JEL-KÉP

KOMMUNIKÁCIÓ, KÖZVÉLEMÉNY, MÉDIA

2017/3. szám

SOCIAL ENGINEERING A GYAKORLATBAN

Manipulációk értelmezése a SPEAKING modellben

Kollár Csaba

kollar.csaba@uni-nke.hu

DOI: 10.20520/JEL-KEP.2017.3.63

Absztrakt

A social engineering típusú támadások részint informatikai, részint humán aspektusúak. Ez utóbbinál a támadó célja az, hogy a gyanútlan áldozattal rövid idő alatt olyan kommunikációs keretet alakítson ki, melyben a diskurzust irányítva el tudja érni a célját. A téma aktualitását az adja, hogy miközben az informatikai rendszerek informatikai biztonsága egyre jobbnak mondható, addig a rendszereket használó és üzemeltető humán erőforrás, vagyis a munkavégző ember biztonságtudatosságában komoly hiányosságok mutatkoznak, amik nem csak a saját munkájára, hanem a szervezetre is veszélyt jelenthetnek. A tanulmányban az elméleti alapok ismertetése után egy esettanulmányon keresztül kerülnek bemutatásra a verbális, a nonverbális és bizonyos szituációkban a metakommunikatív szemiotikai csapdák, s e csapdákból felépített komplex manipulációs folyamat, elsősorban Dell Hymes SPEAKING modellje alapján.

Kulcsszavak

social engineering, SPEAKING modell, manipuláció, információbiztonság

SOCIAL ENGINEERING IN THE PRACTICE

Explaining manipulation in the SPEAKING model

Csaba Kollár

Abstract

Social engineering attacks have partly information technology, partly human aspects. In this latter case, the aim of the attacker is to develop a communication frame with the unsuspicious victim, thus directing the discourse towards achieving their targets. The topic is even more relevant considering the fact that while the information technological security of IT systems is improving, there are serious deficiencies in the security awareness of human resource or staff using and operating the systems. This can be very dangerous both in terms of their own work and the organization. The present study first discusses the theoretical basis, then a case study is presented to introduce the verbal, nonverbal and the metacommunicative semiotic traps, as well as the complex manipulation processes built from these traps, first of all on the basis of Dell Hymes's SPEAKING model.

Keywords

social engineering, SPEAKING model, manipulation, information security

JEL-KÉP

KOMMUNIKÁCIÓ, KÖZVÉLEMÉNY, MÉDIA

2017/3. szám

SOCIAL ENGINEERING A GYAKORLATBAN

Manipulációk értelmezése a SPEAKING modellben*

Kollár Csaba

A social engineering pszichológiai és kommunikációs alapjai

A humán alapú social engineering támadások pszichológiai és kommunikációs alapjait az emberi viselkedés és természet általános jellemzőinek kiterjedt ismerete szolgáltatja. Az ember társas lény (Aronson 1972), aki rendszerint társas környezetben szocializálódik, s haláláig ugyancsak társas környezetben tevékenykedik (dolgozik, tanul, szórakozik, utazik, stb.). Ebben a környezetben – bár lehet, hogy magányosnak érzi magát – mégis interakciót folytat, információt ad, fogad, dolgoz fel, véleményt fogalmaz meg, meghallgat másokat, válaszol a feltett kérdésekre. Az ember social engineering típusú sebezhetősége mögött is ez a személyközi, csoporton belüli interakcióhalmaz áll, mely Oroszi (2008) és saját véleményem szerint a következő tulajdonságokban érhető tetten: befolyásolhatóság, bosszúállás, emberi hanyagság és figyelmetlenség, félelem, hiszékenység és naivság, kényelmesség, konfliktuskerülés, segítőkészség, szexuális vágy/vonzalom, tekintélyelvűség, tudatlanság és szakképzetlenség.

A social engineerek, s általában a hackerek[1] viselkedésének és működésének az egyik törvénye az, hogy minél később jöjjenek rá a sértettek arra, hogy őket/rendszereiket támadás érte, s mikorra már rájönnek, a nyomok el legyenek tüntetve. Bár nem kizárt, hogy a támadás (mint például a social engineer akciók) a nyílt agresszióra épül, többségében finom intelligenciával felépített manipuláció jellemzi (Simon 2009), melynek célja a bizalom megszerzése és megtartása. A bizalom *A magyar nyelv értelmező szótára* szerint „valakinek az olyan személyre irányuló érzése, akinek becsületességéről, helytállásáról, jó képességeiről, szándékainak helyességéről, segítőkészségéről meg van győződve, akiben bízik”. Hankiss (1978) ezt a fogalom-meghatározást azzal egészíti ki, hogy a bizalom azt is jelenti, hogy bízunk valaki szavahihetőségében. A megbízhatóság konnotatív jelentésmezőjét Hankiss (1978) az 1. ábrán látható módon ragadja meg.

* A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett Zrínyi Miklós Habilitációs Program keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

[1] A hacker fogalma az idők folyamán számos változáson ment keresztül, alapjelentése: az informatikai rendszerekhez, berendezésekhez, eszközökhöz magas szinten értő szakember, vagy hobbista. Jelenleg a hacker egyfajta gyűjtőfogalomnak tekinthető, amin belül meg lehet különböztetni többek között az etikus elvek szerint működő hackereket, akiknek célja a rendszerek biztonságosabbá tétele (White-hat hacker) rendszerint megbízás alapján, valamint a Grey-hat hackereket, akik ugyan betörnek rendszerekbe, de a rendszerek sebezhetőségéről azonnal értesítik az üzemeltetőt/tulajdonost. Az etikátlan hackerek (Black-hat hacker) tudásukkal visszaélve jogosulatlanul törnek be rendszerekbe, hogy ott kárt okozzanak. Ez utóbbi szinonimájaként szokták használni a cracker fogalmát.

1. ábra

A megbízhatóság konnotatív jelentésmezője (Hankiss 1978)

Viselkedés	intelligens, iskolázott, kulturált, udvarias, szerény, tartózkodó, VAGY magabiztos, határozott, nyugodt, kedves, természetes
Beszéd	lágy, halk, kellemes, VAGY meggyőző, határozott
Külső	megnyerő, jó, csinos, rendezett, jól öltözött, finom, ápolt kéz, szemüveg
Szociális „erények”	mindennemű társadalmi rang, mindenféle magas társadalmi státussal járó foglalkozás, gazdagság, minden konszolidált életvezetésre mutató mozzanat

Bereczkei (2016) a machiavellistákról azt állítja, hogy gyakran hazudnak, ha érdekeik úgy kívánják, s mindezt nagyon meggyőzően teszik. A sikeres social engineerekre is igaz ez a megállapítás, mivel a támadásokat úgy építik fel, hogy elhitessék az áldozattal, hogy ők intelligensek, hasznosak, hozzáértők, szerethetők, tehát meg lehet bennük bízni. Ugyanakkor hiba lenne azt állítani, hogy aki machiavellista jellemvonásokkal rendelkezik, az egyben jó social engineer is lenne. Ugyan mindkét esetben a sikeres megtévesztési stratégia része lehet egy olyan első benyomás kialakítása, ahol az áldozatok okosnak, bátornak, törekvőnek, megnyerőnek és tehetségesnek vélik a támadót, de a machiavellisták alacsonyabb érzelmi intelligenciája (Pilch 2008) rendszerint nem vezet eredményre a social engineering során.

