A social engineering humán alapú támadási technikái

Deák Veronika

Absztrakt

Napjainkra az infokommunikációs technológiák fejlődésének köszönhetően folyamatosan változnak a kibertámadások végrehajtásának módszerei is. A különféle belső és bizalmas információk megszerzését célzó támadások egyik válfaja a social engineering, amely az emberi tényező befolyásolására, manipulálására, valamint kihasználható tulajdonságaira épít. A támadások célpontja az ember, így hatékony védelem csak a biztonságtudatosság növelésével valósulhat meg, amelynek nélkülözhetetlen eleme a különböző támadási formák, módszerek ismerete. Éppen ezért jelen tanulmányban áttekintésre kerülnek a social engineering támadások humán alapú módszerei, illetve annak vizsgálata, hogy miért tekinthető kedvező célpontnak az emberi tényező.

Kulcsszavak: social engineering, kibervédelem, biztonságtudatosság, információbiztonság, emberi tényező

Abstract

Nowadays, thanks to development of information and communication technologies, methods of implementation of cyber attacks are constantly changing. A variant of attacks aimed at the acquisition of various internal and confidential information is social engineering that builds on influencing, manipulating and exploitable properties of human factor. The target of attacks is the human, so effective protection can only be achieved by increasing the awareness of security, where knowledge of various forms and methods of attacks is an indispensable component. That is why human-based methods and assessment of social engineering attacks are reviewed, and why the human factor is considered a favourable target.

Keywords: social engineering, cyber defence, security awareness, information security, human factor

Napjainkban az infokommunikációs eszközök fejlődésének köszönhetően a különböző támadási technikák fejlődése is megfigyelhető, amely miatt szükséges, hogy a különböző informatikai rendszerek mellett a biztonságtudatosságot is fejlesszük. Nem szabad azonban elfelejtünk, hogy a különböző informatikai eszközök segítségével végrehajtott támadások – a különféle belső és bizalmas információk megszerzése érdekében - sokfélék lehetnek és számtalan veszélyt rejthetnek magukban. A kibertámadások jelentős gazdasági, politikai, nemzetbiztonsági, de a társadalomra is kiterjedő káros következményt idézhetnek elő.

Éppen ezért az ilyen típusú támadások elleni hatékony védekezés egyik legfontosabb része a biztonságtudatosság fejlesztése az egyéneknél és szervezeteknél egyaránt, melynek célja, hogy az emberekben tudatosítsák az információbiztonság fontosságát és felkészítsék az őket fenyegető veszélyekre, illetve egy támadás megelőzésének és a védekezés lehetséges módszereire, eszközeire. Fontos, hogy - függetlenül attól, hogy az ember a munkája során használ-e számítógépet vagy sem, - mindenképpen szükséges az őket érintő kockázatokra, kihívásokra és fenyegetettségekre felhívni a figyelmet. Ahhoz, hogy a védekezés hatékony lehessen, elengedhetetlen a különböző támadási formák ismerete. A bizalmas információk megszerzését célzó támadások számtalan formája ismert, az egyik legjellemzőbb támadási módszer a social engineering.

A social engineering az emberi tényező kihasználható tulajdonságaira, az emberi hiszékenységre építő támadási forma, olyan technikák és módszerek összessége, amely az emberek befolyásolására, manipulálására alapozva teszi lehetővé bizalmas információk megszerzését, vagy éppen egy kártékony program terjedését és működését.[1]

A social engineering támadások során felmerülhet a kérdés, hogy a támadók miért pont az emberi tényezőt veszik célba, ahelyett, hogy a technológiai sérülékenységeket kihasználva jutnának bizalmas információkhoz? A humán tényező kedvező célpontnak tekinthető, hiszen használata kiterjed a különféle hardver és szoftver eszközökre, hozzáféréssel rendelkezik a különféle adatbázisokhoz, rendszerekhez vagy például ügyféladatokhoz.[2] A munkavállalók kapcsolatban állnak egymással, információkat osztanak meg egymással, valamint különféle belső és bizalmas információkkal rendelkeznek, amelyek a támadók számára értékesnek tekinthetőek. A belső és bizalmas információkat érdemes különválasztani egymástól, hiszen a

