# THE EVOLUTION AND FUTURE OF SOCIAL ENGINEERING: EXPLOITING PSYCHOLOGICAL VULNERABILITIES IN THE DIGITAL AGE

# A SOCIAL ENGINEERING FEJLŐDÉSE ÉS JÖVŐJE: A PSZICHOLÓGIAI SEBEZHETŐSÉGEK KIHASZNÁLÁSA A DIGITÁLIS KORBAN

MÁRTON Zoltán[1] – RAJNAI Zoltán[2]

**Abstract**

The study presents the history, evolution, and current threats of social engineering, with a focus on exploiting human psychological vulnerabilities. It discusses both early and modern techniques, such as spear phishing, pretexting, and deepfake manipulation, which are becoming even more targeted with the use of artificial intelligence and machine learning technologies. The study also addresses defense strategies, emphasizing the importance of education, technological safeguards, and strict organizational protocols, while highlighting the future risks of social engineering and the need for continuous protective measures.

**Keywords**

social engineering, psychological vulnerabilities, spear phishing, pretexting deepfake manipulation, Artificial intelligence, machine learning, cybersecurity, defense strategies, organizational protocols

**Absztrakt**

A tanulmány a social engineering történetét, fejlődési irányait és jelenlegi fenyegetéseit mutatja be, különös tekintettel az emberi pszichológiai sebezhetőségek kihasználására. Bemutatásra kerülnek a korai és modern technikák, mint a „spear phishing”, „pretexting” és a „deepfake” manipuláció, amelyek a mesterséges intelligencia és a gépi tanulás technológiákkal még célzottabbá válnak. A tanulmány kitér a védekezési stratégiákra is, kiemelve az oktatás, technológiai védelem és a szigorú szervezeti protokollok fontosságát, valamint figyelmeztet a social engineering jövőbeli veszélyeire és a folyamatos védelem szükségességére.

**Kulcsszavak**

social engineering, pszichológiai sebezhetőségek, spear phishing, pretexting, deepfake manipuláció, mesterséges intelligencia, gépi tanulás, kiberbiztonság, védelmi stratégiák, szervezeti protokollok

[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

DOI: https://doi.org/10.12700/btsz.2024.6.4.45

## BEVEZETÉS

A social engineering az információbiztonság egyik leggyorsabban fejlődő területe, mivel a támadók egyre kifinomultabb eszközöket alkalmaznak az emberi pszichológiai sebezhetőségek kihasználására. Az ilyen típusú támadások középpontjában az emberi természet alapvető jellemzői, mint a bizalom, segítőkészség és kíváncsiság állnak, melyeket a támadók manipuláció révén használnak ki a céljaik elérésére. A social engineering a technológiai fejlődéssel párhuzamosan fejlődik: a digitális kommunikáció és az online adatmegosztás növekedésével egyre több támadási csatorna válik elérhetővé a támadók számára, legyen szó e-mailes, közösségi média vagy mobilalapú támadásokról.

A tanulmány célja, hogy átfogó képet nyújtson a social engineering technikák történeti fejlődéséről és jelenlegi alkalmazásairól, bemutatva a legelterjedtebb támadási formákat és azok pszichológiai alapjait. Emellett részletesen kitér a védekezési stratégiákra, melyek segítségével a szervezetek és egyének csökkenthetik a social engineering támadások kockázatát. A jövőbeli kilátások ismertetésével a tanulmány felhívja a figyelmet azokra az új technológiákra, mint a mesterséges intelligencia és gépi tanulás, amelyek lehetőséget adnak a támadások további személyre szabására és hatékonyságuk növelésére.

## A SOCIAL ENGINEERING FOGALMA ÉS KORAI PÉLDÁI

A social engineering technikái alapvetően az emberi pszichológia sajátosságain alapulnak, és a támadók tudatosan kihasználják az olyan ösztönös emberi tulajdonságokat, mint a bizalom, a segítőkészség, a félelem, vagy a kíváncsiság. [1] Ezeknek a pszichológiai tényezőknek a kihasználásával a támadók az áldozatokból olyan cselekvéseket váltanak ki, amelyek különben nem állnának szándékukban, így tehát érzékeny információkat adnak át vagy jogosulatlan hozzáférést biztosítanak rendszerekhez. [2] A támadások pszichológiai háttere különösen hatékonynak bizonyul, mivel az emberek többsége nem rendelkezik megfelelő ismeretekkel és tudatossággal a social engineering technikáival szemben, és így hajlamosak információkat kiadni akkor is, ha a kérés forrása gyanúsnak tűnhet. [3] A támadók gyakran építenek a hatóság, a szakmai hierarchia vagy a sürgősség érzetére, melyek mind hatást gyakorolhatnak az áldozatok döntéseire, különösen olyan helyzetekben, ahol a felhasználók saját kritikus gondolkodásukat háttérbe szorítva cselekszenek. [4]

