Számítógép alapú social engineering támadási technikái

Deák Veronika

Absztrakt

Rohamosan változó világunkban az egyre újabb és újabb számítástechnikai és elektronikai eszközök a mindennapjaink részeivé váltak. A különböző infokommunikációs eszközök, illetve az információs rendszerek megjelenésének és fejlődésének köszönhetően a támadók egyre fejlettebb és hatékonyabb módszereket alkalmaznak. A social engineering a bizalmas információk megszerzésére irányuló támadási forma, amely a technológiai sérülékenységeket és az emberi tényező gyengeségeit együttesen használja ki. A hatékony védelem biztosítása érdekében nélkülözhetetlen a biztonságtudatosság kialakítása, amelynek központi eleme a különféle támadási formák ismerete, ezért jelen tanulmányban áttekintésre kerülnek az IT alapú social engineering támadási módszerek. A különböző IT alapú támadások módszereit megismerve jelentősen tudjuk csökkenteni a ránk bízott információk kiszivárgását és illetéktelen felhasználását.

Kulcsszavak: social engineering, IT alapú támadások, információbiztonság, kibervédelem

Abstract

In our rapidly changing world, newer and newer computing and electronic devices have become parts of our daily lives. Due to the variety of information and communication technology and development and design of information systems, attackers employ more advanced and more effective methods. Social engineering is an attack focused on obtaining confidential information, which exploits vulnerabilities of technology and weaknesses of human factor together. To ensure effective protection it is essential to provide security awareness, where knowledge of the various forms of attack is a principal component, so in the present methods of IT bases social engineering attacks are reviewed. Learning about different methods of IT-based attacks, we significantly decrease leakage and unauthorized use of the information entrusted to us.

Keywords: social engineering, IT-based attacks, information security, cyber defence

Rohamosan változó világunkban az infokommunikációs eszközök, illetve az információs rendszerek fejlődésével együtt a különböző visszaélések és támadások módja is jelentős fejlődésen megy keresztül. Napjainkban információs társadalomban élünk, mely azt jelenti, hogy az információ központi szerepűvé válik, meghatározza az emberi kapcsolatokat, intézményeket és a kultúrát is, ezáltal az információ előállítása, elosztása, terjesztése, használata-, és kezelése jelentős

gazdasági, politikai és kulturális tevékenység.[1] Az információs társadalom működésének egyik alapja az infokommunikációs eszközök. A különböző infokommunikációs és elektronikai eszközök tárháza szinte végtelen, és az idő előrehaladtával folyamatosan jelennek meg új- és új eszközök, amelyek esetében nem szabad elfelejtenünk, hogy nem csak előnyökkel járnak, hanem számos veszélyt is rejthetnek magukban. Éppen ezért fontos, hogy megvédjük a bizalmas adatokat és információkat a jogtalan hozzáféréstől, ehhez pedig mindenképpen szükséges tudatosítani magunkban, hogy milyen veszélyek várhatnak ránk, és ezek ellen hogyan védekezhetünk. Kiemelendő, hogy a social engineering támadások az állami és nem állami szerveket egyaránt célozzák, valamint a katonai és nemzetbiztonsági életben is gyakran előforduló támadási technikának tekinthetők. A digitális hadszíntéren[2] zajló social engineering támadások sok esetben már a nagyhatalmak között zajló „stratégiai információs háború" részét is képezik, emiatt fontos, hogy a támadásokat felismerjük és ellenük hatékonyan védekezni tudjunk.[3]

E tanulmány előzményéül szolgáló cikkemben[4] megfogalmaztam, hogy a social engineering a befolyásolás és a manipuláció eszközével megtéveszti, valamint kihasználja az embereket, az információszerzés érdekében. Veszélyes támadási formának tekinthető, hiszen célpontja az ember, éppen ezért a védekezés nélkülözhetetlen eleme a támadási módszerek és technikák ismerete, ugyanis kellő felkészüléssel, illetve a biztonságtudatosság kialakításával jelentősen csökkenthető az ilyen típusú támadások bekövetkezésének valószínűsége.

Az IT alapú támadások esetében a támadó valamilyen informatikai eszköz segítségével próbálja meg félrevezetni az áldozatát. Ez a támadási forma kifejezetten kedvező a támadó számára, hiszen ez esetben nem szükséges személyes kapcsolatot kialakítania az áldozatával, a social engineer csupán azt a látszatot kelti, hogy egy valódi rendszerrel kommunikál az áldozat, ezáltal nem veszi észre, hogy valójában csalás áldozatává válik. A technika előnye, hogy a személyes kontaktus hiányában a lebukás veszélye is kevésbé fenyegeti a támadót.

Az IT alapú social engineer módszernek számos technikája ismert, az egyik legjellemzőbb a kártékony programok segítségével végrehajtott támadás. A kártékony programok csoportjába tartozó támadási formák legfőbb célja az információszerzés, amely irányulhat személyes adatokra, jelszavakra, bankkártya adatokra, vagy például az adott szervezet belső bizalmas információira is.