[1] Harl, G. (1997): People Hacking - The Psychology of Social Engineering, http://www.psihoworld.co.ba/The%20Psychology%20of%20Social%20Engineering.pdf (2017.02.16.)
[2] Oroszi Eszter: Social Engineering, 2008, p. 12. http://krasznay.hu/presentation/diploma_oroszi.pdf (2017.02.18.)

belső információk nem minden esetben tekinthetők bizalmas információknak. A belső információk nem titkosnak minősített információk, ennek ellenére mégis az adott szervezet dolgozóira vonatkoznak, éppen ezért nem javasolt megosztani idegenekkel, hiszen az ilyen adott közösségre érzékeny információk birtokában egy támadó könnyen megszemélyesíthet egy kitalált személyt, aki az adott szervezet egy új tagja. Az ember ideális célpontnak tekinthető továbbá a kihasználható tulajdonságai miatt. Ezek olyan tulajdonságok, amelyek mindenkiben megtalálhatóak, nem mindegyik és nem ugyanolyan szinten, de jellemzőek az emberi tényezőre. Ilyen tulajdonságok például a segítőkészség, naivitás, kíváncsiság, nyitottság, befolyásolhatóság, érdeklődés, fáradtság vagy túlterheltség. Vannak olyan kiszámítható tulajdonságok is, amelyek jelentősen kapcsolódnak az áldozat munkahelyéhez is, ettől függ kialakulásuk, ilyen például, hogy ha valaki napi rutin munkát végez, minden nap ugyanolyan típusú problémát old meg, akkor sokkal nehezebb tesz különbség egy napi rutin feladat és a támadó kérése között. Ilyen tulajdonságnak tekinthető még az elégedetlenség, a lefizethetőség vagy például a megzsarolhatóság is, hiszen ha a munkavállaló nem elégedett a munkájával, (esetleg a munkakörnyezetével, megbecsülésével vagy például a fizetésével) akkor a támadó akár lefizetheti vagy befolyásolhatja is az áldozatát, bizalmas és belső információk kiadása érdekében. A támadó számára az is előnyös lehet, ha a kiszemelt áldozata szabadságon vagy betegállományban van, hisz ilyenkor a helyettesítő kollégának azt is mondhatja, hogy a betegállományban vagy szabadságon lévő személy ígérte meg neki bizonyos információk kiadását, így ha a helyettesítő munkavállaló nem ellenőrzi ezt le, a támadó értékes információkkal gazdagodhat. Vannak olyan esetek, amikor az felhasználó szakképzetlenségét, jelszóhasználatát, a biztonságtudatosságának hiányát vagy a hanyagságát, illetve az ezekből adódó mulasztásokat használja ki a támadó. Éppen ezek miatt a social engineer támadások jelentős része csak akkor lehet sikeres, ha a felhasználók nem biztonságtudatosak, nem ismerik a megfelelő biztonsági eljárásokat, követelményeket, technikákat. Nem szabad elfelejteni, hogy a hagyományos biztonsági megoldások (tűzfal, vírusirtó programok, behatolás érzékelő és megelőző rendszerek stb.) nem nyújtanak teljes körű védelmet, minden esetben figyelemmel kell lenni az emberi tényező biztonságtudatosságára is. Hiszen a biztonsági technológiák fejlődésével a technológiai sebezhetőség csökken, emiatt a támadók pedig inkább az emberi tényezőt veszik célba a bizalmas információk megszerzése érdekében. Éppen ezért hatékony védelmet csak a technológiai megoldások és a biztonságtudatos felhasználó együtt jelent, aki betartja a biztonsági irányelveket és szabályokat, illetve megérti, hogy mások hogyan akarják befolyásolni bizalmas és belső információk megszerzése érdekében. Az áldozat személyét

illetően fontos megemlíteni, hogy függetlenül attól, hogy az állami vagy üzleti szféráról van-e szó, bárki lehet célszemély.

