DOI: 10.38146/BSZ-AJIA.2025.v73.SI1.pp65-81

Az operatív technológia kiberbiztonsága kritikus infrastruktúrákban

Cybersecurity of Operational Technology in Critical Infrastructure

Hunorfi Péter
doktorandusz
Óbudai Egyetem,
Biztonságtudományi Doktori Iskola
hunorfi.peter@phd.uni-obuda.hu

Farkas Tibor
Dr. habil., egyetemi docens, oktatási dékánhelyettes
Óbudai Egyetem,
Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar
farkas.tibor@bgk.uni-obuda.hu

Absztrakt

Cél: A tanulmány célja, hogy bemutassa a kritikus infrastruktúrák[1] és az operatív technológia (OT)[2] kapcsolatát, valamint feltárja az IT-[3] és OT-rendszerek integrációjából adódó kiberbiztonsági kihívásokat. A kutatás központi kérdése: Melyek a legfőbb sebezhetőségek, amelyek az OT- és IT-rendszerek összekapcsolása révén merülnek fel a kritikus infrastruktúrákban, és milyen védelmi stratégiák csökkenthetik ezek kockázatait?

Módszertan: A kutatás interdiszciplináris megközelítést alkalmaz, amely ötvözi az elméleti-logikai vizsgálatokat, szakirodalmi áttekintést, esettanulmányok elemzését és gyakorlati példák feldolgozását. A kutatás során a következő hipotéziseket vizsgáltuk.

H1: Az IT- és OT-rendszerek konvergenciája fokozott támadási felületet eredményez, mivel az IT-hálózatokon keresztül az OT-rendszerek is sérülékennyé válhatnak.

1 *„Magyarországon 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."* 234/2011. (XI. 10.) Korm. Rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról.

2 OT az operational technology, magyarul operatív technológia angol rövidítése.

3 IT az information technology, magyarul információs technológia angol rövidítése.

Magyar nyelvű utánközlés. Jelen cikk angol változata megjelent a Belügyi Szemle 2025. évi SI1. számában.
DOI link: https://doi.org/10.38146/BSZ-AJIA.2025.v73.SI1.pp183-197

H2: A kritikus infrastruktúrákban alkalmazott védelmi mechanizmusok nem minden esetben felelnek meg az OT sajátos biztonsági követelményeinek, ami növeli a rendszerek sérülékenységét.

H3: A megfelelő szegmentációs stratégiák, valamint az IT- és OT-hálózatok közötti ellenőrzött kommunikációs csatornák kialakítása csökkentheti a kibertámadások kockázatát.

A kutatás összehasonlító elemzéseket is tartalmaz, amely során az ipari és kritikus infrastruktúrákban alkalmazott védelmi intézkedéseket vizsgáljuk. Az OT-rendszerek kiberbiztonsági kihívásainak jobb megértése érdekében iparági jelentések és esettanulmányok elemzése is történt.

Megállapítások: A kritikus infrastruktúrák operatív technológiai rendszereinek védelme kiemelten fontos a társadalmi és gazdasági stabilitás fenntartásának érdekében. Az OT-rendszerek digitalizációja és az IT-rendszerekkel való egyre szorosabb integrációja új kiberbiztonsági kihívásokat teremt, amelyek kezelése komplex és többszintű megközelítést igényel. A tanulmány rávilágít arra, hogy az IT- és OT-rendszerek megfelelő szegmentációja és biztonságos összekapcsolása kulcsfontosságú a kiberfenyegetések hatékony kezeléséhez.

Érték: A kutatás átfogó képet nyújt az operatív technológia kiberbiztonsági kihívásairól, különös tekintettel a kritikus infrastruktúrákra. Tudományos és gyakorlati szempontból egyaránt hasznos útmutatást kínál a védekezési stratégiák fejlesztéséhez, segítve ezzel az IT- és OT-rendszerek biztonságos integrációját.

Kulcsszavak: kritikus infrastruktúrák, operatív technológia, kibervédelem, hacker támadás

Abstract

Aim: The aim of this study is to present the relationship between critical infrastructures and operational technology (OT) and to explore the cybersecurity challenges arising from the integration of IT and OT systems. The central research question is: What are the main vulnerabilities that emerge in critical infrastructures due to the interconnection of OT and IT systems, and what defense strategies can mitigate these risks?

Methodology: The research adopts an interdisciplinary approach that combines theoretical-logical analysis, literature review, case study analysis, and the examination of practical examples. The following hypotheses were investigated:

H1: The convergence of IT and OT systems results in an increased attack surface, as OT systems become vulnerable through IT networks.

H2: The security mechanisms applied in critical infrastructures do not always meet the specific security requirements of OT, increasing system vulnerabilities.

H3: Proper segmentation strategies and the establishment of controlled communication channels between IT and OT networks can reduce the risk of cyberattacks.

The research also includes comparative analyses examining security measures applied in industrial and critical infrastructure settings. To gain a deeper understanding of the cybersecurity challenges of OT systems, industry reports and case studies were also analysed.

Findings: The protection of operational technology systems in critical infrastructures is crucial for maintaining social and economic stability. The digitalization of OT systems and their increasing integration with IT systems create new cybersecurity challenges that require a complex and multi-layered approach to address. The study highlights that proper segmentation and secure interconnection of IT and OT systems are key to effectively managing cyber threats.

Value: This research provides a comprehensive overview of the cybersecurity challenges associated with operational technology, with a particular focus on critical infrastructures. It offers valuable guidance for developing defense strategies from both scientific and practical perspectives, supporting the secure integration of IT and OT systems.

