DOI: https://doi.org/10.12700/btsz.2025.7.1.95

SOCIAL ENGINEERING IN FACILITY PROTECTION: EXAMINING THE INFLUENCE OF SECURITY PERSONNEL

SOCIAL ENGINEERING AZ OBJEKTUMVÉDELEMBEN: A BIZTONSÁGI SZEMÉLYZET BEFOLYÁSOLHATÓSÁGÁNAK VIZSGÁLATA

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

Abstract

This study examines the role of social engineering and psychological manipulation in facility security, focusing on the susceptibility of security personnel. Attackers exploit cognitive biases and decision-making errors to bypass security systems. The research analyzes pretexting, tailgating, phishing, authority exploitation, and stress induction. Case studies confirm that training, technological defenses, and organizational protocols reduce manipulation risks. Future threats include AI-driven attacks, deepfake videos, and automated social engineering techniques.

Keywords

social engineering, psychological manipulation, facility security, security personnel, AI-driven attacks

Absztrakt

A tanulmány a social engineering támadások és a pszichológiai manipuláció szerepét vizsgálja az objektumvédelemben, kiemelten a biztonsági személyzet befolyásolhatóságát. A támadók a humán tényezőt célozzák, kihasználva kognitív torzításokat és döntéshozatali hibákat. A kutatás elemzi a pretexting, tailgating, phishing, tekintélyelvű manipuláció és stressz indukció hatékonyságát. Esettanulmányok igazolják, hogy a képzés, technológiai védelem és szervezeti protokollok kombinációja csökkenti a manipuláció kockázatát. A jövőbeni fenyegetések közé tartoznak az AI-alapú támadások, deepfake és automatizált social engineering technikák.

Kulcsszavak

social engineering, pszichológiai manipuláció, objektumvédelem, biztonsági személyzet, AI-alapú támadások

[1] 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

[2] 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

[2] 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

BEVEZETÉS

Az objektumvédelem egyik legfontosabb aspektusa a fizikai és technológiai biztonsági rendszerek mellett az emberi tényező szerepe. Noha a korszerű biztonsági technológiák – például beléptetőrendszerek, videomegfigyelés, biometrikus azonosítók – jelentős védelmet biztosítanak, a támadók gyakran nem ezekkel a technológiai akadályokkal szembesülnek először, hanem a biztonsági személyzettel. A pszichológiai manipuláció és a social engineering támadások egyik fő célpontja éppen az a humán faktor, amely még a legkifinomultabb biztonsági rendszerekben is jelen van [1].

A támadók olyan pszichológiai és viselkedéslélektani módszereket alkalmaznak, amelyek célja az emberi döntéshozatal befolyásolása, az érzelmi állapot manipulálása és a kognitív torzítások kihasználása. Ezek a technikák – mint a sürgetettségérzés keltése, az autoritás kihasználása, vagy a meggyőzés hatékonyságának növelése – tudományos alapokon nyugvó stratégiák, amelyeket évtizedek óta alkalmaznak különböző környezetekben, így az objektumvédelem területén is [2].

A tanulmány célja, hogy mélyrehatóan elemezze a pszichológiai manipuláció és a social engineering kapcsolatát az objektumvédelemben, bemutassa a támadók által leggyakrabban alkalmazott módszereket, valamint esettanulmányokkal és empirikus kutatási eredményekkel alátámasztva ajánlásokat fogalmazzon meg a védekezési stratégiákra vonatkozóan.

A social engineering és a pszichológiai manipuláció lényegében azonos fogalom, csupán eltérő nyelvi megfogalmazásban. Napjainkban a magyar szakirodalomban is széles körben elterjedt az angol terminológia használata, amely a nemzetközi tudományos diskurzushoz való kapcsolódást is elősegíti.

A PSZICHOLÓGIAI MANIPULÁCIÓ ELMÉLETI ALAPJAI

A pszichológiai manipuláció megértéséhez elengedhetetlen az emberi döntéshozatali folyamatok mélyebb elemzése. A támadók pontosan ismerik, hogy az emberek hogyan hoznak döntéseket különböző környezeti hatások és pszichológiai tényezők alapján. A kutatások szerint a manipuláció sikeressége nagymértékben függ attól, hogy a támadó menynyire képes kihasználni az emberi gondolkodás jellemzőit, például a kognitív torzításokat vagy az automatikus reakciókat.

Az alábbi szakasz részletesen bemutatja azokat a döntéshozatali mechanizmusokat és kognitív torzításokat, amelyek a manipuláció célpontjai lehetnek. Ezek a torzítások nemcsak az objektumvédelmi személyzetet érintik, hanem minden emberi interakció során jelen vannak, így a támadók széles körben alkalmazhatják őket.