A social engineering támadásokat két csoportba sorolhatjuk. Elhatárolunk humán alapú és IT alapú, vagyis az informatikai eszközök segítségével végrehajtott támadásokat. Mindkét támadási típus középpontjában az emberi tényező befolyásolása áll, függetlenül attól, hogy a leendő áldozat használ-e valamilyen infokommunikációs eszközt vagy sem. Jelen tanulmányban a humán alapú módszerek bemutatását végzem el, míg az IT alapú támadások egy másik cikk részét képezik

A humán alapú támadások végrehajtásához nem szükséges informatikai szaktudás, bárki által kivitelezhető, azonban előzetes megfigyelést és felkészülést igényel. A támadónak a humán alapú támadások esetében nehezebb dolguk van, hiszen ezeket a támadások a legtöbb esetben szemtől-szemben kell végrehajtaniuk, a személyes kontaktus miatt a lebukás veszélye is nagyobb.

A humán alapú támadások számos alternatívája ismert. Ilyen támadási módszer például a bejutás az épületbe. Ez többféle módon történhet, az egyik ilyen technika a „piggybacking”[3], amely más jogosultságának a felhasználásával történik. Ebben az esetben a támadó megpróbálja rávenni a célszemélyt hogy a saját jogosultságával, például a belépőkártyáját kétszer lehúzva engedje be őt az épületbe, így a rendszerben úgy jelenik meg, mintha a munkatárs kétszer lépett volna be. Ez általában úgy történhet meg, hogy a támadó új munkatársnak adja ki magát vagy eljátssza, hogy otthon hagyta saját belépőkártyáját. Az épületbe való bejutás történt a „tailgating”[4], vagyis a szoros követés módszerével. Ebben a módszerben a támadó előzetesen megvizsgálja a vendégek, különböző csoportok érkezésének rendjét, kapnak-e belépőkártyát, ha esetleg valamilyen rendezvényt tartanak, akkor hogyan léptetik be a vendégeket, egyáltalán beléptetik-e őket, vagy csak kinyitják számukra a belépő kapukat, és így gyakorlatilag azonosítás nélkül jutnak-e be az épületbe. Az előkészületek során a támadónak azt is fel kell mérnie, hogy milyen csoporthoz fog csatlakozni, mivel a bejutáshoz magával kell vinnie a különböző felszereléseket, hiszen nem mindegy, hogy milyen típusú csoporthoz csatlakozik, esetleg egy takarítóbrigádhoz, vagy építőipari munkásokhoz, illetve például egy megbeszélésre vagy tárgyalásra érkezik-e a támadó. Ezt

[3] Sörös Tamás et al.: Social engineering a biztonságtechnika tükrében, 2013, p. 16. http://www.uni-obuda.hu/users/horvath.zsolt.laszlo/_szakirodalom/Inform%C3%A1ci%C3%B3biztons%C3%A1g/TDK-Social_Engineering-Soros-Vaci_orszagos.pdf (2017.02.18.)

[4] Sörös Tamás et al. i.m. p. 15.

követően a támadó érkezéskor egy csoporthoz csatlakozik, és úgy tesz, mintha annak tagja lenne, abban az esetben, ha az adott csoport túl kicsi, - ezáltal nagy valószínűséggel mindenki ismeri egymást - a támadó úgy is tehet, mintha a csoport egy elkésett tagja lenne.

