



ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar
Gépészeti és Biztonságtudományi Intézet



SZAKDOLGOZAT

OE-BGK
2021.

Hallgató neve: Balassa Bence

Hallgató törzskönyvi száma: T008158/FI12904/B



ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Óbudai Egyetem
Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar
Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

SZAKDOLGOZAT FELADATLAP

Hallgató neve: Balassa Bence

Szaktervezési szám: SZD21060110565529

Törzskönyvi száma: T008158/FI12904/B

Neptun kódja: Z5XN1P

Szak: biztonságtechnikai mérnöki

Specializáció: biztonságtechnikai mérnöki - biztonságtechnikai

A dolgozat címe:

Pszichológiai manipuláció - Az emberi viselkedés kihasználásának módszerei

A dolgozat címe angolul:

Social Engineering - Methods of exploiting human behaviour

A feladat részletezése:

1. Bevezetés a social engineering világába
2. A social engineering folyamata
3. A social engineering pszichológiai háttere
4. A social engineering eszközei
5. A social engineering elleni védekezés, megelőzés
6. Esettanulmányok

Intézményi konzulens neve: Dr. Kollár Csaba

A kiadott téma elévülési határideje: 2023. december 15.

Beadási határidő: 2021. 12. 15.

A szaktervezési: Nem titkos.

Kiadva: Budapest, 2021. 10. 18.



.....
Intézetigazgató

A dolgozatot beadásra alkalmasnak találom: 2021. 12. 15.

.....
belső konzulens

.....
külső konzulens



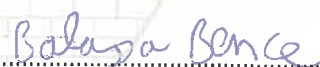
ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar
Gépészeti és Biztonságtudományi Intézet

HALLGATÓI NYILATKOZAT

Alulírott **Balassa Bence Z5XN1P** hallgató kijelentem, hogy a szakdolgozat saját munkám eredménye, a felhasznált szakirodalmat és eszközöket azonosíthatóan közöltem. Az elkészült szakdolgozatban található eredményeket az egyetem és a feladatot kiíró intézmény saját céljára térítés nélkül felhasználhatja, a titkosításra vonatkozó esetleges megkötések mellett.

Budapest, 2021. december 15.



hallgató aláírása

Tartalom

1. Bevezetés	2
2. Bevezetés a Social Engineering világába	4
2.1. A pszichológiai manipulátorok típusai	8
3. A social engineering folyamata	10
3.1. Információszerzés	10
3.2. Célszeméllyel való kapcsolat kialakítása, bizalom megszerzése	12
3.3. A megszerzett bizalom kihasználása	13
3.4. A támadás végrehajtása	13
4. A social engineering pszichológiai háttere	14
4.1. Gesztusok, testbeszéd	14
4.2. Szimpátiateremtés	17
4.2.1. A bizalom kialakítása	17
4.3. Elicitációs technikák	18
4.4. Pretexting	19
4.5. Befolyásolási technikák	20
5. A social engineering eszközei	22
5.1. Fizikai eszközök	22
5.1.1. Álkulcsok	22
5.1.2. Kamerák, hangfelvevő készülékek	22
5.2. Szoftverek	23
5.2.1. Maltego	23
5.2.2. Social Engineering Toolkit (SET)	23
6. A social engineering elleni védekezés, megelőzés	26
6.1. Felhasználói viselkedéselemzés	26
6.2. Információbiztonsági előírások	27
6.3. Biztonságtudatossági programok	28
7. Esettanulmány	30
7.1. A „pizza” módszer	31
7.2. A magabiztos igazgató	32
8. Következtetések, javaslatok	35
9. Összefoglalás	37
10. Summary	39
11. Irodalomjegyzék	40

1. Bevezetés

A dolgozat fő célja a magyar és külföldi szakirodalom feldolgozásával megvizsgálni a social engineering típusú támadások technikáit, eszközeit, az ellene való védekezési módokat. A munkámban célom volt kiemelt figyelmet fordítani a támadók kezében lévő legerősebb fegyverre, az egész támadás lényegét adó pszichológiai tényezőkre.

Ma a 21. században az adatok korát éljük. Államigazgatási- és gazdasági szervezetek, nagyvállalatok, pénzintézetek, kritikus infrastruktúrák rengeteg értéket, adatot kezelnek. Ilyen értékek közé tartozik a készpénz, értékpapír, berendezések és eszközök, információk, adatok, valamint maga az ember, a munkavállaló. Ezek a szervezetek működésüket és tevékenységüket csak akkor tudják megfelelően ellátni, ha folyamatosan, zavartalanul és rendeltetésszerűen üzemelnek. Ezért a bűnözés elleni védekezés mellett, a humán és technikai erőforrások működésének feltételeit is biztosítani kell. [1]

Napjainkban az állam és a szervezetek működése, szolgáltatások biztosítása és igénybevétele, valamint a polgárok mindennapi feladatainak ellátása nagymértékben függ az összetett elektronikus információs rendszerektől. A mai kor gazdasági berendezkedése mellett a társadalom nem elég felkészült arra, hogy kezelni tudja, a kritikus infrastruktúrák, szolgáltatások kiesését. Így ezeknek a védelmét meg kell valósítani, különös figyelmet kell fordítani arra, hogy a működésük során felhalmozódott és használt információk, továbbá az azokban kezelt adatok jelentős vagyont képviselnek. Az elektronikus információs rendszereink egyre összetettebbek, ezáltal egyre nehezebb elérni azok biztonságát, miközben az ellenük irányuló támadások egyre gyakoribbak. Az esetleges adatszivárgások a népesség jelentős hányadát érinti, így fokozódik a fontossága annak, hogy a rendelkezésre álló adatvagyon bizalmasságát, sértetlenségét és rendelkezésre állását biztosítsuk. [2]

„Minden rendszer annyira sebezhető, sérülékeny, mint annak leggyengébb eleme. Egy információs rendszer védelmi kontrolljainak teljes körűnek, valamennyi rendszerelemre kiterjedőnek –így az emberi tényezőre is –, folyamatosnak és zártnak kell lennie.”

A téma időszerűségét igazolják, hogy az elmúlt években egymást érik a különböző zsarolóvírus támadások, nagy adatszivárgások, nemzetbiztonsági kibervédelmi eszközök és adatok kompromittálódása, illetve a különböző, akár államilag támogatott bűnözői csoportok megjelenése és az általuk elkövetett visszaélések és támadások.

Miközben a vállalatok egyre jobb és megbízhatóbb szoftvereket képesek készíteni, jelentősen megnehezítve a támadók dolgát, így a rosszindulatú hackerek inkább a rendszer leggyengébb pontját veszik célba – az embert. Az idő előrehaladtával ezek a támadások egy komplex tudománnyá fejlődtek, ez a Social Engineering, avagy az ember befolyásolásának művészete. A támadás végrehajtóit social engineer-nek hívja a szakirodalom.[3]

.

2. Bevezetés a Social Engineering világába

Ebben a fejezetben betekintést engedek a social engineering világába, megvizsgálom a támadók lehetőségeit, különféle típusait.

Először is határozzuk meg mit is jelent maga a kifejezés, social engineering. Legáltalánosabb magyar fordítása: pszichológiai manipuláció. Annak ellenére, hogy sok megfogalmazás létezik, mit is jelent ez a fogalom, egyelőre nem született egy egységes definíció.

Kevin Mitnick a könyvében az alábbi módon fogalmaz:

„A social engineering a befolyásolás és a rábeszélés eszközével megtéveszti az embereket, manipulálja, vagy meggyőzi őket, hogy a social engineer tényleg az, akinek mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni.”

Talán a legpontosabb megfogalmazás Chris Hadnagy tollából származik, aki a következőképpen fogalmazza meg a Social engineering: The science of human hacking című könyvében:

„Social engineering is any act that influences a person to take an action that may or may not be in his or her best interests.” [7]

A social engineering lényege, hogy a támadó pszichológiai eszközök segítségével megtéveszti áldozatát. Ezáltal érzékeny, bizalmas információkhoz juthat hozzá vagy elérheti egy eszköz kártékony kóddal történő megfertőzését, akár belső hálózati hozzáférést is szerezhet. Egy social engineer olyan módon képes manipulálni, megtéveszteni, befolyásolni az embereket, hogy ezáltal olyan tettet hajtanak végre, ami nem állna szándékában, de a támadó meggyőzi ennek ellenkezőjéről. [10]

A pszichológiai manipuláció nem egy eszköz, hanem eszközök, készségek gyűjteménye, amiket elsajátíthatunk és bevethetünk céljaink elérése érdekében. Alkalmazása a mindennapunk része és minden ember alkalmazza nap mint nap, akár anélkül is, hogy tudomása lenne róla. Használják kisgyerekek a szüleiknél, ha valamit el szeretnének érni, rendőrök kihallgatásoknál, munkavállaló, aki fizetésemelést szeretne elérni, értékesítők, ügyvédek, pszichológusok, orvosok és sajnos csalók, bűnözők is alkalmazzák ezeket a technikákat pénzszerzésre, mások megkárosítására. Láthatjuk tehát, hogy felhasználása igen széleskörű, lehet jó és rossz dolgokra egyaránt alkalmazni. [4]

A social engineering technikákat csoportosíthatjuk humán alapú és IT alapú támadás szerint.

Humán alapú támadások:

Ebben az esetben a támadó nem használ IT eszközöket, általában szemtől-szemben találkozik áldozatával, ezért ez a tevékenység komoly szakértelmet és tapasztalatot igényel, hiszen nagy a lebukás veszélye.

