protokoll, és az 502-es portot használja. Gyakran használják ipari vezérlőrendszerekben, és ha nyitva van az internet felé, az veszélyes lehet, így a támadók akár érzékeny adatokat is kiolvashatnak, vagy manipulálhatják a vezérlési parancsokat. Valamint ez a hozzáférés lehetőséget adhat a támadóknak az ipari folyamatok megzavarására, vagy akár a termelési vagy munkafolyamatok leállítására. 2024 szeptemberében 431 darab magyarországi potenciálisan sérülékeny ipari rendszerelem

[7] *What is Shodan?* [é. n.].



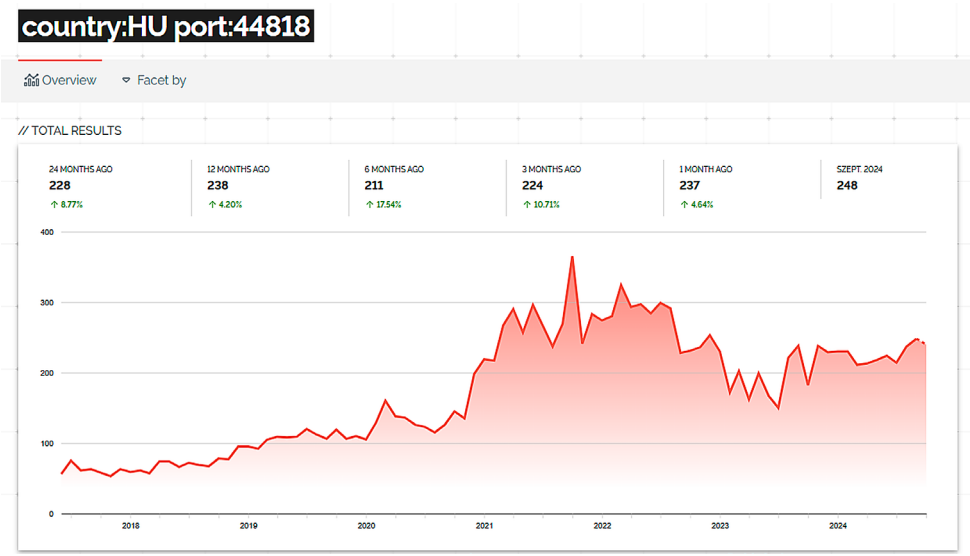
1. ábra: 502-es porton keresztül nyitva lévő magyarországi sérülékeny rendszerelemek számának alakulása
Forrás: Shodan keresőmotor Trends felületének képernyőképe a nyitott 502-es portokkal rendelkező magyar rendszerelemekről, https://www.shodan.io

volt elérhető ezen a nyitott porton keresztül. Az ilyen típusú hozzáférések kockázatait és a lehetséges támadások detektálását mesterséges intelligencia alkalmazásával hazai kutatók vizsgálták egy Modbus-alapú szimulált környezetben, kimutatva, hogy gépi mélytanulási és statikus tanulási módszerek ígéretesek lehetnek hálózati csomagokkal kapcsolatos anomáliák azonosításában.[8]

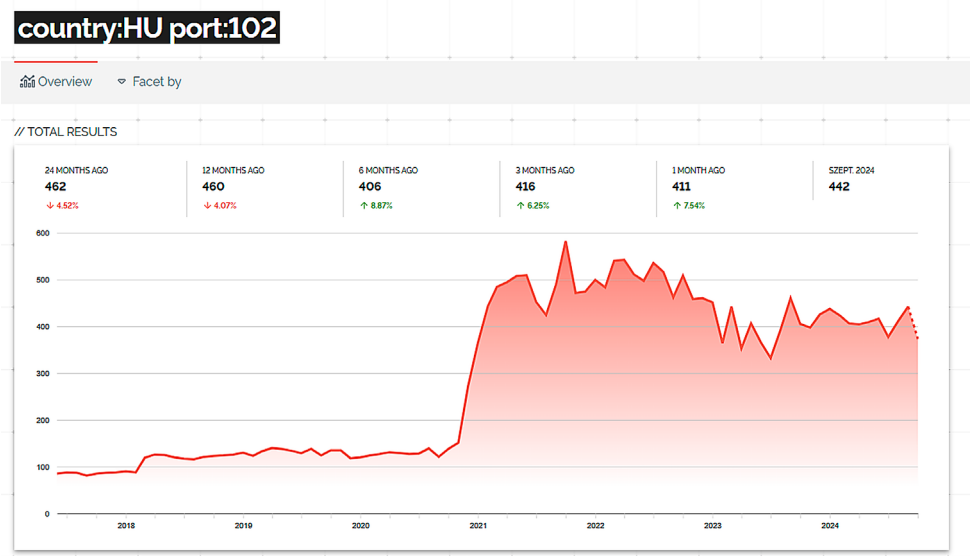
Az internet felé nyitott 44818-as port jelentős biztonsági kockázatot hordoz, mivel az EtherNet/IP protokollt használja, amelyet gyakran alkalmaznak ipari vezérlőrendszerekben, például programozható logikai vezérlőkben (PLC). Ha ez a port védelem nélkül elérhető az interneten, a jogosulatlan behatolók képesek lehetnek hozzáférni a vezérlőkhöz, és így manipulálhatják az ipari folyamatokat, leolvashatják vagy módosíthatják a vezérlési paramétereket, illetve leállíthatják az eszközöket. A szerzők a kutatás idején 248 darab magyarországi potenciálisan sérülékeny ipari rendszerelemet találtak, amelyek ezen a porton keresztül elérhetők voltak.

Az internet felé nyitott 102-es port is rejthet kiberbiztonsági rizikót egy szervezet számára, mivel ezt a portot a Siemens S7 protokoll használja, amelyet gyakran alkalmaznak ipari vezérlőrendszerekben, különösen PLC-k kommunikációjához. Ha ez a port nyitva van és védtelen az interneten, a támadók hozzáférhetnek az ipari vezérlők parancsaihoz és adatfolyamaihoz, lehetővé téve számukra a rendszer működésének manipulálását, a termelési folyamatok megzavarását, túlterhelését vagy leállítását.[9] A kutatás idején

[8] Dobrády–Takács–Hidvégi 2023: 62–68.
[9] CISA 2023a.



2. ábra: A 44818-as porton keresztül nyitott hazai rendszerelemek számának alakulása az elmúlt években
Forrás: Shodan kereső Trends felületének képernyőképe a nyitott 44818-as portokkal rendelkező hazai rendszerelemekről, https://www.shodan.io



3. ábra: A 102-es porton keresztül nyitott hazai rendszerelemek számának alakulása az elmúlt években
Forrás: Shodan keresőmotor Trends felületének képernyőképe a nyitott 102-es portokkal rendelkező hazai rendszerelemekről, https://www.shodan.io

442 darab magyarországi a 102-es porton keresztül nyitott rendszerelem volt megtalálható a Shodan keresőfelülettel.