A bejutás történhet hamis belépőkártya használatával, amely az előzőhöz hasonlóan szintén komoly előkészületet igényel, hiszen, ha beléptető rendszer van az adott szervezetben, akkor speciális technika segítségével lehet csak a kártyákat hamisítani. Abban az esetben, ha nincs beléptető rendszer, akkor a támadónak a kártyát előzetesen meg kell vizsgálnia, illetve lemásolnia, azt remélve, hogy a biztonsági őr úgy sem nézi meg a szervezet összes alkalmazottjának a belépőkártyáját közelről. [5]

Fontos megjegyezni, hogy ha egy támadó bejut a szervezet épületébe, nem csak bizalmas és belső információk birtokába juthat, hanem például rongálhatja eszközeinket, adatállományokat törölhet vagy megsemmisíthet, illetve belső és bizalmas információkat továbbíthat saját magának, átvizsgálhatja a szemetesünket, kártékony programokat (pl. keylogger[6]) telepíthet eszközeinkre, eltulajdoníthat tárgyakat, de akár meg is figyelheti a munkakörnyezetünket. Ez utóbbi azért tekinthető veszélyesnek, mert például az íróasztalunkon számos személyes információt tárolunk, legyen akár az egyik fénykép a családunkról, egy személyes bejegyzés a naptárunkban elfoglaltságainkról, bizalmas információkat tartalmazó dokumentum vagy akár egy feljegyzett jelszó. Éppen ezért fontos, hogy az értékes bizalmas információkat tartalmazó dokumentumokat zárt helyen tartsuk.

Az egyik leggyakoribb social engineering technika a segítségkérés, amely során a támadónak nincs szüksége komoly előkészületekre, szimplán elég, ha csak megkérdezi a célszemélytől a kívánt információt, vagy segítséget kér tőle. Sok esetben a támadók a rutin munkát végző, help-desken, ügyfélszolgálaton, vagy recepción dolgozó munkavállalókat veszik célba, azt remélve, hogy ők azok a személyek, akik napról-napra ugyanolyan típusú feladatokat látnak el, hasonló kérésekkel találkoznak nap, mint nap, így ők azok, akik nehezebben szűrik ki a gyanús megkereséseket, hiszen a napi rutin munka mellett nem biztos, hogy észreveszik, hogy egy támadással állnak szemben.[7] A támadás úgy is megtörténhet, hogy a támadó valakinek a bőrébe bújik, például egy új munkatársába, ezzel hatva a célszemély segítőkészségére, hiszen az emberek általában szívesebben segítenek akkor, ha egy rászorulónak van szüksége segítségre, így mikor egy új munkatárs kér segítséget az áldozat könnyen beleképzeli magát a

[5] Oroszi 2008, i. m. pp. 15-16.

[6] Olyan a billentyűzet naplózására is alkalmas program, amely rögzíti a felhasználó által begépelt karaktereket és rendszeresen pillanatfelvételt készít a számítógép képernyőjéről.

[7] Sörös Tamás et al. i.m. p. 14.

helyzetbe, hisz egyszer ő is volt kezdő. Komoly felkészülést ez a módszer nem igényel, azonban vannak olyan esetek, amikor a segítségkérés előtt a támadónak el kell sajátítania az adott szervezetben használatos szakkifejezéseket, hogy ezzel bizalmat keltsen az áldozatban, azáltal, hogy valóban az, akinek mondja magát, hisz ismeri például a szakzsargont vagy a szervezet összetételét, felépítését.

A segítségkérés fordított változata a „segítség nyújtása", mely során a célszemély kér segítséget a támadótól. Sok esetben ez úgy valósul meg, hogy a támadó előzetesen egy problémát generál áldozatának, így amikor a célszemély segítséget kér a támadótól már nem kell bebizonyítania hitelességét, csupán el kell hárítania a fennálló problémát. [8]