A humán alapú támadások típusai:

- Váll feletti leskelődés (shoulder-surfing).
Az előttünk álló vagy a számítógép előtt ülő személy belépési adatait szerezhetjük meg ezzel a technikával, azáltal, hogy kifigyeljük mit gépel be a billentyűzeten. Ha távolabb vagyunk, akár távcsövet is alkalmazhatunk.
- Hallgatózás.
A támadó az áldozatok közelébe férkőzik és egyszerűen kihallgatja a beszélgetésüket, így próbál értékes információhoz jutni. Jellemzően tömegközlekedési eszközön, buszmegállóban, éttermekben, kávézóban lehet hatékonyan alkalmazni.
- Segítségkérés.
A támadó ez esetben kihasználja az áldozat segítőkészségét és segítséget kérve jut be olyan helyre, ahova nem lenne jogosult vagy szerez meg valamilyen információt.
- Segítségnyújtás.
A támadó valamilyen problémát idéz elő, majd úgy alakítja a helyzetet, hogy az áldozat tőle kérjen segítséget.
- Fordított social engineering.
Ebben az esetben a támadó olyan módon manipulálja áldozatát, hogyha valamilyen hiba lép fel, akkor őt keresse fel.
- Megszemélyesítés (pretexting).
A támadó egy fiktív személy bőrébe bújik, elhitetve áldozatával, hogy ő az, akinek mondja magát.

- Épületbe való bejutás.

Tailgating (szoros követés): ezt a technikát alkalmazva a támadó, egy csoporthoz társul, mintha a csoport tagja lenne.

Piggybacking (más jogosultságának felhasználása): a támadónak nincs jogosultsága belépni, de egy másik jogosultsággal rendelkező személyt eljátszva bebocsátást nyer az épületbe (pl.: azt mondja az őrnök, hogy otthon felejtette a belépőkártyáját).

- Kukabúvárkodás.

A támadó azt használja ki, hogy sokan kidobnak névlistákat, naptárakat, szervezeti ábrákat, akár kinyomtatott e-maileket vagy belső kézikönyveket, jelentéseket. Ezeket a konténerbe bemászva vagy egy kukát átvizsgálva megszerzi, ezáltal fontos információkhoz juthat hozzá, amit további támadáshoz felhasználhat.

- Jelszavak kitalálása.

Vannak nyilvánosan elérhető listák a leggyakoribban használt jelszavakról és ezeket próbálgatva vagy az áldozat személyes adatait összegyűjtve (név, születési dátum, háziállat, családtagok adatai), azokat véletlenszerűen beírogatni, így próbál a támadó jogosultságot szerezni. [8]

IT alapú támadások:

Ide azok a módszerek tartoznak, amikor a támadó a pszichológia mellett IT eszközöket is használ a támadás végrehajtásához.

- Adathalászat (phishing)

A célja banki adatok, jelszavak, érzékeny információk megszerzése, ennek érdekében felhasználók hiszékenységét és naivitását használják ki. A phishing e-maileknek két végrehajtási módja van:

Egyik esetben kártékony kódot tartalmazó mellékletet csatolnak az e-mail-hez, amit a gyanútlan felhasználó letölt és megnyit, így a kód lefut az eszközén.

A másik esetben egy linket helyeznek el az e-mailben, ami egy látszólag valóságos weboldalra vezet (pl.: egy bank vagy szolgáltató oldala), azonban ez egy álweboldal, amit a támadók irányítanak, a bizalmas adatok beírása után, azokat a támadók szerzik meg.

A phishing 2 altípusa:

Spear-phishing (szigonyozás): a phishing egyik fajtája, ilyenkor nem tömegesen, hanem célzottan egy adott személyt vesznek célba.

Whaling (bálnavasászat): ebben az esetben kifejezetten egy felsővezető a célpont.

- Kártékony program

Kártékony programok lehetnek:

Zsarolóvírusok: titkosítják a merevlemezen lévő adatokat és a feloldó kulcsot csak azután kapja meg a felhasználó, ha kifizette a váltságdíjat.

Trójai: látszólag hasznos program, azonban a háttérben káros tevékenységet végez (pl.: belépési adatokat gyűjt).

Kémprogram: figyeli az eszközön lezajló eseményeket (pl.: képernyőképet készít), a logokat pedig továbbítja a támadónak.

Keylogger: figyelik és rögzítik, hogy a felhasználó, milyen billentyűleütéseket hajtott végre, majd az adatokat továbbítják a támadónak.

Backdoor: távoli elérést biztosít a támadónak az eszközhöz.

A kártékony kód eszközre történő feljuttatásának lehetőségei:

Adathordozó elhagyása (baiting).

Ilyenkor a támadó kártékony kódot tartalmazó adathordozót "hagy el" az épület környékén vagy bent az épületben, remélve, hogy aki megtalálja, a szervezet eszközén fogja lefuttatni a fájlt.

Bejutás a szervezetbe.

A támadó bejut az épületbe, és valami manipulációs technika segítségével ráveszi az áldozatot, hogy helyezze be az adathordozót a szervezet egy eszközébe.

Adathalászat.

- Okostelefon

Alkalmazásengedélyek: hozzáférés kérése bizalmas adatokhoz. Látszólag ártatlan, azonban a háttérben káros tevékenységet végző alkalmazások.

Vishing: a támadók telefonon veszik fel a kapcsolatot az áldozattal, egy fiktív személyt megtestesítve próbálnak tőle bizalmas adatokat megszerezni.

Smishing: az adathalász támadások egyik formája. A támadók sms üzenet formájában próbálják rávenni a felhasználót egy álweblap meglátogatására vagy kártékony kóddal fertőzött csatolmány megnyitására. [11]

2.1. A pszichológiai manipulátorok típusai

A pszichológiai manipulátorok típusai az alábbiak:

- **Hacker**

Olyan az információs rendszerekhez és a programozáshoz jól értő személy, aki szeret problémákat megoldani és feszegetni a határokat. Azokat a hackereket, akik a programozáshoz nem értenek, a munkájukhoz használt eszközöket más forrásból szerzik be script-kiddinek hívják.

Fekete kalapos hacker: rossz szándékúak, céljuk a károkozás, mások megkárosítása, belépési adatok, pénzügyi adatok, személyes adatok megszerzése. Tevékenységüket végezhetik magányosan, csoportban vagy egy állam által támogatva. Gyakran szokták a Cracker kifejezéssel is illetni őket.

Szürke kalapos hacker: információs rendszerekben keresnek sérülékenységet, ha találnak azt bejelentik és nem okoznak kárt a rendszerben, azonban tevékenységüket engedély nélkül végzik.

Fehér kalapos hacker: olyan biztonsági szakértők, akik hasonló módszereket alkalmaznak a rendszerekbe való bejutáshoz, mint a fekete kalapos hackerek, azonban tevékenységüket engedéllyel, megbízás alapján, előzetes egyeztetéssel végzik.

- **Kémek**

Kémek munkájában nagyon fontos, hogy saját szándékaikat elrejtve tudják befolyásolni a környezetükben lévő embereket, ezáltal érzékeny információkhoz hozzájutni.

- Értékesítők

Az értékesítőknek ki kell találniuk klienseik igényeit, vágyait, majd rá kell venniük az adott termék megvételére, ehhez különböző befolyásolási taktikákat alkalmaznak.

- Politikusok

Politikusok, ha sikeresek akarnak lenni, fontos, hogy elnyerjék az emberek rokonszenvét, és akár tömegeket tudjanak befolyásolni, ehhez pszichológiai módszerek alkalmazása elengedhetetlen.

- Rendőrök, hatósági személyek

A rendőrök kihallgatásoknál alkalmaznak pszichológiai eszközöket, kitalálni, hogy esetleg hazudik-e a kihallgatott, illetve olyan módon kell irányítaniuk a beszélgetést, hogy vallomást sikerüljön kicsikarni.

- Mindennapi ember.

Kisgyerekek

Szülők

Orvosok

Ügyvédek [9]

3. A social engineering folyamata

Egy social engineering támadás több lépésből épül fel. A folyamat minden egyes lépése fontos szerepet játszik a támadás kivitelezésében, az egyes lépések megalapozzák a következő sikerességét. Ebben a fejezetben az egyes lépések egymásra épülését szeretném bemutatni.

A social engineering támadások 4 fő lépésből állnak:

- Információszerzés (OSINT).
- Célszeméllyel való kapcsolat kialakítása, bizalom megszerzése.
- A megszerzett bizalom kihasználása.
- A támadás végrehajtása.

3.1. Információszerzés

Az információszerzés az első és egyik legfontosabb lépés. Az összegyűjtött információk adják meg a támadás alapját, valamint lehetővé teszik a megfelelő célszemély kiválasztását, illetve ezen információk alapján lehet a támadás további elemeit megtervezni.

Az információ beszerzésének forrásai:

Weboldalak:

A cég weblapjának átböngészése egy nagyon jó alapja lehet nyilvánosan elérhető adatok megszerzésének. Gyakran tesznek fel információkat a felhasználókról, alkalmazottak telefonszámairól, beosztásokat, melyik dolgozó melyik egységben dolgozik, ki a főnöke, térképeket az épületről. [4]

Keresőmotorok:

A Google operátoraival olyan rejtett fájlokat találhatunk, amelyeket nem a nagyközönségnek szántak, azonban valamely hiba folytán szem előtt maradtak. [5]

Közösségi média:

Napjainkban már kevés olyan személy, akinek ne lenne valamilyen közösségi média fiókja. Ezekből a profilokból rengeteg információ kinyerhető, hiszen az emberek sokszor

nem fordítanak kellő figyelmet saját oldaluk információbiztonsággal és a személyes adatainak biztonságával kapcsolatos beállításaira.