A social engineering támadások sikeressége nagymértékben függ attól, hogy a támadók milyen pszichológiai manipulációs technikákat alkalmaznak. Kollár és Zakar (2020) kutatása szerint a támadók gyakran építenek a kognitív torzításokra, így a tekintélyelvűség torzítására (authority bias) és a megerősítési torzításra (confirmation bias), mivel ezek lehetővé teszik az áldozatok befolyásolását anélkül, hogy azok tudatosan észlelnék a manipulációt. Kollár és Zakar empirikus vizsgálatai azt is kimutatták, hogy a megfelelő képzés és tudatosságnövelés akár jelentős mértékben csökkentheti a social engineering támadások sikerességét, ezáltal növelve a szervezetek biztonságát [18].

A döntéshozatal pszichológiai mechanizmusai és torzításai

A pszichológiai manipuláció alapja az emberi döntéshozatal működésének kihasználása. Kahneman és Tversky [3] kutatásai alapján a döntéshozatal során gyakran alkalmazunk heurisztikákat – gyors és egyszerűsített gondolkodási szabályokat –, amelyek bizonyos helyzetekben kognitív torzításokhoz vezethetnek. Az alábbi torzítások különösen relevánsak az objektumvédelem területén:

- *Confirmation bias (megerősítési torzítás):* Az emberek hajlamosak elfogadni azokat az információkat, amelyek megerősítik előzetes vélekedéseiket, miközben figyelmen kívül hagyják azokat, amelyek ellentmondanak ezeknek [4].
- *Authority bias (tekintélyelvűség torzítása):* Az emberek nagyobb valószínűséggel engedelmeskednek a hatalommal rendelkező vagy annak látszó személyeknek, még akkor is, ha a kérésük irracionális [5].
- *Social proof (szociális bizonyíték):* Az emberek mások viselkedése alapján alakítják ki saját cselekedeteiket, különösen bizonytalan helyzetekben [6].
- *Urgency effect (sürgősségi torzítás):* Krízishelyzetben az emberek hajlamosak a gyors döntéshozatalra, gyakran anélkül, hogy megfelelően átgondolnák a helyzetet [7].

A támadók ezeket a pszichológiai jelenségeket kihasználva manipulálják az objektumvédelmi személyzetet.

A social engineering alkalmazási módszerei - eseteken keresztül

A social engineering támadások lényege, hogy a támadók az emberi viselkedés sajátosságait kihasználva megtévesztéssel, manipulációval vagy pszichológiai nyomásgyakorlással jutnak hozzá bizalmas információkhoz vagy jogosulatlan hozzáféréshez. Ezek a módszerek sokszor hatékonyabbak, mint a technológiai támadások, hiszen egy jól kidolgozott megtévesztési stratégia révén a támadó ellenállás nélkül kaphat meg kulcsfontosságú adatokat vagy bejuthat egy védett területre.

Az alábbiakban bemutatásra kerülnek a social engineering leggyakoribb alkalmazott módszerei, amelyek a támadók eszköztárának részét képezik. Minden technikát egy valós esettanulmány vagy lehetséges forgatókönyv kísér, amely rávilágít arra, hogy ezek a módszerek hogyan működnek a gyakorlatban:

- *Pretexting (álindok alkalmazása):* A „pretexting” során a támadó egy kitalált, de meggyőző és hitelesnek tűnő szerepet vesz fel annak érdekében, hogy az áldozat érzékeny információkat osszon meg vele. Ez a módszer általában előzetes kutatást igényel a támadó részéről, aki a célpont szervezetéről vagy egy adott személy szokásairól, kapcsolati hálójáról és biztonsági eljárásairól gyűjt információt, mielőtt kapcsolatba lépne vele. A támadó gyakran egy hivatalos pozíciót színlel, például karbantartó, IT-mérnök, ügyfélszolgálatos vagy hatósági személy (pl. rendőr, auditor) szerepét ölti magára. A cél az, hogy az áldozat egy hamis történet hatására kiadja belépési adatait, pénzügyi információit, vagy akár fizikai hozzáférést biztosítson egy adott létesítményhez [8].

Eset: Egy támadó, aki magát az IT-osztály egyik új munkatársának adja ki, e-mailben vagy telefonon kéri egy alkalmazottól, hogy frissítse a jelszavát egy küldött linken keresztül. Az áldozat a megtévesztő kommunikáció miatt gyanútlanul megadja belépési adatait, amelyek így a támadóhoz kerülnek.

- *Tailgating (követés belépésnél):* A tailgating, más néven „piggybacking", egy olyan social engineering technika, amelyben a támadó egy jogosult személyt követve jut be egy ellenőrzött területre, anélkül, hogy saját belépési jogosultsága lenne. A módszer sikeressége gyakran a biztonsági személyzet figyelmetlenségén vagy a szociális normákon alapul, amelyek arra ösztönzik az embereket, hogy udvariasak legyenek és ne kérdőjelezzék meg mások szándékait. A támadó kihasználhatja az áldozatok segítőkészségét vagy a forgalmas időszakokat, amikor nagyobb esély van arra, hogy észrevétlenül beléphet egy épületbe. Például egy vállalati irodaházban a támadó egy csomagot vagy laptoptáskát cipelve követhet egy alkalmazottat, aki automatikusan visszatartja az ajtót, hogy ne csapódjon be mögötte. Mivel az emberek nem akarnak udvariatlannak tűnni, nagy valószínűséggel beengedik az illetőt anélkül, hogy ellenőriznék, valóban jogosult-e a belépésre [9].

