DOI: 10.38146/BSZ.2018.2.2

KOLLÁR CSABA

Az információbiztonság humán aspektusai[1]

A biztonságtudatossági ellenőrzés során alkalmazott social engineering technikák elemzése a SPEAKING modell segítségével

Az információs társadalomban, illetve az e fogalmat fokozatosan leváltó digitális korban, vagy más néven az adatok korában az ezt megelőző korokhoz képest másfajta értékek kerültek a középpontba. A hálózatba kapcsolt vezetékes és vezeték nélküli kommunikációs eszközök (asztali számítógépek, szerverek, okostelefonok, laptopok, tabletek stb.) révén – feltételezve az aktív infokommunikációs kapcsolatot az egyén készüléke és a hálózat között – az emberek aktivitásának egyre nagyobb része valósul meg a digitális világban, a kibertérben. Az olyan tevékenységek mellett, mint a kommunikáció, vagy a munka, a számunkra értékes adatok és információk tárházai is a kibertérbe költöztek, s e folyamat nemcsak az egyénekre, hanem a szervezetekre is jellemző. Az adatok, az információk felértékelődésével párhuzamosan újfajta egyéni és szervezett bűnözési formák jelentek meg. Az elkövetők számára az értéket nem vagy nem elsősorban maga az eltulajdonított tárgy jelenti, hanem az informatikai adathordozón lévő adatok, információk, adatbázisok. A bűnesetek egy részében nem is tárgyakat, hanem csak adatokat és információkat lopnak el az elkövetők. Ez után a megbízóik kívánságainak megfelelően manipulálják, átírják, vagy törlik az adatbázisok, a publikusan, illetve csak a belső hálózatból elérhető weblapok tartalmát stb. Hiba lenne azt állítani, hogy ezek a feladatok kivétel nélkül jelentős informatikai/programozói tudást igényelnek, annál is inkább, mivel a bűnszervezetekben elkövetett tevékenységek jelentős részénél megfigyelhető a munkamegosztás. Az egy területre (például adathalászat, nyomeltakarítás, szerverek feltörése) szakosodott szakemberek között megjelennek azok a bűnelkövetők, akik elsősorban már nem a kódolással, kódfejtéssel foglalkoznak, hanem a kommunikációs, pszichológiai, szociálpszichológiai modellek és általánosságban az emberi visel-

1 A tanulmány az Emberi Erőforrások Minisztériuma ÚNKP-17-3-I-OE-779/45 kódszámú Új Nemzeti Kiválósági Programjának támogatásával készült.

kedés magas fokú ismerői. A feladatuk pedig, hogy a komplex informatikai védelemmel felvértezett szervezetek legsebezhetőbb pontját, rendszerint az azt üzemeltető, fenntartó, fejlesztő, használó (munkavégző) embert vegyék célba, s olyan helyzeteket teremtsenek, ahol a célszemély az általuk elvárt módon viselkedjen. Magyar nyelven is megjelent a *Kevin D. Mitnick* életével foglalkozó két könyv[2], amelyben a főszereplő-szerző külön fejezetben tárgyalja a megtévesztés művészetét, a *social engineering*et. A szerzők megfogalmazása szerint *„a támadó az emberi természet legnemesebb tulajdonságát használja ki: azt a természetes törekvésünket, hogy segítőkészek, udvariasak, pozitívak legyünk, csapatjátékosként viselkedjünk, illetve azt a vágyunkat, hogy elvégezzük a munkánkat”*.

A hackerszubkultúrától a bűnszervezeteken át az információs hadszíntérig

A hackerkultúrával számos könyv foglalkozik[3], gyökerei egészen az 1980-as évekig nyúlnak vissza[4]. Az 1990-es években a jelenséggel már a hatóságok is foglalkoztak[5], az akkor még a nyomaik eltüntetésével nem igazán foglalkozó, a hackelésre inkább csak szubkultúraként tekintő fiatalok számára egy-egy weboldal feltörése, vagy az adatok megszerzése – bár tevékenységükkel törvényt sértettek – egyfajta elismertség kivívásának számított a csoporton belül. A könyv említést tesz a *Fry Guy* nevű hackerről, aki már a humán típusú *social engineering* technikákkal is foglalkozott („kiváló beszélőkészsége volt”), illetve röviden ismerteti a telefonos *social engineering* technikát, hangsúlyozva, hogy az informatikai rendszerekben az azzal kapcsolatban álló ember a leggyengébb láncszem. Ugyancsak a fiatalok történeteit meséli el érdekes és olvasmányos formában *Dreyfus és Assange*[6]. A szerzők megadják a humán típusú *social engineering* ma is elfogadható rövid leírását, miszerint: *„a social engineering a sima/gördülékeny beszédet jelenti azokkal a hatalmi pozícióban lévő emberekkel, akik tesznek valamit a beszélő számára”*.

2 Kevin D. Mitnick – William L. Simon: A legendás hacker. A megtévesztés művészete. Perfact Kiadó, Budapest, 2003; Kevin D. Mitnick – William L. Simon: A legendás hacker. A behatolás művészete. Perfact Kiadó, Budapest, 2006

3 https://percomis.wordpress.com/2013/05/10/hacker-konyvek/

4 Steven Levy: Hackers: Heroes of the Computer Revolution. O'Reilly, New York, 2010

5 Bruce Sterling: The Hacker Crackdown: Law And Disorder On The Electronic Frontier Mass Market. Bantam, New York, 1993

6 Suelette Dreyfus – Julian Assange: Underground. Red Book, Sydney, 1997

Russel[7] egy olyan, számos gyakorló kiberbiztonsági szakember bevonásával megírt művet jegyez, amelyiknél a történet bemutatja, hogy hogyan használta fel a főszereplő (Bob) a hackereket arra, hogy egymástól függetlenül különböző részfeladatokat teljesítsenek (például betörések, adatmanipuláció, adatlopás) annak érdekében, hogy a végén ő meggazdagodhasson. A regény üzenete az, hogy a kiváló szervezőkészséggel, de alapvetően komoly hackertudással nem bíró személyek hogyan tudják befolyásolni a kellően szűk látókörű, s „csak" az informatikához értő hackereket – ez egyfajta példaként szolgált arra is, amit később vállalkozások/kormányok megvalósítottak: megbíztak (igaz, rendszerint fizetésért cserébe) hackereket a (bűn)cselekmények elvégzésével. *Poulsen*[8] *Max Butler* megtörtént eseteken alapuló történetét meséli el, aki a bankkártyaadatok feketepiaca feletti ellenőrzést vette át. A könyv a kibervilágban működő bűnszervezetek tevékenységével is foglalkozik.

Ha a hackerek tevékenységét, tudását és értékét az idő folyásában vizsgáljuk, akkor megállapíthatjuk, hogy a korábbi tizenévesek által elkövetett informatikai csínytevések (bár a jelenlegi fiataloknak is kihívást jelent egy-egy weboldal, vagy Facebook-profil feltörése) mellett megjelentek, jelenleg pedig arányait és gazdasági/társadalmi hatását tekintve sokkal gyakrabban találkozhatunk a szervezett bűnözés körébe tartozó hackertámadásokkal. Ezeknél a technikai tudás mellett a szervezőkészség és az álcázás jellemzi a csoportot, amely elsősorban a közvetlen és közvetett anyagi haszonszerzés érdekében végzi tevékenységét, eleget téve a szervezeti, illetve kormányzati megbízásoknak.

