DOI: https://doi.org/10.12700/btsz.2025.7.1.SI.103

The importance of protecting critical infrastructure, and critical information infrastructure in domestic and international context

Kritikus infrastruktúrák és kritikus információs infrastruktúrák védelmének igénye hazai és nemzetközi környezetben

RUBINT Péter[1]

Abstract

The main goal of this paper is defining and comparing both domestic and international critical infrastructure, exploring their vulnerabilities and highlighting the importance of security. The widespread adoption of broadband internet technology and „cyber-physical" systems in industrial applications has created additional attack surfaces in critical systems and facilities, where often vulnerable computers are in charge of highly sensitive operations, such as water treatment, power plants, and everything else necessary for today's society to survive. These vital systems have become prime targets for cybercriminals and cyberwarfare, thus enabling threat actors to wreak physical havoc on critical infrastructure remotely. In this research the Stuxnet virus attack is examined to demonstrate the risks and consequences of cyberattacks on critical infrastructure, and emphasise the need for adequate security awareness of human operators.

Keywords

Critical infrastructure, information infrastructure, security awareness, information warfare, vital system

Absztrakt

A tanulmány fő célja a hazai és nemzetközi kritikus infrastruktúra fogalomrendszereinek definiálása, összehasonlítása, a kritikus rendszerek sebezhetőségeinek feltárása és a védelem fontosságának kihangsúlyozása. A szélessávú internet ipari területen való elterjedése, a kiberfizikai rendszerek alkalmazása új támadási felületeket hozott létre az eddig is érzékeny, létfontosságúnak tekintett létesítményekben. Számítógépek vezérlik az erőműveket, a vízellátást, és a társadalom működéséhez elengedhetetlen rendszereket, szolgáltatásokat, ezek azonban gyakran sérülékenyek, és kiemelt célpontnak számítanak a hackerek és kiberbűnözők számára. A kutatás két valós példán, a Stuxnet vírusos támadáson keresztül szemlélteti a kritikus infrastruktúrákat érő kibertámadások kockázatait és hatásait, illetve kiemeli a védelem fontosságát, ezen belül is az emberi biztonságtudatosság növelésének szükségességét.

Kulcsszavak

Kritikus infrastruktúra, információs infrastruktúra, biztonságtudatosság, információs hadviselés, létfontosságú rendszerelem

[1] peter.rubint@stud.uni-obuda.hu | ORCID: 0009-0009-4066-9781 | University Student, Óbuda University | Egyetemi hallgató, Óbudai Egyetem | 59. Tudományos Diákköri Konferencia II. helyezett, konzulens: Prof. Dr. Rajnai Zoltán

PROBLÉMAFELVETÉS, CÉLOK

Az információs társadalom teljes mértékben függ a kritikus infrastruktúrák, és kritikus információs infrastruktúrák zavartalan működésétől, ezért védelmük kiemelten fontos a nemzetek számára. A kritikus infrastruktúrák ellen intézett támadások, illetve természeti károk hatalmas problémát jelentenek, a szélessávú internet elterjedése, és ipari alkalmazása pedig utat nyitott a kritikus infrastruktúrák elleni információs támadásoknak is, amelyek legtöbbször informatikai eszközöket kihasználva igyekeznek kárt okozni az információs és hagyományos infrastruktúrákban egyaránt. Különösen jelentős veszélyforrás lehet a humán munkaerő biztonságtudatosságának hiánya is, mivel a biztonsági szabályzatok, szabályok be nem tartása megkönnyíti a támadók dolgát, és lehetőséget ad a behatolásra, károkozásra. A kritikus infrastruktúrák elleni támadások megnövekedett aránya igazolja, hogy jelentős veszélyekkel lehet számolni és nemzetközi példák is mutatják, hogy a kritikus infrastruktúrák elleni vírusbejuttatási támadások mekkora károkat okozhatnak.

A tanulmány célja a hazai kritikus infrastruktúra fogalmának, kategóriáinak, összetevőinek és fő ágazatainak vizsgálata, a leggyakoribb támadási módok megállapítása és hatásaik szemléltetése példákon keresztül, illetve a magyarországi kritikus infrastruktúrák védelmét ellátó szervezetek bemutatása.

KRITIKUS INFRASTRUKTÚRÁK MAGYARORSZÁGON

Hazánkban a létfontosságú rendszerekként ismert fogalomkategória 2001-től került előtérbe, az Egyesült Államokban az ikertornyok ellen elkövetett támadás után, azóta a világ számos országában felismerték annak jelentőségét, hogy bizonyos infrastruktúra elemeket kritikus infrastruktúraként kezeljenek, és kiemelt hangsúlyt fektessenek a védelmükre.

A létfontosságú rendszerek, infrastruktúrák ismertetése

Mitől kritikus egy infrastruktúra? Az infrastruktúra szó leggyakoribb értelmezésében eszközök, létesítmények, rendszerek és emberek összességét jelenti, ami egy adott ország, kormányzat, vagyis a társadalom működését támogatja. Kritikus infrastruktúrának tekinthető minden olyan létesítmény, eszköz, szervezet, információs hálózat, vagy szolgáltatás, amely alapfeltétele a társadalom működésének. Tekintve, hogy bármely kritikus infrastruktúrában keletkezett jelentős kár valószínűsíthetően a társadalmi rend és a közbiztonság felbomlásához, válsághelyzet vagy katasztrófa kialakulásához vezetne és hosszútávon akár az ország fennmaradását veszélyeztetné, minden kormányzat létfontosságú feladata ezek pontos meghatározása és védelme. [1] Magyarországon a kritikus infrastruktúrák ágazatait a 2012. évi CLXVI. Törvény határozza meg, a következőképpen:

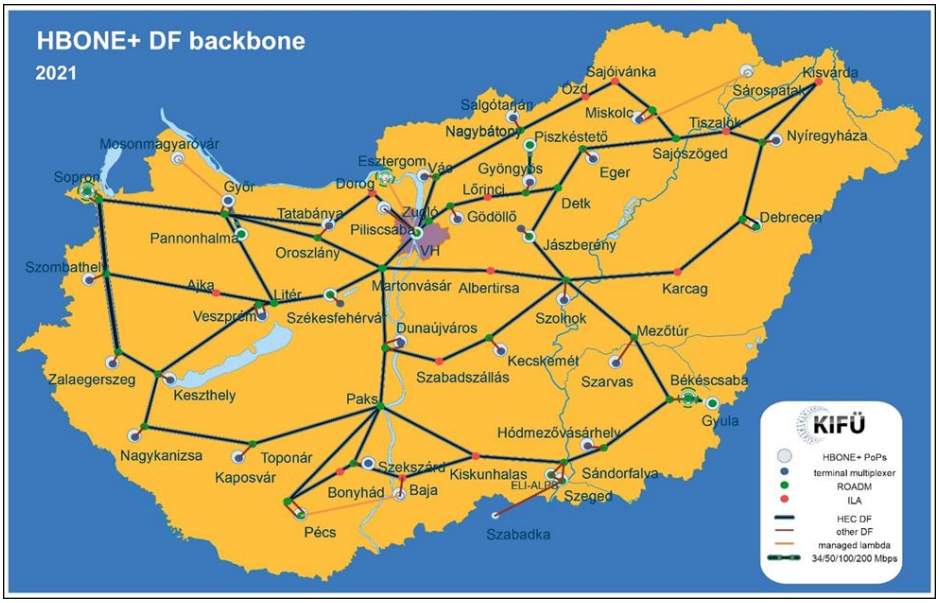
- energia,
- közlekedés,
- agrárgazdálkodás,
- egészségügy,
- társadalombiztosítás,
- pénzügy,
- infokommunikációs technológiák,
- víz,
- honvédelem és közbiztonság-védelem. [2]

A kritikus infrastruktúrák definícióját az Európai Unió Tanácsa a 2008/114/EK irányelvében így határozta meg: „a tagállamokban található azon eszközök, rendszerek vagy ezek részei, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, az egészségügyhöz, a biztonsághoz, az emberek gazdasági és szociális jólétéhez, valamint amelyek megzavarása vagy megsemmisítése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna valamely tagállamban" (Európai Tanács, 2008). Megállapíthatjuk, hogy a 2012. kritikus infrastruktúra törvény által értelmezett nemzeti létfontosságú rendszerelemek fogalma nagyrészt megegyezik a Tanács által közölttel, illetve közös pontot jelentenek a Tanács által európai kritikus infrastruktúrának (ECI), a hazai törvény szerint európai létfontosságú rendszerelemnek nevezett rendszerek is. Ide tartoznak az olyan rendszerek, amelyeknél üzemzavar vagy kiesés esetén legalább két EU tagállam is érintett. Tehát európai kritikus infrastruktúrának tekinthetőek például az országokat összekötő szállítási útvonalak, vagy a villamosenergia továbbító hálózatok. [2], [3]

A kritikus infrastruktúra és a kritikus információs infrastruktúra kapcsolata

Egy információs társadalom alapja, nevéből adódóan az információ. A mindennapi élethez, az ország gazdasági működéséhez folyamatosan szükséges új információk előállítása, közlése, feldolgozása és tárolása, az ezt lehetővé tévő rendszereket funkcionális információs infrastruktúráknak nevezzük. Emellett megkülönböztetünk egy másik fontos csoportot, a támogató információs infrastruktúrákat, amelyek az előbb említett funkcionális rendszerek üzemeléséhez szükséges szellemi és anyagi hátteret biztosítják, ezért ide leginkább kutatással és fejlesztéssel foglalkozó háttérinfrastruktúrák tartoznak. Általánosságban kritikus információs infrastruktúrának tekinthető minden olyan informatikai hálózat, ami a hagyományos infrastruktúra működtetéséhez szükséges, ilyenek például a gazdasági rendszert, egészségügyet, honvédelmet vagy energiaellátást biztosító szervezeteket kiszolgáló számítógép-hálózatok. [5]

Mindennapjainkat teljesen átszövi az Internet, szinte már elképzelni sem tudjuk nélküle az életünket. Tehát ha bármilyen nagyobb üzemzavar történik, azt a népesség jelentős hányada szinte azonnal érzékelné. A magyar lakosság számos Internet szolgáltató cégen keresztül érheti el a világhálót, kiépített országos hálózatok felhasználásával. Az Internet kapcsolatot biztosító cégek hálózatai a Budapest Internet Exchange (BIX) forgalomkicserélő központon keresztül vannak összekapcsolva, amelyet az Internet Szolgáltatók Tanácsa tart fennt. Ez a csomópont lehetővé teszi a hazai és külföldi szolgáltatók közötti hatékony adatátvitelt, és fontos része a hazai kommunikációs infrastruktúrának. [4]



1. Ábra: A HBONE+ gerinchálózat 2021-ben, forrás: hbone.hu [6]

A nyilvánosan elérhető szolgáltatások mellett a magyarországi Internet infrastruktúra fontos eleme az 1993-ban létrehozott HBONE, ami egy nagy sávszélességű, különcélú országos gerinchálózat. Elsősorban felsőoktatási intézményeket, könyvtárakat, kutatás-fejlesztési létesítményeket és egyéb közintézményeket kapcsol össze és lát el szélessávú Internet kapcsolattal. Több fejlődési fázis után 2010-ben zárult le a projekt, ekkora kiépült az egész országot összekötő, DWDM (Dense Wavelength Division Multiplexing) technológiát alkalmazó optikai hálózat, amely akár 100 gigabit per szekundum sebességű adatátvitelre is képes. [4]

