

XXXI. Országos Tudományos Diákköri Konferencia

Had- és Rendészettudományi Szekció

Budapest, 2013. április 16-18.

Nemzeti Köszolgálati Egyetem

Hadtudományi és Honvédtisztképző Kar

**SOCIAL ENGINEERING A BIZTONSÁGTECHNIKA
TÜKRÉBEN**

***Jelige: Avagy a modern támadók már nem símaszkot, hanem álarcot
viselnek!***

Dolgozat lezárásának időpontja: 2012, november

Tartalom

1.	Előszó	3
2.	Bevezetés	3
3.	A social engineering fogalma	5
4.	A social engineering támadási technikáinak csoportosítása.....	8
4.1.	Humán alapú technikák	9
4.1.1.	Identitás lopás	9
4.1.2.	Reverse social engineering (fordított SE).....	13
4.1.3.	Valamit valamiért	13
4.1.4.	Jelszavak kitalálása.....	13
4.1.5.	Rutin munkát végzők segítségkérése.....	14
4.1.6.	Bejutás az épületbe	15
4.1.7.	Egyéb lehetséges módszerek	16
4.2.	IT alapú technikák	17
4.2.1.	Előzetes információszerzés.....	17
4.2.2.	Phishing (Adathalászat).....	19
4.2.3.	Kártékony programok.....	19
4.2.4.	Hálózatok figyelése	21
4.2.5.	Egyéb IT alapú támadások	22
5.	A social engineering pszichológiai vonatkozása	25
5.1.	Gondolkodási módok	26
5.2.	Mimika és apró árulkodó gesztusok (Microexpressions)	28
5.3.	Összhang-, szimpátiateremtés (Building rapport).....	29
5.4.	Személyiség felvétel (Pretexting)	31
5.5.	Kiderítési/kérdezési technikák (Elicitation).....	32
5.6.	Befolyásolási taktikák (Influence tactics).....	33
6.	A social engineering, mint a vagyonvédelem lehetséges támadási felülete	36
6.1.	Az őrzés-védelem támadási felületei a social engineering tekintetében.....	36
6.1.1.	A mechanikai védelem támadási felületei	37
6.1.2.	Az elektronikus rendszerek támadási felületei	39
6.1.3.	Az élőerős őrzés-védelem támadási felületei	41
6.2.	Adat- és információ biztonság támadási felületei social engineering tekintetében ...	42
6.2.1.	Menedzsment felületekhez való hozzáférés	42
6.2.3.	Szerverek	44
6.2.4.	Adatbázisok	45
7.	Kritikus infrastruktúrához tartozó objektum támadása (biztonsági-, social engineering audit).....	46
7.1.	Social engineering támadás felépítése	46
7.2.	A támadás menete	47
7.2.1.	Előzetes információszerzés.....	48
7.2.2.	Bejutás az épületbe	48
7.2.3.	Belső hálózathoz történő hozzáférés	49
7.2.4.	Személyes kontaktusok	50
7.2.5.	Biztonságtudatosság tesztelése egyéb módszerekkel	51
8.	Összefoglalás	54
9.	Irodalomjegyzék	57
10.	Ábrajegyzék.....	59

1. Előszó

Ezúton szeretnénk a sok fáradozásért és odaadó munkáért köszönetet mondani elsősorban két konzulensünknek Dr. Szádeczky Tamásnak és Oroszi Eszternek.

Köszönetünket szeretnénk kifejezni a gyakorlati helyszín biztosításáért és segítőkész közreműködésükért Sándornak és Ivettnek.

Továbbá hálásak vagyunk Varga Péternek, aki szakmai tanácsaival sokat segített a dolgozat előre menetelésében, Szécsi Bencének, a technikai segítségért, és mindenki másnak, akik egyéb módon segítették munkánkat.

2. Bevezetés

Napjaink információs társadalmában látjuk el feladatainkat, töltjük be szerepünket mindannyian. A biztonság, mint fogalom egy szűk réteg számára a foglalkozásukat, szakmájukat jelenti. A technika, az elektromos berendezések, és e mellett az informatika folyamatos és dinamikus, szinte forradalmi szinten fejlődik. Ennek következtében, akinek nem szakmája, vagy komoly érdeklődési köre, az használni használja, de a felhasználói szintnél jobban nem tájékozott az innovatív technika műszaki hátterében, sem az általa birtokolt információ, vagy adat megfelelő védelme tekintetében. Az átlagember nem megfelelően körültekintő személyes, vagy környezete biztonságát illetően, és emberi mivoltukból fakadóan sokszor könnyelmű, és naiv magatartásra hajlandó a biztonság szempontjából.

Ahogy a technika, úgy a biztonság tudomány is dinamikusan kell, hogy fejlődjön ahhoz, hogy megfelelő biztonsági intézkedésekkel, megoldásokkal, technikával tudjunk védekezni az esetleges veszélyek, kockázatok ellen. Az 1980-as évektől kezdődően főleg az Amerikai Egyesült Államok területéről, majd későbbiekben szerte a világból olvashattunk híreket, történeteket a kor biztonságtechnikai, informatikai-, információ védelmi fejlettségi szintjéhez mérten komplexen védett objektumokba, adatbázisokba való sikeres behatolásokról. Ez a jelenség, először mint a biztonságot érintő probléma volt jelen, majd aztán jelent meg ez a problémát orvosolni képes tudomány . Ezt a tudományt úgy hívjuk:

Social Engineering. Csupán az ezredforduló időszakában kezdhettünk komolyan beszélni ennek az „újkeletű” tudománynak a jelenlétéről.

Az emberi befolyásolás művészete korántsem számít egy újonnan feltalált eljárásnak, mindez csupán a humán pszichológia magas szintű ismeretén és gyakorlatán áll, vagy bukik. Persze ha nem a megfelelő alanyt választjuk tervünk kivitelezéséhez, könnyen megeshet, hogy kudarcba fullad próbálkozásunk, „rossz ajtón kopogtatunk”. Ha ez a pszichológiai tudás párosul a megfelelő technikai, biztonságtechnikai, és informatikai tudással és jártassággal, akkor a komplex vagyonsvédelmi rendszereket megkerülve támadásunk tervezésének, kivitelezésének csupán a fantáziánk szabhat határt.

Ezeket a támadásokat végrehajtó személyek lehetnek magánnyomozók, ipari kémek, hackerek¹, crackerek², szélhámosok, profi bűnözők, manapság már akár auditorok, szakértők, biztonsági szakemberek, akik fő célja lehetett pusztán pénzszerzés, ipari kémkedés, tudásuk és képességeik fitogtatása, vagy akár a bosszúvág, jó esetben biztonsági audit, a belső komplex vagyonsvédelmi rendszer biztonsági réseinek, az munkavállalók biztonságtudatosságának felmérése. Mindenesetre tény, hogy a vagyonsvédelmi rendszerek komplex megvalósítás esetén sem szolgálnak akadályul szándékuk megvalósításában.

A social engineering egy felettébb sarkalatos pontnak bizonyul a vagyonsvédelem szempontjából. Különös tekintettel az őrzés-védelemre, és adat- és információvédelemre, továbbá az IT biztonságra. Ennek oka, hogy egy komplex védelmi rendszer leggyengébb láncszeme az ember. Más kifejezéssel élve a legmagasabb biztonsági kockázatot mindig is a humán faktor jelenti. Ez alatt a biztonsági szempontú tervezési, kivitelezési hibáktól elindulva, a be nem tartott belső biztonsági szabályzat, az üzleti titkok és minősített információk helytelen kezelésén, az élőerős őrzés-védelem szakképzetlen állományán keresztül, a munkavállalók nem megfelelően biztonságtudatos magatartásán át számos humán kockázati lehetőséget érthetünk.

¹ **Hacker:** Egy területhez értő személy, akit a megismerés vágya hajt, élvezi a bonyolult problémákkal való foglalkozást, és a rendszerek működési határainak kiterjesztését. Elegáns, egyre jobb minőségű megoldások elérése törekszik. Az "igazi" hacker jellemzői: szaktudás, kitartás, kíváncsiság, segítőkészség. Ellentétben a sajtóban történő használatával a szónak, ez pozitív, és nem negatív jelző. – Kevin D. Mitnick – A megtévesztés művészete c. könyv előszava alapján

² **Cracker:** Olyan valaki, aki a meglévő hacker képességeit, tudását támadási célokra használja, ez az, aminek negatív tartalma van. – Kevin D. Mitnick - A megtévesztés művészete c. könyv előszava alapján

A fentiekben említettek alapján könnyen belátható, hogy a sok sikeresen végrehajtott támadás nagyrészt azért valósulhat meg, mert meglehetősen nagy párhuzam vonható a vagyonsvédelem legnagyobb kockázati egysége, és a social engineering legalapvetőbb tézisének kihasználása között, ami nem más, mint: maga az emberi tényező.

Mikor elkezdünk komolyabban érdeklődni, és olvasni a social engineering tudománya után, biztonságtechnikai mérnökhallgató létünkre hamar felismertük ezt a párhuzamot, és ekkor határoztuk el, hogy kutatjuk ezt a témát egy TDK dolgozat keretein belül. Legjobb tudomásunk szerint még nem készült eddigieken egyetemünkön efféle tanulmány, ami ezt a két különálló, ámár több szempontból összefüggő tudomány párhuzamait kutatja.

TDK dolgozatunk elkészítése során a következő célokat tűztük ki magunk elé:

- felkutatni és feldolgozni a jelenleg rendelkezésünkre álló nyomtatott és internetes szakirodalmakat a social engineering területén
- felkutatni a komplex vagyonsvédelmi rendszerek legéletszerűbb támadási felületeit a social engineering tükrében
- felkutatni az elméleti összefüggéseket és párhuzamokat a biztonságstudomány és a social engineering között
- kutatásunk gyakorlati részeként egy social engineering audit formájában megtámadni egy kritikus infrastruktúrához tartozó objektumot
- megválaszolni a következő kérdéseket:
 - Kiket kell jobban felkészíteni e támadási formák ellen?
 - Mennyire valós probléma ez jelenleg Magyarországon?
 - Mely módszerekkel lehet felkészíteni a munkáltatókat, munkavállalókat efféle támadások ellen?

3. A social engineering fogalma

Ahhoz, hogy pontosabban tudjuk értelmezni ezt a témakört, feltétlenül szükséges, hogy definiáljuk, több forrásból meghatározzuk az social engineering (továbbiakban SE) fogalmát. Aki találkozott már ezzel a fogalommal, vagy azt gondolja, hogy tudja, miről szól a SE, többnyire kérdésünkre, hogy „Mit is jelent ez?”, a fogalmat felszínesen épphogy érintő válaszokat ad.

Eddigiekben nem született még általános érvényű definíció a SE kifejezésre, mely bizonyára szoros összefüggésben áll annak tényével, hogy a témában könyv formában megjelent szakirodalmak száma nem haladja meg a tízet. Ennek ellenére, mivel a fogalom nem teljesen egzak, érdemes megemlítenünk azon szakmai fogalom meghatározásokat, melyekkel a téma irodalmában kutatva találkoztunk.

Kevin D. Mitnick, a méltán híres hacker, és a SE úttörője, írt néhány könyvet, melyek egyikében, *A legendás hacker* című művében így fogalmazott:

*„A social engineering a befolyásolás és 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.”*³

Douglas P. Twitchell az Illinois állami egyetem adjunktusa, akinek fő kutatási-, és szakterülete az informatikai és információs rendszerek biztonsága, így határozta meg a SE fogalmát:

*„Social engineering is the practice of using deception or persuasion to fraudulently obtain goods or information, and the term is often used in relation to computer systems or the information they contain.”*⁴

Azaz:

A social engineering a csalásnak vagy rábeszélésnek a gyakorlati alkalmazása információ-, vagy ingóságok szerzése érdekében. A -kifejezést gyakran használják számítógépes rendszer, vagy annak információ tartalmával kapcsolatban.

Végül, de nem utolsó sorban, a szakmában előjáró, kiváló szakember Christopher Hadnagy a következőképpen fogalmazza meg a *Social Engineering – The Art of Human Hacking* című könyvében mit is jelent ez a fogalom:

*„... social engineering is the art or better yet, science, of skillfully maneuvering human beings to take action in some aspect of their lives.”*⁵

³ Kevin D. Mitnick: *A legendás hacker a megtévesztés művészete*; előszó

⁴ Douglas P. Twitchell: *Social engineering in information assurance curricula*. 191-193, 3. InfoSecCD 2006: Kennesaw, Georgia, USA

Vagyis:

...social engineering a művészete, még inkább a tudománya annak, hogy gyakorlatias műveletekkel befolyásoljuk az emberi lényeket, azért hogy a célunk érdekében cselekedjenek az életük néhány helyzetében.

Mielőtt a mi elgondolásunk szerint határoznánk meg a SE-t, mint fogalom, érdemes, mint kifejezést értelmeznünk. Első fele: *Social*, azaz szociális, társadalmi, közösségi. *Engineering*: mérnökség. Ha figyelembe vesszük azt a feladatkört, amit általánosan egy mérnök ellát, akkor arra a következtetésre juthatunk, hogy egy social engineer társadalmi jellegű, embereket érintő kihívásokra, problémákra, fennálló helyzetekre keres a tervezett céljára megoldásokat, a szabályrendszerek és folyamatok ismeretében. Felméri a szituációt, információkat gyűjt, amiket felhasznál arra, hogy a speciális helyzethez képest el tudja készíteni a terveket, majd kivitelezni, mindezt társadalmi kommunikációs környezetben.

Ha tágabb értelemben nézzük, akkor számtalan, a hétköznapi életben előforduló esetben tapasztalhatjuk ezt a jelenséget. A síró kisgyerek, amikor nyalókát kér, az autókereskedő, amikor rábeszél minket, hogy nála vásároljunk, a politikusok, az üzletkötők, az ügyvédek, orvosok, és belátható, hogy mi is folyamatosan arra törekszünk, hogy céljainkat elérjük valamilyen úton-módon. Szeretnénk információt szerezni minél több dologról és ezért sokszor képesek vagyunk ferdíteni a valóságot, más arcunkat mutatni. A biztonság tekintetében is erre kell gondolni. A social engineer mindig úgy viselkedik, hogy megkapja azokat az információkat, amire szüksége van.

Ezen kontextusban a mi definíciónk a következő:

Olyan információszerzésre irányuló cselekvés, támadási forma, mely technikai ismeretekkel, vagy a nélkül az emberi lény alapvető pszichológiai tulajdonságait használja ki.

A SE-t mi a biztonságtechnika tükrében vizsgáljuk. Arra vagyunk kíváncsiak, hogy a különböző vagyónvédelmi rendszereket, hogy lehet megkerülni, vagy biztonsági réseit kihasználni ezen technikákkal. Fontosnak tartjuk, hogy ezekre a problémákra fel tudjon készülni a biztonságstudomány, hiszen a „rabló-pandúr” elsőbbségi harc mindig is jelen volt a

⁵ Christopher Hadnagy: Social Engineering. 10.o.

szakmában és mindig is törekedni kellett, és a jövőben is kelleni fog arra, hogy a lépéselőny a mi kezünkben legyen. Közös kihívása, és célja mindkét tudománynak, hogy az emberek biztonság tudatosan gondolkodjanak és cselekedjenek mind munkahelyi, mind magánéleti szférában, hiszen közös érdekünk, hogy az információs környezetünket, hétköznapi életünket, vagyontárgyainkat biztonságba érezhessük.

4. A social engineering támadási technikáinak csoportosítása

Ha megkérdezzük valakit, hogy mit is ért egy social engineering támadáson, többnyire az általános kép a telefonon történő átverés. Azonban ennél sokkal több és sokkal árnyaltabb az ehhez a fogalomhoz tartozó technikák tárháza. Egy támadás kapcsán beszélhetünk alapvetően humán és IT (számítógép) alapú támadásokról. Az utóbbi annyit tesz, hogy a social engineer egy közvetítő közegen, a számítógépen vagy más informatikai eszközön keresztül támadja meg az áldozatot. Ez utóbbi egyfajta könnyedséget jelent, hiszen nem kell személyesen találkozni az áldozattal.

A humán alapú egy kicsit nehezebb, hiszen ott élő a kontaktus. Az ilyen helyzetben sokkal nagyobb a lebukás veszélye, ezért fontos a megfelelő áldozat kiválasztása.

A kategorizálást Mitnick,⁶ Hadnagy⁷ és Oroszi⁸ munkássága alapján készítettük

Ebben a fejezetben bemutatásra kerülnek a legáltalánosabb támadási módok, technikák. A dolgozat nem általánosan a SE-ről szól, hanem a biztonságtechnika szemszögéből vizsgálja ezt a témát. Ezért a későbbiekben ezekre hivatkozva mutatjuk be az őrzés-védelemre, valamint az adat- és információ védelemre különösen érzékeny támadási módokat.

A felsoroláskor kitérünk egyenként arra is, hogy miért is működik maga a technika (*pszichológiai tényező*), hiszen a social engineer teljes mértékben tisztában van azzal, hogy miként működik az emberi lény.

⁶ Kevin D. Mitnick: A legendás hacker 1-2

⁷ Christopher Hadnagy: Social Engineering

⁸ Oroszi Eszter: Social Engineering, 28-54. o.

