DOI: https://doi.org/10.12700/btsz.2026.8.1.11

INTERACTIVE DEFENSE MECHANISMS: INTEGRATING PROTECTION AGAINST SOCIAL ENGINEERING INTO INCIDENT MANAGEMENT PROCESSES

INTERAKTÍV VÉDELMI MECHANIZMUSOK: A PSZICHOLÓGIAI MANIPULÁCIÓ ELLENI VÉDEKEZÉS INTEGRÁLÁSA AZ INCIDENSKEZELÉSI FOLYAMATOKBA

MÁRTON Zoltán[1] – RAJNAI Zoltán[2] – PETŐ Richárd[3]

Abstract

This study analyzes social engineering as a systemic risk and strategic challenge. It highlights that technical defenses alone cannot ensure digital immunity, as most attacks exploit the human factor. The paper examines leadership accountability under NIS2 and the dependence of Return on Security Investment (ROSI) on human resilience. It demonstrates that without addressing cognitive vulnerabilities, the efficiency of technical controls declines. As a solution, an innovative Minecraft-based gamified methodology is presented, built on "cognitive slowing." Empirical results prove that through experiential learning, the manipulation success rate can be reduced from 60% to 20%, significantly enhancing organizational resilience and security culture.

Keywords

social engineering, resilience, security awareness training (SAT), proactive incident management, gamified learning environments (GLE), human-centric security management

Absztrakt

A tanulmány a pszichológiai manipulációt (social engineering) rendszerszintű kockázatként és stratégiai kihívásként elemzi. Rávilágít, hogy a technikai védelem önmagában nem garantál digitális immunitást, mivel a támadások az emberi tényezőt célozzák. Vizsgálja a NIS2 szerinti vezetői felelősséget és a biztonsági megtérülés (ROSI) függőségét a humán rezilienciától. Igazolja, hogy a kognitív sebezhetőségek kezelése nélkül a technikai kontrollok hatékonysága romlik. Megoldásként innovatív, Minecraft-alapú gamifikált módszertant mutat be, amely a „kognitív lassítás” elvére épít. Az eredmények bizonyítják, hogy a tapasztalati tanulás révén a manipulációs sikerességi ráta 60%-ról 20%-ra csökkenthető, érdemben növelve a szervezeti ellenálló képességet.

Kulcsszavak

pszichológiai manipuláció, reziliencia, biztonságtudatossági képzés, proaktív incidenskezelés, gamifikált tanulási környezetek, emberközpontú biztonságmenedzsment

[1] marton.zoltan@uni-obuda.hu | ORCID: 0009-0006-7795-076X | PhD Student, Doctoral School on Safety and Security Sciences Obuda University | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola
[2] rajnai.zoltan@uni-obuda.hu | ORCID: 0000-0002-9139-736X | professor, Obuda University, Banki Donat Faculty of Mechanical and Safety Engineering | egyetemi tanár, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar
[3] peto.richard@bgk.uni-obuda.hu | ORCID: 0000-0002-6757-0863 | adjunct professor, obuda University Banki Donat Faculty of Mechanical and Safety Engineering | egyetemi adjunktus, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

BEVEZETÉS

Az informatikai rendszerek biztonságmenedzselése során a technológiai védelmi rétegek – mint a tűzfalak vagy a behatolásjelző rendszerek (IDS/IPS) – elsődleges szerepe vitathatatlan, azonban a védelem önmagában már nem képes garantálni a szervezet teljes körű digitális immunitását [1]. Napjaink kiberbiztonsági incidenseinek domináns hányada nem technikai hiányosságokra, hanem az emberi tényező célzott kihasználására vezethető vissza. Ez a felismerés a pszichológiai manipulációt (social engineering, SE) fokozottan kritikus, rendszerszintű kockázattá emelte [2].

Ebben a megközelítésben az információbiztonság már nem csupán informatikai, hanem stratégiai vállalatirányítási kérdés, ahol a humán sebezhetőségek kezelése a kockázatmenedzsment szerves részét képezi. A biztonságmenedzsment alapvető célja az információs vagyon bizalmasságának, sértetlenségének és rendelkezésre állásának (CIA triád) fenntartása [1]. A menedzsment feladata a kockázatok precíz azonosítása, ahol a kockázat mértéke (K) a fenyegetettség (F), a sebezhetőség (S) és az eszközérték (E) szorzataként határozható meg ($K = F \times S \times E$). A pszichológiai manipuláció során a támadó a humán erőforrás kognitív sebezhetőségeit aknázza ki, megkerülve a robusztus technikai kontrollokat.