Nábrády (2014) Albert Vrijre hivatkozva négyféle hazugságot különböztet meg: manipulátorok, színészek, szociábilis emberek és alkalmazkodók. A manipulátorokat általában magas Machiavelli-pontszám jellemzi, gyakran mondanak önző hazugságokat, s úgy vélik, hogy könnyű dolog hazudni. Rendszerint magabiztosak, laza stílusúak, általában kedvelik őket. A színészek szerepet játszanak, jó előadókészség és társas kifejezőkészség jellemző rájuk. Nem kellemetlen számukra a hazugság. A szociábilis – többnyire extrovertált – emberek az átlagosnál többet hazudnak, s ragaszkodnak hazugságaikhoz. Az alkalmazkodók jó benyomást akarnak kelteni, hogy csökkentsék bizonytalanságukat. A leírás alapján az a vélemény körvonalazódik bennem, hogy a nevezett és bemutatott négy kategória egyikébe sem illeszthető bele a profi social engineer, tehát célszerű megalkotni számára egy külön kategóriát.

Hogan (2008) nagy fontosságot tulajdonít annak, hogy akik meg akarják győzni embertársukat, azok szinte valamennyi megnyilvánulási formában megnyerők és ezáltal szavahihetők és bizalomgerjesztők legyenek. Kiemelt jelentősége van az első négy másodpercnek, amikor a manipulátor nonverbális megnyilvánulásai (testalkat, öltözet, ékszerek, kiegészítők, cipő, stb.) már a megszólalás előtt megalapozhatják a social engineer sikerét.

A megjelenés a verbális üzenettel együtt hat olyan tényezőre van hatással, amelyek meghatározzák a hitelességet. Ezek a következők.

(1) hozzáértés. A hozzáértés rendszerint a tapasztalatban és a képzettségben mutatkozik meg, a social engineer tehát a támadást megelőzően felkészül az adott szakmához tartozó ismeretekből. Mivel a social engineerek többsége átlag feletti műveltséggel rendelkezik, így számos, akár diplomához kötött foglalkozás esetében is képes hitelesen alakítani a szerepét, vagy „visszaminősíteni” magát alacsonyabb szintre (pl. egy nem túl művelt/tanult takarítót, vagy karbantartót alakít).

(2) megbízhatóság. Stresszes vállalati környezetben a munkájában elbizonytalanodott munkavállaló számára egyfajta megoldást jelent egy olyan személy megjelenése, akiben megbízhat. Az ilyen ember könnyen kifecsegi a vállalati titkokat, s nagyon hamar a bizalmába fogadja a

számára szimpatikus social engineert. Az emberek jelentős része inkább a jót tételezi fel az embertársáról, így ha például egy esőben elázott pizzafutár bekéredzkedik a mosdóba a csak belépőkártyával megközelíthető folyosón, akkor a gondoskodó és/vagy anyatípusú nők jelentős része beengedi.

(3) szakszerűség. Amikor a social engineerek rendszergazdának adják ki magukat, s néhány szakkifejezést is használnak, akkor az áldozatok többnyire természetes módon fogadják el, hogy egy szakember jött hozzájuk a gépet javítani, s magától értetődően megadják a számítógépükhöz és a vállalati adatbázisokhoz történő valamennyi belépési nevet és jelszót.

(4) szerethetőség, szimpátia. Bizonyos social engineerek viszonylag könnyedén tudják manipulálni az áldozataikat annak érdekében, hogy szeressék őket. Ennek az az alapja, hogy még a támadás előtt felmérik, hogy milyen relációk lehetnek közöttük és az áldozat között.

A gyakoribb szereprelációk (T = támadó, Á = áldozat és/vagy balek):

- feltűnően csinos és kívánatos nő (T) – saját magát túlértékelő, szexuális vágytól fűtött férfi (Á),
- beszállító cég intelligens, sármos középvezetője (T) – a harmincas éveiben járó, a férfiak megbecsülését és igaz szerelmét kereső nő (Á),
- esőben elázott, vékony testalkatú, szemüveges pizzafutár, kerékpáros futár (T) – hasonló életkorú gyermeket nevelő nő (Á),
- a vállalat székhelyén dolgozó, legfrissebb híreket ismerő kolléga (T) – a telephelyen dolgozó, az információhiány miatt sorsukat bizonytalannak ítélő kollégák (Á),
- a dohányzó külsős kolléga, beszállító, vásárló (T) – a kijelölt helyen (vagy éppen a tilosban) dohányzók (Á),
- az új kolléga, aki segítséget kér a vállalat informatikai rendszereinek a használatához (T) – a kollégák, akik segítenek neki (Á).

A szakszerűség és megbízhatóság szereprelációi:

- a vállalat tevékenységét ellenőrző külsős személy (T) – a vállalat alkalmazottai (főleg azok, akik tudják, hogy valamilyen munkát nem, vagy nem megfelelő minőségben, vagy csak a megadott határidőn túl végeztek el) (Á),
- az informatikus/rendszergazda (T) – a számítógéphez és/vagy az informatikai rendszerhez nem értő kolléga (Á).

Egyéb szereprelációk (általában nem alakul ki szimpátia, de hagyják tevékenykedni az álcázott támadókat):

- takarítók (T) – dolgozók (Á).
- karbantartók, javítók (T) – dolgozók (Á).
- kerékpáros futárok, postások, csomagszállítók (T) – dolgozók (Á),
- pénz- és értékszállítók (T) – dolgozók (Á).

(5) önuralom. A social engineering típusú támadások ugyan felépítettek, de az esetek többségében nem jellemző, hogy a támadó és az áldozat többször olyan helyzetben találkozik egymással, hogy az áldozat emlékezne a támadó arcára (kivételt képeznek például a belső social engineerek, a kémek, az ügynökök). Ha nem az első találkozás alkalmával akarja a támadó végrehajtani a támadást, hanem többször találkozik az áldozatával (pl.: beszállító egy cégnél), akkor önuralmat kíván meg a megfelelő alkalom kivárása. Az önuralom azért tartozik a hitelesség hat tényezőjének a sorába, mert megtanítja a social engineert arra, hogy kontrollálni tudja saját indulatait és szenvedélyeit.

(6) társas hajlam. Egy social engineer – ha a magánéletben az átlaghoz képest esetleg zárkózottabb is – amikor a támadó tevékenységet végez, akkor természetesen kell viselkednie a

társas közösségben. Fel kell tudnia vetni a csoport érdeklődésére számot tartó témákat, vagy aktívan hozzá kell szólnia mások megjegyzéseihez/kérdéseihez. Amikor a támadó egy csoport ellen, vagy annak felhasználásával hajt végre támadást (pl. hozzácsapódik az ebédről visszaérkező kollégák csoportjához, s belépőkártya nélkül megy be a vállalat lezárt részeibe), akkor a csoporthoz illeszkedő természetes viselkedése „védi meg" attól, hogy a biztonsági szolgálat emberei, vagy a recepciósok felfigyeljenek rá a csoportban.