Magyarország elektronikus közigazgatásának szempontjából kritikus információs infrastruktúra az Elektronikus Kormányzati Gerinchálózat és az EKG-t, illetve egyéb internetes kormányzati szolgáltatásokat, például az Ügyfélkaput magába foglaló Központi Elektronikus Szolgáltatási Rendszer. Az EKG köti össze és teszi elérhetővé a közigazgatási- és kormányzati adatbázisokat és informatikai rendszereket. Kiépítése a 2000-es években indult, elsődleges rendeltetése a kormányzati szervek közötti kommunikáció leegyszerűsítése, az elektronikus ügyvitelhez szükséges technológiai háttér megteremtése, és a kapcsolat megteremtése az Európai Unió TESTA hálózatához. Ezutóbbi lehetővé teszi a hatékony információcserét az uniós országok között, itt érhető el többek között a menedékkérők ujjlenyomatainak nyilvántartása, az export-import engedélyek kezelésének integrált rendszere, vagy a közúti balesetek adatbázisa. [4]

A mobilszolgáltatók közcélú hálózatokat üzemeltetnek, céljuk elsősorban a lakosság ellátása GSM, VoIP és adatátviteli szolgáltatásokkal az ország teljes területén. Ma már mindenkinek van mobiltelefonja, és napi szinten használja az internetet, így könnyen belátható, hogy a mobilhálózat létfontosságú a társadalom működése szempontjából, kiesése vagy üzemzavara pedig elégedetlenséget vagy pánikot okozhat. [4]

Különcélú hálózatnak nevezünk minden olyan adat- vagy távbeszélő hálózatot, ami szervezetek vagy vállalatok működtetéséhez szükséges. Ezeknek a hálózatoknak fontos szerepe van a létfontosságú rendszerek irányításában is, ilyen a korábban tárgyalt HBONE+, valamint az összes kritikus infrastruktúrát üzemeltető cég kommunikációját, koordinációját segítő információs infrastruktúra. Kitűnő példa a különcélú hálózatokra az OTR, azaz Országos Telemechanikai Rendszer, amely Magyarország földgázellátásáról szolgáltat információt az üzemeltetőnek. [4], [7]

Hazánk kritikus információs infrastruktúráját a lakosság, vállalatok és állami szervezetek által használt kommunikációs hálózatok alkotják. Legfontosabb sarokpontjai a nyilvános hozzáférésű telefonhálózat, a publikus Internet és a BIX, a hagyományos kritikus infrastruktúrát irányító különcélú hálózatok, mint az OTR, a közintézményeket összekapcsoló HBONE+ és a kormányzati szervezetek által használt EKG. A felsoroltak károsodása, kiesése vagy megsemmisülése mindenképpen negatívan befolyásolná az ország működését, ezért védelmük és karbantartásuk kiemelt figyelmet igényel.

KRITIKUS INFRASTRUKTÚRÁK ELLENI FENYEGETÉSEK, VÉDEKEZÉS

Ebben a fejezetben ismertetésre kerülnek a kritikus infrastruktúrákat fenyegető veszélyek, az ellenük irányuló támadások leggyakoribb módszerei, valamint az emberi tényező és a biztonságtudatosság szerepe a létfontosságú rendszerek védelmében. A kritikus infrastruktúrákat célzó kibertámadások hatásai és metodikája egy megtörtént eset feltárásával fejeződik be. A támadások után a védekezés, elsősorban a magyarországi kritikus rendszerek védelmét ellátó szervezetek felépítése és működése kerül bemutatásra.

A kritikus infrastruktúrákra ható veszélyforrások

A létfontosságú rendszerelemek védelménél rengeteg kockázati tényezőt kell számba venni, a természeti katasztrófák és balesetek mellett legfőképpen a szándékos károkozás jelenthet veszélyt a kritikus infrastruktúrákra. Kétféle támadási módszert különböztethetünk meg, ezek a fizikai és az információs támadások. [4]

Fizikai támadásnak tekinthető minden olyan cselekedet, ami a létfontosságú rendszerek üzemfolytonosságát vagy fennmaradását fizikai úton igyekszik befolyásolni. Ilyenek például a villamos alállomások, erőművek vagy adóközpontok ellen elkövetett robbantások vagy rongálások, illetve az üzemeltetéshez kulcsfontosságú személyzet kiiktatása is. [4]

A társadalom működéséhez elengedhetetlen információs infrastruktúrát fenyegető egyik legnagyobb veszély az információs hadviselés. Ez az új hadviselési forma a 21. század elején, az információs korszak beköszöntével kezdett elterjedni. Komplex, összehangolt információs támadásokat alkalmaz a fizikai, információs és tudati dimenziókban, amelyek kritikus infrastruktúrák ellen bevetve súlyos következményekkel járhatnak gazdasági és politikai területen egyaránt. Fokozza a kockázatot az a tény, hogy a létfontosságú rendszerek interdependenciában vannak, azaz egymás szolgáltatásaitól is függ a működésük, esetlegesen információs hálózatokon keresztül is kapcsolatban állnak. Emiatt egy gondosan kiválasztott célpont sikeres megtámadása dominó-effektust vagy láncreakciót indíthat el további rendszerek körében, ami megnöveli a támadás hatását és bonyolítja a kialakult krízishelyzetet [4]

Többféleképpen is csoportosíthatjuk az információs támadásokat, a dimenziókon kívül például az elkövetőik, céljaik, eredetük és szervezettségük szempontjából. Információs támadást hajthat végre egyedülálló személy, aktivista csoportok, terrorszervezetek vagy akár ellenséges országok katonai, hírszerző és félkatonai egységei is. Céljuk lehet információszerzés, fizikai vagy információs pusztítás, ellenséges nemzetek népességének, döntéshozóinak félrevezetése, társadalmi feszültség keltése, illetve újabb támadások előkészítése. [4]