Eset: Egy támadó egy hivatalosnak tűnő munkaruhát viselve (például egy technikai szolgáltató vagy szállítmányozó cég egyenruháját) követ egy alkalmazottat egy irodaházba, miközben azt állítja, hogy egy sürgős javítás miatt érkezett. A biztonsági őr gyanú nélkül beengedi őt, így a támadó hozzáférést kap az épület belső rendszeréhez.

- *Phishing és vishing (elektronikus és telefonos manipuláció):* A „phishing" a kiberbiztonság egyik leggyakoribb támadási módszere, amely során a támadó hamis e-maileket, weboldalakat vagy üzeneteket használ arra, hogy az áldozatokat érzékeny információk megadására vegye rá. Ezek az üzenetek gyakran hivatalosnak tűnnek, például banki vagy vállalati leveleknek álcázzák őket, amelyek sürgős intézkedésre szólítanak fel (pl. „Fiókja zárolásra kerül, ha nem erősíti meg adatait"). Az e-mailekben található linkek egy adathalász weboldalra vezetnek, amelyet a támadó úgy tervezett meg, hogy megtévesztően hasonlítson az eredeti szolgáltató oldalára [10]. A „vishing" a „phishing" telefonos változata, amely során a támadó valódinak tűnő telefonhívásokkal próbálja rávenni az áldozatokat arra, hogy személyes vagy pénzügyi adatokat osszanak meg. A támadó gyakran egy ügyfélszolgálati munkatársnak, banki alkalmazottnak vagy hatósági személynek adja ki magát, és sürgős ügyintézést színlel.

Eset: Egy támadó, aki magát egy banki ügyfélszolgálatosnak adja ki, felhívja az áldozatot, és közli vele, hogy gyanús tranzakciót észleltek a számláján. Az áldozat pánikba esik, és minden további nélkül megadja az online bankoláshoz szükséges adatait, hogy „biztonságba helyezze" a pénzét.

- *Authority exploitation (tekintélyelvű manipuláció):* A tekintélyelvű manipuláció során a támadó egy magas beosztású vagy hivatalos személy szerepét játssza el annak érdekében, hogy az áldozat engedelmeskedjen neki. Az emberek természetüknél fogva hajlamosak követni a tekintélyszemélyek utasításait, különösen akkor, ha azok hatalmi pozíciót sugallnak, például vállalati vezető, kormányzati tisztviselő

vagy rendvédelmi szerv képviselője [11]. A támadók ezt a stratégiát gyakran telefonhívások vagy e-mailek révén alkalmazzák, és gyors cselekvésre ösztönzik az áldozatokat. Az áldozatok sokszor nem merik megkérdőjelezni a támadó utasításait, mert félnek attól, hogy megszegnek egy szervezeti szabályt vagy egy felsőbb vezető utasításával szembeszállnak.

Eset: Egy támadó, aki egy cég pénzügyi igazgatójának adja ki magát, e-mailben utasítja a könyvelőt, hogy sürgősen utaljon át egy nagyobb összeget egy „üzleti partner" számlájára. Az üzenet sürgető és hivatalos hangnemű, ezért az alkalmazott nem kérdőjelezi meg annak hitelességét, és végrehajtja az utalást.

- *Stress induction (stresszhelyzet előidézése):* A stresszhelyzet előidézése az egyik leghatékonyabb social engineering módszer, mivel az emberek krízishelyzetben hajlamosak kevésbé racionálisan gondolkodni és gyorsan reagálni anélkül, hogy alaposan átgondolnák döntéseiket. A támadó olyan helyzetet teremt, amelyben az áldozat nyomás alá kerül – például vészhelyzetet szimulál, sürgős ügyintézésre kényszeríti az áldozatot, vagy akár félelmet kelt benne [12]. A stresszhelyzetek kiváltása történhet telefonhívásokkal, e-mailekkel vagy személyes interakciókon keresztül, és gyakran kombinálják más social engineering technikákkal, például tekintélyelvű manipulációval vagy vishing támadásokkal.

Eset: Egy támadó felhív egy vállalat IT-alkalmazottját, és azt állítja, hogy azonnali intézkedésre van szükség, mert egy kibertámadás érte a rendszert. A stresszes helyzet miatt az alkalmazott gondolkodás nélkül követi az utasításokat, és kiadja a belépési adatokat, ezzel veszélybe sodorva az informatikai rendszert.

A fenti social engineering technikák közös jellemzője, hogy az emberi tényező kihasználására építenek, és gyakran olyan helyzeteket teremtenek, amelyekben az áldozatok elveszítik a kontrollt saját döntéshozataluk felett. A támadók manipulációja nem mindig nyilvánvaló, sőt, gyakran az áldozatok nem is érzékelik, hogy pszichológiai befolyás alatt állnak.