### Korai social engineering technikák

A korai social engineering módszerek a manipuláció alapvető, de hatékony technikáira épültek, melyek már ekkor bizonyították a támadók pszichológiai hatalomgyakorlásának erejét. Az egyik legismertebb módszer a „pretexting” volt, amely során a támadók kidolgozott fedősztorikkal operáltak, és mesterséges helyzeteket hoztak létre annak érdekében, hogy az áldozatokat megtévesszék és a hitelesség látszatát keltsék. [2] Ilyenkor a támadók egy megbízható személy, adott esetben egy banki alkalmazott vagy kormányzati tisztviselő képviselőjeként jelentek meg, így növelve annak esélyét, hogy az áldozatok önként rendelkezésre bocsájtsák a bizalmas információkat. [1]

A „baiting” technika különösen alattomos volt, hiszen a támadók olyan csalogató eszközöket – „talált” USB-meghajtókat vagy ingyenes szoftvereket – használtak, amelyekkel kihasználták az áldozatok természetes kíváncsiságát. Az ilyen eszközöket a támadók kártékony szoftverrel fertőzték meg, amely az áldozat rendszerébe kerülve azonnal aktiválódott, ezzel lehetővé téve a támadó számára a rendszer teljes körű hozzáférését. [4] Az

ilyen korai technikák rávilágítanak arra, hogy a social engineering hogyan használja ki a felhasználói figyelmetlenséget és bizalmat, kihasználva az emberi természet alapvető hajlamait az adathalászat, rendszerhozzáférés és további kártékony tevékenységek eléréséhez. [3]

### A social engineering kezdeti hatékonysága és jelentősége

A social engineering korai története világosan bemutatja, hogy a támadók miként igazodtak az adott korszak technológiai és társadalmi környezetéhez, folyamatosan tökéletesítve módszereiket. E technikák nemcsak egyszerű manipulációs eszközök voltak, hanem alapvető szociálpszichológiai törvényszerűségekre építkeztek, amelyek a bizalom, a segítőkészség, valamint a félelem ösztönös emberi reakcióit használták ki. [1] Az emberi természet ezen alapvető jellemzőinek kihasználása révén a social engineering lehetővé teszi, hogy a támadók az áldozatok viselkedését precízen irányítsák, gyakran az áldozatok tudtán kívül. [3]

A módszer történelmi jelentősége különösen abban rejlik, hogy rámutat az emberi tényező sebezhetőségére, amely semmilyen technikai védelemmel nem küszöbölhető ki teljesen. Az emberek természetes reakcióit nem képesek befolyásolni még a legkifinomultabb kiberbiztonsági rendszerek sem. A social engineering ezen sebezhetőség kiaknázására épült, és alapját képezi a modern kibertámadási módszereknek, amelyek napjainkban is jelentős fenyegetést jelentenek. [2] A korai technikák, mint a „pretexting” és „baiting”, megágyaztak azoknak a kifinomult támadási formáknak, amelyek csak folyamatos oktatással, a felhasználói tudatosság növelésével, valamint a szociálpszichológiai tényezők mély megértésével kezelhetők hatékonyan. [3]

## FEJLŐDÉSE ÉS A SOCIAL ENGINEERING EVOLÚCIÓJA

### Az internet megjelenése és az e-mail alapú támadások

Az internet térhódítása forradalmi hatást gyakorolt a social engineering technikák fejlődésére, új lehetőségeket nyitva a támadók számára, és ezáltal jelentős kihívást jelentve az információbiztonság számára. [1] Az e-mail alapú adathalászat, vagy „phishing”, az egyik legelterjedtebb módszerré vált, mivel viszonylag alacsony költséggel és kockázattal jár a támadók számára, ugyanakkor széleskörű elérhetőséget biztosít számukra. Az ilyen támadások során az e-mailek gyakran hivatalos szervezetek - bankok vagy neves vállalatok nevében érkeznek, és megtévesztő tartalommal manipulálják a felhasználókat, arra ösztönözve őket, hogy bizalmas információikat – jelszavaikat és banki azonosítóikat – kiadják.

A Verizon Data Breach Investigations Report (2021) adatai szerint a kibertámadások több mint 90%-a social engineering technikákra épít, különösen az adathalászat révén, amely egyre finomodik és egyre több formát ölt. [5] Az e-mailes adathalászat különböző típusai, a hamis számlaértesítések és megtévesztő promóciós ajánlatok, tovább növelték a social engineering fenyegetését azáltal, hogy az áldozatok hitelesség iránti bizalmára építenek, így könnyen manipulálhatók a gyanútlan felhasználók.