Jelen tanulmány célja a pszichológiai manipuláció anatómiájának feltárása döntéshozói nézőpontból. Vizsgáljuk az adathalászat (phishing) és az online félrevezetés (pretexting) hatásait az üzleti folytonosságra, valamint rávilágítunk a NIS2 irányelv által támasztott kiterjesztett vezetői felelősségre [3]. A dolgozat keretében bemutatjuk a manipuláció kognitív hátterét és egy innovatív, gamifikált módszertant, amely képes mérhetően növelni a szervezeti rezilienciát.

PSZICHOLÓGIAI MANIPULÁCIÓ, MINT RENDSZERSZINTŰ KOCKÁZAT

Az informatikai rendszerek biztonságának menedzselése során a technológiai védelmi rétegek (a tűzfalak vagy a behatolásjelző rendszerek) elsődleges szerepe vitathatatlan, azonban önmagukban elégtelenek a szervezet teljes körű védelméhez [1]. A kiberbiztonsági incidensek szignifikáns része nem szoftveres bug-okra, hanem az emberi tényező célzott kihasználására vezethető vissza, ami a pszichológiai manipulációt (social engineering-et) elsődleges fenyegetési vektorrá emeli [2].

Ebben a kontextusban az információbiztonság már nem csupán IT-üzemeltetési, hanem stratégiai menedzsmentet érintő kérdés, ahol a humán sebezhetőségek azonosítása és mitigálása a kockázatkezelési folyamat integráns részét kell, hogy képezze. Jelen fejezet célja a pszichológiai manipuláció mechanizmusainak feltárása vezetői nézőpontból, rávilágítva arra, hogy az adathalászat és az online félrevezetés típusú támadások miként veszélyeztetik az informatikai rendszerek integritását és az üzletmenet-folytonosságot (Business Continuity) [3].

A rendszerszintű megközelítés keretében vizsgáljuk a humán sebezhetőségek hatását a kritikus infrastruktúrák védelmére [5], valamint a NIS2 irányelv által támasztott új típusú vezetői elszámoltathatóságot a biztonságtudatosság növelése terén [3]. A következőkben részletesen elemezzük a nagy gyakorisággal előforduló támadási vektorokat és azokat a pszichológiai mechanizmusokat, amelyek a védelmi protokollok sikeres kijátszását teszik lehetővé.

Adathalászat, online félrevezetés és a menedzseri kontrollok

Az informatikai biztonságmenedzsment alapvető célja az információs eszközök bizalmasságának, sértetlenségének és rendelkezésre állásának (CIA követelményrendszer) fenntartása [1]. A menedzsment feladata a kockázatok azonosítása, ahol a kockázat mértéke (K) a fenyegetettség (F), a sebezhetőség (S) és az eszközérték (E) szorzataként határozható meg:

$$K = F \times S \times E$$

A pszichológiai manipuláció során a támadó nem a szoftverekben rejlő biztonsági réseket, hanem a humán erőforrás pszichológiai sebezhetőségeit használja fel a rendszerbe való bejutáshoz, így a szervezet különösen nehezen kiismerhető pontját támadja [2]. A pszichológiai manipuláció támadások egyik széles körben elterjedt formája az adathalászat, amely során a támadó legitimnek tűnő forrásból származó elektronikus kommunikáció útján próbál bizalmas adatokat vagy jelszavakat megszerezni [3].

Ennél specifikusabb a szigonyozás (spear phishing), amely során a támadó előzetes információgyűjtést követően egy konkrét személyt vagy munkaköri csoportot céloz meg, jelentősen növelve az üzenet hitelességét [3]. Az online félrevezetés során a támadó egy előre kidolgozott forgatókönyvre vagy ürügyre alapozva próbálja megnyerni a felhasználó bizalmát, gyakran olyan szerepbe bújva (rendszergazda vagy éppen hatósági ellenőr), amely felhatalmazza őt a biztonsági protokollok ellenőrzésére vagy megkerülésére [3]. A menedzsment szempontjából e támadások közvetlen hatással vannak az incidenskezelési folyamatokra, mivel a sikeres manipuláció révén a támadó legitim jogosultságokkal rendelkező „belső” szereplőként tűnhet fel, ami kritikusan megnehezíti a behatolás észlelését [6]. Az incidens átlagos észlelési idejének (Mean Time to Detect) növekedése a kritikus infrastruktúrák és a közszolgálat esetében hatványozott kockázatot hordoz, ahol a hierarchikus felépítés és a tekintélytisztelet megkönnyítheti a felsőbb vezető nevében elkövetett visszaéléseket [7]. A proaktív kontrollok hiánya ilyen környezetben nem csupán informatikai hiba, hanem a rendszerszintű biztonsági kultúra hiányossága, amelynek fejlesztése a Magyar Honvédség és más rendvédelmi szervek esetében is kiemelt prioritás [8].