Az információs fenyegetések eredetük szerint külső vagy belső eredetűként osztályozhatóak. Külső eredetű információs támadást az országon vagy szervezeten kívül álló személyek vagy csoportok követnek el, míg a belső eredetűeket a saját dolgozók tudatlansága, vagy rosszindulata válthatja ki. Szervezettségük szempontjából megkülönböztetünk magasan és alacsonyan szervezett beavatkozásokat. Magasan szervezett támadást az imént említett hírszerző, katonai, vagy terrorszervezetek követhetnek el, akiknek rendelkezésére áll megfelelő erőforrás és szaktudás egy összehangolt, több létesítményt is érintő művelet kivitelezésére. Ezzel szemben az alacsonyan szervezett támadások mögött általában egyének vagy kollektívák állnak, elsődleges céljuk a haszonszerzés és a magasan szervezett támadásokhoz képest kisebb fenyegetést jelentenek. [4]

Napjainkban az információs hadviselés elterjedt formája az úgynevezett cyberhadviselés. A hálózatba kapcsolt eszközök, legfőképpen az Internet alkotta cybertérben folyó műveletek komoly veszélyt jelentenek a kritikus információs infrastruktúrákra. Magasan szervezett, gyakran állami támogatással rendelkező hacker csoportok képesek a létfontosságú rendszereket kiszolgáló számítógépes hálózatok ellen olyan módon támadást indítani, hogy az adott szolgáltatás üzemfolytonosságát távolról, akár fizikai pusztítás nélkül befolyásolni tudják. A cyberhadviselésen belüli tevékenységek három fő csoportja az elektronikai felderítés, az elektronikai hadviselés és a hálózati műveletek. Az elektronikai hadviselés elsősorban katonai rendszerekre korlátozódik, célja az ellenség elektronikai berendezéseinek működésképtelenné tétele, és a saját rendszerek megóvása támadások ellen. [4]

Elektronikai felderítés keretében a támadók célja egy adott rendszerelem fizikai környezetének, hardver és szoftver összetételének, adatvagyonának, felhasználóinak, üzemeltetőinek és esetleges gyenge pontjainak feltérképezése. Az összegyűjtött információkat a cyberhadviselés két másik területén történő cselekmények előkészítésére használják a leggyakrabban, erre jó példa a következőkben tárgyalt Stuxnet vírusos támadás előkészítése. [4], [8]

Hackelés néven közismert hálózati műveleteket a névből adódóan hálózatba kapcsolt elektronikai eszközök ellen követnek el. Általában elektronikai vagy hálózati felderítés előzi meg, ami elősegíti, hogy támadók a célpont rendszerei ellen leghatásosabb eszközöket alkalmazhassák. Számos, jól dokumentált módszert különböztetünk meg, többek között:

- Számítógépes vírusok (malware)
- Féregprogramok (worm)
- Trójai vírusok (trojan)
- Hátsó ajtók (backdoor)
- Kémprogramok (spyware)
- Adathalászat (phishing)
- Szolgáltatásmegtagadással járó támadás (DoS vagy DDoS)

Nap mint nap jelennek meg újabb módszerek, a számítógépes és Internetes protokollok és eszközök végtelen lehetőségeit kiaknázó újabb támadási módszerek, ezért bármilyen rendszer, de legfőképpen a kritikus információs infrastruktúrák esetében fontos a kibervédelem folyamatos fejlesztése. [4]

Kibertámadások hatásai a Stuxnet vírus alapján

A Stuxnet vírus az első olyan ismert „kiberfegyver", amelyet kifejezetten kritikus infrastruktúra fizikai megrongálására hoztak létre, a 2000-es évek közepén. Célpontja az iráni Natanz mellett található fokozottan védett urándúsító üzem, egészen pontosan a gáz halmazállapotú urán dúsítását végző IR-1 és IR-2 gázcentrifugák és az ezeket felügyelő ipari irányítási rendszerek voltak. A kártékony programot feltehetően az Amerikai Egyesült Államok és Izrael hozta létre, azért, hogy Iránt megakadályozzák egy atomfegyver kifejlesztésében. [8], [9]

A kód kifejlesztését átfogó felderítés előzte meg, a támadók minden technikai adatot megszereztek az üzemi hálózatról és a dúsítást végző berendezésekről, egészen a konkrét modellekig és sorozatszámokig bezárólag. Ilyen részletes információk kiszivárgása szinte biztosan emberi mulasztás és a biztonságtudatosság hiánya miatt következhetett be. [9] Begyűjtött információikat felhasználva a Stuxnet tervezői úgy konfigurálták a kártevőt, hogy csak és kizárólag a dúsító eszközeire telepítve kezdjen pusztításba, minden más eszközt hagyjon figyelmen kívül. Ez a tulajdonság kiemelten fontos volt a lelepleződés elkerülése végett, ugyanis a vírus minden számítógépre átterjedt, amivel érintkezett, és a támadók nem kockáztathatták, hogy a fegyverük kárt tegyen olyan rendszerekben, amelyek nem szerepelnek a célpontok között, és ezáltal lelepleződjön. [9] A natanzi dúsító rendszerei fizikailag el voltak vágva a külvilágtól, így a vírust nem lehetett közvetlenül bejuttatni, azonban az ellátási láncot képező beszállítók hálózatai közel sem voltak ilyen biztonságosak, ezért fertőzött USB adathordozókon keresztül kezdődött el a Stuxnet terjedése. Ez a módszer minden bizonnyal sikerrel járt volna, és egészen 2024. elejéig a támadást vizsgáló elemzők között elfogadottnak tekintették, hogy a Stuxnet pendrive-okon keresztül jutott be a dúsítóba, azonban egy januári cikkben a holland Volkskrant című lap már Erik van Sabben holland származású mérnököt gyanusítja a program bejuttatásával, a holland titkosszolgálatok megbízásából, amerikai és izraeli támogatással. [9], [10]