Nagyon sok vállalatnak is van közösségi oldala, hiszen ezáltal viszonylag olcsón nagyon sok emberhez tudnak eljutni, akár fizetett hirdetések segítségével.

Egyéb:

- Konferenciákon, szakmai előadásokon is elhangozhatnak a céggel kapcsolatos információk, ezen anyagok felkutatása.
- Nyilvános adatbázisok átböngészése pl.: whois.com, ahol különféle domain információk lelhetők fel.
- Blogok, sajtóanyagok felkutatása. [4]

Kukabúvárkodás:

A cég telephelyén lévő kukák átvizsgálása, kidobott, fontos információt tartalmazó dokumentumok, pendrivok, merevlemezek, egyéb informatikai eszközök megtalálása érdekében.

Telefon, e-mail, személyes megkeresés:

Információt gyűjthetünk azáltal, hogy felvesszük a kapcsolatot egy alkalmazottal, és megpróbálunk tőle új dolgokat megtudni.

Ez történhet telefon segítségével, ilyenkor a támadó általában megszemélyesít egy másik személyt pl.: egy partnercég munkatársát, egyik beszállító munkatársát, nagy cégek esetén belső munkatársként vagy új munkavállalóként mutatkozik be vagy akár egy cégen belüli vezetőnek adja ki magát.

E-mailként lehet kérdőíveket küldeni egy cég munkavállalóinak, akár valamilyen ajándékot felajánlani kitöltés esetén. Ilyenkor a munkatárak személyes adatainak, érdeklődési körének, cégen belüli elégedettségének a felkutatása a cél, egy későbbi személyre szabott támadás elindítása érdekében.

Személyes felkeresés az egyik legkockázatosabb módszer, hiszen itt a támadónak jelen kell lennie. Ez történhet a telefonos módszerhez hasonlóan, azaz támadó egy másik személyt testesít meg, így veszi fel a kapcsolatot a célponttal például dohányzó

helyiségben vagy egy közeli kávézóban, vagy bejut az épületbe, ahol az irodákat, különféle helyiségeket körbejárva próbál meg érzékeny információkhoz hozzájutni.

Egy másik módszer, hogy egy kiválasztott személyt „véletlenül” megszólítja a támadó egy kávézóban vagy étteremben és beszélgetésbe elegyedve vele, próbál meg információt szerezni. [5]

3.2. Célszeméllyel való kapcsolat kialakítása, bizalom megszerzése

A célszemély kiválasztásában és a kapcsolat kialakításában fel tudjuk használni az előző lépésben megszerzett információkat. A cél egy felvett személyiség kitalálása és a támadás megtervezése, egy potenciális áldozat kiválasztása és a megszerzett információk alapján a támadó eldönti, hogy mely tulajdonságára alapozva hajtja végre a kapcsolat kiépítését vagy akár a támadást. Kihasháználható tulajdonságok:

- segítőkészség,
- befolyásolhatóság,
- naivság,
- érdeklődés,
- magány,
- kíváncsiság,
- hiszékenység,
- figyelmetlenség,
- monotonitás,
-
- hanyagság,
- elégedetlenség,
- bosszúállás,
- szakértelem hiánya,
- biztonságtudatosság hiánya. [11]

„Gyakori esetek:

- Fiatal, csinos nő középkorú egyedülálló férfi.
- Megnyerő modorú közép- vagy felsővezető középkorú, gyermekeit egyedül nevelő nő.
- Belépő kolléga, aki segítséget kér alkalmazottak, akik segítenek neki

- Rendszergazda az informatikai rendszerekhez nem értő munkavállaló.
- Takarító, karbantartó, futár a vállalat segítőkész dolgozói.” [6]

3.3. A megszerzett bizalom kihasználása

Ebben a lépésben megtörténik a korábban megszerzett bizalom kihasználása és az alkalmazottat tudta nélkül olyan tevékenységre készítetni, amit nem áll szándékában megtenni. Ez két módon történhet meg:

- A támadó segítséget kér az áldozattól, aki segít neki.
- A támadó szándékosan valamilyen hibát generál az áldozatnál, akivel korábban olyan módon alakította a kapcsolatot, hogy a munkavállaló tőle kérjen segítséget a probléma megoldásában.[5]

3.4. A támadás végrehajtása

A támadónak ebben a lépésben lehetősége nyílik bejutni egy szervezet informatikai rendszerébe, érzékeny adatokhoz férhet hozzá, azokat elolvashatja, törölheti, módosíthatja.[5]

4. A social engineering pszichológiai háttere

A pszichológia a legfontosabb elem, ez adja az alapját a social engineering támadásoknak. Ebben a fejezetben megvizsgálom a különböző pszichológiai módszereket, technikákat. Hogyan történik az áldozattal való összhang kialakítása, az arc rezdüléseinek, testbeszéd jeleinek értelmezése, majd felhasználása. Milyen lehetőségei annak a támadónak az áldozat befolyásolására és az információ megszerzésére.

4.1. Gesztusok, testbeszéd

Amikor két ember beszélget, az információk nagyobb részét (több mint 50%-át) nonverbális úton adják át egymásnak, tehát a testbeszéd, mikro- és makrokifejezések nagyon fontos szerepet játszanak a social engineering területén. A makrokifejezések az arcon lévő, bizonyos érzelmi események hatására bekövetkező apró izommozdulatok. Ezeket a mozdulatokat nem lehet irányítani, teljesen önkéntelenek és egy másodperc tört részéig tartanak. Ezzel szemben a makrokifejezések hosszabb ideig láthatóak az arcon, így könnyebb észrevenni és tanulmányozni, viszont könnyebb megjátszani is, hiszen irányíthatók.

A terület egy jeles szaktekintélye, Dr. Paul Ekman kutatásai nyomán tudjuk, hogy ezek a gesztusok nem az egyén kulturális helyzetétől függenek, hanem univerzálisak.

Dr. Ekman tudományos kutatásai során 7 alapvető univerzális érzelmet azonosított:

- harag,
- undor,
- félelem,
- öröm,
- szomorúság,
- meglepődés,
- megvetés. [4]

Külső ingereket 5 érzékünkkel tudunk felfogni: Látás, hallás, szaglás, tapintás, ízlelés. Ezeket az ingereket az agyunk feldolgozza, majd az inger kivált egy alapérzelmet a hét közül. A létrejött érzelem hatására bizonyos fiziológiai reakciók jönnek létre a testünkben, ami megjelenik mind az arcunkon, mind a testbeszédünkön. Minden érzelem hatására más izmok jönnek mozgásba, így jön létre az egyes érzelmek közötti észrevehető különbség. Az, hogy milyen érzelem jön létre az függ a korábbi tapasztalatainktól,

természetünktől, mentális állapotunktól. Az érzelem utóhatása lesz az érzés, ami hosszú távon megmarad, tehát az érzelmek hosszabb távon érzésekké fognak átalakulni. Ezek alapján tehát érzés például a szerelem, boldogság, aggodalom, kétségbeesés. [15]

Az érzelem kiváltására alkalmas az is, ha tudatosan öltjük magunkra az adott kifejezést vagy ha visszaemlékezünk egy olyan időpillanatra, amikor azt az érzést éreztük – az izmok emlékezni fognak és reagálnak.

Ha megtanuljuk olvasni az arc kifejezéseit és a testbeszéd jeleit, akkor megtudhatjuk a beszélgetőpartnerünk érzelmi állapotát, ami nagyon hasznos, hiszen ezáltal, tudjuk alakítani a saját kommunikációnkat, valamint szükség esetén formálhatjuk partnerünk érzelmeit. Ha értelmezni akarjuk egy másik személy nonverbális kommunikációját, nagyon fontos, hogy ne csak egy testrészre vagy mozdulatra koncentráljunk, hanem az egész testet figyeljük. A kar, a láb, a fej mozdulatait, valamint az arcon megjelenő gesztusokat, illetve a körülményeket egyaránt figyelembe kell venni. Fontos tehát, hogy az egyes jeleket kontextusba helyezzük és ezek alapján vonjuk le következtetéseinket. Másik lényeges pont, hogy ne csak a partnerünk jelzéseit figyeljük, hanem próbáljunk meg választ találni a **Miért** kérdésre. Vajon az illető miért ilyen jelzéseket küld irányunkba, mi állhat a háttérben? Ezzel elkerülhetjük, hogy téves megállapításokat tegyünk beszélgetőtársunk jelzéseit illetően. Például, ha valaki összefont karral és lehajtott fejjel ül télen egy padon, egyáltalán nem biztos, hogy szomorú, lehet, hogy csak fázik. [7]

Alkalmazása:

Nagyon fontos egy social engineer számára, hogy megtanulja értelmezni a vele szemben álló személy mikrokifejezéseit, ezáltal fel tudja ismerni, ha az illető verbális és nonverbális kommunikációja ellentmond egymásnak, így megelőzheti, hogy esetleg csalás áldozata legyen.

Másik fontos elem, hogy ő maga is megtanulja és alkalmazza a gesztusokat. Ez biztosítja, hogy a felvett személyiség és a verbális kommunikációja egyezni fog a mutatott érzellemmel, mert, ha nem így lenne, az könnyen bizalmatlanságot ébreszthet a célszemélyben.