Haig és Várhegyi[9] megkülönbözteti az információs hadműveletek között a fizikai, az információs és a tudati dimenziót. Utóbbinál *„közvetlenül az emberi gondolkodást, észlelést, érzékelést, értelmezést, véleményt, vélekedést veszik célba valós, csúsztatott hamis üzenetekkel, amelyeket többek között […] közvetlen beszéd formájában továbbítanak"*. A leírtak és a humán alapú *social engineering* típusú támadások közötti kapcsolat egyértelmű.

7 Ryan Russell: A Háló kalózai. Hogyan lopjunk kontinenst. Kiskapu Kiadó, Budapest, 2005

8 Kevin Poulsen: Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground. Broadway Paperbacks, New York, 2011

9 Haig Zsolt – Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest, 2005

A social engineering értelmezése a személyközi kommunikációs viszonyok között

Ahogy arra már utaltam, a humán alapú *social engineer* támadások alapját elsősorban nem az informatikai, hanem a kommunikációs, pszichológiai, szociálpszichológiai és szociológiai tudás, s e tudás gyakorlati felhasználása és alkalmazása jelenti. Az ember születésétől egészen haláláig szocializációs folyamat(ok)ban vesz részt. Ennek részeként megtanulja az interperszonális kommunikációt fenntartó és mozgató erőket, a különböző társas viszonyokat[10], az első benyomásból megszerezhető információkat, a csoportnormákhoz történő igazodást, a szeretet (szimpátia) és a segítségnyújtás módjait és lehetőségeit, a csoportközi konfliktusok kezelését[11]. Ez a gyakorlati tudás/tapasztalat segíti az egyént abban, hogy a társadalomban, és azon belül a kisebb csoportokban (család, munkahely, iskola, baráti kapcsolatok stb.) otthonosan mozogjon, felismerje a csoporton belüli erőviszonyokat, kialakítsa, meghatározza, megerősítse helyét a csoporton belül, olyan diskurzusokat folytasson, amelyek révén el tudja érni és/vagy céljai érdekében tudja manipulálni beszélgetőpartnerét. Azzal, hogy az ember társas lény[12], késztetést érez arra, hogy egy vagy több csoport tagja legyen, s ha a csoporton belül biztonságban érzi magát, akkor rendszerint megtöri a csendet, és magáról, maga és a csoport viszonyáról közöl információkat, illetve ha a személyes/intim szféráját nem érintő kérdéseket kap, akkor azokra magától értődő módon válaszol is. A közlések és a válaszok többségében megjelennek az érzelmek, illetve az egyén olyan szituációban van/szituációba hozható, amikor megnyilvánulásai mögött érzelmek vannak, mint például harag, félelem, meglepődés, öröm, szomorúság, vidámság, megelégedettség, bűntudat. *Atkinson*[13] nyolc elsődleges érzelmet és a hozzájuk tartozó helyzeteket ismerteti *(táblázat)*.

A *social engineer* már az alapérzelmek és a felismert, beazonosított helyzetek alapján is sikeres támadást tud megvalósítani áldozatával szemben. A személyközi kommunikáció során az Atkinson és társai[14] által bemutatott helyzeti tényezőket is ki tudja használni a támadó azzal, hogy olyan kommunikációs helyzetet épít fel, amelynek az alapját a következő tényezők jelentik:

10 Miles Hewstone – Wolfgang Stroebe – Jean-Paul Codol – Geoffrey M. Stephenson (szerk.): Szociálpszichológia európai szemszögből. KJK, Budapest, 1999

11 Eliot R. Smith – Diane M. Mackie: Szociálpszichológia. Osiris Kiadó, Budapest, 2001

12 Elliot Aronson: The Social Animal. Freeman, San Francisco, 1972

13 Rita L. Atkinson – Richard C. Atkinson – Edward E. Smith – Daryl J. Bem: Pszichológia. Osiris Kiadó, Budapest, 1997

14 Uo.

1. kívánatos és megtörténik: öröm;
2. kívánatos és nem történik meg: bánat;
3. nemkívánatos és megtörténik: aggódás;
4. nemkívánatos és nem történik meg: megkönnyebbülés.

Az eddig felsorolt érzelmek mellett *Oroszi*[15] és a saját véleményem szerint a következő tulajdonságok teszik sebezhetővé, kihasználhatóvá a *social engineer*ek által megtámadott személyt: bosszúállás, befolyásolhatóság, emberi hanyagság és figyelmetlenség, hiszékenység és naivság, kényelmesség, konfliktuskerülés, segítőkészség, tekintélyelvűség, tudatlanság és szakképzetlenség, (szexuális) vonzalom, szimpátia/antipátia.

Érzelem	Helyzet	Munkahelyi példa
1. Szomorúság	Szeretett személy elvesztése	Munkahely elvesztése. Kolléga kilép/kirúgják a munkahelyről.
2. Félelem	Fenyegetettség	Elveszíthetem a munkahelyemet. Nálam jobb, okosabb, csinosabb stb. új kolléga pályázik a helyemre. Nem tudom idejében elvégezni a munkámat. Félek, hogy megint megszid/megszégyenít a főnököm.
3. Harag	Akadály	Utálom a főnökömet, kollégáimat. Nem tudok szakmailag fejlődni. Nem tudom ezt az új rendszert használni.
4. Öröm	Potenciális társ	Kedvelem a kollégáimat. Ő a legjobb munkatársam.
5. Bizalom	Csoporttag	Tudom, hogy a kollégákkal együtt meg tudom csinálni. Jó, hogy van olyan kollégám, akire számíthatok.
6. Undor	Förtelmes tárgy	Utálom a munkámat. Utálom a munkaeszközeimet (például számítógép).
7. Anticipáció	Új territórium	A főnököm magasabb pozíciót ígért nekem, ha megteszem, amit kér. Elhitetik velem, hogy a ranglétrán feljebb léphetek.
8. Meglepődés	Hirtelen új tárgy	Új szoftvert kell alkalmazni holnaptól. Új belépési rend lépett életbe.

15 Oroszi Eszter Diána: Social Engineering: Az emberi erőforrás, mint az információbiztonság kritikus tényezője. Budapesti Corvinus Egyetem, Budapest, 2008. http://krasznay.hu/presentation/diploma_oroszi.pdf

Balázs[16] úgy fogalmaz az érzelmi zavarok kapcsán, hogy *„túlzott emocionális reakcióknál általában a helyzet téves értékelése, az észlelés beszűkülése és torzulása következhet be, valamint a magatartáskészlet kimerülése”. A social engineer* sikerességének tehát az az alapvető mércéje, hogy érzelmi zavarkeltés során képes-e a megtámadottban elérni, hogy a helyzetet a támadó által kívánt módon értékelje, a megtámadott észlelése csak a támadó által szabályozott módon történjen, magatartáskészletében a támadó által elvárt eszközöket használja, illetve szerepet vegye fel.