PSZICHOLÓGIAI MECHANIZMUSOK ÉS HUMÁN SEBEZHETŐSÉGEK

A pszichológiai manipuláció sikeressége nem a technikai ismeretek hiányán, hanem az emberi gondolkodás, az észlelés, a megismerés, az információfeldolgozás mentális folyamatai és a szociálpszichológiai automatizmusok célzott kihasználásán alapul. Az informatikai rendszerek biztonságmenedzsmentje során a humán sebezhetőséget olyan komplex kockázati faktorként kell definiálni, amely az egyéni kognitív architektúra és a szervezeti kultúra interakciójából fakad [1], [2].

A kritikus infrastruktúrák védelmében a pszichológiai manipuláció különösen veszélyes, mivel a támadók a rendszert üzemeltető személyzet bizalmát és segítőkészségét használják fel a fizikai vagy logikai védelem megkerülésére [5], [9].

A Kognitív Kettős Folyamat elmélet alkalmazása

A manipuláció megértéséhez a Kognitív Kettős Folyamat elmélet (Dual-Process Theory) alkalmazása nyújt megfelelő keretet. Az emberi információfeldolgozás két, egymástól eltérő működésű rendszerre bontható: az 1. rendszerre, amely gyors, intuitív és érzelmi alapú, valamint a 2. rendszerre, amely lassabb, analitikus és logikus működésű. [10].

A pszichológiai manipuláció során a támadók manipulatív ingerek - például sürgető adathalász e-mailek vagy vészhelyzetet imitáló hívások - alkalmazásával elsősorban az 1. rendszer aktiválására törekednek (lásd: 1. ábra). Ez a rendszer heurisztikákra, érzelmi reakciókra (sürgetés, félelem) és tekintélyelvű mintákra támaszkodik, ami lehetővé teszi a 2. rendszer kritikus elemző és ellenőrző funkcióinak megkerülését. Ennek következtében elmaradhat a biztonsági szabályzatok tudatos ellenőrzése és az információk hitelesítése, ami közvetlenül hozzájárulhat rosszindulatú cselekvésekhez (például linkekre való kattintás, érzékeny adatok felfedése) [10].

A folyamatot tovább erősítik a különböző kognitív heurisztikák, ahogyan az 1. ábra is szemlélteti és torzítások (biases), mint a túlzott magabiztosság (overconfidence bias), a megerősítési torzítás, illetve az optimizmus-torzítás, amelynek hatására a munkavállalók hajlamosak alábecsülni saját szervezetük kitettségét a kiberbiztonsági fenyegetésekkel szemben [11]. Ez a kognitív „rövidzárlat” jelentősen csökkenti az éberségi szintet, és növeli a manipuláció sikerességének esélyét.

1. ábra - A kognitív kettős folyamat elmélet alkalmazása pszichológiai manipuláció során (saját ábra)

Az egyéni sebezhetőséget jelentősen befolyásolják a személyiségjegyek is. A kutatások szerint a „Big Five” személyiségmodell elemei közül a magas barátságosság (agreeableness) és az extraverzió szignifikánsan növelheti a manipulációval szembeni kitettséget, mivel az ilyen jegyekkel rendelkező egyének hajlamosabbak a gyors bizalomépítésre [12]. Ezzel szemben a lelkiismeretesség (conscientiousness) gyakran védelmi faktorként jelenik meg, mivel a szabálykövetőbb magatartás szorosabb összefüggést mutat a biztonsági protokollok betartásával [12].

A menedzsment számára ez azt jelenti, hogy a biztonságtudatossági stratégiákat nem lehet uniformizáltan kezelni, hanem figyelembe kell venni a munkavállalói állomány

pszichológiai heterogenitását. A hierarchikus szervezetekben, különösen a közigazgatásban és a rendvédelmi szerveknél, a tekintélynek való engedelmesség és a társas megfelelési kényszer válik a legfőbb sebezhetőségi ponttá [7], [8]. A támadók a legitimáció látszatával és az időkényszer alkalmazásával olyan érzelmi állapotot hoznak létre, amelyben a munkavállaló hajlamosabb a szabályok áthágására egy „felsőbb cél" vagy sürgős vezetői kérés érdekében [4].

A hagyományos biztonságtudatossági programok gyakran vallanak kudarcot, mert csupán az elméleti tudásátadásra fókuszálnak, és nem kezelik ezeket a mélyen gyökerező viselkedési automatizmusokat [13]. Az incidenskezelés proaktív szakaszában a menedzseri kontrolloknak ki kell terjedniük ezen pszichológiai kiváltó okokra (trigger-ekre), azok monitorozására és szimulált tesztelésére [6]. A reziliencia kialakításához olyan interaktív módszertanra van szükség, amely a kognitív lassítás elvét alkalmazva képessé teszi a felhasználót a manipulációs technikák valós idejű (real-time) felismerésére és a 2. rendszer tudatos aktiválására.