A célja egy social engineernek, hogy olyan érzelmeket, majd érzéseket keltsen egy személyben, amivel könnyebben befolyásolni tudja. Az öröm, a félelem, a szomorúság és

a meglepődés azok az érzelmek, amikkel könnyen lehet manipulálni valakit. Az undor, megvetés és a harag azok az érzelmek, amiket célszerű kerülni. Több olyan tényező is van, amivel irányítani tudjuk egy másik személy érzelmeit. Ilyen a megjelenésünk, a saját testbeszédünk, gesztusaink. Például, ha láthatóan szomorú arckifejezéssel és testtartással szólítunk meg valakit, akkor könnyen tudunk részvétet kelteni, ugyanígy, ha széles mosollyal, nyitottságra utaló testtartással közelítünk meg valakit, az pozitív légkört fog teremteni, tehát nagy valószínűséggel, öröm érzését fogja a környezetünkben generálni. Kutatások bizonyítják, hogy ha egy adott makrokifejezést felvesszünk, az beszélgetőtársunkra jó eséllyel hatással lesz, és ő is hasonló érzelmeket fog mutatni. Fontos célja a támadónak, hogy különbséget tudjon tenni egy valós és egy megjátszott gesztus között. Ehhez a testbeszéd különböző jegyeinek, valamint az arcon megjelenő mikrokifejezések készségi szintű felismerése elengedhetetlen, amihez rengeteg gyakorlásra van szükség. Van azonban néhány olyan árulkodó jel, amit kevesebb tapasztalattal is észre lehet venni:

- Ellentmondás

Ha valakit gyakran azon kapunk, hogy állításai ellentmondóak, vagy arckifejezései, testbeszéde ellentmond a szavainak, akkor el kell gondolkodni beszédpartnerünk szavahihetőségén.

- Hezitálás

Ha a kommunikációs társ válaszadás előtt hezitál vagy bizonytalan, esetleg gyakran visszakérdez, hogy húzza az időt, az könnyen annak a jele lehet, hogy partnerünk nem mond igazat.

- Viselkedésbeli változás

Ha beszélgetőpartnerünk viselkedése, testbeszéde, gesztusai mindig megváltozik, ha egy bizonyos téma előkerül, akkor félrevezetésre gyanakodhatunk.

- Kéz gesztusai

Sok ember nagyon aktívan használja a kezét mondandójának ábrázolására, ha ezek a kéz gesztusok nincsenek összhangban az arckifejezéssel vagy a mondandóval, akkor az gyanút keltő. [4]

4.2. Szimpátiateremtés

A szimpátia egy érzést jelent, ami lehetővé teszi, hogy jól érezzük magunkat egy másik személy társaságában, bizalom alakuljon ki az egyének között. Szimpátiát érzünk valaki iránt, ha rokonszenvezünk a gondolkodásmódjával, életmódjával. Pszichológiai értelemben egy olyan érzelmi tényező, amely befolyásolja az emberek hozzáállását, viselkedését. Bizalmi környezetet teremt az egyén számára, és ezáltal könnyebben befolyásolható egy cél elérése érdekében.[12]

4.2.1. A bizalom kialakítása

A szimpátia megteremtésének egyik legfontosabb eleme, hogy elnyerjük beszélgetőpartnerünk bizalmát. Egy személlyel szemben érzett bizalom kialakulásában biológiai és környezeti tényezők egyaránt szerepet játszanak. Környezeti tényező például a szocializáció, kultúra, korábbi tapasztalatok, viselkedés, testbeszéd, megjelenés, míg a biológiai tényezők közé a gének, hormonok és az agyi aktivitás tartozik. [13]

A bizalom kialakításában nagyon fontos szerepe van két vegyületnek, az oxitocinnak és a dopaminnak:

Oxitocin:

Az oxitocin egy olyan hormon és neurotranszmitter, aminek számos jótékony fiziológiai hatása van.

Az oxitocin viselkedésre kifejtett pozitív hatásai:

- stresszcsökkenés,
- csökken a depresszió, a szorongás és a félelem,
- elősegíti a társas támasz nyújtását és fogadását,
- erősíti a szociális kapcsolatok kialakítását,
- növeli a bizalmat. [14]

Az oxitocin bizalommövelő hatását számos kutatás bizonyítja. [18] Többek között kimutatták, hogy nem csak a bizalom és a bőkezűség fokozódott meg, hanem az érzékeny információk átadására való hajlam is. Oxitocin hatására 44-szer gyakrabban osztottak meg másik személlyel bizalmas információt. [17] A kutatások azt is bizonyítják, hogy a bizalom csak abban az esetben nő, ha a másik fél is megbízhatónak tűnik. [16]

Dopamin:

A másik fontos vegyület a dopamin, amely az agy jutalmazási feladatait látja el, az agy jutalomközpontjának is hívják. A dopamin az oxitocin együttes jelenléte nagymértékben növeli a bizalmat és a pozitív szociális interakciókat. [13]

Számos olyan technika létezik, amellyel megszerezhetjük beszédpartnerünk szimpátiáját:

- Nonverbális kommunikáció legyen összhangban a felvett személyiséggel vagy megjelenéssel
- Kellemes megjelenés, ruházat illeszkedjen a felvett személyiséghez
- A beszéd sebessége és stílusa illeszkedjen a beszélgetőpartneréhez
- Hagyjuk partnerünket kibontakozni, legyünk jó hallgatóság
- Fontos az empátia társunk irányában
- Legyünk kíváncsiak a másik iránt, tegyünk fel kérdéseket, a beszélgetőpartnerünk érdeklődési körében legyünk olvasottak, legyen lexikális tudásunk.
- Kölcsönös önzetlenség: adjunk partnerünknek számára értékes információt vagy akár tárgyat, ezt jó eséllyel viszonzni fogja. [7]

4.3. Elicitációs technikák

Az elicitációs, avagy kikérdezési technikák megfelelő használata nagyon erős fegyver lehet egy social engineer kezében. A támadó egy általa tudatosan kiválasztott alannal beszélgetésbe elegyedik, és úgy irányítja azt a megfelelő kérdések feltevésével, hogy megszerezze a kívánt információt anélkül, hogy az alany rájönne a támadó valódi szándékaira. Ez azért is egy fontos eszköz, mert a beszélgetés általában egy teljesen hétköznapi, ártatlan szituációban valósul meg egy bárban, kávézóban esetleg egy étteremben, így a célalany számára nehéz felismerni a helyzet veszélyességét.

A beszélgetés kívánt irányba történő terelésére három fő technika létezik:

- az alany egójának növelése,
- közös érdeklődési területek kialakítása,
- szándékosan hamis állítás tétele.

Különbféle kérdéstípusokat lehet alkalmazni a támadás sikeres végrehajtásához:

- nyitott végű kérdések,
- zárt végű kérdések,

- irányító kérdések,
- feltételező kérdések.

A támadás sikeres végrehajtásához elengedhetetlen, hogy a támadó lazán, természetesen viselkedjen, szimpátiát keltsen az alanyban. Célszerű teljesen átlagos, közömbös kérdéssel kezdeni, utána nyitott végű kérdésekkel beindítani a társalgást, zárt végű kérdésekkel irányítani a beszélgetést, majd irányító kérdésekkel megszerezni a kívánt információt.

A támadás kivitelezéséhez nagyon fontos a megfelelő tervezés. Először a célt kell meghatározni, milyen információt kívánunk megszerezni, utána meghatározzuk az ehhez szükséges kérdések típusait. [4]

4.4. Pretexting

A pretexting, avagy személyiség felvétel célja, hogy egy más ember bőrébe bújva, azt megformálva, a támadó átejtí áldozatát. majd a megtévesztés által információt szerezzen meg tőle. Ez egy összetett social engineering technika. Nemcsak háttértörténet, öltözk, viselkedésmód szükséges hozzá, hanem teljes egészében a megformált személlyé kell válni, mind belső, mind külső személyiségjegyeiben. A támadónak el kell sajátítania a beszédmódját, akcentusát, mozgását, testbeszédét a siker érdekében.

A támadás kivitelezéséhez szükséges főbb szempontok:

- Információgyűjtés
Ennek középpontjában a már ismerttetett OSINT technikák állnak, a cél minél több információ megszerzése.
- Személyes érdeklődés bevonása
Elősegíti a szimpátiateremtést, a bizalom megszerzését azáltal, hogy egy bizonyos témában kellően tájékozottak és magabiztosak vagyunk.
- A felvett személyiség egyszerűsége.
Fontos az általunk kitalált történet egyszerűsége, minimalizálni a részleteket, ezáltal hihetőbb lesz a történet és kisebb a hibázás lehetősége, természetesebbnek fogunk hatni.
- Spontán viselkedés.
Fel kell készülnünk a váratlan szituációkra is, és adott esetben szükség lesz improvizációra. Ezeket ismereteink bővítésével, valamint gyakorlással érhetjük

el. Lényeges, hogy a stílusunk ne legyen túl monoton, erőltetett mintha egy begyakorolt szöveget mondanánk fel, ezáltal esetleg gyanút ébresztve beszélgetőpartnerünkben.

- Sajátos beszédstílus, zsargon használata

Nagyon fontos, hogy az adott szakma vagy közeg által használt szakszavakat, kifejezéseket elsajátítsuk, ezáltal is növelve szavahihetőségünket [4]

4.5. Befolyásolási technikák

A befolyásolási technikák megfelelően alkalmazva rendkívül hatékony eszközök lehetnek egy támadó kezében.

