DOI: https://doi.org/10.12700/btsz.2025.7.1.145

GLOBAL CHALLENGES IN CYBERSPACE: HUMAN RISK MANAGEMENT IN THE PROTECTION OF CRITICAL INFRASTRUCTURES

GLOBÁLIS KIHÍVÁSOK A KIBERTÉRBEN: HUMÁN KOCKÁZATOK KEZELÉSE A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK VÉDELMÉBEN

KÁRÁSZ Balázs[1]

Abstract

This paper examines the indirect impacts of global climate change on the functioning of society, and its effects in cyberspace, which are dominantly impacting on warfare and security policy in the 21st century. The focus of the research is on the protection of critical infrastructures, which are increasingly exposed to threats in cyberspace. When threats are complemented by internal vulnerabilities, both components of identifiable risk, impact and likelihood, can increase. Therefore, among the many pillars of protection, it is of paramount importance to prepare critical infrastructure workers by improving their information security awareness and preparedness. The paper explores the context for developing possible ways to manage these risks in a way that is appropriate to the organisational functioning of the critical infrastructure.

Keywords

climate change, critical infrastructure protection, cyberspace, risk management, information security awareness

Absztrakt

Jelen tanulmány a globális klímaváltozásnak a társadalom működésére közvetetten gyakorolt hatásai közül a 21. század hadviselését és biztonságpolitikáját nagymértékben befolyásoló kibertérben megvalósuló hatásait vizsgálja. A kutatás fókuszában a kritikus infrastruktúrák védelme áll, amelyek egyre növekvő számban kitettek a kibertérben megvalósuló fenyegetéseknek. Amennyiben a fenyegetéseket belső gyenge pontok egészítik ki, az azonosítható kockázatok mindkét komponense, a hatás és valószínűség egyaránt növekedhet. Ezért a védelem számos pillére közül kiemelkedő fontosságú a kritikus infrastruktúrák dolgozóinak felkészítése, információbiztonság-tudatosságuk és felkészültségük fejlesztése útján. A tanulmány feltárja azokat az összefüggéseket, amelyek alapján kidolgozhatók e kockázatok kezelésének lehetséges, az adott kritikus infrastruktúra szervezeti működéséhez illeszkedő módszerei.

Kulcsszavak

klímaváltozás, kritikus infrastruktúra védelem, kibertér, kockázatkezelés, információbiztonság-tudatosság

[1] karaszb@gmail.com | ORCID: 0000-0003-2065-4928 | Former PhD Student, National University of Public Service, Doctoral School of Military Engineering | Volt PhD hallgató, Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola

BEVEZETÉS ÉS A KUTATÁS RÉSZLETEI

Korunk társadalma globális kihívásokkal küzd, amelyek egyrészt a mindennapi élet bármely területén képesek jelentős hatást gyakorolni, másrészt kölcsönösen befolyásolják egymást, így a felmerülő külső fenyegetettségek és belső gyengeségek folyamatos változásban vannak. Az információbiztonsági törekvéseknek olyan társadalmi, jogi és digitális technológiai környezetben kell hatékonyan megvalósulniuk, mely egyre gyorsabb alkalmazkodást kíván az egyre komplexebbé váló helyzetekhez, folyamatokhoz.

Az információs társadalom tendenciái arra késztetik a szervezeteket, hogy könnyen elérhető és alkalmazható, naprakész eszközöket vegyenek igénybe az IT-biztonság, a fizikai biztonság, valamint a humán kockázatok kezelése terén (különösen a szervezetfejlesztés és a tudatosságra nevelés tekintetében). Az e célokat szolgáló eszköztár napjainkig folyamatosan bővül és minőségében is fejlődik, hiszen a fentiekből következően alkalmazkodni kénytelen az olyan, globális kihívások által jelentősen befolyásolt információs környezethez is, mint amilyet a 2020-as év járványügyi intézkedései közvetlenül és közvetetten teremtettek.

A kritikus infrastruktúrák, mint – többek közt – az energiaellátás, vízgazdálkodás, közlekedési hálózatok és egészségügyi rendszerek, valamint az egyre növekvő jelentőségű információs infrastruktúrák alapvető szerepet töltenek be a társadalmak működésében, illetve ahhoz egyenesen nélkülözhetetlenek, így védelmük nemcsak gazdasági, hanem biztonságpolitikai szempontból is kulcsfontosságú. Egy-egy létfontosságú rendszerelem kiesése súlyos társadalmi és gazdasági következményekkel járhat, ezért azok folyamatos védelme, fenntarthatóságuk biztosítása és az ellenállóképességük növelése kiemelt feladat az infrastruktúrákat üzemeltetők számára.

Tudományos probléma

Az előzőek fényében felmerül a kérdés, miként befolyásolják napjaink globális kihívásai a kritikus információs infrastruktúrák belső gyengeségeit és hogyan alakítják külső fenyegetettségeit abban a tekintetben is, hogy milyen kockázatkezelési módszerek állnak rendelkezésre a védelem minél magasabb szintű hatékony megvalósításában.

Kutatási cél

A kutatás célja, hogy rövid áttekintést nyújtson a kritikus információs infrastruktúrák mibenlétéről, valamint a 21. század globális kihívásairól, a kibertér aktuális trendjeiről. Ezt követően azonosításra kerülnek a kritikus információs infrastruktúrák főbb fenyegetései és gyengeségei a kiberkörnyezet aktualitásai tükrében. Végezetül a fókusz a humán kockázatok azonosítására, és az ezeket leghatékonyabban kezelő módszerekre, best practice-ekre tevődik.

Kutatási módszerek

A szerző elméleti és empirikus kutatási módszereket alkalmaz, részben a grounded theory eszközével. Kapcsolódó magyar és nemzetközi szakirodalom kerül feldolgozásra, a gyakorlati aspektus hozzáillesztéséhez szervezeti példákból születik inspiráció, összehasonlítást nyújtva egyúttal kritikus infrastruktúrát üzemeltető, és más jellegű szervezetek tulajdonságai között.

A 21. SZÁZAD GLOBÁLIS KIHÍVÁSAI

Jelen fejezetben bemutatásra kerülnek a kritikus (információs) infrastruktúrák, valamint korunk legjelentősebb globális kihívásai és ezek kölcsönhatásai közül azok, amelyek a kritikus infrastruktúrák működése tekintetében a legnagyobb kockázatot, és így megoldási utak kidolgozására váró problémákat jelentenek.

Kritikus infrastruktúrák

Jelen tanulmány a kritikus infrastruktúra és a létfontosságú rendszerelem kifejezést szinonimaként használja, előbbi a nemzetközi gyakorlatban használt terminológiának szó szerinti fordítása, míg utóbbi a magyar jogszabályokban alkalmazott terminus.

A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény létfontosságú rendszerelemként gazdasági ágazatok széles körének valamelyikébe tartozó szolgáltatás, eszköz, létesítmény vagy rendszer olyan rendszerelemét, továbbá azok által nyújtott szolgáltatásokat határozza meg, „amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához, az ország honvédelméhez –, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna.” [1] Az érintett gazdasági ágazatok – melyek alágazatait a törvény tételesen is felsorolja – a következők: energia, közlekedés, agrárgazdaság, egészségügy, társadalombiztosítás, pénzügy, infokommunikációs technológiák, víz, honvédelem, közbiztonság-védelem.

Már 2005-ben megfogalmazásra került [2] a kritikus információs infrastruktúra fogalma, mely kifejezés alatt azokat az infokommunikációs rendszereket értjük, amelyek önmagukban is kritikus infrastruktúra elemek, vagy lényegesek az infrastruktúra elemei működésének szempontjából (távközlés, számítógépek és szoftver, internet, műholdak stb.).

Klímaváltozás

A korábban számos fórumon megtalálható globális felmelegedés kifejezés helyett jelen tanulmány a globális klímaváltozást használja, mely átfogóbb, a valósághoz közelebbi és tudományos szempontból is elfogadott, semleges összefoglalását adja mindazon folyamatoknak, amelyek meghatározzák mindennapjainkat, kihatással vannak a politikai és társadalmi viszonyokra, a regionális éghajlat és lokális időjárás alakulására világszerte, a természeti katasztrófák előfordulásának gyakoriságára, és magára a klímaváltozásra adott eltérő reakciókra is.

A klímaváltozás a 21. század egyik legösszetettebb globális kihívása, amely nem csak a természeti környezetet érinti, hanem a társadalom működésére is hatást gyakorol. A szélsőséges időjárási jelenségek, az óceánok szintjének emelkedése és az akár emberéleteket követelő természeti katasztrófák olyan rendszerszintű változásokat idéznek elő, amelyek közvetlenül és közvetetten is hatnak az infrastruktúrákra, a gazdasági folyamatokra és a biztonságpolitikára. [3] Hozzá kell tenni, hogy a természeti katasztrófák által okozott károk növekvő költségei egyre nagyobb terhet rónak a nemzetgazdaságokra és a védelmi rendszerekre.

Trendek a kibertérben és a digitális világban

A digitális világ folyamatos fejlődése az elmúlt évtizedekben exponenciálisan növelte az adatok és hálózatok jelentőségét a társadalom és a gazdaság működésében. A telekommunikáció aktuális sarokköveként a 5G-hálózatok, a szintén hálózatos kommunikációra épülő IoT-eszközök és a mesterséges intelligencia elterjedése új lehetőségeket teremt, ugyanakkor ezekkel párhuzamosan a kibertérben megjelenő fenyegetések is egyre összetettebbé válnak. Az állami és nem állami szereplők által elkövetett kibertámadások száma is folyamatosan növekszik, de még fontosabb, hogy egyre inkább célba veszik az alapvető szolgáltatásokat biztosító rendszereket.

A kritikus infrastruktúrák elleni kibertámadások azért lehetnek különösen veszélyesek, mivel az üzemzavar vagy részleges, esetleg teljes leállás súlyos következményekkel járhat egy teljes ország vagy régió gazdaságára és biztonságára nézve, tekintve, hogy egyik infrastruktúra sem értelmezhető pusztán önmagában. Az ellátási láncok digitális sérülékenysége miatt a kibertérben történő incidensek nemcsak egy célba vett vállalatot, hanem teljes iparágakat is megbéníthatnak. A zsarolóvírusok, a social engineering technikák és az ún. fejlett folyamatos fenyegetések (APT-k) már a 2000-es évek elején olyan eszközökké váltak, amelyeket állami és bűnözői csoportok egyaránt alkalmaznak geopolitikai célok elérésére. [4]

Meghatározó szükséglet a kiberbiztonság szempontjából az ellenállóképesség növelése és a megelőző védelmi stratégiák fejlesztése. A mesterséges intelligencia és a gépi tanulás új lehetőségeket kínál a védelmi oldalon is, mégpedig a fenyegetések felismerésére és semlegesítésére, ugyanakkor a kapcsolódó etikai és jogi kérdések is egyre nagyobb figyelmet kapnak. A kiberbiztonsági tudatosság növelése a szervezetek minden szintjén alapvető fontosságú, hiszen a támadások jelentős része továbbra is emberi hibák kihasználásán alapul.

Új típusú koronavírus-járvány

A 2019 végén kirobbant és Magyarországon 2020 márciusa óta jelen lévő új típusú koronavírus-járvány számos társadalmi, gazdasági, ökológiai és politikai folyamat áttervezésére nyújtott lehetőséget, valamint némelyeket ezek közül kényszerpályára segített. Nem véletlen a pozitív hangvétel, ugyanis a nemzetközi szinten jelentős hatású járvány és a kapcsolódó válsághelyzet nem csupán negatív kontextusban értelmezhető. A következő három jelentősebb területen a jelen tanulmány témája vonatkozásában előre mutató folyamatok tapasztalhatók.

A szervezetek, köztük kritikus infrastruktúrát üzemeltető vállalatok szervezetei is munkaerő-szervezési problémákkal szembesültek. A társadalmi felelősségvállalás jegyében igyekeztek az elsődleges hangsúlyt a munkavállalóik és a kiszolgált ügyfelek egészségének megőrzésére helyezni. Kreativitás és megoldás-központú gondolkodás vált azonnal szükségessé ahhoz, hogy a gazdasági élet folytatódhasson, ugyanis a szervezetek működésének alapja a munkavállalók rendelkezésre állása. Különösen igaz ez a kritikus infrastruktúrákra, ahol más szervezetekhez képest összességében a leginkább jellemző a személyes jelenlétet igénylő munkakörök túlsúlya. Bevezetésre került a biztonságos távolságtartás ipari környezetben is, a más kontextusban hosszú távon is hasznosnak bizonyuló higiéniai előírások, egyes irodai munkakörökben pedig az otthoni munkavégzés.

Áthidalandó a kényszerűségből átgondolt munkaerő-szervezési problémákat, felgyorsult a digitalizáció számos szektorban. Az eddig kevésbé hatékonynak bizonyuló törekvések az ügyfélkiszolgálás digitalizálására, valamint a papíralapú adminisztráció volumenének drasztikus csökkentésére hirtelen lehetőségből kényszerűséggé váltak. A vezető testületei átstrukturálták a tervezett költségeket, mely jelenség negatív hozadékai ellenére is a digitalizációra, ehhez kapcsolódóan pedig az információbiztonságra szánt keret növekedésében mutatkozott régóta elvárt, kismértékben javuló tendencia. [5]

Nem utolsó sorban pedig kedvező folyamatok indultak el a klímaváltozás elleni harcban, mely részben köszönhető az ipari létesítmények mérséklődő termelési volumenének, részben az otthoni munkavégzés, kijárási korlátozások és lezárások, valamint az emberek fogyasztási és főként közlekedési hajlandóságának csökkenése által vezérelt alacsonyabb károsanyag-kibocsátásnak.

A KRITIKUS INFRASTRUKTÚRÁK KOCKÁZATAI

Jelen fejezet egy SWOT-analízishez hasonló megközelítésben elemzi a kritikus infrastruktúrák külső tényezők – folyamatok, eszközök, helyzetek – által jelentett fenyegetéseit, és a belső adottságok közül a gyengeségeket, amelyeknél fogva a működésüket veszélyeztető és a védelmi rendszereket próbára tevő hatások felmerülnek. Kiemelten fókuszba kerül továbbá néhány fontos, az adatfeldolgozással és a mesterséges intelligenciával kapcsolatban felmerülő kockázat.

Kritikus infrastruktúrák fenyegetései

A kritikus információs infrastruktúrák külső fenyegetettségei érkezhetnek a fizikai, és az információs vagy virtuális dimenzióból, ezek veszélyei hatást gyakorolhatnak az infrastruktúrák működésére közvetlen és közvetett módon egyaránt. A fizikai fenyegetések közül legjelentősebb hatással a természeti katasztrófák, ipari (technikai jellegű) katasztrófák, terrorizmus és fegyveres konfliktusok. [6]

Az információs dimenzióból érkező fenyegetések mögött ugyan különböző mértékben, de minden esetben megjelenik az emberi tényező, valamint valamilyen személyes, politikai, üzleti érdek. A kibertér már a legalapvetőbb, fizikai komponense jellegénél fogva is elősegíti az ilyen érdekek érvényesítését, ti. a hálózatba kapcsolt eszközök és rendszerek közötti kommunikáció segítségével szélesebb körben biztosított az átjárás, az információhoz való hozzáférés. [7]

A klímaváltozás következtében egyes térségekben romlik az élelmiszer- és vízellátás biztonsága, ami társadalmi feszültségekhez, migrációs hullámokhoz és geopolitikai instabilitáshoz vezethet. Ezek az instabilitási tényezők fokozzák az államok és a nemzetközi szervezetek biztonsági kockázatait, különösen az energia- és vízellátás sérülékenységének növekedése miatt. Az aszályok és árvizek gyakoribbá válása komoly kihívásokat jelent a mezőgazdaság számára, ami az ellátási láncokban is fennakadásokat eredményezhet. [8]

A klímaváltozás okozta társadalmi-gazdasági változások közvetve befolyásolják a kibertér biztonságát is. A klímakatasztrófák során az infrastruktúrák sérülékenyebbé válnak, és a kibertámadások egyre gyakrabban kihasználják az ilyen válsághelyzeteket. Az energiahálózatok és közműszolgáltatások védelme kritikus jelentőségű, mivel ezek célpontjai lehetnek állami és nem állami szereplők általi kibertámadásoknak. A természeti katasztrófák és az azok nyomán fellépő kiberfenyegetések együttesen új típusú biztonsági kihívásokat

eredményeznek. Ide értendő a Covid-19 járvány leküzdése jelentette eltolódott fókusz a védelmi intézkedések kárára, amely exponenciálisan növekvő számú kibertámadás kivitelezésének adott teret. [9]

A klímaváltozás hatására a kritikus infrastruktúrák egyre nagyobb terhelésnek vannak kitéve, hiszen az extrém időjárási körülmények, például hőhullámok vagy áradások, jelentősen befolyásolják működésüket. Egyre fontosabbá válik az infrastruktúrák alkalmazkodóképességének növelése és a rugalmas, ellenálló rendszerek kialakítása. [10] Ezzel párhuzamosan azonban a digitalizáció előretörése miatt a kibertérben megjelenő fenyegetések is növekednek, amelyek célkeresztjében gyakran éppen a kritikus infrastruktúrák állnak.

Kritikus infrastruktúrák gyengeségei

A kritikus infrastruktúrák védelmében kiemelt szerepe van a humán tényezőnek, hiszen az emberi mulasztások és a nem megfelelő információbiztonsági tudatosság jelentős kockázatokat hordoz. A védelem egyik kulcseleme az infrastruktúrát üzemeltető szakemberek folyamatos képzése, az információbiztonsági protokollok betartása és az új fenyegetések felismerésének képessége. Az automatizáció és a mesterséges intelligencia szerepe is egyre növekszik, azonban ezek sem helyettesíthetik az emberi felügyeletet és a megfelelő kockázatkezelési stratégiákat. [3]

A kritikus infrastruktúrák védelmének egyik jelentős belső gyengesége az elavult technológiai rendszerek jelenléte, amelyek nem felelnek meg a modern biztonsági követelményeknek. Számos ilyen infrastruktúra még mindig régi, gyakran évtizedes hardver- és szoftvermegoldásokra épül, amelyeket eredetileg nem a jelenlegi kiberfenyegetések kivédésére terveztek. Ezek a rendszerek gyakran nem kapnak rendszeres biztonsági frissítéseket, és sok esetben olyan sérülékenységeket tartalmaznak, amelyeket a támadók könnyen kihasználhatnak. Az elavult technológia nemcsak a támadásoknak teszi ki az infrastruktúrát, hanem megnehezíti a hatékony incidenskezelést és helyreállítást is. [11]

Egy másik kritikus belső gyengeség a nem megfelelő hálózati felosztás, együtt az elkülönítés hiányával. Sok kritikus infrastruktúrában az informatikai és ipari irányítási és automatizálási rendszerek közvetlenül vagy közvetett módon kapcsolódnak a nyilvános hálózatokhoz, ami növeli a támadások kockázatát. Ha egy rosszindulatú szereplő hozzáférést szerez egy kevésbé védett rendszerelemhez, az egész hálózat kompromittálódhat, mivel a támadó könnyedén továbbterjedhet a rendszeren belül. Az elégtelen hálózati elkülönítés lehetővé teszi, hogy a támadók gyorsan kihasználják az infrastruktúra gyenge pontjait, és akár teljes szolgáltatásokat bénítsanak meg.

A kritikus infrastruktúrák további gyenge pontja a nem megfelelő incidensészlelési és válaszadási képesség. Bár egyre több szervezet alkalmaz kiberbiztonsági monitoring rendszereket, ezek sok esetben nem képesek időben azonosítani a komplex, célzott támadásokat. Az automatizált biztonsági megoldások hiánya és a fenyegetések elemzésére szolgáló eszközök korlátozott kapacitása megnehezíti az anomáliák észlelését és a gyors beavatkozást. Ennek következményeként egy támadás hosszabb ideig észrevétlen maradhat, növelve a potenciális károkat és a helyreállítás költségeit. [12]

Adatelemzés, feldolgozás és a mesterséges intelligencia közreműködése

A környezetmonitorozó szenzorok és az általuk gyűjtött adatok feldolgozásáért felelős rendszerek kibertámadásokkal szembeni sebezhetősége komoly kockázatokat hordoz,

különösen akkor, ha az adatok manipulálása nem szándékolt, akár irányelvekkel szembemenő döntésekhez vezetnek. Ha egy támadó megváltoztatja vagy hamisítja az érzékelők által mért értékeket – például a levegőminőség, vízszennyezettség, hőmérséklet vagy radioaktivitás szintjét illetően –, a döntéshozók vagy a mesterséges intelligenciával kiegészített beavatkozó rendszerek téves következtetésekre juthatnak. Ennek következtében szükségtelen vagy elégtelen válaszlépések történhetnek, például egy ipari létesítmény indokolatlan leállítása vagy egy veszélyes helyzet figyelmen kívül hagyása. Ugyancsak megemlítendő e helyen, hogy az egyes infrastruktúrák nem értelmezhetők önmagukban, önálló rendszerként, szükséges az átfogó megközelítés a hasonló problémák megoldásában.

A kibertámadások által generált hibás adatok különösen veszélyesek lehetnek olyan rendszerek esetében, amelyekben automatikus vészhelyzeti intézkedések kerültek betáplálásra. Ha például egy fejlett árvízvédelmi rendszer szenzorjai meghamisított adatok alapján tévesen érzékelnek áradást, a gátak nem tervezett módon nyílhatnak ki, ami más területeken súlyos következményekkel járhat. Hasonlóképpen, ha egy erdőtüzeket monitorozó rendszer nem érzékeli időben a tüzet egy kibertámadás miatt, a tűzoltás késedelmet szenvedhet, ami súlyosabb károkat és nagyobb emberi áldozatokat eredményezhet. Az ilyen manipulációk kritikusak az ipari és katonai rendszerek vonatkozásában, ahol a hibás döntések stratégiai következményekkel is járhatnak.

A mesterséges intelligencia (AI) alapú döntéshozatali rendszerek különösen sebezhetők közvetett módon, az adatok szándékos torzításával, mivel ezek a modellek részben előre betáplált paraméterekre, részben pedig valós időben érkező adatokra támaszkodva működnek. [13] Ha egy támadó képes meghamisítani az AI tanítására vagy működésére szolgáló adatokat, az hosszú távon is negatívan befolyásolhatja a rendszer teljesítményét, ami nem csupán egyetlen döntést, hanem az egész döntéshozatali folyamatot, valamint a társadalom biztonságérzetét és a védelmi rendszerekkel szembeni bizalmát hosszú távon veszélyezteti. [14]

HUMÁN KOCKÁZATKEZELÉSI LÉPÉSEK

Jelen fejezetben a bemutatott összefüggésekre alapozva azonosításra kerülnek a kritikus infrastruktúrák gyengeségeiből adódó, a humán tényezővel összefüggésbe hozható kockázatainak hatékony menedzselésére szolgáló eszközök, az információbiztonság eszköztárának egy e célból meghatározott módon történő csoportosítása segítségével.

Humán kockázati tényezők kezelése

A kritikus információs infrastruktúrák védelme szempontjából kiemelten fontos a humán tényezőből eredő kockázatok csökkentése. A tanulmány a már korábban is használt „humán tényező” kifejezést annak a kérdéskörnek a leírására alkalmazza, hogy az emberi mulasztás, a figyelmetlenség, valamint a szándékos károkozás jelentős kockázatot jelenthet a rendszerek biztonságára nézve. Ennek megfelelően több olyan eszköz is létezik, amely segíthet minimalizálni az emberi tényezőből adódó sérülékenységeket. Öt kulcsfontosságú intézkedést mutatok be, amelyek hatékonyan járulhatnak hozzá a kockázatok kezeléséhez.

Az első legfontosabb eszköz a folyamatos képzés és a biztonságtudatosság növelése. A munkavállalók rendszeres kiberbiztonsági oktatásban való részesítése elengedhetetlen ahhoz, hogy felismerjék és megfelelően kezeljék a különböző fenyegetéseket. A szimulációs gyakorlatok, például az adathalász támadások elleni tréningek, hozzájárulnak ahhoz,

hogy a dolgozók megtanulják az ilyen próbálkozások kiszűrését. Ezen túlmenően, a szervezeteknek olyan belső kommunikációs stratégiákat kell kialakítaniuk, amelyek folyamatosan informálják az alkalmazottakat az aktuális fenyegetésekről és a legjobb védekezési gyakorlatokról. Az információs biztonság nem egyszeri feladat, hanem folyamatos fejlődést és alkalmazkodást igénylő folyamat, ezért az oktatásnak és az érzékenyítésnek hosszú távon is prioritást kell élveznie.

A második kulcsfontosságú lépés a szigorú hozzáférés-kezelési és jogosultságkezelési rendszer bevezetése. A legkisebb jogosultság elve alapján minden alkalmazottnak kizárólag azokhoz az adatokhoz és rendszerekhez kell hozzáférést biztosítani, amelyek munkájához elengedhetetlenek. A többlépcsős hitelesítés (MFA) kötelezővé tétele jelentősen növeli a védelmet az illetéktelen hozzáférések ellen, hiszen egyetlen ellopott jelszó nem elegendő a rendszerekbe való bejutáshoz. Emellett fontos a jogosultságok rendszeres felülvizsgálata, hogy időben észlelhetők és megszüntethetők legyenek a szükségtelen vagy elavult hozzáférések. Egy jól felépített hozzáférés-kezelési rendszer segít csökkenteni annak esélyét, hogy egy kompromittált fiók vagy egy rosszindulatú belső szereplő kárt okozzon az infrastruktúrában.

A harmadik lényeges elem a belső ellenőrzési és incidensfigyelési rendszerek kiépítése, a hálózaton gyanús tevékenységeket azonosítani képes eszközökkel, amelyek folyamatosan elemzik a felhasználók viselkedését, és riasztást generálnak, ha szokatlan vagy potenciálisan veszélyes műveleteket észlelnek. A rendszeres auditok és naplóelemzések lehetővé teszik a szervezetek számára, hogy időben felfedezzék az esetleges belső fenyegetéseket vagy szabályszegéseket. Egy hatékony incidensfigyelési rendszer nemcsak a megelőzést szolgálja, hanem lehetőséget ad a gyors reagálásra is, így minimalizálva a potenciális károkat.

Negyedikként elengedhetetlen egy erős biztonsági kultúra és felelősségi rendszer kialakítása. A szervezeteknek ösztönözniük kell a dolgozókat arra, hogy aktívan vegyenek részt a biztonsági intézkedések betartásában, például azáltal, hogy jelentik a gyanús eseményeket vagy betartják az előírásokat. A szabályszegések következményeit egyértelművé kell tenni, ugyanakkor a dolgozókat pozitív ösztönzőkkel is motiválni lehet a biztonságtudatos viselkedésre. A belépési és kilépési folyamatok szigorú szabályozása biztosítja, hogy a szervezet érzékeny adatai ne kerüljenek illetéktelen kezekbe. Egy erős biztonsági kultúra hosszú távon hozzájárul a szervezet ellenállóképességének növeléséhez és a humán tényezőből fakadó kockázatok csökkentéséhez.

Egy végső kulcsfontosságú eszköz lehet a válságkezelési és ún. incidensreakciós terv kidolgozása és rendszeres tesztelése, amely részletezi azokat a lépéseket, amelyeket egy kibertámadás vagy egy súlyos biztonsági esemény bekövetkeztekor kell megtenni. Ez magában foglalja az érintett rendszerek izolálását, a károk minimalizálását, az illetékes csapatok riasztását és a helyreállítási folyamatok beindítását. Egy jól kidolgozott válságkezelési terv lehetővé teszi a károk minimalizálását és az üzletmenet gyors helyreállítását egy esetleges támadás után.

Az terv azonban önmagában nem elegendő, hanem kiegészítendő rendszeres gyakorlatokkal és szimulációkkal ahhoz, hogy minden érintett tisztában legyen a teendőivel egy valós helyzetben. A tesztelések segítenek feltárni az esetleges hiányosságokat és finomhangolni a folyamatokat, mielőtt egy éles helyzetben kellene rájuk támaszkodni. Egy jól kidolgozott és kipróbált incidenskezelési stratégia nemcsak az emberi hibákból eredő problémák

enyhítésére alkalmas, hanem az olyan külső fenyegetésekre is gyorsabb és hatékonyabb választ ad, mint a kibertámadások vagy a belső adatlopások.

Eszközök klasszifikációja

A kritikus információs infrastruktúrák védelmében a humán tényező kockázatának csökkentésére alkalmazott eszközök három fő kategóriába sorolhatók: fizikai eszközök, logikai eszközök és adminisztratív eszközök. A humán tényezőből eredő kockázatok csökkentése érdekében a fizikai, logikai és adminisztratív eszközök kombinált alkalmazása jelentősen növeli a kritikus információs infrastruktúrák védelmét, és hozzájárul a szervezet biztonsági szintjének folyamatos fejlődéséhez. [15] Az alábbiakban az előzőekben jellemzett öt kulcsfontosságú eszközt ezeknek megfelelően csoportosítva mutatjuk be.

Az információbiztonsági képzés és tudatosságnövelés az adminisztratív eszközök közé tartozik, hiszen ezek elsősorban az emberi tényezőre fókuszálnak. Az alkalmazottak rendszeres képzése segít megelőzni az olyan gyakori támadásokat, mint az adathalászat vagy a social engineering. Egy szervezet biztonsága nagyban múlik azon, hogyan tudja biztosítani, hogy az alkalmazottak képesek legyenek naprakész módon felismerni és elkerülni a potenciális fenyegetéseket.

A szigorú hozzáférés-kezelési és jogosultságkezelési rendszer részben fizikai, részben logikai eszközöket igényel. Az adatközpontokhoz, szervertermekhez és egyéb érzékeny helyiségekhez való hozzáférést fizikai biztonsági eszközökkel, például beléptető rendszerekkel, biometrikus azonosítókkal vagy intelligens belépőkártyákkal lehet szabályozni. A hozzáférési jogosultságokat nemcsak digitálisan kell felülvizsgálni, hanem a fizikai belépési jogosultságokat is rendszeresen ellenőrizni kell, különösen a távozó alkalmazottak vagy partnerek esetében.

A belső ellenőrzési és incidensfigyelési rendszerek a logikai eszközök kategóriájába tartoznak, hiszen ezek olyan szoftveres megoldásokat jelentenek, amelyek a felhasználói viselkedést és a rendszereseményeket figyelik: például elemzik a hálózat forgalmát, keresve a gyanús tevékenységeket, például a szokatlan bejelentkezéseket vagy az érzékeny adatok tömeges letöltését.

Az erős biztonsági kultúra és felelősségi rendszer kialakítása szintén adminisztratív eszköznek tekinthető. Ez nemcsak azt jelenti, hogy a szervezetnek szigorú szabályokat kell lefektetnie, hanem azt is, hogy ezek betartását folyamatosan ellenőrizni és ösztönözni kell. A biztonsági szabályszegéseknek következményei kell, hogy legyenek, ugyanakkor fontos a pozitív ösztönzés is, például a biztonságtudatos magatartás jutalmazása. Egy jól kialakított biztonsági kultúra hosszú távon hozzájárul a szervezet ellenállóképességének növeléséhez és csökkenti az emberi tényezőből fakadó kockázatokat.

Végül, a válságkezelési és incidensreakciós terv kidolgozása és tesztelése egy másik kulcsfontosságú adminisztratív eszköz, megfelelő dokumentáció és rendszeres frissítés kapcsolódik hozzá. Elengedhetetlen az érintettek folyamatos felkészítése a szimulációs gyakorlatokkal, ennek megszervezése erősíti az adminisztratív jelleget.

ÖSSZEGZÉS

A tanulmány rövid áttekintést nyújt a kritikus információs infrastruktúrákról, azonosítva főbb fenyegetéseiket és gyengeségeiket a 21. század globális kihívásainak, különösen a kibertér aktuális trendjeinek tükrében. A fókusz a humán kockázatok bemutatására,

valamint az ezeket leghatékonyabb módon kezelő módszerekre, szervezeti legjobb gyakorlatokra tevődik. Az e körbe tartozó eszközök, folyamatok és módszerek végezetül az információbiztonság eszköztárának egy meghatározott szempontjából csoportosításra kerülnek. Ez az áttekintés és elemzés feltárja a lehetőséget, hogy a kritikus információs infrastruktúrákat egymással kölcsönhatásban, a tágabb társadalombiztonsági összefüggések fényében értelmezhessék a humán kockázatokat górcső alá vevő további biztonságtudományi kutatások.

FELHASZNÁLT IRODALOM

[1] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. https://njt.hu/jogszabaly/2012-166-00-00.12 (Elérés: 2025.02.14.)

[2] Zöld Könyv a kritikus infrastruktúrák védelem európai programjáról. (Előterjesztette a Bizottság). Európai Közösségek Bizottsága, Brüsszel, 2005. 11. 17.

[3] Bleszity J., et al., "Műszaki kutatások és hatékony kormányzás." *Hadmérnök* vol. 11. no. 3, 2016, pp. 221-242.

[4] Németh Z., Völgyi Z. "A kritikus információs infrastruktúra védelem pszichológiai szempontú megközelítése: Humán biztonsági kockázatelemzés", *Hadtudományi Szemle* vol. 11, no. 3, 2018, pp. 324-337.

[5] Jenei Sz., Módosné Szalai Sz. "A digitális átalakulás és a koronavírus járvány hatásai a munkaerőpiacon." *Új Munkaügyi Szemle* vol. 3, no. 2, 2022, pp. 2-12.

[6] Muha L., *A kritikus információs infrastruktúrák védelme,* Budapest: RelNet, 2015

[7] Haig Zs., *Információs műveletek a kibertérben*, Budapest: Dialóg Campus, 2018

[8] Földi L., "A klímaváltozás által jelentkező új kihívások a kritikus infrastruktúra védelmében." in: *Báthy Sándor [et al.], Ed., Fejezetek a kritikus infrastruktúra védelemből: Kiemelten a közlekedési alrendszer.,* Budapest: Magyar Hadtudományi Társaság, 2013, pp. 268-280.

[9] J. Chigada, R. Madzinga, „Cyberattacks and threats during COVID-19: A systematic literature review.” *South African Journal of Information Management*, vol. 23, no. 1, 2021, pp. 1-11. doi: 10.4102/sajim.v23i1.1277

[10] Horváth A., „A kritikus infrastruktúra védelem komplex értelmezésének szükségessége.” in: *Horváth A., Ed.: Fejezetek a kritikus infrastruktúra védelemből–Kiemelten a közlekedési alrendszer,* Magyar Hadtudományi Társaság, Budapest, 2013, pp. 18-37.

[11] Kralovánszky K., „A villamosenergia-rendszer kiber- és nemzetbiztonsági kockázatai (1. rész).” *Nemzetbiztonsági Szemle (Online),* vol. 7, no. 3, 2019, pp. 40-57, doi: 10.32561/nsz.2019.3.4 (Elérés: 2025.02.14.)

[12] Nagy R., "A klímaváltozás hatása a kritikus infrastruktúrák védelmére." *Nemzet és Biztonság, Biztonságpolitikai Szemle,* vol. 3, no. 2, 2010

[13] Kollár Cs., „A mesterséges intelligencia kapcsolata a humán biztonsággal” *Nemzetbiztonsági Szemle (Online)* vol. 6, no. 1, 2018, pp. 5-23, https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1508 (Elérés: 2025.02.14.)

[14] Kollár Cs., „A mesterséges intelligencia és a kapcsolódó technológiák bemutatása a biztonságtudomány fókuszában” In: Rajnai Z., Ed., *Kiberbiztonság – Cybersecurity 2.*,

Budapest, Magyarország: Óbudai Egyetem, Biztonságtudományi Doktori Iskola, 2019, pp. 47-61.

[15] Kárász B., „Analysis Possibilities of the Toolset of Information Security.” *Biztonságtudományi Szemle,* vol. 7, no. 1, 2025