Keywords: Critical Infrastructure, Operational Technology, Cyber Defense, Hacker Attack

Bevezetés

A modern társadalmak és gazdaságok működésének alapvető fundamentumai a kritikus infrastruktúrák, melyek alapvető szolgáltatásokat biztosítanak, például többek között az energiaellátás, pénzügyi rendszerek, vízellátás, kommunikáció, közlekedés, egészségügy és közbiztonság zavartalan működését (Haig et al., 2009). Ezek az infrastruktúrák azért kiemelt jelentőségűek, mivel megszűnésük vagy bizonyos szintű működési zavaraik súlyos következményekkel járhatnak az emberek és nemzetek életében.

A kritikus infrastruktúrák különösen sebezhetőek a természeti katasztrófák, kibertámadások és más egyéb veszélyforrások miatt, ezért a nemzeti és gazdasági szereplőknek kiemelt figyelmet kell fordítaniuk azok megvédésére és fenntarthatóságára (Muha, 2007). Például az energiaellátás megőrzésének érdekében nagyon fontos a modern technológiák biztonságos alkalmazása, a kockázatelemzés, valamint a megelőző biztonsági intézkedések kidolgozása és betartatása (Répás & Dalicsek, 2015). A decentralizált energiatermelés,

a megújuló energiaforrások használata, az energiatároló technológiák fejlesztése, vagy az intelligens hálózatok (smart grids) (Vijayapriya & Kothari, 2011) nemcsak a fenntarthatóságot erősítik, hanem hozzájárulnak a rendszerek biztonsági szempontból történő ellenállóképességének növeléséhez is. A kritikus infrastruktúrák védelme terén elengedhetetlen a törvényi szabályozás (2024. évi LXXXIV. törvény a kritikus szervezetek ellenálló képességéről), a szabványok kialakítása (Hunorfi, 2024), auditrendszerek kialakítása, valamint a nemzetközi együttműködés, mivel a globális fenyegetések, például a klímaváltozás és a kiberbiztonsági támadások hatásai országhatárokon átívelő problémákat és kihívásokat jelentenek.

Az energiaellátás és más kritikus infrastruktúrák folyamatos működésének biztosítása nemcsak technikai és gazdasági, hanem társadalmi és politikai feladat is. Az érintett felek – kormányzatok, vállalatok, tudományos intézmények és civil szervezetek – közötti szoros együttműködés elengedhetetlen a hatékony védelem érdekében. A kritikus infrastruktúrák hosszú távú biztonságának kialakításához szükséges a stratégiai tervezés, amely figyelembe veszi a jövőbeli kihívásokat és a technológiai fejlődést. A mesterséges intelligencia és az adatvezérelt (big data) elemzés alkalmazása lehetővé teszi a rendszerek jobb monitorozását a kibertérben[4] és a potenciális problémák előrejelzését, így minimalizálva a váratlan meghibásodások kockázatát.

Fontos hangsúlyozni, hogy a kritikus infrastruktúrák védelme nem csupán a fizikai rendszerek megerősítését jelenti, hanem a kibertérben történő támadások kivédésére is ki kell terjednie. Az egyre komplexebb digitális hálózatok sérülékenysége miatt elengedhetetlen a kiberbiztonsági rendszerek folyamatos fejlesztése és a szakértők képzése. Az információmegosztás és a valós idejű kommunikáció az érintett szervezetek között meghatározó jelentőségű lehet egy válsághelyzet gyors és hatékony kezelésében.

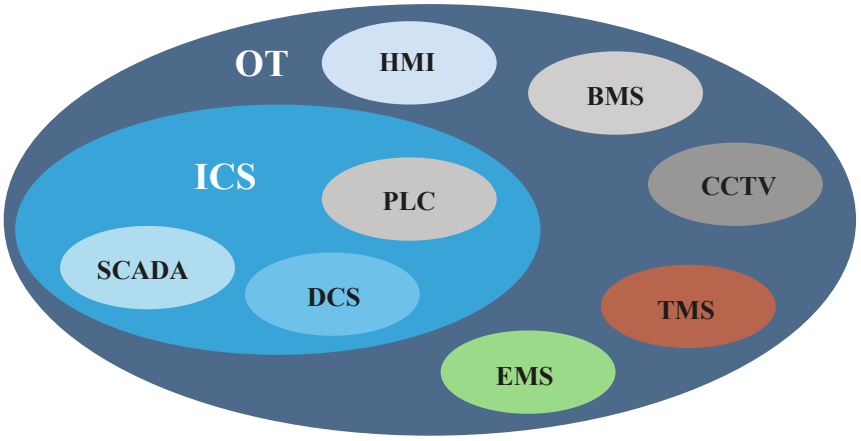
Összességében jól látható, hogy a kritikus infrastruktúrák biztonságának megőrzése a nemzetek stabilitása és fejlődése szempontjából alapvető fontosságú. Ezért a társadalmi, gazdasági és politikai szinteken egyaránt prioritást kell élveznie, hogy a rendszerek ellenállóképessége és rugalmassága a lehető legmagasabb szintre emelkedjen, biztosítva ezzel a jelen és a jövő társadalmának jólétét. A közlemény célja tehát egyrészt az OT-kiberbiztonság és a kritikus infrastruktúrák kapcsolatának átfogó feltárása, másrészt a gyakorlati védekezési stratégiákra vonatkozó javaslatok megfogalmazása.

4 *„A kibertér a hálózatba kötött számítógépek által létrehozott virtuális valóság világa, annak összes objektumával egyetemben."* 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.

Mi is az operatív technológia?