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

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

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

16 Balázs István (szerk.): Pszichológiai lexikon. Magyar Könyvklub, Budapest, 2002

A biztonságtudatossági ellenőrzés kommunikációelméleti megközelítése

A kommunikációs fókuszú biztonságtudatossági ellenőrzés során a szervezet és belső érintettjei, így munkatársai, vezetői, bizonyos esetekben alvállalkozói és beszállítói által közölt információkat, illetve a különböző (személyközi) kommunikációs helyzetekben tanúsított magatartásukat vizsgálják. Tanulmányomban csak a nyílt forrású hírszerzéssel és a *social engineering* típusú módszerekkel foglalkozom, a szabályozásokkal, munkaköri leírásokkal, a fizikai biztonság kialakításának és fejlesztésének módszereivel stb. nem, vagy csak érintőlegesen.

A nyílt forrású hírszerzés *(Open Source Intelligence; OSINT)* során az ellenőrök (illetve, ha nem ellenőrzésről van szó, akkor a támadók) egyebek között a következő forrásokból szereznek szervezeti információkat (NATO, *Lévay*[17]*, Izsa*[18]*,* illetve saját megjegyzések):

- a szervezet munkatársainak digitális lábnyomai;
- a szervezet munkatársaival folytatott beszélgetések;
- a szervezet beszállítóival, vásárlóival, versenytársaival folytatott beszélgetések;
- a szervezet publikus sajtóanyagai (például sajtóközlemények);
- a szervezet weboldalai és egyéb webes platformjai (például LinkedIn, Facebook);
- a szervezetről a nyomtatott és elektronikus médiában megjelenő hírek, információk;
- az internetes keresőkkel megtalálható tartalmak;
- az internet sötét tartalmai *(dark web);*
- kereskedelmi (fizetős) online szolgáltatók tanulmányai, adattárai;
- kereskedelmi műholdak felvételei;
- nem kormányzati szervek (NGO) (például Amnesty International, Nemzetközi Vöröskereszt, Orvosok Határok Nélkül) hivatalos anyagai és az alkalmazottjaival, szakembereivel folytatott beszélgetések;
- szakmai szövetségek, kamarák, érdekképviseleti szervezetek adott szervezetről is szóló beszámolói, elemzései;
- személyes tapasztalatok;

17 Lévay Gábor: OSINT (Open Source Intelligence). Nyílt információs hírszerzés. Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2006

18 Izsa Jenő: Nemzetbiztonsági alapismeretek. Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2009

– szürke irodalom: nem publikált és nem is minősített dokumentumok, tanulmányok, jelentések, amelyek „okos böngészéssel” megtalálhatók;
– tudományos előadások, konferenciák, ahol a szervezetről elhangzanak információk;
– tudományos-kutató szervezetek, egyetemek (például az adott szervezettel közösen végzett kutatások, fejlesztések).

Az adatok és információk feldolgozását segítheti, ha valamelyik kommunikációs modellt használják az elemzők. *Griffin*[19] és *Horányi*[20] számos, a gyakorlatban is alkalmazható kommunikációs modellt mutat be könyveiben, ezek közül az OSINT esetében *Shannon és Weaver*[21] alapmodellje is megfelelő lehet. A küldő meghatározása során ki lehet térni a jogosultságokra (például van-e joga az adott személynek a szervezetről információt megadni), a küldés céljára, a szándékolt, vagy épp ellenkezőleg a felelőtlen közlésre (például egy titkárnő egy Facebook-csoportban kér segítséget azzal a megjegyzéssel, hogy most vezette be az önkormányzat az új szoftvert, de senki nem tudja kezelni). A csatorna elemzésekor részint szabályozni lehet, hogy kinek van joga az adott csatornán a szervezettel kapcsolatos információkat megosztani, de akár az is szabályozható, hogy az adott személy ezt a csatornát nem használhatja. A szervezet azt is megvizsgálhatja, hogy melyek azok a csatornák, amelyeken a szervezetről megjelennek ugyan bizonyos információk, de ezeket a csatornákat nem szeretné a jövőben használni, vagy ellenkezőleg: markánsabban szeretné. A címzett a nyílt forrású információknál mindenki lehet, aki az üzenetet olvassa (még akkor is nyíltnak tekinthető, hogy egy olyan zárt Facebook-csoportban került sor a publikálásra, amihez csatlakozni kell ahhoz, hogy az ott közölt tartalom megtekinthető legyen). Ez lehetővé teszi, hogy a szervezet a konkurencia tudatos félrevezetése céljából hamis információkat adjon meg.

A humán alapú *social engineering* biztonságtudatossági ellenőrzés célja az, hogy modellezett helyzetben/szituációban az ellenőrzés alá vont személyek hogyan viselkednek akkor, amikor a támadó (aki szerepe szerint ügyfél, kolléga stb.) olyan dologra kéri őket, ami a biztonsági szabályzattal ellentétes, vagy olyan kérdésekre válaszolnak, aminek révén ha nem is titkos, de bi-

19 Em Griffin: Bevezetés a kommunikációelméletbe. Harmat Kiadó, Budapest, 2001
20 Horányi Özséb (szerk.): Kommunikáció I–II. General Press, Budapest, 2003
21 Claude E. Shannon: The mathematical theory of communication. In: Claude E. Shannon – Warren Weaver: The mathematical theory of communication. The University of Illinois Press, Urbana, 1964

zalmas információkat mondanak el illetékteleneknek. A *social engineering* (akár támadó, akár ellenőrző céllal történik is) 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 négy másodperc, valamint az első néhány mondat).
6. A megszerzett bizalom kihasználása (például 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 támadás elemzésére az előbbiekben nevezett forrásokban található modellek közül alapozásként *Philipsen* elméletét, a bemutatott három esettanulmánynál pedig *Hymes* SPEAKING modelljét veszem alapul.

Philipsen beszédkódelmélete

Philipsen beszédkódelmélete[22] öt tételben foglalható össze. Tanulmányomban az öt tétel *social engineering*gel kapcsolatos saját meglátásom szerinti átiratát ismertetem.

1. tétel: egy sajátos kultúrához minden esetben egy sajátos beszédkód társul. Ha a vállalati diskurzusokat leírjuk, akkor felületes szemlélőként közel sem biztos, hogy észrevesszük a sajátos beszédkódokat. A munkatársak egymás közötti beszélgetéseiben, vagy a szervezet hivatalos kommunikációjában (például sajtóközlemények, reklámok, vállalati tájékoztató anyagok) használt szavak és szófordulatok gyakorlatilag mindenki számára megérhetők, akik az

22 Gerry Philipsen: A beszédkódok elmélete. A kommunikáció etnográfiája. In: Em Griffin: i. m. 428–439. o.

adott nyelven beszélnek. Ha azonban a rendelkezésünkre álló szövegkorpuszokat alaposabban elemezzük, legalább két fontos különbségre figyelhetünk fel. 1. Vannak olyan rövidítések, szavak, szókapcsolatok, szófordulatok, amelyeket az adott szervezet kizárólag, vagy legalábbis az átlaghoz képest sokkal gyakrabban használ. Ha ezeken a szövegeken szógyakorisági elemzést végeznénk, s az eredményeket egy szófelhőben ábrázolnánk, egyértelművé és láthatóvá tudnánk tenni, hogy melyek ezek a szavak, szókapcsolatok, szófordulatok. 2. Vannak olyan szavak és szókapcsolatok, amelyek egy adott iparágban/ágazatban dolgozók számára egyfajta összetartozást jelentenek (kulturális/szakmai közösség és hovatartozás), s már néhány mondat után képesek lehetnek észrevenni azt, ha valaki csak felszínesen és hibásan tárja fel ezeket az ismereteit a beszélgetés során. Az összetartozás beszédkódjai egyebek között: a szakmai fogalmak, a szakma alapművei és szerzői, a szakma fontosabb képzőhelyei (közép- és felsőoktatási intézmények), a szakma hazai és nemzetközi rendezvényei, a szakmai tevékenységet folytatók egyesületei/szövetségei, illetve a különböző felügyeleti szervek.