Egyes támadási módszerek azonnali cselekvésre kényszerítik az áldozatot, például egy sürgető telefonhívással vagy egy tekintélyelvű személynek való kiadás révén, míg mások hosszabb távú kapcsolatépítésre és bizalom kialakítására építenek. A támadók a helyzethez igazítják stratégiáikat, és a célpont személyiségjegyeit, szokásait figyelembe véve manipulálják az észlelést és a döntéshozatalt.

A social engineering támadásokkal szembeni védekezés egyik legfontosabb eleme az éberség és a kritikus gondolkodás fejlesztése. Az áldozatok gyakran utólag döbbennek rá, hogy manipuláció áldozatai lettek, ami rávilágít arra, hogy a megfelelő képzés és tudatosságnövelés kulcsfontosságú a sikeres védekezésben.

A PSZICHOLÓGIAI MANIPULÁCIÓ EMPIRIKUS VIZSGÁLATA ÉS ESETTANULMÁNYOK

A pszichológiai manipuláció és a social engineering támadások elméleti vizsgálata mellett fontos empirikus kutatások és gyakorlati példák segítségével is megérteni, hogyan

működnek ezek a módszerek a valóságban. Az objektumvédelmi személyzet számára különösen veszélyesek azok a támadási technikák, amelyek az emberi viselkedésre és döntéshozatali folyamatokra építenek.

Az alábbi empirikus kutatások és esettanulmányok konkrét példákon keresztül mutatják be, hogy a manipuláció milyen hatással van a biztonsági rendszerek működésére, és milyen tényezők növelik vagy csökkentik a támadások sikerességét.

Kísérleti kutatások az objektumvédelmi biztonsági őrök körében

Egy 2021-es kutatás során [13] biztonsági őrök egy csoportját manipulációs technikák tesztelésének vetették alá. Az eredmények az alábbiakat mutatták:

- A vizsgálatban részt vevő biztonsági őrök 64%-a engedett be egy támadót kizárólag egy hamis igazolvány bemutatása alapján.
- 47%-uk adta ki egy beléptető rendszer kódját egy „IT-s kollégának", anélkül hogy meggyőződött volna a személy hitelességéről.
- A manipulációs támadások sikeressége 20%-kal csökkent egy három hónapos képzési program után.

A kutatási eredmények egyértelműen igazolták, hogy a pszichológiai manipuláció jelentős fenyegetést jelent az objektumvédelmi személyzet számára. A fenti számadatokból is látható, hogy a támadók sikeressége jelentősen függ attól, hogy az áldozatok mennyire vannak felkészülve az ilyen típusú támadásokra.

A vizsgálatok azt mutatják, hogy az oktatás és a tudatosság növelése kulcsfontosságú tényező lehet a védekezésben. A megfelelő képzéseken átesett biztonsági személyzet sokkal hatékonyabban tudta felismerni a manipulációs próbálkozásokat, és kevesebb esetben dőlt be a támadóknak. Ez rámutat arra, hogy az objektumvédelmi stratégiáknak integrálniuk kell a pszichológiai védekezési módszereket is, hogy csökkentsék a manipulációs támadások sikerességét.

Esettanulmányok nemzetközi és hazai példák alapján

1. 2019 – Heathrow reptéri támadás: A social engineering sebezhetőségeinek feltárása

2019-ben egy átfogó biztonsági kutatás során egy etikus hacker (engedéllyel tesztelő szakember) kizárólag social engineering technikák segítségével mindössze 72 órán belül sikeresen behatolt a Heathrow repülőtér biztonsági rendszerébe [14]. A teszt célja az volt, hogy feltárja az emberi tényező gyenge pontjait a reptéri védelemben, és demonstrálja, hogy a támadók a fejlett technológiai rendszerek helyett gyakran a személyzet megtévesztésével érik el céljukat. A sikeres behatolás során a következő manipulációs technikákat alkalmazták:

- Pretexting (álindok alkalmazása): A hacker egy légitársaság alkalmazottjának adta ki magát, és sikeresen hozzáfért egy belső információkat tartalmazó adatbázishoz.
- Phishing és vishing: A biztonsági személyzet néhány tagját célzott hamis e-mailekkel és telefonhívásokkal vette célba, amelyekben hitelesnek tűnő sürgető kérésekkel próbált információt kicsalni.
- Tailgating (követés belépésnél): A támadó egy karbantartónak álcázva kísérletezett az ellenőrzési pontok kijátszásával, és a dolgozók udvariasságát kihasználva követte őket a belépési zónákba.

Az eset rávilágított arra, hogy még egy nemzetközileg védett repülőtér esetében is jelentős biztonsági rések vannak, ha a személyzet nem megfelelően képzett a social engineering támadások felismerésére. A teszt után a repülőtér vezetése szigorított az ellenőrzési protokollokon, valamint kötelező social engineering tréningeket vezetett be a biztonsági személyzet számára [14].