Amint a Stuxnet érzékelte, hogy a megfelelő környezetbe került, megkereste a célpontként kijelölt programozható logikai vezérlőket, és megkezdte az ámokfutását. Beépült a centrifugák és az őket felügyelő rendszerek kommunikációjába, a fordulatszámokat és a nyomást manipulálva pedig elérte, hogy a centrifugák meghibásodjanak és elpazarolják a bennük lévő urán-hexafluorid gázt. Ebből a dúsítóban dolgozó személyzet a gyakori leállásokon és tönkrement centrifugákon kívül nem érzékelt mást, mert a vírus hamis információkkal megtévesztette a szenzorokat és a biztonsági rendszereket, ezért az üzemzavart jelző riasztók sosem szólaltak meg. Összességében ez a digitális szabotázsakció nagyjából két évvel vetette vissza Irán atomprogramját, rengeteg nyersanyagot és eszközt emésztett fel mielőtt felfedezték. [9]

Az agresszív terjedési mechanizmusának köszönhetően a vírus a kijelölt célponton kívül rengeteg másik rendszert is elért, többek között az összes, a Nemzeti Atomenergia Ügynökség közös hálózatára kapcsolt nukleáris létesítményt is. Elsőként a fehérorosz VirusBlokAda vállalat elemzői vettek mintát a Stuxnet kódjából, előzetes jelentésük publiká-

lása után pedig a Symantec és számos egyéb kiberbiztonsági cég megkezdte a saját vizsgálatait. Viszonylag hamar kiderült, hogy az újonnan felfedezett kártevő nem egy hobbista, vagy bűnözőcsoport fejéből pattant ki, hanem egy számottevő anyagi erőforrásokkal és átfogó szaktudással rendelkező, valószínűsíthetően állami támogatású csoport vagy csoportok összehangolt műveletének eszköze. Ezt a következtetést erősen alátámasztja, hogy a vírusban megtalálhatóak az iráni dúsító berendezéseit egyedileg azonosító technikai adatok és a terjesztéshez felhasznált, a Microsoft számára még ismeretlen sérülékenységek, amelyek kiaknázása önmagában is rengeteg időt és szakértelmet igénylő feladat. Számos oknyomozó riport és elemzés következtetései szerint a 2009. és 2010. között Irán nukleáris üzemanyag dúsító infrastruktúráját szabotáló kártékony program nagy valószínűséggel az Amerikai Egyesült Államok, Izrael és egyéb, velük szövetséges országok katonai, nemzetbiztonsági és hírszerző szolgálatainak együttműködésével jött létre. [8]

A Stuxnet kiváló példa arra, hogy állami támogatású szervezetek a kellő szaktudás, anyagi- és egyéb erőforrások, valamint a célpontról megfelelő mennyiségű technikai információ birtokában képesek távolról csapást mérni egy ország kritikus infrastruktúráját képező létesítményre, hálózataira akár teljesen észrevétlenül is. A Stuxnet felfedezése után több ország is megkezdte a saját kritikus infrastruktúra ellen bevethető vírusainak fejlesztését és bevetését, háborús és békés kontextusban egyaránt. [9], [8]

A létfontosságú rendszerek védelme

Az emberi személyzet viselkedése mindig fontos tényező a biztonságban, mert minden előírás, szabályzat vagy stratégia csak akkor hatékony, ha a szervezet tagjai pontosan és kivétel nélkül betartják őket. Kiemelten fontos átfogó védelmi szabályzatok kidolgozása a kritikus infrastruktúra rendszereket kezelő munkaerő részére, mert így megelőzhetőek vagy legalább lelassíthatóak az esetleges támadások. A dolgozók biztonságtudatosságát folyamatosan ellenőrizni kell, a hiányosságokat mielőbb felfedezni és megfelelő képzésekkel, tudatosítással fejleszteni, hogy mindig naprakész ismereteik legyenek az ellenük bevethető támadási technikákról.

Támadó csoportok már a műveleteik kezdeti fázisaiban is igyekeznek kihasználni a kezelő személyzet vagy vállalati dolgozók naivitását vagy figyelmetlenségét információszerzés céljából. Egy szofisztikált, kritikus infrastruktúra ellen intézett támadás sikeréhez a megcélzott rendszerekről minél részletesebb technikai adatokra van szükség, ezért ezeknek a kiszivárgását feltétlenül meg kell akadályozni. Tehát a működésre vonatkozó részleteket, például eszköz- és szoftvertípusokat, a hálózatok kialakítását és a szervezet belső kommunikációját érintő információk nem jogosult felek részére történő továbbítását feltétlen meg kell akadályozni.

Az információs támadások fontos lépése a vírus, vagy egyéb rosszindulatú program vagy eszköz bejuttatása a célpont épületébe vagy hálózatára. Ennek több, nem megfelelő szintű tudatosságot kiaknázó módja van, mint például fertőzött adathordozók terjesztése a létesítmény környékén, vagy dolgozók által frekventált helyszíneken. Gyakran előfordul, hogy valaki egy ismeretlentől kapott, vagy talált pendrive-ot a munkahelyi számítógépéhez csatlakoztat, és így utat enged a behatolóknak az eszközéről elérhető munkahelyi hálózatra.