Megjegyzem, hogy léteznek olyan vállalatok, ahol a(z írásbeli) kommunikáció hatékonyságának növelésére kidolgoztak és bevezettek olyan, néhány betűből álló mozaikszavakat, amelyek például az anyacég és a külföldi leányvállalatai közötti kommunikációt azzal teszik időben hatékonyabbá, hogy nem kell a levelezésekben, vagy beszámolókban kiírni a mozaikszavak jelentését, hiszen azok a vállalati beszédkódok mindenki által ismert halmazába tartoznak. Az ilyen mozaikszavak jelentésének ismerete és használata révén a *social engineer*ek sokkal könnyebben képesek a vállalat alkalmazottainak a bizalmába férkőzni.

2. tétel: egy beszédkód magában foglal bizonyos kulturális vonatkozású pszichológiai, társadalmi, retorikai különbségeket. A pszichológiai manipuláció során a megtámadott kommunikációs ágens viselkedésével, mondataival elárulja a szervezetben betöltött szerepét, sőt az esetek jelentős részében azt ki is hangsúlyozza. A manipuláció részeként e szerep megerősítése sikeresebbé teheti a támadást. A szociológiai megközelítésnél az egyén nemcsak magáról, hanem maga és a szervezet többi tagjának kapcsolatáról is ad információt. A *social engineer*ek szerint, ha az egyén tudatosan el akar határolódni a szervezettől, vagy annak bizonyos csoportjaitól (például mérnökök kontra fizikai munkások), akkor ezt a beszédkódokban is kifejezésre juttatja. Ennek felismerése révén a támadó olyan beszédkódokat alkalmazhat, amelyek segítségével könnyebben tud a megtámadott ágens bizalmába férkőzni (például „legalább mi, melósok tartsunk össze"). A retorikai megközelítésnél – igazodva Philip-

sen felvetéséhez – fontos a tekintély vizsgálata és a beszédkódok révén a megfelelő tekintélyviszony kialakítása a támadó és az áldozat között. Amikor a támadás során a támadó az adott szituációt valós időben elemzi, könnyen felméri, hogy inkább az egy csapatba tartozás (szociológia), vagy inkább az alá-fölé rendeltség (tekintély) elve szerint alakítsa-e ki a kommunikációs keretet. Utóbbinál például a segítséget kérő harmincas, dögös támadó nő kihangsúlyozza, hogy mennyire férfiasnak értékeli a manipulálandó biztonsági őrt.

3. tétel: a beszéd jelentősége függ a beszélő és a hallgató által használt beszédkódoktól, amelyeket abból a célból alkalmaznak, hogy segítségükkel létrehozzák és értelmezzék kommunikációjukat. Ezt a tételt némiképp át kell fogalmazni a *social engineering* típusú támadások elemezhetősége érdekében: a manipuláció technikáit jól ismerő támadó olyan keretet ad a beszélgetésnek, ahol akár közvetlen, akár közvetett irányító szerepben határozza meg a beszéd jelentőségét. A *social engineering* típusú támadásoknál a kialakított beszédaktusok bensőségesek, nyíltak, támogató jellegűek lehetnek. A bensőséges viszony rövid időn belüli kialakítása azért is fontos, mert ha a megtámadott ágens mindvégig távolságtartó marad, akkor nem vagy csak részben mondja el a megszerezni kívánt információkat. A nyílt kapcsolat keretében a támadó rugalmas, és úgy alakítja a beszélgetést, hogy ez a rugalmasság megváltoztassa az ágens esetleg merev hozzáállását. A *social engineer* a megtámadott ágens bizalmába tud férkőzni azáltal, hogy támogató jellegű kapcsolatot épít ki és tart fenn a beszédesemény során [például segítséget nyújt neki, vagy bizalmas(nak tűnő) információkat oszt meg vele].

4. tétel: a beszédkódot meghatározó fogalmak, szabályok, premisszák kibogozhatatlanul bele vannak szövődve magába a beszédbe. Az 1. tételnél leírtakat azzal szeretném itt kiegészíteni, hogy a szervezetek jelentős része nem kellő körültekintéssel szabályozza azt, hogy melyek azok az információk, amelyek bárki számára elérhetők a nyilvános platformokon (beleértve a munkatársak/vezetők Facebook-és LinkediIn-oldalait is). A beszédkód fogalmát ennél a tételnél vizsgálódásom fókuszában célszerű kiterjesztett formájában használni. A szervezet és a támadó közötti kommunikáció során elfogadjuk azt, hogy mindkét fél multiplatformos kommunikációt folytathat úgy, hogy a támadási szándék csak a *social engineert* jellemzi, illetve az információ átadásában harmadik, negyedik stb. fél, felek is részt vehetnek.

5. tétel: egy közös beszédkód mesteri alkalmazása elegendő feltétel ahhoz, hogy előre jelezzük, értelmezzük vagy kontrolláljuk a kommunikációs viselkedés érthetőségéről, tisztaságáról és moráljáról folyó diskurzust. Mivel a beszédkódok körébe tartoznak a verbális, nonverbális, illetve metakommu-

nikatív kódok is (a tétel eredeti értelmezésében elsősorban ez utóbbival foglalkozik a szerző), ezek ismerete az adott szituációban segíti a *social engineer*t, hogy megjósolja, illetve kellő szakmai tudás birtokában irányítsa is a beszélgetést úgy, hogy a megtámadott ágens ebből semmit ne vegyen észre.

Az öt tétel összefoglalva:

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 SPEAKING modell

Hymes a személyközi kommunikáció beszédeseményeinek bemutatására és elemzésére egy olyan modellt dolgozott ki, aminél a beszélő szó angol változatának (SPEAKING) egyes betűiből épül fel a modell a következők szerint:

– *Setting/scene* (beszédhelyzet): a jelenet fizikai körülményeinek (hely, idő) leírására szolgál.
– *Participants* (résztvevők): támadó(k), áldozat(ok), mellékszereplők (például többi kolléga, ügyfél).
– *Ends* (lezárások): melyek azok a célok, amelyeket a támadó el akar érni? Ezek rendszerint a következők: bizalmas/titkos információk megszerzése beszélgetéssel, elérni, hogy beengedjék a nyilvánosságtól elzárt részekre, kapcsolatot kialakítani és fenntartani a további támadások érdekében.
– *Act sequences* (cselekménysorozatok): hogyan épül fel a támadás, milyen kulturális közegbe helyezhető (például köszönés, búcsúzás).