A humán alapú módszerek csoportjába sorolható a jelszavak kitalálása is. Ebben az esetben a támadó a felhasználók figyelmetlenségének és hanyagságának köszönhetőem tudja kitalálni a jelszavakat, mert például a célszemély nem változtatta meg az alapértelmezett jelszót, saját személyére utaló jelszót adott meg, vagy feljegyezte valahova azt, amit a támadó a támadás előtt megtalált. Vannak olyan esetek, amikor a felhasználók nem változtatják meg az alapértelmezett jelszavukat, amely azért problémás, mert sokak számára ismertek ezek a jelszavak, amely lehet például a „password", 1234, 0000, vagy akár a születési dátum is, valamint az alapértelmezett jelszavak számos változata az internetes keresőmotor segítségével is könnyedén megtalálható.[9] A személyünkre utaló jelszavak azért jelentenek könnyebbséget a támadónak, hiszen ha ilyen jelszót adunk meg – legyen az például a háziállatunk, hobbink, gyermekünk neve, vagy a születési dátumunk – ezek kis utánajárással, például a közösségi oldalunkat megvizsgálja könnyen kideríthetők. A jelszavak harmadik csoportjába a túl bonyolult jelszavak tartoznak, amikor a felhasználó túl bonyolult jelszót talál ki, például többféle karakterből és írásjelből álló jelszót választ, amit azonban a megjegyzés nehézsége miatt általában feljegyez valahova, amelyet a támadó könnyedén megtalálhat.

A humán alapú technikák csoportjába sorolható az „identitás lopás", vagyis a megszemélyesítés módszere, mely során a támadó egy másik személy bőrébe bújik. Ez a személy lehet kitalált vagy valós személy is, a lényeg, hogy a támadó úgy választja ki az adott szerepkört, hogy az a legjobban illeszkedjen hozzá, ezáltal lesz hiteles a szerepe. A támadó megszemélyesítheti a kiszolgáló személyzet tagjait, lehet takarító vagy karbantartó, amely azért előnyös mert nem valószínű, hogy minden takarítót vagy karbantartót ismerünk a

[8] Kevin D. Mitnick: legendás hacker. A megtévesztés művészete. Perfact-Pro, Budapest, 2003, pp. 55-75.
[9] Sörös Tamás et al. i.m. pp. 13-14.

szervezetben.[10]A támadó egy futár bőrébe is bújhat, azonban ennél a módszernél fontos, hogy előzetes terepszemlét kell tartania a támadónak, hogy felmérje az adott szervezet hogyan fogadja a különböző futárokat, beengedik-e vagy sem. A támadó kiadhatja magát új munkatársnak vagy a szervezeten belül egy másik részlegen dolgozó alkalmazottnak is, mely előnye szintén hasonló az előbbihez, miszerint nem biztos, hogy minden munkatársat ismerünk, illetve minél nagyobb egy szervezet annál kisebb az esélye, hogy mindenkit ismerünk. További előnye még a szervezeten belüli alkalmazott megszemélyesítésének, hogy az áldozatban egyfajta bizalmat kelt, hogy a támadó a szervezet tagja, ezáltal nem feltétlenül kérdőjelezi meg hitelességét, így mindenféle gyanakvás nélkül nyújthat betekintést a különféle belső és bizalmas információkhoz. A támadó a rendszergazda vagy informatikai munkatárs bőrébe is bújhat, amely azért célszerű a támadó szempontjából, mert az alkalmazottak jelentős része csak felhasználói szinten ért a különböző infokommunikációs eszközökhöz, így ha a támadó elhiteti az áldozatokkal, hogy ő a rendszergazda, használó az informatikai szakkifejezéseket, akkor nagy valószínűséggel nem kérdőjelezi meg a támadó hitelességét.[11] A támadó ezen kívül a szervezetbe érkező vendéget is megszemélyesíthet. Ez a vendég lehet például egy hallgató, aki szakdolgozatot ír, és a konzulenséhez érkezett, egy újságíró, egy másik szervezet alkalmazottja vagy vezetője, aki egy fontos megbeszélésre érkezett vagy akár egy állásinterjúra érkező személy is. Ebben az esetben a támadó előzetesen felkeresi a szervezet egyik alkalmazottját, hogy legyen a konzulense vagy például egy interjút szeretne vele készíteni, és mivel sok esetben a célszemélyek segítőkészek, ezért fogadni is fogják a támadót.[12] Ennél a támadási módszernél a problémát az okozza, hogy az adott interjú elkészítése után sok esetben nem kísérik ki az interjút készítő támadókat, így felügyelet nélkül az épületben tartózkodva számos belső és bizalmas információ birtokába juthat a támadó. Ezen kívül a támadó, - ha már bent van az épületben - könnyen más bőrébe is bújhat, amely segítségével szintén számos bizalmas vagy belső információt szerezhet meg, vagy akár még közelebb kerülhet a célszemélyhez. A megszemélyesítés célpontja egy ellenőr vagy auditor is lehet, aki például egy rövid interjút készítenek az egyik alkalmazottal, hogy hogyan használják és alkalmazzák a különféle szabályzatokat, előírásokat, illetve akár a fizikai biztonsági intézkedésekről is kérdezheti a támadó a célszemélyt, amely segítségével újabb értékes információhoz juthat. A korábban említett esetek mellett a támadó egy már elhunyt