Befolyásolási módszerek:

- Kölcsönösség

Ennek a technikának a lényege, hogy a támadó adósság érzetet keltsen az áldozatban, azáltal, hogy valami számára nagyon értékes információt, tárgyat ad neki vagy egyszerűen tesz neki egy szívességet. Viszonzásul az áldozat nagy valószínűséggel eleget fog tenni a támadó kérésének, még akkor is, ha ez a szabályok áthágását jelenti.

- Kötelezettség

Ez a módszer hasonlít a kölcsönösséghez, annyi különbséggel, hogy ebben az esetben, olyan helyzetet, hoz létre a támadó, amiben az áldozat egy társadalmi elvárás vagy erkölcsi norma miatt kötelességének fogja érezni, hogy segítsen a támadónak. Például mindenki megtartja az ajtót egy nőnek vagy egy olyan személynek, aki nehéz dobozokat cipel, esetleg egy mozgássérült személynek és ezt a támadó könnyen kihasználhatja.

- Hiány

Ha valami ritka vagy kevés van belőle az növeli az értékét. Egy social engineer ezt úgy tudja kihasználni, hogy sietteti áldozatát, azt állítva, hogy nincs ideje visszajönni vagy többször nem lesz mód valamit megtenni, ezáltal az időből lesz hiány, ami cselekvésre fogja ösztönözni az áldozatot.

- Hatóság, felettesi viszony

Ennek a technikának az előnye, hogy az emberek könnyebben engedelmeskednek egy a hierarchiában felettük álló személynek. A támadó ezt úgy használja ki, hogy egy adott szervezeten belüli főnöknek vagy hatósági személynek adja ki magát, vagy egy ilyen személyre hivatkozik. Nagyon fontos, hogy a támadó a testbeszédével, megjelenésével, magabiztosságot sugározzon, máskülönben könnyen hitelét vesztheti.

- Szimpátia

Ha egy személy kedvel egy másikat, van közös érdeklődési területük, hobbijuk, hasonló az ízlésük valami iránt, akkor az áldozat könnyebben eleget fog tenni a támadó kérésének.[7]

5. A social engineering eszközei

Egy social engineer kezében számos eszköz van, amit felhasználhat egy információbiztonsági audit során, vagy akár rosszindulatú támadás alkalmával. Ezek az eszközök két csoportba sorolhatók: Fizikai eszközök és szoftveres eszközök. A fejezet célja ezeknek az eszközöknek a bemutatása.

5.1. Fizikai eszközök

A fizikai eszközök közé tartoznak az álkulcsok, kamerák, hangfelvevő eszközök.

5.1.1. Álkulcsok

Az álkulcsok közé soroljuk azokat a tárgyakat, amelyekkel zárszerkezeteket lehet működtetni. Ezek lehetnek kör vagy négyzet keresztmetszetű vas vagy fémszálak, amik kulcs formára vannak kialakítva, vagy akár lehet egy sima drótdarab is. Nagyon sok olyan mindennapos használati tárgy van, ami kisebb átalakításokkal vagy akár anélkül szakértő kezekben álkulcsként használható. Ilyen például a sarló alakú konzervnyitó. Mivel sok fajta zár van, így az eltérő rendszerekhez más és más kialakítású álkulcs szükséges, azonban a működési elvük megegyezik az egyes típusoknál: „a zár belső reteszelő elemeit egyenként, vagy csoportosan, vagy együttesen működteti, ill. nyitási határpozícióba tereli, vagy kiiktatja oly módon, hogy a záróretesz, (tolókavivő, zárreteszvas, kilincs) működtethető legyen.” [19]

5.1.2. Kamerák, hangfelvevő készülékek

Manapság számos üzletben vagy online boltban lehet olyan apró rejtett kamerákat és hangfelvevő eszközöket vásárolni, amiket könnyen el lehet rejteni a ruházaton, nyakkendőn, golyóstollban, órában, sapkában vagy akármilyen hétköznapi használati tárgyban. Alkalmazásuknak számos előnye van:

- Sok olyan apró mozzanatot örökíthetünk meg, amiket elkerült a figyelmünk a helyszínen. Utólag kielemezve a felvételeket ezeket könnyebben észre lehet venni és a támadás későbbi szakaszában még a segítségünkre lehet, valamint lehet belőle tanulni, mi az, amit rosszul csináltunk a támadás során és mi az, amit jól.
- A megbízónak átadva egyrészt bizonyítékként szolgálhat a munka elvégzését illetően, másrészt visszanézve és/vagy hallgatva a felvételeket a szervezet tanulhat

a hibákból és a munkavállalók célirányosabb képzését, tájékoztatását segítheti elő.
[4]

5.2. Szoftverek

Egy social engineering támadás során nagyon fontos az előzetes információgyűjtés, viszont ezeket az adatokat tárolni, katalogizálni és rendezni kell a jobb átláthatóság érdekében, hogy azt később összefüggéseiben lehessen felhasználni. Erre a feladatra számos alkalmazás áll rendelkezésünkre, ilyen például a Maltego vagy a Social Engineering Toolkit (SET).

5.2.1. Maltego

A Maltego egy információs adatbázis. Segítségével információt tudunk gyűjteni, majd a megszerzett adatokat, valamint a közöttük lévő kapcsolatot, összefüggéseket vizuálisan is, gráfszerűen megjeleníti a szoftver. Az összegyűjtött információt lementhetjük PDF formátumban, amiben átláthatóan, egymásra épülve jelennek meg a különféle adatok, ezáltal bármikor, könnyen fel lehet használni. A program számos keresési feladatot automatikusan elvégez, ezáltal rengeteg Google kereséssel eltöltött munkaórát tud használójának megspórolni.

A program Java nyelven íródott és használható Windows-on, Linuxon és Mac-en is. A biztonsági tesztelésre alkalmazott Kali Linux operációs rendszeren előre feltelepítve megtalálható.

5.2.2. Social Engineering Toolkit (SET)

A Social Engineering Toolkit egy nyílt forráskódú, rendkívül egyedi és hasznos eszköz egy social engineer számára. Mivel alkalmazása széleskörű és automatizálni lehet vele a támadásokat, a SET egy nagyon hatékony fegyver a támadó kezében, ezért ezt a szoftvert kicsit részletesebben ismertetem.

Menüből kell kiválasztani a nekünk szükséges lépéseket:

- 1) Spear-Phishing Attack Vectors
- 2) Website Attack Vectors
- 3) Infectious Media Generator
- 4) Create a Payload and Listener
- 5) Mass Mailer Attack

- 6) Arduino-Based Attack Vector
- 7) SMS Spoofing Attack Vector
- 8) Wireless Access Point Attack Vector
- 9) QRCode Generator Attack Vector
- 10) Powershell Attack Vectors
- 11) Third Party Modules

Az alábbiakban az alkalmazás főbb funkcióit tekintem át:

Spear-Phising Attack Vector:

Az 1-es gomb megnyomásával tudunk ebbe a menüpontba belépni. Célzott adathalász e-maileket tudunk küldeni egy vagy több célpontnak, az e-mailhez káros kódot tartalmazó csatolmányt is csatolhatunk. További 3 opció áll rendelkezésünkre:

- 1) Perform a Mass Email Attack
- 2) Create a FileFormat Payload
- 3) Create a Social-Engineering Template

Az 1-es esetben az alkalmazás mindent maga elvégez az alapbeállítások szerint, míg a második esetben mi magunk tudjuk beállítani a támadás részleteit. Milyen formátumú fájlt szeretnénk a célszemély esetén megtámadni és eszerint tudjuk kiválasztani a csatolmányt. A harmadik esetben előre elkészített sablonokkal tudunk dolgozni.

Infectious Media Generator:

Egy kódot készít, amit egy USB eszközön vagy egy DVD-n lehet elhelyezni és ha csatlakoztatják az adathordozót egy eszközhöz, képes kompromittálni a rendszert.

Create a Payload and Listener

Egy kódot készít, amit aztán átalakítva .EXE kiterjesztés formátumba az áldozat gépére juttatva le tudunk futtatni és távoli elérést szerezhethünk az eszközhöz.

Mass Mailer Attack

Ennek a modulnak a fő célja nagyszámú e-mail küldés, sok címzettnek. Tömeges adathalász kampányokra lehet alkalmazni, de egy címzettnek való küldésre is lehetőség van.

SMS Spoofing Attack Vector

SMS üzeneteket lehet küldeni ezzel a funkcióval, úgy, hogy a küldő fél kiléte titkos marad. Lehet egy számra üzenetet küldeni, de akár tömeges kiküldésre is alkalmas. Ennél a modulnál is lehet előre beállított sablonokat alkalmazni.