### Közösségi média és social engineering

A közösségi média platformok, mint a Facebook, Twitter vagy Instagram, új csatornákat nyitottak a social engineering számára, mivel a felhasználók személyes információkat osztanak meg, amelyeket a támadók célzott támadások kivitelezésére használnak fel.

[1] Ezeken a platformokon végzett adatgyűjtés során a támadók képesek részletes személyes profilokat kialakítani az áldozatok kapcsolatai, érdeklődési körei és mindennapi tevékenységei alapján, lehetővé téve a támadások finomhangolását és a személyre szabott megközelítést. Ezen közösségi oldalak különösen alkalmassá teszik a „spear phishing" típusú támadások lebonyolítását, ahol a támadók konkrét személyeket céloznak meg az emberek közösségi kapcsolatait és online viselkedési mintáit kihasználva, így növelve a siker valószínűségét. [5], [6]

**Mobiltechnológia és social engineering**

A mobiltelefonok és okoseszközök széles körű elterjedése új támadási felületeket biztosított a social engineering számára. Az SMS-alapú adathalászat, vagy „smishing", valamint a hangalapú adathalászat, azaz „vishing", lehetőséget adnak a támadóknak arra, hogy közvetlen üzenetekben, sürgősséget színlelve manipulálják áldozataikat. [4] Az ilyen támadások gyakran fenyegető vagy sürgető üzeneteket tartalmaznak - banki műveletek vagy szolgáltatások felfüggesztésének hivatkozásával -, amellyel az áldozatokat azonnali cselekvésre késztetik. A mobil eszközök adathalászat elleni védelme kiemelt biztonsági kihívás, mivel a felhasználók gyakran kevésbé körültekintőek mobil eszközeiken, mint asztali környezetben, így nagyobb eséllyel válnak támadások áldozataivá.

## MODERN SOCIAL ENGINEERING TECHNIKÁK

**„Spear phishing"**

A „spear phishing" célzott adathalász támadás, amely során a támadók részletes információgyűjtést követően egy adott személyt vagy szervezetet céloznak meg, hogy megtévesszék és érzékeny adatokat szerezzenek tőle. [5] A támadók gyakran átfogó kutatást végeznek a célpontjukról, beleértve annak munkahelyi szerepét, érdeklődési köreit, szokásait és közösségi média jelenlétét, hogy az üzenet a lehető leghitelesebbnek tűnjön. Az ilyen típusú támadások sokkal kifinomultabbak, mint az általános „phishing" kísérletek, mivel a személyre szabott üzenetek fokozzák a hitelességet, és növelik a siker esélyét. Konkrét esetet nézve, egy pénzügyi vezető számára küldött üzenet belső üzleti szabályozásokra hivatkozhat, vagy akár valós kapcsolati neveket és eseményeket tartalmazhat, hogy elérje a kívánt manipulációs hatást. [8]

A „spear phishing" támadások jellemzően alaposan megtervezettek, hogy a hagyományos biztonsági szűrők elől rejtve maradjanak. Ezt a hatást a támadók egyre gyakrabban mesterséges intelligencia segítségével érik el, amely képes a célpont online aktivitását figyelemmel kísérni, és az érdeklődési körök alapján optimalizálni a támadási módszereket. [8] Az 1. ábrán látható a „spear phishing" támadás teljes folyamata, amely bemutatja a támadó adatgyűjtési fázisától kezdve a célzott üzenet kidolgozásán át egészen az áldozat reakciójáig.