A saját biztonságunk érdekében célszerű egyfajta biztonságtudatos gondolkodást elsajátítani, mely segít a különböző helyzetekben megfelelően reagálni. Ebben a fejezetekben javaslatokat teszünk a lehetséges védelmi intézkedésekre.

4.1. Humán alapú technikák

Ezek a technikák gyűjteménye azokat foglalja magában, melyekhez a támadónak nincsen szüksége számítógéphez. Mivel egyszeri és általában visszakövethetetlen, az ilyen támadás kapcsán nagyon fontos, hogy résen legyünk. Sokszor fel sem fogjuk, hogy áldozatok lettünk és rekonstruálni is nehéz az esetet, mert csak az emlékeinkre hagyatkozhatunk, melyeket az agyunk szelektíven tárol.

A humán alapú social engineering támadások gyakori ismertetője, hogy a belső szlenget és szakkifejezéseket használják. A legkisebb gyanú felmerülésekor célszerű úgy alakítani a beszélgetést, hogy meggyőződjünk a hitelességről.

4.1.1. Identitás lopás

A humán alapú technikák nagy része alapvetően arra irányulnak, hogy a támadó egy másik személynek adja ki magát, amely lehet valós vagy fiktív személy.

Az ember alapvetően sztereotípiákra épít tudat alatt, melynek pszichológiai vonatkozása van. Azért van erre szüksége, hogyha találkozik valakivel tudja kategorizálni, tudjon viszonyulni hozzá. Ugyan ahhoz az egyénhez másként viszonyulunk, ha öltönyben jelenik meg, ha postás ruhában vagy ha koszos, tépett ruhában jelenik meg előttünk. Egyből egy képet alkotunk az agyunkban afelől, hogy mit vagyunk hajlandóak az illetőnek elhinni. Ezt a tulajdonságunkat nagyon jól ismerik a social engineerek és ki is használják, amikor csak tehetik.

4.1.1.1. Álruhába bújás

Legegyszerűbb technika, amikor valamilyen jelmezbe bújik a támadó. Ez lehet például vízvezeték szerelő, takarító, pizza futár, rendőr, stb. Előnye, hogy ez egy teljesen fiktív személy, tehát olyan tulajdonságot vesz fel a támadó, ami ideális.

Pszichológiai tényező: Azért könnyű így átverni az embereket, mert itt egyértelműen meg van a fejünkben egy kép, hogy mit kérhet az illető és mit nem. Mivel az egyenruha egyfajta biztosíték, egyfajta megnyugvást okoz, könnyebben osztunk meg az ezt viselőkkel információt, hiszen miért is gyanakodnánk?

Javaslat: Ha egyenruhát viselő emberrel van dolgunk, bizonyosodjunk meg arról, hogy

jogosan hordja-e ezt az öltözetet. Legegyszerűbb, valamilyen igazolványt kérni. Ezen kívül, ha ismeretlen „szakembert” (vízvezeték-, telefon szerelő stb.) engedünk az otthonunkba, munkahelyünkre, célszerű folyamatosan ellenőrizni tevékenységét.

4.1.1.2. Céges alkalmazottnak adja ki magát

Egy multinacionális vagy egy több telephellyel rendelkező vállalatnál nem alapfeltétel az, hogy ismerünk minden kollégánkat, minden alkalmazottat. Ezért gyakran előfordul, hogy ezt kihasználva próbálják az áldozatot befolyásolni.

Pszichológiai tényező: A csapatba tartozás az ember olyan igénye, melyet ősidők óta hordoz, hiszen enélkül nem élte volna túl az elmúlt pár ezer évet. A fennmaradáshoz a tagok folyamatosan segítették egymást. Ez a támadási mód is erre épít. A csapat egyik tagja rászorul a segítségünkre, ezért általában fenntartások nélkül adunk ki információkat ilyen megkeresésekkor.

Javaslat: Győződjünk meg arról, hogy az ismeretlen tényleg a cégnél dolgozik-e és ha igen, jogosult-e az információk megszerzésére. Ennek módja lehet, hogy mielőtt kiadnánk, egy kis időt kérünk és visszahívjuk a céges adatbázisban szereplő telefonszámon. Célravezető lehet az is, hogy a felettesét kérdezzük meg arról, hogy jogosult-e az információk megszerzésére.

4.1.1.3. Partner cég alkalmazottjának adja ki magát

Ez a támadás az előzőnek egy speciális esete, melyben a partnercég, beszállító, szolgáltató (biztonsági szolgálat, külsős IT szolgáltató) emberének adja ki magát. Ez akkor a leghitelesebb, ha szinte napi kapcsolatban van a két szervezet.

Pszichológiai tényező: A 4.1.1.2-ben leírtakkal nagyon hasonlít. A különbség az, hogy itt a két csapat egymásra utaltsága a meghatározó tényező.

Javaslat: A 4.1.1.2-ben leírtak.

4.1.1.4. Új munkaerőnek adja ki magát

Szintén a nagyobb vállalatoknál, ahol nem ismer mindenki mindenkit, gyakran előforduló támadás az új alkalmazottként történő bemutatkozás.

Pszichológiai tényező: Amikor egy új munkahelyre kerülünk, sok dolgot nem ismerünk. Ezért szükségünk van segítségre a beilleszkedéshez. Általában szívesen adunk tanácsot és mondunk el információkat azoknak, akik újak a csapatban, hiszen ezt mi is elvárnánk ellenkező esetben.

Javaslat: A 4.1.1.2-ben leírtak.

4.1.1.5. Magas pozíciójú embernek adja ki magát

A támadó valamilyen vezetőnek, magas pozíciójú emberként kér, utasít valakit arra, hogy adja oda az információkat. Ez a megközelítés is akkor működik, ha elég nagy a cég ahhoz, hogy ne ismerjen mindenki mindenkit.

Pszichológiai tényező: Az ember alapvetően konfliktuskerülő lény. Nem szeret olyan dolgokba beleavatkozni, mely az ő komfort-zónáját veszélyeztetni. Vitatkozni, megkérdőjelezni valamely, a hierarchiában magasabban álló személyt veszélyes lehet. Szélsőséges helyzetben akár az állásunkba is kerülhet, ezért nem szívesen szegülünk szembe a vezetőink döntésével.

Javaslat: Mivel felmerülhetnek gondok a „számonkérésből”, ezért az 1.1.2-ben leírtakhoz hasonlóan győződjünk meg személyéről és annak hitelességéről. Azonban célszerű ezt minél diszkrétebben megtenni.

4.1.1.6. Fontos embernek adja ki magát

Nagyon hasonlít az előző pontban említetthez. A különbség annyi, hogy nem cégen belüli személy bőrébe bújik az illető, hanem például hatósági személy, külső auditor, NAV ellenőr, stb. Ez egy ritkábban használt technika, mivel nehezebben kivitelezhető, de egy telefonos támadásnál nem kizárt, hogy találkozunk vele.

Pszichológiai tényező: A 4.1.1.5-ben leírtak.

Javaslat: A 4.1.1.5-ben leírtak.

4.1.1.7. IT szakembernek/rendszergazdának adja ki magát

Ennél a támadásnál a támadó egy számítógépes szakembernek adja ki magát.

Pszichológia tényező: Mivel az emberek nagy része nem ért a számítógépekhez, csak a felhasználói platformokhoz (néha még ahhoz sem teljes mértékben), könnyen megtéveszthetők egy kis szakzsargon használatával. Ha a támadó minimálisan ért az informatikához, könnyen átverheti a gyanútlan áldozatokat.

Javaslat: Mielőtt odaengednénk bárkit is a számítógépünkhöz, győződjünk meg arról, hogy tényleg jogosult-e ehhez. Célszerű tudni, hogy a rendszergazdának az esetek legnagyobb részében nem kell az adott géphez közvetlenül odamennie, illetve anélkül is elér mindent, hogy mi a jelszavunkat megadnánk.

4.1.1.8. „Tombstone theft” („sírkő lopás”)

Egy igen ritka támadási technika⁹. A támadó egy már elhunyt embert személyesít meg. Ez úgy lehetséges, hogy amikor a tragédia megtörténik valakivel, nem automatikusan törlődik minden rendszerből. Maradhatnak bankszámlái, különböző adatbázisokból sem törlődik egyből. Ezt kihasználva tudnak személyiséget lopni a támadók.

Pszichológiai tényező: Jelen esetben szintén az emberek naívságára építenek a támadók. Nagyon sok munkahelyen nem néznek utána az embereknek. Mivel a megszemélyesített ember már nem tud közbeszólni, szabadon használhatják még az ő adatait, mintha élne.

Javaslat: Nézzünk utána annak a személynek, aki érdeklődik. Ennek módja lehet például a 4.1.1.2-ben leírtak.

4.1.1.9. „Third party authorization” (felhatalmazás)

Itt nem konkrét megszemélyesítésről van szó. Ezen technikában a támadó egy harmadik személyre hivatkozik, mely gyakorlatilag a 4.1.1.1-4.1.1.7-ig bármelyik személy lehet.

Pszichológiai tényező: A korábban leírt pszichológiai tényezők itt is ugyan úgy jelen vannak. Ez a social engineer ügyességétől függően, a hivatkozás kapcsán, lehet erősítő vagy gyengítő körülmény.

Javaslat: Ha egy másik személyre hivatkozik valaki, célszerű utána kérdezni a 4.1.1.2-ben leírtak alapján.

4.1.1.10. Hamis bizalomkeltés

Ezekben az esetekben a támadó nem próbálja más szerepét felvenni. Egyszerűen úgy viselkedik, hogy pozitív benyomást keltsen. Erről részletesebben a 4.3. fejezetben olvashatunk.

Pszichológiai tényező: Az emberek a mai rohanó világban számos esetben találkoznak olyan társaikkal, akik viselkedése zavarja őket. Ezért amikor egy udvarias, kedves emberrel van dolguk szívesen engedik magukhoz közel.

Javaslat: Amikor valaki túl kedves, célszerű egy picit gyanakodni. Nem törvényszerű, hogy az ilyen emberek kárt szeretnének okozni, de első pillanatra ne bízunk meg valakiben feltételek nélkül.

⁹ http://www.social-engineer.org/framework/Social_Engineers:_Identity_Thieves#Tombstone_Theft; 2012.11.04.

4.1.2. Reverse social engineering (fordított SE)

Sokszor előfordul az a támadási mód, hogy a támadó felvet egy még nem létező problémát az áldozatnak. Biztosítja róla, hogy ha véletlen fellépne mégis az adott helyzet, őt bizalommal keresheti, szívesen segít. Kis idő elteltével előidézi a problémát, mely után az áldozat örül, hogy tudja kihez kell fordulnia. Megkeresi a támadót, aki segít. Persze így a saját számítása szerint fér hozzá a számára szükséges információkhoz.

Pszichológia tényező: A kedves figyelemfelhívást mindenki hálásan veszi. A probléma bekövetkezése után pedig energiát takaríthatunk meg, ha tudjuk kihez kell fordulni és nem kell szakembert keresni.

Javaslat: Ez már egy kicsit összetettebb támadás. Ha felmerül valami hiba, mindenképpen tájékozódjunk annak eredetéről és kérdezzünk meg mást is, azon a személyen kívül, aki felhívta a figyelmünket erről. Ez különösen akkor fontos, ha nem ismerjük személyesen az illetőt.

4.1.3. Valamit valamiért

A reverse social engineering egy speciális esete. Az előidézett hiba megoldása után a támadó kér egy szívességet, melyről tudja, hogy normál esetben nemleges választ kapna. Pszichológiai tényező: Ha valaki ad, a társadalmi normák szerint jogosan vár cserébe valamit. Ezért amikor segítenek nekünk, úgy érezzük, hogy tartozunk a másiknak. A támadó ezt használja ki.

Javaslat: A 4.1.2-höz hasonlóan járunk a probléma után. Illetve, miután szívességet kérnek tőlünk, ne tegyünk hasonló esetekben többet meg, mint normál esetben tennénk.

4.1.4. Jelszavak kitalálása

A jelszavak megszerzésének több módja van. Ezeknek egy részéhez szükséges valamilyen informatikai tudás, szoftver. Azonban a jelszavak egy része az emberi butaság, figyelmetlenség miatt könnyen kitalálható, megfejthető. Nem kell hozzá csak egy kis informálódás az illetőről, akiét ki szeretnénk találni. Az alpontokban ismertetjük milyen lehetőségek tartoznak a humán alapú technikákhoz.

4.1.4.1. Alapértelmezett jelszavak

Sok rendszerben találunk alapértelmezett jelszavakat, melyek megváltoztatásának fontosságát a felhasználói utasítások, biztonsági ajánlások mindig hangsúlyoznak. Ezt nagyon

sokszor elfelejtik, vagy egyszerűen nem tulajdonítanak neki jelentőséget.

Példák az alapértelmezett jelszavakra: admin, 0000, 1234, 123456, stb.

Pszichológiai tényező: Az emberek nagytöbbségével még nem történt jelszószerzésből adódó visszaélés. Ezért úgy gondolják, hogy ez csak rémisztgetés, ezért nem is veszik komolyan. Az érdektelenség, a figyelem hiánya mindig is kedvezett a rosszakaróknak.

Javaslat: Az alapértelmezett jelszavakat mindig változtassuk meg a biztonsági kritériumoknak megfelelően.

Azért is fontos ezzel tisztában lenni, mert sok informatikai eszköznek az alap felhasználónevét és jelszavát megtalálhatjuk az interneten (*default password*).

4.1.4.2. Személyre utaló jelszavak

A másik ilyen kategóriát képezik azok a jelszavak, melyek a személyhez kötődnek. Születési időpont, rokonok, kedvencek dolgok neve, hobbi stb. Ezeket egy kis kutatómunkával meg lehet tudni, rá lehet jönni.

Pszichológiai tényező: Sok helyen kell jelszót megadnunk, ezért próbálunk számunkra megjegyezhető kitalálni, így kézenfekvőnek bizonyul a fent felsorolt kategóriákból választani egyet. Ezzel az a baj, hogy tudják mások is és könnyen kideríthetik, ha tanulmányozzák az adatainkat, szokásainkat. Ez a közösségi oldalak korszakában igen kritikus pont.

Javaslat: Ha lehet, kerüljük az effajta jelszavakat (vagy egészítsük ki azokat egy bonyolultabb karaktersorozattal).

4.1.5. Rutin munkát végzők segítségkérése

A funkciójából fakadóan a help desk-en, titkárságon, ügyfélszolgálaton, tanulmányi osztályon stb. dolgozók igen nagy veszélynek vannak kitéve a social engineering támadásoknál. Szerencsére a kritikus helyzet miatt az ő figyelmüket jobban fel szokták hívni az ilyen jellegű támadásokra, de ennek ellenére előfordulhat az, hogy álsegítséget kérnek a támadók. Ha nem elég képzett a munkatárs, nagyobb valószínűséggel előfordulhat sikeres támadás.

Pszichológiai tényező: Gyakorlatilag bármilyen mese kitalálható, hiszen pont a segítség kérés megoldása az ilyen munkakörök feladata.

Javaslat: Ha ilyen területen dolgozunk járjunk utána a kérő személyének és a kérés jogosságának.

4.1.6. Bejutás az épületbe

Egy támadás kivitelezéséhez sokszor az épületbe kell bejutni. Egy gyakorlott social engineernek ez nem jelent akadályt. Ebben a fejezetben bemutatásra kerülnek azok a technikák, melyekkel a beléptető rendszereket ki lehet kerülni. Ez a fejezet kiemelten fontos, ha a biztonságtechnika szemszögéből vizsgáljuk a social engineeringet.

4.1.6.1. Tailgating

A technika lényege, hogy bejutáskor egy csoporthoz csapódik a támadó. Azaz kiadja magát egy üzleti partnerekből álló delegáció, takarítóbrigád, stb. tagjának. Ehhez egy jó álca (öltöny vagy munkásruha) szükséges. A támadó alakíthatja az elkésett csoporttagot is, ez különösen akkor célszerű, amikor a csoport tagjai ismerik egymást.

Pszichológiai tényező: A hiteles alakítás lényege az előzetes informálódás. Sok esetben a biztonsági szolgálatot teljesítők nem ellenőrzik minden egyes belépő személyazonosságát. Ennek két oka van. Egyik, hogy hanyagok és figyelmetlenek, a másik pedig az, hogy nem illik például egy magas rangú delegációt végigkérdezgetni.

Javaslat: Célszerű a lehetőségekhez mérten mindig ellenőrizni a belépési jogosultságot például egy előre megadott névsor alapján, amit személyes okirattal igazolnak. Másik ellenőrzési forma lehet a beléptető kártya alkalmazása (pl.: vendégkártya). A jól konfigurált, helyesen beállított beléptető rendszer nagyobb biztonságot teremt és a munkavégzést is megkönnyíti.

4.1.6.2. Késés

Az előző pontban már érintett technika teljesen alap szituációban is alkalmazható. Egyszerű munkaruhában (cég specifikusan) a támadó azt színleli, hogy késésben van. Egy hamis RFID kártya használatával tudja imitálni, hogy a rendszer valamiért nem működik helyesen. De nincs ideje ezt megvizsgálni, mert pl. fontos tárgyaláson kellene már lennie. Pszichológiai tényező: Az emberi jóindulatot használja ki ez a bejutási forma. A rendszert felügyelő személy jót szeretne cselekedni a késésben lévő egyénnel. Megnyugtatóják azok a szimbólumok, amiket lát. A ruházat, a viselkedési forma mind hitelessé teszi a „későt”. Ezek mellett alkalmazott helyi specifikációs szavak (Pl.: „A B2-ben van egy fontos tárgyalásom a vezérigazgatóval”) elősegítik a támadás sikerességét.