Tanulmányomban több helyen is kiemelem, hogy a sikeres social engineering akciók elképzelhetetlenek a támadás logikus megtervezése nélkül. A social engineering általános lépései a következők:

1. A terv alapozása (találkozás a megbízóval, „szerződés" előkészítése)
2. Felderítés, információszerzés (hírszerzés nyílt forrásokból)
3. Megfelelő célszemély(ek) kiválasztása
4. A támadás előkészítése (információk kiértékelése, helyszín, módszer, szereplők, történet, időtáv, stb. kiválasztása, a megszerzendő adatok és információk meghatározása, „szerződés" elfogadása)
5. Megtévesztés – a bizalom megszerzése (a social attack indítása – az első 4 másodperc, valamint az első néhány mondat)
6. A megszerzett bizalom kihasználása (pl. beszélgetés folytatása, bejutás elzárt részekbe)
7. A támadás előkészítése során meghatározott adatok és információk megszerzése
8. A beszélgetés zárása és/vagy a nyomok eltüntetése
9. A helyszín elhagyása
10. A megszerzett adatok és információk feldolgozása és/vagy átadása a megbízónak feldolgozásra
11. A támadás kiértékelése, tapasztalatok megfogalmazása

A social engineer a megtévesztés kezdetekor, vagyis a játszma indulásakor az áldozatát belekényszeríti egy szerepbe, aki „a szerepben megtapad, beleragad, s nem próbálja meg többé azt feloldani, átfordítani. Többnyire azért, mert a szélhámos kínálta szerep a testére van szabva. A jó szálhámos ugyanis azonnal letapintja, hogy áldozata milyen szerepben 'utazik', és viselkedésével, fellépésével megjeleníti a kiegészítő szerep kellékeit" (Hankiss 1978: 341–342). Ha ez a beragadás sikerül, akkor a bizalom már könnyen kihasználható, s a bizalmas és titkos információk könnyen megszerezhetők.

Nem lehet egyértelmű választ adni arra, hogy mennyi ideig tart egy támadás. Ha a támadó a tervezés során jól megkonstruált helyzetet realizálni is tudja, akkor elég lehet néhány mondat ahhoz, hogy hozzáférjen eszközökhöz, kódokhoz, vagy hogy lemásoljon adatokat. Előfordulhat azonban olyan eset is, hogy a támadás hosszabb időt vesz igénybe (pl. flörtölés a biztonsági szolgálat embereivel, vagy a recepciós hölgyekkel). A lebukás elkerülése és más emberek értelmetlen bevonódása miatt azonban a leggyakoribb az, hogy a social engineer a minimálisra próbálja csökkenteni azt az időt, amit a megtámadott szervezet épületében, telephelyén az áldozatával tölt.

Hymes és Philipsen

Ray és Chinmay (2011) tanulmányukban Elizabeth Keatingre hivatkozva azt írják, hogy Hymes John Gumperz-zel és hallgatóikkal közösen egy újszerű programot indítottak a nyelvi kutatás területén előbb a *Beszéd etnográfiája*, majd *A kommunikáció etnográfiája* néven. 1962-ben Hymes azonos című tanulmánya révén lett a tudományos diskurzusok tárgya a

kommunikáció etnográfiája, melyről Carbaugh (1989) úgy vélekedett, hogy a kommunikáció etnográfiája a kommunikáció kulturálisan jellemző eszközei és jelentései tanulmányozására szolgáló megközelítés, nézőpont és módszer. Maldona (2009) szerint a kommunikáció néhány aspektusa változhat földrajzi területek, társadalmi osztály, nemek, életkor vagy iskolázottság szerint, ami kiterjesztett értelmezésben igaz lehet iparágakra és ágazatokra is, a szervezeteket érő humán alapú social engineering támadásoknál pedig véleményem szerint foglalkozni kell az adott szervezetre jellemző egyedi kulturális elemekkel és eszközökkel, illetve azok használatával is (szervezeti kultúra). Zand-Vakili, Kashani és Tabandeh 2012-es tanulmányukat arra az alapfeltevésre építik, miszerint a beszédet sokféle módon használják a különféle csoportokban levő emberek, s minden csoport kialakítja a nyelvi viselkedés saját szabályait. Annak érdekében, hogy egy adott csoport nyelvét/nyelvhasználatát elemezni tudjuk, meg kell határoznunk az elemzés keretét. Hymes (1974) az elemzés három szintjét javasolja, mégpedig: (1) beszédhelyzet, (2) beszéd(esemény), (3) beszédaktus. Richards és Schmidt (2013) úgy vélik, hogy a három szint közül a beszédesemény az, ami megadja az elemzés igazi értékét, vagyis az esemény során a kölcsönös üdvözlés, a kölcsönös érdeklődés, stb. vizsgálata; tanulmányomban én is ezzel foglalkozom elsősorban.

A szóbeli befolyásolás nyelvészeti, pszichológiai és kognitív keretét az antropológus Duranti gazdagítja, aki tanulmányában – követve a beszélés néprajzi felfogását – „a társas-társadalmi és kulturális dimenziót állítja a beszélgetés tanulmányozásának középpontjába" (Síklaki 2008: 20). Hymes alapján Duranti is azt állítja, hogy a társas esemény (vizsgálódásunk fókuszában a szemtől-szembeni kommunikáció) alapja az, hogy létrejön maga a beszédesemény. Hymes szerint „a beszédesemény kizárólag olyan tevékenységekre, vagy tevékenységek aspektusaira vonatkozik, amelyeket a beszédhasználattal kapcsolatos szabályok vagy normák közvetlenül szabályoznak. Egy ilyen esemény állhat egyetlen beszédcselekményből, de gyakran inkább több cselekményből" (Hymes 1972: 56).

A beszédesemény elemzésénél Hymes a SPEAKING mozaikszót javasolja, amelynél az egyes betűk jelentése a következő:

- Setting/scene: beszédhelyzet,
- Participants: résztvevők,
- Ends: lezárások,
- Act sequences: cselekménysorozatok,
- Key: kulcs,
- Instrumentalities: eszközök,
- Norms: normák,
- Genre: műfaj.

Hymes hatása többek között Philipsen munkásságában is tetten érhető. Beszédkód elméletében a fogalmat úgy határozza meg, hogy az „egy jelképekből, jelentésekből, premisszákból és szabályokból álló társadalmilag megalkotott kommunikációs magatartásra vonatkozó rendszer" (Philipsen 2001: 428–429). Akik ismerik és használják ezt a rendszert, azok képesek a társadalom/közösség aktív tagjai lenni, így azt is állíthatjuk, hogy a társas együttélés alapja ez az ismeret. A philipseni meghatározás némi átírat után a szervezeti kommunikáció, illetve a szervezeti kultúra vonatkozásában is helytálló: a szervezet és tagjai által kialakított és elfogadott értékrend, normatíva, etika, magatartásforma, tudás, tapasztalat, melyet a szervezet megőriz, átörökít, megújít (Magyar PR Szövetség). A szervezetek tehát a társadalmi csoportokhoz hasonlóan megalkotják beszédkódjaikat, magatartásformáikat, ahol az általános emberi tulajdonságok egyaránt jellemzik a szervezet munkatársait, de vannak olyan, az adott szervezetre jellemző ismeretek is (és ezen ismeretekre épülő magatartásformák, pl. belépéskor az arcképes igazolvány bemutatása, illetve a vállalati emblémával ellátott nyak-

kendő viselése), amelyeket a sikeres social engineering akció érdekében a támadóknak előzetesen fel kell térképeznie. Ez a megállapítás akkor is megállja a helyét, ha egyébként a humán típusú social engineering támadásoknál a pillanatnyi helyzet azonnali felismerésére épülő improvizáció elengedhetetlen.