A nyitott port önmagában nem zárható ki pusztán portokollszintű megoldásokkal, azonban az ipari kommunikáció titkosítása jelentősen csökkenti a támadók által megszerezhető információ értékét. Ezzel a megközelítéssel foglalkozott Antal József és Hidvégi Timót is, akik olyan titkosított ipari kommunikációs protokollt és tesztkörnyezetet dolgoztak ki, amely képes biztosítani a csomagok védelmét az illetéktelen olvasással és manipulációval szemben, még akkor is, ha a hálózati elérés technikailag lehetséges marad a fent bemutatott portokon keresztül. További előnye, hogy ez a kriptográfiai protokoll meglévő rendszerekbe is integrálható.[10]

Esettanulmányok

Colonial Pipeline

A Colonial Pipeline elleni kibertámadás 2021 májusában történt, és az Amerikai Egyesült Államok egyik legnagyobb kritikus infrastruktúra elleni zsarolóvírus-támadása volt, amely nyilvánosságra került. A Colonial Pipeline az Egyesült Államok egyik legjelentősebb olajvezetéke. Ezen keresztül történik az olaj szállítása a Mexikói-öbölből a keleti parti államokba. A támadók, a feltehetőleg kelet-európai kötődésű DarkSide nevű hackercsoport egy virtuális privát hálózathoz (VPN) tartozó jelszó kiszivárgását kihasználva fért hozzá a Colonial Pipeline informatikai hálózatához, ahol 100 GB adatot loptak el, majd zsarolóvírust telepítettek. A támadás több lépcsőben zajlott a Colonial Pipeline informatikai rendszerei ellen. A csővezeték kiberfizikai (OT) rendszerei, amelyek ténylegesen felelnek az olajszállításért, nem kerültek közvetlen veszélybe a támadás során. Azonban a vállalat megelőző intézkedésként leállította az üzemanyag-ellátó rendszert, amelynek kiesése jelentős hiányt és pánikot okozott az Egyesült Államok keleti partján. A vállalat 75 bitcoin (mintegy 4,4 millió dollár) váltságdíjat fizetett a támadóknak a rendszerei és adatai visszaállításáért, azonban a hatóságok később visszaszereztek abból 63,7 bitcoint (körülbelül 2,3 millió dollár).

A DarkSide hackercsoport tagjai nem állami háttérrel működő kiberbűnözők. Állításuk szerint egészségügyi, oktatási, állami és nonprofit szervezetek ellen nem követnek el kibertámadást. Elsődleges működési modelljük az RaaS (Ransomware as a Service), ransomware vírusokat fejlesztenek és terjesztenek más kiberbűnözői szervezetek számára, amelyek aztán önállóan végzik a vírusok telepítését a célpont hálózatokon, a váltságdíjak egy bizonyos százalékát a vírus fejlesztői kapják meg. A DarkSide Ransomware egy olyan RaaS, amely gyakran alkalmaz kettős zsarolási taktikát. A célhálózatba való beszivárgás után az érzékeny adatokat titkosítja, és váltságdíjat követel azok feloldásáért cserébe. Emellett a kiberbűnözők azzal is fenyegetőznek, hogy ha nem fizetik ki a váltságdíjat, nyilvánosságra hozzák a megszerzett adatokat, vagy a dark weben keresztül értékesítik azokat.

A DarkSide az adathalászatot, a gyenge hitelesítő eszközöket és az ismert sebezhetőségeket (például a CVE-2021-20016-ot, a SonicWall SMA100 SSL VPN megoldás

[10] Antal–Hidvégi 2021: 106–112.

SQL-injekcióját) használja fel a rendszerekhez való kezdeti hozzáférés megszerzéséhez. Ezután a kártékony kód rendszergazdai jogosultságokat szerez, megkerülve az UAC-t a CMSTPLUA COM interfész segítségével, így a támadók teljes hozzáférést kapnak az érzékeny adatokhoz, illetve fontosabb műveletek végrehajtásához. A fájlok titkosítására Salsa20 szimmetrikus titkosítási kulcsot használ, majd egy RSA-1024 aszimmetrikus kriptográfiai algoritmus publikus kulcsával titkosítja a Salsa20 kulcsot, így annak feloldása csak az RSA privát kulcsával lehetséges (ez a támadóknál van). Ez a módszer azért hatékony, mert a Salsa20 gyors, míg az RSA-1024 lehetővé teszi a Salsa20 kulcs megfelelő erősségű titkosítását.[11]

A Colonial Pipeline Company elleni kibertámadásnak szinte azonnali hatása volt, hiszen az üzemanyag-ellátás üzemfolytonossága megszakadt, ami számos negatív következménnyel járt. A légi közlekedés esetén számos légitársaságnál, köztük az American Airlinesnál üzemanyaghiány lépett fel, így a keleti parti reptereken korlátozott fennakadások alakultak ki. Emellett az Amerikai Egyesült Államok társadalmi mobilitásának alappillére a személygépkocsik széles körű használata, így a lakosság körében a benzinhiánytól való félelem pánikvásárlást eredményezett, aminek következtében az üzemanyagok ára is jelentősen megnőtt, valamint egyes területeken üzemanyaghiány lépett fel, mivel a fogyasztók a megszokottól eltérően jelentős többletüzemanyagot vásároltak.[12]

A CISA elemzése a Colonial Pipeline elleni 2021-es zsarolóvírus-támadás kapcsán hangsúlyozza az amerikai kritikus infrastruktúrák sebezhetőségét és a kiberbiztonsági intézkedések fontosságát. A támadás nyomán az Egyesült Államok kormánya számos intézkedést hozott, beleértve a Shields Up kampányt, a Joint Ransomware Task Force létrehozását, valamint a CyberSentry kibervédelmi program bővítését. 2021 májusában a Biden-kormányzat végrehajtási rendeletet adott ki, amelyben utasította az amerikai állami szerveket, hogy hajtsanak végre proaktív lépéseket a kiberbiztonság megerősítése érdekében.[13]

Német kórházak elleni támadás

2023. december 24-én több német kórház is kibertámadás áldozatává vált, amely mögött a Lockbit nevű kiberbűnözői csoport állt. A támadók célpontjai a Kelet-vesztfáliai Katolikus Kórházi Szövetség (KHO) intézményei voltak. A Szövetségbe tartozó hat kórházból háromnál történt szolgáltatás-összeomlás a Lockbit 3.0 ransomware támadás következtében. A támadások súlyosan érintették a kórházak működését támogató rendszereket, ezek aztán több sürgősségi ellátás megszakadását is okozták.