6. A social engineering elleni védekezés, megelőzés

Az utóbbi időben megnőtt a szakadék a támadó és a védelmi oldal között a kibertérben, a támadó fél javára. Egyre összetettebb és szofisztikáltabb támadási formák jelennek meg, amikkel nagyon nehéz védelmi oldalról felvenni a versenyt. A támadások sikerességének fő okaként a felhasználók biztonságtudatosságának hiányát szokták megjelölni a szakértők. Ezért manapság nagyon fontos szerepe van az olyan programoknak, előadásoknak, továbbképzéseknek, amikkel akár a munkavállalókat, akár a hétköznapi számítógéphasználót tudják felkészíteni a különféle támadásokkal szemben. Amióta megnőtt a támadások száma, a hétköznapi ember is érezheti a hatását, így a biztonságtudatosság is egyre jobban beépül a közbeszédbe. Ez azonban még kevés. A tapasztalatok szerint a támadók idővel megtalálják azokat a réseket, amiken keresztül be tudnak jutni egy rendszerbe. Fontos lenne egy olyan biztos módszer, amivel, ezeknek a támadásoknak a sikerességét csökkenteni lehet. Bár mindig vannak megoldások, új ötletek, ezen a téren még jelentős áttörést nem sikerült elérni. [20]

6.1. Felhasználói viselkedéselemzés

Különösen fontos egy szervezet számára meghatározni annak a mértékét, hogy egyes felhasználók mennyire vannak veszélynek kitéve. Ennek a vizsgálata két szempontból történhet:

- Egy felhasználó milyen gyakran kerül olyan döntési helyzetbe, ami befolyással lehet a szervezet biztonságára: például egy HR osztályon dolgozó munkatárs vagy egy vezető beosztású személy, akik gyakran kapnak leveleket a vállalaton kívülről, sokszor csatolmányokkal, ők nagyobb veszélynek vannak kitéve, mint egy takarító.
- Ha egy felhasználó döntési helyzetbe kerül, akkor milyen valószínűséggel sodorja veszélybe a vállalatot tetteivel.

A felhasználók viselkedésének elemzése kétféleképpen történhet.

Az egyik módszer passzív jellegű. [21] Ilyenkor a felhasználó tevékenységének monitorozásával, fel lehet építeni egy olyan profilt, amit a munkavállaló megszokott tevékenységeiből tevődik össze. Ebből következően, ha ismerjük a „szokásost”, abból következtethetünk a „szokatlanra” is, ami lehetővé teszi a védelmi rendszer kiépítését.

Ugyanis, ha a támadó egy alkalmazott hozzáférési jogosultságával visszaélve bejut a hálózatba, akkor az ő tevékenysége más mintázatot fog követni, ezt a változást az alkalmazott védelmi erőforrások sikeresen azonosíthatják. A védelem felépítése azonban megfigyeléssel jár, ami által sok adat keletkezik a felhasználóról, ez viszont felvet bizonyos adatvédelmi aggályokat. A vállalatnak nagyon oda kell figyelnie, hogy a hatályos adatvédelmi törvényeknek megfelelően kezeljék az adatokat. [20]

A másik az aktív módszer. Ebben az esetben a szervezet szándékosan idéz elő olyan helyzetet, amely során a felhasználó döntési helyzetbe kényszerül. [21] Ezek a social engineering auditok, amely során az auditor, előre meghatározott feltételek szerint, szerződés alapján, hoz létre olyan szituációt, ami a vállalatra nézve veszélyt jelent. Ez lehet akár egy adathalász kampány, de akár személyes megjelenéssel is történhet. Az eredményeket utólag kielemezve a vállalat fontos információhoz juthat a munkavállalói biztonságtudatosság szintjéről, illetve a tapasztalatokat feldolgozva tréninganyagokat lehet készíteni, ezzel is növelve az alkalmazottak felkészültségét.

6.2. Információbiztonsági előírások

Minden szervezetnek és cégnek rendelkeznie kell biztonsági szabállyal. A social engineering módszerek ellen alkalmazott szabályozásnak először is a fizikai behatolás megelőzésére kell nagy hangsúlyt fektetnie. Legyen beléptető rendszer, portaszolgálat, személyazonosítás alkalmazása. Ha vendég érkezik, csak a látogatás céljának leellenőrzése, validálása és személyazonosítás után szabad beengedni, szükséges esetben kísérő személyt kell biztosítani.

Előfordulhat, hogy egy illetéktelen személynek mégis sikerül bejutnia az épületbe, vagy akár szabályosan, látogatóként, ha olyanok a körülmények. Ezért nagyon fontos az „üres íróasztal – tiszta képernyő politika” betartása.

- Ne hagyjanak személyes tárgyakat, naptárakat, jegyzetfüzetet, adathordozót az asztalon és zárolják a képernyőt, ha elhagyja a munkavállaló a munkaállomást.
- A jelszavakat ne írják le és ragasszák az asztalra vagy a monitorra.
- Programok telepítésének jogosultságához kötése.
- USB portok tiltása.

Egyéb, a szervezetre vonatkozó szükséges előírások:

- Kidobandó iratok, papír alapú dokumentumok iratmegsemmisítővel legyenek megsemmisítve, úgy, hogy egy későbbi kukaátvizsgálás során ne legyenek visszaállíthatók.
- Leselejtezett informatikai eszközök tartalmának megfelelő törlése.
- Kilépő munkatársakkal kapcsolatos szabályzatok megoldása.
- Munkavállalók oktatása, biztonságtudatossági programok szervezése.
- Biztonsági előírások, azok betartásának rendszeres felülvizsgálata auditok formájában.
- Kötelezni a felhasználót megfelelő jelszavak használatára és azok rendszeres (legalább félévente) cseréjére. [5]

6.3. Biztonságtudatossági programok

Az információs rendszerek elleni támadások jó része elkerülhető lenne, ha a felhasználók tudatosabban használnák eszközeiket. Ebben a folyamatban nagyon fontos szerepet játszanak a biztonságtudatossági programok, amik minden szervezetnél központi helyre kell, hogy kerüljenek. Célszerű lenne egy kérdőív formájában előzetesen felmérni a felhasználók biztonsági szokásait, jártasságuk szintjét. Az eredmény alapján, a hiányosságokra fókuszálva, ki lehet alakítani a képzési programot, összeállítani a tananyagot. Évente kellene tartani egy informáló előadást a szervezet minden munkatársának a veszélyekről és a lehetséges megelőzésről. Az előadás végén teszt formájában a résztvevőknek számot kellene adniuk, mennyire értették meg és fogadták be az elhangzott információkat. Az előadásnak tartalmaznia kellene a következőket:

- Lehetséges támadási módok bemutatása.
- Esettanulmányokon keresztül bemutatni a téma gyakorlati megvalósulásait.
- Védekezési technikák bemutatása.
- Információátadás arról, ha valaki felismer egy ilyen támadást, mi a teendője, kinek kell szólnia.

Ezen képzésen felül a nagyobb veszélyeztetettségű munkatársak, valamint a vezetők számára évenkénti kiegészítő képzést kellene tartani, a mélyebb tudás elsajátítása érdekében. Pszichológus vagy social engineering szakértő bevonásával, lehetne akár több

napos tréningeket is tartani, ahol az elméleti tudás mellett, szituációs gyakorlatok és egyéb játékos feladatok végrehajtásával gyakorlatiasabb szemlélet alakítható ki.

Az évenkénti előadásokon kívül minden belépő munkatártnak részt kellene vennie egy információbiztonsági képzésen mielőtt elkezd a munkát. A figyelem folyamatos fenntartása érdekében lehetne rendszeresen hírleveleket, tájékoztató jellegű anyagokat küldeni a munkavállalóknak.

Nagyon fontos lenne, hogy a felhasználókban kialakuljon egy biztonság tudatos szemléletmód, és megjelenjen az igény, hogy a tanult megelőzési technikák alkalmazásra is kerüljenek, idővel pedig a mindennapok természetes része legyen a használatuk, nemcsak a munka során, hanem azon kívül is (például a megfelelő jelszó kezelés, biztonsági frissítések rendszeres elvégzése.) Viszont ahhoz, hogy ide eljussunk véleményem szerint az embereknek meg kell érteniük a háttérben futó folyamatokat, nemcsak magát a következményt tudatosítani, hanem hogy azok miért is jelentenek fenyegetést. Ez pedig csakis közérthető módon elmagyarázott felvilágosítás útján valósulhat meg.

7. Esettanulmány

Az elmúlt évtizedekben számos kutatás és tanulmány született a kommunikáció tanulmányozásával és elemzésével kapcsolatban. A kommunikáció jellegét befolyásolja a társadalmi és kulturális környezet, az életkor, a földrajzi elhelyezkedés. Különböző csoportoknál és szervezeteknél sajátos kommunikációs formák jelennek meg. Egy social engineering audit során is figyelembe kell venni a szervezeti kultúra sajátosságait. Ezen beszédesemények elemzésére számos elmélet született, ilyen például Hymes SPEAKING modellje. Bár Hymes a modellt az interperszonális kommunikáció elemzésére fejlesztette ki, és nem auditra, az eddigi kísérletek információbiztonsági területen történő alkalmazására ígéretesek. A social engineering támadások nyolc szempont szerint vizsgálhatók a modell segítségével. A korábban elvégzett tanulmányok alapján kijelenthető, hogy jól alkalmazható esettanulmányok elemzésére. Olyan hozzáértő szakmabeliek számára is kellő információval szolgált, akik korábban nem ismerték a modellt. Megfelelő alapot szolgáltat az információbiztonsági képzési programok kialakítására és fejlesztésére. [24]

A SPEAKING modellben a betűk a következő szavakat jelentik:

- „Setting/scene: beszédhelyzet.
- Participants: résztvevők.
- Ends: lezárások.
- Act sequences: cselekménysorozatok.
- Key: kulcs.
- Instrumentalities: eszközök.
- Norms: normák.
- Genre: műfaj.” [22]

A social engineering alkalmazása a modell segítségével:

A **beszédhelyzet** adja a fizikai körülményeket. Ide tartozik az idő és a tér. Mennyi időre van szükség a támadás végrehajtására, valamint jelenti a helyszínt, ahol a támadás végrehajtódik.