– *Key* (kulcs): milyen verbális, nonverbális, esetleg metakommunikációs elemeket használ a támadó (például a szerepéhez illeszkedő ruházat és kiegészítők, beszédstílus).
– *Instrumentalities* (eszközök): ide soroljuk a kommunikációs csatornákat (szóbeli, írásbeli, telefonos, internetes, közösségi média), a beszéd aktuális formáját (nyelv, szaknyelv, dialektus), valamint a formális nyelvet is (például jogi nyelvezetű üzenet az Országos Rendőr-főkapitányságtól).
– *Norms* (normák): a támadó eldöntheti, hogy a támadást normaszegésre, vagy normakövetésre építi-e fel, illetve meg tudunk különböztetni eltérő érintkezési normákat is (hangos/halk beszéd, kézfogás, távolság, összenézés, megölelés stb.).
– *Genre* (műfaj): fontosabb műfajok lehetnek a tájékoztató, az általános/szakmai beszélgetés, az általános információ kérése/adása, a javaslat, a segítségkérés és -nyújtás, a flörtölés stb.

Tanulmányomban terjedelmi okokból eltekintek a modell részletes bemutatásától, mivel az megtalálható egyebek között Hymes[23], *Ray és Biswas[24], Zand-Vakili és társai[25], Matel[26],* illetve *Kollár[27]* írásaiban, így inkább három esettanulmányt mutatok be a modell gyakorlati felhasználását és hasznosságát szemléltetendő.

Három esettanulmány az elmélet bemutatására

A biztonsági ellenőrzés során a megadott szerepet játszó ellenőr (támadó) és az erről nem tudó munkatárs (áldozat) beszélgetéséről, tehát magáról a humán alapú *social engineering* típusú támadásról hang- és videofelvétel ké-

23 Dell Hymes: Models of the Interaction of Language and Social Life. In: John Gumperz – Dell Hymes (eds.): Directions in Sociolinguistics: The Ethnography of Communication. Holts Rinehart & Winston, New York, 1972, pp. 35–71.; Dell Hymes: Foundations in Sociolinguistics: An Ethnographic Approach. University of Pennsylvania Press, Philadelphia, 1974

24 Manas Ray – Chinmay Biswas: A study on Ethnography of communication: A discourse analysis with Hymes 'speaking model'. Journal of Education and Practice, vol. 2, no. 6, 2011, pp. 33–40.

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

26 Maldona Matel: "The Ethnography of communication". Bulletin of the Transilvania University of Brasov, vol. 2, no. 51, 2009

27 Kollár Csaba: Social engieering a gyakorlatban. Manipulációk értelmezése a SPEAKING modellben. JEL-KÉP, 2017/3.

szül, így rendelkezésre áll egy olyan nyersanyag, ami alkalmas lehet a tudományos igényességű és a gyakorlati életben is alkalmazható elemzésre, majd ennek alapján a biztonságtudatossági programok és tananyagok fejlesztésére. Az esettanulmányok megszervezésénél és elemzésénél *Horváth és Mitev*[28], *Dooley*[29] és *Klenke*[30] munkáira hagyatkozom. Az esettanulmányok elemzésénél két kérdésre keresem a választ: 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 feldolgozása után. Az adatgyűjtésre 2016 negyedik és 2017 első negyedéve között került sor egy kereskedelmi bank két-két helyszínén (egy budapesti központ, egy regionális/megyei igazgatóság, két kiemelt bankfiók). Mivel a kiválasztott helyszíneken voltak videokamerák (igaz, egy részüket nagyobb felbontásúra kellett cserélni), s előzetesen mikrofonokat is telepítettünk, így a támadás napjára rendelkezésre állt a hang- és videorögzítéshez szükséges technikai háttér. A támadást az ellenőr/auditor a megadott forgatókönyv szerint hajtotta végre, a felvételek elemzése előtt erről tájékoztatták az érintetteket (áldozatok), akik hozzájárultak ahhoz, hogy a felvételeket tudományos céllal elemezzék. Jelen tanulmányban három esetet ismertetek: pizzafutár az ügyfélpultnál, informatikus kolléga a központból, dohányzásra kijelölt hely. Azért esett a választás ezekre az esetekre, mert nagyon világosan és teljeskörűen be lehet mutatni az ellenőrzés során alkalmazott humán típusú *social engineering* támadást a SPEAKING modellben.

Pizzafutár az ügyfélpultnál

Beszédhelyzet

A beszédhelyzet külső időbeli határa, vagyis a támadás teljes időtartama és a térbeli határ is több részre osztható. A teljes időkeret tizenhárom perc volt, ebből a belső időhatár (vagyis, aminek az elemzése az esetleírásnál részletesebben szerepel) négy perc, ezt követte egy másik térben (folyosóról nyíló szoba/szobák) megvalósított adatgyűjtés (ez nem része az elemzésnek), ami hét perc, majd visszatérés az eredeti helyszínre, elköszönés és távozás (két perc). A külső térbeli határ a bankfiók ügyfélpultja és annak környéke. A tá-

28 Horváth Dóra – Mitev Ariel: Alternatív kvalitatív kutatási kézikönyv. Alinea Kiadó, Budapest, 2015

29 Larry M. Dooley: Case Study Research and Theory Building. Advances in Developing Human Resources, iss. 4, 2002, p. 335.

30 Karin Klenke: Qualitative Research in the Study of Leadership. Emerald Group, Bingley, 2008

madás szempontjából a külső térbeli határhoz tartozik az időjárás (borongós, esős idő), a belső térbeli határon a támadó nem változtatott, vagyis a beszélgetést mindvégig úgy irányította, hogy a banki munkatárs a helyén maradjon. A bankban több ügyfélpult volt, a támadó azt választotta ki, amelyiknél a számára optimális banki ügyintéző foglalt helyet (lásd később), s legközelebb volt a biztonsági őr által (elvileg) védett, a lezárt folyosóra nyíló ajtóhoz. A támadás délelőtt történt, a hónap elején (az eső ellenére is többen intézték a banki ügyeiket), az időjárás miatt az emberek hangulata nyomott volt.

Résztvevők

A támadó munkáját megkönnyítette, hogy a biztonsági őr nem volt a helyén. A résztvevőket a támadás szempontjából a következő csoportokba lehet sorolni:

– közvetett résztvevők: ügyfelek, banki alkalmazottak. A banki alkalmazottak kizárása fontos volt a támadás eredményessége szempontjából;
– közvetlen résztvevők: támadó, banki alkalmazott (ügyfélpultos).

A támadó szerepe: kinézetre pizzafutár (céges póló, pizzaszállító táska a kezében), aki elázott, s szeretne elmenni a mosdóba. Húsz év körüli, vékony testalkatú, szimpatikus fiatal.

Az áldozat: negyvenes évei közepén járó nő, akinek a feltételezés szerint hasonló életkorú gyereke/keresztgyereke van/lehet, mint a támadó.