[10] Sörös Tamás et al. i.m. p. 10.
[11] Sörös Tamás et al. i.m. p. 10.
[12] Oroszi Eszter: Social engineering támadási technikák. Avagy a végső megoldás: a felhasználó. http://www.securinfo.hu/termekek/it-biztonsag/1295-social-engineering-tamadasi-technikak-avagy-a-vegso-megoldas-a-felhasznalo.html (2017. 02.26.)

személy bőrébe is bújhat, ezt a technikát „thombstone theft”-nek[13] is nevezik, amely azért ideális a támadó számára, mert a halál beállta után nem azonnal, illetve nem automatikus törlődnek az elhunyt hozzáférési jogosultságai a különböző rendszerekhez, valamint adatbázisokhoz. Elhunyt személy identitás lopása úgy is történhet, hogy a támadó kiválaszt egy már gyerekkorában elhunyt személyt, akinek az identitását felhasználják, adataira hamis iratokat készítenek, és így próbálnak bejutni az adott szervezetbe. A hozzáférési jogosultság kapcsán érdemes megemlíteni azt is, hogy sok esetben, ha egy alkalmazottat elbocsátanak vagy felmond, akkor is visszaélhet ezzel a támadó, hisz ilyenkor sem rögtön törlődnek a volt munkatárs hozzáférési jogosultságai.

További humán alapú social engineering technika a „dumpster diving”[14], vagyis a kuka átvizsgálása, mely során a támadó valamely korábban ismertetett technika segítségével bejut az épületbe, ezt követően pedig átvizsgálja a szemetesünket. A kukánk számos értékes információt tartalmazhat, például személyes adatokat, kinyomtatott munkahelyi levelezést, vagy akár jelszót tartalmazó cetlit, de ezeken kívül számos olyan belső és bizalmas információk birtokába juthat, amely segítséget nyújthat a támadó számára zsaroláshoz, vagy a kuka tulajdonosának megszemélyesítéséhez is.

Humán alapú módszernek tekinthető a „shoulder surfing”, másnéven a váll szörfölés technikája, amely során a támadó úgy szerzi meg például a célszemély azonosítóját, jelszavát, esetleg pénzfelvételnél a PIN kódját, hogy egyszerűen csak átnéz a válla felett, miközben az áldozat begépeli azt. A technika előnye, hogy a támadónak nem kell az áldozat bizalmába férkőznie, elég csak fizikálisan a közelébe kerülnie, hogy könnyen kifigyelhesse az azonosító vagy éppen jelszó begépelését.[15]