A kórházak IT-hálózatához hozzáférve a támadók titkosították az adatokat, az első tesztek alapján egyértelmű volt, hogy ransomware támadás történik. A támadás hatókörébe tartozó rendszerek visszaállítási ideje nem volt előre meghatározható. A kórházak központi IT-osztálya leállította az összes rendszert, és gondoskodott az intézmények értesítéséről. A kórházak kritikus szerepet játszanak az egészségügyi szolgáltatások nyújtásában az adott

[11] Chiscariu 2021.
[12] Kerner 2022.
[13] Easterly 2023.

régióban, így egy, az informatikai rendszereiket érintő kibertámadás súlyos következményekkel járhat az orvosi vészhelyzetben lévő emberek számára.

A KHO közleménye egyértelművé teszi, hogy a betegellátás a normális keretek között folytatódott az érintett kórházakban, és minden klinikai tevékenység továbbra is elérhető volt, bizonyos technikai korlátozásokkal. A biztonsági mentések sikeres helyreállítása révén a betegek alapvető adatai továbbra is hozzáférhetők maradtak. A sürgősségi ellátás azonban a három KHO-kórházban nem volt elérhető, így a sürgős orvosi ellátásra szoruló embereket máshová irányították, ami kritikus késedelmeket okozhatott, valamint általános elégedetlenséget szült az érintett kórházakkal szemben, a német egészségügy feltehetően reputációbéli veszteséget könyvelhetett el.[14]

Nem található arra vonatkozó információ, hogy a támadók hogyan jutottak be a kórházak IT-hálózatába, azonban a Lockbit Ransomware-t (RaaS) használók gyakran a sebezhető Remote Desktop Protocol (RDP) szerverek vagy a dark weben vásárolt, kompromittált hitelesítő adatok használatával szerzik meg a kezdeti hozzáférést. A kezdeti hozzáférési vektorok közé tartoznak még az e-mailek rosszindulatú mellékletei vagy a linkeket tartalmazó adathalász e-mailek, illetve a Fortinet VPN-ek olyan sebezhetőségének kihasználása, mint például a CVE-2018-13379.

A hitelesítő eszközök megszerzésére, valamint a hálózat felderítésére gyakran ingyenesen elérhető, legális eszközöket, szoftvereket használnak fel, ilyen például az AdFind GMER és a Mimikatz, ezek mellett gyakran alkalmaznak penetrációs vizsgálatokhoz használt eszközöket, mint a Cobalt Strike és a Metasploit. A vírus laterális-oldalirányú terjedéssel más, a hálózatban részt vevő rendszerelemeket is képes célba venni.

A LockBit AES és RSA titkosítást használ a fájlok enkriptálására. A vírus csak az első néhány kilobájtot titkosítja a gyorsabb működés érdekében, valamint az érintett fájlhoz egy *.lockbit* kiterjesztést fűz, ezzel jelezve, hogy titkosítva van. Ezt követően a vírus lecseréli az asztali háttérképet egy váltságdíjat követelő üzenetre, amennyiben pedig a megtámadott eszközre vagy hálózatra nyomtatók is csatlakoztatva vannak, a váltságdíjat követelő üzeneteket automatikusan kinyomtatja, hogy az áldozatok biztosan észrevegyék, hogy az adataik kompromittálódtak. Ennél az esetnél nem kerültek nyilvánosságra az utólagos vizsgálat eredményei, így nem derült ki, hogy a kiberbűnözők ellopták-e a betegek adatait vagy más érzékeny információkat.[15]

Az elmúlt években számos kibertámadásért a LockBit Ransomware volt a felelős, aminek megállítása érdekében az Europol, az FBI és a brit Nemzeti Bűnüldözési Ügynökség egy összehangolt nyomozás keretében végül 2024 februárjában elfogta a zsarolóvírust fejlesztő kiberbűnözői banda feltételezett vezetőjét, akit vád alá helyeztek és elítéltek. Természetesen a támadások nem értek véget, hiszen a Lockbit 3.0 zsarolóvírus szolgáltatásként történő értékesítése (RaaS) a mai napig tart. A többi vezető felkutatásáért 10 millió dolláros nyomravezetői díjat tűzött ki az amerikai kormány. A japán rendőrség által kifejlesztett LockBit 3.0 dekódoló elérhető a NoMoreRansom weboldalán, a felhasználásával nagy valószínűséggel a titkosított adatok visszaszerezhetők váltságdíj megfizetése nélkül.[16]

[14] Toulas 2023.
[15] CISA 2023b.
[16] Euronews 2024.

Ez az eset rávilágít arra, hogy az Európai Unió alapvető szolgáltatásokat nyújtó szervezetei ki vannak téve a kibertámadásoknak, amelyek akár emberéleteket is veszélyeztethetnek, valamint zavart kelthetnek a társadalomban. A hatékony megelőzés és védelem kialakítása érdekében az Európai Unió NIS2 és CER direktívái által szorgalmazott védelmi intézkedések megfelelő implementációja csökkentheti az ilyen jellegű támadások sikeres bekövetkezésének valószínűségét.

Dán villamosenergia-rendszer elleni kibertámadás-sorozat

A dán SectorCERT, amely Dánia kritikus infrastruktúrái felett lát el kiberbiztonsági felügyeletet, mint incidenskezelő központ publikált a dán villamosenergetikai szervezeteket ért kibertámadásokról egy részletes tanulmányt. A támadók összesen, két hullámban, 22 sikeres támadást hajtottak végre energiaszektorbéli szervezetek ellen. A jelentés szerint államilag támogatott támadócsoportokról lehet szó, amelyek előre kiválasztott célpontokat vettek célba alaposan előkészített, fejlett technikákkal. Az elkövetők pontosan tudták, mely szervezeteket érdemes megcélozniuk, és milyen sérülékeny rendszerelemeket kell támadniuk. Továbbá a támadásra utaló jeleket igyekeztek elfedni az áldozatok hálózati forgalmában.

A támadások első hulláma 2023. május 10-én kezdődött, a támadók a CVE-2023-28771 sérülékenységet használták ki, amely a Zyxel tűzfalak egyik súlyos biztonsági hibája volt. A sebezhetőség lehetővé tette a támadók számára, hogy egy speciálisan kialakított hálózati csomagot az 500-as porton keresztül küldve teljes irányítást szerezzenek az érintett tűzfal felett, anélkül, hogy felhasználóneveket vagy jelszavakat kellett volna ismerniük. Ez azért különösen súlyos, mert maga a tűzfal az első védelmi vonal a kritikus rendszerekhez való hozzáférés megakadályozásában. Azonban a támadókat leleplezték és még idejében kizárták a megtámadott szervezetek hálózataiból, köszönhetően a SektorCERT, a tűzfal beszállítói és a szervezetek szakemberei együttes erőfeszítéseinek.