*1. ábra - A "spear phishing" támadás lépései (saját ábra)*

## A „spear phishing” támadás lépései

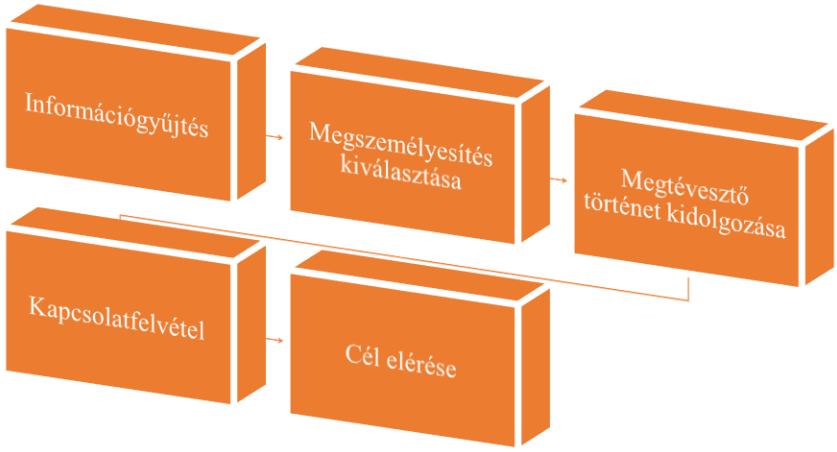
- A támadó kiválaszt egy konkrét személyt vagy szervezetet, akit célba kíván venni. Ezt követően részletes információkat gyűjt róla, beleértve személyes, szakmai vagy online jelenlétéhez kapcsolódó adatokat, hogy a támadás hitelesnek tűnjön és növelje a megtévesztés esélyét.
- Az információgyűjtést követően a támadó egy hitelesnek látszó e-mailt hoz létre, amely megfelel a célpont érdeklődési körének, szakmai környezetének vagy kapcsolatainak. Az üzenet formázása és tartalma a megtévesztést szolgálja, gyakran megbízhatónak tűnő forrásként, például egy ismerős személy vagy szervezet nevében érkezik.
- A célpont megkapja az e-mailt, és amint megnyitja vagy rákattint az üzenetben található linkre, a rosszindulatú program aktiválódik. Ez lehet egy rejtett malware, amely hozzáférést biztosít a támadónak a célpont eszközeihez vagy hálózatához.
- Miután a rosszindulatú program települt, a támadó hozzáférést nyer a célpont érzékeny adataihoz, beleértve bizalmas információkat, jelszavakat vagy egyéb fontos adatokat, amelyeket később visszaélés céljából felhasználhat.

## „Pretexting”

A „pretexting” egy kifinomult social engineering technika, amelynek célja, hogy a támadó előre megtervezett és részletesen kidolgozott történetet – pretextet – használjon az áldozat megtévesztésére. A támadó részletes előkészületeket tesz, beleértve az áldozat munkahelyi vagy személyes környezetének, érdeklődési köreinek és kapcsolatrendszerének tanulmányozását, hogy minden elem hitelesnek tűnjön, így meggyőző szerepjátékot tudjon folytatni. Ennek során a támadó akár egy hivatalos szereplő – akár egy IT-támogató vagy egy pénzügyi tanácsadó – bőrébe bújik, akinek látszólag jogosult hozzáférése van az áldozat bizalmas információihoz.

A „pretexting” különösen veszélyes, mert az áldozatok gyakran hajlamosak megbízni olyan személyekben, akikről feltételezik, hogy hivatalos pozícióban vagy megbízható intézmény képviseletében állnak. Az ilyen támadások gyakran hosszú távú meggyőzési stratégián alapulnak: a támadó fokozatosan építi fel az áldozat bizalmát, hogy az végül önként adjon át érzékeny adatokat. [9]

Mouton, Leenen és Venter social engineering támadási keretrendszere szerint a „pretexting” az egyik legnehezebben felismerhető social engineering módszer. Ennek oka, hogy a támadók komplex, többfázisú stratégiákat használnak, amelyek során az áldozat érzelmi biztonságérzetére és segítőkészségére építenek. A támadó gyakran személyre szabott történetekkel, részletes szerepjátékokkal erősíti a hitelesség látszatát, így még a jól képzett felhasználók számára is nehéz felismerni a megtévesztést.[7]




*2. ábra - A "pretexting" támadás lépései (saját ábra)*

A „pretexting” egy komplex social engineering módszer, amelynek során a támadó részletesen kidolgozott történetet vagy szerepet használ annak érdekében, hogy bizalmat építsen ki és megtévessze az áldozatot. A „pretexting” támadás sikeressége gyakran a támadó előkészületein és az áldozat bizalmának fokozatos megszerzésén alapul. Az alábbiakban bemutatjuk a „pretexting” támadás fő lépéseit, amelyet a 2. ábra szemléltet. [8]