Lezárások

A cél két, egymásra épülő részből tevődik össze. 1. elérni az áldozatnál, hogy engedje be a támadót az ügyfelektől elzárt részbe, ahol a mosdó található; 2. amint a támadó bejutott, szerezzen meg valamelyik munkatárstól bizalmas adatokat, információkat úgy, hogy az irodájából elhoz valamilyen „adathordozót" (például okostelefon, névjegyek, banki szerződések stb.). A támadás mindkét cél tekintetében megvalósult.

Cselekménysorozat

A cselekmény felépítése a következő: 1. az esőben elázott pizzafutár belép a bankfiókba; 2. sorszámot kér az automatából; 3. az automata egy másik ügyintézőhöz irányítja, de ezt nem veszi figyelembe; 4. amikor a kijelzőn a ki-

szemelt ügyintéző pultszáma megjelenik, a kezében hangsúlyosan mutatva a számát tartalmazó lapot, odalép az ügyintézőhöz, a pizzafutáros hordtáskát a széken hagyja. Megjegyzem, hogy itt annyiban szerencséje volt, hogy az az ügyfél, akit az automata a kiszemelt ügyintézőhöz irányított volna, szintén felállt a székről, de a támadó nonverbálisan jelezte, hogy hamar fog végezni, s azt is, hogy siet; 5. a támadó illedelmesen köszön az ügyintézőnek, beszélgetnek néhány mondatban az időjárásról, majd megemlíti, hogy még „pisilni sincs időm, annyi megrendelést kell ma kivinnem", majd szól egy mondatban arról, hogy egyetemista, tandíjra gyűjt, ezért dolgozik; 6. a támadó elmondja a kérését, miszerint szeretne elmenni a mosdóba, illetve megkéri az áldozatot, hogy addig vigyázzon a pizzaszállító táskára; 7. az áldozat először a szabályokra hivatkozik ugyan, de néhány megerősítő mondat után beengedi a támadót azzal a megjegyzéssel, hogy siessen, s addig vigyáz a pizzaszállító táskára. Megjegyzem, hogy a modell szerint idáig tartott a cselekménysorozat, amely után a támadó meg tudta szerezni a szükséges bizalmas/titkos adatokat, s fennakadás nélkül el is hagyta a helyszínt.

Kulcs

A támadó emblémái és kulturális szignáljai (nonverbális kódok) két archetípus köré épültek. A fő archetípus a pizzafutár volt, aki egy létező cég emblémájával ellátott pólóban, farmerban, tornacipőben, kezében pizzaszállító táskával jelenik meg a beszédhelyzetben. Az érzelmileg jobban megérintő (a verbális és nonverbális üzenetek kongruenciájára épülő) archetípus „az én egyetemista gyerekem is lehetne" volt. Itt a támadó – ahogy arra már utaltam – sikeresen alakította az esőben elázó, a tandíjáért dolgozó egyetemistát, aki életkorából adódóan akár az áldozat egyetemista gyereke is lehetne. A szemüveg, a szemüveg megtörlése, a nedves haj és póló tovább erősítette ezt a szerepet. A támadó kedves, illemtudó, hangszíne barátságos. A társadalmi közhelyek szintjén bebizonyítja (elsősorban az áldozatnak), hogy vannak még rendes, dolgos fiatalok. A banki ügyintéző archetípusa a távolságtartó, az ügyre fókuszáló dolgozó, akiben a támadó kulcsainak segítségével ezt az archetípust át tudja írni anyára, keresztanyára.

Eszközök

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

Normák

A támadó ráveszi áldozatát, hogy normaszegést kövessen el, vagyis hogy beengedje az ügyfelektől elzárt területre.

Műfaj

Segítségkérés/-nyújtás, rövid beszélgetés.

Az informatikus kolléga a központból

Beszédhelyzet

A támadás három beszédhelyzetből tevődik össze: 1. a személyes látogatást megelőzően, ebédidőben a támadó felhívja a vidéki központ/igazgatóság egyik osztályát azzal az ürüggyel, hogy a budapesti központ informatikai igazgatóságáról jön, mindjárt odaér, és mivel nincs helyismerete, ezért megkéri az áldozatot, hogy várja a bejáratnál. 2. A támadó megérkezik a vidéki központba, ahol a kollégák szeretettel fogadják. A támadás időkerete nem lényeges, mivel az információkat valamennyi – számára fontos – gépről meg tudta szerezni, illetve az áldozatok hozzáférésein keresztül el tudja érni a vállalati adatbázisokat is. Megjegyzem, hogy ha nem audit, hanem éles támadás lett volna, akkor a támadó kártékony kódokat is tudott volna telepíteni a gépekre (kihasználva az informatikai biztonsági réseket), az audit során azonban csak azt vizsgálták, hogy a *social engineering* támadás elérte-e a célját, vagyis hogy elhitték-e a kollégák, hogy a támadó a bank központjában dolgozó informatikus. Külső térbeli határnak jelen esetben a regionális központ/igazgatóság irodáit, belsőnek pedig az egyes áldozatok mikrokörnyezetét, vagyis az íróasztaluk és a számítógépük környezetét értem. 3. A támadó beszédhelyzetei az egyes áldozatokkal. Ezt az elemzésem szempontjából nem tekintem jelentősnek, mivel a dialógusok néhány egyszerű mondatra korlátozódnak, s ezekről nem is készült külön felvétel.

Résztvevők

Az első esettel ellentétben a résztvevőket másfajta szempontok szerint osztályoztam ennél a leírásnál:

– Az a kolléga, aki felvette a telefont (első beszédhelyzet). Az ő feladata az volt a támadásban, hogy még a támadó megérkezése előtt megerősítse a helyi kollégákat abban, hogy a pesti informatikus kolléga mindjárt itt lesz. Ezzel akaratán kívül eloszlatott minden esetlegesen meglévő fenntartást az idegen, soha nem látott támadó kapcsán.
– Helyi kollégák: áldozatok, akik természetes módon engedték a számítógépükhöz a támadót.
– Támadó. A támadónak az első két esethez képest nem csak humán alapú *social engineering* ismeretei vannak. Az archetípusa rendszergazda/informatikus, aki szemüveges, farmernadrágban, kissé gyűrött ingben, a nyakában a vállalat hamisított (színesben kinyomtatott) belépőkártyájával jelent meg. Előzetesen felkészült a vállalatból a vállalatról szóló nyilvánosan elérhető információk alapján (OSINT).

Megjegyzem, hogy a támadás sikeressége nagymértékben azon múlt, hogy a támadás napján a vidéki központ valamennyi informatikai munkatársa a budapesti központban egy konferencián vett részt. Mivel a bank támogatta ezt a konferenciát, így tudni lehetett, hogy a kollégák részt is vesznek rajta. A támadó felhívta előzetesen a szervezőket, akik elkotyogták, hogy a vidéki igazgatóság teljes létszámmal képviselteti magát.

Lezárások

A három beszédhelyzet célja rendre a következő: 1. telefonon bizalmat ébreszteni a kollégákban, hogy jön egy informatikus a központból, aki megszereli a gépeket; 2. megerősíteni a vidéki kollégákat abban, hogy a budapesti informatikus kolléga néhány beállítást hajt végre a gépeken, aminek következtében a gépek gyorsabbak lesznek; 3. az áldozatok számítógépéről és annak környezetéből megszerezni a szükséges belépési neveket/jelszavakat, illetve hozzáférni a banki adatbázisokhoz.