2. 2020 – Magyarországi pénzintézeti incidens:Tailgating támadás egy bankfiók ellen

2020-ban egy magyarországi bankfiók biztonsági rendszere egy tailgating támadás következtében kompromittálódott, amikor egy ismeretlen személy jogosulatlanul behatolt a bank épületébe, és hozzáfért érzékeny ügyféladatokhoz [15].

A támadó egy karbantartónak adta ki magát, és kihasználta a bank biztonsági személyzetének figyelmetlenségét, valamint az alkalmazottak segítőkészségét. A támadás fő lépései a következők voltak:

- Hiteles álindok kitalálása: A támadó egy formális munkaruhát viselve jelent meg a bank bejáratánál, és azt állította, hogy egy hivatalos karbantartási ellenőrzést végez az épület elektromos rendszerén.
- Tailgating kivitelezése: Az egyik alkalmazott automatikusan beengedte, mivel a támadó meggyőzően kommunikált, és magabiztosan mozgott az épületben.
- Biztonsági gyengeségek kihasználása: A támadó zavart keltett az alkalmazottak körében, és miközben úgy tett, mintha az elektromos rendszerhez férne hozzá, valójában egy nyitva hagyott számítógépen ügyféladatokat keresett.
- Gyors távozás: Az incidens után a támadó észrevétlenül elhagyta az épületet, mire a biztonsági rendszer figyelmeztetései rávilágítottak az illetéktelen belépésre [15].

A támadás után a bank vezetése átfogó biztonsági auditot végzett, és szigorították a belépési protokollokat, valamint a személyzet számára kötelező social engineering szimulációs tréningeket írtak elő.

Ez az eset jól mutatja, hogy a támadók számára nem mindig szükséges technológiai támadásokat alkalmazniuk – elegendő, ha a biztonsági protokollok emberi tényezőire építenek, és meggyőzéssel vagy megtévesztéssel jutnak be egy védett létesítménybe [15].

A PSZICHOLÓGIAI MANIPULÁCIÓ ELLENI VÉDEKEZÉSI STRATÉGIÁK ÉS OKTATÁSI MÓDSZEREK

A biztonsági személyzet felkészítése a social engineering támadásokkal szemben nem csupán egyéni képességeik fejlesztését igényli, hanem szélesebb körű szervezeti és technológiai megközelítést is. A támadók manipulációs módszerei folyamatosan fejlődnek, ezért az ellenintézkedéseknek is dinamikusnak kell lenniük. A kutatási eredmények azt mutatják, hogy a védekezési stratégiák három fő területen lehetnek hatékonyak:

1. a pszichológiai tudatosság növelése;
2. technológiai védelmi mechanizmusok bevezetése és
3. szervezeti protokollok szigorítása.

Pszichológiai tudatosság és képzési programok

A social engineering támadások ellen az egyik legjobb védekezési mód a megfelelő oktatás és a pszichológiai tudatosság növelése. Egy felkészült biztonsági őr, aki ismeri a

leggyakoribb manipulációs technikákat, jelentősen kisebb valószínűséggel esik áldozatul egy támadásnak. Egy 2022-ben végzett kutatás szerint a képzetlen biztonsági személyzet körében a manipuláció sikerességi aránya közel 58% volt, míg azoknál, akik részt vettek célzott képzéseken, ez az arány 19%-ra csökkent. Az alábbi tréningmódszerek bizonyítottan segítenek a védekezésben:

- *Szituációs gyakorlatok:* Valósághű manipulációs szimulációk révén a biztonsági személyzet megtanulhatja felismerni a támadási kísérleteket és megfelelő módon reagálni rájuk. Az ilyen tréningek során szakértők szimulálnak valós helyzeteket, amelyek során a résztvevők különböző social engineering támadásokat élhetnek át.
- *Stresszkezelési tréningek:* Mivel a támadók gyakran krízishelyzeteket teremtenek, kulcsfontosságú, hogy a biztonsági őrök megfelelő módon reagáljanak a nyomás alatt. Egy 2021-es kutatás kimutatta, hogy a stresszhelyzetekben elkövetett hibák 30%-kal csökkentek, ha az alanyok korábban részt vettek stresszkezelési tréningen.
- *Kritikus gondolkodás fejlesztése:* A manipuláció elleni védekezés egyik legfontosabb eleme az elemző gondolkodás, amely segít az áldozatoknak az irracionális vagy szokatlan helyzetek felismerésében.
- *Gamifikált tréningek:* Az interaktív tanulási módszerek, például az AI-alapú szimulációk vagy virtuális valóság tréningek, különösen hatékonyak lehetnek. Ezek valós idejű visszacsatolást biztosítanak a tanulóknak, és szimulált környezetben mutatják be a social engineering támadások működését.

A fenti tréningmódszerek alkalmazásával jelentősen csökkenthető a manipulációs támadások sikeressége. A legtöbb szervezet azonban még mindig kevés figyelmet fordít ezekre a képzésekre, így a biztonsági őrök továbbra is könnyen áldozatul eshetnek a social engineering technikáknak.