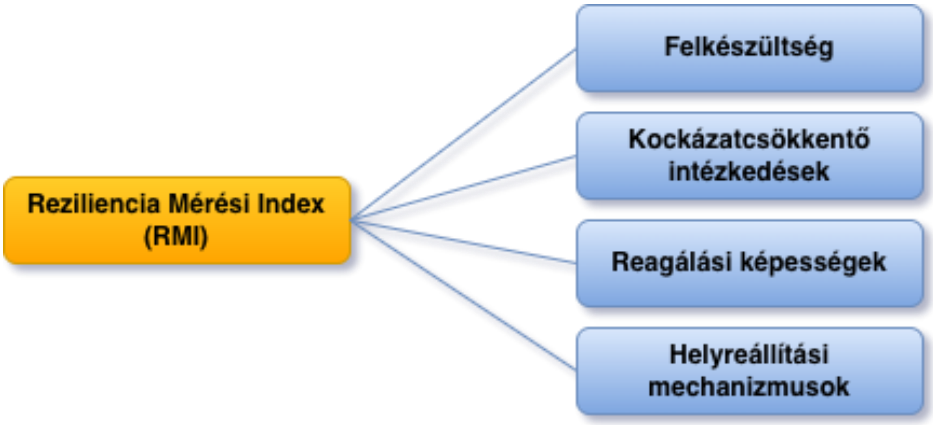
A MANIPULÁCIÓ HATÁSA AZ INFORMATIKAI RENDSZEREK BIZTONSÁGÁRA

A pszichológiai manipuláció nem csupán elszigetelt incidens, hanem olyan rendszerszintű fenyegetés, amely az informatikai architektúra alapvető biztonsági pilléreit támadja. A pszichológiai manipuláció alapú támadások jelentősége abban rejlik, hogy képesek megkerülni a korszerű technikai védelmi rendszereket is, mivel nem a szoftveres sebezhetőségeket, hanem a humán interakciók bizalmi láncát kompromittálják [14].

Incidenskezelési aspektusok és észlelési nehézségek

Az incidenskezelés során a pszichológiai manipuláció alapú behatolások azonosítása jelenti a legnagyobb kihívást. Mivel a támadók sikeres manipuláció révén érvényes felhasználói hitelesítő adatokat szereznek, tevékenységük a hagyományos behatolásjelző rendszerek számára legitim felhasználói viselkedésnek tűnhet [15]. Az észlelés elhúzódása kritikus kockázatot jelent a kritikus infrastruktúrákban, ahol a válaszadási idő minimalizálása alapvető fontosságú az üzletmenet-folytonosság szempontjából [5], [9].

A modern észlelési stratégiáknak ezért túl kell lépniük a statikus szabályokon, és olyan vizualizációs eszközöket vagy viselkedéselemző algoritmusokat kell alkalmazniuk, amelyek képesek az anomáliák felismerésére a *felhasználó–forrás–célpont* triász mentén [15]. A kritikus infrastruktúrák ellenálló képességének mérésekor a Reziliencia Mérési Index (Resilience Measurement Index - RMI) alkalmazása elengedhetetlen, amely a felkészültséget, a mérséklési intézkedéseket, valamint a válaszadási és helyreállítási képességeket összesíti (lásd: 2. ábra). A pszichológiai manipuláció közvetlenül rontja ezeket a mutatókat, mivel a humán sebezhetőség gyengíti a megelőző kontrollok hatékonyságát, így növelve a rendszer helyreállítási idejét és költségeit.

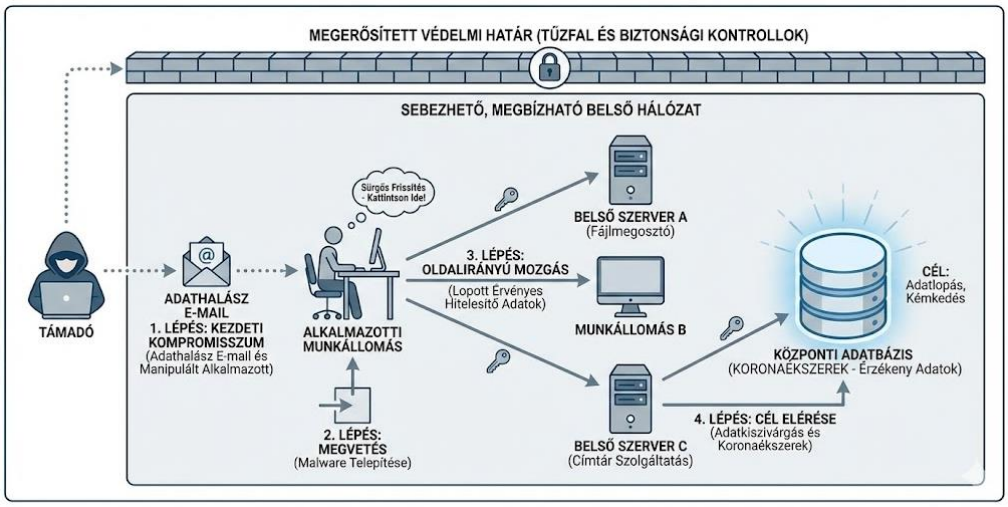


2. ábra - A Rezlliencia Mérési Index (RMI) 1. szintű összetevői (saját szerkesztés) [17]