Cselekménysorozat

1. telefonos beszélgetés a vidéki igazgatóság egyik munkatársával. a) A támadó ebédidőben felhívja a bank vidéki igazgatóságának egyik osztályát, hogy rövidesen érkezik, de eltévedt. Mivel a nyilvános forrásokból megismerhető vállalati kultúra része, hogy a kollégák egymást tegezik, ezért a támadó is tegezi a kollégát. b) Elmondja, hogy a budapesti központból jön, mert a szá-

mítógépeken el kell végeznie néhány nagyon fontos beállítást, mindjárt odaér, s megkéri a kollégát, hogy mivel nem ismeri a helyszínt, várja a bejáratnál. 2. c) a támadó megérkezéséig a kolléga elmondja az osztály többi dolgozójának, hogy mindjárt megérkezik a budapesti informatikus kolléga (gyakorlatilag megismétli azt, amit a támadó neki mondott); d) a telefonos áldozat várja a bejáratnál; e) a recepciós kolléga a hamis belépő alapján feljegyzi a támadó adatait, s beengedi őt; f) a telefonos áldozat bemutatja a támadót az osztály többi munkatársának; g) a támadó még egyszer elismétli a látogatása célját (egy fontos beállítást kell elvégeznie az osztály valamenynyi számítógépén az új biztonsági protokollok életbelépése miatt). 3. h) a támadó leül az áldozatok számítógépéhez; i) megkéri őket, hogy lépjenek be az általuk használt adatbázisokba, illetve ellenőrizzék, hogy a támadónál lévő név/jelszó páros egyezik-e (természetesen nem egyezik, merthogy a támadó „véletlenül" egy másik listát hozott magával); j) mivel nem egyezik, ezért új nyilvántartó lapot készítenek, ahol megadják a szükséges adatokat; k) a támadó kihasználva a rendszer biztonsági réseit, az adatbázisok számára releváns tartalmát egy másik tárhelyre másolja.

Kulcs

A támadás során az alapvető kulcs a támadó rendszergazda/informatikus szerepének az eljátszása. A korábban leírt formai jegyek mellett fontos, hogy a támadónak legyen valódi informatikai tudása, illetve legalább alapszinten ismerje a bank működését és szervezeti kultúráját/stílusát. A támadó stílusa precíz és szakmaiságot tükröző („végre egy rendes rendszergazda"), aki készségesen válaszol a feltett kérdésekre (a kérdések kivétel nélkül a szövegszerkesztő és táblázatkezelő szoftverekkel, a levelezőrendszerrel, illetve a nyomtatással voltak kapcsolatosak. Ezek a kérdések szinte valamennyi cégnél előfordulhatnak, tehát nem tekinthetők iparág-, illetve ágazatspecifikusnak).

Eszközök

A kommunikációs csatorna a személyközi és a csoportkommunikáció során verbális és nonverbális. A támadás csatornái között megjelenik a telefonos is.

Normák

A támadó elsősorban a normakövetésre épít, kihangsúlyozva, hogy a beállítások utáni nap – amikor az új rendszer elindul – a gépek sokkal gyorsabbak lesznek, így a munka is hatékonyabbá és kényelmesebbé válik.

Műfaj

A támadás során több műfajjal lehet találkozni: telefonon általános információ adása, szakmai beszélgetés, segítségnyújtás.

Dohányzásra kijelölt hely

Beszédhelyzet

A dohányzásra kijelölt hely – a helyi adottságok figyelembevételével – olyan, rendszerint a szabadban található hely lehet, amit mindenféle engedély nélkül meg lehet közelíteni, illetve ott lehet tartózkodni. A bank székhelye ilyen volt. Az időbeli keretnél a támadás két részre bontható (az elemzésben részletesen csak az első rész szerepel): a dohányzás közbeni rész és a nyilvánosságtól elzárt részekbe (folyosó, irodák) történő bejutás jelenti a keret első, míg a bejutás után a kémkedés a második részt. Az időbeli külső határ tizenkét perc volt, mialatt részint a cigarettázás, részint az elzárt részekbe történő bejutás megtörtént. A külső térbeli határ a dohányzásra kijelölt helyet, a recepciós pultot, valamint a csak belépőkártyával megközelíthető területeket jelenti. A belső térbeli határnál a dohányzás helyszínén a „megszokott" körbeállás, a recepciós pult környékén a csoportos vonulás, az elzárt részekbe történt bejutás után pedig a szétválás, illetve közös liftezés volt a jellemző. Az eset tehát két beszédhelyzetet azonosít: 1. dohányzás közbeni eszmecsere; 2. proxemika segítségével történő bejutás.

Résztvevők

A támadásban a következő résztvevők/szerepek azonosíthatók:

– Aktív áldozatok, akik a dohányzásra kijelölt helyen cigarettáznak, s érdeklődve hallgatják a támadó rövid beszámolóját arról, hogy milyen új törvényi változások várhatók a bankszabályozás területén.

– Recepciós (passzív áldozat), aki nem figyel arra, hogy a banki belépőkártyával bíró kollégák közé keveredett a támadó, akit így tudtán kívül átenged a lezárt részekbe.
– Biztonsági őrök (passzív áldozat), akik nem figyeltek arra, hogy a csoporthoz egy idegen is csatlakozott.
– Támadó, aki a pénzügyi szervezetek felügyeletéért felelős hatóság munkatársának adta ki magát. Megjelenése: határozottságot és magabiztosságot, egyszersmind egyfajta barátságot is sugall. A dohányzásra kijelölt helyen lévő áldozatokkal (közel) azonos konzervatív, sötét színű öltönyt, fehér inget, nyakkendőt, bőrcipőt visel, kezében kisebb, bőr aktatáska. Nyakában a hatóság hamisított belépőkártyája, illetve van hamis névjegykártyája arra az esetre, ha az áldozatok közül valaki kérne tőle. Életkorát tekintve a harmincas évei elején jár.

Lezárások

A támadás célja a cigarettázás befejezése után a dohányosokhoz csapódva bejutni a csak a bank érvényes belépőkártyájának felmutatása után megközelíthető elzárt irodarészekbe.