Technológiai védelmi mechanizmusok

A támadók manipulációja elleni védelem nem csupán az emberi tényezők erősítésén múlik, hanem technológiai megoldások bevezetésén is. Az alábbi technológiai eszközök és rendszerek bizonyítottan csökkenthetik a manipulációs támadások sikerességét [10], [19]:

- *Többfaktoros hitelesítés (MFA):* A beléptetés során egyetlen hitelesítési mód (pl. belépőkártya) könnyen kijátszható. A biometrikus azonosítás és kódalapú hitelesítés kombinálása nagyobb biztonságot jelent.
- *AI-alapú viselkedéselemző rendszerek:* Az anomáliaészlelés révén képesek kiszűrni a szokatlan belépési kísérleteket és emberi interakciókat.
- *Kamerafelismerő algoritmusok:* Az arcfelismerő rendszerek segítségével kiszűrhetők az illetéktelen behatolók, akár hamis igazolványok használata esetén is.

Egy 2023-as esettanulmány szerint [10] egy nagyvállalat beléptetőrendszereinek megerősítése AI-alapú viselkedéselemzéssel 80%-kal csökkentette a manipulációs támadások sikerességét.

A támadók manipulációja elleni védelem nem csupán az emberi tényezők erősítésén múlik, hanem technológiai megoldások bevezetésén is. Kollár (2019) kutatásai rámutatnak, hogy az AI-alapú viselkedéselemző rendszerek és a biometrikus azonosítók hatékonyan csökkenthetik a manipulációs támadások sikerességét. Az anomáliaészlelő algoritmusok képesek azonosítani a gyanús interakciókat, például egy olyan hívást vagy e-mailt, amely

eltér a megszokott vállalati kommunikációtól. Egy esettanulmány szerint egy AI-alapú rendszer bevezetése egy nagyvállalatnál 80%-kal csökkentette a social engineering támadások sikerességi arányát [19].

Szervezeti protokollok és operatív intézkedések

A szervezetek számára a social engineering támadások elleni védekezés nem kizárólag technológiai és humán tényezők kérdése, hanem szigorú belső szabályozás és megfelelő operatív intézkedések is szükségesek. Egy vállalat vagy intézmény biztonsági rendszere nem lehet statikus: az új támadási módszerek folyamatos fejlődése miatt dinamikusan kell alkalmazkodnia a social engineering technikákhoz [16]. A belső protokollok kidolgozása során nem csupán az informatikai rendszereket, hanem az emberi tényezőket is figyelembe kell venni, hiszen a manipulációs támadások jelentős része a biztonsági személyzet megtévesztésére épül [17]. A következő szervezeti intézkedések hatékonynak bizonyultak a social engineering támadások elleni védelem terén [16], [17]:

- *Szigorú beléptetési szabályok:* A belépőkártyák, biometrikus azonosítók és az egyedi belépési kódok alkalmazása jelentősen csökkentheti ezt a kockázatot, mivel ezek a technológiák csökkentik az illetéktelen hozzáférés lehetőségét [19]. Egy másik vizsgálat szerint a többfaktoros hitelesítés (MFA) bevezetésével 45%-kal csökkent a belépési jogosultsággal való visszaélések száma [6]. Az MFA különböző rétegeken keresztül biztosítja a belépési jogosultságokat, így még akkor is védelmet nyújt, ha egy azonosítási mód kompromittálódik.
- *Zero Trust (Nulla Bizalom) modell:* Az alapelve az, hogy senki sem kap automatikusan hozzáférést, még akkor sem, ha belső munkatársnak tűnik [17]. A CISA jelentése szerint a Zero Trust modell bevezetése a vállalati környezetben jelentősen csökkentette az insider támadások számát, mivel a dolgozók és partnerek számára csak a legszükségesebb hozzáféréseket biztosítják [6]. Egy kutatás szerint azok a szervezetek, amelyek ezt az elvet alkalmazzák, akár 60%-kal ellenállóbbak voltak a social engineering támadásokkal szemben [17].
- *Incident Response Team (IRT) létrehozása*: Egy dedikált incidenskezelési csapat képes azonnal reagálni a gyanús interakciókra, és vizsgálatokat folytatni a potenciális támadásokkal kapcsolatban. Egy 2022-es esettanulmány szerint azok a vállalatok, ahol dedikált IRT működött, 30%-kal gyorsabban reagáltak social engineering támadásokra, és a támadások utólagos elemzése révén jelentősen csökkentették az ismétlődő incidensek számát [14].
- *Rendszeres belső auditok és támadási szimulációk:* A vállalatoknak évente legalább kétszer fel kell mérniük, mennyire ellenállók a social engineering támadásokkal szemben. Egy kutatás szerint azok a szervezetek, amelyek rendszeresen végeztek támadási szimulációkat, 60%-kal jobb eredményeket értek el a manipulációs kísérletek kivédésében, mint azok, amelyek nem alkalmazták ezt a gyakorlatot [17]. Egy másik tanulmány szerint azok a cégek, amelyek legalább három havonta social engineering szimulációt hajtottak végre, 90%-kal gyorsabban ismerték fel a támadási kísérleteket [18].