Hálózati integritás és laterális mozgás

A hálózati integritás szempontjából egyetlen manipulált munkavállaló a teljes rendszer kompromittálódásának forrásává válhat. A pszichológiai manipulációs támadások során az áldozat nem csupán adatokat ad át, hanem egy „hídfőállást" (foothold) biztosít a támadónak a belső hálózaton [15]. A laterális mozgás (lateral movement) fázisában a támadó már nem kívülről próbál áttörni a tűzfalon, hanem a megszerzett, legitimnek tűnő jogosultságokkal „belülről" navigál az erőforrások között - ahogyan ezt a 3. ábra is mutatja.

Siadati és munkatársai rámutatnak, hogy az észlelés kulcsa a kontextuális anomáliák figyelése: ha egy legitim felhasználó szokatlan forrásból szokatlan célpontot próbál elérni, az laterális mozgásra utal [15]. A pszichológiai manipuláció taxonómiája szerint a támadók rétegzett módszereket alkalmaznak a jogosultságok kiterjesztésére, szisztematikusan kihasználva a hálózati szegmentáció hiányosságait [14].



3. ábra - A manipuláció alapú behatolás és a laterális mozgás folyamata a vállalati hálózatban
Forrás: Saját szerkesztés Zaoui et al. [14] és Siadati et al. [15] alapján

Adatbiztonság, üzleti folytonosság és megtérülés (ROSI)

A manipulációból eredő adatvesztés hatásai messze túlmutatnak a közvetlen gazdasági károkon. A szervezeti bizalom elvesztése – mind belső, mind külső, ügyféloldali szempontból - olyan immateriális kár, amely hosszú távon veszélyezteti a piaci pozíciót. A menedzsment számára a legnagyobb kihívást az jelenti, hogy a technikai védelembe fektetett tőke nem hoz arányos megtérülést, ha a humán faktor tudatossága és rezilienciája elmarad a fenyegetettségi szinttől .

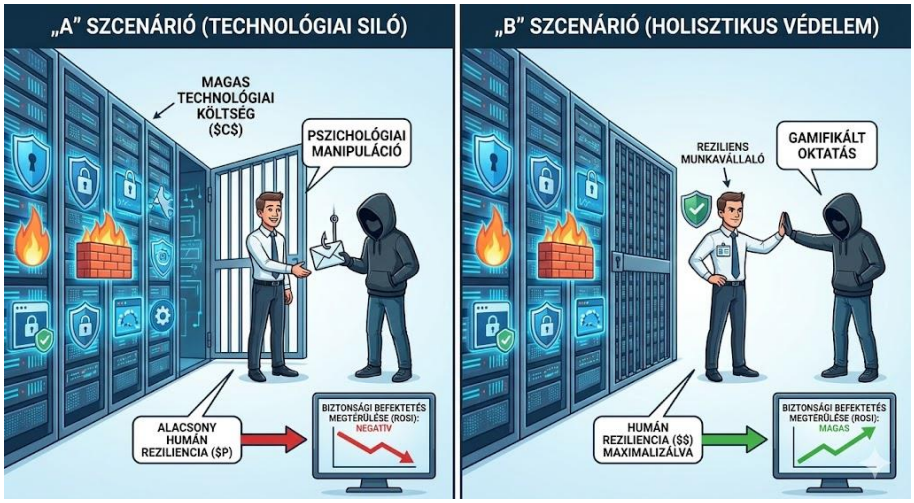
A kiberbiztonsági beruházások gazdasági racionalitása a biztonsági befektetések megtérülési mutatójával (Return on Security Investment - ROSI) szemléltethető legpontosabban, amely figyelembe veszi a védelmi intézkedések kockázatcsökkentő hatását:

$$ROSI = \frac{(ALE \times P) - C}{C}$$

A képletben az **ALE** (Annual Loss Expectancy) az éves várható veszteséget jelöli, a **C** a védekezés költsége, míg a **P** (Mitigation Factor) a védelmi intézkedés - jelen esetben a humán reziliencia-fejlesztés - hatékonyságát mutatja.

Amennyiben a munkavállalók manipulálhatósága miatt a P értéke alacsony marad (például a felejtési görbe miatt a hagyományos oktatás után), úgy a technikai eszközökbe fektetett tőke megtérülése is romlik. A gamifikált oktatás gazdasági előnye éppen a P tényező időbeli stabilizálásában rejlik: az élményalapú tanulás mélyebb memórianyomokat hagy, így a védekezés hatékonysága hosszabb távon is magas marad, javítva a ROSI mutatót (lásd: 4. ábra).