A korábbi alfejezetekben tárgyalt kritikus infrastruktúra ellen elkövetett támadások szoftver sérülékenységek mellett a személyzet hiányos biztonságtudatosságát és nem megfelelően betartott biztonsági szabályokat kihasználva valósulhatnak meg, ezért mindenkép-

pen szükséges az ilyen rendszereket üzemeltető dolgozókat felkészíteni a pszichológiai manipuláció, átverés és egyéb „social engineering" technikák felismerésére, ezenfelül pedig fontos még a biztonsági szabályzatok betartása, rendszeres frissítése is. [21]

Magyarországon a kritikus infrastruktúraelemek védelmének első lépése a nemzeti, vagy európai létfontosságú rendszerelemmé nyilvánítás folyamata. A 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről, röviden Lrtv. 1. mellékletében felsorolt ágazatokba tartozó szolgáltatást nyújtó üzemeltetőknek a törvény értelmében kötelező egy azonosítási jelentést készítenie. Ez a jelentés vizsgálja az adott szolgáltatás folytonosságát veszélyeztető kockázatokat, és a kiesés esetén teljesülő ágazati és horizontális kritériumokat, valamint javaslatot tesz a létfontosságú rendszerelemmé való kijelölésére. [2] Ágazati kritériumnak számítanak azok a szempontok, műszaki és funkcionális tulajdonságok, amelyek egy létfontosságú rendszer kiesése által kiváltott hatásra vonatkoznak, például az energia ágazat egyik ágazati kritériuma a 374/2020. (VII. 30.) Korm. Rendelet alapján a következő: „A villamos energia rendszerirányítás tekintetében nemzeti létfontosságú rendszerelemként kell azonosítani azt a rendszerelemet, amelynek kiesése esetén az ellátásbiztonság nem tartható fenn, és amely 30 percen belül nem helyettesíthető." [15] Horizontális kritériumként azokat a kiesés esetén bekövetkező szempontokat vizsgálják, amelyek az emberiélet-veszteségre, gazdasági, társadalmi, egészségügyi és környezeti hatásokra vonatkoznak. A 65/2013. (III. 8.) Korm. Rendelet 1. melléklete tartalmazza a létfontosságú rendszerelemmé történő kijelölés horizontális kritériumait, az emberélet-veszteségekről szóló így hangzik: „24 óra leforgása alatt az áldozatok száma a 20 főt meghaladja, vagy a súlyos sérültek száma legalább 75 fő, vagy 72 óra leforgása alatt az áldozatok száma a 40 főt meghaladja, vagy a súlyos sérültek száma legalább 150 fő." [16] Az elkészült azonosítási jelentést a szolgáltató köteles benyújtani az ágazati ellenőrző hatóságnak, amely megkezdi a kijelölési eljárás lefolytatását. Minden ágazat számára külön kormányrendelet azonosítja az ágazati kijelölő hatóság szerepében eljáró szervezetet, például a villamosenergia- és földgázrendszer esetében a Magyar Energetikai és Közmű-szabályozási Hivatal. [15] Az eljárás keretében szakhatóság bevonásával megvizsgálják a jelentésben azonosított ágazati és horizontális kritériumok teljesülését. Amennyiben a vizsgálat megállapítja, hogy legalább egy ágazati és egy horizontális kritérium teljesül kiesés esetén, az adott rendszerelemet kijelölik létfontosságúnak, nyilvántartásba kerül, az üzemeltetőt pedig felveszik az alapvető szolgáltatásokat nyújtó szereplők jegyzékébe. Ezt követően a működtető köteles egy üzemeltetési biztonsági tervet készíteni, illetve biztonsági összekötő személyt alkalmazni. Az elkészített tervnek tartalmaznia kell az üzemeltető adatait, a rendszerelem és környezetének bemutatását, a kockázatok elemzését, a rendkívüli esemény bekövetkezésekor alkalmazható védelmi eszközrendszer leírását és az üzemfolytonossághoz elengedhetetlen szolgáltatásokat is. Szükséges egy biztonsági összekötő személy alkalmazása is, aki a létfontosságú rendszerelem és az ágazati kijelölő hatóság közötti kapcsolattartásért felelős. A rendszerelem biztonságát és az előírások betartását 5 évente helyszíni ellenőrzés keretében tesztelik, a mulasztások pénzbírságot vonnak maguk után. [2], [16]

A Belügyminisztérium Országos Katasztrófavédelmi Főigazgatósága (BM OKF) fontos szerepeket tölt be a kritikus infrastruktúrák védelmében. Félévente felmérést készít az ágazatok állapotáról, amit az ágazati kijelölő hatóságok részére továbbít. Szakhatóság-

ként részt vesz a korábban tárgyalt azonosítási jelentések horizontális kritériumainak vizsgálatában, véleménynyilvánító szervezetek, például a Nemzeti Adó- és Vámhivatal, vagy az Alkotmányvédelmi Hivatal segítségével. Nyilvántartja az üzemeltetőkre vonatkozó adatokat, helyszíni ellenőrzéseket és komplex biztonsági gyakorlatokat szervez a létfontosságú rendszerként kijelölt létesítményekben. [17]

A kritikus információs infrastruktúra rendszereket elsősorban információs támadások veszélyeztetik. Az ilyen támadások kivédésére, észlelésére és hatékony elhárítására Magyarországon több CERT, azaz Computer Emergency Response Team működik. A CERT-ek szakértői csoportok, akik a hatáskörükbe tartozó szervezetek informatikai rendszereiben bekövetkező incidensek elhárításával és az okozott károk helyreállításával foglalkoznak. A HunCERT a Számítástechnikai és Automatizálási Kutatóintézeten (SZTAKI) belül működik, elsődleges feladata az Internetszolgáltatók Tanácsába tartozó vállalatoknál előforduló biztonsági incidensek megelőzésében, elemzésében és kezelésében való segítségnyújtás. Emellett a magyar internetes közösség körében tudatosítást végez, és naprakész információkat oszt meg a kiberbiztonságról. [18]