Javaslat: Amennyiben nem ismerjük az illetőt győződjünk meg a belépés jogosságáról a céges adatbázis leellenőrzésével, hiszen az azonosítás minimális időt vesz igénybe.

4.1.6.3. Hamis ID használata

Utánajárást, kutató munkát követően kideríthetjük hogyan néznek ki a belépőkártyák. Amennyiben nincs megfelelő beléptető rendszer könnyen elkészíthető egy valósághű másolat, melyet felmutatva az őrk elhiszik annak hitelességét és a belépésre való jogosultságot.

Belépőrendszer meglétével is másolhatóak az RFID kártyák, de ehhez már speciális technika használata szükséges, mely nem a dolgozat tárgyát képezi.

Pszichológiai tényező: Az őrben hamis biztonságérzetet kelt a kártya jelenléte. Könnyen készíthető kiváló minőségű másolat. Az természetesen nem várható el egy biztonsági szolgálatot végző személytől, hogy az összes kártyát tüzetesen vizsgálja át.

Remek példa a budapesti metróknál a bérlet érvényességét vizsgáló ellenőrök, akik legtöbbször ugyan ott állnak, mégsem ellenőriznek kellő képen, csupán rápillantanak a felmutatott iratokra, melynek során a lejárt, illetve hamisított bérleteket, illetve igazolványokat nem feltétlenül veszik észre.

Javaslat: Célszerű bevezetni egy jól működő beléptető rendszert, amennyiben a cég kapacitása igényli. Ennek pontosabb leírását később ismertetjük.

4.1.6.4. Piggybacking

A piggybacking magyarul más jogosultságának felhasználását jelenti. A támadó, aki nem jogosult a belépéshez kiadja magát egy olyan személynek, aki beléphet az adott helyre. Jellemzően az otthonmaradt kulcs, belépőkártya történetet játszik el. Többek között a VIP jegyeket a koncertekre, bulikra név alapján adják ki. Ha bemutatkozunk mint egy, a listán szereplő vendég, könnyen belépést nyerhetünk.

Pszichológiai tényező: A hanyagság, a figyelmetlenség, a segítőkészség mind jelen van ennél a technikánál. Ha az otthon maradt eszköz története kerül elő, a már megismert pszichológiai tényezők az érvényesek, míg egyszerűen névre történő belépésnél pedig a hiszékenység kihasználása dominál.

Javaslat: A piggybacking ellen legegyszerűbb védekezési forma, ha nem engedünk be a saját kártyánkkal másokat, hanem ilyen eseteknél vendégkártyát kérünk az illetőnek. Ennek bővebb kifejtése a 5.1.2-es fejezetben található.

4.1.7. Egyéb lehetséges módszerek

Ebbe a kategóriába az egyéb humán alapú technikák kerülnek, melyek az előző kategóriákba nem tartoztak közvetlen bele.

4.1.7.1. Shoulder surfing

A „váll szörfölés” kedvelt technikája a PIN- kód, jelszószerzésnek. A támadónak nincs más dolga, mint közel kerülni az áldozathoz akkor, amikor beüti a karaktereket. Egyszerűen úgy csinál, mint ha nem nézné.

Pszichológiai tényező: Az emberek nemtörődömsége, hanyagsága könnyű prédává teszi őket. Javaslat: Ha más személy van a közelünkben figyeljünk oda, hogy ne láthassa a beírt jelszavunkat, kódunkat, annak beütése során amennyire lehet, takarjuk azt.

4.1.7.2. Dumpster diving (kuka búvárkodás)

Rengeteg értékes információt dobnak ki az emberek felelőtlenül a szemétkbe. A támadónak nincs más dolga, mint hogy a megfelelő szemétkben keresgéljen. Ezek az információk lehetnek például számlaszámok, jelszavak, adatbázisok, stb.

Pszichológiai tényező: Az emberek úgy gondolják tudat alatt, hogy ami a szemétkbe került, az már meg is semmisült. Ez természetesen egy hamis érzet, melyet odafigyeléssel el lehet kerülni. Javaslat: Gondoljuk végig mit helyezünk a szemétkünkbe. Az érzékeny információt tartalmazó papírokat célszerű egy iratmegsemmisítő berendezéssel ledarálni.

4.2. IT alapú technikák

Ez a fejezet tárgyalt technikák ugyan informatikai eszközöket használnak, de mégis az emberi mulasztás, hiszékenység kihasználása a fontos. A social engineer ezeknél a támadásoknál nem töri meg a rendszereket, csupán kihasználják azok gyengeségeit.

Az ilyen típusú social engineering az előzetes információszerzésre vagy a folyamatos információáramoltatásra irányul.

4.2.1. Előzetes információszerzés

Ezek azok a támadások, amik a kiindulási pontot jelentik egy-egy hosszabb támadási ciklus során. Ezen esetekben a támadónak könnyű dolga van, hiszen nincs közvetlen kapcsolat az áldozattal. Közös jellemző, hogy elhitetik a gyanútlan emberekkel, hogy egy valós rendszerrel kommunikálnak, hogy így könnyen megszerezhessék a számukra szükséges információkat. Az ilyen technikák a következők:

4.2.1.1. Internet böngészése

Meglepően sok információ található meg az Interneten. A kereső oldalak segítségével emberekről, cégekről, rendszerekről nagyon sok dolog megtalálható. Különösen kritikusak a blogok és közösségi oldalak.

Pszichológia tényező: Alapvető dolog az életünkben, hogy szeretnénk közölni a külvilággal létezésünket, így biztosítani az üzletet.

Fontos szempont, hogy nem csak saját magunk oszthatunk meg a világgal információkat, hanem tőlünk függetlenül, a mi akaratunkon kívül ezt más is megteheti. Sajnos ez nagy kockázati tényező, hiszen névtelenül, felelősség nélkül áramlanak az információk, melyeket nagyon könnyen ki tudnak használni a rosszakarók.

Javaslat: Fontos, hogy legalább a saját magunk által közzétett információkat úgy válogassuk meg, hogy tisztában legyünk annak kockázatával. Ez nem azt jelenti, hogy semmit ne tegyünk közzé. Legyünk körültekintőek és használjuk ki az opcionális csoportokat, kik láthatják a közzétett információkat.

A biztonságtudatos kezelése az adatoknak természetesen csak megnehezíti a támadó dolgát, nem akadályozza meg. Azonban ez elegendő lehet arra, hogy ne mi legyünk az elsődleges célpontok.

4.2.1.2. Közösségi portálok figyelése

A támadó valós személyként, vagy egy frissen létrehozott felhasználói fiók segítségével a különböző közösségi oldalakon kutat információk után. Ez lehet személyes vagy különleges adat,¹⁰ esetleg az egyén szokása. Rengeteg információt hordoznak a bejelölt kedvencek, a feltöltött képek és a videók is. Ez azért fontos, mert ezek az adatok a támadások alapötletei lehetnek.

Pszichológiai tényező: A közösségi oldalak már a mindennapjainkhoz nőttek olyannyira, hogy egyfajta függőséget is okoztak. A túlzott megosztás, a felelőtlen magatartás következtében létrejövő adatmennyiség tárházat biztosít azoknak akik szeretnének utánunk kutatni.

Javaslat: Rengeteg ajánlás létezik már arra, hogy miként viselkedjünk az ilyen típusú oldalakon. A TDK munkánk tartalma nem terjed ki ezek tárgyalására, de összességében

¹⁰ Id. 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról 3. §

legyünk körültekintőek a kapcsán, hogy mit adunk ki magunkról, és kik láthatják az általunk megosztott tartalmakat.

4.2.2. Phishing (Adathalászat)

A támadás lényege, hogy a támadók valamilyen elektronikus csatornán keresztül (pl. e-mail) olyan üzenetet juttatnak el az áldozathoz, ami egy olyan oldalra irányít, ami a saját bizalmas adatainak, jelszavának megadására kéri a célszemélyt.

Az adathalászatnak sok változata jelent már meg. Ezek felsorolás szinten kerülnek említésre. A tagok után zárójelben lévő kifejezések a specifikációra utalnak:

- Hagyományos adathalászat (hamis levél és hamis weboldal)
 - Nyereményt, jutalmat ajánl fel a „regisztrációért”
 - Szankciókkal fenyegetőzik
- Vishing (telefon üzenetrögzítőn, messenger programokon)
- Smishing (SMS)
- Pharming (DNS szerver sebezhetőségeit használja ki)
- Whaling (cégvezetőkre irányul)

Pszichológiai tényező: A hiszékenységet és a tudatlanságot használja ki ez a támadás. Általában az oldalak, ahova irányítanak valamilyen regisztráció, bejelentkezési felület, esetleg „közvélemény kutatás” oldalának tűnnek, melyeket a gyanútlan ember készségesen kitölt. Javaslat: Az ehhez hasonló oldalak általában valamilyen hibát rejtenek magukban. Ez lehet a szöveg értelmetlensége (mert egy fordító program segítségével küldték), a weblap domain címének furcsasága, biztonságos kapcsolat hiánya (<https://> helyett <http://>) stb.

4.2.3. Kártékony programok

Ezek a támadási formák általában egy szoftver segítségével többszöri információlopásra alkalmasak, de van, hogy csak egy jelszó megszerzése a cél. Fontos megjegyezni, hogy a vírusirtók, tűzfalak ezek egy részét képes felismerni, megakadályozni. Azonban az egyedi készítésű, célzott támadásra szánt kártékony programok sokszor gond nélkül tevékenykednek.

4.2.3.1. Frissítés/javítás felajánlása

A gyártó nevében egy ingyenes frissítési/javítási lehetőség érkezik. Ennek letöltése valamilyen kárt okoz.

Pszichológiai tényező: A levél küldője gyakorlatilag szívességet tesz nekünk azzal, hogy elküldi a szoftver ingyenes továbbfejlesztett változatát. Az igazi üzleti életben az ilyen felajánlások fontosak lehetnek. A lényeg, hogy a naivságunkat tegyük félre.

Javaslat: Győződjünk meg, hogy valóban van-e olyan frissítés, szükségünk van-e erre. A túlzott jóindulat vagy erőszakosság is gyanús lehet.

4.2.3.2. Csatolmányok

A kártékony programok leggyakoribb terjedési módja. Valaki nevében küldött e-mail (üzleti vagy magán jellegű) csatolmányára hivatkozik a feladó. Arra kéri a címzettet, hogy nyissa meg, mert egy fontos képet, egyéb dokumentumot tartalmaz. A megnyitással aktiválódik a kártékony program.

Pszichológiai tényező: Sokszor kaphatunk fontos e-mailben történő mellékleteket családtagunktól, üzletfelünktől. Ezt kihasználva küldenek álcímekről leveleket.

Javaslat: Győződjünk meg, hogy tényleg az adott személy küldte az e-mailt. Az esetek nagy többségében a fontos ilyen jellegű file-okra számítunk, ezért a váratlan ilyen jellegű üzenetekre különösen érdemes figyelmet fordítani.

Ha bármilyen gyanú is felmerül a melléklet hitelességéről nem szabad megnyitni azt.

4.2.3.3. Keylogger

A keylogger, billentyűzet leütés figyelő két fő típussal rendelkezik. A szoftveres és a hardveres változat lényege ugyan az. A leütött karakterekről vagy a képernyő tartalmáról készít egy napló file-t, amit vagy passzívan eltárol, melyet később a géphez ismét hozzáférve szereznek meg, vagy továbbküldi egy távoli gépre.

Pszichológiai tényező: A keylogger a figyelmetlenségre és a tudatlanságra épít.

Javaslat: Ha valami gyanús eszköz van a számítógépünkhöz csatlakoztatva, legyünk óvatosak. A szoftveres megoldásoknak azon részét, ami aktívan küldené az információt a tűzfalak kiszűrjük. A többi ellen csak a körültekintéssel, folyamatos ellenőrzéssel tudunk védekezni.

4.2.3.4. Baiting

Gyakori SE támadás az, amikor valamilyen adathordozót (CD, pendrive) otthagynak valahol, célszerűen egy számítógép közelében. Amikor a gyanútlan áldozat csatlakoztatja a számítógépbe az eszközt, hogy megnézze kié lehet, megtörténik a fertőzés. A figyelemfelkeltés érdekében szöveg elhelyezése gyakori az ilyen disk-eken, pendrive-okon. Ez lehet pl.: szexi képek, bizalmas, stb.

Pszichológiai tényező: A gyanútlan áldozat vagy azért, mert nem tudja kié lehet és megszeretné nézni, vagy információ vágy miatt, de behelyezi a számítógépbe az ismeretlen adathordozót.

Javaslat: ha találunk ilyen eszközt, kérdezzük meg kié lehet. Amennyiben nem kapunk rá megfelelő választ fenntartással kezeljük az eszközt. Ha cégnél találjuk adjuk oda az IT-nak (esetleg az információ biztonságnak), hogy vizsgálja meg, kié lehet illetve van-e rajta káros tartalom.

4.2.3.5. Trójai programok

Azokat a programokat nevezzük trójaiaknak, melyek látszólag valami hasznos, szórakoztató funkcióval bírnak, de eközben a háttérben kártékonyan tevékenykednek. Ez a hatás lehet romboló, megfigyelő, stb. A program eljuttatása az előzőekben leírt módon történhet.

Pszichológiai tényező: Az ilyen programok másodlagos funkciója az, amit a „kirakatba” mutatnak elénk. Azt használja ki, hogy nem gondolunk bele abba, hogy a felszín mögött lehet más is.

Javaslat: Csak tiszta szoftvereket töltsünk le licensz megvásárlásával. Ha mégsem tudjuk ezt megtenni, használjunk ingyenes, ugyanilyen funkcióval rendelkező programot.

4.2.4. Hálózatok figyelése

A hálózatok kutatása egyrészt hacker tevékenység. Azonban felderíteni különböző ingyenes programokkal, melyek letölthetők az internetről, gyakran a social engineerek kedvelt tevékenysége. Leggyakrabban a WiFi hálózatokat könnyű a különböző okostelefonokra írt alkalmazásokkal kideríteni. Kicsit komolyabb támadások vitelezhetőek ki notebook segítségével.

Ezek nagyon jó információtárat nyújtanak a későbbi támadások során. (Pl.: „kérlek segíts, nem tudom a WiFi jelszót”)

Pszichológiai tényező: A hálózatbiztonsághoz mégannyira sem értenek az átlag emberek, mint az alap számítógép biztonsághoz. Egy rosszul kiépített hálózat ezért könnyű támadási felület lehet.

Javaslat: Rengeteg ajánlás van a hálózat biztonságra, például SSID szórásának tiltása, MAC adress alapján való szűrés, WPA használata. Ennek bővebb kifejtése nem tartozik a dolgozat témájában.

4.2.5. Egyéb IT alapú támadások

Azok a támadások, melyek nem férnek bele az előző két csoportba, illetve valamilyen más eszköz (telefon, PDA, stb.) használatát igénylik ebbe a csoportba soroljuk.

4.2.5.1. Telefonbeszélgetés

Ez egy klasszikus social engineer támadási technika. A támadó felhívja az áldozatot telefonról. Megszemélyesít valakit az 1.1-ben leírtak alapján és távolról próbálja elérni, hogy megkapja az információkat. Gyakran cél az ilyen támadásoknál egy dokumentum elkérése. Pszichológiai tényező: A telefon, mint közvetítő közeg sokkal személyesebb, mint az e-mail. Ezen okból kifolyólag sokkal meggyőzőbb is tud lenni és nem hordozza magában azt a veszélyt, hogy az áldozat később kép alapján felismerje a támadót. A 4.1.1. fejezetben leírt pszichológiai tényezők itt is vonatkoznak megszemélyesítésekre.

Javaslat: Ha egy ismeretlen személy kér tőlünk bármilyen adatot, dokumentumot mindig kezeljük fenntartással. Győződjünk meg a kérés valóságáról, a személy azonosságáról. Ez utóbbit legjobban kérdésekkel tudjuk megtenni.

4.2.5.2. Látszólag belső cím

A social engineer létrehoz egy belső e-mail címre nagyon hasonlító másikat. Ez után valamilyen csatornán megkéri az áldozatot, hogy juttasson el egy file-t.

Gyakori változata, hogy egy telefonálás kapcsán megkéri az áldozatot a támadó, hogy juttasson el neki egy belső dokumentumot. Arra hivatkozva, hogy nem tartózkodik a cégnél két címre kéri a file-t. Egyik egy nem létező, mely a céges szabályoknak megfelel, míg a másik egy magán postafiók. Természetesen a nem létezőről visszapattan a levél, de a másolatot már meg is szerezte a támadó.

Pszichológiai tényező: A figyelmetlenséget és hiszékenységet kihasználva nem nehéz átejtetni a gyanútlan áldozatokat.

Javaslat: Érdemes létrehozni egy olyan rendszert, mely meghatározza, milyen dokumentumot, kinek küldjünk. A jól működő e-mail karantén rendszer is megoldást nyújthat ebben az esetben, ahol meg van határozva mit lehet külsős e-mail címre kiküldeni és mit nem. Ennek oktatása kiemelten fontos egy cég életében, hiszen az elektronikus levelezés egy kritikus pont az információ biztonság kapcsán.