Fontos megemlíteni, hogy napjainkra a közösségi média a social engineer támadások legfőbb eszközévé vált, jelentőseb megkönnyítve a támadások kivitelezését. Információszerző szerepe van, a támadó számtalan hasznos dolgot megtudhat a célszemélyről, az elérhetőségeit, személyes adatait, érdeklődési körét, illetve sokszor azt is, hogy leendő áldozata éppen hol van, kivel és mit csinál. Éppen ezért fontos a felhasználókban a biztonságtudatosság növelése, ezen belül a különböző közösségi oldalak adatvédelmi beállításainak megfelelő alkalmazása, hogy ezáltal jelentősen csökkenthessük a támadók által megszerezhető információk körét. A támadók információszerzése történhet az OSINT (Open Source Intelligence), vagyis a nyílt

[13] Sörös Tamás et al. i.m. p. 12.
[14] Oroszi 2008, i.m. pp. 37-38.
[15] Oroszi 2008, i.m. pp. 38.

forrású információszerzés segítségével is, amely során a támadó a nyilvánosan elérhető forrásokból fér hozzá a számára szükséges információkhoz. Nyílt forrásnak tekinthetők a hagyományos média (elektronikus és nyomtatott), könyvtárak anyagai, tanulmányok, nyilvános konferenciák előadásai, rádió- és televízióadások, fényképek, reklámanyagok, illetve az Internet is. A támadók számára az OSINT és a közösségi média általi információszerzés is kedvező, hisz ezek segítségével kis költséggel nagy mennyiségű információ szerezhető meg.[16]

Többféle humán alapú social engineering technika is tökéletesen szemléltethető a 2017-es ProDay Nemzeti Kiberversenyen zajlott események által. A ProDay 2017 egy informatikai biztonsági rendezvény, amely elsődleges célja a kiberbiztonsági ismeretek és tudatosság növelése, a támadó és védekező technikák oldaláról vizsgálódó prezentációk és workshopok kíséretében. A Nemzeti Kiberverseny egy olyan forgatókönyv alapú stratégiai döntéstámogató szimuláció, mely során a csapatok megvitatják a lehetséges stratégiai és taktiai döntéseket, melyeket egy jelentős kibertámadást követő napon kell meghozniuk.[17]

Számos jel utal arra, hogy a versenyen akár egy social engineering támadás kísérletet is végrehajthattak. Nem azt állítom, hogy az egy kísérlet volt, de vannak ráutaló jelek, így akár az is lehetett volna. Az első ilyen jel a tárgynyereményekhez szolgáló adatlapok kitöltése. A rendezvényen tárgynyereményeket is kisorsoltak, amelyeket adatlapok kitöltésével lehetett megnyerni. Az adatlapokon a regisztrációhoz általában szükséges adatok, mint például a név, beosztás, cím, elérhetőség, szervezet szerepeltek, azonban ezeken kívül olyan adatokat is elkértek, amelyek nem indokoltak egy pár ezer forintos tárgynyeremény átvételéhez. Ilyen szokatlan adatok voltak például a személyi igazolvány szám vagy például a ruhaméret, amelyek semmiképpen sem szükségesek a nyeremények kisorsolásához. Az adatlapot dekoratív hostess lányok segítségével lehetett kitölteni. Számtalan social engineering technika alapja a vonzó, dekoratív megjelenés általi befolyásolás, arra alapozva, hogy a támadásra utaló jelek háttérbe kerülnek a külső tulajdonságoknak köszönhetően. A social engineering támadások az ember kihasználható tulajdonságaira építenek, így például a naivitásra és a befolyásolhatóságra is. Abban az esetben, ha a szervezők egy kísérlet részének szánták volna a nyereményjáték adalapjainak kitöltését, a befolyásolhatóság tökéletes eszközét szolgálták volna a dekoratív hostessek. A hostessek befolyásolás eszközeként használásának célja, hogy