Philipsen beszédkód elmélete öt tételének social engineering-gel kapcsolatos saját meglátásom szerinti átiratát az alábbiakban adom meg.

1. tétel: a szervezeti kultúrához minden esetben sajátos beszédkód társul, aminek megismerése a sikeres social engineering akciók egyik alapfeltétele.
2. tétel: a szervezetek munkatársai által használt beszédkód magában foglal bizonyos kulturális vonatkozású pszichológiai, társadalmi, retorikai különbségeket, ezek ismerete és felismerése révén a social engineer a megtámadott munkatárs bizalmába tud férkőzni.
3. tétel: a manipuláció technikáit jól ismerő social engineer olyan keretet ad a beszélgetésnek, ahol akár közvetlen, akár közvetett irányító szerepben határozza meg a beszéd jelentőségét, tartalmát és folyamát.
4. tétel: a szervezet és a social engineer közötti kommunikáció során elfogadjuk, hogy mindkét fél multiplatformos kommunikációt folytat, s a támadó igazi szándéka a beszédből önmagában nem, vagy csak nehezen bogozható ki.
5. tétel: a social engineer a verbális, nonverbális, illetve metakommunikatív kódok ismeretében úgy képes alakítani a beszélgetést, hogy abból a megtámadott ágens nem vesz észre semmit.

A social engineering értelmezése a SPEAKING modellben

A **beszédhelyzet és/vagy a jelenet** a beszéd konkrét fizikai körülményeit, vagyis az időt és a helyet jelentik. Az időbeli és a térbeli határokat két részre oszthatjuk, úgymint (1) külső időbeli/térbeli határok, és (2) belső időbeli/térbeli határok. A külső időbeli határ azt jelenti, hogy a social engineering támadás összességében hány percet vesz/vehet igénybe. A támadás forgatókönyve szerint ez az időkeret kisebb részekre osztható, s ezeket a részeket hívjuk belső időbeli határoknak. A külső térbeli határ jelenti a támadás helyszínét (pl. recepciós pult, dohányzásra kijelölt hely, iroda), a belső térbeli határt pedig a szereplők egymással kapcsolatban határozzák meg. Ide sorolható, hogy a megtámadott ágens elhagyja-e a helyét (pl. kilép a pult mögül, vagy átmegy egy másik irodába), vagy a támadó az idő függvényében mennyire szakszerűen szabályozza maga és a beszélgetőpartner(ek) között a fizikai távolságot. A beszédhelyzet egy keretbe helyezhető, s ennek részei az épület belső tere és bútorai, a világítás, a zene, az időjárás, a napszak, a hőmérséklet, stb. A támadás során a forgatókönyv szerint megadott szereppel kongruens díszletet/jelmezt kap a social engineer (pl.: pizzafutár, vamp nő, felügyeleti/ellenőrző szerv munkatársa), illetve viselkedésével igazodik a díszlethez (pl.: iroda, recepciós pult, dohányzásra kijelölt hely, igazgató szobája). A támadás előkészületei közé tartozik a beszédhelyzet térbeli határainak (vagyis magának a helyszínnek és környezetének) a bejárása. Sor kerül többek között a hely építészeti tulajdonságainak az elemzésére (bejáratok száma, irodák és mosdók elhelyezkedése, recepciós pult helyzete, mérete), az azonosítás módjainak a számbavételére (pl. arcképes igazolvány, biometrikus, mágneskártyás), a vázlatos alaprajz elkészítésére.

A **résztvevők** leírásánál részint a szereplők számát, részint pszichológiai/kommunikációs aktivitását célszerű bemutatni. A social engineer egyaránt kezdeményezhet támadást magányos ágens ellen (pl. recepciós pultban ülő személy, biztonsági őr), illetve csoport ellen is (pl. közösen dohányzók, közösen étkezők, résztvevők egy konferencia szekcióülésén). A támadásra felkészült social engineer akár előre eldöntött módon, akár improvizatíve egy

bizonyos szerepet játszik el (pl. esőben elázott pizzafutár, akinek ki kell mennie a mosdóba, felügyeleti szerv munkatársa), szükség esetén menet közben is alakíthat ezen, hogy elkerülje a szerepkonfliktust.

A **lezárások** egyfelől azokra a célokra utalnak, amelyeket a támadó a beszélgetés során el szeretne érni. Ezek rendszerint a következők lehetnek: bizalmas/titkos információk megszerzése beszélgetéssel, elérni, hogy beengedjék a nyilvánosságtól elzárt részekre, kapcsolatot kialakítani és fenntartani a további támadások érdekében. A social engineernek arra is fel kell készülnie, hogy a lezárás nem az előzetesen elképzelt tervek szerint valósul meg, mert például egy ellenőrzési ponton fennakad, lebukik, feltartóztatják, bezárják egy szobába, értesítik a rendőrséget. A lezárások során természetesen a megtámadott ágensnek is vannak céljai (vagy a támadó úgy alakítja, hogy legyenek céljai). Ilyen cél lehet például a női támadóval való intim viszony kialakítása, az önzetlen segítségnyújtás, a fontos(nak mondott) információk megszerzése.

A **cselekménysorozat** tanulmányom fókuszában magát a felépített humán alapú social engineering támadást jelenti. A cselekmények sorrendje rendszerint kulturálisan meghatározott, része többek között a köszönés és a búcsúzás, a magázásból tegezésre váltás (bizalmaskodás elindítása), illetve az is, hogy milyen szavakat és szófordulatokat használnak.

A **kulcs** alatt a verbális, nonverbális, illetve adott esetben metakommunikációs kódokat értjük. A megfelelő kulcs alkalmazása a social engineering támadások egyik, ha nem a legfontosabb eleme. A támadó felvett szerepének sikeres eljátszásában döntő jelentőségű az, hogy az üzenet egyes elemei kongruálnak-e egymással. A támadó modora/stílusa többek között könnyed, komoly, tekintélyt parancsoló, precíz, tudálékos, nagyképű, beképzelt, gunyoros, szarkasztikus lehet, míg nonverbális jelzéseinél a gesztikuláció, a testtartás, a térközszabályozás, a mimika stb. képezik a lehetséges social engineering arzenált. A hipnózisban és általánosságban a manipulációban vannak olyan esetek, amikor a megtámadott ágens összezavarása a cél. Ha a beszéd tartalma és a hozzá kapcsolódó, használt kulcs között nincs megfelelő összhang, akkor a hallgató inkább a kulcsnak szentel nagyobb figyelmet, semmint az aktuális tartalomnak.