Hazánkban a kormányzati hálózatok és kritikus információs infrastruktúra védelmének központi szervezete a 2015-ben létrehozott Nemzeti Kibervédelmi Intézet (NKI). A Nemzetbiztonsági Szakszolgálat alá tartozó Intézet a kormányzati informatikai rendszerek teljes életciklusát felügyeli. Az NKI-n belül működik a GovCERT, vagyis a kormányzati eseménykezelő központ. Legfőbb feladata a 2013. évi L. törvényben meghatározott szervezetek informatikai rendszereinek védelme, és a biztonsági incidensek kezelése. Az érintett szervezetek közé tartozik többek között az Országgyűlési Hivatal, az Alkotmánybíróság, az Országos Bírósági Hivatal, az Állami Számvevőszék és a Magyar Nemzeti Bank, valamint a Magyar Honvédség, és nem utolsósorban a létfontosságúként kijelölt rendszerelemek működtetői. Védelmi tevékenysége elsősorban a szoftversérülékenységek felfedezésére, összegyűjtésére és az érintettek tájékoztatására terjed ki. Emellett a bekövetkezett információbiztonsági incidensek kivizsgálását és megfelelő kezelését felügyeli. [18], [19] Szintén az NKI része a Nemzeti Elektronikus Információbiztonsági Hivatal, röviden NEIH. Feladata a 2013.-as információbiztonsági törvény és egyéb jogszabályok által előírt információbiztonsági követelményeknek való megfelelés ellenőrzése, és az ehhez szükséges informatikai fejlesztések felügyelete az érintett szervezeteknél. Éves ellenőrzési terv szerint fizikai, logikai és adminisztratív ellenőrzést végez, mulasztások esetén jogosult bírságot kiszabni, vagy információbiztonsági felügyelőt kirendelni. [18] A Nemzeti Kibervédelmi Intézet Biztonságirányítási és Sérülékenységvizsgálati Osztályán belül sérülékenységvizsgálattal és informatikai biztonsági tanácsadással foglalkozik. Sebezhetőségi vizsgálataik kereteiben az Intézet munkatársai szoftveres sérülékenységeket, külső és belső fenyegetéseket, illetve a dolgozók biztonságtudatosságának hiányosságait kutatják fel, ezekről az érintett szerv részére jelentést készítenek. Szakmai segítséget nyújt a NEIH, és egyéb állami vagy önkormányzati szervezet részére, illetve információbiztonsági irányítási rendszereket (IBIR) üzemeltet. [18]

A kritikus infrastruktúráknak kijelölt létesítmények informatikai hálózatbiztonságát a 2013-ban, a BM Országos Katasztrófavédelmi Főigazgatóságon belül létrehozott Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja (LRLIBEK) felügyeli. Eseménykezelő központként reagál a létfontosságú informatikai

rendszereket érő támadásokra, elhárításában segítséget nyújt az üzemeltetőknek. Az incidensek elkerülése végett tájékoztatást nyújt az aktuális fenyegetésekről, valamint információbiztonsági és kibervédelmi gyakorlatokat szervez. Az Országos Katasztrófavédelmi Főigazgatóság után 2019. óta a Nemzeti Kibervédelmi Intézet felügyelete alá tartozik. [18], [20]

Összefoglalva, Magyarországon a kritikus infrastruktúrák és kritikus információs infrastruktúrák védelmét számos egymással szorosan együttműködő szervezet látja el. A létfontosságúnak kijelölt rendszerelemek fizikai biztonsága és üzemfolytonossága elsősorban az üzemeltetők felelőssége, az ágazati kijelölő hatóságok és az Országos Katasztrófavédelmi Főigazgatóság felügyelete mellett. Információs támadások elleni védelmet nyújt a Nemzeti Kibervédelmi Intézet, amely az összes kormányzati és kritikus infrastruktúrát kiszolgáló hálózat biztonságát és a törvényben előírt információbiztonsági követelményeknek való megfelelést felügyeli, valamint sérülékenységi vizsgálatokkal és tanácsadással igyekszik megelőzni az incidenseket.

ÖSSZEFOGLALÁS

A számítógépek és informatikai rendszerek széleskörű adoptációja új korszakot nyitott az emberiség történelmében, a magasszintű technológiai fejlettség eredményeképpen beléptünk az információs korba, a modern ember immár egy információs társadalom tagja. A nap minden percében hatalmas mennyiségű információ előállítása, továbbítása és feldolgozása zajlik a világ minden táján, ami soha nem látott mértékű fejlődést és a tudás széleskörű hozzáférését biztosítja mindenki számára. Ez az új világrend azonban hatalmas mértékben függ bizonyos alapvető szolgáltatásoktól, melyeknek akár csak rövid ideig tartó kiesése katasztrofális gazdasági és politikai következményekkel járhat.

A modern élethez elengedhetetlen rendszereket kritikus infrastruktúráknak nevezzük, hiszen ezek biztosítják alapvető szükségleteink ellátását. A villamosenergia, ivóvíz, egészségügy, élelmiszeripar, fűtés, szállítás és kommunikáció mind életbevágóan fontos, nélkülük a szervezett rend felbomlása, válsághelyzetek és emberi-élet veszteségek szinte biztosra vehetőek. Fenntartásukhoz egyre inkább támaszkodunk számítógép-hálózatokra, informatikai rendszerekre. Ezek az eszközök, az Internettel és minden, információ továbbításra és kezelésre alkalmazott megoldással együtt alkotják a kritikus információs infrastruktúrákat. Segítségükkel hatékonyabban működnek létfontosságú rendszereink, azonban kitettséget is jelentenek a hadviselés legújabb fajtája, az információs hadviselés ellen. A nem megfelelő védelemmel ellátott informatikai hálózatok gyengeségeit, illetve az üzemeltető személyzet biztonságtudatosságának hiányosságait rendszeresen használják ki rosszindulatú csoportok. Motivációik, hátterük és módszereik széles spektrumon mozognak, egy azonban közös bennük: képesek létfontosságú infrastruktúra rendszerek üzemfolytonosságát információs támadásokkal olyan módon befolyásolni, hogy az alapvető szolgáltatásokban elakadást, üzemzavart okozzanak.