A támadássorozat második hulláma 2023. május 22-én kezdődött, ekkor a támadók már új technikákat és eszközöket vetettek be. Az egyik energetikai szervezet tűzfalára egy nem biztonságos kapcsolaton keresztül új szoftvert töltöttek le, ami gyanút keltett. A tűzfal ezután úgy kezdett el viselkedni, mintha egy botnet részévé vált volna, a támadók egy elosztott szolgáltatásmegtagadással járó támadást (DDoS) készítettek elő a rendszerelemek megfertőzésével. A kompromittált szervezet eszköze két célpontot érintő DDoS-támadásban vett részt az Egyesült Államokban és Hongkongban. Ekkor a SektorCERT értesítette az áldozattá vált szervezetet, amely azonnal szigetüzemre állt át, a tűzfal beszállítója pedig segített újrakonfigurálni a kompromittálódott eszközt, valamint meggyőződtek arról, hogy a támadók a DDoS-támadásokon kívül másra nem használták a hozzáférést. Ezt követően ismét hasonló incidens történt a tűzfallal, így a szervezet szigetüzemre állt vissza.

Május 23-án egy másik energetikai szervezet infrastruktúráját kompromittálták, hogy Secure Shell (SSH) kriptográfiai protokollon keresztüli brute-force – vagyis olyan automatizált módszer, amely különböző jelszó- vagy kulcskombinációkat próbál végig

a hozzáférés megszerzése érdekében – támadásban használják fel egy kanadai szervezet ellen, a SektorCERT és a dán cég végül ki tudta zárni a támadókat a kompromittált hálózatból.

Május 24-én a SektorCERT felügyelete alá tartozó négy energetikai vállalat tűzfala kompromittálódott egy MIPSkiller nevű rosszindulatú kódsor miatt (payload) és kezdett el DDoS-támadásokban önkéntelenül részt venni, ameddig meg nem szakították a hackerek irányítását. Egy esetben a tűzfal túlterhelődött és leállt, ami az adott szervezet hálózatának leállását is előidézte. Az egyik szervezet kamerarendszere volt egy Zyxel tűzfal mögött, amit szintén kihasználtak, és a MIRAI Moobot része lett.

A második hullámú támadásoknál feltűnő volt, hogy a támadók olyan sérülékenységekről is tudhattak, amelyeket a Zyxel még nem hozott nyilvánosságra. A SektorCERT a támadások elemzése alapján úgy vélte, hogy a május 11-én észleltektől eltérő típusú támadásról van szó. Ez gyakorlatilag zero-day támadás volt, mert olyan sérülékenységeket használt ki, amelyek nem voltak ismertek akkor, a tűzfal gyártója napokkal később jelentette ezeket (CVE-2023-33009 és CVE-2023-33010).

Május 24-én este a SektorCERT a Sandworm APT csoportra utaló hálózati forgalmat azonosított a riasztás alapján. Az APT csoport jellemzően akkor kezd el műveleteket végrehajtani, ha valamely állam működését politikai vagy katonai megfontolások miatt meg akarják zavarni. A támadók ügyeltek arra, hogy észrevétlenek maradjanak, a kompromittálódás után mindössze egyetlen csomagot küldtek vissza, (egy pinget) a hálózati forgalommal. Jellemzően ezek tesztkapcsolatok a támadó command and control (C2) szerverével vagy egy rejtett azonosító jelzés, amely megerősíti a támadók számára, hogy sikerült kompromittálni a rendszert, és az elérhetővé vált számukra. A Sandworm csoportra utaló jelek megjelenésekor a SektorCERT a dán rendőrségen belül működő Nemzeti Kiberbűnözési Központ bevonása mellett döntött. Az érintett szervezet tűzfalát lefoglalták, hogy a lehető legtöbb bizonyítékot szerezhessék meg. Így a vállalat 6 napig szigetüzemben működött, amíg az addig használt Zyxel tűzfalakat nem cserélték le más márkájúakra.

Másnap egy másik létfontosságú szervezetnél ismétlődött meg a Sandworm-féle támadás, azonban itt már a távoli ipari rendszerek elérhetetlenné váltak a szervezet központi felügyeleti rendszere számára, mert a megtámadott tűzfal belső routerként is működött az OT-hálózatban, ezért az üzemnek manuális irányításra kellett átállnia a távoli helyszíneken is. Párhuzamosan ezzel a támadással másik két biztonsági incidens is volt, a nyomok alapján azonban itt más típusú támadás történt a tűzfalakkal szemben, vélhetően más elkövetők álltak mögötte.

Amint a dán kritikus infrastruktúrák által alkalmazott tűzfal-sérülékenységek nyilvánosságra kerültek, a dán kritikus szervezetek elleni támadási kísérletek száma drasztikusan megnőtt főként lengyel és ukrán IP-címekről, azonban eddigre már ezen IT- és OT-hálózatok tűzfal-sérülékenységeit kijavították, így a támadási kísérletek sem voltak hatásosak. A támadások után az amerikai CISA is felvette a Zyxel tűzfalak sérülékenységeit az aktívan kihasználható sebezhetőségek listájára.[17]

Az esettanulmány rávilágít arra, hogy a dán energetikai infrastruktúrák hatékony és gyors reagálású védekezési képessége a SektorCERT-nek, a beszállítóknak és az adott szervezeteknek az együttműködésével valósulhatott meg. Ennek köszönhetően meg lehetett állítani a további eszkalációt, ami súlyos következményekkel járt volna a szolgáltatás

[17] SektorCERT 2023.

folytonosságára és magára a kiberfizikai rendszerekre nézve is, valamint a dán nemzetbiztonságra. A jövőben gondoskodni kell arról, hogy rendszerszintű sérülékenységek ne forduljanak elő egy-egy ágazat szereplőinek infrastruktúráiban, amelyek kihasználása révén a támadók egy időben tudnak végrehajtani célzott támadásokat valamennyi szereplő ellen. A folyamatos biztonság fenntartása érdekében számos olyan védelmi intézkedést szükséges bevezetni, amely a kockázatokkal arányos módon biztosítja egy-egy szervezet kibervédelmi képességét, ezek tételes ismertetésére a jelentés kitér.