A **résztvevők** az akcióban szereplők bemutatását jelenti.

A **lezárások** jelentik a támadó célját. Ez lehet nem nyilvános adat megszerzése, elzárt területre való bejutás, vagy szabályszegésre rávenni egy dolgozót.

A **cselekménysorozat** utal magára az események folyamatára, a támadó milyen módon ér el célját, milyen technikákat használ.

A **kulcs** a verbális és nonverbális kommunikációs jeleket jelentik. Egy támadás akkor lesz sikeres, ha a tartalom és a stílus egyezik a testbeszéddel, mikrokifejezésekkel.

Az **eszközök** az alkalmazott kommunikációs csatorna. Ez lehet e-mail, telefon vagy személyes társalgás.

A **normák** a szereplők viselkedésére utal. A támadó milyen hatással van a résztvevőkre, szabályszegésre vagy szabálykövetésre alapozza a támadást.

A **műfaj** a beszédhelyzet típusát takarja. Ez lehet beszélgetés, kérés, segítségnyújtás, tanácsadás, felmérés, szolgáltatásnyújtás.

Az alábbiakban egy esetet dolgozok fel ennek a modellnek a segítségével, aminek az alapját egy social engineering audit adta. Az adatgyűjtést az interneten végeztem. [24]

7.1. A „pizza” módszer

Az esettanulmány alapjául <https://cyberforces.com/> weboldalon található eset szolgált, ami egy social engineering audit során zajlott le.[23]

A SPEAKING modell alapján a következőket tételeztem fel:

Beszédhelyzet:

Az esemény tágabb helyszíne a vállalat irodaépület, szűkebben az iroda, ahol az átvétel megtörténik.

Résztvevők:

- éhes alkalmazottak,
- pizzafutárt megtestesítő auditor.

Lezárások:

A támadás célja, hogy az áldozta bedugjon egy lámpát a számítógép az USB csatlakozójába, ezáltal távoli elérést sikerüljön szerezni a vállalati belső hálózathoz.

Cselekménysorozat:

A cselekmény a következőképpen épül fel: a támadók egy hamisított weboldalt készítettek, ahonnan pizzát lehet rendelni. Az információt elküldték a támadni kívánt szervezet munkavállalóinak vállalati e-mail címére, amit a cég honlapjáról gyűjtöttek be. Az üzenetben 30%-os árkedvezményt ajánlottak az elsők között rendelőknek. Amint egy

rendelés beérkezett, a támadó egy közeli üzletben megvásárolta a szükséges mennyiségű pizzát, a korábban elkészített saját logóját ráhelyezte a dobozokra, végül pedig kiszállította a pizzát. A rendelés átadásakor átnyújtott az alkalmazottnak ajándék gyanánt egy LED lámpát, ami a zene ritmusára változtatta a színét és USB-vel lehetett egy számítógéphez csatlakoztatni. A lámpában azonban elrejtettek egy memóriakártyát, ami egy olyan kódot tartalmazott, ha a lámpát a számítógéphez csatlakoztatják, akkor a kód lefut a számítógépen, így a támadók be tudnak jutni a vállalat belső hálózatába.

Kulcs:

A támadás sikerességének kulcsa, hogy a támadó saját logójú felszerelésben jelent meg, amivel bizalmat ébresztett a vásárlókban, majd az árkedvezmény és az ajándéktárggyal szimpátiát sikerül kelteni az áldozatban.

Eszközök:

Többféle kommunikációs csatorna is szerepet játszik a történetben. Először e-mailben veszik fel a kapcsolatot a cég alkalmazottjaival a támadók, majd az átadás során személyes találkozással verbális és nonverbális eszközök is megjelennek.

Normák:

A támadó szabályszegésre veszi rá áldozatát, azzal, hogy egy idegentől kapott eszközt csatlakoztat a vállalati számítógépéhez.

Műfaj:

Beszélgetés, szolgáltatásnyújtás. [22]

7.2. A magabiztos igazgató

Az esettanulmány Cristopher Hadnagy: Social engineering: Art of human hacking című könyvéből származik. [4]

A SPEAKING modell alapján a következőket tételeztem fel:

Beszédhelyzet:

A támadás beszédhelyzetei egyrészt az információszerzés érdekében megvalósult beszélgetések (például a banki ügyintézővel), másrészt az áldozattal történő telefonbeszélgetés, majd az e-mail elküldése. A térbeli és időbeli körülmény jelen esetben

nem érdekes, mert nincs a szereplők részéről se fizikai helyváltoztatás, se fizikai kapcsolat.

Résztvevők:

- az igazgató, mint áldozat,
- a támadást végrehajtó auditor,
- a banki alkalmazott.

Lezárások:

Social engineering módszerek segítségével hozzáférést szerezni a vállalat szerveréhez és bizalmas adatokat szerezni.

Cselekménysorozat:

A támadás információgyűjtéssel indult. Az auditornak sikerült e-mail címeket, telefonszámokat, fizikai címeket, IP címeket összeszednie. Talált információt az áldozat családtagjairól, szokásairól, kedvelt helyeiről. A munka során a támadó kezébe akadt egy számla. A számlán szereplő bank egyik alkalmazottjától sikerült megtudni, hogy egy jótékonyági adományról lett kiállítva. Az adomány egy alapítványnak szólt, akik daganatos gyerekek megsegítésére gyűjtenek. További kutakodás után kiderült, hogy az igazgató egyik rokona betegségben szenvedett, ezért adományozott minden évben egy jelentősebb összeget ennek az alapítványnak. A támadó erre a tényre építette fel az álszemélyiségét. Egy daganatos kutatást támogató alapítvány munkatársának kiadva magát. (Ez elsőre etikátlannak tűnhet, azonban figyelembe kell venni, hogy a rossz szándékú támadók sem etikusak és nem fognak válogatni az eszközökben). Az auditor felhívta az áldozatot és felajánlotta neki a támogatás lehetőségét, és tájékoztatta, hogy cserébe minden adományozó között kisorsolnak 2 jegyet egy sportrendezvényre és egy ingyenes ebédet egy étterembe. Az étterem természetesen az áldozat kedvenc helye volt és a sportrendezvényeket is rendszeresen látogatta. Ezeket az információkat az auditor az előzetes online kutatásai alapján szerzett meg. Miután az áldozat megörült a lehetőségnek, a támadó elküldött egy tájékoztató anyagot, amit PDF formátumban lett az e-mailhez csatolva. Amikor az igazgató megnyitotta a csatolmányt a dokumentumban lévő káros kód lefutott, és hozzáférést engedélyezett a támadónak a számítógépéhez. Az eszközről sikerült letölteni a szerverhez tartozó jelszavakat.

Kulcs:

A siker kulcsa, a megfelelő minőségű és mennyiségű információ összeszedése volt. A támadó az áldozat érzelmeire hatott. Mivel személyes érintettsége is volt, ezért gondolkodás nélkül minden alkalmat megragadott az ilyen jellegű támogatásra, ezt használta ki az auditor.

Eszközök:

A kommunikációs csatorna, amin keresztül megvalósult a támadás az e-mail volt. A támadás korai fázisában, az információk összegyűjtésében a telefonos kommunikáció is szerepet játszott.

Normák:

A támadó szabályszegésre veszi rá áldozatát, azzal, hogy megnyitja az e-mailhez csatolt dokumentumot, és egy olyan számítógépen nyitja meg amin érzékeny adatok vannak.

Műfaj:

Beszélgetés. [22]

8. Következtetések, javaslatok

A kutatómunka során számos tudományos igényű könyv és cikk elolvasása után arra a megállapításra jutottam, hogy ez egy rendkívül összetett és szerteágazó témakör. Ahhoz, hogy valakiből jó social engineer váljon számos tulajdonsággal kell rendelkeznie. Ezek nagyrésze tanulható, viszont rengeteg gyakorlásra és tapasztalatra van szükség az alkalmazásukhoz. Egy támadás sikeres kivitelezéséhez nagyon gondos előkészítő munka szükséges a támadó részéről. Minden egyes lépést meg kell tervezni, ugyanakkor készen kell állni a rögtönzésre is, hiszen bármikor előállhat előre nem látott esemény, és ezt tudni kell kezelni. Egy social engineernek nagy műveltséggel kell rendelkeznie különböző szakterületeken, hiszen eltérő szerepeket kell eljátszania. A siker érdekében meg kell tanulnia a szakmában használt zsargont, kompetensnek kell mutatkoznia az adott szakterületen. Ezt be lehet tanulni a támadás előtt, azonban a folyamatot nagymértékben megkönnyíti, ha az illető már rendelkezik valamilyen alaptudással az adott területen. Társasági embernek kell lennie, aki szeret másokkal beszélgetni, kapcsolatot teremteni. Úgy látom, hogy a social engineering egyben művészet, tudomány és szakma. Tudomány, mert az ismeretanyaga elérhető, tanulható. Szakma, mert nagyon nagy szerepe van a biztonságtudatosság fejlesztésében. Művészet, mert csak kevesen tudják igen magas színvonalon művelni.

Bár egyre jobb és fejlettebb technikákat sikerül kialakítani a támadások elhárítása érdekében, és egyre inkább beépül ez a terület a közbeszédbe még nagyon sok munka vár a társadalomra, ha biztonságban akarjuk tudni magunkat. A támadások egyre gyakoribbak, pusztítóbbak és szervezettebbek. Mostmár nem az a kérdés, ki lesz áldozat, hanem hogy mikor, ezért szükségünk van olyan szakemberekre, akik felveszik a harcot a kiberbűnözéssel szemben.