Számos **eszköz** áll a social engineer rendelkezésére arra utalva, hogy milyen kommunikációs csatornákat használ fel a támadás során. A csatorna lehet szóbeli, írásos, telefonos (hívás és SMS), internetes (e-mail-es), s az eszközök közé sorolja Hymes a beszéd aktuális formájára, vagyis a nyelvre, dialektusra, választott kódra, hangnemre történő utalást is. Eszköz lehet a formális, írásos, jogi nyelv (pl. a NAV-tól, vagy egy ügyvédtől származó üzenet) is.

Az **érintkezés normáinál** egy specifikus viselkedést értünk, illetve azt, hogy ezt a viselkedést és annak jellemzőit hogyan ítélik meg a beszélgetésben részt vevő ágensek. A social engineer eldöntheti, hogy a támadást a normaszegésre és/vagy a normakövetésre építi-e fel. Az előbbi esetre példa, amikor a női támadó flörtöl a biztonsági őrrel, az utóbbira, amikor a támadó (pl. valamelyik felügyeleti szerv munkatársának adja ki magát) megerősíti a megtámadott félben azt a viselkedési normát, amit elvárnak tőle a munkahelyén (precíz, a törvényi előírások szerinti munkavégzés). Az érintkezési normák közé sorolható a hangos, vagy éppen halk beszéd (suttogás), a cinkos/erotikus összenézés, a verbális flörtölés, az intim szférába történő belépés, az érintés, a kézfogás, stb.

A **műfaj**, amelyben a beszédaktus létrejön többek között vers, közmondás, mondóka, prédikáció, ima, cikk, előadás, illetve a social engineerek gyakorlatában rendszerint üzleti tájékoztató, általános információ, felvilágosítás, tanácsadás, javaslat, segítségkérés/nyújtás, beszélgetés, interjú, riport lehet.

Egy esettanulmány, mint a téma gyakorlati bemutatása

Az elméleti modell információbiztonsági célú alkalmazásának gyakorlati bemutatására az alábbiakban egy esettanulmányt ismertetek, melynek alapját egy kereskedelmi bankban végzett információbiztonsági audit adta. Az informatikai és információbiztonsági auditok célja az, hogy feltérképezze a rendszer biztonsági réseit, majd ennek ismeretében elősegítse a hálózati infrastruktúra fejlesztését (Rajnai – Nguyen 2015).

Horváth – Mitev (2015) Dooley (2002) és Klenke (2008) munkáira hivatkozva az esettanulmány lépéseit a következők szerint határozták meg:

A. kutatási kérdés meghatározása
B. az eset(ek) kiválasztása
C. az adatgyűjtési és elemzési technikák kiválasztása
D. Adatgyűjtés előkészítése és kutatói reflexió
E. adatgyűjtés
F. adatok elemzése és interpretálása
G. kutatási beszámoló elkészítése
H. minőségi kritériumok meghatározása

A. A kutatási kérdés meghatározása

Tanulmányomban alapvetően két alapvető kérdést vizsgálok: (1) alkalmas-e Hymes SPEAKING modellje a humán típusú social engineering támadások elemzésére, illetve, ha alkalmas, akkor (2) milyen általánosítható következtetések fogalmazhatók meg az esettanulmányok feldolgozását követően.

B. Az eset(ek) kiválasztása

Bár Creswell (2007) az esetek kiválasztásánál azt javasolja, hogy egy tanulmány elkészítésekor célszerűen 4-5 esetet érdemes feldolgozni, jelen írásomban terjedelmi korlátok miatt csak egy esettanulmányt ismertetek azokból az esetekből, melyek két kereskedelmi bank információbiztonsági auditja során elemzett hang- és videofelvételek alapján rendelkezésemre álltak. A minta elemzésére a SPEAKING modellt használtam fel. Mivel szereplőként kerül megnevezésre a biztonsági őr, ezért a vezető auditorral előzetesen megvizsgáltuk, hogy a személy- és vagyonbiztonságnak milyen személyi feltételei vannak (Berek – Berek – Berek 2016), illetve, hogy ezek a feltételek hogyan jelennek meg a munkaköri leírásokban.

C. Az adatgyűjtési és elemzési technikák kiválasztása

Az adatgyűjtés során a nem résztvevő megfigyelést választottam. Ennek oka az volt, hogy nem akartam részvételemmel befolyásolni a humán típusú támadást végrehajtó, a forgatókönyvben előírt szerepet játszó auditort, s nem volt célom az sem, hogy – azzal, hogy tudatában van annak, hogy külön is megfigyelem – esetleg kizökkenjen a szerepéből. Mivel a teszttámadásról megfelelő minőségű (hallható, látható) hang- és videofelvétel készült részint a támadást megelőzően elrejtett mikrofon, részint jobb képfelbontású biztonsági kamera és a folyamatos videofelvételt lehetővé tevő rögzítőberendezés segítségével, így a felvett anyag alkalmas volt arra, hogy jó alapot jelentsen az adatok SPEAKING modell szerinti elemzésére.

D. Az adatgyűjtés előkészítése és kutatói reflexió

A külön felvett hang- és videóanyag szinkronizálásának (együttfutásának) elvégzése után szükség volt némi hang-utómunkára annak érdekében, hogy a közepesen zajos környezet háttérzajából a diskurzusok elkülöníthetők és jobban érthetők legyenek. A kutatásról csak a vezető információbiztonsági auditor tudott, s megállapodásunk szerint nem vonta be előzetesen sem a munkatársait, (s értelemszerűen) sem a leendő tesztalanyokat a kutatási folyamatba annak érdekében, hogy a tesztkörnyezet a többi auditor, illetve a megtámadásra kiválasztott munkavállalók számára egyaránt természetes legyen. Bár Gall – Borg – Gall (2007) azt javasolja a kutatóknak, hogy szubjektivitás auditot célszerű végezniük, de mivel én nem vonódtam be érzelmileg a kutatásba, így ezt nem tartottam fontosnak.

E. Az adatgyűjtés

Mivel sem a bankok, sem az auditot végző szervezet nem járult hozzá a bankok nevének, illetve elhelyezkedésének a megadásához, ezért írásomból ezeket az információkat én is kihagyom. A tanulmányomban bemutatott esettanulmányhoz kapcsolódó adatgyűjtésre 2016. negyedik és 2017. első negyedéve között került egy kereskedelmi bank 2-2 helyszínén (1 budapesti központ, 1 regionális/megyei igazgatóság, 2 kiemelt bankfiók). Az információbiztonsági audit, s így az adatgyűjtés (ez a gyakorlatban hang- és videofelvétel formájában valósult meg) napját megelőzően a vezető auditorral közösen elhelyeztük a szükséges mikrofonokat, illetve a bankok technikusaival lecseréltették két helyen a nem megfelelő felbontású videokamerákat. Az audit napján az előre megírt forgatókönyvek szerint a humán típusú social engineering támadást az auditorok végrehajtották, melyről sikeres hang- és videofelvétel készült. Az adatgyűjtés lezárását követően – még az adatok elemzése előtt – a felvételkészítés tényéről tájékoztattuk az auditorokat, illetve a teszttámadást elszenvedett munkavállalót, akik hozzájárultak ahhoz, hogy a felvételeket tudományos céllal elemezzük.