A CER és a NIS2 irányelv szerepe a hazai kritikus szervezetek esetén

Az Európai Unió kritikus szervezeteinek és kritikus infrastruktúráinak fokozott kiberkitettségei és fizikai sebezhetőségei ellen az Európai Parlament és a Tanács még 2022 decemberében kiadta a két irányelvét, hogy előmozdítsa az Unióban lévő fontos és alapvető szolgáltatást nyújtó szervezetek teljes körű rezilienciájának kialakítását.[18] Hazánk kritikus szervezeteire az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedések érvényesek, *az Európai Parlament és a Tanács (EU) 2022/2555 irányelve a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről* (a továbbiakban: NIS2), illetve *az Európai Parlament és a Tanács (EU) 2022/2557 irányelve a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről* (a továbbiakban: CER) irányelv hazai jogszabályai is vonatkoznak, aminek köszönhetően ezen szervezetek képesek lesznek egy hatékony, a kockázatokkal arányos védelmi képességet kialakítani. A NIS2 irányelv 15 ágazatra terjeszti ki a hatályát, így nemcsak a kritikus infrastruktúrák, hanem egyéb, nemzetbiztonsági szempontból kiemelt szervezetek is a hatókörébe tartoznak. Az egységes uniós szabályozás elősegíti a tagállamok együttműködését, gyorsabbá és hatékonyabbá téve az incidenskezelést. Magyarország számára ez magasabb szintű kiberbiztonsági védelmet, hatékonyabb incidenskezelést és erősebb nemzetközi együttműködést jelent, elősegítve a digitális gazdaság és az ipari szektor biztonságos fejlődését. A hatósági felügyelet, a szigorúbb biztonsági követelmények és auditok ösztönözhetik a szervezeteket a kiberbiztonság folyamatos fejlesztésére, ezáltal növelve a kockázatos ágazatok ellenálló képességét a kibertámadásokkal szemben. Az irányelvet a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény, annak végrehajtási rendelete, valamint a 7/2024 (VI.24.) MK rendelet implementálta a hazai jogrendbe. A jogszabály hatálya alá tartozó szervezetek számára magas szintű kiberbiztonsági követelmények teljesítése szükséges, beleértve a kockázatkezelési keretrendszerek kialakítását, a beszállítói lánc értékelését és a rendszeres biztonságtudatossági képzéseket. A szervezeteknek kiemelt figyelmet kell fordítaniuk az incidensek kezelésére, kivizsgálására, az üzletmenet-folytonosság biztosítására és a gyors helyreállásra. Az üzemeltetőknek biztosítaniuk kell a rendszereik folyamatos felügyeletét, ennek keretében többek között sérülékenységvizsgálatokat kell lefolytatniuk, és független auditokon kell megfelelniük az amerikai NIST 800-53 rev5[19] dokumentumon alapuló 7/2024 MK rendelet követelményeinek. A követelmények számosságát a szervezet

[18] Ambrusz–Dobor–Vásárhelyi 2024: 57–69.
[19] National Institute of Standards and Technology 2020.

rendszereinek száma és azok biztonsági osztályai (alap, jelentős, magas) befolyásolják. Azoknak a szervezeteknek, amelyeket a Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH) 2025. január 1. előtt nyilvántartásba vett, az idei év végéig kell számot adniuk felkészültségükről az első kiberbiztonsági audit során. Ha egy kritikus szervezet többségi tulajdona az államhoz köthető, annak ellenőrző és felügyeleti hatósága a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI). Amennyiben a szervezet felett egy gazdálkodó szervezet rendelkezik döntő tulajdoni hányaddal, a felügyeleti hatósági szerepkört az SZTFH tölti be.[20]

Magyarország, mint valamennyi tagállam, kijelölt egy nemzeti incidenskezelő központot és nemzeti kiberbiztonsági hatóságot is, mindkét szerepkört az NBSZ NKI látja el. A nemzeti kiberbiztonsági hatóság feladatai közé tartozik a kritikus szervezetek és az ország szempontjából jelentős szervezetek információbiztonsági szabályzatainak továbbítása a nyilvántartó hatóság számára, valamint az elektronikus információs rendszerek biztonságáért felelős személyek (IBF-ek) listájának közzététele. Az SZTFH által biztosított adatok figyelembevételével összeállítja az alapvető és fontos szervezetek jegyzékét, amelyet kétévente felülvizsgál. A hatóság jogosult sérülékenységvizsgálatok elvégzésére, akár hivatalból, akár az érintett szervezet kérésére. A nemzeti kiberbiztonsági hatóság alapvető vagy fontos szervezetként azonosíthatja azon szervezeteket, amelyek eddig valamilyen okból kifolyólag nem jelentkeztek be a hatóságnál, továbbá jogosult a szervezetek rendszereinek biztonsági osztályait felülbírálni.

A nemzeti kiberbiztonsági incidenskezelő központ feladata a kiberfenyegetések és incidensek kezelése, valamint a kritikus infrastruktúrák és szervezetek védelmének támogatása. Valamennyi, a NIS2 hatálya alá tartozó szervezetnek kötelessége haladéktalanul jelenteni minden releváns fenyegetést, incidensközeli helyzetet és kiberbiztonsági eseményt, ideértve az üzemeltetési incidenseket is. A központ proaktív, behatolásmentes sérülékenységvizsgálatokat végez a nyílt interneten elérhető rendszerek biztonsági állapotának felmérése céljából, és szükség esetén egyedi vizsgálatokkal is támogatja a szervezeteket. Emellett részt vesz a kiberbiztonsági stratégiák és szabályozások kidolgozásában, valamint szabványosított gyakorlatokat, ajánlásokat és kötelező érvényű állásfoglalásokat adhat ki az incidensek megelőzésére és kezelésére. A központ szükség esetén működtetheti a kormányzati információtechnológiai és kiberbiztonsági incidenskezelési együttműködési fórumot.

A NIS2 és CER irányelvek egymást kiegészítve erősítik az európai uniós kritikus szervezetek és infrastruktúrák rezilienciáját. A CER irányelv előírja a kritikus szervezetek azonosítását, a kockázatok értékelését, a fizikai védelmi intézkedések biztosítását, továbbá deklarálja a kiberbiztonsági védelmi intézkedések meglétének fontosságát. Magyarország és az EU számára ez megerősíti az ellátási láncok stabilitását, a közszolgáltatások védelmét és az állampolgárok biztonságát. A CER irányelv emellett elősegíti a tagállamok érintett hatóságai közti együttműködést és gyors reagálást válsághelyzetekben, így csökkentve az infrastruktúrákat érintő támadások és katasztrófák hatásait. Hazánk az irányelvet a kritikus szervezetek ellenálló képességéről szóló 2024. évi LXXXIV. törvény (a továbbiakban:

[20] Marsi–Orosházi 2025, 94. epizód.