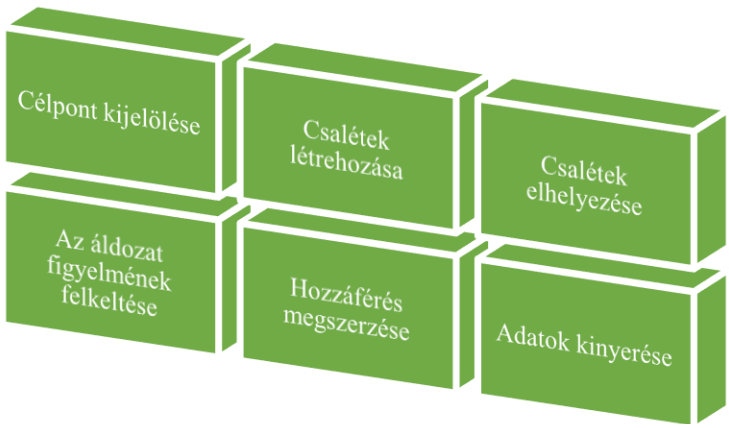
- Az első lépésben a kiberbűnöző alapos kutatást végez az áldozatról. Célja, hogy minél több személyes vagy szakmai adatot gyűjtsön össze, amelyek később felhasználhatók a megtévesztés során. Ezek az információk lehetnek az áldozat munkahelyi szerepkörei, kapcsolati hálója, online jelenléte vagy akár a közösségi médián megosztott személyes információk. A támadó ezek alapján megérti, milyen adatok és kapcsolatok révén közelíthet az áldozathoz hitelesen. [8]
- Az információgyűjtést követően a támadó kiválasztja a megfelelő megszemélyesítést, vagyis eldönti, hogy milyen szerepet fog betölteni az áldozattal való kommunikáció során. A támadó gyakran egy megbízhatónak tekintett személy vagy pozíció szerepébe helyezkedik, például egy banki alkalmazott, egy munkahelyi felettes vagy egy közeli ismerős szerepét ölti magára. A megfelelő személy vagy szerep kiválasztása alapvető fontosságú, mivel ez biztosítja a támadás hitelességét az áldozat szemében. [8]
- Miután kiválasztotta a megszemélyesítést, a kiberbűnöző részletes, hitelesnek tűnő történetet dolgoz ki. Ez a narratíva gyakran valósághű eseményekre vagy helyzetekre épül, amelyekkel az áldozat valószínűleg találkozott már, vagy amelyek kapcsolódnak az áldozat környezetéhez. A megtévesztő történet célja, hogy felkeltse az áldozat bizalmát és elhitesse vele, hogy a támadó valóban az, akinek mondja

magát. Ez a történet lehet sürgető vagy bizalmas jellegű, hogy az áldozat úgy érezze, gyorsan kell cselekednie. [8]

- A támadó ezután kapcsolatba lép az áldozattal a kiválasztott szerep és megtévesztő történet felhasználásával. A kapcsolatfelvétel történhet e-mailben, telefonhíváson, közösségi média üzeneten vagy más kommunikációs csatornán keresztül. Ebben a lépésben a támadó célja, hogy az áldozat figyelmét felkeltse, és bizalmi kapcsolatot alakítson ki vele, így megteremtve a sikeres támadás alapját. A támadó gyakran kifinomult szerepjátékot alkalmaz, amely révén képes elérni, hogy az áldozat ne érezze gyanúsnak a megkeresést. **[**8]
- A támadás végső célja, hogy a támadó megszerezze az áldozattól a kívánt információt vagy anyagi javakat. Ezt a támadó a hitelesen előadott történeten és a kialakult bizalmi kapcsolaton keresztül éri el. Gyakori cél lehet pénz átutalása, bizalmas adatok, jelszavak, azonosítók vagy egyéb érzékeny információk megszerzése. A támadó a bizalomra és hitelességre alapozva manipulálja az áldozatot, hogy saját döntéséből, önként adja ki a kért információkat vagy kövesse a támadó utasításait. [8]

**„Baiting”**

A „baiting” során a támadók valamilyen csábító ajánlatot vagy ígéretet használnak arra, hogy az áldozatokat káros cselekvésre késztessék (lásd: 3 ábra): fertőzött fájl letöltésére vagy kártékony weboldalak felkeresésére. [2] Gyakori eset az ingyenes zene- vagy filmletöltés, amely mögött kártékony szoftverek rejtőznek. A támadók előnyükre fordítják az áldozatok kíváncsiságát és érdeklődését, így gyakran elegendő egy vonzó, de megtévesztő üzenetet közvetíteniük ahhoz, hogy elérjék céljukat. Karen, Ryan, Shay, Daphana tanulmánya szerint a „baiting” hatékonysága nagymértékben azon múlik, hogy mennyire igazodik a célcsoport érdeklődési köreihez. A támadás sikeresnek ítélhető, ha a csaléteknek használt ajánlat vonzó és releváns a célzott felhasználók számára, ezáltal növelve annak esélyét, hogy az áldozatok figyelmen kívül hagyják az esetleges biztonsági kockázatokat. [9]




*3. ábra - A "baiting" támadás lépései (saját ábra)*

A „baiting” az egyik leggyakrabban használt szociális manipulációs technika a kiberbiztonság területén, amely egy vonzó ajánlat vagy fájl segítségével próbálja rávenni az

áldozatot arra, hogy önkéntesen biztosítson hozzáférést a támadónak. Az alábbiakban bemutatjuk a baiting technika működését lépésről lépésre, amelyet a 3. ábra szemléltet:

- A támadó kiválaszt egy megfelelő célpontot – lehet ez egy vállalat vagy egy egyén –, aki valószínűleg érdeklődést mutat a csali iránt.
- A támadó vonzó csalit hoz létre, egy érdekesnek tűnő digitális fájlt (program, zene, dokumentum) vagy egy elhagyott USB meghajtót akár.
- A csalit elhelyezhetik digitális térben, így e-mailekben vagy közösségi média linkek formájában, vagy fizikai térben, tehát egy munkahely közelében elhagyott USB meghajtón.
- A csali célja az áldozat kíváncsiságának felkeltése. Az áldozat gyakran azt hiszi, hogy a csali valamilyen előnnyel jár, példának kedvéért: hasznos információkat vagy ingyenes hozzáférést biztosít.
- Amikor az áldozat rákattint egy linkre vagy megnyitja a csalival ellátott fájlt, a támadó hozzáférést szerez az áldozat eszközéhez vagy hálózatához, malware vagy adatgyűjtő szoftver révén.
- A támadó a megszerzett hozzáférés révén érzékeny adatokat szerezhet meg, amelyeket felhasználhat vagy akár zsarolásra is alkalmazhat.

## VÉDEKEZÉSI STRATÉGIÁK A SOCIAL ENGINEERING ELLEN

### Oktatás és tudatosság

Az egyik leghatékonyabb védekezési stratégia a social engineering támadásokkal szemben a felhasználók folyamatos oktatása és tudatosságnövelése. A social engineering támadások sikeressége gyakran a felhasználók tájékozatlanságán múlik, ezért fontos, hogy rendszeres képzésekkel, szemináriumokkal és szimulációkkal fejlesszék a dolgozók éberségét és felkészültségét. [1] A szimulációk lehetőséget adnak arra, hogy a felhasználók biztonságos környezetben tanulják meg felismerni a gyanús e-maileket, linkeket vagy telefonhívásokat, és hogy azonnal felismerjék a manipulációs kísérleteket, így tehát a „phishing" vagy a „pretexting" technikákat. Karen, Ryan, Shay, Daphana tanulmánya szerint a rendszeres oktatás és a folyamatos tudatosságnövelés nemcsak a támadások észlelésében, hanem a felhasználók gyors és megfelelő reagálásában is jelentős javulást eredményez. Az oktatási programok során a felhasználók nagyobb elkötelezettséget mutatnak a kibervédelmi protokollok betartása iránt, ezáltal csökkentve a szervezet sebezhetőségét. [9]

### Technikai megoldások

A technológiai eszközök használata szintén fontos szerepet játszik a social engineering támadások elleni védekezésben. A kétfaktoros hitelesítés (2FA) jelentősen csökkentheti a támadások sikerességét azáltal, hogy további védelmi réteget biztosít, melyet a támadóknak le kell küzdeniük. [10] Emellett a fejlett spamszűrők és a biztonsági szoftverek használata fontos az adathalász e-mailek kiszűrésére, valamint a hálózati fenyegetések automatikus észlelésére. A rendszeres szoftverfrissítések és biztonsági javítások kulcsfontosságúak, mivel számos social engineering támadás a sebezhetőségeken alapul. Tushaar, Jaidhar & Bhabesh tanulmánya szerint a gépi tanulással támogatott korszerű spamszűrők jelentős fejlődést képviselnek a célzott támadások, ezáltal a „phishing" e-mailek kiszűrésé-

ben. Ezek a rendszerek képesek hatékonyan azonosítani az e-mailekben rejlő gyanús mintákat és anomáliákat, ezáltal fokozva a támadásokkal szembeni védekezés hatékonyságát. [11]

### Szervezeti intézkedések

A vállalati biztonság erősítése érdekében a szervezeteknek szigorú biztonsági protokollokat kell bevezetniük. Az információkhoz való hozzáférés szigorú szabályozása, a minimális hozzáférés elvével (principle of least privilege), csökkenti a social engineering kockázatát azáltal, hogy csak a szükséges információkat és rendszereket teszi elérhetővé az alkalmazottak számára. [7] Emellett a gyanús tevékenységek azonnali jelentésének ösztönzése – egy egyszerűen használható bejelentési rendszer révén – gyorsabb reagálást tesz lehetővé. A belső auditok, biztonsági tesztek és sérülékenységvizsgálatok szintén segíthetnek a lehetséges sebezhetőségek feltárásában és orvoslásában, mielőtt azok valódi támadások célpontjává válnának. [12] A rendszeres belső ellenőrzés és a biztonsági incidensek kivizsgálása tovább növeli a szervezet ellenálló képességét.