4.2.5.3. Távoli e-mail hozzáférés

Ez egy forgatókönyve a telefonos social engineeringnek. A támadó betegségre vagy más okra hivatkozva kéri, hogy hozzá férhessen a leveleihez otthonról. Az ok általában egy sürgős e-mail várása, mely egy nagyon fontos üzlethez szükséges. Ennél nehezebb körülmény, hogy általában az illető számítógépe is szükséges lehet, ha a célszemély csak azon keresztül képes csatlakozni a vállalati hálózathoz.

Pszichológiai tényező: Egy ilyen kérés megtagadása komoly következményekkel jár, főleg, ha a támadó valamilyen vezető beosztású embernek adja ki magát.

Javaslat: Győződjünk meg arról, hogy valóban érvényes a jogosultsága a kérőnek. Ennek legegyszerűbb esete a felettes megkérdezése.

4.2.5.4. Okostelefonok/PDA-k támadásai

Az egyre több funkcióval bíró kisméretű, nagy tudású készülékek rengeteg veszélyt hordoznak magukban. A legtöbb támadás a különböző kapcsolatokon (WiFi, Bluetooth stb.) és a letöltött programokon keresztül történik. Ennek számos módja ismert, amelyek ismertetése viszont nem tartozik bele a dolgozat témájába, ám fontos biztonságtudatosan kezelni ezeket a készülékeket.

Pszichológiai tényező: Ezek nagyon rohamosan fejlődő eszközök, melyhez az emberek nagy része nem tud alkalmazkodni. Nem ismerik a lehetőségeket és sokszor nem is tartják fontosnak azokat.

Javaslat: Érdemes a bluetooth-t, WiFi-t letiltani és csak a használat idejére engedélyezni. Az utóbbi esetében javasolt beállítani, hogy milyen, általunk engedélyezett hálózathoz csatlakozhat. Ha letöltünk egy alkalmazást célszerű elolvasni a kommenteket, hiszen abban megtudhatjuk, hogy vírusos-e az adott program.

4.2.5.5. WiFi

A mai modern világban a vezeték nélküli internet már a hétköznapiak része. Azonban, mint sok új keletű technikai vívmány még nem jutott el arra a szintre, hogy biztonságosan használják. A nyitott WiFi hálózatok hatalmas veszélyt jelentenek, melyet sokan nem értenek meg. A támadók gond nélkül kihasználják ezt az emberi felelőtlenséget. Erre egy tökéletes példa, amikor egy olyan helyen, ahol tömegesen használják a vezeték nélküli hálózatot (pl.: kávézó) létrehoznak egy nagy jelerősségű csatlakozási pontot a támadók. A gyanútlan áldozat ehhez kapcsolódik, mit sem sejtve arról, hogy eközben megfigyelik a tevékenységét. Ilyen esetekben ellopható a bankszámla szám, jelszavak és bármi más.

Pszichológiai tényező: Mint több másik támadásnál a tudatlanság a fő veszélyforrás ezekben az esetekben.

Javaslat: Amikor csatlakozunk egy nyílt WiFi hálózathoz lehetőség szerint válasszunk olyat, mely biztonságos(abb)nak tűnik. Nem ajánlott az e-bankunk, fontosabb levelező rendszer, egyéb olyan platform használat, melyeket, ha valaki megfigyel komoly kárunk keletkezhet.

Az átláthatóság kedvéért a következő ábra szemlélteti a social engineering támadások csoportosítását:



Humán alapú technikák

- Identitás lopás
- Áltudába bújás
- Céges alkalmazott
- Partner cég alkalmazott
- Új munkatárs
- Magas pozíciójú ember
- Fontos ember
- IT szakember/rendszerkezelő
- Tombstone theft
- Third party authorization
- Hamis bizalomkeltés
- Reverse social engineering
- Valamit valamiért
- Jelszavak kitalálása
 - Alapértelmezett jelszavak
 - Személyre utaló jelszavak
- Rutin munkát végzők segítségkérése
- Bejutás az épületbe
 - Tailgating
 - Késés
 - Hamis ID használata
 - Piggybacking
- Egyéb lehetséges módszerek
 - Shoulder surfing
 - Dumpster diving



IT alapú technikák

- Előzetes információszerzés
- Internet böngészése
- Közösségi portálok figyelése
- Phishing
- Kártékony programok
- Frissítés/javítás felajánlása
- Csatlakozások
- Keylogger
- Baiting
- Trójai programok
- Hálózatok figyelése
- Egyéb IT alapú támadások
 - Telefonbeszélgetés
 - Látszólag belső cím
 - Távoli e-mail hozzáférés
 - Oskotelefonok/PDA-k támadásai
- WiFi

1. ábra: Social engineering technikák csoportosítása¹¹

5. A social engineering pszichológiai vonatkozása

A SE-hez kapcsolódó cselekedetek mindegyikében jelen van valamilyen formában az ember. Ha egy vagyonsvédelmi rendszert megtervezünk, majd kivitelezünk, és működését üzemserűnek találjuk, akkor pontosan behatárolt elvárásaink lehetnek funkcióit illetően, továbbá támadási felületei is tisztázottak a szakemberek számára, és a fennmaradó biztonsági kockázatok is könnyűszerrel elemezhetjük. Viszont e rendszerek felügyeletéhez, és a komplex védelem létesítéséhez elengedhetetlen az emberi közreműködés.

Egy objektumban telepített behatolás jelző rendszer, vagy CCTV rendszer tökéletesen funkcióját veszti az azt felügyelő élőerős őrzés-védelem hiányában. Egy szervezet belső

¹¹ Saját készítésű ábra

biztonsági szabályzata, vagy az információbiztonsági irányelvek szintén csupán papírként vagy digitális adatként funkcionálnak, ha nincsenek dolgozók, akikre vonatkoznak, vagy nem tartják be őket. A hozzáférési jogosultságot szabályozó hierarchia, a vírusirtó programok, és tűzfalak is feleslegessé válnának, ha nem lennének a számítógépes rendszereket megtámadni, azokba behatolni szándékozó emberek, vagy akik ilyen funkciót betöltő kártékony programokat fejlesztenek. Számos szemléletes példát találhatunk még a tény bizonyítására, hogy a komplex vagyonvédelem emberi erőforrás nélkül nem valósulhat meg.

Az ember, és az emberi tudat nem működik olyan kiszámíthatóan, mint egy elektronikus rendszer, vagy egy szoftver. Sokkalta könnyebben befolyásolható, átverhető, meggyőzhető, irányítható célzott szándékunk szerint, amit a komplex biztonság kontextusában vizsgálva komoly kockázatként értékelhetünk. Az emberi tudatból, és személyiségből fakadó befolyásolhatósággal, mint emberi tulajdonsággal foglalkozó tudomány a pszichológia. Ezen belül két szakterület¹², a személyiséglélektan¹³, és a szociálpszichológia¹⁴ vizsgálja a támadások által is jól felhasználható tulajdonságokat, jelenségeket, gyakorlati ténytérületeket. Ezek a pszichológia által jól körülhatárolt ismeretek kiválóan alkalmazhatók a SE gyakorlatban, persze a meglehetősen nagy felkészültség és alkalmazott jártasság elengedhetetlen a témában. Fontos leszögeznünk, hogy ezek a technikák és tézisek korántsem működnek olyan határfokkal, mint például egy gépezet. Ennek oka, hogy minden ember különböző. Ettől eltekintve, az elmúlt másfél évszázadban munkálkodó kutató pszichológusoknak köszönhetően, meglehetősen jól elkülöníthetők, és meghatározhatók ezek a technikák.

5.1. Gondolkodási módok

A gondolkodási módok meghatározására¹⁵ több tudományos lehetőség is rendelkezésünkre áll. Ha SE szempontból vizsgáljuk a kérdést, akkor célszerű, ha a környezetünkben érkező hatások, és üzenetek feldolgozására jellemzően használt érzékszervünk szerinti besorolást használjuk. A lényege, hogy a kommunikáció során (ami

¹² Estefánné Varga Magdolna et al: Pszichológia elméleti alapok

¹³ Szamosközi István : Személyiséglélektan

¹⁴ Sándor Judit Szociálpszichológia

¹⁵ Christopher Hadnagy: Social Engineering; 103-109. o.

lehet verbális, és nonverbális egyaránt) a résztvevők az információt kognitívan értelmezik. Ezen felül némelyik üzenet tartalma különleges pszichológiai hatást képes kiváltani az vevő félből, az adott üzenet feldolgozása is dinamikusabb, egyszerűbb. Ez a jelenség annak köszönhető, hogy minden ember az érzékei szintjén fejezi ki magát, és fogadja be az információt, viszont valamelyik érzéke minden embernek erősebb hatást fejt ki a tudatalattira. Ezek a gondolkodási módok a következők:

- Látás alapján, vizuálisan gondolkodók: az emberek nagytöbbsége ebbe a csoportba tartozik. Könnyebben képesek feldolgozni a könnyen vizualizálható információt, ezen a gondolkodási síkon sokkalta egyszerűbb kommunikálni egy ilyen alannal. A könnyebb információ cserén kívül számos technika alkalmazásánál felhasználható ez az ismeret. Jellemzően az üzletkötők, kereskedők is sűrűn élnek ezzel az eszközzel. Felismerni ezt a típust az általa használt kifejezésekből lehet, mivel egyértelműen valamilyen vizuális tartalomra utalnak.
- Hallás alapján gondolkodók: ebbe a csoportba tartozó emberek a hallásuk, és a hangok alapján sokkal gyorsabban képesek tanulni, és sokkal jobban emlékeznek egy eseményre, cselekményre a hangja alapján. Az ilyen típusú emberekben keltett hatást nagyban befolyásolja a beszéd hangereje, tónusa, hanglejtése, gyorsasága a beszéd távolsága. Ugyanezek az akusztikai tulajdonságok jellemzők a partner beszédére is, innen jól beazonosíthatók gondolkodásuk módja szerint.
- Tapintás, érzelmek alapján gondolkodók: az ide tartozó emberek legintenzívebb emlékei, élményei, tudatos reflexei ahhoz kötődnek, hogy a bekövetkezésük alkalmával milyen fizikális, és mentális érzést és ahhoz párosult érzelmet váltanak ki. Erre a típusra hatást gyakorló kommunikációs körülmények az intenzitás, a helyszín, a mintázat, a hőmérséklet, és a súly. A megfelelő módon a legkönnyebben lenyűgözhető csoportba tartoznak ezek az emberek. Ezt a gondolkodási módot a híres Nobel-díjas orosz pszichológus, Ivan Petrovich Pavlov bizonyította¹⁶ a kutyákon végzett kísérleteivel. A kísérlettel azt bizonyította a 20. század elején, hogy a kognitív tudatunk képes a környezet változáshoz tanult, és tudatos reflexet kötni.

¹⁶ Ivan Petrovics Pavlov válogatott művei, 256. oldal , Klasszikus kondicionálás

5.2. *Mimika és apró árulkodó gesztusok (Microexpressions)*

A mimika, az árulkodó arckifejezések, és a sokatmondó gesztusok területén egészen 1872-ig visszatekint a kutatástörténet, mivel ekkor jelent meg Charles Darwin könyve, ami az emberek és az állatok kifejezéseit dolgozta fel az érzelmeik függvényében¹⁷. Majdnem száz évvel Darwin művét¹⁸ követően a témában szintén úttörő kutató pszichológus, Dr. Paul Ekman számos kutatást és kísérletet végzett az arckifejezések, és mikrokesztusok területén, ami következtében tizenegy könyvön keresztül pontosan meghatározta az emberi arckifejezésekhez kötődő érzelmi hátteret. Dr. Ekman 1972-ben azonosította a tudományosan elfogadott hét különböző általános, vagy biológiailag elkülöníthető érzelmet¹⁹:

- Harag
- Undor
- Félelem
- Öröm
- Szomorúság
- Meglepődés
- Lenézés

Ezeket az érzelmeket, és a velük járó biológiai változásokat pontosan meghatározta Dr. Ekman. Jellemző ismertető jegyeit is definiálta, melyek a felismerésüket, és az abból fakadó következtetések levonását segíti elő, és lehetővé teszi egyértelműen a valós és hamis kifejezések megkülönböztetését. Tény, hogy csupán rengeteg gyakorlással lehet eljutni készség szintű felismerésükre, de ez a készség birtokában hatásos eszközként funkcionál a social engineerek kezében. Az 1970-es években főleg Nyugat-Európában a nyomozók és rendvédelmi dolgozók komoly, több éves képzést kaptak ezen ismeretek elsajátítása céljából.

A SE szempontjából a témához kötődő néhány árulkodó jelenség sokat segíthet a valódi, vagy hamis információ kiszűrésében egy kommunikációs szituáció során:

¹⁷ Ekman, P. & Friesen, W. V. UNMASKING THE FACE: A GUIDE TO RECOGNIZING EMOTIONS FROM FACIAL CLUES,

¹⁸ Charles Darwin: The Expression of the Emotion in Man and Animals

¹⁹ Christopher Hadnagy: Social Engineering; 109-135. o.

- **Ellentmondás:** sokszor tapasztalhatjuk, hogy a kommunikációs partner hamis üzenetek közvetítésénél az üzenet tartalmának ellentmondó arckifejezést, gesztusokat használ. Ez jellemzően feszültséggel és izgalommal párosul, nagy pontossággal azonosítható.
- **Tétovázó, hezitáló magatartás:** a hétköznapi életben sokszor tapasztalhatunk olyat, hogy egy válasz előtt az alany hezitál, majd gyorsan érkezik a felelet. Ilyen esetekben, ha a mikrogesztusok ellentmondásra vallanak, nagy a valószínűsége, hogy a válasz nem igaz.
- **Viselkedésmód változás:** legtöbbször párosul a hezitálással, a további kommunikáció késleltetése a cél. Ez idő alatt a jelenséget prezentáló alany a tényeket, és arra épülő lehetséges válaszait gondolja végig. Meglehetősen tipikus jelenség.
- **Kéz gesztusok:** nem minden emberre jellemző, de akire igen, arról rengeteg információt kaphatunk ezáltal. Amit fontos megfigyelnünk, hogy a kéz gesztusok és az arckifejezések milyen összhangban vannak. Ha megszűnik a harmónia a kettő között, hamar leszűrhetjük a tanulságot, miszerint az állítása nem valós.

5.3. ***Összhang-, szimpátiateremtés (Building rapport)***

Ennek a technikának²⁰ az alap elgondolása, hogy ha az adó-vevő felek között a szimpátia, és összhang uralkodik, akkor sokkal segítőkészebbek, nyíltabbak egymás iránt. Ezt a szimpátiát olykor hónapokba telik megteremteni, viszont SE kontextusban ez az intervallum csak korlátozott mértékben áll rendelkezésére a cselekvőnek egy beszédshituáció során. Az elsődleges célja egy social engineernek, hogy ezt az állapotot minél rövidebb idő alatt megteremtse, és kihasználja célja elérése érdekében. Szoros összefüggésben van ez a technika a személyiség felvétellel (4.4. alfejezet), a gyakorlatban egymásra épülnek. A sikere az összhangteremtésnek néhány evidensnek tűnő, mégis elengedhetetlen részleten múlik. Néhány ökölszabály a sikeres szimpátiateremtéshez²¹:

- Legyünk természetesekek a kapcsolatteremtés, kommunikáció kezdeményezés során!

²⁰ Dr. William Glasser: Choice Theory: A New Psychology of Personal Freedom

²¹ Christopher Hadnagy: Social Engineering, 162-172. o

- Figyeljünk a megjelenésünkre!
- Legyünk lelkes hallgatóság!
- Ne vigyük túlzásba az emberekre gyakorolt érzelmi hatáskeltést!
- Tereljük el magunkról a beszélgetést, érdeklődjünk a beszédpartnered iránt!
- Mindig tartsuk szem előtt, hogy a sikeres összhangteremtés kulcsa az empátia!
- Legyünk megfelelően felkészültek a beszédtema kapcsán, a lexikális tudásunk kulcsfontosságú lehet!
- Előre gondoljuk át a lehetséges kérdéseinket, legyünk kíváncsi természetűek!
- Találjuk meg a módot, hogy kiderítsük a beszédpartnerünk fő érzelmi szükségleteit!

Ezeknek a közhelyesnek tűnő szabályszerűségeknek óriási jelentőségük van a gyakorlatban. Nagyrészüik létjogosultsága könnyen belátható és értelmezhető.

A 9)-es pontot szükséges részletesen elemeznünk, mivel korántsem olyan evidens, mint amilyennek tűnik. Dr. William Glasser pszichológus azonosította Choice Theory című könyvében az emberek alapvető pszichológiai szükségleteit, és ezeket négy csoportra bontotta:

- Hovatartozás/emberi kapcsolatok/szerelem
- Erő/jelentőség/szakértelem
- Szabadság/felelősség
- Szórakozás/tanulás

Majdnem minden ember számára a négy csoport egyike valamekkora előnyt élvez a többivel szemben, Dr. Glasser kutatásai szerint az emberek 0.1%-ánál van tökéletes harmónia a szükségletek közt. Ha egy social engineer a négy csoportból képes megtalálni a legfontosabbat, és az alany gondolkodási módszerén keresztül (4.1. alfejezet) azonosulni, akkor nagy eséllyel sikeresen meg van teremtvé az összhang.