A NIS2 irányelv értelmében a kiberbiztonsági kockázatkezelésnek ki kell terjednie a teljes ellátási láncra, felismerve, hogy a manipuláció nemcsak a belső állományt, hanem a beszállítókat és partnereket is célba veheti [3].



4. ábra - A biztonsági befektetések megtérülésének (ROSI) összefüggései a humán faktor függvényében
Forrás: Saját szerkesztés Kostic [16] alapján

A GAMIFIKÁLT TANULÁSI KÖRNYEZETEK SZEREPE A PREVENCIÓBAN

A kiberbiztonsági tudatosság növelésének egyik akadálya a hagyományos, frontális oktatási módszerek használata, amely ritkán vezet tartós viselkedésváltozáshoz [13]. Ezzel szemben a gamifikáció és a játékalapú tanulás (Game-Based Learning - GBL) olyan innovatív megközelítést kínál, amely a tanulást kötelezettség helyett élménnyé alakítja. A módszertan pedagógiai alapjai John Dewey tapasztalati tanulásról alkotott nézeteire és Csíkszentmihályi Mihály flow-elméletére vezethetők vissza. A flow-állapotban a tanuló annyira elmélyed a tevékenységben, hogy a tanulás érdekessé és kihívást jelentővé válik, a nehézségek pedig nem elriasztják, hanem megoldásra inspirálják.

A tapasztalati tanulás és a biztonságtudatosság

A gamifikált környezetek, így a mesterséges intelligencia (MI) alapú szimulációk vagy virtuális valóság tréningek, valós idejű visszacsatolást biztosítanak a tanulóknak, lehetővé téve a pszichológiai manipulációs támadások mechanizmusainak biztonságos megtapasztalását. A kutatások igazolják a módszer hatékonyságát: míg a képzetlen személyzet körében a manipuláció sikerességi aránya elérheti az 58–64%-ot, addig a célzott tréningek után ez az arány 19–20%-ra csökkenthető.

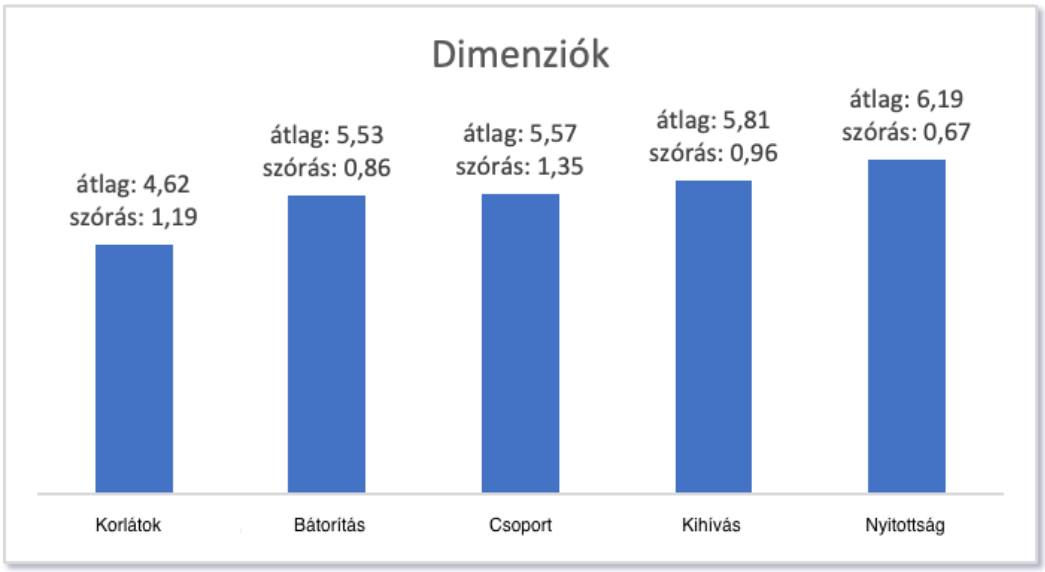
A játék elemei – többek között a pontrendszerek és ranglisták – fenntartják a motivációt és ösztönzik az analitikus (2-es típusú) gondolkodás aktiválását kritikus helyzetekben. A gamifikáció hatása közvetlenül mérhető a korábban bemutatott ROSI képlet P (mérséklési tényező) elemében is. A tapasztalati tanulás során a munkavállaló aktív részese lesz a védelmi folyamatnak, így képessé válik az olyan kognitív torzítások korrigálására, mint az optimizmus-torzítás vagy a tekintélynek való automatikus engedelmesség.