## JÖVŐBELI KILÁTÁSOK ÉS A SOCIAL ENGINEERING VÁRHATÓ FEJLŐDÉSE

A social engineering támadások egyre kifinomultabbá és célzottabbá válnak, mivel a támadók gyorsan alkalmazkodnak a technológiai újításokhoz, kihasználva a mesterséges intelligencia (továbbiakban: AI), a gépi tanulás (továbbiakban: ML) és az adatelemzés által kínált lehetőségeket. Ezek a technológiák lehetővé teszik a támadók számára, hogy sokkal pontosabb és személyre szabottabb támadásokat hajtsanak végre, miközben minimalizálják a felfedezés kockázatát. Az elkövetkező években ezek a technikák még összetettebbé és nehezebben felismerhetővé válhatnak, különösen az alábbi területeken.

### AI és ML alapú célzott támadások

Az AI és a gépi tanulás ML lehetőséget biztosítanak a támadók számára, hogy nagy mennyiségű adatot gyorsan feldolgozzanak és rendszerezzenek, ezzel jelentősen növelve a célzott támadások hatékonyságát. Az AI segítségével a támadók képesek automatikusan feltérképezni a célpontok közösségi média profiljait és egyéb nyilvános adatforrásokat, hogy személyre szabott támadási stratégiákat dolgozzanak ki. Az ML-algoritmusok folyamatos tanulási képessége révén optimalizálják a támadások sikerességét, például olyan adathalász üzenetek generálásával, amelyek pontosabban célozzák az áldozatok gyenge pontjait, növelve a bizalmas információk kiszivárogtatásának valószínűségét. [13]

### „Deepfake” technológia és hamisított tartalom

A „deepfake” technológia, amely AI-alapú képi és hangmanipulációt használ, különösen veszélyes lehet a social engineering területén. A támadók a „deepfake” eszközöket arra használhatják, hogy meggyőző hamis videókat és hangfelvételeket hozzanak létre, például egy vállalat vezetőjének „hangján” adjanak utasítást egy pénzügyi tranzakció végrehajtására. Mivel ez a technológia egyre fejlettebbé válik, a hamis tartalmak egyre hitelesebbek lesznek, és így nehezebb lesz felismerni az ilyen jellegű csalásokat. [14]

**Széles körű adatelemzés és célzott social engineering kampányok**

A „big data” és az adatelemzés eszközeinek fejlődése lehetőséget nyújt a támadóknak arra, hogy részletes profilt alkossanak az áldozatokról. Az adatelemzés lehetővé teszi, hogy a támadók még inkább személyre szabott módszerekkel célozzák meg az egyéneket és a szervezeteket. A célzott kampányok során egyéni érdeklődési körökre és viselkedési mintákra szabott csalogató üzeneteket készítenek, amelyek sokkal nagyobb eséllyel vezetik félre az áldozatot. [7]

**Automatizált social engineering rendszerek**

Az automatizálás terén elért eredmények szintén jelentős hatással lehetnek a social engineering fejlődésére. Az automatizált rendszerek segítségével a támadók nagyobb mennyiségű támadást képesek végrehajtani kevesebb idő és erőforrás felhasználásával. Az automatizált chatbotok generálhatnak olyan üzeneteket, amelyek utánzási algoritmusokat használnak az emberi beszélgetéshez, így megtévesztve az áldozatokat. Az ilyen rendszerek különösen veszélyesek a vállalati ügyfélszolgálatok számára, mivel az automatizált chatbotok könnyen beépíthetők az adathalász támadásokba, növelve azok hatékonyságát és csökkentve a detektálhatóság esélyeit. A támadók olyan gépi tanulási algoritmusokat is beépíthetnek, amelyek folyamatosan optimalizálják az interakciókat a sikeres manipuláció érdekében. [15]

**IoT és social engineering**

Az „Internet of Things” (továbbiakban: IoT) eszközök térhódítása újabb támadási felületeket biztosít a social engineering számára. Az IoT-eszközök gyakran kevésbé biztonságosak, és nem minden esetben frissíthetők megfelelően, így a támadók könnyebben hozzáférhetnek az ilyen eszközökön keresztül tárolt vagy továbbított információkhoz. A támadók kihasználhatják ezeket a gyenge pontokat, hogy manipulálják a felhasználókat, hamis biztonsági figyelmeztetések küldésével, amelyek arra ösztönzik az áldozatokat, hogy bizonyos adatokhoz vagy rendszerekhez biztosítsanak hozzáférést. Az IoT-eszközöket így a támadók a social engineering új eszközeiként használhatják. [16]

## ÖSSZEGZÉS

A social engineering egy összetett és folyamatosan fejlődő fenyegetés, amely az emberi pszichológiai tényezők kihasználásával manipulálja az áldozatokat, és az adatbiztonság egyik legsúlyosabb kihívását jelenti. A tanulmány áttekintést nyújtott a social engineering történeti fejlődéséről, bemutatva a korai technikákat, valamint a modern támadási formák kialakulását, amelyek közé tartozik a „phishing”, a „pretexting” és a „deepfake” manipuláció. A technológiai fejlődés – különösen az AI és ML alapú módszerek elterjedése – lehetővé teszi, hogy a támadások még célzottabbá és nehezebben felismerhetővé váljanak, ami tovább növeli a social engineering veszélyeit.