Cselekménysorozat

A támadást megelőzően a támadó elkészíti a szükséges hamisított belépő-, illetve névjegykártyát. Előzetes megbeszélés szerint a támadó mindvégig tegezi az aktív áldozatokat. A cselekménysorozat fontosabb elemei a következők: 1. támadó megkérdezi, hogy a csoport ismeri-e azt a vezetőt, akinek a hivataltól egy nagyon fontos borítékot hozott (ehhez előzetesen olyan személyt választ ki, akit arcról felismer, s nem dohányzik legalább a támadás idején); 2. tüzet kér a dohányzásra kijelölt helyen cigarettázó banki alkalmazottaktól; 3. a támadó belefolyik a csoportos beszélgetésbe; és 4. felméri, hogy az aktuális csoportban ki a hangadó, illetve azt is, hogy miként tudja néhány perc alatt felhívni magára a figyelmet. Esetünkben ez az új banki szabályozásról szóló bizalmas információk megosztása volt, ami valóban felkeltette a csoporttagok érdeklődését. A dohányzás befejezése után 5. a beszélgetést folytatták; miközben 6. beértek a bank székhelyének az előcsarnokába. Az előcsarnokban a biztonsági őrök egymással beszélgettek, így 7. nem vették észre, hogy a csoporthoz egy idegen is csatlakozott. A recepciós nő – mert így szokás – 8. a pultból vezérelte azt a kaput, amelynél a kollégák ellenőrzés

nélkül át tudtak menni csoportosan. A támadó 9. bejutott a védett részekbe. Az audit során csak eddig vizsgáltuk a támadást, ha azonban éles támadás lett volna, akkor a támadó a bejutás után olyan irodákba megy be, ahonnan értékes/titkos információkat, vagy „csak" céges mobiltelefonokat lop el.

Kulcs

Ennél a támadásnál az adott szerep eljátszása mellett fontos tényező a proxemika. A csoporttal történő rövid (kb. tízperces) interakció során, a magasabb, így a támadót bejutáskor takaró áldozat, illetve a csoporton belüli tagok és a támadó közötti távolság helyes megválasztása révén valósítható meg a sikeres *social engineering* akció.

Eszközök

A kommunikációs csatorna a személyközi és a csoportkommunikáció során verbális és nonverbális.

Normák

A támadás alapvetően a normakövetésre épít. A banki alkalmazottak örömmel hallgatják a munkájukat segítő bizalmas információkat.

Műfaj

A támadás során több műfaj is megjelenik: az elején segítségkérés, majd felvilágosítás, illetve tanácsadás.

Összegzés

Az esettanulmányok feldolgozása után a következő konzekvenciák fogalmazhatók meg (második hipotézis). Az esettanulmányok rámutattak azokra a pszichológiai és kommunikációs csapdákra, amelyekbe mindannyian beleeshetünk. Ezek a csapdák nemcsak a vizsgált üzleti, hanem a magánéletben is megtalálhatók. Vannak olyan emberek, akik különösebb előképzettség nélkül is eredményesen képesek manipulálni a környezetükben élőket. A *social engineerek* erre a „szakmára" rendszerint tudatosan készülnek, s ha birtoká-

ban vannak is egy bizonyos manipulatív eszközkészletnek, szakmai ismereteiket folyamatosan fejlesztik. Jelen korunk programozói és hálózati ismeretekkel felvértezett hackereihez hasonlóan a humán alapú támadásokkal (vagy azzal is) foglalkozó *social engineerek* is egyre ritkábban dolgoznak szórakozásból, a háttérben szervezeti és kormányzati megrendelők állnak. A szervezetek informatikai sebezhetősége egyre nehezebb feladatot ad valamennyi szervezet számára. Ennek része, hogy a *social engineer* tudással felvértezett ellenőrök/auditorok a szervezetnél ad hoc jelleggel különböző teszttámadásokat hajtanak végre, és a tapasztalatok alapján a biztonsági előírásokra, képzésre, a tudatosság fejlesztésére vonatkozó ajánlásokat fogalmaznak meg, illetve programokat indítanak el. Meggyőződésem, hogy ebben a folyamatban Hymes SPEAKING modelljének használata többletinformációval gazdagítja az információbiztonsági eseteket/incidenseket elemző szakembereket. A tanulmányomban bemutatott, illetve további esettanulmányok elemzése után az első hipotézist, miszerint Hymes SPEAKING modellje alkalmas a humán típusú *social engineering* támadások elemzésére, szintén elfogadottnak tekintem.

IRODALOM

Aronson, Elliot: The Social Animal. Freeman, San Francisco, 1972

Atkinson, Rita L. – Atkinson, Richard C. – Smith, Edward E. – Bem, Daryl J.: Pszichológia. Osiris Kiadó, Budapest, 1997

Balázs István (szerk.): Pszichológiai lexikon. Magyar Könyvklub, Budapest, 2002

Dooley, Larry M.: Case Study Research and Theory Building. *Advances in Developing Human Resources,* iss. 4, 2002

Dreyfus, Suelette – Assange, Julian: Underground. Red Book, Sydney, 1997

Griffin, Em: Bevezetés a kommunikációelméletbe. Harmat Kiadó, Budapest, 2001

Haig Zsolt – Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest, 2005

Hewstone, Miles – Stroebe, Wolfgang – Codol, Jean-Paul – Stephenson, Geoffrey M. (szerk.): Szociálpszichológia európai szemszögből. KJK, Budapest, 1999

Horányi Özséb (szerk.): Kommunikáció I–II. General Press, Budapest, 2003

Horváth Dóra – Mitev Ariel: Alternatív kvalitatív kutatási kézikönyv. Alinea Kiadó, Budapest, 2015

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

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

Izsa Jenő: Nemzetbiztonsági alapismeretek. Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2009

Klenke, Karin: Qualitative Research in the Study of Leadership. Emerald Group, Bingley, 2008

Kollár Csaba: Social engieering a gyakorlatban. Manipulációk értelmezése a SPEAKING modellben. *JEL-KÉP,* 2017/3.

Lévay Gábor: OSINT (Open Source Intelligence). Nyílt információs hírszerzés. Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2006

Levy, Steven: Hackers: Heroes of the Computer Revolution. O'Reilly, New York, 2010

Matel, Maldona: "The Ethnography of communication". *Bulletin of the Transilvania University of Brasov,* vol. 2, no. 51, 2009

Mitnick, Kevin D. – Simon, William L.: A legendás hacker. A behatolás művészete. Perfact Kiadó, Budapest, 2006

Mitnick, Kevin D. – Simon, William L.: A legendás hacker. A megtévesztés művészete. Perfact Kiadó, Budapest, 2003

Oroszi Eszter Diána: Social Engineering: Az emberi erőforrás, mint az információbiztonság kritikus tényezője. Budapesti Corvinus Egyetem, Budapest, 2008. http://krasznay.hu/presentation/diploma_oroszi.pdf

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

Poulsen, Kevin: Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground. Broadway Paperbacks, New York, 2011

Ray, Manas – Biswas, Chinmay: A study on Ethnography of communication: A discourse analysis with Hymes 'speaking model'. *Journal of Education and Practice,* vol. 2, no. 6, 2011

Russell, Ryan: A Háló kalózai. Hogyan lopjunk kontinenst. Kiskapu Kiadó, Budapest, 2005

Shannon, Claude E.: The mathematical theory of communication. In: **Shannon, Claude E. – Weaver, Warren:** The Mathematical Theory of Communication. The University of Illinois Press, Urbana, 1964

Smith, Eliot R. – Mackie, Diane M.: Szociálpszichológia. Osiris Kiadó, Budapest, 2001

Sterling, Bruce: The Hacker Crackdown: Law And Disorder On The Electronic Frontier Mass Market. Bantam, New York, 1993

Zand-Vakili, Elham – Kashani, Alireza Fard – Tabandeh, Farhad: The Analysis of Speech Events and Hymes' SPEAKING. Factors in the Comedy Television Series: "FRIENDS". New Media and Mass Communication, no. 2, 2012