A szimpátiateremtésnek van továbbá három fontos eszköze, amelyek a beszédpartnerünk tudatalattijára képesek hatni. Ezek meglehetősen egyszerűek a gyakorlatban, mégis kiemelkedő jelentőséggel bírnak:

- A légzésszám összehangolása a beszédpartnerével.

- A beszédstílus és hangtónus sémájához való igazodás.
- A partner testbeszéde, és sajátunk összehangolása.

5.4. Személyiség felvétel (Pretexting)

A személyiség felvétel²², mint sokszor használt SE technika lényege, hogy a támadó mind információ csere, mind szituáció szempontjából előre eltervezett magatartás szerint cselekszik hasonlóképp, mint egy színész. A színészettel szemben viszont nem egy előre megtanult szöveget ad elő, sokkal inkább egy bizonyos szerepben improvizál. Jellemző még az adott környezethez mérten minél hitelesebb kitalált keretszituáció, vagy történet, amivel valamilyen reakciót szándékozunk kiváltani. Fontos megállapítanunk, hogy a személyiség felvételt professzionális módon cselekedni meglehetősen összetett, de nem minden esetben szükséges, hogy minden részletében tökéletes legyen a sikeres támadáshoz. Ettől eltekintve egy mindenre felkészült támadónak mélyen, gyakorlati szinten otthon kell lennie a pszichológiában. A gondolkodási módokban, az apró arckifejezések, és gesztusok területén, a szimpátiateremtésben, és a következő alfejezetekben tisztázandó kiderítési/kérdezési technikák gyakorlatában, továbbá a befolyásolási technikák is hasznosnak bizonyulnak a profi social engineerek számára (4.1. ; 4.2. ; 4.3. ; 4.5. ; 4.6. *alfejezetek*).

A tervezési lépcsőfokai és alapelvei a személyiség felvételnek a következők²³:

- Minél több energiát fektetünk a felkészülésbe és tervezésbe, annál nagyobb az esély a sikeres támadásra. Itt fontos szerepük van az információgyűjtési technikáknak a megfelelő SE technika alkalmazásához (3. fejezet).
- Fontos a személyes érdeklődésünk a beszédpartnerünk, áldozatunk iránt, mivel meglehetősen növeli az esélyünket a cél elérésében. Ez egy evidens alapelvnek tűnik, de ha mégsem alkalmazza az ember, könnyen sikertelen támadáshoz, esetleg lebukáshoz vezethet. Annál könnyebben semmi sem rombolja le az összhangot, mint ha valaki érdektelen hallgatóság.
- Szerezzünk információt, és tájékozódjunk a munkakörnyezetben használatos szavak, szakmai szleng, speciális kifejezések kapcsán. Felettébb meggyőző a SE támadások áldozatai szempontjából, ha egy támadó az adott környezetben

²² Audri Lanford, Jim Lanford: What's New With Identity Theft? Pretexting.

²³ Christopher Hadnagy: Social Engineering. 77-100 o.

használatos kifejezéseket használ a kommunikáció során. Dolgozói viszonyt feltételeznek, és az összhangteremtést elősegíti.

- A telefon használata nagyban elősegíti a támadás kimenetelét, és nem igényel nagy erőfeszítést. A telefonos támadásoknál sokban leegyszerűsödik a személyiség felvétel, kisebb a hiba lehetőség, és komoly hatást lehet elérni a segítségével, akár önállóan, akár valamilyen komplex támadás részeként is alkalmazzuk.
- Minél egyszerűbb a felvett személyiségünk, annál jobb esélyünk vannak a sikerre. Nem szabad túlságosan bonyolult személyiséget magunkra erőltetni, vagy bonyolult keretszituációt kitalálni, mert annál nagyobb a hiba, esetleg sikertelen támadás esélye.
- Előfordul, hogy egy támadás során olyan szituációval találkozunk, amire nem készültünk fel előre. Ilyenkor szükséges spontán cselekednünk, és improvizálnunk, ami sok gyakorlatot, és színészi képességeket is igényelhet. Megesik, hogy nem marad más ésszerű megoldás.
- A felkészülés során gondoskodjunk az alapvető tervünk logikai összefüggéseiről, egymásra épülő részleteiről, mindezt a célalanyra levetítve.

5.5. *Kiderítési/kérdezési technikák (Elicitation)*

Ezek a technikák magában foglalják a kérdés típusokat, és a körülményeket is melyben érdemes őket használni. Ezeken felül még azt is, hogy milyen gondolkodásmódú embereknél (4.1. alfejezet), és milyen felvett személyiséggel (4.4. alfejezet) érdemes érdeklődni a kívánt információ iránt. Összetettségét tekintve itt is sok gyakorlás, és felkészülés szükséges a professzionális végrehajtáshoz.

A sikeresen végrehajtott kikérdezések sokszor egyszerű pszichológiai eszközök segítségével valósulnak meg²⁴. A nehézséget mégis a hatásos eszköz kiválasztása jelenti. Ezekre az eszközökre jó példa, ha a célalany egóját növeljük, és így férközünk közel hozzá érzelmileg. Az efféle információszerzési technika sokszor több időt vesz igénybe, mint a legtöbb technika, és a környezet is specifikus, ahol ezt sikeresen alkalmazni lehet.

²⁴ Christopher Hadnagy Social Engineering: 55-76 o.

A célalannal közös érdeklődés mutatása is egy hatásos technika, viszont ebben az esetben konkrét információink kell, hogy legyenek az áldozatunkról, továbbá meglehetősen sok felkészülést igényel, ha esetleg nem vagyunk otthon a témában.

Egy előre megfontolt hamis állítás tétele, ha már kommunikálunk az áldozattal sokszor kiváltja a kívánt hatást, ami az állításunk tényszerű cáfolataként lép fel, ami magával hozza a keresett információt.

Megszokott, mondhatni klasszikus helyszínei ezeknek a támadásoknak a bárók, vagy vendéglátó egységek, ahol szituáció függően az alkohol hatását is ki érdemes használni támadásunk sikere érdekében.

Fontos részét képezik a kérdezési technikáknak a kérdéstípusok:

- Nyitott végű kérdések: az olyan kérdéseket értjük ez alatt, amire a kommunikációs partnernek, ha udvarias, akkor több választ kell adnia, mint az igen, vagy a nem. Érdemes használni a beszédssituáció kezdetekor, vagy ha a folyamat alatt megakadna a beszélgetés menete.
- Zárt végű kérdések: akkor használjuk ezt a kérdéstípust, ha valami konkrét, információink által pontosan körülhatárolt dologra szeretnénk rákérdezni, és célunk, hogy pontos információinkkal meggyőzzük a partnerünket arról, hogy mi jogosultak vagyunk tudni a választ.
- Irányító kérdések: ez a kérdéstípus eszközül szolgál arra, hogy kiderítsük vajon a közös összhangot és szimpátiát milyen mértékben sikerült megteremtenünk. Továbbá Megadjuk a lehetőséget a partnerünknek, hogy a saját élményeiről meséljen. Tulajdonképpen a zárt, és a nyílt végű kérdések kombinációja ez a típus.
- Feltételezett kérdések: a lényege ennek a kérdéstípusnak, hogy a célalannak olyan kérdést teszünk fel, aminek feltétele némi háttér információ, viszont ez nem áll rendelkezésünkre, csupán sejtjük, vagy feltételezzük annak valóságát.

5.6. Befolyásolási taktikák (*Influence tactics*)

A befolyásolás eszköze²⁵ egy hasznos, és meglehetősen erős fegyver a social engineerek kezében, ha megfelelő szinten képesek alkalmazni. Számos vonatkozása van

²⁵ Cialdini, Robert: A befolyásolás lélektana

további területeken is, például a politikában, a médiában, a csalók és szélhámosok körében sokszor alkalmazott módszer. Elég tág ezen taktikák és eszközök köre, sokszor a taktikát felhasználó fantáziáján múlik csak a különböző lehetőségek és változatok száma²⁶.

A befolyásolási taktikák közül néhány²⁷:

- Apró szívességekért cserébe elvárás: lényege ennek a taktikának, hogy a támadó, ha a megfelelő körülmények adóttak, szándékosan valami apró szívességet tesz áldozatának. Ez lehet pusztán egy udvarias gesztus, de sok esetben az általa kreált és az áldozatára kiható problémára nyújtott megoldás, esetleg az adott szituációban való észrevétel, amely az áldozat javát szolgálja. Itt is sokszor improvizál egy social engineer, de ennél a taktikánál sokkal több lehetősége nyílik az előre tervezésre. Az emberi természet velejárója, hogy ilyen esetekben készséggel viszonyozza a szívességet, és ezt a jelenséget használja ki a támadó a legkülönbözőbb módokon az információszerzésre. Ezt a jelenséget vizsgálta, és kutatta Alvin Gouldner, a st. louis-i Washingtoni Egyetem szociológia professzora. A szociálpszichológia kutatási módszereivel modellezte, és részletes tanulmányt írt erről a befolyásolási technikáról.
- Lekötelezés: ez a taktika több szempontból kötődik az 1) pontban tisztázott módszerre, viszont van némi különbség a kettő között. A támadó célja, hogy áldozatában valamilyen téren adósság érzetet keltsen. Ezek célszerűen társadalmi, törvényszerű, vagy erkölcsi kívánalmak, kötelességek, megegyezések, ígérek, melyek létrejötte a támadó fő indíttatása. Steve Bressert amerikai pszichológus, a befolyásolás pszichológiájának szakértője végzett felmérést a taktika létjogosultságáról. Az eredményei magáért beszélnek: levélben kérelmeket küldött az amerikai leszázalékolt veteránok szervezete tagjainak, melyben arra kérte a megszólítottat, hogy küldjön vissza neki érdemleges további postacímeket valamilyen hamis ürügy kapcsán. A megkeresettek 18%-a küldött vissza további címeket. Ezt a felmérést úgy is megvalósította, hogy az elküldött levélben ígért a beérkezett címekért cserébe, postafordultával valami kis ajándékot. Ennek hatására kis híján a duplája, 35%-uk küldött vissza postacímeket.

²⁶Christopher Hadnagy: Social Engineering 187-215.o.

²⁷ Steve Bressert: Persuasion and How to Influence Others

- Engedmény tétele: ezt a taktikát előszeretettel használják számos területen, például a reklám, a marketing, és a kereskedelem gyakorlatában. Alaptézise, hogy az emberek tudat alatti reflexből hajlandóak inkább azt az ajánlatot elfogadni, azt az alternatívát választani, amelyekben van valamiféle kedvezmény, engedmény számukra az eredeti opcióhoz képest. Például sokszor meg sem vásárolják az adott terméket ezen feltétel nélkül. Vannak persze társadalmi és kulturális eltérések világszerte ebben a tekintetben, de általánosítva azt mondhatjuk, hogy törvényszerű. A SE vonatkozásában ügyelni kell arra, hogy egy befolyásolási szituációban a szívesség tétele, vagy a lekötelezés mindig kedvező, és csábító legyen az áldozat számára.

- Félelem keltése, megfélemlítés: szintén kedvelt taktika a kereskedelemben, és reklámok területén, mivel meglehetősen hatásos. A félelem, vagy aggály egy nagyon erős érzelem, ezen keresztül könnyen befolyásolható az emberek többsége. Jellemző szituációk ebben a technikában a limitált darabszámmal való félelem keltése, és a titkolt, esetleg fals információ megosztása, és ezzel nagy jelentőség, félelem, aggodó légkör teremtése.

- Hatalom, felettes viszony kihasználása: ebben a befolyásolási taktikában kiemelkedően fontos a felkészültség, és a gyakorlat, de legfőképp a hitelesség. Ha egy hatalommal rendelkező ember a felvett személyiségünk (4.4. alfejezet), akkor minden részletnek a helyén kell, hogy legyen, különben pillanatok alatt, egy rossz lépéssel hitelét vesztheti az előadott személyiségünk és biztos lebukással számolhatunk. Mind a megjelenés, vagy beszédstílus, gesztusok az általunk megszemélyesített hatalommal bíró személyt kell, hogy tükrözze. Fontos tisztázni, hogy az adott környezetben fellelhető sztereotípiák és kulturális szokások, lokális szokások mind nagyon számottevők egy efféle támadás esetén. Több mintát is megkülönböztethetünk ebben a technikában:

- Hivatalos személy megszemélyesítése, például valamilyen rendvédelmi dolgozót.
- Szervezetén belüli vezetőt, feletttest személyesítünk meg.
- Egy társadalmi csoportnak egy hatalommal bíró emberét személyesítjük meg.

- Elkötelezettség és következetesség: lényege a taktikának, hogy a célalannal való beszélgetés folyamán olyan kérdésekkel faggatjuk, amivel elkötelezi magát egy álláspont mellett. Persze ezeket a kérdéseket ügyesen el kell rejtetni a mondandóban, mert a túlzott rámenősség eredménytelenséghez vezet. Ha az elkötelezettsége már megvan az áldozatnak, akkor állításokkal és utalásokkal szükséges irányítani a kívánt cél felé, ami SE szempontból az információszerzés. Robert Cialdini az Arizona State University professzora ismerte fel ennek a technikának, és a befolyásolás „művészetének” törvényszerűségeit, melyek nélkülözhetetlenek a társas interakciók működéséhez, és a SE tudomány fejlődéséhez egyaránt.

6. A social engineering, mint a vagyonvédelem lehetséges támadási felülete

Az előző fejezetek során tisztáztuk, hogy a két tudomány közti párhuzam, az emberi tényezőben rejlik. Ezt belátni nem nehéz, viszont konkrétumok szintjén meglehetősen sok oldala van ennek a tézisnek. A vagyonvédelemnek két fő részét, az őrzés-védelmet, és az adat-és információ védelmet érinti a SE, mint újkeletű biztonsági kihívás.

A fő célja ennek a fejezetnek, hogy a teljesség igénye nélkül bemutassa és szemléltesse néhány példán keresztül a SE viszonylatában a biztonságtechnika e két területének támadási felületeit. Mindezeket nem csak szigorúan SE technikák szempontjából, hanem arra szeretnénk rávilágítani, hogy milyen szoros összefüggésben van a biztonságtechnika és a SE a gyakorlatban, mennyire fontos egy social engineernek naprakésznek lennie a modern biztonsági megoldások területén is.

6.1. *Az őrzés-védelem támadási felületei a social engineering tekintetében*

Az őrzés-védelmet²⁸, mint a vagyonvédelem egyik szakterületét további három részre szükséges bontani: mechanikai védelemre, elektronikus rendszerekre, és élőerős őrzés-védelemre. Ezeknek a részeknek mind megvannak a sajátos gyenge pontjaik, mivel tökéletes védelem, mint olyan nem létezik. Ezek egy része hardver, másik része szoftver alapú, melyek jellemzően a nem megfelelő telepítésből, kivitelezésből, konfigurációból, vagy technológiából

²⁸ Szabó Lajos: A komplex biztonsági rendszer, előadás

kifolyólag, némely esetben a kulcsfontosságú információk nem megfelelő kezeléséből adódnak.

Egy social engineernek meglehetősen fontos minél több információval rendelkeznie az adott objektumról, különös tekintettel a védelme felől. Egy SE támadást a komoly technikai és terv szintű felkészültség jellemez, melyben kiemelten fontos tudnunk, mivel is állunk szemben. Különös hangsúlyt kell fektetnünk az információszerzésre, mivel komoly helyszínismeret nélkül csupán a sötétben tapogatózunk. Egy sikeresen végrehajtott SE támadásnak kulcsfontosságú összetevője az őrzés-védelmi szempontú felkészültség, és célzott technikai ismeret. A következő alfejezetekben a teljesség igénye nélkül feltárja a dolgozat a realitás talaján maradván az őrzés-védelmi rendszerek, s azokat alkotó eszközök támadási felületeit és jellemző szabotázsai módszereit.

6.1.1. A mechanikai védelem támadási felületei

A mechanikai védelmi megoldások a komplex vagyónvédelmi rendszerek szerves részét képezik. Ezek ellen történő támadások alapvetően kétfélek lehetnek: durva behatolásos, és finom behatolásos módszerek. A durva behatolásnál a konkrét cselekvés roncsolásos módszerekkel történik. Ennek komoly eszközigénye van, és további hátránya, hogy a cselekvést követően a nyomok feltűnőek és egyértelműen tükrözik a behatolást. Ez sok esetben előnytelen, mivel fokozottan felhívja a figyelmet, ellehetetleníti a további támadást.

A finom behatolásnál elengedhetetlen a helyszínismeret, mivel a védelmet képviselő technikára célzottan szükséges felkészülnie a támadónak. Fontos cél, hogy a behatolást nyom nélkül, vagy csak részletes és alapos nyomozással feltárható nyomokkal hajtsa végre a behatoló. Efféle jellemző mechanikai védelmi eszközök az ajtóknak, kapuknak használatos zárai, hengerzárberetéi. Persze itt nincs vége azon eszközök és megoldások listájának, amelyekkel egy social engineer találkozhat támadás során, viszont a technikai felkészülés a zárai finom nyitása tekintetében meghatározó lehet.