A Stuxnet vírus felfedezése egyben a kiberhadviselés kezdetét is jelentette. Célkeresztbe kerültek a kritikus információs infrastruktúra rendszerek és az elkövetkező években számos hasonló támadást követtek és követnek el továbbra is, ezért a védekezés minden nemzet számára létfontosságúvá vált. Magyarországon a Nemzeti Kibervédelmi Intézet és a Katasztrófavédelmi Főigazgatóság számos más szervezettel éjjel-nappal az alapvető szolgáltatások megfelelő védelmén dolgozik, a fizikai és kibertérben egyaránt.

FELHASZNÁLT IRODALOM

[1] „A kritikus infrastruktúra védelmi fogalmi rendszere, hazai és nemzetközi szabályozása”. Katasztrófavédelmi Tudományos Tanács. Elérés: 2024. március 19. [Online]. Elérhető: https://www.vedelem.hu/letoltes/anyagok/382-a-kritikus-infrastruktura-vedelem-fogalmi-rendszere-hazai-es-nemzetkozi-szabalyozasa.pdf

[2] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. 2012.

[3] „A TANÁCS 2008/114/EK IRÁNYELVE (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről”, Az Európai Unió Hivatalos Lapja, köt. L 345, sz. 51., o. 75–82, dec. 2008.

[4] L. Kovács és Z. Haig, „Kritikus infrastruktúrák és kritikus információs infrastruktúrák”. Katonai Üzemeltető Intézet, 2012.

[5] Z. Haig, L. Kovács, és L. Muha, „A kritikus információs infrastruktúrák meghatározásának módszertana”. ENO Advisory Kft., 2009.

[6] KIFÜ, HBONE+ DF Backbone. 2021. Elérés: 2024. április 11. [Online]. Elérhető: https://hbone.hu/

[7] FGSZ, „FGSZ FÖLDGÁZSZÁLLÍTÓ ZÁRTKÖRŰEN MŰKÖDŐ RÉSZVÉNYTÁRSASÁG ÜZLETSZABÁLYZATA ORSZÁGOS TELEMECHANIKAI RENDSZER 1.2 MELLÉKLET”. FGSZ, 2024. január 1. Elérés: 2024. április 12. [Online]. Elérhető: https://fgsz.hu/documents/show/12-melleklet-orszagos-telemechanikai-rendszer-20240101-tol

[8] M. Kamiński, „Operation “Olympic Games.”Cyber-sabotage as a tool of Americanintelligence aimed at counteractingthe development of Iran’s nuclear programme”, Secur. Def. Q., köt. 29, sz. 2, o. 63–71, jún. 2020, doi: 10.35467/sdq/121974.

[9] A. Cserháti, „A Stuxnet vírus és az iráni atomprogram”, Nukleon, köt. IV., sz. 85, márc. 2011, Elérés: 2024. március 17. [Online]. Elérhető: http://nuklearis.hu/sites/default/files/nukleon/Nukleon_4_1_85_Cserhati_.pdf

[10] „Dutch man sabotaged Iranian nuclear program without Dutch government’s knowledge: report”, NL Times, 2024. január 8. Elérés: 2024. április 10. [Online]. Elérhető: https://nltimes.nl/2024/01/08/dutch-man-sabotaged-iranian-nuclear-program-without-dutch-governments-knowledge-report

[11] A. Bowen S., „Russian Military Intelligence: Background and Issues for Congress”. Congressional Research Service, 2021. november 15. Elérés: 2024. március 30. [Online]. Elérhető: https://sgp.fas.org/crs/intel/R46616.pdf

[12] N. Beach-Westmoreland, J. Styczynski, és S. Stables, „When the lights went out - A comprehensive review of the 2015 attacks on Ukrainian critical infrastructure”. Booz Allen Hamilton, 2016. november. Elérés: 2024. március 30. [Online]. Elérhető: https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf

[13] A. Greenberg, Sandworm: a new era of cyberwar and the hunt for the Kremlin’s most dangerous hackers, First edition. New York: Doubleday, 2019.

[14] A. Cherepanov, „WIN32/INDUSTROYER A new threat for industrial control systems”. ESET, 2017. június 12. Elérés: 2024. március 30. [Online]. Elérhető: https://web-assets.esetstatic.com/wls/2017/06/Win32_Industroyer.pdf

[15] 374/2020. (VII. 30.) Korm. rendelet az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. 2020.
[16] 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról. 2013.
[17] Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság, „Kritikus infrastruktúrák védelmével összefüggő hatósági feladatok, jogszabályok". Elérés: 2024. április 13. [Online]. Elérhető: https://www.katasztrofavedelem.hu/109/kritikus-infrastrukturak-vedelmevel-osszefuggo-hatosagi-feladatok-jogszabalyok
[18] L. Dornfeld, R. Gyaraki, T. Kiss, A. Kovács Zoltán, Z. Nagy, és B. Simon, Kibervédelem a bűnügyi tudományokban. in Sub Lege Libertas. Ludovika Egyetemi Kiadó, 2020.
[19] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról. 2013.
[20] B. Dr. Bognár, „Tájékoztató az LRL IBEK feladatrendszeréről", előadás Energetikai Szakmai Nap, 2014. március 10. Elérés: 2024. április 15. [Online]. Elérhető: http://www.bte.hu/files/20140310_BOGNR_BALZS.pdf
[21] I. Jagodics és C. Kollár, „21. századi social engineering támadások, védekezés és szervezeti hatások Európában", BSZ, köt. 71, sz. 1, o. 111–126, jan. 2023, doi: 10.38146/BSZ.2023.1.6.