A kritikus infrastruktúrák műszaki szempontból az operatív technológia alapjaira épülnek, mivel ezek a rendszerek felelnek a működésük irányításáért és automatizálásáért. Az operatív technológia olyan hardverek és szoftverek összessége, amelyek közvetlenül irányítják, monitorozzák és kezelik a fizikai eszközöket és folyamatokat. Míg az IT elsősorban adatok kezelésével foglalkozik, az OT a fizikai világra gyakorol közvetlen hatást. Az operatív technológia (1. számú ábra) magában foglalja többek között az ipari vezérlőrendszereket, például a felügyeleti vezérlő- és adatgyűjtő rendszereket, a programozható logikai vezérlőket és az elosztott vezérlőrendszereket. Ezek a technológiák alapvető fontosságúak a különböző ágazatok, például az energia, a vízellátás, a közlekedés és a gyártás zavartalan működéséhez.

1. számú ábra
OT-rendszerek összefoglalása



ICS: Industrial Control System – ipari irányító rendszerek.
SCADA: Supervisory Control and Data Acquisition – folyamatirányító és adatgyűjtő rendszer.
DCS: Distributed Control System – elosztott vezérlő rendszer.
PLC: Programmable Logic Controller – programozható logikai vezérlő.
EMS: Energy Management System – energia menedzsment rendszer.
TMS: Transportation Management System – szállítmányozási menedzsment rendszer.
BMS: Building Management System – épület felügyeleti rendszer.
CCTV: Closed-Circuit Television – zárt láncú kamera rendszer.
HMI: Human Machine Interface – ember–gép kapcsolati felület.

Forrás. A szerzők saját szerkesztése.

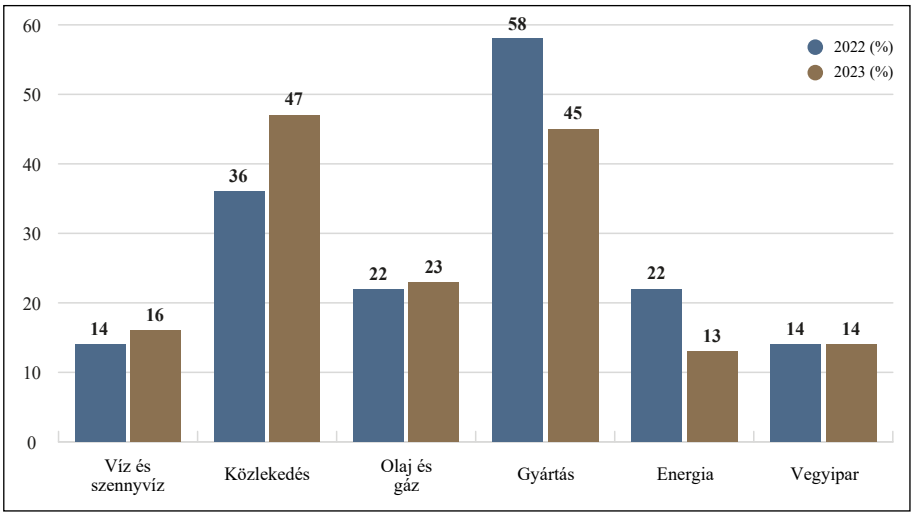
Az operatív technológia lehetővé teszi a kritikus infrastruktúrák automatizált és hatékony működését, amely biztosítja az alapvető szolgáltatások gyors és megbízható ellátását. Az energiaellátásban például a felügyeleti vezérlő rendszerek valós időben gyűjtik az adatokat a hálózat állapotáról, és szükség esetén azonnal beavatkoznak a zavarok elhárítása érdekében. Az operatív technológia további előnye a valós idejű monitorozás és vezérlés, amely lehetővé teszi az üzemeltetők számára, hogy gyorsan reagáljanak a hibákra vagy fenyegetésekre. Ez különösen fontos olyan ágazatokban, ahol a késlekedés súlyos társadalmi és gazdasági károkat okozhat. Az operatív technológia rendszerei közvetlenül integrálódnak a fizikai eszközökhöz, például szelepekhez, motorokhoz és szivattyúkhoz, amelyeket vezérelnek és monitoroznak. Ez az integráció biztosítja a komplex folyamatok precíz és biztonságos működését. Ugyanakkor az OT-rendszerek kihívásokat is hordoznak, mivel sok rendszer elavult vagy eleve nincs felkészítve a modern kiberbiztonsági fenyegetések ellen. Az informatikai rendszerekkel való integráció és az internetkapcsolat növelte a sebezhetőségüket, így kibertámadások révén a támadók átvehetik az irányítást és zavarokat okozhatnak. A biztonság érdekében az OT-rendszerek korszerűsítése és karbantartása kiemelten fontos, beleértve a kiberbiztonsági intézkedések alkalmazását, például a hálózatok szegmentálását és a behatolásérzékelő rendszerek telepítését.

A kiberfenyegetések növekvő kockázata

Az OT-rendszerek korábban gyakran zárt, elszigetelt hálózatokként működtek, azonban az ipar 4.0 (Hearn et al., 2023) és a digitalizáció előrehaladtával egyre inkább integrálódnak az IT-rendszerekkel. Ez az integráció növeli a hatékonyságot és a rugalmasságot, viszont ezzel együtt a kiberfenyegetések kockázatát is jelentősen megnöveli. A hackerek, államilag támogatott csoportok, vagy akár rosszindulatú belső szereplők célpontként tekintenek ezekre a rendszerekre, mivel azok sikeres megzavarása komoly következményekkel járhat mind a gazdaságra, mind a társadalomra nézve. A hálózati szegmentációs problémák növekedése (2. számú ábra) elsősorban az ipari rendszerek digitalizációjából és a komplex infrastruktúrák biztonsági gyengeségeiből fakad, amelyeket gyakran nehéz modern elvekhez igazítani. Emellett a támadók egyre kifinomultabb támadási módszereket alkalmaznak, miközben a biztonsági beruházások és a megfelelő szegmentációs szabályok végrehajtása elmarad. Az erőforráshiány, a képzetlenség és az üzleti prioritások a biztonság rovására súlyosbítják a helyzetet, növelve a sérülékenységek kihasználásának lehetőségét. 2023-ban a Dragos megfigyelései szerint az OT-rendszerekkel kapcsolatos incidensek körülbelül

70%-a az IT-környezetből indult ki (Dragos, 2024). Az ilyen problémák megelőzésére kulcsfontosságú megoldásként javasolják a hálózati szegmentációt és az IT- és OT-rendszerek külön tartományra (domainre) való elkülönítését.

2. számú ábra
Szegmentációs hiányosságokat tartalmazó jelentések



Forrás. A szerzők saját szerkesztése a Dragos jelentések alapján.

Az OT-rendszerek védelme számos egyedi kihívással jár. Ezek közül néhányat bemutatunk:

a) Hagyományos rendszerek: sok OT-rendszer több évtizedes technológián alapul, amelyeket nem a mai kiberbiztonsági fenyegetésekre terveztek. Ezeket a rendszereket gyakran nehéz frissíteni vagy modernizálni anélkül, hogy a működést megszakítanánk.
b) Zárt rendszerek: az OT-rendszerek gyakran zárt protokollokat és rendszereket használnak, amelyek nehezebbé teszik a kiberbiztonsági eszközök és módszerek alkalmazását. A biztonsági javítások vagy frissítések alkalmazása is nehézkesebb lehet ezeknél a rendszereknél, mivel minden változtatás kihatással lehet a folyamatok stabilitására.
c) Folyamatos működés: az OT-rendszerek esetében a rendelkezésre állás és a folyamatok zavartalansága kiemelt fontosságú. Egyes iparágakban, például az energiaellátásban, a leállás komoly gazdasági és társadalmi következményekkel járhat, így a biztonsági frissítések vagy javítások alkalmazása időigényes és kockázatos folyamat.

d) Különböző prioritások: az OT-rendszerek kezelése és biztonságának fenntartása eltérő megközelítést igényel az IT-rendszerekkel szemben. Míg az IT világában az adatbiztonság, a hozzáférés védelme és az adatok titkosítása az elsődleges szempontok, addig az OT esetében a fizikai rendszerek működésének folyamatos biztosítása az elsődleges cél.

Kritikus infrastruktúra támadói kiberbiztonsági szempontok alapján

A kritikus infrastruktúrákat számos különböző támadótípus fenyegetheti, akik eltérő motivációkkal és célokkal rendelkeznek. Ezek a támadók lehetnek külső vagy belső szereplők, akik gazdasági, politikai, ideológiai vagy akár technológiai célokat követnek. A támadások módszerei és céljai széles skálán mozognak, kezdve a kémkedéstől és adatlopástól a rendszerek működésének szándékos megzavarásáig. Az infrastruktúrák növekvő digitalizációja és a technológiai rendszerek integrációja tovább növeli a támadási felületeket, amelyek kihasználása súlyos következményekkel járhat.

Nemzetállamok

A nemzetállamok által szponzorált támadások a kritikus infrastruktúrák elleni kiberfenyegetések egyik legjelentősebb kategóriáját jelentik. Ezek a támadások gyakran háttértudománnyal és jelentős erőforrásokkal rendelkező szereplők által valósulnak meg. Céljaik között szerepelhet érzékeny adatok megszerzésére irányuló kémkedés, a működés megzavarása vagy ellehetetlenítése, illetve politikai és gazdasági nyomásgyakorlás.

Egy ismert példa a 2010-es Stuxnet támadás, amely az iráni urándúsító művek ellen irányult. Illetve figyelemre méltó másik példa volt egy sikeres, államilag támogatott kibertámadásra a 2015-ös ukrajnai áramszünet, amelyet orosz hátterű hackerek hajtottak végre. A vizsgálatok során három szolgáltató rendszereiben azonosították a BlackEnergy[5] nevű rosszindulatú szoftvert, valamint megállapították, hogy a KillDisk[6] malware[7] alkalmazásával törölték a működéshez elengedhetetlen fájlokat. Ezek a vírusok célzott adathalászati támadások, úgynevezett spear phishing[8] módszerekkel kerültek a rendszerekbe. A tá-

5 Kártékony szoftver, melyet távoli kódfuttatásra és adatlopásra fejlesztettek és sikeresen használtak.
6 Kártékony szoftver, melyet adatok megsemmisítésére fejlesztettek ki és sikeresen használtak.
7 Rosszindulatú szoftver.
8 Személyre szabott adathalászat.

madás következtében körülbelül 225 ezer háztartás maradt áramellátás nélkül (URL1; Müller, 2016).

Kibertámadásokra szakosodott bűnözői csoportok

A szervezett bűnözői csoportok a kiberbűnözés másik leggyakoribb szereplői. Céljuk legtöbbször a haszonszerzés, amelyet zsarolóprogramok (ransomware)[9], adathalászat vagy egyéb illegális tevékenységek által érnek el. Ezek a csoportok különösen veszélyesek, mivel magasan specializált eszközöket és technikákat használnak, gyakran „bűnözés mint szolgáltatás" (Crime-as-a-Service, CaaS) modellben működnek.

A Colonial Pipeline elleni 2021-es támadás az egyik legismertebb példa a kritikus infrastruktúrát célzó zsarolóvírus-eseményekre. A támadók, a DarkSide nevű hackercsoport, sikeresen kompromittálták a Colonial Pipeline IT-rendszereit, ami miatt a vállalat kénytelen volt leállítani a teljes üzemanyag-vezeték működését. Ez a vezeték az Egyesült Államok keleti partvidéki üzemanyag-ellátásának körülbelül 45%-át biztosítja, így a leállás azonnali gazdasági és társadalmi hatásokat váltott ki, beleértve a pánikszerű üzemanyag-vásárlást és hiányt. A támadás fő célpontja a vállalat számlázási rendszere volt, amelynek kompromittálásával a csoport megakadályozta a tranzakciók feldolgozását. A Colonial Pipeline vezetősége a biztonság érdekében úgy döntött, hogy izolálja IT-rendszereit az OT-hálózatoktól, megelőzve a zsarolóvírus terjedését a vezeték működéséhez szükséges operációs technológiákra. A helyreállítás érdekében a vállalat 4,4 millió dollárt fizetett ki Bitcoinban a támadóknak (Insurica, 2021).

Hacktivisták

A hacktivisták olyan egyének vagy csoportok, akik valamilyen ideológiai, politikai vagy társadalmi célból hajtanak végre támadásokat. Ezek a támadások gyakran figyelemfelkeltésre irányulnak, de súlyos károkat is okozhatnak. Jellemző támadásaik közé tartozik weboldalak deface-elése (vizuális megsértése), elosztott szolgáltatásmegtagadás-támadások (DDoS), valamint bizalmas adatok nyilvánosságra hozatala.

Egy 2023-as példa a kritikus infrastruktúrákat érintő támadásokra, amikor a CyberAv3ngers és a Team Insane Pakistan nevű hackercsoportok izraeli infrastruktúrák ellen hajtottak végre akciókat. Állításuk szerint sikeresen megzavarták

9 Kártékony szoftver, melyet eszközök zárolására vagy az eszközökön lévő adatok titkosítására fejlesztettek ki.

az izraeli vasúti rendszerek működését, amelyek alapvető szerepet játszanak az ország szállítmányozásában és utasszállításában. Emellett támadásokat hajtottak végre egy izraeli város elektromos hálózata ellen, ami áramkimaradásokat eredményezett, komoly hatást gyakorolva a lakosságra és a helyi szolgáltatások működésére. Továbbá célba vettek egy izraeli vízierőmű-rendszert, amely az energiaellátás és az infrastruktúrák fenntartása szempontjából kritikus jelentőségű, állításuk szerint sikeresen megzavarva annak működését (Dragos, 2024).

Insiderek (belső alkalmazottak)

A belső támadók, vagyis az adminisztrációban és infrastruktúrákban dolgozó alkalmazottak szintén jelentős fenyegetést jelenthetnek. Szándékos vagy gondatlan magatartásuk a kiberbiztonság súlyos megsértéséhez vezethet. Az insider fenyegetések például szándékos adatlopást vagy károkozást foglalhatnak magukban, illetve gondatlan adatkezelés és gyenge jelszóhasználat formájában is megnyilvánulhatnak.

Egy figyelemre méltó eset a 2000-es támadás az ausztráliai Maroochy Shire szennyvízkezelő rendszere ellen, ahol egy elégedetlen alkalmazott hozzáférést szerzett a szennyvízkezelő telep telemetriai rendszeréhez, amelyet SCADA-rendszerek irányítottak (Slay & Miller, 2007). Többször megzavarta a szennyvízszivattyúk működését, ami a szennyvíz kiömlését eredményezte a környező folyókba és parkokba, ezáltal jelentős ökológiai és közegészségügyi károkat okozva. Ez az eset volt az egyik első dokumentált támadás, amelyben egy kritikus infrastruktúra OT-rendszerét manipulálták, és ami világszerte előmozdította a kritikus infrastruktúrák által is használt SCADA-rendszerek kibervédelmi protokolljainak fejlesztését.

Egyéni hackerek és úgynevezett etikus hackerek

Míg az egyéni hackerek kártékony szándékkal támadnak, az etikus hackerek gyakran a gyenge pontok feltárásában segítenek. Azonban, ha egy hacker átlépi a határt jószándék és a véletlen vagy szándékos károkozás között (grey hat hacker), akkor jelentős fenyegetést jelenthet.

2021-ben az oldsmari víztisztító rendszert kibertámadás érte, amikor egy támadó a TeamViewer távoli hozzáférési szoftvert használva megemelte a vízhez adott nátrium-hidroxid (NaOH) dózisát (Cervini et al., 2022) A támadást a helyszíni kezelő gyorsan észlelte és visszaállította a normál értékeket, így a víz minősége nem lépte túl a megengedett határértékeket. Az eset rámutatott a távoli hozzáférési eszközök és az OT-rendszerek sebezhetőségére, valamint

arra, hogy fokozott átláthatóságra, jobb szegmentációra és szigorúbb biztonsági intézkedésekre van szükség a hasonló incidensek elkerülésének érdekében.

Terrorista szervezetek

A terrorista szervezetek is felfedezték a kiberhadviselés lehetőségeit. Egyre gyakrabban használják a kiberteret propagandacélokra, támogatóik mozgósítására, illetve támadások szervezésére. Különösen hatásos és fenyegető lehet részükről a kritikus infrastruktúrák elleni támadásokkal keltett pánik és bizonytalanság, valamint adatok manipulálása vagy megsemmisítése.

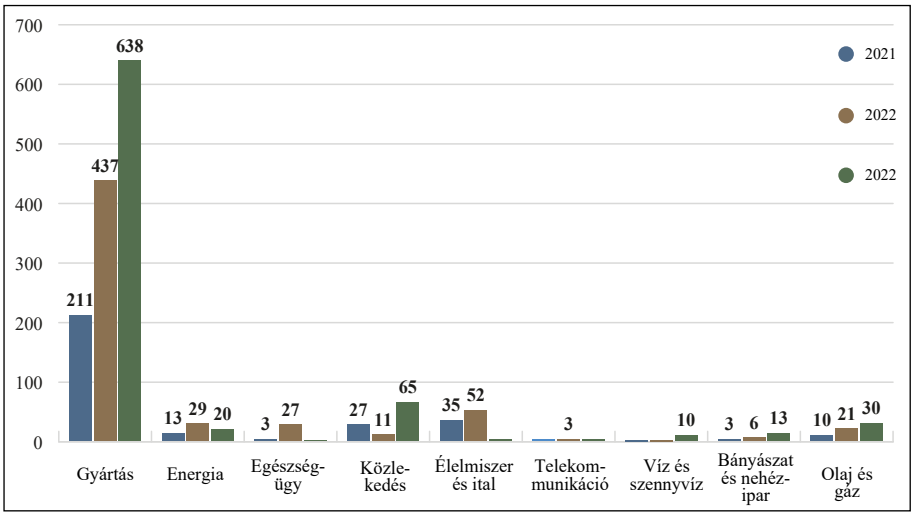
A Dragos jelentésekben kiemelkedő példa a Xenotime nevű csoport, amelyet terrorista jellegű tevékenységekkel hoztak összefüggésbe (Dragos, 2024). Ez a csoport különösen a kritikus infrastruktúrák, például az energiaipar rendszereinek támadásairól ismert. A Xenotime fejlesztette ki a Trisis nevű rosszindulatú szoftvert, amelyet kifejezetten ipari biztonsági rendszerek, az úgynevezett Safety Instrumented Systems (SIS) megzavarására terveztek (Geiger et al., 2020). Ezek a rendszerek létfontosságúak az ipari folyamatok biztonságos működésének fenntartásában. A támadások célja gyakran ezek leállítására irányul, ami robbanásokhoz vagy súlyos károkhoz vezethet.

2017-ben a Trisist egy szaúd-arábiai petrolkémiai létesítményben használták, ahol a támadók a biztonsági rendszerek kikapcsolásával próbálták veszélyeztetni a létesítmény működését (Green, 2022). Ez az eset rámutatott arra, hogy a Xenotime célja nemcsak a rendszerek működésének megzavarása, hanem potenciálisan emberi életek veszélyeztetése is volt.

Trendek a kritikus infrastruktúrákat ért támadásokban

A Dragos 2021, 2022 és 2023-as ICS/OT kibervédelmi jelentései alapján megfigyelhető, hogy az OT-rendszereket érő támadások száma és kifinomultsága évről évre növekszik (Dragos, 2024). Pontos számokat nem lehet biztosan állítani, mivel az incidensek sok esetben nem kerülnek nyilvánosságra. Ez a nemzetek, cégek és szervezetek alapvető érdeke, hogy bizonyos információk, különösen az infrastruktúrákat ért támadások ténye és eredményei ne lássanak napvilágot biztonsági és gazdasági érdekeikre való tekintettel. Ugyanakkor sok esetben az információk elérhetőek a zsarolóvírus-támadásokról, melyek segítenek megérteni a trendek alakulását. A ransomware támadások folyamatosan emelkednek (3. számú ábra), 2023-ban közel 50%-os növekedést regisztráltak a 2022-es adatokhoz képest.

3. számú ábra
2021 és 2023 között regisztrált ransomware támadások szektoronkénti lebontása



Forrás. A szerzők saját szerkesztése a Dragos jelentések alapján.

Ezek a támadások leggyakrabban a gyártás, az energiaipar, a közlekedés, az egészségügy és az élelmiszeripar rendszereit célozták meg, ami a támadók pénzügyi motivációját tükrözi. Emellett minden évben új fenyegetési csoportok jelentek meg, mint például 2021-ben a KOSTOVITE, ERYTHRITE és PETROVITE, 2022-ben a CHERNOVITE és BENTONITE, 2023-ban pedig a GANANITE, LAURIONITE és VOLTZITE. Ezek a csoportok egyre kifinomultabb technikákat alkalmaznak, mint például az ipari protokollok kihasználása és moduláris támadási keretrendszerek fejlesztése. A geopolitikai konfliktusok, mint az Oroszország és Ukrajna közötti háború vagy a Közel-Keleten zajló események, jelentős szerepet játszottak az OT-rendszerek elleni támadások számának növekedésében. Például az ELECTRUM nevű fenyegetési csoport több ukrán kritikus infrastruktúrát célzott meg destruktív támadásokkal.

A támadások célpontjai közül a gyártás továbbra is a leggyakrabban érintett szektor, hiszen 2023-ban az összes zsarolóvírus-támadás 70%-a erre irányult. Az energia- és vízszolgáltatók szintén kiemelt célpontok, mivel ezek zavarása jelentős hatással lehet a lakosságra és a gazdaságra. A technológiai és sérülékenységi trendek között kiemelkedik, hogy 2023-ban a rendszerek 80%-ában nem volt megfelelő OT hálózati monitoring, ami megnehezítette a támadások észlelését. A hálózati szegmentáció és az IT/OT-felhasználók elkülönítése is problémát jelentett, az OT-rendszerek 54%-ában ugyanis azonos hitelesítő

adatokat használtak mindkét környezethez. Az OT-rendszerek sérülékenységei is egyre gyakoribbá váltak, 2023-ban az elemzett sérülékenységek 31%-a tartalmazott helytelen adatokat, és sok esetben nem álltak rendelkezésre alternatív mitigációs lépések. Új támadási eszközök, mint például a PIPEDREAM, szintén megjelentek, amelyek új szintre emelték az OT-rendszerek elleni támadásokat, mivel képesek több iparágat is célba venni és a natív ipari protokollokat kihasználni. Ezek a trendek egyértelműen rámutatnak az OT-rendszerek védelmének fontosságára, valamint arra, hogy az ilyen típusú támadások jelentős veszélyt jelentenek a kritikus infrastruktúrákra.

Mit tehetünk a védekezés érdekében?

A kritikus infrastruktúrák védelme életbevágóan fontos, hiszen ezek a rendszerek társadalmaink ellátásának és kiszolgálásának alapjait képezik. A fent említett fenyegetések ellen csak komplex és integrált védelmi stratégiával lehet hatékonyan fellépni (Berzsenyi, 2014). A kiberbiztonság folyamatos fejlesztése és az esetleges fenyegetések előrejelzése kulcsfontosságú a fenntartható és biztonságos működés szempontjából. Ahhoz, hogy hatékonyan kezeljük az OT kiberbiztonsági kihívásait, átfogó megközelítésekre van szükség. Az IT- és OT-rendszerek összekapcsolása elkerülhetetlen, azonban ezt biztonságosan, ellenőrzött módon kell megvalósítani. Ennek egyik kulcseleme a megfelelő hálózati szegmentáció, amely nem a teljes elkülönítést jelenti, hanem a biztonságos és szabályozott kommunikációt teszi lehetővé az egyes rendszerek között. Bár a régebbi OT-rendszerek esetében nehézkes lehet a frissítések alkalmazása, a rendszeres biztonsági javítások és a sérülékenységek kezelése elengedhetetlen a kiberbiztonság fenntartásához (Nyári & Kerti, 2021). Szükséges az informatikai és OT-rendszerek folyamatos monitorozása, a behatolásfigyelés, valamint a hálózati anomáliák keresése, hogy a rendellenességeket időben azonosítsák. A munkavállalók folyamatos képzése és a kiberbiztonsági tudatosság növelése alapvető fontosságú nemcsak az IT-, hanem az OT-rendszerek védelmében (Kerti, 2023). Az alkalmazottaknak tisztában kell lenniük a potenciális kockázatokkal, és megfelelő eljárásokat kell követniük a biztonságos működés fenntartása érdekében. Az OT-hálózatok esetében is egyre inkább szükséges a Zero Trust elv alkalmazása, ahol minden hozzáférést folyamatosan ellenőriznek és felügyelnek, függetlenül attól, hogy az belső vagy külső forrásból származik.

Konklúzió

Az operatív technológia kiberbiztonsága a kritikus infrastruktúrák védelmének egyik legfontosabb és legégetőbb területe, amely nemcsak a technológiai, hanem a gazdasági és társadalmi stabilitás szempontjából is kiemelkedő jelentőségű. A globális digitalizáció és az automatizáció rohamos fejlődése alapvetően átalakítja a kritikus infrastruktúrák működését, miközben egyre nagyobb sebezhetőséget eredményez az ilyen rendszerekben. Ezért elengedhetetlen, hogy az OT-rendszerek védelmét integrált, holisztikus megközelítéssel kezeljük, amely figyelembe veszi az információbiztonsági, működésbiztonsági és technológiai aspektusokat is.

Az OT- és IT-rendszerek egyre szorosabb integrációja nemcsak előnyökkel, hanem új kihívásokkal is jár. Az OT-rendszerek hagyományosan zárt környezete a digitalizációval megnyílik az IT-infrastruktúrák felé, amely jelentősen növeli a kiberfenyegetések kockázatát. Ezért alapvető fontosságú, hogy a különböző rendszerek közötti kapcsolatok biztonságosan legyenek kialakítva, és az informatikai megoldások alkalmazása során a rendszerfolyamatok folytonosságának és stabilitásának megőrzése prioritást élvezzen. A kutatás eredményei alátámasztják, hogy a kritikus infrastruktúrákban alkalmazott védelmi mechanizmusok sok esetben nem igazodnak teljes mértékben az OT-rendszerek sajátos biztonsági követelményeihez, ami növeli a sérülékenységet.

Az OT-rendszerek sebezhetőségének kezeléséhez az egyik legfontosabb lépés a rendszeres biztonsági auditok elvégzése, valamint a dolgozók folyamatos képzése. A kiberbiztonsági fenyegetések felismerése és azok elhárítása csak akkor lehet hatékony, ha az emberi erőforrások és a technológiai eszközök harmonikusan együttműködnek. A mesterséges intelligencia és az adatvezérelt megoldások alkalmazása lehetőséget nyújt arra, hogy a rendszerek valós időben reagáljanak a fenyegetésekre, ezzel csökkentve a leállások és zavarok kockázatát.

Az OT-rendszerek biztonságának növelése hosszú távú tervezést és nemzetközi összefogást igényel. A globális fenyegetések, mint például a kiberterrorizmus vagy az államilag szponzorált kibertámadások országhatárokon átívelő kihívásokat jelentenek, amelyek kezelése csak szoros nemzetközi együttműködéssel valósítható meg. Az elemzett esetek alapján a megfelelő hálózati szegmentáció és az IT- és OT-rendszerek ellenőrzött integrációja jelentős mértékben csökkentheti a kibertámadások kockázatát, ezért ezen megoldások széles körű alkalmazása kulcsfontosságú. Az olyan eszközök, mint a szabványosított protokollok és a globális kiberbiztonsági irányelvek, jelentős szerepet játszanak a rendszerek ellenállóképességének növelésében.

Összességében az operatív technológia kiberbiztonsága nem csupán technológiai kihívás, hanem egy átfogó társadalmi, gazdasági és politikai feladat is,

amely megfelelő egyensúlyteremtést igényel a modernizáció és a biztonság között. Csak komplex, integrált stratégiákkal lehet biztosítani, hogy ezek a rendszerek hatékonyan és biztonságosan szolgálják a társadalmat.

Mindezeknek megfelelően egyértelmű, hogy a nemzetközi szabványok, például az IEC 62443 (Hauet, 2012) és az ISO/IEC 27019 alkalmazása hozzájárulhat az OT-rendszerek biztonságosabbá tételéhez, különösen az ipari vezérlőrendszerek esetében. Emellett a nemzeti szintű kiberbiztonsági központok együttműködése, valamint az információmegosztó platformok (például ISAC[10]-ek) jelentős szerepet játszanak a fenyegetések gyors felismerésében és kezelésében. Látható tehát, hogy a jövőbeli kutatásoknak különös figyelmet kell fordítaniuk az OT és IT integrációja során alkalmazott új generációs technológiák, például a mesterséges intelligencia és a gépi tanulás biztonsági aspektusaira. Emellett fontos feltárni az egyes iparág-specifikus kiberbiztonsági kihívásokat, ahol az OT-rendszerek sebezhetősége különösen kritikus.

Felhasznált irodalom

Berzsenyi D. (2014). Kiberbiztonsági analógiák és eltérések: A Közép-európai Kiberbiztonsági Platform részes országai által kiadott kiberbiztonsági stratégiák összehasonlító elemzése. *Nemzet és Biztonság, 7*(4), pp. 110–138. https://folyoirat.ludovika.hu/index.php/neb/article/view/4097/3352

Cervini, J., Rubin, A., & Watkins, L. (2022). Don't drink the cyber: Extrapolating the possibilities of Oldsmar's water treatment cyberattack. *International Conference on Cyber Warfare and Security, 17*(1), pp. 19–25. https://doi.org/10.34190/iccws.17.1.29

Dragos. (2024). *OT cybersecurity: The 2023 year in review*. https://www.dragos.com/ot-cybersecurity-year-in-review/

Geiger, M., Bauer, J., Masuch, M., & Franke, J. (2020). An analysis of Black Energy 3, Crashoverride, and Trisis, three malware approaches targeting operational technology systems. In *Proceedings of the 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)* (1537–1543). IEEE. https://doi.org/10.1109/ETFA46521.2020.9212128

Green, M. (2022, April 19). Throwback attack: TRISIS malware mystifies industrial community. *Industrial Cybersecurity Pulse*. https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-trisis-malware-mystifies-industrial-community/

Haig Z., Hajnal B., Kovács L., Muha L. & Sik Z. N. (2009). *A kritikus információs infrastruktúrák meghatározásának módszertana*. ENO Advisory Kft.

Hauet, J.-P. (2012). *ISA99/IEC 62443: A solution to cyber-security issues?* Paper presented at the ISA Automation Conference.

10 Information Sharing and Analysis Center – információmegosztó és elemző központ.

Hearn, G., Williams, P., Rodrigues, J. H. P., & Laundon, M. (2023). Education and training for industry 4.0: A case study of a manufacturing ecosystem. *Education + Training, 65*(8/9), 1070–1084. https://doi.org/10.1108/ET-10-2022-0407

Hunorfi P. (2024). Az ISO/IEC 27001 szabvány elmélete és gyakorlati alkalmazása OT/ICS-rendszerek kiberbiztonsági jelentéseinek tükrében. *Scientia et Securitas, 5*(3), 323–332. https://doi.org/10.1556/112.2024.00228

Kerti A. (2023). Az információbiztonsági tudatosság fejlesztésének tervezése. In Tóth A. (Szerk.), *Új típusú kihívások az infokommunikációban* (pp. 181–194). Dialóg Campus Kiadó.

Muha L. (2007). *A Magyar Köztársaság kritikus információs infrastruktúráinak védelme* [Master's thesis, Zrínyi Miklós Nemzetvédelmi Egyetem].

Müller T. (2016). *Kiberfenyegetések és kibervédelem* (Infojegyzet 2016/44). OGY Hivatal Közgyűjteményi és Közművelődési Igazgatóság Képviselői Információs Szolgálat. https://www.parlament.hu/documents/10181/595001/Infojegyzet_2016_44_kibervedelem.pdf

Nyári N. & Kerti A. (2021). *A szoftverminőséggel kapcsolatos ISO szabványok áttekintése*. Biztonságtudományi Szemle, 3(2), pp. 61–72. https://biztonsagtudomany.hu/index.php/btsz/article/view/284

Répás S. & Dalicsek I. (2015). *Az információbiztonsági kockázatelemzés módszertani kérdései a kritikus infrastruktúra elemeket üzemeltető szervezetek esetében*. Pro Publico Bono – Magyar Közigazgatás, 3(4), pp. 22–33. https://folyoirat.ludovika.hu/index.php/ppbmk/article/view/2639

Slay, J. & Miller, M. (2007). Lessons learned from the Maroochy water breach. In E. Goetz & S. Shenoi (Eds.), *Critical infrastructure protection* (Vol. 253, pp. 73–82). Springer. https://doi.org/10.1007/978-0-387-75462-8_6

Vijayapriya, T. & Kothari, D. P. (2011). Smart grid: An overview. *Smart Grid and Renewable Energy*, 2(4), pp. 305–311. https://doi.org/10.4236/sgre.2011.24035

A cikkben szereplő online hivatkozás

URL1: *Cyber-Attack Against Ukrainian Critical Infrastructure (2015).* America`s Cyber Defence Agency. www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

Alkalmazott jogszabályok

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

2024. évi LXXXIV. törvény a kritikus szervezetek ellenálló képességéről

234/2011. (XI. 10.) Korm. Rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról

A cikk APA szabály szerinti hivatkozása

Hunorfi P. & Farkas T. (2025). Az operatív technológia kiberbiztonsága kritikus infrastruktúrákban. *Belügyi Szemle*, *73*(SI1), 65–81. https://doi.org/10.38146/BSZ-AJIA.2025.v73.SI1.pp65-81

Nyilatkozatok

Összeférhetetlenség

A szerzők nem jelentettek összeférhetetlenséget.

Finanszírozás

A szerzők nem kaptak pénzügyi támogatást a kutatáshoz, a szerzőséghez és/vagy a cikk publikálásához.

Etikai nyilatkozat

Az adatokat kérésre rendelkezésre bocsátják.

Levelező szerző

A cikk levelező szerzője Hunorfi Péter, aki a hunorfi.peter@phd.uni-obuda.hu e-mail címen érhető el.