A védekezési stratégiák bemutatásával a tanulmány hangsúlyozza az oktatás, a technikai eszközök és a szigorú szervezeti protokollok fontosságát a social engineering elleni harcban. A jövőben elengedhetetlen lesz a védekezési mechanizmusok folyamatos fejlesztése és a felhasználók rendszeres oktatása annak érdekében, hogy lépést tarthassanak a social engineering támadások gyors ütemű fejlődésével.

## FELHASZNÁLT IRODALOM


[1] [1] C. Hadnagy, Social Engineering: The Science of Human Hacking, 2nd ed. Hoboken, NJ, USA: Wiley, 2018. ISBN: 978-1-119-43338-5.

[2] K. D. Mitnick és W. L. Simon, The Art of Deception: Controlling the Human Element of Security. Indianapolis, IN, USA: Wiley, 2002. ISBN: 978-0-471-23712-9.

[3] R. B. Cialdini, Influence: The Psychology of Persuasion, Revised ed. New York, NY, USA: HarperCollins, 2009. ISBN: 978-0-06-189987-4.

[4] D. Gragg, "A Multi-Level Defense Against Social Engineering," SANS Institute, 2003. [Online]. Elérhető: https://www.sans.org/reading-room/whitepapers/engineering/multi-level-defense-social-engineering-1232. [Hozzáférés dátuma: 2024. november 15.].

[5] P. Bányász, "Közösségi média és social engineering," Nemzetbiztonsági Szemle, vol. 5, no. 1, pp. 59–77, 2017. ISSN: 2064-3756.

[6] K. Krombholz, H. Hobel, M. Huber és E. Weippl, "Advanced social engineering attacks," Journal of Information Security and Applications, vol. 22, pp. 113–122, 2015. doi: 10.1016/j.jisa.2014.09.005.

[7] F. Mouton, M. Malan, L. Leenen és H. S. Venter, "Social Engineering Attack Framework," in Proceedings of the Information Security for South Africa Conference, Johannesburg, South Africa, 2014, pp. 1–9. doi: 10.1109/ISSA.2014.6950510.

[8] 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/. [Hozzáférés dátuma: 2024. november 15.].

[9] M. J. Guitton, "Cyberattacks, cyber threats, and attitudes toward cybersecurity policies," Journal of Cybersecurity, vol. 7, no. 1, tyab019, 2021. doi: 10.1093/cybsec/tyab019.

[10] P. A. Grassi, M. E. Garcia és J. L. Fenton, "Digital Identity Guidelines," NIST Special Publication 800-63-3, 2017. [Online]. Elérhető: https://doi.org/10.6028/NIST.SP.800-63-3. [Hozzáférés dátuma: 2024. november 15.].

[11] T. Gangavarapu, C. D. Jaidhar és B. Chanduka, "Applicability of machine learning in spam and phishing email filtering: review and approaches," Artificial Intelligence Review, vol. 53, no. 7, pp. 5019–5081, 2020. doi: 10.1007/s10462-020-09814-9.

[12] Deloitte Insights, "The value of cyber investments," 2020. [Online]. Elérhető: https://www2.deloitte.com/content/dam/insights/us/articles/5002_Value-of-cyber-investments/DI_Value-of-cyber-investments.pdf. [Hozzáférés dátuma: 2024. november 15.].

[13] M. Malatji és A. Tolah, "Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI," AI and Ethics, 2024. doi: 10.1007/s43681-024-00427-4.

[14] D. K. Citron és R. Chesney, "Deepfakes and the New Disinformation War," Foreign Affairs, vol. 98, no. 1, pp. 147–155, 2019. [Online]. Elérhető: https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war. [Hozzáférés dátuma: 2024. november 15.].

[15] 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/. [Hozzáférés dátuma: 2024. november 15.].
[16] N. Zlatanov, "Computer Security and Mobile Security Challenges," 2015. [Online]. Elérhető: https://www.researchgate.net/publication/283349998_Computer_Security_and_Mobile_Security_Challenges. [Hozzáférés dátuma: 2024. november 15.].