A Minecraft, mint a komplex rendszerek modellezésének eszköze

A Minecraft „sandbox” típusú videojáték kiváló platformot biztosít a biztonságtechnikai ismeretek és a kritikus infrastruktúrák védelmének oktatásához. A szoftver módosításával (esetünkben 50–60 speciális „mod” használatával) a valósághoz hű szimulációk hozhatók létre, ahol a résztvevők intelligens épületeket, megújuló energiaforrásokat vagy objektumvédelmi rendszereket tervezhetnek és üzemeltethetnek.

A kutatásunk egyik legfontosabb megállapítása, hogy a Minecraft-ban végzett erőforrás-menedzsment és a logikai áramkörök építése **kognitív lassítást** eredményez. Ez a mentális állapot homlokegyenest ellentétes azzal a „sürgetett” állapottal, amit az adathalász támadások igyekeznek előidézni. A játék során a felhasználók megtanulják vizuálisan azonosítani az anomáliákat a térben, ami transzferálható képességként jelenik meg a hálózati log-ok vagy e-mail fejlécek vizuális ellenőrzésekor.

Az oktatási kísérleteink során a résztvevők 55,6%-a számolt be a problémamegoldó képesség szubjektív fejlődéséről. Bár ez önbevalláson alapuló adat, a kompetenciaérzet növekedése (self-efficacy) pozitív korrelációt mutat a valós biztonságtudatos viselkedéssel, mivel a magabiztosabb felhasználó kevésbé hajlamos a pánikszerű (1. rendszer) reakciókra egy incidens során (lásd: 5. ábra). A gamifikált módszer előnye, hogy a tanulók büntetlenül hibázhatnak a virtuális térben, miközben megtapasztalják döntéseik súlyát és a biztonsági protokollok betartásának jelentőségét.



5. ábra - A gamifikált tanulási környezet kreatív klímájának dimenziói
Forrás: Saját szerkesztés Holik et al. [20] és Kersánszki et al. [21, 22] alapján

ÖSSZEGZÉS

A kutatás rávilágított arra, hogy a pszichológiai manipuláció nem elszigetelt incidensek sorozata, hanem olyan rendszerszintű fenyegetés, amely az informatikai architektúra humán bizalmi láncát kompromittálja [14]. A kognitív kettős folyamat elmélet alkalmazásával bizonyítottuk, hogy a támadók módszeresen az intuitív, érzelemalapú „1. rendszert" aktiválják, ezzel iktatva ki a logikus és analitikus kontrollt végző „2. rendszert" [10].

A menedzsment számára kritikus felismerés, hogy a technikai védelembe fektetett tőke megtérülése (ROSI) drasztikusan romlik, ha a humán faktor mérséklési képessége (P) alacsony marad. A tanulmányban bemutatott összefüggés rávilágít arra, hogy a biztonságtudatosság nem csupán elméleti elvárás, hanem gazdasági és üzletmenet-folytonossági kényszer.

A hagyományos, statikus oktatási módszerek kudarca után a játékalapú tanulás (Game-Based Learning) és a Minecraft-alapú szimulációk új utat mutatnak a prevencióban. Az empirikus eredmények igazolták, hogy a gamifikált környezetben végzett tréningek hatására a manipuláció sikerességi aránya szignifikánsan csökkenthető. Zárásként megállapítható, hogy a NIS2 irányelvnek való megfelelés és a kritikus infrastruktúrák védelme megköveteli a proaktív biztonsági kultúra kialakítását. A humán reziliencia ily módon a modern kiberbiztonsági stratégia megkerülhetetlen pillérévé válik.

FELHASZNÁLT IRODALOM

[1] A. Bodáné Kendelényi, "Kiberbiztonság menedzseri szemmel," oktatási segédanyag, Nemzeti Közszolgálati Egyetem, Budapest, 2023.
[2] Cs. Kollár, "A biztonság megjelenése a humán tudományokban (3. rész)," Biztonságtudományi Szemle, vol. 6, no. 4, pp. 1–14, 2024, doi: 10.12700/btsz.2024.6.4.1.