F. Az adatok elemzése és interpretálása

A felvett és a háttérzajtól megtisztított felvételeket többször megnézve/meghallgatva, esetenként külön-külön rögzítettem megfigyelésem eredményeit szöveges leírás formájában a SPEAKING modellben. Megjegyzem, hogy az információbiztonsági auditot végző vezető auditor nem járult hozzá ahhoz, hogy a cselekménysorozatnál a teljes dialógust bemutassam (részint a saját módszertanuk védelme érdekében), ezért a cselekménysorozat fontosabb – publikus – részével foglalkozom az alábbiakban. Az elemzés elvégzését követően a hang- és videofelvételeket, valamint az adott eset beazonosíthatóságára utaló kutatói megjegyzéseket töröltem az auditor cég kérésének megfelelően.

Esettanulmány: vamp nő beszélget a biztonsági őrrel

Beszédhelyzet

A támadás külső időbeli határa 25 perc időtartamú volt. A belső időkeretek fontosabb mérföldkövei: (1) megszólítás, (2) bemelegítés, (3) bizalmaskodás (tegezés), (4) fontos információk megszerzése, (5) ígéret a későbbi találkozásra, (6) a beszélgetés zárása, elköszönés. A támadásnak volt egy másik belső időkerete is, nevezetesen, hogy a támadó az ügyfél szerepét eljátszva nem zárhatta le a beszélgetést, miután a szükséges információkat megszerezte, tehát a folyamatban figyelemmel kellett lennie arra is, hogy kb. hány perc, míg sorra kerül, s odamegy az ügyintéző asztalához.

A külső térbeli határ a bankfiók ügyfélterülete, azon belül a bejárat, ahol a biztonsági őr „őrhelye” található. A belső térbeli határt a támadó úgy határozta meg, hogy a beszédhelyzet időbeli lefutása során az áldozattal egy csendesebb részbe elvonulva tudjanak beszélgetni. A támadó a fizikai távolságot úgy szabályozta, hogy szinte az egész beszélgetés során az áldozat privát szférájában tartózkodott. Ezt részint helyezkedésével, részint a halkabb beszédével érte el. A „helyezkedés” kölcsönös volt, az áldozat sem akarta, hogy a banki alkalmazottak, illetve az ügyfelek hallják, hogy hogyan udvarol a támadónak. A támadás ideje: a hét második felében, délután, amikor sokan vannak a bankfiókban. Ez azért volt fontos, mert így több ideje volt a támadónak az áldozattal beszélgetni, mielőtt az ügyfélhívó rendszer révén sorra került volna.

Résztvevők

A résztvevőket közvetett és közvetlen szereplőkként definiálhatjuk. A közvetett szereplők az ügyfelek és a banki alkalmazottak. A közvetlen – a támadás szempontjából fontos – résztvevők:

- áldozat: a húszas évei végén járó biztonsági őr, akinek imponál, ha egy feltűnően csinos nő megszólítja, s elbeszélget vele.
- támadó: kifogástalan, szexi ruhában (kiskosztüm, rövid szoknya), kihívó, de nem hivalkodó sminket viselő, 25-30 év körüli szőke, göndör hajú nő. Vörös kéz- és lábkörmök, magas sarkú nyári szandál, ékszerek (gyűrűk, nyaklánc, kar- és bokalánc, fülbevaló), kis retikül, napszemüveg. Ő az a nő, aki után a férfiak jelentős része megfordul.

Lezárások

A támadás célja, hogy a bankfiók viszonyait jól ismerő biztonsági őr minél több információt adjon meg a bankfiók munkatársairól, elsősorban a fiókvezetőről, annak – előzetes információk alapján feltételezett – titkos szerelmi viszonyáról. Ez a támadás – ha nem egy audit, illetve kutatásom része lett volna – alapozta volna meg a fiókvezető elleni további közvetett és közvetlen támadásokat (pl.: zsarolás), illetve gyengeségei révén további adatok és információk megszerzését tette volna lehetővé.

Cselekménysorozat

A cselekmény felépítése a következő: (1) belépés a bankfiókba, (2) a biztonsági őr megszólítása és nyitó kérdés feltétele még magázva: „nem tudja, hogy mennyit kell várni, amíg sorra kerülök?” (3) beszélgetés folytatása arról, hogy a támadó mennyire siet, milyen idegölő a várakozás, mennyire fárasztó lehet a biztonsági őrnek egész nap álldogálnia (biztos esténként a barátnője megmasszírozza), (4) a támadó „véletlenül” letegezi az áldozatot, aki ezt láthatóan örömmel fogadja, (5) beszélgetés folytatása a bankfiók működéséről (milyen a beosztás, ha a biztonsági őr elfárad, ki váltja, a fiókvezető biztosan már az összes csinos ügyintézővel lefeküdt, stb…), a fókuszban annak kiderítése áll, hogy igaz-e a pletyka, hogy a pedáns családi életet élő fiókvezető viszonyt folytat egy fiatal nővel, akivel napközben szokott találkozgatni. A biztonsági őrben a támadó erősíti az irigység érzését azzal, hogy kihangsúlyozza, hogy a fiókvezetőnek biztos sportkocsija van, mennyire sikeres, biztos minden nő szerelmes belé. A biztonsági őr elkezd kompenzálni (az a támadás szempontjából nem fontos, hogy mennyire lódít saját szerelmi életét illetően), s a kompenzálás során elmeséli a fiókvezető valamennyi viselt dolgát, a napi rutinját (mikor érkezik, napközben mikor távozik, mennyi időre, milyen gépkocsija van, hol szokott parkolni, hol, s mit sportol), s arról is szól, hogy hogyan néz ki a feltételezett barátnő. Tulajdonképpen itt le is lehetne zárni a cselekménysorozat bemutatását, mivel a támadó elérte a célját. Az audit során azonban a támadó tovább

játszotta a szerepét, s (6) ugyan nem adta meg a telefonszámát, de elkérte a biztonsági őrét, mondván, ha unatkozik, felhívja majd, illetve (7) megígérte, hogy jövő héten is beugrik a bankba, amikor az áldozat szolgálatban lesz. Végül (8) lezárta a beszélgetést „ahogy látom, mindjárt én következek a sorban", s mint egy hagyományos ügyfél (9) elintézte az ügyét (néhány általános információt kért bankszámlanyitással kapcsolatban).

Kulcs

Mindkét szereplő a túlhangsúlyozott nemi archetípusát (vamp nő, macsó férfi) játszotta el a támadás során. A vamp nő – ahogy arra már fentebb utaltam – kinézete figyelemfelkeltő (emblémák és kulturális szignálok), szexi. Hangja és modora kedves, ugyanakkor csak moderáltan határozott, mivel a feltételezés szerint a túlzott határozottsága elbizonytalanítja a biztonsági őrt. Ismeri a szexuálmágia valamennyi elemét, beleértve a nézést, a test- és különösen a fejtartást, a térközszabályozást, az ön- és társérintést, az ajkak nedvesítését. A biztonsági őr egyébként kimért és unottságot tükröző viselkedése a vamp nő megjelenésének a pillanatában átváltott macsó férfivá, aki elfelejtette eredeti feladatát, s csak arra koncentrált, hogy a támadónak imponáljon. A támadónak viszonylag könnyű dolga volt, mivel a szexuális tartalmú nonverbális jelzések visszatükrözésével és felerősítésével megerősítette és macsó szerepének további markáns játszására ösztönözte az áldozatát.