Erre egy bevált és elterjedt eljárás a lockpicking.²⁹ Számos alkalommal és a legkülönbözőbb helyszíneken tapasztalhatjuk, hogy olcsó, és nem megfelelő biztonsági szintet

²⁹ <http://lockpick.blog.hu/> zárszerkezetek finomnyitási módszerei 3. és 4. fejezet

képviselő zárszerkezeteket alkalmaznak. A lockpicking az említett hengerzárbetétek, lakatok, s egyéb mechanikai védelmi eszközök kulcs nélküli, roncsolásmentes nyitását jelenti. Elég gyakorlatigényes eljárás, melyet csupán készség szinten elsajátítva lehet hatásosan alkalmazni, ahol a zár kinyitásához felhasznált idő az egyik legfontosabb tényező, ami néhány percben, de sokszor egy percen belül maximalizálódik. Habár eszközigénye specifikus, a szükséges eszközök (pick-ek és forgatók) akármelyik zsebben könnyen elérnek. A lockpicking eljárás nem csak a SE viszonylatában alkalmazott, sokan hobbyként űzik, a betörők számára is kedvelt módszer, a biztonságtechnikai szakemberek is tájékozottak ezen a területen, a bűnügyi szakértők sem kivételek ez alól, és még sok vonatkozásban találkozhatunk a témával.

Az ajtók zármechanizmusai nem csak kulccsal nyithatók, számos más megoldás is lehetséges. Erre példa a mágneszárok, amelyeknél tulajdonképpen egy relé felel a nyitott, és zárt állapotért. Ennek szabotálása egy méretre hajtogatott papírlap segítségével kivitelezhető. A megfelelő méretű papírt betömődve a zárnyelv horonyba a benne lévő kapcsoló zárt állásban marad. Ezután egy vékony merev tárggyal könnyűszerrel betolhatjuk a zárnyelvet, ezzel nyitva az ajtót.

Minden zárszerkezetnek megvan a gyenge pontja, melynek ismerete egy SE támadás alkalmával komoly előnyt jelenthet. Számos esetben előfordul, hogy a zárnyelvhez egy hosszú hegyes szerszámmal (például egy késpenge) hozzáférhetünk, és egy egyszerű és határozott mozdulattal a zárnyelvet betolva nyitjuk is ki az ajtót.

A modern vagyonvédelmi megoldások közé tartoznak az olyan zárszerkezetek, melyek nem kulccsal, hanem más információ tartalmú eszközzel, mint például RFID, vagy biometrikus érzékelővel vannak ellátva. Ezek szabotálása történhet fokozottan nagy és költséges felkészüléssel, például RFID scannerrel, és a különböző biometrikus érzékelők megkerülési módszereinek kutatásával, de sokkalta egyszerűbb, ha a SE taktikákat használja a támadó. Célorientáltabb alternatívát kínálnak az adott ajtón való bejutásra az emberi tényezőt (3. és 4. fejezetek) kihasználó módszerek, mint a hosszas felkészülést igénylő hardvert és szoftvert egyaránt megkerülő bonyolult eljárások.

6.1.2. Az elektronikus rendszerek támadási felületei

Az elektronikus vagyonvédelmi rendszerek³⁰ magukban foglalják a CCTV, behatolás-jelző, beléptető, járőrkövető, tűzjelző rendszereket. Mindezek tervezési, kivitelezési hibáik, gyenge pontjaik specifikusak lehetnek a technológiából eredően. Mind a technológiából, mind a SE technikákból fakadó lehetséges támadási felületek szoros összefüggésben vannak egymással, mivel a rendszerfelügyeleti, és kivitelezési munkálatokat, feladatokat emberek látják el.

A zárt láncú videó megfigyelő rendszereknél (CCTV) számos filmbe illő eljárás a valóságban is alkalmazható, azonban meg kell különböztetnünk a SE behatolás és a klasszikus betörés közti módszereket, habár sok esetben átfedés van köztük. Mindkét esetben nélkülözhetetlen a helyszínismeret és a felkészültség. Egy betörés esetében a kamerarendszerre való tekintettel fontos a személyes inkognitó. Ennek érdekében az orvosi gyakorlatban használatos latex kesztyű, az arc elmaszkírozása, vagy elfedése, a jelzés nélküli öltözet és a lehetőség adta átlagos testmagasság alapvetőnek bizonyul a támadó szempontjából. Továbbá egy profi betörő törekszik a dezinformatív kivitelezésre támadása során, mely eszközéül szolgálhat akár az őrszemélyzet egyenruhájához hasonló öltözet viselete is. A támadás szempontjából fontos helyszíneken a kamerák üzemképtelenné tétele történhet több módon is. Egyszerűen az optika festékszóróval történő lefújása célravezető, ámbar feltűnő. Körültekintő megfigyelés, és előkészület következtében egy megfelelő látószögben készített fénykép optika elé ragasztása az optimális környezeti hatások meglétével szintén használható taktikának bizonyul. A gyakorlatiasabb taktikák közé tartozik az aktuális kamera tápfeszültség ellátásának szabotálása. Komoly kivitelezési hibaként könyvelhetjük el, hogy némely helyen a tápellátás nincs szünetmentesítve, vagy könnyedén hozzáférhető a bekötési helye.

A fentiekben említett célzottan a CCTV rendszerek ellen történő szabotálási és támadási módszerek a SE támadások tekintetében nem reálisak a feltételezett szituációkat figyelembe véve. Habár alap elgondolások szintjén mindenképp számottevőek, de egy social engineernek fontosabb a figyelmét a kommunikációra és csupán részben a kamerákra

³⁰ Dr. Lukács György: Új vagyonvédelmi nagykönyv

fordítania. Fontos figyelmet fordítanunk arra, hogy ne nézzünk teljes tekintetünkkel a kamera objektívébe, mivel a rendszerügyeleten a kamerákat figyelő vagyondőr számára ez bizonyul a legfeltűnőbbnek, és a felvételeken is gyanút ébreszthet. Egy kamera észlelését követően a feltűnés mentes szemrevételezése is meghatározó információként szolgálhat egy behatolás során. Egy szakértő szem számára egy szemrevételezett kamera közelítő műszaki paraméterekkel szolgálhat, melyek hasznosak lehetnek egyes cselekvések szempontjából, erre példa a becsült fókusz távolság. Továbbiakban általánosnak tekinthetjük a szerverszobák, és egyéb vagyondvédelmi rendszer központok mind mechanikai, mind elektronikai védelmét, de ha mégis könnyen be tud jutni a támadó ezen helyiségekbe, akkor konkrét anyagi kár okozása nélkül könnyedén sabotálni tudja a kamerarendszert, s egyéb rendszereket különösebb feltűnés nélkül. Erre példa, ha egy IP kamerarendszer esetén a switch-ből kihúzzuk az egyik szegmens hálózati plug csatlakozóját, és átdugjuk az egyik nem használt bemeneti egységbe.

Egy behatolás-jelző rendszer sabotálási módszerei között is számos alternatíva fedezhető fel. Az érzékelők szintjén támadva azt sok esetben elvi szinten egyszerű a dolga a támadónak. A PIR típusú érzékelőket pusztán egy papírlappal kit tudjuk takarni feltéve, ha nincs az eszközben kitakarás védelem. Az ilyen védelemmel ellátott érzékelőket, úgynevezett félaktív infra érzékelőket ugyanezzel a módszerrel tudjuk sabotálni, csupán különös gondot kell fordítani arra, hogy az a papírlap a fresnel-lencsét takarja csupán, az aktív részt egyáltalán ne, vagy csak a papír élével látszódjon számára. A kombinált érzékelők esetében szintén meglehetősen egyszerű a dolgunk, mivel a legtöbb esetben a kétféle különböző elven működő érzékelő egy eszközbe integrálva „és” kapcsolatban vannak. Ennek következtében, ha a PIR részét kitakarjuk, máris sabotáltuk az érzékelőt. Ezek a módszerek kivitelezhetősége nagyban függ a helyszíni adottságoktól, a telepítés hiányosságaitól, és az alapvető tervezés során elkövetett hibáktól, figyelmetlenségektől, amik meglehetősen jellemzőek. A biztosabb és kézenfekvőbb támadási módszer ezen rendszerek ellen, ha megszerezzük a jelzőközponthoz tartozó telepítői, vagy mesterkódot, esetenként a felhasználói kód is rendelkezik a megfelelő jogosultsággal. Mindenképp az adott jelzőközpont kapcsán fontos a felkészültség, és alkalmazott műszaki ismeret egy efféle támadás kivitelezése során. Ha valamelyik megfelelő jogosultsággal rendelkező kód a birtokunkban van, akkor néhány perc alatt kezelőegységtől függően a kívánt érzékelőket bypass üzemmódba állíthatjuk. Ehhez persze például SE technikákkal meg szükséges szereznünk a kívánt kódot, amiért az előerős

őrzés-védelem állományához, azon belül is a rendszerügyeletes vagyonőrnél érdemes próbálkozni.

A beléptető rendszerek támadási felületei főként a SE technikákban rejlik, habár akad néhány drága eszközigenyű technológiából fakadó lehetőség is a kijátszásra. A passzív RFID alapon működő rendszerek beléptető eszközei, jellemzően kártyák, másolhatók RFID scanner segítségével, de ez felettébb költséges és körülményes. A biometrikus elven működő beléptetés is esetenként átverhető, de talán még ez bizonyul a szabotázs szinten legmegbízhatóbb technológiának. Sokszor találkozhatunk azzal a jellemző konfigurációs hibával, hogy a be- és kilépésre jogosult személynek lehetősége nyílik egymást követően korlátlan engedélyezett belépésre, és kilépésre egyaránt. Azaz egy azonosító eszközzel több személy is be-, vagy kijuthat az objektumból, technikai akadály nélkül. Ez a jelenség kiváló eszközül szolgál néhány SE technikának (3.1.6. alfejezet). A passzív RFID alapú, közismertebb nevén proximity kártyás beléptető rendszereknél kézenfekvő bejutási taktika lehet a saját kártya otthon felejtésének, elvesztésének szimulálása. Ennek következtében esetenként lehetséges az ideiglenes be- és kiléptetés az őrszemélyzet segítségével. Erre szolgál biztonsági megoldásként a vendégkártya használata. Sok esetben erre az eshetőségre fel vannak készítve, mert arra az időre az eredeti kártya jogosultságát megszüntetik.

A mechanikai védelmi megoldásoknál és az elektronikus rendszereknél az esetenként eltérő támadási, szabotálsi lehetőségek megállapítása, alkalmazás tekintetében egyaránt kulcsfontossággal bír a technológia működésének ismerete. Ha tudjuk, hogy is működik egy szerkezet, vagy egy rendszer, akkor gyors és kézenfekvő megoldásokat tudunk találni annak kijátszására, komplex tervet alkotni a szabotálásra.

6.1.3. Az élőerős őrzés-védelem támadási felületei

Az élőerős őrzés-védelem³¹ támadási lehetőségeit nagyrészt a SE technikákban, és a pszichológia alkalmazásában kereshetjük. Ennél a résznél is komoly szerepe van az információgyűjtésnek. A vagyonőrök szolgálati szabályzatát, a belső biztonsági szabályzatot és esetleg a speciális szolgálati feladatokat ismerve teljes képet kaphatunk a biztonsági őrség felépítéséről, működéséről. Beleláthatunk az élőerős vagyonvédelmi feladatok, folyamatok

³¹ Őrzés-védelem, Jegyzet a biztonságtechnikai mérnök hallgatók részére

dinamikájában, amely óriási előnyt jelenthet a támadó számára tervezési és kivitelezési szempontból egyaránt.

Fokozottan érvényesíteni és használni lehet a 3. és 4. fejezetekben tisztázott technikákat, és pszichológiai eszközöket, mivel a vagyonvédelmi feladatokat nem szerkezetek, hanem emberek látják el. Kiemelkedően fontosak a befolyásolási és kérdezési technikák, továbbá a belső szak szleng, kifejezések használata, továbbá a vagyonőröktől lehetséges beszerezni számos finombehatólást elősegítő információt, tárgyat. Erre például szolgálnak a behatólászjelző rendszer kódjai, és különböző kulcsok megszerzése. Az utóbbiak másolatának elkészítése egyszerű feladatnak bizonyul, csupán egy jó minőségű fénykép, és mintázatuk lenyomata szükséges hozzá.

6.2. Adat- és információ biztonság támadási felületei social engineering tekintetében

Az adat- és információ védelem³², mint a vagyonvédelem fontos területe, szerves részét képezi a komplex biztonságnak. Célja az adatok bizalmasságát, sértetlenségét, rendelkezésre állását biztosítani.

A cégeknél a social engineering elleni védekezés általában az információbiztonsági osztály hatáskörébe tartozik. Az informatikai rendszerek elleni támadások egy része a számítógép gyengeségeit, míg a másik az emberi hanyagságot használja ki.

Ebben a fejezetben megvizsgáljuk egy informatikai infrastruktúra elemei ellen elkövethető social engineering támadási lehetőségeket. A téma terjedelmét figyelembe véve, nem törekszünk a teljességre. Azok az elemek kerülnek felsorolásra, melyek a leggyakrabban előfordulnak tapasztalataink szerint.

Itt kifejezetten igaz, hogy a social engineering támadások csak az előkészítés fázist jelentik. Az ebben a fejezetben tárgyalt támadások többnyire már magasabb informatikai tudással párosulnak.

6.2.1. Menedzsment felületekhez való hozzáférés

A támadások egy részében a social engineer célja, hogy valamilyen eszköz menedzsmentfelületekhez férjen hozzá.

³²http://www.itb.hu/ajanlasok/a8/html/a8_3-3.htm

6.2.1.1. Aktív eszközök

A támadók a legtöbbet a hálózatok (vezetékes és vezeték nélküli) aktív eszközeit (router, gateway, switch, stb.) próbálják meg átkonfigurálni. Ehhez a legjobb út, ha a menedzser felülethez férnek hozzá, ahol az eszközök alapvető beállításait tudják elérni.

Az összes ilyen támadás azon alapszik, hogy szakzsargon és minimális informatikai ismeretek segítségével a tudatlan felhasználó utat nyit az elkövetőnek azzal, hogy hozzáférést biztosít az ilyen felületekkel.

Itt tipikus a reverse social engineering, valamilyen IT szakember identitásának ellopásával. A támadó jelzi, hogy esetleges probléma esetén őt hívják, majd előidézi azt. Ilyenkor a gyanútlan áldozat a telefonos utasításra, mit sem sejtve, akár saját maga is beállíthatja azokat a szükséges opciókat, melyek a támadónak kedvezhetnek.

Gyakori hiba, hogy nem változtatják meg az alapértelmezett jelszavakat, illetve, hogy egyszerű, személyhez kötöttet adnak meg.

A megfelelő jelszó megléte ebből is látszik, mennyire fontos. Célszerűen minél hosszabb, nem kitalálható, de megjegyezhető legyen. Egy egyszerű példa rá: „ReverseTS0cialD3ngineeringK”

6.2.1.2. Tűzfalak

A tűzfalak támadási módja hasonló a hálózati elemekéhez. Tipikusan a menedzsment felületet támadják meg. Szeretnének az előző pontban leírt módszerekkel hozzáférni a beállításokhoz.

6.2.1.3. IDS/IPS

Azaz „intrusion detection system”s és „intrusion prevention systems”³³, magyarul a behatolást észlelő és védő rendszerek. Feladatuk, hogy az internet irányából jövő adatokat vizsgálják, valamint a gyanús elemeket blokkolják.

Ha a támadó hozzáfér ezekhez a beállításokhoz, ő átírja a szabályokat, amik szerint dolgozik az IDS vagy az IPS, akkor gyakorlatilag már azt csinál, amit szeretne.

Sajnos a gyakorlat azt bizonyítja, hogy egy jó social engineer még a rendszergazdákat is ki tudja játszani. A forgatókönyvben általában leghatásosabb, ha egy szakembert személyesít meg a támadó, de lehetősége van egy partnercég alkalmazottjaként is felvenni a kapcsolatot a

³³<http://www.itbc.hu/index.php?p=22>

célszeméllyel.

Egy rendszergazda jogosultsággal bíró felhasználó gépéhez, ha a támadó hozzáfér, bármilyen indokkal szintén megváltoztathatja a beállításokat. A jogosultság megléte nem ritka, hiszen a lustaság és figyelmetlenség miatt, sok esetben nem törődnek az elszeparálástól.

A hozzáférés egy egyszerű „valami probléma van a hálózattal, vetek rá egy pillantást” szöveggel könnyen megoldható. Persze ehhez fontos a megtámadott személy kiválasztása, hiszen ahhoz, hogy sikerüljön a biztonságtudatosság hiánya szükséges.

6.2.1.4. Hálózati egyéb eszközök

Fontos odafigyelni azokra a be/kimeneti eszközökre, melyek a hálózathoz férnek hozzá. Ezek lehetnek például nyomtatók, szkennerek, multi funkciós irodai gépek. Ha ezek beállításaihoz hozzáfér egy social engineer, könnyen be tudja állítani, hogy a be/kivitt adatok hozzá is eljussanak. Ezenkívül az újabb gépeknek memóriája is van, mely tartalmához való hozzáférés rengeteg információval (pl.: a levelek tartalma, címzettek stb.) szolgálhat egy adott támadás kapcsán. A felhasználókra is jellemző, hogy sokszor egyszerűen ezen eszközök mellett felejtik a kinyomtatott dokumentumokat, informatikai adathordozókat, amiket az visz később el, aki szeretne.