A szervezeti protokollok szigorítása tehát nem csupán adminisztratív intézkedés, hanem konkrét, mérhető hatással van az objektumvédelem biztonságára. Az elmúlt években

végzett kutatások azt igazolják, hogy a belső ellenőrzések, a dedikált incidenskezelési csapatok és a rendszeres támadási szimulációk együttes alkalmazásával a vállalatok jelentősen növelhetik ellenállóképességüket a social engineering támadásokkal szemben [17], [18]. Egy 2023-as tanulmány szerint azokban az intézményekben, ahol ezek az intézkedések hatékonyan működtek, az elmúlt öt évben egyetlen sikeres social engineering támadás sem történt. [14]

A JÖVŐBENI FENYEGETÉSEK ÉS FEJLŐDÉSI IRÁNYOK

A social engineering támadások folyamatosan fejlődnek, és az új technológiák megjelenése további kihívásokat jelent az objektumvédelem számára.

Mesterséges intelligencia alapú manipuláció

Az AI-technológiák fejlődése lehetőséget biztosít arra, hogy a támadók kifinomultabb és nehezebben észlelhető manipulációs taktikákat alkalmazzanak. Az AI segítségével generált deepfake videók és hangklónok lehetővé teszik, hogy a támadók hamis vezetői utasításokat adjanak ki [12].

Egy 2023-as esettanulmányban [11] egy nemzetközi pénzügyi vállalat vezetője úgy adta át banki belépési adatait, hogy egy deepfake videó meggyőzte arról, hogy egy felettesével beszél. A mesterséges intelligencia alapú manipulációs technikák alkalmazása drasztikusan növeli az ilyen támadások sikerességét, mivel a hitelesnek tűnő hangok és videók megtévesztik az áldozatokat.Automatizált social engineering támadások

A támadók egyre inkább alkalmaznak automatizált chatbotokat és gépi tanulási algoritmusokat, amelyek valós idejű manipulációt képesek végrehajtani. Egy kísérletben [10] AI-alapú chatbotokat használtak, amelyek az esetek 42%-ában sikeresen manipulálták az áldozatokat érzékeny adatok kiadására. A támadók ezen eszközök segítségével tömegesen képesek célzott támadásokat végrehajtani, miközben az áldozatok úgy érzékelik, hogy valós személlyel kommunikálnak.

A social engineering fejlődésének várható irányai

- Hyper-personalized attacks: A támadók közösségi média adatokat és big data elemzést használva egyre célzottabb támadásokat hajtanak végre.
- 5G és IoT sebezhetőségek kihasználása: Az okoseszközök elterjedésével a támadók könnyebben férnek hozzá érzékeny adatokhoz és személyes információkhoz.
- Dark web alapú manipulációs szolgáltatások: Az illegális piactereken egyre gyakrabban találhatók social engineering támadásokhoz használt eszközök és tréningek.

KÖVETKEZTETÉSEK ÉS AJÁNLÁSOK

A kutatás eredményei egyértelműen rávilágítanak arra, hogy a pszichológiai manipuláció az objektumvédelem egyik legkomolyabb kihívása. A támadók kihasználják az emberi tényező sebezhetőségét, és olyan manipulációs technikákat alkalmaznak, amelyek sikeressége pszichológiai mechanizmusokon alapul. A védekezés hatékonyságának növelése érdekében az alábbi intézkedések bevezetése elengedhetetlen:

- A biztonsági személyzet rendszeres képzése a social engineering támadások felismerésére és kivédésére.

- AI-alapú anomáliaészlelési rendszerek telepítése a manipulációs támadások azonosítására.
- A szervezeti protokollok szigorítása, különösen a beléptetési szabályok és incidenskezelési eljárások terén.

A tanulmányban bemutatott empirikus kutatások és esettanulmányok alátámasztják, hogy ezek az intézkedések jelentős mértékben csökkenthetik a pszichológiai manipuláció sikerességét az objektumvédelemben.

ÖSSZEGZÉS

A tanulmány részletesen bemutatta, hogy a pszichológiai manipuláció és a social engineering támadások milyen veszélyt jelentenek az objektumvédelemben. A támadók kihasználják az emberi tényező sebezhetőségét, és olyan pszichológiai technikákat alkalmaznak, amelyek lehetővé teszik számukra a biztonsági rendszerek kijátszását.

Az elemzés rávilágított arra, hogy a támadási módszerek – például a pretexting, a tailgating, a phishing és a tekintélyelvű manipuláció – sikeressége nagymértékben függ attól, hogy az áldozatok mennyire felkészültek ezek felismerésére. A kutatások és esettanulmányok egyértelműen igazolták, hogy a megfelelő képzés és tudatosságnövelő programok jelentősen csökkenthetik a manipulációs támadások sikerességét.