Eszközök

A kommunikációs csatorna a személyközi kommunikáció során verbális és nonverbális. A jelentéstartalmak tekintetében épít a metakommunikatív jegyekre is.

Normák

A támadó alapvetően normaszegésre építette a támadást, de a megkonstruált helyzetnek köszönhetően az áldozat minden fenntartást nélkülözve szegte meg a normákat.

Műfaj

Személyközi – intim – beszélgetés.

G. A kutatási beszámoló elkészítése

Írásművemben két kérdést fogalmaztam meg. Az elsőre adott válaszom szerint Hymes SPEAKING modellje alkalmas a social engineering támadások elemzésére. Jogos lehet a felvetés, hogy vajon négy esettanulmány (melyek közül egyet ismertettem) alapján magabiztosan ki lehet-e jelenteni, hogy a válaszomat kellő mérlegelés után adtam meg. Mivel az általam feldolgozott források még csak érintőlegesen sem foglalkoznak a modell és az informatikai támadások kapcsolatával, így úgy gondolom, hogy az esettanulmányok elemzése révén a válaszomat inkább elfogadom, semmint további elméleti irodalmat feleslegesen felvonultatva próbálok meg bizonytalanul állást foglalni. Természetesen fenntartom a jogot arra vonatkozóan, hogy további kutatások (esettanulmányok) során véleményemet kiegészítsem, illetve megváltoztassam.

A másik kérdésemre – miszerint milyen általánosítható következtetések fogalmazhatók meg az esettanulmányok feldolgozását követően – az alábbiakban adom meg a választ.

A humán alapú social engineering típusú támadások elemzésénél a sikeres esetek mellett több sikertelen támadás is volt. A sikertelen esetekről általánosságban a következő megállapítások tehetők:

- A támadást megelőzően az auditor nem készült fel kellő alapossággal a szervezet működéséből, kultúrájából, holott a megbízó bankokról valamennyi esetben rendelkezésre állnak olyan nyilvánosan elérhető információk, amelyek ezt a felkészülést lehetővé tették volna.

  Természetesen éles helyzetben is előfordulhat, hogy a támadó nem készül fel a vállalatból, s tevékenysége idegennek hat. Ugyanakkor, ha a támadó kilétét fel is fedik a munkatársak, nem tudják, hogy mit kell tenniük, s a támadó elfuthat. Megjegyzem, hogy amikor az auditot végző támadó lebukott, akkor bemutatkozott, s elmondta, hogy ez csak teszt volt. Véleményem szerint ez hibás gyakorlat, mert nem vitte végig a folyamatot.
- A támadást megelőzően az auditor nem sajátította el a felvett szerepéhez illeszkedő szakma alapvető ismereteit, s néhány mondat után lebukott. Ez szintén elkerülhető lett volna, ha a felkészülésre több időt szán.
- Az auditor nem vette figyelembe, hogy az előzetesen megtervezett akciók (helyszín, szereplők, szituáció, stb.) a támadás időpontjára megváltoztak, s nem tudta kezelni a kialakult helyzetet. Egy gyakorlottabb social engineer vélhetőleg nagyobb rutinnal tudott volna improvizálni.
- A kiszemelt áldozatok felismerték, hogy a támadó auditor verbális és nonverbális jelzései nem kongruálnak egymással.
- A cselekménysorozatban az auditor nem tudta fenntartani a kommunikáció dinamizmusát, a kiszemelt áldozata sokkal kevésbé volt közlékeny, a számára elképzelt szerepet nem, vagy nem az elvárásoknak megfelelően játszotta.
- Olyan szereplők is bevonódtak a cselekménysorozatba, akikre az auditor előzetesen nem számított, s a kialakult beszédhelyzetet nem tudta kellő szakmaisággal kezelni.
- A szervezetnél olyan biztonsági előírások vannak életben, amelyek blokkolják például a pendrive-ok használatát, vagy ha a felhasználó 30-60 másodpercig nem üt le egy billentyűt sem, akkor csak a megfelelő jelszóval kikapcsolható képernyővédő indul el a számítógépén.
- A szervezet a biztonságot, s ennek részeként az információbiztonságot helyezi a fókuszba, rendszeres információbiztonsági előadásokat, tréningeket, gyakorlatokat tartva, illetve tanácsadással, coachinggal, mentorálással erősítve a (felső)vezetők biztonságtudatosságát.

H. A minőségi kritériumok meghatározása

Klenke (2008) és Paré (2002) (hivatkozza Horváth – Mitev 2015) az esettanulmányok minőségi kritériumait négy dimenzió mentén határozza meg. Az általuk felvázolt lehetséges stratégiák közül a (1) fogalmi érvényesség dimenziójában a fogalmak korrekt használatára törekedtem. Mivel a két terület metszéspontja üres halmaz volt, így több esetben saját fogalmi átirataimat használtam annak érdekében, hogy előzetes felvetésem szerint Hymes modelljét a jövőben fel lehessen használni az információbiztonsággal kapcsolatos éles és modellezett (audit) támadások elemzésére. A (2) belső és a (3) külső érvényesség ellenőrzésekor megállapítottam, hogy a modell lehetővé tette, hogy a social engineering típusú támadások és azok folyamata nyolc szempont szerint vizsgálható, s a levont következtetések az információbiztonsággal foglalkozó szakemberek számára – még ha a modellt nem is ismerték – informatív

jelleggel bírnak. Ennek érdekében az esettanulmányokat cikkem kéziratának leadása előtt odaadtam több olyan szakembernek, akik a Nemzeti Közszolgálati Egyetem Elektronikus információbiztonsági vezető szakán, illetve az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában tanulnak. Az esetleírásokat, a feldolgozási rendszert megértették, s úgy ítélték meg a modellt, hogy az akár a jelenlegi, akár egy néhány további szemponttal kiegészített változatában (pl.: anyagi veszteség mértéke, a használt eszközök markánsabb informatikai típusú leírása, biztonsági kockázat-besorolás) alkalmas a további elemzésre, s iparágtól/ágazattól függetlenül az adott szervezet információbiztonsági programjának az elkészítéséhez, illetve a fejlesztéséhez kellő alapot szolgáltat. Úgy gondolom, hogy a (4) megbízhatóság dimenziójában is megállja a helyét a modell. Hymes kritériumai szerint akár az esettanulmányokban bemutatott, akár más social engineering típusú támadások is elemezhetők, értékelhetők a segítségével. Amennyiben rendelkezésre állnak a hang- és videofelvételek, akkor a teszttámadások jól dokumentálhatók.