6.2.2. Fejlesztői felületek

Egy speciális eset, mikor a támadó a programok fejlesztői felületéhez fér hozzá. Ennek a problémának veszélye evidens, hiszen az itt változtatottak kihatással vannak a működésre. Ha egy támadó ért hozzá, itt kénye kedvére nyúlhat hozzá a különböző jogosultságokhoz, létrehozhat magának „back door”-okat (hátsó ajtókat), amiken keresztül később hozzáfér távolról is a programhoz.

6.2.3. Szerverek

A különböző architektúrájú szerverekhez történő hozzáférés sok esetben a támadók, hackerek célja. A szerverek, mint több klienst egyidejűleg kiszolgáló egység különösen nagy kockázatot rejt, hiszen egyszerre nem csak egy gépet tudnak elérni, ha megtörték a rendszert. A veszélyt az jelenti, ha a social engineer hozzáférést kap az áldozat szerveréhez. Lehet ez a fizikailag a cégénél, szervertermekben, vagy a világ másik végén lévő egységnél.

Az esetek többségében IT szakembernek adja ki magát a támadó, hiszen az emberek azt

gondolják, hogy ő ért hozzá, így könnyebb megvezetni a tudatlanokat. Természetesen, amikor az IT dolgozók a célpont, a támadás kerettörténete lehet a klímatakarító személyes, stb. Ennek a kategóriának speciális esete, a legújító szerverek. A social engineer akkor profi, ha nyom nélkül tudja végrehajtani a munkáját. A naplóelemző szerverekhez történő hozzáférés biztosíthatja a tevékenységét bizonyító bejegyzések törlését. Akkor tökéletes egy támadás, ha visszakövethetetlen.

6.2.4. Adatbázisok

Az adatbázisok tartalma rengeteg információval bírnak a social engineereknek. Ahhoz, hogy megszerezzék egyszerűen egy géphez kell odaülnie. Ha már ott ülnek, a következő lépés, hogy rávegyék az áldozatot, hogy ne nézze tevékenységüket és utána szabadon másolhatnak, exportálhatnak.

Másik megszerzési mód az, hogy felhívják az áldozatot és megkérik valamilyen megismerés használatával, hogy küldjék el a fájlt.

Gyakori hiba, hogy például a tűzfalak és egyéb védelmi szoftverek menedzser felületein, a megjegyzés rovatba kerülnek a használt adatbázisok. Ez azért van, mert keveset használtak ezek a felületek és a felelőseik nem szentelnek elég figyelmet a biztonságos kezelésre.

6.2.5. Mobil eszközök

Egyre több olyan irodai alkalmazás van, mely elérhető a különböző mobil eszközökről (pl.: okostelefonok, tabletek, stb.). Annak kockázata, hogy a belső levelezést egy könnyen ellopható készüléken is elérhető, igen magas. Az ilyen eszközökön rengeteg információ lehet eltárolva, mely személyiség lopás alapjául szolgálhat, illetve konkrétan károkozásra ad lehetőséget.

A megszerzett információk sok támadásra is adhatnak ötletet hiszen a telefonban tárolt névjegyek, céges adatok erre jó alapot adnak.

Nem elhanyagolható veszély, hogy sokan a telefonjukban tárolják a különböző jelszavaikat papír fecnik helyett.

Fontos, hogy meg legyenek határozva az ezeken az eszközökön letölthető/futtatható alkalmazások, biztonsági beállítások, követelmények.

7. Kritikus infrastruktúrához tartozó objektum támadása (biztonsági-, social engineering audit)

A dolgozat gyakorlati részeként szándékunkban állt tesztelni a feltárt technikákat, felkutatott összefüggéseket, és ezek létjogosultságát valós környezetben. Erre egy valós és hiteles SE audit elvégzését találtuk a legjobb módszernek. Sikerült eljutnunk egy budapesti székhelyű kritikus infrastruktúrához tartozó szervezethez, melynek a főépületét állt szándékunkban megtámadni ilyen módon. A gyakorlati kutatási munkánk keretein belül szigorú jogi háttérfeltételekkel (gyakorlati megállapodás, titoktartási nyilatkozat) engedélyt kaptunk, hogy az objektum biztonsági vezetőjével való kapcsolattartás, és folyamatos konzultáció mellett elvégezzük az auditot.

A szempontjaink a helyszínválasztás kapcsán a következők voltak: mindenképp egy szigorúan őrzött objektum legyen, ahol több száz dolgozó végzi a munkáját és közismert vállalat legyen.

Gyakorlati munkánk egyik fő célja, hogy teszteljük a SE technikákat egy komplex vagyonsvédelmi rendszerrel védett objektumban, másfelől hogy felmérjük Magyarországon ilyen környezetben kivitelezhető-e egy ilyen támadás. Ebből következtetéseket vonhatunk le a magyarországi dolgozók, és munkaadó szervezetek biztonságtudatossági szintje kapcsán, esetleg arról, hogy mennyire jellemző biztonságot érintő probléma, és modern kihívás is ez.

Hosszas kutakodás után, belevágtunk ebbe a gyakorlati projektbe. Sok előkészület és hosszas tervezés következtében elvégeztük az SE auditot (SE pentesting), amit ebben a fejezetben részletesen leír a dolgozat.

7.1. *Social engineering támadás felépítése*

A SE támadások meglehetősen különbözőek, és változatosak, de néhány mindenképp szükséges lépést³⁴ el kell végeznünk ahhoz, hogy maximalizáljuk a siker valószínűségét:

- **A cél(ok) meghatározása:** fontos a támadás felépítése során azzal kezdenünk, hogy pontosan meghatározzuk céljainkat, és célirányosan építjük fel továbbiakban a cselekvést. Mindig szem előtt tartva a fő célunkat kell haladnunk a megfelelő támadási taktika kiválasztásánál.

³⁴ Oroszi Eszter: Social Engineering diplomamunka

- **Információgyűjtés:** minden támadáshoz szükséges a megfelelő mennyiségű információ, annak begyűjtése különböző módokon történhet (3.2. alfejezet), akár egy másik támadással is, melynek pont az igényelt információ megszerzése a célja.

- **Tervezés, előkészületek:** ennél a lépésnél a vélt leghasznosabb technika és részleteinek eltervezése, technológiai felkészítése a cél, amely meghatározó jelentőséggel bír a támadás sikerének valószínűsége szempontjából. Például az épületbe való bejutástól elindulva, a helyszínismeret megszerzésén keresztül, a használt eszközök vagy technológia beszerzése és előkészítésén át, a kapcsolatok kiépítéséig sokfél lehetőséget rejt magában.

- **A támadás kivitelezése:** a kivitelezés közben fontos tartanunk magunkat a tervünkhöz, és a felkészülés során meghatározottakhoz, de emellett rugalmasnak is kell lennünk az adódó szituációkban. Az ember nem egy gépezet, nem számíthatók ki pontosan a reakciók és cselekedeteik, ezért a nem várt szituációkhoz alkalmazkodnunk szükséges. Ilyenkor improvizálunk, vagy esetleg felkészülve más szituációkra is változtatunk a körülmények függvényében a tervünkön. Fontos szempont, hogy ne hagyjunk magunk után pontosan beazonosítható nyomokat. Olykor ez elkerülhetetlen, viszont mértéküket, vagy evidens jellegüket befolyásolhatjuk. Meghatározó a támadó részéről, hogy cselekedet időbeli felismerésének késleltetése, amely az adott folyamat, vagy további cselekvés érdekét szolgálja.

Fontos megjegyezni, hogy a kötött megállapodás szerint nem okozhattunk semmilyen anyagi, eszmei, presztízsbeli kárt, ezért semmilyen kártékony programot nem telepítettünk, illetve nem tulajdonítottunk el tárgyakat.

7.2. A támadás menete

A támadásnak konkrét céljai a következők voltak:

- megszerezzük a belső telefonkönyvet,
- minősített információkhoz jussunk hozzá
- belépési adatokhoz férjünk hozzá (azonosító, jelszó)
- teszteljük az ott dolgozók biztonságtudatosságát.

Támadásainkat úgy építettük fel, hogy az előző fejezetekben megismert technikák minél szélesebb tárházát próbáljuk ki a gyakorlatban.

7.2.1. Előzetes információszerzés

Legelőször az interneten böngésztünk számunkra hasznos információk után. Reméltük, hogy a kereső programok segítségével rátalálhatunk a telefonkönyvre. Számunkra sajnálatos módon ez a kísérlet kudarcba fulladt, de ennek ellenére az épületről és magáról a szervezetről értékes információkat gyűjtöttünk, például szervezeti felépítés, e-mail címek, telefonszámok, építészeti adatok, illetve olyan információkat, melyek későbbi támadások kiötlésében segítettek.

Az előzetes információ gyűjtés másik internetes része a közösségi portálok böngészése. Ennek két célja volt. Esetleges kapcsolatot kiépíteni illetve olyan információkat gyűjteni kép, bejegyzés, más kapcsán, mely előre viheti a további lépéseket.

Létrehoztunk egy fiktív felhasználót, aki ismerősnek jelölte azokat az embereket, akiknél be volt jelölve a vállalat, mint munkahely. A vártakhoz mérten kiváló eredményre jutottunk, az emberek 60%-a visszaigazolt kérdés nélkül, 10% visszakérdezett, de ennek ellenére elfogadta az ismerősnek jelölést, 30% pedig nem reagált a felkérésre.

Ezeket a kapcsolatokat a későbbiekben sikerült kihasználni, melyet majd az adott támadásnál részletezünk.

Fizikailag körbejártuk az épületet felderítve a lehetséges be/kijutási pontokat, a fizikális méreteit, építészeti felépítését, kültéri kamerák elhelyezkedését.

Az ott dolgozókkal beszélgetésbe elegyedve értékes információkkal gazdagodtunk. megtudtuk milyen operációs rendszert használnak, elmondták a belső kommunikáció eszközét, stb.

7.2.2. Bejutás az épületbe

Ahhoz, hogy az épületen belül képesek legyünk tevékenykedni, ki kellett építeni egy olyan működő rendszert, mellyel bármikor, a legkisebb kockázattal bejuthassunk az épületbe.

Egy hosszabb folyamat végeredménye képen sikerült elkészítenünk az eredeti belépőkártya nem működőképes, de kinézetre hasonló másolatát. Ennek lépései röviden a következők voltak:

- A körbejárást követően detektáltuk a belépés menetét.
- Észleltük, hogy az őr vizsgálja a belépés jogosultságát, mely a belépőkártya ellenőrzésével történik.

- Legelső alkalommal a belépés úgy történt, hogy elegáns öltözet segítségével azt a látszatot keltettük, hogy a cég alkalmazottai vagyunk, majd tailgating technikát alkalmazva, hozzacsapódtunk más belépő alkalmazottakhoz.
- Bejutva az épületbe tüzetesen megvizsgáltuk a kártya kinézetét, illetve tudomást szereztünk arról, hogy hozzájuthatunk egy más célt szolgáló (étkezési fizetőeszközt, mely egy RFID kártya), de majdnem ugyan úgy kinéző változatról.
- Második alkalommal a megvizsgáltak szerint elkészítettünk egy közelítő változatot tervező program, színes nyomtató, öntapadós fotópapír és egy lejárt bankkártya segítségével.
- Ezt felmutatva bejutottunk ismételten, majd a fent említett kártyát megszereztük. Ez és az előzőekben felsorolt eszközök segítségével elkészíthettünk egy, ugyan más funkcióval rendelkező, kinézetileg azonban az eredeti mását képező belépőkártyát, mely segítségével szabadon ki és bejáráshattunk az épületbe.

7.2.3. Belső hálózathoz történő hozzáférés

Célunk itt is az volt, hogy ha egyszerűen, törés nélkül hozzáférjünk a hálózathoz, akkor valószínűsítve találunk ott belső adatokat, esetleg a telefonkönyvet.

Több támadási módot is alkalmaztunk. Először, a nyílt WiFi hálózat tesztelésekor irányított antennák, GPS és az inSSIDer program segítségével felderítettük a szoba jöhető kapcsolati lehetőségeket. Kívülről hozzáfértünk a router menedzser felületéhez, ahol nem jártunk sikerrel, mert az alapjelszavak meg voltak változtatva. A műveletet az objektum mellett parkírozó gépjárműből éjszaka hajtottuk végre.

Emellett az okos telefonra töltött különböző alkalmazások segítségével (Fing, G-MoN, Network Discovery, Wifi Analyzer, WiFiFoFum, stb.) felderítettük a jelerőségeket, detektáltuk a routerek elhelyezkedését illetve megtudtuk milyen kódolású hálózatokról van szó.

A megszerzett információk segítségével, miután már az épületbe jutottunk különböző egyszerű kérdések feltételével megpróbáltuk megszerezni a vendégek számára fenntartott nyílt vezeték nélküli kapcsolat jelszavát. Pontos választ nem kaptunk senkitől, de a beszélgetésekből kiderült, hogy felesleges foglalkoznunk ezzel a hálózattal, mert lényeges információkhoz nem tudunk hozzájutni.

Miután szabadon járhattunk az épületben találtunk szabad hálózati végpontokat. Erre rácsatlakozva próbáltunk meg titkosítatlan adatsomagokat elkapni, melyek tartalmazhatnak esetleges jelszavakat. Idő hiányában ez a módszer is sikertelennek bizonyult.

További hasonló technikák már számunkra nem tartoztak volna az emberi hanyagságból eredő hibákhoz, ezért más irányba indultunk tovább.

7.2.4. Személyes kontaktusok

A SE támadások sikeressége abban rejlik, hogy a megfelelő alanyt válasszuk ki, illetve hogy hiteles legyen a pretexting, vagyis a felvett személyiség. Ennek érdekében többször végigjártuk az épületet. Megvizsgáltuk mely osztályok merre helyezkednek el. Felmértük apró kérdések segítségével, hol mennyire segítőkészek, kommunikatívak az emberek. Kiderítettük a vagyonvédelmi rendszerek alapvető struktúráját, hogy a későbbiek során ezt elkerüljük.

A fontosabb megállapítások a következők voltak:

- analóg kamera rendszer a forgalmasabb közlekedési csomópontokon, folyosókon és a lépcsőházakban;
- a beléptető rendszer csak munkaidő nyilvántartásra szolgál;
- a behatolás jelző számunkra nem rejt kockázatot;
- kiderítettük az örök alapvető tartózkodási helyét és járőr útvonalukat;
- a járőrmunka szervezettsége kiszámíthatóvá tette azt, így tudtuk, hogy mikor számítsunk rájuk.

Céljaink eléréséhez, mivel a hálózathoz nem férünk hozzá a várt módon, más módszert kellett kitalálni. Ki kellett választani egy cél személyt, akinek a gépéhez oda tudunk ülni. Konkrétan, bekopogtunk, mint IT biztonsági gyakornok. Megkérdeztük, hogy van-e valami gond a hálózati hozzáféréssel, mert többen jelezték a problémát. Miután nemleges választ kaptunk, jó szándékúan felajánlottuk a segítségünket, hogy azért megnézzük, később ne is legyen. A munkavállaló odaengedett a számítógépéhez, így szabadon tevékenykedhettünk azon. Kereshetettünk olyan információkat, melyeket el lehet tulajdonítani, hogy felhasználjuk azt később, illetve egyet, mely más tulajdonba kerülésével komoly kárt okozhat a vállalatnak.

Egy újraindítást követően az áldozat bármilyen óvatosság nélkül írta be a felhasználói nevét és jelszavát, melyet a vizsgálatot végző személy shoulder surfing technikával megszerzett. Így céljaink egyik pontja teljesült: belépési adatok megszerzése.

Ezt követően pendrive-ra mentésre került minősített belső információ, illetve a vállalat teljes magyarországi belső telefonkönyve.

7.2.5. Biztonságtudatosság tesztelése egyéb módszerekkel

Az eddig említetteken kívül a próbálkoztunk egyéb módszerekkel is, melyek nem feltétlen az első három cél elérését segítette elő, egyszerűen csak az emberek biztonságtudatosságát tesztelte.

Az objektum bejárása közben értékes információkhoz jutottunk. A tárgyalóban felejtett belső információk, az nyitott irattárak, a szabadon hagyott irodák elegendő ötlettel szolgáltak a későbbi támadások tervezéséhez.

Sétánk során találtunk kinyomtatva belső, minősített dokumentumokat (pl.: a szervezet vidéki telephelyeinek hálózati átjárói), prezentációs anyagokat, melyek nem feltétlenül tartoznak mindenkire még a cégen belül sem.

Fontos megjegyzés, hogy sok olyan helyen tartózkodtunk (alagsor, igazgatói váróterem, tárgyaló termek, kevesek által használt folyosók, stb.), ahol kérdés nélkül hagytak minket tevékenykedni.

7.2.5.1. Baiting

Végrehajtottunk egy baiting támadást. 5 ártatlannak tűnő, állat formájú pendrive-ot helyeztünk el az épület különböző pontjain. Az eszközre vegyesen másoltunk adatokat és elhelyeztünk rá egy „tulajdonos.txt” file-t (amiben a kapcsolattartónk volt megjelölve), azzal a reménnyel, hogy hátha valaki visszaviszi. Biztonsági és ellenőrzési pontnak az IT osztály egyik munkatársával egyeztetésre került, hogy figyelje a belső portokat, hogy az eszközök csatlakozásra kerülnek-e.