[16] Bányász Péter: A közösségi média, mint a nyílt forrású információszerzés fontos területe, in: Nemzetbiztonsági Szemle (online) III: (2) pp. 23-24. (2015)
[17] https://blackcell.pro/ (2017.02.28)

a férfiak nem az adatlap segítségével kért adatokra koncentráljanak, hanem a vonzó és mosolygós hostessekre. Ennek segítségével például az egyébként furcsának tűnhető adatok kérésére is könnyebben válaszolnak a leendő áldozatok. A tárgynyeremény, mint például egy pendrive, akár a baiting technika egyik eszköze is lehetett volna. A baiting technikája, amely magyarul szétszórást jelent, amikor is a támadó egy fertőzött adathordozót (pendrive, CD, DVD, SD kártya) „véletlenül" elhagy, és amikor a gyanútlan felhasználó megtalálja azt, csatlakoztatja a számítógépéhez az eszközt, hogy kiderítse, kié lehet, vagy mit tartalmaz az eszköz, ezt követően pedig már települ is a kártékony kód a saját számítógépére. A rendezvény eseményei közé tartozott a borkóstoló is, amely szintén segítséget nyújthat egy social engineering támadás kivitelezésese során, hiszen ha a leendő áldozatok alkoholt fogyasztanak – annak mértékétől függően – készségesebben rendelkezésre bocsájtják a támadó által megszerezni kívánt bizalmas információkat. Az alkoholos befolyásoltság és a szexualitás együttes kihasználása pedig még valószínűbbé teszi, hogy a rendezvény résztvevői még olyan adatokat is megadnak a lap kitöltése során, amilyeneket egyébként normál esetben nem tennének meg.

Összességében a humán alapú social engineering technikák tökéletesen ábrázolják, hogy kis ráfordítással (utánajárással, előkészületekkel) hogyan lehet a manipuláció eszközével bejutni egy épületbe és bizalmas információkat megszerezni. Éppen ezért kiemelkedő jelentőségű az alkalmazottak biztonságtudatosságának növelése a social engineering támadások bekövetkezésének valószínűségének csökkentése érdekében. Ahhoz, hogy a humán tényező felkészült legyen az ilyen támadásokkal szemben, szükségszerű, hogy felismerje azt. Az alkalmazott csak akkor tudja, hogy az adott segítségkérés nem csak egy szimpla segítségkérés, hanem egy social engineering támadás, ha tudatában van annak, hogy milyen támadások léteznek, illetve, hogy a social engineer hogyan, milyen eszközök és módszerek segítségével képes befolyásolni az embereket.

Felhasznált irodalom

- Bányász Péter: A közösségi média, mint a nyílt forrású információszerzés fontos területe, in: Nemzetbiztonsági Szemle (online) III: (2) pp. 21-36. (2015)
- Harl, G. (1997): People Hacking - The Psychology of Social Engineering, Forrás:http://www.psihoworld.co.ba/The%20Psychology%20of%20Social%20Engineering.pdf (2017.02.16.)
- Oroszi Eszter: Social Engineering, 2008, Forrás:http://krasznay.hu/presentation/diploma_oroszi.pdf (2017.02.18.)
- Sörös Tamás et al.: Social engineering a biztonságtechnika tükrében, 2013, Forrás:http://www.uni-obuda.hu/users/horvath.zsolt.laszlo/_szakirodalom/Inform%C3%A1ci%C3%B3biztons%C3%A1g/TDK-Social_Engineering-Soros-Vaci_orszagos.pdf
- Kevin D. Mitnick: legendás hacker. A megtévesztés művészete. Perfact-Pro, Budapest, 2003
- Oroszi Eszter: Social engineering támadási technikák. Avagy a végső megoldás: a felhasználó. http://www.securinfo.hu/termekek/it-biztonsag/1295-social-engineering-tamadasi-technikak-avagy-a-vegso-megoldas-a-felhasznalo.html (2017.02.26.)
- https://blackcell.pro/ (2017.02.28)