Összefoglalás

Mitnick – Simon (2006: 268) a social engineerek tevékenységével és annak megakadályozásával foglalkozó fejezetét a szociálpszichológus Sagarin azon megállapításával indítja miszerint „a social engineer ugyanazokat a meggyőző technikákat alkalmazza, amiket mindannyian használunk a mindennapok során”. Szerepeket veszünk fel, törekszünk megteremteni a hitelességünket, azon dolgozunk, hogy kedvesek legyünk, s ha egyszerű kéréssel fordulnak hozzánk, akkor azt rendszerint megpróbáljuk teljesíteni. Férfiként/nőként keretet adunk a kapcsolatainknak, minden kedvező tulajdonságunkat bevetjük, hogy elnyerjük szívünk választottja kegyét, megkapjuk az áhított álommunkát, vagy csak hogy imponáljunk a környezetünkben levő embertársainknak. A meggyőző technikák tesznek minket sikeressé az üzleti és magánéletben, s alapvetően nem úgy gondolunk rájuk, mint valami rossz és elvetendő dologra. „A social engineer azonban – idézi Sagarint Mitnick – Simon (2006: 268) – manipuláló és megtévesztő, nagyon etikátlan módon alkalmazza a technikákat – és gyakran elsöprő sikert ér el velük”. Ezek a technikák megismerhetők, tanulhatók, fejleszthetők, de ugyan úgy tanulható a technikák felismerése és kivédése is. Nagyon fontos az információbiztonság, s annak tudatosítása, hogy a social engineering típusú támadás bármelyik szervezetet, s a szervezet bármely vezetőjét/alkalmazottját érheti, illetve újabban akár a családtagjaikat is. Véleményem szerint a társadalom és a benne levő ember számára minden olyan modellt és eljárást elemezni kell, amelyik révén a biztonságtudatossága fejleszthető. Meggyőződésem, hogy Dell Hymes SPEAKING modellje is ezekhez az építő jellegű, az információbiztonság-tudatosság gyakorlatában is sikeresen alkalmazható modellekhez tartozik.

Irodalom

A magyar nyelv értelmező szótára. (vezetőszerk.: Bárczi Géza – Országh László) Budapest, Magyar Elektronikus Könyvtár. http://mek.oszk.hu/adatbazis/magyar-nyelv-ertelmezo-szotara

Bereczkei Tamás (2016) *Machiavellizmus. A megtévesztés pszichológiája*. Budapest, Typotex

Berek Lajos – Berek Tamás – Berek László (2016) *Személy- és vagyonbiztonság.* Budapest, Óbudai Egyetem.

Carbaugh, Donald (1989) Fifty terms for talk: A cross-cultural study. *International and Intercultural Communication Annual*, 1989/13, 93–120.

Creswell, John W. (2007) *Qualitative inquiry and research design: Choosing among five approaches.* Thousand Oaks, Sage.

Dooley, Larry M. (2002) Case Study Research and Theory Building. In: *Advances in Developing Human Resources*, 2002 4: 335. https://doi.org/10.1177/1523422302043007

Duranti, Alessandro (1985) Sociocultural Dimensions of Discourse. In: Teun A. Van Dijk (ed.) *Handbook of Discourse Analysis*. London, Academic Press Limited.

Gall, Meredith W. – Borg, Walter R. – Gall, Joyce P. (2007) *Educational Research: An Introduction*, 8th Edition. Cambridge, Pearson

Hankiss Ágnes (1978) A bizalom anatómiája. In: T. Kiss Tamás (1999 szerk.) *A szemtől szembeni formációk kommunikációs viszonyai.* Budapest, Új Mandátum. 320–346.

Hogan, Kevin (2008) *A meggyőzés tudománya.* Budapest, Danvantara Kiadó.

Hováth Dóra – Mitev Ariel (2015) *Alternatív kvalitatív kutatási kézikönyv.* Budapest, Alinea Kiadó.

Hymes, Dell (1972) Models of the Interaction of Language and Social Life. In: Gumperz, John – Hymes, Dell (szerk.) *Directions in Sociolinguistics: The Ethnography of Communication.* New York, Holts Rinehart & Winston, 35–71.

Hymes, Dell (1974) *Foundations in Sociolinguistics: An Ethnographic Approach.* Philadelphia, University of Pennsylvania Press.

Klenke, Karin (2008) *Qualitative Research in the Study of Leadership*. Bingley, Emerald Group. https://doi.org/10.1108/9781785606502

Matel, Maldona (2009) The Ethnography of communication. *Bulletin of the Transilvania University of Brasov.* Vol. 2(51) 2009, Series IV; Philosophy and cultural Studies.

Mitnick, Kevin D. – Simon, L. William (2006) *A legendás hacker. A behatolás művészete*. Budapest, Perfact-Pro Kiadó.

Nábrády Mária (2014) *A megtévesztés művészete*. Budapest, Libri.

Oroszi Eszter Diána (2008) *Social Engineering: Az emberi erőforrás, mint az információbiztonság kritikus tényezője.* Budapest, BCE.

Paré, Gui (2002) Enhancing the Rigor of Qualitative Research: Application of a Case Methodology to Build Theories of IT Implementation. *The Qualitative Riport*, 2002, vol 7, no 4. 1–34.

Philipsen, Gerry (2001) A beszédkódok elmélete. A kommunikáció etnográfiája. In: Griffin, Em (szerk.) *Bevezetés a kommunikációelméletbe*. Budapest, Harmat. 428–439.

Pilch, Irena (2008) Machiavellianism, emotional intelligence and social competence: Are Machiavellians interpersonally skilled? In: *Polish Psychological Bulletin*, 2008/39/3. https://doi.org/10.2478/v10059-008-0017-4

Rajnai Zoltán – Nguyen Huu Phouc Dai (2015) General audit of the infrastructure, improvements in network security features, fixing potential security holes in a company. In: Rajnai Zoltán – Nyikes Zoltán – Milan Pavlovic (szerk.) Proceedings on Applied Internet and Information Technologies. 258 p. Konferencia helye, ideje: Zrenjanin, Szerbia, 2015.10.21–2015.10.23. Zrenjanin: University of Novi Sad, Faculty of Technical Sciences, 148–151.

Rajnai Zoltán (2017) Információbiztonság tudatosság. In: Bitay Enikő (szerk.) *A XXII. Fiatal Műszakiak Tudományos Ülésszak előadásai: Proceedings of the XXII-th International Scientific Conference of Young Engineers.* 418 p. Konferencia helye, ideje: Kolozsvár, Románia, 2017.03.23–2017.03.24. Kolozsvár: Erdélyi Múzeum Egyesület (EME); Óbudai Egyetem, 37–43.

Ray, Manas – Biswas, Chinmay (2011) A study on Ethnography of communication: A discourse analysis with Hymes 'speaking model'. *Journal of Education and Practice*, 2011/2/6. 33–40.

Richards, Jack Croft – Schmidt, Richard W. (2013) *Dictionary of Language Teaching and Applied Linguistics.* New York, Longman Publications.

Síklaki István (2008 szerk.) *Szóbeli befolyásolás I. Nyelv, gondolkodás, kultúra*. Budapest, Typotex.

Simon, George (2009) *Báránybőrben. A nyílt agressziótól a manipulációig.* Budapest, Háttér Kiadó.

T. Kiss Tamás (1999) *A szemtől-szembeni formációk kommunikációs viszonyai*. Budapest, Új mandátum.

Zand-Vakili, Elham – Fard Kashani, Alireza – Tabandeh, Farhad (2012) The Analysis of Speech Events and Hymes' SPEAKING. Factors in the Comedy Television Series: "FRIENDS". *New Media and Mass Communication*, 2012/2. 27–43.