Kszetv.), valamint annak végrehajtási rendelete, a 474/2024 (XII. 31.) Korm. rendelet által implementálta a hazai jogrendbe. A jogszabályi keret célja a magyarországi székhellyel rendelkező kritikus szervezetek ellenálló képességének növelése az alapvető szolgáltatások folyamatosságának biztosítása érdekében. Részletesen foglalkozik az egyes ágazatokkal és alágazatokkal, például az energetikai ágazattal. Az új törvény új fogalmakat vezet be, mint például a *kritikus szervezet,* a *kritikus szervezet ellenálló képességéért felelős vezető.* Előírja a kritikus szervezetek ellenálló képességére vonatkozó nemzeti stratégia és nemzeti kockázatértékelés kidolgozását, amely segíti a kritikus szervezetek kockázatértékelési tevékenységeit, és amelyet adott szervezet figyelembe vesz, amikor a saját kockázatértékelését, ellenálló képességi mátrixát és ellenálló képességi intézkedéseit hozza meg. Ennek az új szerepkörnek a betöltéséhez elengedhetetlen az NKE Katasztrófavédelmi Intézete által biztosított kritikusinfrastruktúra-védelmi biztonsági összekötő személy szakirányú továbbképzési szak elvégzése. Az Intézet a vonatkozó hazai jogi környezet figyelembevételével, valamint több mint két évtizedes iparbiztonsági oktatási tapasztalataira építve alakította ki a képzés tananyagát és struktúráját.[21]

A kritikus szervezeteknek ellenálló képességi tervet kell kidolgozniuk, és belső auditokat kell végezniük annak érdekében, hogy megfeleljenek a 474/2024 (XII. 31.) Korm. rendeletben előírt követelményeinek. Az állam az ellenálló képesség kialakítására támogatást nyújthat megfelelő szakmai útmutatók és segédletek kidolgozásával. A szabályozás kiemelten kezeli a határokon átívelő együttműködéseket, és létrehoz egy egyedüli kapcsolattartó pontot, amely az Európai Bizottsággal és más országok egyedüli kapcsolattartó pontjaival működik együtt. Az ellenőrző hatóság jogosult ellenőrzéseket végezni, szükség esetén pedig szankcionálni. Amennyiben a Kszetv.-ben előírtaktól a NIS2 hazai jogszabályai eltérően rendelkeznek, akkor az azokban foglaltak élveznek elsőbbséget. A szabályozás célja a proaktív védelem, vagyis a kockázatok előzetes felismerése és kezelése.

A kritikus szervezeteknek a fent felsorolt követelményeken túl szükséges a törvény végrehajtási rendelete által meghatározott biztonsági követelményeket teljesíteniük attól függően, hogy az általános ágazatkijelölő hatóság a három ellenálló képességi szint közül melyikbe sorolta. Az ellenálló képességi szintbe történő besoroláskor az illetékes hatóság figyelembe veszi az érintett kritikus szervezet által beküldött dokumentumokat, valamint a jogszabály 1. számú melléklete által meghatározott horizontális kritériumok teljesülését. A besorolásról hivatalos értesítést kapnak az érintett szervezetek.

A kritikus szervezetek rezilienciáját szabályzó hazai jogszabályok ezen szervezetek ellenálló képességének növelését célozzák, valamint azon túlmenően hozzájárulnak Magyarország nemzetbiztonságának megerősítéséhez is. A szabályozás meghatározza a szervezetek kijelölésének, ellenálló képességi szintbe sorolásának és kockázatértékelésének kereteit, miközben előírja az ellenálló képességi tervek kidolgozását, bemutatja a hatósági ellenőrzés és felügyelet rendszerét, valamint ismerteti a szintbe sorolástól függően és függetlenül megvalósítandó követelménykatalógus kontrolljait. Azonban ezen jogszabályok nem rendelkeznek az alapvető szolgáltatást igénybe vevő lakosság felkészítéséről, ha ezen infrastruktúrák egyesével vagy csoportosan kompromittálódnak.

[21] Kátai-Urbán – Bleszity – Vass 2025: 220–236.

A lakosságvédelem nemzetbiztonsági aspektusai

Napjaink információs társadalmában már elengedhetetlen, hogy a lakosságvédelmi tájékoztató kiadványok és a lakosságfelkészítő anyagok ne csak nyomtatott formában létezzenek, hanem széles körben, online is elérhetők legyenek. A lakosság digitális platformokon keresztül való felkészítése a válsághelyzetekre csökkenti a nemzetbiztonsági kockázatokat, mert minimalizálhatja azok kialakulásának valószínűségét. Mindez elősegíti az állami erőforrások hatékonyabb felhasználását, lehetővé téve azok célzottabb alkalmazását preventív intézkedésekben és válságkezelésben. Azonban napjainkban a lakosságot a természeti és civilizációs katasztrófák, valamint azok hatásai mellett fel kell készíteni az álhírek kiszűrésére is, ki kell alakítani a lakosság megfelelő médiaműveltségét.[22] Ez segít ellensúlyozni a dezinformációs kampányok és a digitális médián keresztül terjedő álhírek hatásait. Az Európai Unió 2022-ben kiadta a megerősített *Dezinformációs Gyakorlati Kódex*ét,[23] amelynek célja a dezinformáció elleni fellépés és az átláthatóság fokozása; ez egy önszabályzó keretrendszer, a benne foglaltakat az azt aláíró online platformok önként vállalják. Ennek a kódexnek részét képezi a felhasználói tudatosság növelése, valamint független tényellenőrző szervezetek működtetésének (fact-checkers) a lehetősége. Ma a dezinformációs kampányok súlyos nemzetbiztonsági kihívást jelentenek valamennyi állam számára. Ezek ellen a leghatásosabb védelem a lakossági médiaműveltségi programok elindítása. Néhány uniós tagállam ezeket már középiskolás kortól, a közoktatás infrastruktúráját is felhasználva alkalmazza. Jelenleg Magyarországon még nem elterjedtek ezek a médiaműveltségi programok, azonban az Európai Unió honlapján számos magyar nyelvű oktatóanyag és videó is elérhető a témával kapcsolatban.[24] Az EU Külügyi Szolgálata (EEAS) létrehozta az East StratCom Task Force-t, amelynek fő feladata a hamis információk azonosítása, elemzése és cáfolata. Az East StratCom Task Force együttműködik a tagállamok kormányaival, kutatóintézetekkel és médiapartnerekkel dezinformáció elleni fellépés érdekében, eddig változó eredménnyel.[25]

Már több uniós tagállam is bevezetett veszélyhelyzet-kezelő és/vagy -értesítő okostelefon-alkalmazást. Németországban a lakosság számára elérhető egy ingyenes mobilapplikáció, amely széles körű funkcionalitással bír. A Német Szövetségi Polgári Védelmi és Katasztrófavédelmi Hivatal (BBK) által fejlesztett NINA (Notfall-Informations- und Nachrichten-App) nevű alkalmazás lehetőséget biztosít arra, hogy a felhasználók az aktuális tartózkodási helyük alapján figyelmeztetéseket és riasztásokat kapjanak telefonjukra hang- és fényjelzésekkel egybekötve, miközben nem tárolja a felhasználó helyadatait. A NINA célja, hogy megbízható és gyors információkat nyújtson a lakosságnak a veszélyhelyzetek kezeléséhez, és elősegítse a megfelelő felkészülést és viselkedést különböző katasztrófahelyzetekben. A felhasználóknak lehetőségük van vészhelyzeti tippeket olvasniuk, amelyek kategorizálva vannak a természeti és ipari katasztrófatípusoknak megfelelően. Az eseményleírás mellett cselekvési ajánlásokat is megfogalmaztak számukra. Továbbá az adott veszély típusának megfelelő hatóság elérhetőségét és hivatalos honlapját is feltüntették az esetek leírásánál.[26]

[22] Európai Bizottság 2024.
[23] European Commission 2022.
[24] Európai Unió [é. n.].
[25] European Union External Action 2021.
[26] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe [é. n.].