[3] Á. Kiss and Cs. Kollár, "Az információbiztonság időszerű kérdései a magyarországi kkv-k körében," Scientia et Securitas, vol. 4, no. 2, pp. 98–107, 2023, doi: 10.1556/112.2023.00010.
[4] Z. Németh and Z. Völgyi, "A kritikus információs infrastruktúra védelem pszichológiai szempontú megközelítése (Humán biztonsági kockázatelemzés)," Hadtudományi Szemle, vol. 11, no. 3, pp. 324–337, 2018.
[5] M. Kis, A. Bódi, and R. Számadó, "A NIS2 hazai bevezetésének folyamata és kockázatai," Hadmérnök, vol. 19, no. 3, pp. 115–130, 2024, doi: 10.32567/hm.2024.3.8.
[6] I. Jagodics and Cs. Kollár, "21. századi social engineering támadások, védekezés és szervezeti hatások Európában," Belügyi Szemle, vol. 71, no. 1, pp. 115–134, 2023, doi: 10.38146/BSZ.2023.1.7.
[7] L. Kovács, „Kibervédelmi kihívások a közszolgálat személyi állományában," Publikáció, 2024.
[8] Z. Szabó, „Az emberi tényező szerepe az információbiztonság megvalósítása és erősítése terén. Az információbiztonsági kultúra fejlesztésének lehetőségei a Magyar Honvédségben," doktori értekezés, 2023.
[9] V. Greavu-Şerban, F. Constantin, and S.-C. Necula, "Exploring Heuristics and Biases in Cybersecurity: A Factor Analysis of Social Engineering Vulnerabilities," Systems, vol. 13, no. 4, art. no. 280, Apr. 2025, doi: 10.3390/systems13040280.
[10] F. Bano, M. A. Ghazanfar, and A. Alqahtani, "Understanding Social Engineering Through the Lens of Human Cognition: A Systematic Literature Review," IEEE Access, vol. 12, pp. 11046–11062, 2024, doi: 10.1109/ACCESS.2024.3353456.
[11] M. K. Alshaikh, "Reviewing Cyber Security Social Engineering Training and Awareness Programs—A Systematic Literature Review," IEEE Access, vol. 11, pp. 113327–113345, 2023, doi: 10.1109/ACCESS.2023.3323490.
[12] I. Ghafir, J. Saleem, M. Hammoudeh, et al., "Security threats to critical infrastructure: the human factor," The Journal of Supercomputing, vol. 74, no. 10, pp. 4986–5002, Oct. 2018, doi: 10.1007/s11227-018-2337-2.
[13] S. Uebelacker and S. Quiel, "The Social Engineering Personality Framework," in 2014 Fourth International Workshop on Socio-Technical Aspects in Security and Trust (STAST), Vienna, Austria, 2014, pp. 24–30, doi: 10.1109/STAST.2014.12.
[14] M. Zaoui, Y. Belfaik, Y. Sadqi, Y. Maleh, and A. Mamouni, "A Comprehensive Taxonomy of Social Engineering Attacks and Defense Mechanisms: Toward Effective Mitigation Strategies," IEEE Access, vol. 12, pp. 72224–72241, 2024, doi: 10.1109/ACCESS.2024.3403197.
[15] H. Siadati, B. Saket, and N. Memon, "Detecting Malicious Logins in Enterprise Networks Using Visualization," in 2016 IEEE Symposium on Visualization for Cyber Security (VizSec), Baltimore, MD, USA, 2016, pp. 1–8, doi: 10.1109/VIZSEC.2016.7739582.
[16] L. C. Kostic, "Information Security Awareness Techniques that Reduce Data Breaches Caused by Social Engineering Attacks." Order No. 27832769, Capella University, United States -- Minnesota, 2020.
[17] F. D. P. Petit, G. W. Bassett, R. Black, et al., "Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience," Argonne National Laboratory, Argonne, IL, USA, Tech. Rep. ANL/DIS-13-1, Apr. 2013, doi: 10.2172/1087819.

[18] Z. Rajnai, L. Berek, and Z. Márton, „Social engineering az objektum-védelemben: a biztonsági személyzet befolyásolhatóságának vizsgálata," Biztonságtudományi Szemle, vol. 7, no. 1, pp. 95–106, 2025, doi: 10.12700/btsz.2025.7.1.95.
[19] Z. Márton and Z. Rajnai, „A social engineering fejlődése és jövője: a pszichológiai sebezhetőségek kihasználása a digitális korban," Biztonságtudományi Szemle, vol. 6, no. 4, pp. 45–56, 2024, doi: 10.12700/btsz.2024.6.4.45.
[20] I. Holik, T. Kersánszki, I. D. Sanda, and Z. Márton, "Improving Security and Environmental Awareness through Game-Based Learning with Minecraft", Int. J. Eng. Ped., vol. 14, no. 4, pp. pp. 90–107, May 2024.
[21] T. Kersánszki, Z. Márton, K. Fenyvesi, Z. Lavicza, and I. Holik, „Implementation of Minecraft in Education to Introduce Sustainable Development Goals: Approaching Renewable Energy Through Game-Based Learning," in Smart Learning Ecosystems as Engines of the Green and Digital Transition, M. Dascalu, Ó. Mealha, and S. Virkus, Eds. Singapore: Springer, 2023, pp. 219–232, doi: 10.1007/978-981-99-5540-4_13.
[22] T. Kersánszki, I. Holik, and Z. Márton, "Minecraft Game as a New Opportunity for Teaching Renewable Energy Topics", Int. J. Eng. Ped., vol. 13, no. 5, pp. pp. 16–29, Jul. 2023.