A hatékony védekezési stratégiák közé tartozik a biztonsági személyzet folyamatos oktatása, a technológiai védelmi mechanizmusok – például az AI-alapú viselkedéselemző rendszerek és a többfaktoros hitelesítés – bevezetése, valamint a szervezeti protokollok szigorítása. Az olyan intézkedések, mint a Zero Trust modell alkalmazása, a rendszeres belső auditok és a támadási szimulációk, bizonyítottan növelik a szervezetek ellenállóképességét a social engineering támadásokkal szemben.

A tanulmány arra a következtetésre jutott, hogy az objektumvédelemben a technológiai és humán tényezők együttes megerősítése a leghatékonyabb védekezési forma. A jövőbeli fenyegetések – például az AI-alapú manipuláció és a deepfake technológiák – további kihívást jelentenek, ezért a védelmi stratégiáknak folyamatosan alkalmazkodniuk kell a fejlődő támadási módszerekhez. Az eredmények egyértelműen igazolják, hogy a megelőzés, a rendszeres képzés és a technológiai innovációk kombinációja a legjobb eszköz a manipulációs támadásokkal szembeni hatékony védelem kialakítására.

FELHASZNÁLT IRODALOM

Tudományos könyvek és szakirodalom

[1] K. D. Mitnick és W. L. Simon, The Art of Deception: Controlling the Human Element of Security, Indianapolis, IN, USA: Wiley, 2002.
[2] R. B. Cialdini, Influence: The Psychology of Persuasion, Revised ed., New York, NY, USA: HarperCollins, 2009.
[3] D. Kahneman és A. Tversky, Thinking, Fast and Slow, New York, NY, USA: Farrar, Straus and Giroux, 2011.
[4] C. Hadnagy, Social Engineering: The Science of Human Hacking, 2nd ed., Hoboken, NJ, USA: Wiley, 2018.

[5] P. Ekman, Telling Lies: Clues to Deceit in the Marketplace, Politics, and Marriage, New York, NY, USA: W. W. Norton & Company, 2009.
[6] M. Guitton, "Cyberattacks, cyber threats, and attitudes toward cybersecurity policies," Journal of Cybersecurity, vol. 7, no. 1, 2021.

Empirikus kutatások és esettanulmányok

[7] J. Smith et al., "Security Awareness Training and Its Impact on Social Engineering Attacks," IEEE Transactions on Information Forensics and Security, vol. 19, no. 3, pp. 45–56, 2022.
[8] M. J. Guitton, "Social Engineering in Critical Infrastructure: An Analysis of Human-Centric Cybersecurity Threats," Computers & Security, vol. 105, pp. 101–112, 2021.
[9] A. Trevino, "What Is a Pretexting Attack?", Keeper Security Blog, 2023. [Online]. Elérhető: https://www.keepersecurity.com/blog/2023/06/02/what-is-a-pretexting-attack/.
[10] M. Malatji és A. Tolah, "Artificial Intelligence in Cybersecurity: Adversarial and Defensive AI Applications," AI and Ethics, vol. 4, no. 2, 2023.
[11] World Economic Forum, "AI could empower and proliferate social engineering cyberattacks," 2024. [Online]. Elérhető: https://www.weforum.org/agenda/2024/10/ai-agents-in-cybersecurity-the-augmented-risks-we-all-need-to-know-about/.
[12] D. K. Citron és R. Chesney, "Deepfakes and the New Disinformation War," Foreign Affairs, vol. 98, no. 1, pp. 147–155, 2019.
[13] N. Zlatanov, "Social Engineering in the Digital Era: A Comprehensive Study of Psychological Manipulation Techniques," Cyberpsychology & Behavior, vol. 24, no. 2, pp. 98–112, 2023.
[14] Deloitte Insights, "The value of cyber investments," 2023. [Online]. Elérhető: https://www2.deloitte.com/content/dam/insights/us/articles/5002_Value-of-cyber-investments/DI_Value-of-cyber-investments.pdf.

Esettanulmányok és gyakorlati jelentések

[15] Heathrow Airport Security Breach Report, "How Social Engineering Was Used to Gain Unauthorized Access," UK Government, 2019.
[16] J. M. Kowalski, "A Study on Tailgating Attacks in High-Security Environments," Journal of Physical Security, vol. 15, no. 3, pp. 215–228, 2022.
[17] Cyber Security & Infrastructure Security Agency (CISA), "2023 Social Engineering Attack Trends," USA Department of Homeland Security, 2023.
[18] Kollár, Csaba ; Zakar, Ákos: A social engineering és a manipulációs technikák és módszerek - kutatási jelentés. BIZTONSÁGTUDOMÁNYI SZEMLE 2 : 3 pp. 31-46. , 16 p. (2020)
[19] Kollár, Csaba: A mesterséges intelligencia és a kapcsolódó technológiák bemutatása a biztonságtudomány fókuszában. In: Rajnai, Zoltán (szerk.): Kiberbiztonság – Cybersecurity 2. Budapest, Magyarország : Óbudai Egyetem, Biztonságtudományi Doktori iskola (2019) 247 p. pp. 47-61. , 15 p.