Hazánkban jelenleg okostelefonokra az Országos Katasztrófavédelmi Főigazgatóság (BM OKF) által fejlesztett ingyenes mobilalkalmazás érhető el iOS és Android operációs rendszeren, a neve VÉSZ (Veszélyhelyzeti Értesítési Szolgáltatás). Az applikáció segítségével a felhasználók képesek valós időben tájékozódni veszélyhelyzetekről, például közlekedési balesetekről, tűzesetekről vagy időjárási riasztásokról. Az alkalmazás olyan kiegészítő funkciókkal rendelkezik, mint a felolvasási lehetőség és a nagykontrasztos mód. Valamint lehetőséget biztosít a helyalapú értesítések beállítására, így a felhasználók a tartózkodási helyükhöz kapcsolódó riasztásokat is megkaphatják. A VÉSZ célja, hogy megbízható, gyors és pontos információkkal segítse a lakosságot a veszélyhelyzetek elkerülésében és kezelésében. Azonban az applikáció a lakosság felkészítését jelen formájában nem támogatja, nincsenek felkészítéssel kapcsolatos funkciói.[27]

Fejlesztési lehetőségek a hazai katasztrófavédelmi rendszerben

Javasolt lenne a hazai katasztrófavédelem rendszerében nagyobb hangsúlyt fektetni olyan lehetőségek kihasználására, amelyeket a közösségi média és a rövid videók megosztására specializálódott platformok nyújtanak. Ezek a digitális felületek hatékonyan támogathatják az aktív lakosságfelkészítést, hiszen a figyelemfelkeltő és könnyen érthető tartalmak gyorsan eljuthatnak a célközönséghez. Amennyiben az adott tartalom terjedését segítő faktorokat is megfelelően kihasználjuk (például aktuális trendeknek megfelelő tartalom, hashtagek használata, aktív kommentelési lehetőség stb.), akkor a videó még szélesebb tartalomfogyasztó körökhöz is eljuthat. A különböző közösségimédia-platformok a célzott hirdetési eszközökkel lehetővé teszik, hogy a tartalomkészítők demográfiai, földrajzi és viselkedési adatok alapján szűkítsék és optimalizálják célközönségüket. A digitális oktatás, úgymint az e-learning, hatékony eszköz lehet a lakosság felkészítésében, mert lehetőséget teremt a rugalmas, interaktív és széles körben elérhető oktatási anyagok biztosítására. Olyan ingyenesen elérhető digitális platformot javasolt kialakítani, amely bármikor alkalmazható, visszanézhető oktatási anyagokat és feladatokat tartalmaz. A digitális tananyagok segíthetnek a lakosságnak elsajátítani a vészhelyzetkor alkalmazandó óvintézkedéseket és magatartási szabályokat, például áramszünetek, kibertámadások vagy természeti katasztrófák esetén. További előnyei az online biztosított képzéseknek, hogy gyorsan frissíthetők a tananyagok, és különböző társadalmi csoportokhoz igazíthatók, továbbá hozzájárulhatnak a lakosság ellenálló képességének növeléséhez. A VÉSZ mobilapplikáció is fontos szerepet kaphat a digitális oktatás eszköztárában, ennek az alkalmazásnak a kiegészítése különböző veszélyhelyzet-kezeléshez kapcsolódó információkkal hasznos lehet olyan katasztrófahelyzetek esetén, ahol a lakosság is érintett.

Javasolt megfontolni a lakossági felkészítési programok és oktatási anyagok kiegészítését az energiaellátásban, az infokommunikációs és vízkezelő rendszerekben, valamint a rendszerelemekben jelentkező zavarok kezelésének ismereteivel. Ezek a kritikus infrastruktúrák közvetlen hatással vannak a mindennapi életre, így a lakosság alapvető

[27] BM OKF [é. n.].

tájékozottsága hozzájárulhat egy esetleges incidens hatékonyabb kezeléséhez, a bizonytalanság és a pánikhelyzet kialakulási kockázatának a csökkentéséhez. A célzott és könnyen érthető oktatási anyagok segíthetnek a lakosság tudatos felkészítésében, erősítve ezzel a közösségi ellenálló képességet és az önálló problémamegoldás lehetőségét.

A helyi szintű lakossági tájékoztató kiadványok nem biztosítanak a lakosság számára megfelelő információkat a településen lévő alapvető szolgáltatást nyújtó szervezetekről, valamint azok átmeneti vagy tartós kiesése esetén az alkalmazandó óvintézkedésekről és követendő magatartási szabályokról, annak ellenére, hogy a lakosságfelkészítés fő célja, hogy megismertesse a polgárokkal a településükre és annak közvetlen környezetére jellemző kockázatokat, valamint a veszély vagy riasztás esetén alkalmazandó magatartási szabályokat.[28] Míg a veszélyes anyagokkal foglalkozó üzemek által veszélyeztetett területen élők rendszeres és kérés nélküli tájékoztatást kapnak az adott veszélyes üzem működési sajátosságából fakadó kockázatokról és azok hatásairól, addig a kritikus szervezetek nem képezik ezen kiadványok részét. A lakosság tájékoztatása során kiemelt figyelmet kell fordítani arra, hogy ne kerüljenek nyilvánosságra olyan nem publikus információk, amelyek a kritikus szervezetek rendszereinek működésével kapcsolatban potenciális támadási felületek lehetnek. A tájékoztatás és a felkészítés célja nem a kritikus infrastruktúra működésének ismertetése, hanem a zavarok és a kiesések következményeinek bemutatása, valamint a megfelelő reagálási formák elsajátítása. A lakosság ez irányú tájékoztató kiadványai, illetve oktatási anyagok összeállításakor javasolt lehet bevonni a település szempontjából releváns kritikus szervezetek ellenálló képességért felelős vezetőit.[29]

Összegzés

A nemzetbiztonság, a lakosságvédelem és a kritikusinfrastruktúra-védelem szoros összefüggése megköveteli az integrált stratégiai megközelítést. Az utóbbi években, különösen nemzetközi színtéren is bekövetkezett változások miatt a kritikus szervezetek ellen elkövetett célzott kiber- és fizikai támadások száma jelentősen megnőtt, amelyekből három esetet mutattak be a szerzők. A CER és NIS2 irányelvek előrelépést jelentenek uniós és hazai szinten is ezen üzemek védelmében, de a lakosság rezilienciájának kérdéskörére nem terjednek ki. A lakosság felkészítése az alapvető szolgáltatást nyújtó szervezetek elleni támadásokat követő hatásokra, valamint a dezinformációs kampányokkal szemben szintén egy fontos és időszerű lépés annak érdekében, hogy a kritikus szervezeteink mellett a magyar lakosság is teljes körű ellenálló képességgel rendelkezzen. A passzív és aktív lakosságtájékoztatás és felkészítés hagyományos eszközei mellett a 21. század által kínált platformok is rendelkezésre állnak, amelyek révén az információk gyorsan és hatékonyan eljuttathatók, a felkészítésbe pedig szélesebb társadalmi rétegek is bevonhatóvá válnak.