Az eredmény az lett, hogy 5-ből 1 a hálózaton csatlakoztatásra került, 1 más módon került vissza és 3-nak nyoma veszett. Ez a 20%-os arány egy fertőzött pendrive esetén sikeresnek mondható. Illetve a 3 másik valószínűleg otthoni gépet fertőzött volna meg.

7.2.5.2. Idegen eszköz csatlakoztatása vállalati számítógéphez

A támadás lényege annak vizsgálata, hogy a vállalat munkatársai megengedik-e idegeneknek, hogy saját adathordozójukat csatlakoztassák a vállalati rendszerhez, ezáltal fennáll-e annak kockázata, hogy egy kártékony programot tartalmazó eszköz kerül csatlakoztatásra. Teszteltük azt a szituációt, hogy a gyakornokságra hivatkozva ki szeretnénk nyomtatni egy anyagot pendrive-ról. Az áldokumentum végül a biztonság kedvéért 2 példányban került kinyomtatásra.

7.2.5.3. Tiszta asztal politika betartásának vizsgálata

A céggel megállapodva, nem helyeztünk el keyloggert, lehallgató készüléket, vagy annak látszó tárgyat a nyitva hagyott irodákban, de tapasztalataink szerint az emberek nem figyeltek kellő képen ennek a veszélyére. Amikor be tud hatolni egy támadó az irodába, nem csupán kártékony hardver, esetleg szoftvert tud elhelyezni az illető számítógépén, esetleg mellette, hanem számos fontos iratot tulajdoníthat el az irodából.

Az is előfordul számos esetben, hogy a dolgozók felelőtlenül egy papírra írva kéznél tartják jelszavukat, melyet egy esetleges rosszakaró könnyen leleshet.

A nyitva hagyott irattárakba sem mentünk a bejárat ajtajánál beljebb egy esetet kivéve, viszont a lehetőség adott volt számunkra, mivel teljesen felügyelet nélkül, nyitva volt számunkra az ajtó. Egy kritikus pontot kiválasztottunk, mellyel teszteltük a megfigyelő személyzet munkáját.

A célpontunk egy olyan teremre esett, aminek a folyosóra nyíló nyitott ablaka állandóan tárva volt. Az irattár felett egy kamera volt elhelyezve, így ha megfelelő az élőerős őrzésnek a hatékonysága, detektálják a helyzetet és megakadályozzák a támadás kivitelezését.

Az ablakon történő beugrás, majd a dokumentum kivitele zökkenőmentesen történt. A kihozott anyagot a főbejáratig vittük, ahol a kapcsolattartónk várt, akinek átadtuk a bizonyítékot.

7.2.5.4. Notebook eltulajdonítása

Célunk volt egy notebook irodából történő lehozatala valamilyen indokkal. Sajnos erre nem került sor, mert a kiszemelt áldozat végül nem tartózkodott a helyszínen. Alternatív megoldásokat keresve sem végződött sikerrel a próbálkozás, mert a rögtönzött alanyok asztali számítógépet használtak.

7.2.5.5. Phishing

Annak ellenére, hogy sikerült már egy felhasználói nevet, jelszavat megszereznünk, úgy éreztük, hogy ez a támadássorozat nem lehet teljes egy adathalász akció nélkül. Mivel tudtuk a telefonkönyvből, hogy kik azok, akik az épületben dolgoznak, létre tudtunk hozni egy saját adatbázist. Ez az adathalmaz 200 embernek a feltételezett e-mail címét tartalmazta, melyet mi generáltunk, tudván, hogyan épül fel a belső levelezési cím.

Létrehoztunk és egy ingyenes tárhelyre feltöltöttünk egy belső dizájnú és szövegezésű ál-honlapot, mely a munkahelyi ergonómia növelésére irányuló kérdőíves felmérést tartalmazott. A felhasználók kíváncsiságának felkeltése végett a kérdőív egy nyereményjátékot is tartalmazott, ennek érdekében az első oldalon egy, a személyes adatokra kérdező felületet illesztettünk. Ebben kértük a vállalati rendszerbe történő bejelentkezéshez használt felhasználónevet és jelszót, illetve egyéb (tulajdonképpen lényegtelen) adatokat.

A „tovább” gombra kattintva az oldal elküldte egy általunk erre a célra létrehozott e-mail címre a kitöltött mezők tartalmát.

A honlaphoz tartozott még két felület, ami már csak a díszítés és hitelesség céljából illesztettünk be.

Az egy nap alatt 15%-os kitöltési arány eredményesnek mondható. Ez azt jelenti, hogy ahány ember kitöltötte annyi féle képpen tudtunk volna belépni egy felügyelet nélkül hagyott céges gépről az említett felhasználói nevekkal, ahonnan egyéb értékes információkat tulajdoníthattunk volna el.

Természetesen teljes jelszavakat nem loptunk el, csak a kezdő betűiket írtattuk ki, valamint megjelenítettük mennyi karakterből áll az, vagyis így a diszkréció miatt teljes jelszavak birtokába nem kerültünk. Maga a honlapba ágyazott parancs küldte el az adatokat e-mail formájában.

A levelet délután 4 órakor küldtük ki. Másnap reggel a cégnél nagy kavarodást váltott ki. 11 órakor került kihirdetésre, hogy ez egy adathalász levél és akkor tiltották le a honlapot.

Ugyan a fent említett pontnál nem mentünk tovább, de a támadás veszélye miatt fontos megjegyeznünk, hogy az itt megadott jelszavak egy része, valószínűleg több magánjellegű felületen (közösségi oldalak, magán e-mailcímek, stb.) megegyező lehet, így akár több potenciális alanyunk lett volna a későbbiekben a pontos megszemélyesítéshez.

8. Összefoglalás

A dolgozat elkészítése során feldolgoztuk a könyv, és főleg internetes tudományos keresőportálokon fellelhető szakirodalmakat a SE témakörben. Ezek az irodalmak nagy része angolul, tudományos szakirodalmi stílusban készült, ezért a legtöbb időt a feldolgozásuk vett igénybe a dolgozat elkészítése során.

Részleteztük a SE technikai és pszichológiai vonatkozását, majd az elméleti összefüggéseket a vagyonvédelem tekintetében, melynek kiindulás pontja és alap tézise az emberi tényező volt. Ezt követően ismertettük a támadási felületek és módszerek lehetőségeit a vagyonvédelem két fontos szakterülete szempontjából, majd levetítve életszerű példákra az azt megelőző fejezetekben tisztázott SE taktikák felhasználásával.

A kutatómunkánk gyakorlati része sok időt, és energiát emésztett fel részünkről. Az audit végzésének helyszíni feltételeinek megteremtése is komoly feladatnak bizonyult, de a java csupán ennek abszolválásával kezdődött. Sokat terveztünk és készültünk az audit egyes támadásaira, számos alkalommal jártunk konzultálni Oroszi Eszterrel, és további szakemberekkel a támadások számunkra kódos részletei kapcsán. Folyamatosan egyeztettünk a szervezeti kapcsolattartónkkal ötleteinkről, terveinkről, és tájékoztattuk a projekt mindig aktuális fázisáról. A gyakorlati helyet biztosító vállalat számára szükséges audit eredményekről beszámoló jelentést, dokumentumot is célunk elkészíteni, amely pontosan rávilágít az adott objektum biztonsági réseire, és biztonsági szempontú gyenge pontjaira.

Az elméleti és a gyakorlati munkánkból fakadóan levonhatunk néhány következtetést, tehetünk megállapításokat a SE biztonságtechnikára gyakorolt hatása kapcsán.

A SE, mint jelenség számottevő hatást gyakorol a vagyonvédelemre, és komoly kockázati egységként tarthatjuk számon. Magyarországon jellemző, hogy a biztonságot szolgáló intézkedéseket és megoldásokat nem a megfelelő körültekintéssel tervezik, és óriási kivitelezési hibákat vétenek az ezért felelős szakemberek. Minél olcsóbb megoldásokra törekszenek és azt is gyorsan. Fontos, hogy egy objektumot vagy az információt az annak megfelelő mechanikai védelemmel lássuk el, és ne olcsó kínai gyártmányú eszközökkel. Továbbá, ha elektronikus rendszereket tervezünk és telepítünk, akkor a biztonsági elvárásoknak, céloknak megfelelően tegyük, és a kivitelezést alapos körültekintéssel

végezzük, minél kevesebb és kivitelezhetetlenebb támadási felületeket hagyva azokon. Az élőerős őrzés-védelem állománya kiemelkedően fontos SE tekintetben, hogy jól képzettek legyenek, ne megszokásból, hanem figyelmesen végezzék munkájukat. Ők kiemelt célpontok a social engineerek számára mivel a legtöbb esetben nincsenek felkészítve, oktatva az SE taktikák kivédésére, felismerésére, nincs meg bennük a kellő elővigyázatosság. Az adat- és információvédelemnek naprakésznek kell, hogy legyen napjaink informatikai támadásaival szemben. Manapság egy szervezet adatai jellemzően digitális formában vannak raktározva, és a dolgozók meghatározó része is számítógéppel végzi munkáját. Mind az adatvédelmi irányelvek és szabályzatok, mind az IT biztonsági megoldások, ha jól strukturáltak és a dolgozók be is tartják őket, akkor meglehetősen megnehezíthetik, sok úton szabotálhatják is a social engineerek cselekvéseit.

Talán az egyik legfontosabb és leghatásosabb védekezési forma a SE támadások ellen, ha felkészültek vagyunk gondolkodás szintjén, biztonságtudatosan gondolkodunk. Mivel ma Magyarországon az általános biztonságtudatos gondolkodás egyáltalán nem elterjedt, a gyakorlati tevékenységünk és az feldolgozott anyagok alapján kijelenthetjük, hogy a social engineering támadások kiküszöbölésére figyelmet kell fordítani.

Munkánk során rá kellett jönnünk, hogy szükséges ennek a problémának ismertetése az emberekkel, hogy ne érje őket váratlanul, ha ilyen szituációba kerülnek. A kis- és közép vállalkozásoktól elindulva, a multinacionális nagyvállalatokig mindenki ki van téve ezeknek a támadásoknak, és a fenyegetettségük fent áll attól eltekintve, hogy nem hallunk nap mint nap a hírekben ilyen akciókról. A magánszférában mindenki tapasztalhatja a SE hatását, mivel nem csak tudományos szinten elméleti, vagy gyakorlati vonatkozása van, hanem a hétköznapi életben is használjuk sokan ezeket a taktikákat. Meglehetősen fontosnak találjuk az emberek, de szervezetek szintjén a munkavállalók oktatását, és biztonságtudatos magatartásra való felkészítését, mivel ez a legfőbb kulcsa annak, hogy a SE támadásokat kivédhessük. Persze nem szükséges a paranoia tüneteit prezentálva gyanakodnunk mindenkire aki él és mozog, de meg kell találnunk az arany középutat a biztonsági szempontból tudat szintjén felkészült állapot, és a munkamenetre hátrányos mentalitás között.

Ahhoz, hogy biztonságtudatosan gondolkodjanak a munkavállalók, folyamatosan fent kell tartani a figyelmet különböző oktatásokkal, auditszerű gyakorlati tesztekkel. Fontos szempont, hogy túl gyakran nem szabad éles helyzetbe állítani a munkavállalókat, mert egy idő után megszokássá válik és nem fordítanak rá elég figyelmet. Lényeges szempont

az is, hogy a figyelemfelhívó tréningek és más kommunikációk kreatívak, változatosak legyenek.

Kevin Mitnick, A megtévesztés művészete című könyve és a gyakorlati tapasztalataink alapján, a következő pontok megvitatását tartjuk fontosnak egy oktatás keretén belül³⁵:

- A személyazonosság ellenőrzése
 - Hívószám kijelzés
 - Visszahívás
 - Felettes megkérdezése
 - Digitálisan hitelesített dokumentumok
 - Személyes megjelenés
- Alkalmazási státusz ellenőrzése
 - Céges adatbázis
 - Felettes megkérdezése
- Jogosultság ellenőrzése
 - Felhatalmazások megléte
 - Jogosultságrendszer pontos kialakítása
- Nem alkalmazottak ellenőrzésének kritériumai
 - Személyazonosság, kapcsolat azonosítása
 - Titoktartási nyilatkozatok meglétének ellenőrzése
 - Engedély kérése a felettesektől

Ezen pontok ismertetésével, a megfelelő biztonsági szabályok betartásával egy nagy kockázati tényezőt minimalizálhatunk. Az ilyen irányú oktatás, figyelemfelhívás költsége csekély ahhoz a kárhoz képest, amit okozhatnak az esetleges károkozók.

³⁵ Kevin D. Mitnick: A legendás hacker 334-335. o.

9. Irodalomjegyzék

- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról 3. §
- Bressert, Steve: Persuasion and How to Influence Others. <http://psychcentral.com/lib/2006/persuasion-and-how-to-influence-others/>, [2012.11.04.]
- Charles Darwin: The Expression of the Emotion in Man and Animals. D. Appleton and Company, New York, 1899, Online kiadás, http://www.pdfbooks.co.za/library/CHARLES_DARWIN/CHARLES_DARWIN-THE_EXPRESSION_OF_EMOTION_IN_MAN_AND_ANIMALS.pdf, [2012.11.04.]
- Cialdini, Robert: A befolyásolás lélektana, Corvinus kiadó, 1999, ISBN: 963906226X
- Ekman, P., Friesen, W. V.: Unmasking the face: A guide to recognizing emotions from facial clues. Prentice Hall, New Jersey, 1975. Újranyomtatott kiadás : Malor Books, Cambridge, 2003.
- Estefánné dr. Varga Magdolna, Dávid Mária, Hatvani Andrea, Héjja-Nagy Katalin, Taskó Tünde: Pszichológiai elméleti alapok, Eszterházy Károly Főiskola, http://www.ektf.hu/hefoppalyazat/pszielmal/a_pszichologia_terletei.html [2012.11.04.]
- Glasser, William: Choice Theory: A New Psychology of Personal Freedom, HarperCollins, 1998, kiadó: felhasználva: tartalmi összefoglaló-<http://ebookbrowse.com/glasser-choice-theory-pdf-d117603701>, [2012.11.04.]
- Gouldner, Alvin W. 1960. "The Norm of Reciprocity: A Preliminary Statement." American Sociological Review 25: 161-178, <http://media.pfeiffer.edu/lridener/courses/NORMRECP.HTML>, [2012.11.04.]
- Hadnagy, Cristopher: Social Engineering – The Art of Human Hacking, Wiley Publishing, Indianapolis, 2011. ISBN: 978-0-470-63953-5

- i. sz.: Őrzés-védelem, Jegyzet a biztonságtechnikai mérnök hallgatók részére. PRO LEX Kkt., Budapest, 1995.
- i.sz.: Social Engineers: Identity Thieves. [http://www.social-engineer.org/framework/Social_Engineers: Identity Thieves#Tombstone Theft](http://www.social-engineer.org/framework/Social_Engineers:_Identity_Thieves#Tombstone_Theft); [2012.11.04.]
- i.sz.: Zárszerkezetek finomnyitási módszerei 3. és 4. fejezet, <http://lockpick.blog.hu/> [2012.11.01.]
- IT Business Consulting: Behatolás-védelmi (IDS/IPS) tanácsadás. <http://www.itbc.hu/index.php?p=22>, [2012.11.04.]
- Lanford, Audri, Lanford, Jim: What's New With Identity Theft? Pretexting. <http://www.scambusters.org/pretexting.html>, [2012.11.04.]
- Lukács György: Új vagyónvédelmi nagykönyv. CEDIT Kft., Budapest, 2002.
- Miniszterelnöki Hivatal Informatikai Koordinációs Iroda: Informatikai biztonsági módszertani kézikönyv, MeH, Budapest, 1994. [2012.11.04.]
- Mitnick, Kevin D.: A legendás hacker. A rábeszélés művészete. Perfact-Pro, Budapest, 2003.
- Mitnick, Kevin D.: A legendás hacker. A behatolás művészete. Perfact-Pro, Budapest, 2006.
- Pavlov, Ivan Petrovics válogatott művei, Budapest, Akadémiai Kiadó, 1953. 256. oldal, Klasszikus kondicionálás (kutyás kísérlet)
Oroszi Eszter: Social Engineering. diplomamunka, Corvinus Egyetem, Budapest, 2008.
- Szabó Lajos: A komplex biztonsági rendszer, előadás, <http://www.gbi.bgk.uni-obuda.hu/oktatas/segedanyagok/kornyezet/index.php?dir=biztonsagszervezes>, [2012.11.04.]
- Szamosközi István: Szociálpszichológia, Személyiséglélektan. <http://eznembla-bla.uw.hu/tananyagok/eet/1felev/szocpszicho.pdf> [2012.11.04.]

- Twitchell, Douglas P.: Social engineering in information assurance curricula, 3rd Annual Conference on Information Security Curriculum Development, InfoSecCD 2006, Kennesaw, Georgia, USA, September 22-23, 2006. ACM 2006, ISBN 1-59593-437-5

10. Ábrajegyzék

1. ábra: Ábrát készítette Váczi Dániel

- A kisméretű illusztrációk forrásai:
- <http://joyintruth.com/blog/?cat=27> , [2012.11.04.]
- <http://www.vanderlande.com/en/Customer-Services/IT-Controls-support/Additional-IT-Controls-services.htm>, [2012.11.04.]