A sikeres támadások számának csökkentése érdekében fontos lenne nagyobb figyelmet fordítani a képzésre és a népszerűsítésre. Lehetne informáló előadásokat szervezni középiskolában, de akár játékos jellegű bevezető programokat lehet tartani általános iskolásoknak is. A területet bemutató televíziós műsorok, youtube videók, újságcikkek segítségével lehetne szélesebb embertömegekhez eljuttatni a szakmát.

Célszerű lenne a lakosság szempontjából is folyamatosan a közbeszédben tartani az információbiztonságot. Ezt tájékoztató anyagok készítésével, előadások szervezésével

lehetne elérni, illetve nagyobb médiafelületet kellene biztosítani a területnek. Több hír jelenhetne meg az aktuális veszélyekről, csalásokról.

9. Összefoglalás

A dolgozat elkészítése közben feldolgoztam a témában az interneten fellelhető magyar és idegen nyelvű szakirodalmat.

A social engineering lényege, hogy a támadás elsősorban nem informatikai, hanem pszichológiai és kommunikációs eszközökkel történik.

Megvizsgáltam a támadók különféle típusait, rendszereztem a lehetséges támadási módszereket. Létezik humán és IT alapú támadás. Ezeket a technikákat jó és rossz szándékú hackerekén kívül alkalmazzák politikusok, pszichológusok, kémek, ügyvédek, orvosok, értékesítők, sőt még az átlagember is a hétköznapiak során.

Áttekintettem, hogy egy támadás milyen lépésekből áll. A kiindulási alapot a megfelelő mennyiségben és minőségben összegyűjtött információ adja. Erre építve tud a támadó kapcsolatot kiépíteni az áldozattal, majd kihasználni ezt a kapcsolatot, aminek következtében végre tudja hajtani a támadást.

A támadónak számos lehetősége van, hogy az áldozat pszichéjére hasson. A social engineer felismeri az arcon megjelenő makro- és mikrogesztusok, vagy a testbeszéd különböző jeleit. Ennek megfelelően az áldozat bizalmába tud férkőzni vagy éppen tudja őt befolyásolni, eközben különféle biokémiai folyamatok játszódnak le az emberi testben. Összegyűjtöttem, hogy milyen eszközök állnak a támadó rendelkezésére. Ezek között vannak szoftverek, amik nagymértékben megkönnyítik a munkavégzést, segítségükkel automatizálhatók a folyamatok. Vannak olyanok (kamerák, mikrofonok) amikkel az eseményeket rögzíthetik későbbi elemzés céljából és vannak álkulcsok, amikkel lezárt területekre lehet bejutni.

Megvizsgáltam, hogy milyen lehetőségei vannak egy átlagembernek a védekezésre és annak felismerésére, hogy támadás áldozatává válik, akár munkavégzés során, akár a mindennapi életben. Fontos, hogy a felhasználókban kialakuljon egy biztonság tudatos szemléletmód, és ennek megfelelően kezeljék eszközeiket. Ennek kialakításában nagy szerepe van a biztonság tudatossági programoknak, előadásoknak. A cégek szempontjából fontos, hogy segítsék munkavállalóikat a biztonságos számítógéphasználat elsajátításában, azáltal, hogy előadásokat, képzéseket szerveznek nekik. Egy vállalat biztonságos működése szempontjából lényeges, hogy legyen egy jól érthető, betartható

információbiztonsági szabályzat, amit bizonyos időközönként felülvizsgálnak, valamint auditokkal ellenőrzik annak betartását a munkavállalók részéről.

A dolgozatom végén két esettanulmány elemzésével a téma gyakorlati részébe tekintettem be, a SPEAKING modell segítségével.

10. Summary

This work offers an overview of social engineering techniques. Social engineering is the concept of an attacker exploiting human behaviour to gain access to the targeted network. I analysed the different types of social engineers and the types of attacks. Hackers, penetration testers, spies, politicians, salespeople, psychologists, lawyers and everyday people also use these methods. There are IT- based and human-based attacks.

There are a lot of steps in a social engineering attack. Firstly, one of the most important is information gathering. This is the most fundamental part of an attack. Sources for information gathering: social media, webpages, search engines, blogs. When the attacker has enough information, he chooses a victim and he makes contact with this person, build trust and finally he exploits the vulnerability.

Many psychological methods are used in social engineering. Social engineers know how to influence or manipulate the victim, how to build rapport. They can read facial expressions and body language, and they can use the information to reach their goals.

Prevention and mitigation are among the most important aspects of social engineering. Nowadays, ransomware attacks happen every day, organized criminal groups are rising and commit these crimes. To stop this process, we should create a security awareness culture. People must understand that anyone can be a target and realise how vulnerable we are. People should learn how to identify attacks, keep software updated and manage passwords properly. Companies should implement Security Awareness programs, as well as develop realistic policies.

In my research, my goal was to collect and understand the main principles behind these attacks. I have found this to be a very wide and exciting area. Preventing social engineering is challenging. One has to learn and practice nearly as much as a professional social engineer. It needs motivation, willingness to try and confidence. However, it is worth all the trouble, as we need professionals to teach us how to take our security awareness to a higher level, and defend us from the dark side.

11.Irodalomjegyzék

- [1] Dr. Lukács György – Döring András – Hell Péter: Vagyonvédelmi rendszerek I. – jegyzet (letöltve: 2020.09.26) – 9. oldal
- [2]
http://neak.gov.hu/felso_menu/lakossagnak/adatvedelem/elektronikus_informaciobiztonsag (online)
- [3] Bubán Márton: Információbiztonság tudatosság fejlesztése – előadás (letöltve: 2021.04.25)
- [4] Cristopher Hadnagy: Social engineering: Art of human hacking, Wiley, 2011, (letöltve: 2021.03.28)
- [5] Oroszi Eszter Diána: Social Engineering: Az emberi erőforrás, mint az információbiztonság kritikus tényezője, Budapesti Corvinus Egyetem, 2008 (letöltve: 2021.08.14)
- [6] Dr. Kollár Csaba: Hackerpszichológia – <https://www.slideshare.com/drkollarcsaba/hackerpszichologia> (online)
- [7] Cristopher Hadnagy: Social engineering: The science of human hacking, Wiley 2018, (letöltve: 2021.09.07)
- [8] Kollár Csaba, Zakar Ákos: A social engineering és a manipulációs technikák és módszerek – Biztonságtudományi Szemle II. évf., 2020/2 - 23-37. oldal (letöltve: 2021.04.12)
- [9] <https://www.social-engineer.org/framework/general-discussion/categories-social-engineers/> (online)
- [10] Bányász Péter, Bóta Bettina, Csaba Zágon – A social engineering jelentette veszélyek napjainkban (letöltve: 2021.08.05) -
- [11] Deák Veronika: Kártékony programok terjedése social engineering technikákon keresztül (letöltve: 2021.09.21) – 12-37.o.
- [12] <https://hu.encyclopedia-titanica.com/significado-de-simpat>
- [13] René Riedl, Andrija Javor: The Biology of Trust: Integrating Evidence From Genetics, Endocrinology, and Functional Brain Imaging - Journal of Neuroscience, Psychology, and Economics, V, 2012/2, 63-91.o. (letöltve: 2021.10.05)
- [14] Varga Katalin: Szexualitás, szülés, kötődés: Az oxitocin pszichoemotív hatásai (letöltve: 2021.10.17) – 449-476.o.
- [15] Cristpher Hadnagy: Unmasking the social engineer, Wiley, 2014 (letöltve: 2021.04.12)

- [16] Olivier Luminet, Delphine Grynberg, Nicolas Ruzette, Moïra Mikolajczak - Personality-dependent effects of oxytocin: Greater social benefits for high alexithymia scorers, *Biological Psychology*, (2011), <https://doi.org/10.1016/j.biopsycho.2011.05.005>. (letöltve: 2021.10.18)
- [17] Mikolajczak, M., et al. - Oxytocin not only increases trust when money is at stake, but also when confidential information is in the balance, *Biol. Psychol.* (2010), doi: 10.1016/j.biopsycho.2010.05.010 (letöltve: 2021.10.18),
- [18] Zak PJ, Stanton AA, Ahmadi S - Oxytocin Increases Generosity in Humans. (2007) *PLoS ONE* 2(11): e1128. <https://doi.org/10.1371/journal.pone.0001128>, (letöltve: 2021.10.18)
- [19] Elek Imre: Vagyon elleni cselekmények kulcskérdései (letöltve: 2021.11.14)
- [20] Kiss Attila, Krasznay Csaba - A felhasználói viselkedéselemzés kiberbiztonsági előnyei és adatvédelmi kihívásai - *Információs Társadalom XVII*, 2017/1: 55–71.o. (letöltve: 2021.11.20)
- [21] Leitold Ferenc: A felhasználói viselkedés, mint információbiztonsági kockázat becslése (letöltve: 2021.09.21)
- [22] Kollár Csaba: Az információbiztonság humán aspektusai, *Belügyi Szemle*, 2018/2, 22-45.o. (letöltve: 2021.04.12)
- [23] <https://cyberforces.com/en/the-pizza-method-a-social-engineering-case-study>, (online)
- [24] Dr. Kollár Csaba: Social Engineering a gyakorlatban. Manipulációk értelmezése a SPEAKING modellben, *JEL-KÉP*, 2017/3., 64-77.o. (letöltve: 2021.04.12)