[28] Ambrusz 2017: 33–39.
[29] Bonnyai 2013: 58–73.

Felhasznált irodalom

Ambrusz, József (2017): An Overview of Disaster Preparedness Training in Hungary, With Special Regard to Public Administration Leaders. *Ecoterra – Journal of Environmental Research and Protection,* 14(1), 33–39.

Ambrusz József – Beke Zoltán (2023): A lakossági tájékoztatás feladatai. In Szabó Csaba (főszerk.): *A katasztrófavédelem lakosságfelkészítési feladatai*. Budapest: Pytheas Könyvmanufaktúra, 603–725.

Ambrusz József – Dobor József – Vásárhelyi Örs (2024): Létfontosságú rendszerek,-rendszerelemek rezilienciájának fejlesztési lehetőségei az Európai Unió direktíváinak tükrében. *Polgári Védelmi Szemle,* 16(különszám), 57–69. Online: https://mpvsz.hu/pv_szemlek/pvszemle2024/index.html

Antal, József – Hidvégi, Timót (2021): Test Environment for Special Protocols for Industry Computer Systems. In Abonyi-Tóth, Andor – Stoffová, Veronika – Zsakó, László (szerk.): *Proceedings of XXXIV. DidMatTech 2021 Conference New Methods and Technologies in Education, Research and Practice*. Budapest: Eötvös Loránd University (ELTE) Faculty of Informatics, 106–112.

BM OKF [é. n.]: *VÉSZ*. Online: https://www.katasztrofavedelem.hu/37/vesz

Bonnyai Tünde (2013): A lakosságfelkészítés lehetséges módszertana a létfontosságú rendszerek és létesítmények védelmének rendszerében. *Hadmérnök,* 8(3), 58–73. Online: http://hadmernok.hu/133_07_bonnyait.pdf

Brucker Balázs – Jóna László – Szemerédi Eszter (2024): Magyarország energiapiacának átfogó elemzése az Európai Unió változó prioritásainak tükrében. *Tér és Társadalom,* 38(1), 155–182. Online: https://doi.org/10.17649/TET.38.1.3516

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe [é. n.]: *Warn-App NINA*. Online: https://www.bbk.bund.de/DE/Warnung-Vorsorge/Warn-App-NINA/warn-app-nina_node.html

Chiscariu, Radu Emanuel (2021): DarkSide Ransomware Behavior and Techniques. *Keysight,* 2021. május 18. Online: https://www.keysight.com/blogs/en/tech/nwvs/2021/05/18/darkside-ransomware-behavior-and-techniques

CISA (2023a): Siemens Multiple Denial of Service Vulnerabilities in Industrial Products. *Cisa.gov,* 2023. január 13. Online: https://www.cisa.gov/news-events/ics-advisories/icsa-22-349-03

CISA (2023b): Understanding Ransomware Threat Actors: LockBit. *Cisa.gov,* 2023. június 14. Online: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a

Dobrády, Zoltán – Takács, Szilárd L. – Hidvégi, Timót (2023.). Use of AI in Operational Technology Networks and Packet-Based Attacks Detection. Varbanov, Petar S. – Wang, Bohong – Kapustenko, Petro: *Széchenyi István University Proceedings of Sustainable Development Research*. Győr: Universitas-Győr Nonprofit Kft., 62–68. Online: https://doi.org/10.62897/COS2023.1-1.62

Easterly, Jen (2023): The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years. *Cisa.gov,* 2023. május 7. Online: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

Európai Bizottság (2024): *Médiaműveltség.* Online: https://digital-strategy.ec.europa.eu/hu/policies/media-literacy

Európai Unió [é. n.]: *Éberség az interneten: fel tudja Ön ismerni az információmanipulációt?* Online: https://learning-corner.learning.europa.eu/learning-materials/how-spot-and-fight-disinformation_hu

European Commission (2022): *Strengthened Code of Practice on Disinformation*. Online: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation

European Union External Action (2021): Questions and Answers about the East StratCom Task Force. *Eeas.europa.eu,* 2021. október 27. Online: https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en#11234

Kátai-Urbán Lajos – Bleszity János – Vass Gyula (2025): A kritikus infrastruktúra védelmi felsőoktatási tapasztalatok a kritikus szervezetek ellenállóképességéről szóló szabályozás tükrében. *Polgári Védelmi Szemle,* 17(különszám), 220–236. Online: https://mpvsz.hu/pv_szemlek/pvszemle2025/index.html

Kerner, Sean Michael (2022): Colonial Pipeline Hack Explained: Everything You Need to Know. *TechTarget,* 2022. április 26. Online: https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

Kiss Álmos Péter (2019): A hibrid hadviselés természetrajza. *Honvédségi Szemle,* 147(4), 17–37. Online: https://honvedelem.hu/images/media/5f58be696dc30542944535.pdf

Marsi Tamás – Orosházi Dávid (2025): Új fejezet a kiberbiztonságban: a 2024. évi LXIX. törvény [aktuális]. *Kibertámadás! Podcast,* 94. epizód. Online: https://nki.gov.hu/podcast/

Microsoft Digital Defense Report 2024. Online: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf

Most „Harmful" Hacker Network LockBit Disrupted by Global Police Operation. *Euronews,* 2024. február 20. Online: https://www.euronews.com/2024/02/20/most-harmful-hacker-network-lockbit-disrupted-by-global-police-operation

National Institute of Standards and Technology (2020): *Security and Privacy Controls for Information Systems and Organizations.* Online: https://doi.org/10.6028/NIST.SP.800-53r5

SektorCERT (2023): *The Attack Against Danish Critical Infrastructure.* Online: https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf

Toulas, Bill (2023): Lockbit Ransomware Disrupts Emergency Care at German Hospitals. *BleepingComputer,* 2023. december 27. Online: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-disrupts-emergency-care-at-german-hospitals/

What is Shodan? [é. n.] Online: https://help.shodan.io/the-basics/what-is-shodan

Jogi források

2024. évi LXIX. törvény Magyarország kiberbiztonságáról
2024. évi LXXXIV. törvény a kritikus szervezetek ellenálló képességéről
418/2024 (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról
474/2024. (XII. 31.) Korm. rendelet a kritikus szervezetek ellenálló képességéről szóló törvény végrehajtásáról
1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről
Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve 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)
Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről