DOI: https://doi.org/10.12700/btsz.2025.7.2.57

CRITICAL INFRASTRUCTURE FACILITY PROTECTION CHALLENGES IN THE CONTEXT OF SOCIAL ENGINEERING ATTACKS

KRITIKUS INFRASTRUKTÚRÁK OBJEKTUMVÉDELMÉNEK KIHÍVÁSAI A SOCIAL ENGINEERING TÁMADÁSOK KONTEXTUSÁBAN

MÁRTON Zoltán [1] – RAJNAI Zoltán[2] – BEREK Lajos[3]

Abstract

Critical infrastructure facilities face growing threats from social engineering attacks that exploit human behavior. This article explores how psychological manipulation endangers physical security in sectors such as energy, transport, and healthcare. A STEAM-based, interdisciplinary approach is proposed, combining scientific, technological, engineering, artistic, and mathematical elements to enhance resilience. The study highlights gamified and adaptive training methods as effective tools for strengthening security culture. Recent cases and literature (post-2020) demonstrate how phishing, impersonation, and the AI-powered „deepfakes" can be countered by integrating technology with improved human preparedness.

Keywords

social engineering; critical infrastructure; facility protection; STEAM; gamification

Absztrakt

A kritikus infrastruktúrák egyre nagyobb veszélynek vannak kitéve a social engineering támadások révén, amelyek az emberi viselkedést használják ki. A cikk bemutatja, miként veszélyezteti a pszichológiai manipuláció a fizikai biztonságot az energetikai, közlekedési és egészségügyi szektorban. STEAM-alapú, interdiszciplináris megközelítést javasolunk, amely ötvözi a tudományos, technológiai, mérnöki, művészeti és matematikai elemeket a reziliencia növelése érdekében. A kutatás kiemeli a játékosított és adaptív képzések szerepét a biztonsági kultúra erősítésében. Friss esetek és szakirodalmak igazolják, hogy a phishing, megszemélyesítés és az MI-alapú „deepfake" technikák hatékonyan kivédhetők a technológiai és humán védelem együttes alkalmazásával.

Kulcsszavak

social engineering; kritikus infrastruktúra; objektumvédelem; STEAM; játékosítás

[1] marton.zoltan@uni-obuda.hu | ORCID: 0009-0006-7795-076X| PhD Student, Doctoral School on Safety and Security Sciences Óbuda University | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] rajnai.zoltan@bgk.uni-obuda.hu | ORCID: 0000-0002-9139-736X | full professor, Óbuda University, Bánki Donát Faculty of Mechanical and Safety Engineering | egyetemi tanár, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

[3] berek.lajos@bgk.uni-obuda.hu| ORCID: 0000-0003-1705-1173| professor emiritus, Óbuda University, Bánki Donát Faculty of Mechanical and Safety Engineering | professzor emiritus, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

BEVEZETÉS

A kritikus infrastruktúrák – ahogyan az energiatermelő létesítmények, közlekedési hálózatok irányító központjai vagy kórházak – védelme kiemelt fontosságú nemzetbiztonsági és társadalmi érdek. E létesítmények objektumvédelme hagyományosan a fizikai biztonsági rendszerekre (kerítések, beléptető rendszerek, videó megfigyelő rendszerek) és az informatikai védelemre egyaránt támaszkodik. Az utóbbi években azonban egyre nyilvánvalóbbá vált, hogy a legmodernebb technológiai védelem is sebezhető, amennyiben a támadók az emberi tényezőt veszik célba [1], [2]. A social engineering, vagyis a pszichológiai manipuláció eszköztárával a támadó nem a zárt ajtókat próbálja feltörni vagy a tűzfalakat megkerülni, hanem megkeresi a „gyenge láncszemet" jelentő alkalmazottat vagy biztonsági őrt, és manipulációval ráveszi a védelmi protokoll megsértésére. E módszer lényege, hogy **az emberi hibát és viselkedést kihasználva próbál hozzáférést szerezni védett információkhoz, rendszerekhez vagy létesítményekhez**, sokszor a megtévesztés kifinomult formáit alkalmazva [1].

A digitalizáció és a hálózatba kapcsoltság növekedésével a social engineering támadások száma és kifinomultsága is emelkedik világszerte [3]. A támadók gyakran összehangoltan alkalmazzák a kibertérben és a fizikai térben végrehajtott behatolási technikákat: egy jól megszerkesztett adathalász (phishing) e-maillel jutnak be egy erőmű vezérlőrendszerének hálózatába, vagy egy hamis karbantartónak adva ki magukat személyesen próbálnak belépni egy védett objektumba.

A kritikus infrastruktúrák ellen irányuló kibertámadások jelentős része indul valamilyen **social engineering módszerrel**, különösen adathalászattal vagy illetéktelen hozzáférési adatok megszerzésével [3]. Az Egyesült Államok kiberbiztonsági hatóságainak 2023-as kockázatértékelési jelentése (Risk and Vulnerability Assessment Analysis – RVAA) szerint a sikeres behatolások 40%-ában kompromittált, de legitim felhasználói fiókokat használtak ki (akár ellopott hitelesítési adatok révén), míg a második leggyakoribb módszer célzott adathalász link alkalmazása volt, az incidensek több mint 25%-ában [11]. A Cybersecurity Dive szakmai beszámolója szerint e jelentés megállapításai rámutatnak arra, hogy a humán kockázatok megfelelő kezelése nélkülözhetetlen a létfontosságú rendszerelemek védelmében [3].

A social engineering támadások nemcsak a kibertérben, hanem a fizikai világban is megjelennek. A hagyományos objektumvédelmi intézkedések – beleértve az épületőrzést, a beléptetést és a járőrszolgálatot – nem nyújtanak megfelelő védelmet, ha egy támadó pszichológiai manipulációval ráveszi a személyzetet a biztonsági eljárások kijátszására. Ilyen lehet, amikor egy támadó **idegenként bejut egy védett létesítménybe úgy, hogy** az ajtónál várakozva egyszerűen bemondja, hogy *„Hoztam a megrendelt eszközöket a szerverkarbantartáshoz"* – és a jóhiszemű biztonsági őr beengedi.

Számos beszámoló és esettanulmány igazolja, hogy még a szigorúan védett objektumokba is be lehet jutni megtévesztéssel. **Kowalski (2022) tanulmánya** kimutatta, hogy a tailgating – azaz egy jogosult személy nyomában történő illetéktelen belépés – a magas biztonságú környezetekben is komoly fenyegetést jelent [10]. E megállapítást gyakorlati tesztek is alátámasztják, többek között **az amerikai kormányzati RVAA jelentés** 2023-as kiadása, amely szerint számos fizikai behatolási kísérlet sikeres volt a humán tényező kihasználásával [11]. A támadók gyakran viselnek hivatalosnak tűnő egyenruhát vagy kitűzőt,

magabiztosan viselkednek, és kihasználják az emberi udvariasságot vagy az esetleges rutinokat a beléptetésnél. Az ilyen támadások sikeressége rávilágít arra, hogy a fizikai biztonság és a humán tényező szorosan összefügg: a **technikai biztonsági berendezések** (pl. beléptető kapuk, biometrikus azonosítók) csak addig hatékonyak, amíg az ember nem kapcsolja ki őket vagy nem hoz rossz döntést.

Mindezek fényében egyre hangsúlyosabbá vált az igény egy **holisztikus, interdiszciplináris megközelítésre** a kritikus infrastruktúrák védelmében. A STEAM[4] alapú szemlélet – amely a természettudományosés a műszaki tudást, a művészetek és a kreatív pedagógiai módszerekkel ötvözi – új perspektívát kínál a biztonságtudatosság növelésében. Jelen cikk célja, hogy a korábbiaktól eltérő koncepcionális keretben tárgyalja a kritikus infrastruktúrák objektumvédelmének és a social engineering fenyegetéseknek a metszéspontját. A fókusz az emberi tényező megerősítésén van: bemutatjuk, miként integrálható a STEAM szemlélet a biztonsági képzésbe, és hogyan tehetők ellenállóbbá a szervezetek a manipulációval szemben játékosított, adaptív képzési megoldások révén. A következőkben áttekintjük a legújabb social engineering módszereket és trendeket a kritikus szektorokban, majd ismertetjük az ezekkel szembeni lehetséges védekezési stratégiákat, különös tekintettel a humán kockázatok csökkentésére.

SOCIAL ENGINEERING FENYEGETÉSEK A KRITIKUS INFRASTRUKTÚRÁK ELLEN

A kritikus infrastruktúrák elleni social engineering támadások rendkívül sokfélék lehetnek, az egyszerű megtévesztéstől a komplex, több lépcsős, kifinomult módszerekig. Közös bennük, hogy a támadó a védelmi rendszerek **az emberi tényezőt, elsősorban az üzemeltetőket és felhasználókat veszi célba** és rajtuk keresztül próbál meg kárt okozni vagy hozzáférést szerezni. Az alábbiakban áttekintjük, hogyan jelennek meg a social engineering jellegű fenyegetések négy fő dimenzióban: az energetikai, közlekedési és egészségügyi ágazatokban; az új technológiai eszközök – mesterséges intelligencia (továbbiakban: MI) alkalmazásában; valamint a korábban ismert, klasszikus megtévesztési módszerek viszszatérésében.

Energetikai létesítmények

Az energiatermelő és -elosztó rendszerek (erőművek, elektromos hálózatok vezérlő központjai) kiemelt célpontjai a nemzetállami és bűnözői csoportoknak. Gyakori módszer a „**spear phishing"**[5] alkalmazása, amikor az erőmű dolgozóit célzott, hitelesnek tűnő e-mailekkel veszik célba. Ezek az üzenetek sokszor sürgős műszaki problémára hivatkoznak vagy valamilyen utasítást tartalmaznak, amelyre a dolgozó automatikusan reagálni akar.

2021-ben az energiaszektor a kibertámadások egyik leggyakoribb célpontja volt az Egyesült Királyságban, az összes támadás 24%-át ez a szektor szenvedte el, és számos esetben a támadók adathalász e-mailekkel jutottak be a hálózatba [4]. A „**spear phishing"** le-

[4] az angol Science, Technology, Engineering, Arts, and Mathematics (tudomány, technológia, mérnöki tudományok, művészetek és matematika) szavak kezdőbetűiből álló mozaikszó, amely az oktatásban ezeket a területeket integráltan kezeli a kreatív és problémamegoldó gondolkodás fejlesztése érdekében.

[5] célzott adathalászati módszer, amely során a támadó személyre szabott, hitelesnek tűnő üzenetekkel próbálja rávenni az áldozatot bizalmas információk kiadására vagy rosszindulatú fájl megnyitására.

hetővé teheti, hogy a behatoló megszerezze egy mérnök belépési adatait, majd azokkal távolról bejelentkezve átvegye az irányítást egyes rendszerek felett, vagy káros szoftvert (pl. zsarolóprogramot) juttasson a hálózatba.

Emellett fizikai social engineering is veszélyt jelent: ismert eset, hogy egy támadó **külső karbantartónak kiadva magát** próbált bejutni egy vízerőmű gépházába, hamis megbízólevelekkel és egyenruhában. Amennyiben a személyzet nincs kellően felkészítve az ilyen helyzetek felismerésére, az objektumvédelmi protokoll könnyen kijátszható.

Közlekedési rendszerek

A légiközlekedés, vasúti hálózatok, városi tömegközlekedés irányító rendszerei egyre inkább automatizáltak és hálózatba kötöttek, ugyanakkor emberek üzemeltetik és felügyelik őket. A támadók kihasználhatják, hogy ezen szervezeteknél is sok múlik a diszpécserek, forgalomirányítók, karbantartók éberségén.

Előfordulhat, hogy egy vasúti társaság informatikusának **telefonos átverésével („vishing" [6])** szereznek meg hozzáférést a belső hálózathoz: a támadó a telefonban a cég egyik beszállítójának IT-támogató mérnökének adja ki magát, és azt állítja, sürgősen szüksége van egy adminisztrátori jelszóra egy "rendszerhiba" elhárításához. Ha a megtévesztett alkalmazott kiadja a jelszót, a támadó azonnal beléphet a rendszerbe és megnyithatja az utat további támadásokhoz. A közlekedési ágazatban a **fizikai social engineering** is fenyeget: repülőtereken vagy vasúti csomópontokban gyakran dolgoznak külsős vállalkozók, beszállítók. Egy támadó egy hamis szállítói azonosító kártyával megpróbálhat behajtani a repülőtér védett területére arra hivatkozva, hogy árut hozott.

2019-ben a londoni Heathrow repülőtéren történt biztonsági incidens során kiderült, hogy a protokollok figyelmen kívül hagyása (egy USB eszköz engedély nélküli használata) és a dolgozók megtévesztése jelentős szerepet játszott a védelmi rendszer kijátszásában . Bár ez az eset korábbi, jól szemlélteti, hogy a közlekedési infrastruktúrákban is számolni kell az emberi tényezőből fakadó résekkel [2].

Egészségügyi szektor

A kórházak és egészségügyi létesítmények kritikus fontosságú adatokkal (betegek egészségügyi adatai) és berendezésekkel (életfenntartó rendszerek, gyógyszeradagolók) rendelkeznek, amelyek kiesése emberéleteket veszélyeztethet. Az egészségügy sajnos gyakran célpontja **zsarólóvírus (**azaz ransomware**)** támadásoknak is, melyek sokszor social engineeringgel kezdődnek. A támadó e-mailben küldhet egy fertőzött dokumentumot a kórházi pénzügynek, mely látszólag egy beszállítói számla – a dokumentum megnyitásával a kártevő települ és titkosítja a rendszereket. Ezen túl a „**vishing"** is megjelent ebben a szektorban: 2022 óta egy **Scattered Spider** néven ismert hackercsoport kifejezetten híressé vált arról, hogy **telefonon hívja fel az egészségügyi intézmények dolgozóit**, és az MI segítségével más személy (adott esetben egy vezető) hangján beszél, hogy érzékeny adatokat vagy hozzáférést szerezzen [5]. Az Amerikai Egészségügyi és Emberi Szolgáltatások Minisztériumának 2024-es figyelmeztetése szerint ez a csoport **MI-alapú hangklónozást** vetett be, hogy a célpont szervezeteknél az elsődleges hozzáférést megszerezze [5].

[6] (voice phishing) olyan megtévesztési technika, amely során a támadó telefonhíváson keresztül próbál bizalmas információkat kicsalni az áldozattól, például úgy, hogy hivatalos személynek (pl. rendszergazda, vezető) adja ki magát.

Egy ilyen támadás során a kórház informatikusa kaphat egy hívást a főigazgató "hangján", aki utasítja, hogy sürgősen adjon távoli hozzáférést egy külső szakértőnek – ha az informatikus nem elég óvatos, könnyen engedélyezhet egy támadónak hozzáférést a hálózathoz, nem is sejtve, hogy átverték.

Az egészségügyben a **fizikai social engineering** is jelen van: színlelt betegek, csalók próbálhatnak meg bejutni korlátozott területekre (gyógyszerraktár, szerverközpont) egy kórházban. Amennyiben a biztonsági protokollokat nem tartják be – ha egy támadó másolt belépőkártyával vagy csupán fehér köpenyt viselve követi az orvosokat egy védett területre –, az objektumvédelem működése meghiúsulhat.

Új technológiák a social engineering szolgálatában

A fenti szektorok mindegyikében megfigyelhető, hogy a támadók egyre gyakrabban alkalmaznak **új technológiákat** a megtévesztés hatékonyságának növelésére. Az MI térhódítása új dimenziót ad a social engineeringnek.

A generatív MI modellek, mint amilyen a ChatGPT, képesek olyan meggyőző adathalász üzeneteket írni, amelyek nyelvtanilag és stilisztikailag is kifogástalanok [1]. Míg korábban a gyanús e-maileken gyakran lehetett érezni, hogy nem anyanyelvi író tollából származnak (helyesírási hibák, furcsa megfogalmazások jelezték), addig ma már egy MI által generált szöveg professzionálisnak tűnhet.

Ez megnehezíti a felhasználók számára a támadói e-mailek felismerését. Továbbá a „**deepfake"** technológia – legyen szó **hamis hangokról vagy videókról** – kezd gyakorlati eszközzé válni a kiberbűnözésben. Ahogy arra hazai szakértők is rámutattak, a közösségi médiában hozzáférhető hang- és videóanyagok alapján bárkiről készíthető olyan hamis felvétel, amely első hallásra/látásra megtévesztő lehet [1].

Bár jelenleg a valós idejű, teljesen hihető „deepfake" videók előállítása még technológiai kihívás, a fejlődés gyors, és a jövőben az MI által támogatott social engineering támadások további emelkedésére számíthatunk [1]. A gyakorlatban ez azt jelentheti, hogy egy kritikus infrastruktúra üzemeltetője, egy videóhívás során azt hiheti, a jól ismert beszállítójával egyeztet, miközben valójában egy támadó generált avatárja kéri tőle a hozzáférési kódokat [8].

Hagyományos manipulációs technikák a fizikai térben

A pandémia alatt előtérbe került online támadások mellett újra felbukkannak a fizikai világban megvalósuló social engineering módszerek. A Nemzeti Kibervédelmi Intézet 2024-es jelentése szerint ismét gyakoribbá váltak az **"elhagyott" fertőzött USB pendrive-okkal végrehajtott támadások**, ahol a támadó a céges parkolóban elejt egy pendrive-ot abban bízva, hogy egy alkalmazott megtalálja és a kíváncsiságtól vezérelve a munkahelyi gépére csatlakoztatja azt [1]. Szintén említik a hamis QR-kódok terjesztését: plakátokra vagy épületen belül elhelyezve olyan QR matricákat ragasztanak ki, amelyek egy belső szabályzatra vagy ebédlői menüre hivatkoznak, de valójában egy adathalász weboldalra vezetnek [1]. Ezek a módszerek mind arra alapoznak, hogy a legfejlettebb technológiai védelmi rendszereket is meg lehet kerülni, ha az emberi kíváncsiságot, segítőkészséget vagy figyelmetlenséget kihasználják.

Összességében látható, hogy a social engineering támadások a kritikus infrastruktúrák mindhárom vizsgált területén komoly fenyegetést jelentenek. A támadási módszerek

folyamatosan bővülnek: a **klasszikus pszichológiai trükkök** (sürgetés, tekintélyre hivatkozás, bizalmi viszony kialakítása) mellé felsorakoztak a **korszerű technológiai eszközök** (MI, „deepfake") a megtévesztés hatékonyságának növelésére.

Mindez indokolja, hogy a kritikus infrastruktúrák védelmét ne csak technikai és procedurális oldalról közelítsük meg, hanem a humán tényezőre és annak fejlesztésére kiemelt figyelmet fordítsunk. A következő fejezetben azt tekintjük át, milyen stratégiák segíthetnek a social engineering jellegű fenyegetések mérséklésében, és hogyan integrálható egy interdiszciplináris (STEAM) szemlélet ezekbe a stratégiákba.

VÉDEKEZÉSI STRATÉGIÁK: TECHNOLÓGIA, EMBERI TÉNYEZŐ ÉS STEAM-ALAPÚ SZEMLÉLET

A kritikus infrastruktúrák védelmében a **hagyományos biztonsági megközelítések** a következő pillérekre támaszkodnak: (1) **technológiai védelmi megoldások** – ilyenek a tűzfalak, a behatolásészlelő rendszerek, a fizikai beléptető kapuk, a behatolásvédelmi rendszerk is.; (2) **szervezeti protokollok és eljárások** – biztonsági szabályzatok, hozzáférési jogosultságok szigorú kezelése, kétfaktoros hitelesítés előírása, látogatói kísérés és azonosítás; (3) **humán tényező** – a személyzet képzettsége, ébersége és biztonságtudatossága. Egy valóban hatékony védelmi rendszer e három elem összehangolt működésére épül.

Az utóbbi évek támadási trendjei azonban rámutattak, hogy a **humán faktor megerősítése** terén vannak a legnagyobb hiányosságok [3]. Hiába kiváló a technológiai pajzs, ha a kezelő „lyukat üt rajta" – tételezzük fel, hogy leírja a jelszavát egy cetlire, vagy gondolkodás nélkül rákattint egy ismeretlen linkre.

A védekezési stratégiák kulcsa **a technikai, szervezeti és humán biztonsági intézkedések összehangolt alkalmazása**. Ennek részeként kiemelt jelentősége van azoknak a technológiai megoldásoknak, amelyek képesek minimalizálni az emberi hibalehetőséget.

Erős azonosítás és jogosultságkezelés

Minden kritikus rendszerhez többlépcsős (két- vagy többfaktoros) hitelesítés szükséges, így ha egy alkalmazott véletlenül kiadná is a jelszavát egy támadónak, önmagában azzal ne lehessen bejutni. A jogosultságokat ráadásul a minimálisan szükséges szintre kell korlátozni (legkisebb jogosultság elve) [12] hogy egy esetleg kompromittált fiókkal se lehessen bármit elérni.

Rendellenesség alapú behatolás érzékelő rendszerek [13]

A hálózatban szokatlan viselkedést detektáló szoftverek (akár egy alkalmazott belép éjjel egy rendszerbe, amit amúgy sosem használ – ez lehet egy támadó) figyelmeztetést adhatnak, még mielőtt nagyobb baj történne. Emellett a fizikai biztonságban is vannak hasonló eszközök, hiszen az okoskamerák, amelyek MI-vel felismerhetik, ha valaki egy ajtó mögött átsurran a jogosult személy mellett.

Beépített biztonság („Secure by Design") elvek

Olyan rendszerek és folyamatok tervezése, amelyek alapból számolnak az emberi tényező gyengeségével. A vezérlőtermek ilyeneek, ahol a belépést úgy lehet kialakítani, hogy mindig két személy együttes jelenléte kelljen (négy szem elve) [14], így egy embert sokkal nehezebb manipulálni, ha a másik is ott van és figyel.

Ezek az intézkedések fontosak, de önmagukban nem elegendőek. A social engineering ellen a **szervezeti kultúra** fejlesztése és az emberek folyamatos képzése a leghatékonyabb fegyver [4], [9]. Itt lép be az **interdiszciplináris szemlélet** fontossága. A humán viselkedés megértése és befolyásolása ugyanis nem pusztán informatikai vagy biztonságtechnikai kérdés, hanem **pszichológiai, sőt pedagógiai feladat** is. A STEAM megközelítés integrálása lehetővé teszi, hogy a biztonsági képzési programokat és eljárásrendeket célszerű komplexebb, rugalmasabb formában kialakítani:

Tudományos (Science) alapok

A döntéshozatal és az emberi tényező kutatása – így a kognitív torzítások, a megtévesztés pszichológiája – tudományos megalapozást ad ahhoz, hogy felismerjük, miért dőlnek be az emberek a trükköknek. A biztonsági képzésekbe szükségszerű beépíteni ezen ismereteket, hogy a dolgozók megértsék a saját sebezhetőségüket (többek között, hogy miért hajlamosak engedelmeskedni egy látszólagos felettes utasításának, vagy miért kattintanak rá impulzívan egy sürgősnek tűnő e-mailre).

Technológiai és Mérnöki (Technology, Engineering) megoldások

A védelmi rendszerek tervezésekor a mérnöki gondolkodás és a technológiai innováció segíthet minimalizálni a social engineering kockázatát. A hozzáférési rendszerek terén a **"zero trust"** elv alkalmazása – azaz soha senkiben nem bízunk meg implicit módon, még a belső hálózatban sem – technológiai kontrollokat eredményez (állandó hitelesítés, hálózati szegmentáció), amelyek csökkentik egy sikeres social engineering támadás mozgásterét.

Ugyanakkor a mérnöki szemlélet abban is segít, hogy a humán védelmi elemeket (folyamatok, képzések) éppoly gondos tervezéssel kezeljük, mint a szoftvereket vagy gépeket.

Művészetek (Arts) és kreatív módszerek

A képzések és tudatosságnövelő programok hatékonyságát nagymértékben növelhetik a kreatív, élményalapú elemek. Ide tartozik a **gamifikáció** (játékosítás) – a következő fejezet e kérdéskört részletesen tárgyalja –, valamint a szemléltető gyakorlatok, szimulációk, történetmesélés. A művészetek bevonása alatt érthetjük a **színészek bevonását szituációs gyakorlatokba** (eljátszanak egy támadót és egy megtévesztett alkalmazottat, amit a dolgozók együtt elemeznek ki), vagy akár egy képzőművészeti kampányt a szervezeten belül (plakátverseny a legötletesebb „Ne engedd be az idegent!" üzenetre). Az ilyen kreatív megközelítés segít abban, hogy a biztonságtudatosság mélyebb élménnyé váljon, ne csak egy kötelező oktatás legyen.

Matematika és adatelemzés (Mathematics)

A modern szervezetek rengeteg adatot tudnak gyűjteni a biztonsági eseményekről és a dolgozók viselkedéséről – kiemelve egyet: hányan kattintottak egy próba-phishing e-mailre. Ezen adatok elemzése kvantitatív alapot ad a képzés fejlesztéséhez. A statisztikai kiértékelés megmutathatja, mely területeken vannak „**vakfoltok"** a szervezetben – ha a pénzügyi osztály sokkal gyakrabban esik áldozatul adathalász teszteknek, akkor ott célzottabb oktatás kell. A matematika tehát a **mérhetőség** és a folyamatos visszacsatolás miatt fontos: rendszeres riportokkal, metrikákkal lehet követni a biztonságtudatosság fejlődését vagy épp romlását, és ennek alapján finomhangolni a programokat.

Látható, hogy a STEAM megközelítés nem valami különálló, idegen elem a biztonságtudományban, hanem sokkal inkább egy **keretrendszer**, amely emlékeztet bennünket arra, hogy a komplex problémák – mint a kritikus infrastruktúrák védelme a social engineering ellen – komplex megoldásokat igényelnek. A mérnöki-technikai megoldások és az emberi viselkedésformálás nem egymást kizáró, hanem egymást kiegészítő tényezők. Egy atomerőmű védelmi vezetőjének éppúgy értenie kell a fizikai védelem technológiájához, mint ahhoz, hogyan lehet megtanítani az ott dolgozóknak, hogy soha ne engedjenek be kíséret nélkül senkit a vezérlőterembe. E szemlélet jegyében a következő alfejezetben részletesen foglalkozunk a **humán tényező fejlesztésének** egyik legígéretesebb modern eszközével: a játékosított, adaptív képzési programok révén, amelyek jelentősen növelhetik a dolgozók biztonságtudatosságát és rezilienciáját.

JÁTÉKOSÍTOTT ÉS ADAPTÍV KÉPZÉSMEGOLDÁSOK A HUMÁN ELLENÁLLÓKÉPESSÉG NÖVELÉSÉRE

A humán kockázatok csökkentésének leghatásosabb módja, ha a szervezet minden tagja – a biztonsági őrtől az informatikuson át a felső vezetésig – **tudatában van a social engineering veszélyeinek**, ismeri a támadók módszereit, és begyakorolta a helyes reakciókat. A hagyományos oktatások (évente egyszer egy biztonságtudatossági oktatás, hosszú előadásokkal vagy szöveges tananyagokkal) sajnos sokszor kevéssé hatékonyak: unalmasak, nem ragadják meg a figyelmet, és így a tanultak rövid idő alatt elhalványulnak.

Ezzel szemben a **játékosított (gamifikált) oktatás** az utóbbi években ígéretes alternatívaként jelentek meg a biztonsági képzések terén [4], [6]. A gamifikáció lényege, hogy a tanulási folyamatba **játékmechanizmusokat** építünk be – melynek központi elemei az pontgyűjtés, a verseny, a jutalmak, és a történetvezérelt küldetések– ezáltal növeljük a résztvevők motivációját és elköteleződését.

Egy **játékosított kiberbiztonsági oktatás** során a dolgozók nem pusztán passzív befogadói az információnak, hanem aktív résztvevők, akik döntéseket hoznak, problémákat oldanak meg és azonnali visszajelzést kapnak a tetteik következményéről.

Kialakítható egy „Cybersecurity Challenge" játék a szervezeten belül: a résztvevők különböző szinteken mennek keresztül, ahol fiktív szcenáriókban kell felismerniük a támadási próbálkozásokat. Az egyik pályán az e-mailek között kell kiszűrni a phishing kísérletet, a másikon egy látogatót kell helyesen protokoll szerint kezelni (udvariasan, de határozottan azonosítani és kísérni). Minden jó döntésért pont jár, a hibákért pontlevonás. A végén ranglista készül, a legjobbak elismerést kapnak. Az ilyen barátságos versengés növeli a részvételi kedvet – hiszen a játékban való jó szereplés belső motivációt jelent – és közben észrevétlenül tanít [4].

Kutatások igazolják, hogy a gamifikált megközelítés javítja a tanulási eredményeket: egy 2024-ben publikált tanulmányban [15] az energiagazdálkodási szektor okoshálózati (smart grid) üzemeltetői számára fejlesztett játékos oktatóprogram 29–40%-kal növelte a résztvevők kvízpontszámait három nehézségi szinten, jelezve a tudatosság és ismeretek jelentős bővülését [4].

A gamifikáció mellett egyre nagyobb hangsúlyt kap az **adaptív (személyre szabott) tanulás** a biztonsági oktatásban. Ez azt jelenti, hogy a képzési rendszer figyeli a résztvevők teljesítményét és reakcióit, és ennek alapján alakítja a további tartalmat az egyén igényeihez.

Példa: A dolgozó sorozatosan hibázik a phishing e-mailek felismerésében, akkor számára több olyan gyakorló feladatot ad a rendszer, ami ezen a területen segíti a fejlődést. Ugyanakkor, aki már jártas benne, annak nem pazarolja az idejét ismétlődő alapfeladatokkal, hanem tovább lép egy haladóbb szintre.

Az adaptivitást gyakran **MI algoritmusok** támogatják, amelyek elemzik a felhasználók interakcióit. A modern digitális oktatási platformok lehetővé teszik azt is, hogy **részletes metrikákat** gyűjtsenek a tanulókról: mennyi idő alatt válaszolnak, hányszor tévesztenek, mely kérdést hányszor néznek vissza. Egy magyar fejlesztésű, játékosított kiberbiztonsági oktatási rendszer (Cyber Drill Studio) tapasztalatai szerint a résztvevők tanulási folyamatáról gyűjtött adatok elemzése révén pontosan beazonosíthatók a problémás területek, és ennek alapján a képzési tartalom módosítható az adott szervezet és az egyének igényeihez illeszkedően [7]. Ily módon az oktatás folyamatosan fejlődik a visszajelzések alapján, és az egyének is testre szabott támogatást kapnak, akárcsak egy magántanártól – csak épp digitális formában.

A játékosítás és az adaptivitás ötvözése különösen hatékony: a résztvevők élvezettel tanulnak és versengenek, miközben a rendszer **automatikusan igazodik** a tudásszintjükhöz és tanulási tempójukhoz. Ez a megközelítés áthidalja az unalmas kötelező oktatás és a valós kihívások közti szakadékot. A dolgozók „biztonsági szimulátorban" gyakorolhatnak, akár ismétlődően is, kockázatmentesen hibázhatnak és tanulhatnak a hibákból. Egy jól kidolgozott képzési program **élménnyé teszi a tanulást** – a résztvevők szinte észre sem veszik, hogy épp egy biztonsági protokollt sajátítanak el, mert leköti őket a játék vagy a történet. Ráadásul a játékban szerzett pozitív élmények révén a biztonsági előírások betartása nem kényszernek fog tűnni számukra, hanem belső igénnyé válhat, hiszen saját sikerük kapcsolódik hozzá.

Számos gyakorlati példa létezik már az ilyen képzésekre. Több nagy nemzetközi vállalat alkalmaz **„cybersecurity escape room"** gyakorlatokat, ahol a csapatoknak különféle biztonsági rejtvényeket kell megoldaniuk egy szimulált kiber-incidens során, hogy „kiszabaduljanak" – ez egyszerre épít csapatmunkára és tanít meg konkrét eljárásokat. Magyarországon is volt példa kreatív megoldásokra: egy bank belső biztonsági kampánya keretében interaktív videósorozat készült, melyben a dolgozók maguk választhatták meg, hogyan reagál a főhős egy social engineering helyzetben, és a történet a döntéseik szerint alakult tovább. Az ilyen **interaktív oktatóanyagok** bevonják a nézőt és személyes élménnyé teszik a tanulságokat.

Természetesen a játékosított képzések is megfelelően illeszkedniük kell a szervezet kultúrájába. Fontos, hogy ne hozzanak létre nem kívánt versengést vagy szégyenérzetet a gyengébben teljesítőkben – ezért célszerű a hangsúlyt az egyéni fejlődésre és csapaton belüli együttműködésre helyezni, nem feltétlenül a nyilvános rangsorolásra. Továbbá biztosítani kell, hogy a vezetőség is aktívan támogassa és részvételével legitimálja ezeket a programokat, különben a dolgozók játék helyett gyerekes időpocsékolásnak is gondolhatnák. A tapasztalatok azonban azt mutatják, hogy ahol jól implementálták, ott a gamifikált képzések **gyorsabb bevonódást és jobb tanulási hatékonyságot** eredményeztek a hagyományos oktatáshoz képest [7].

Példa: a fent említett Cyber Drill Studio esetében egy átlagos osztálytermi foglalkozásban 2-3 óra kellett a résztvevők "feloldódásához", míg a játékos platformon mindez alig néhány perc alatt megtörtént, és a végén a kötelező vizsgák átlageredménye jelentősen

javult a korábbi évekhez képest [7]. Ez azt jelenti, hogy a résztvevők gyorsabban kezdtek el aktívan tanulni és jobban rögzültek bennük az ismeretek.

A gamifikált, adaptív képzések mellett is fontos a folyamatos éberség fenntartása. Jó gyakorlat, ha időnként **váratlan teszteket** iktatnak be – például a cég biztonsági csapata időről-időre szándékosan phishing e-mailt küld szét a dolgozóknak, vagy megpróbál bejutni fizikai védelem alá tartozó területre social engineering módszerrel (kvázi belső „red team" gyakorlatként). Az így kapott eredményeket (hányan dőltek be, hol kell javítani) fel lehet használni az adaptív képzés finomhangolására. Lényeges továbbá a **pozitív visszacsatolás**: ha egy dolgozó helyesen jár el egy kísérleti vagy valós incidens során (például jelent egy gyanús telefonhívást vagy megakadályozza egy illetéktelen bejutását), ismerjük el nyilvánosan, ezzel is ösztönözve a többieket a hasonló viselkedésre.

Összefoglalva, a modern, játékosított és adaptív képzésmegoldások integrálása a kritikus infrastruktúrák biztonsági protokolljaiba nagymértékben növelheti a humán védelmi vonal hatékonyságát. Az emberi tényező így nem a „leggyengébb láncszem" lesz, hanem épp ellenkezőleg, a védelmi rendszer tudatos és erős pillére. Az ilyen oktatás révén **kialakítható egy erős biztonságtudatossági kultúra**, ahol minden dolgozó tisztában van a rá leselkedő manipulációs próbálkozásokkal és magabiztosan, begyakorolt módon reagál azokra. Ezzel a kritikus infrastruktúrák védelme egy magasabb szintre emelhető, ahol a technológiai és emberi védelem valódi szinergiában működik.

KÖVETKEZTETÉSEK ÉS AJÁNLÁSOK

A kutatás rámutatott, hogy a pszichológiai manipuláció az objektumvédelemben az egyik legnagyobb kihívás: a támadók az emberi tényező sebezhetőségét kihasználva képesek kijátszani a legfejlettebb biztonsági rendszereket is. A hatékony védekezés érdekében elengedhetetlen a biztonsági személyzet rendszeres képzése a social engineering támadások felismerésére és kivédésére, az MI-alapú, vagy a rendellenesség alapú behatolás technológiák alkalmazása, valamint a szervezeti protokollok – különösen a beléptetési és incidenskezelési eljárások – szigorítása. Empirikus kutatásaink és esettanulmányaink igazolták, hogy e lépések együttes alkalmazása jelentősen csökkenti a manipulációs kísérletek sikerességét. Összességében a tanulmány megállapította, hogy a technológiai és humán védelmi tényezők párhuzamos erősítése nyújtja a leghatékonyabb védelmet a social engineering támadásokkal szemben. Ugyanakkor a jövőben várhatóan megjelennek olyan új fenyegetések is, mint az MI által támogatott manipulációk és a „deepfake" technikák; ezért a védelmi stratégiákat folyamatosan fejleszteni és adaptálni kell a változó támadási módszerekhez.

ÖSSZEGZÉS ÉS JÖVŐBELI KUTATÁSI IRÁNYOK

A tanulmány átfogóan bemutatta, hogy a humán tényezőt célzó social engineering támadások komoly veszélyt jelentenek a kritikus infrastruktúrák védelmére, és rávilágított a folyamatos képzés, a technológiai támogatás és a szigorú biztonsági protokollok együttes alkalmazásának jelentőségére. **Főbb eredményeink és tanulságaink** szerint a biztonságtudatosság növelése és a pszichológiai manipuláció elleni védelmi intézkedések integrálása

alapvetően fontos az objektumvédelemben. Ugyanakkor a social engineering jellegű fenyegetések dinamikusan fejlődnek, így **további kutatásokra és fejlesztésekre** van szükség a védelmi képességek fenntartása érdekében. Az alábbiakban összefoglaljuk a legfontosabb jövőbeli kutatási és fejlesztési irányokat:

Játékosított, adaptív képzésprogramok fejlesztése

Eredményeink tükrében indokolt olyan *gamifikáció* alapú, interaktív oktatási programok továbbfejlesztése, amelyek képesek alkalmazkodni a résztvevők egyéni tudásszintjéhez és reakcióihoz. Az ilyen adaptív képzések –szituációs gyakorlatok, szimulációk vagy kiberbiztonsági játékok – élményszerű tanulást biztosítanak, növelve a biztonsági személyzet bevonódását és hosszú távú tudásmegtartását. A jövőben érdemes vizsgálni, miként tehetők ezek a programok még hatékonyabbá a kritikus infrastruktúrák védelmében dolgozók számára, különös tekintettel az újonnan felbukkanó támadási formákra.

STEAM-alapú szemlélet kiterjesztése más biztonsági területekre

A tanulmányban alkalmazott megközelítés és a megszerzett tapasztalatok alapján javasolt a **STEAM**-alapú (a műszaki-természettudományos és matematikai oktatást a művészetekkel kreatív módon kiegészítő) szemlélet továbbvitele más, hasonlóan kritikus területekre is. Ilyen lehet a közösségi média manipulációja és a dezinformáció elleni küzdelem, ahol a technológiai ismeretek mellett a pszichológiai, médiaszempontú és kreatív gondolkodásmód integrálása kulcsfontosságú. Egy interdiszciplináris, STEAM-alapú megközelítés segíthet új oktatási modulok és tudatosságnövelő programok kidolgozásában, amelyek szélesebb körben – az iskolai oktatástól a szakmai továbbképzésekig – fejleszthetik a fenyegetések felismerésének és kezelésének képességét.

Nemzetközi együttműködés és sztenderdizáció

Mivel a kritikus infrastruktúrák elleni social engineering támadások globális problémát jelentenek, a védekezés terén elengedhetetlen a nemzetközi szintű együttműködés erősítése. Ajánlott a tapasztalatok és bevált gyakorlatok megosztása nemzetközi fórumokon, valamint közös képzési szabványok és minősítések kialakítása. Európai uniós szinten és más nemzetközi szervezetek keretében érdemes kidolgozni egységes irányelveket a biztonságtudatossági képzésekre és a social engineering incidensek kezelésére. A sztenderdizáció – legyen szó oktatási tananyagokról, minőségbiztosítási keretrendszerekről vagy akár *benchmarking* jellegű támadásszimulációkról – hozzájárulhat ahhoz, hogy a szervezetek világszerte összehangoltan és magas színvonalon készüljenek fel a manipulációs módszerek ellen.

Összefoglalva, a fenti javaslatok mentén haladva tovább növelhető a kritikus infrastruktúrák ellenálló képessége a kifinomult social engineering támadásokkal szemben. A folyamatos innováció, az interdiszciplináris megközelítés és az együttműködés erősítése együttesen biztosíthatja, hogy a védelmi gyakorlatok lépést tartsanak a fenyegetések evolúciójával, és hosszú távon is magas szintű védelmet nyújtsanak az emberi tényezőt kihasználó támadások ellen.

FELHASZNÁLT IRODALOM

[1] National Cyber Security Center (NKI), „Éves kiberbiztonsági jelentés 2023," Budapest, 2024. [Online]. Available: https://nki.gov.hu/wp-content/uploads/2024/07/Eves-kiberbiztonsagi-jelentes.pdf

[2] M. Z. Rajnai, B. László, „Az objektumvédelem biztonságtudatos szemlélete a social engineering támadások tükrében," *Biztonságtudományi Szemle*, vol. 12, no. 1, pp. 1–24, 2024.

[3] M. Kapko, „Valid accounts remain top access point for critical infrastructure attacks, officials say," *Cybersecurity Dive*, Dec. 2023. [Online]. Available: https://www.cybersecuritydive.com/news/cisa-critical-infrastructure-attacks/727225

[4] Y. Ahmed, A. Mahfouz, A. Baroudi, and D. Khalil, „Enhancing Security Awareness Through Gamified Approaches," *arXiv preprint*, arXiv:2404.09052v1, Apr. 2024. [Online]. Available: https://arxiv.org/html/2404.09052v1

[5] Industrial Cyber, „HC3 warns of Scattered Spider hackers leveraging AI, social engineering to infiltrate healthcare," *Industrial Cyber*, Jan. 2024. [Online]. Available: https://industrialcyber.co/medical/hc3-warns-of-scattered-spider-hackers-leveraging-ai-social-engineering-to-infiltrate-healthcare-other-sectors

[6] P. A. Bartel and R. L. Smith, „Gamification of Cybersecurity for Workforce Development in Critical Infrastructure," *ResearchGate*, Oct. 2022. [Online]. Available: https://www.researchgate.net/publication/365104009_Gamification_of_Cybersecurity_for_Workforce_Development_in_Critical_Infrastructure

[7] Digital Hungary, „A magyar Games for Business-szel a kiberbiztonság is fogyasztható," *DigitalHungary.hu*, Oct. 2021. [Online]. Available: https://www.digitalhungary.hu/e-kereskedelem/A-magyar-Games-for-Businessel-a-kiberbiztonsag-is-fogyaszthato/8764

[8] C. Owen-Jackson, „Social engineering in the era of generative AI: Predictions for 2024," *IBM Think*, Jan. 2024. [Online]. Available: https://www.ibm.com/think/insights/social-engineering-generative-ai-2024-predictions

[9] M. J. Guitton, „Social Engineering in Critical Infrastructure: An Analysis of Human-Centric Cybersecurity Threats," *Computers & Security*, vol. 105, 2021. [Online]. Available: https://doi.org/10.1016/j.cose.2021.102252

[10] J. M. Kowalski, „A Study on Tailgating Attacks in High-Security Environments," *Journal of Physical Security*, vol. 15, no. 3, pp. 42–55, 2022.

[11] Cybersecurity and Infrastructure Security Agency (CISA) and U.S. Coast Guard (USCG), „Fiscal Year 2023 Risk and Vulnerability Assessment Analysis," U.S. Department of Homeland Security, 2023. [Online]. Available: https://www.cisa.gov/resources-tools/resources/fiscal-year-2023-risk-and-vulnerability-assessment-analysis

[12] V. Békefi, „Gamifikáció az oktatásban és a szervezetfejlesztésben," EOQ MNB Szakbizottsági Konferencia, Budapest, 2018. [Online]. Available: https://eoq.hu/szakb/11/ea180924.pdf

[13] T. Rudas, „Gamifikáció az oktatásban – lehetőségek és kihívások," Miskolci Egyetem, Automatizálási és Infokommunikációs Intézet, 2020. [Online]. Available: https://gepesz.uni-miskolc.hu/intezetek/HATVANY/news_files/26_0.pdf

[14] M. Hegedüsné Baranyai, „A gamifikáció hatása a pénzügyi tudatosság fejlesztésére," Magyar Nemzeti Bank, 2019. [Online]. Available: https://www.mnb.hu/letoltes/0328j000.pdf

[15] I. K. Holik, T. Kersánszki, I. D. Sanda, and Z. Márton, „Improving Security and Environmental Awareness through Game-Based Learning with Minecraft," International Journal of Engineering Pedagogy (iJEP), vol. 14, no. 4, pp. 1–18, 2024. [Online]. Available: https://doi.org/10.3991/ijep.v14i4.48127