Ilyen kártékony programnak tekinthető a keylogger, vagyis a billentyűzet naplózó. Ez olyan a billentyűzet naplózására is alkalmas program, amely rögzíti a felhasználó által begépelt karaktereket

---

[1] Haig Zsolt: Információ – társadalom – biztonság. NKE Szolgáltató Kft., Budapest, 2015. pp. 29-39.
[2] A digitális hadszíntér, ahol az információk megszerzésére, előállítására, feldolgozására, tárolására, továbbítására és védelmére irányuló tevékenységek, valamint a számítógép-hálózati hadviselés folyik.
[3] Fekete Csanád: Információ és hadviselés: háború a kognitív hadszíntéren II., Szakmai Szemle 2016/4. szám, in: http://knbsz.gov.hu/hu/letoltes/szsz/2016_4_szam.pdf, p. 41-86. (2017. 02.17.)
[4] Deák Veronika: A social engineering humán alapú támadási technikái, Biztonsagpolitika.hu 2017.04.10., in: http://biztonsagpolitika.hu/publikaciok-2017/deak-veronika-a-social-engineering-human-alapu-tamadasi-technikai, (2017. 04. 16.)

és rendszeresen pillanatfelvételt készít a számítógép képernyőjéről. Továbbá naplózza még a csevegéseket és beszélgetéseket a szociális hálókon, valamint nyilvántartja a számítógépen használt összes internetes alkalmazást is. A program által megszerzett információk bármikor lekérdezhetők, amely segítségével a támadó könnyen hozzáférhet a bizalmas információkhoz, akár az azonosítókhoz, jelszavakhoz, bankkártya adatokhoz is.[5]

A kártékony programok csoportjába sorolható a baiting technikája, amely magyarul szétszórást jelent, amikor is a támadó egy fertőzött adathordozót (pendrive, CD, DVD, SD kártya) „véletlenül" elhagy.[6] Amikor a gyanútlan áldozat megtalálja azt, kíváncsiságából fakadóan 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. Sok esetben figyelemfelkeltő feliratokkal (szexuális tartalom, bizalmas információk, bérrel kapcsolatos információk) látják el az adathordozókat, hogy ezáltal még csábítóbb legyen a felhasználó számára. [7] A csatlakoztatást követően a kártékony kód megkezdi működését és számtalan bizalmas információhoz nyújt hozzáférést, amelyekkel később könnyen visszaélhet a támadó vagy akár meg is zsarolhatja az áldozatát.

Kártékony kódot tartalmazó adathordozó az előzőhöz képest számos egyéb módon is eljuthat a gyanútlan felhasználókhoz. Történhet például, hogy a támadó postán[8] küldi áldozatának az adathordozót, amelyhez kísérőlevelet mellékel, melyben meghatározza, hogy milyen okból kapja a felhasználó az adathordozót. Ez lehet például reprezentációs anyag, szoftverfrissítést tartalmazó CD, promóciós ajándék, nyereményjáték során nyert adathordozó, egy ajándék, ha a felhasználó részt vesz egy kutatásban, de akár egy hivatalosnak tűnő levél mellékleteként is érkezhet az eszköz. Továbbá a célszemélyhez kerülhet úgyis az adathordozó, ha például egy konferencián vagy rendezvényen a részvétel mellé ajándékba kap a felhasználó például egy pendrive-ot, vagy a rendezvény egyéb résztvevőjétől valamilyen reprezentációs anyagot kap CD-n vagy DVD-n, amely akár kártékony kódot is tartalmazhat. Ezek a technikák azért tekinthetők hatékonynak, mert az áldozatok az esetek döntő többségében gyanútlanul csatlakoztatják az eszközt, hiszen nem gondolják, hogy egy hivatalos eseményen kártékony kódot tartalmazó adathordozókat osztogatnának, így fel sem merül bennük a támadás gyanúja.

---

[5] Oroszi Eszter: Social Engineering, 2008, pp. 52-54. http://krasznay.hu/presentation/diploma_oroszi.pdf (2017.02.25.)
[6] Muha Lajos, Krasznay Csaba: Az elektronikus információs rendszerek biztonságának menedzselése. Nke Szolgáltató Kft., 2014, p. 52.
[7] Sörös Tamás et al.: Social engineering a biztonságtechnika tükrében, 2013, p. 21. http://www.uni-obuda.hu/users/horvath.zsolt.laszlo/_szakirodalom/Inform%C3%A1ci%C3%B3biztons%C3%A1g/TDK-Social_Engineering-Soros-Vaci_orszagos.pdf (2017.02.21.)
[8] Oroszi Eszter: Kártékony programok terjedése social engineer szemmel, Dunakavics 2015/VIII. szám in: http://dunakavics.uniduna.hu/online_1508.pdf (2017. 02.21.)

A kártékony programok csoportjába sorolható a javítás, frissítés felajánlás módszere is, melynek lényege, hogy a támadó a gyártó nevében egy ingyenes javítási vagy frissítési lehetőséget ajánl fel, amely valamilyen kártékony kódot tartalmaz. A felhasználó naivan azt hiszi, hogy ez egy kihagyhatatlan lehetőség, ami megbízható, hiszen a gyártótól érkezett, így mindenféle gyanakvás nélkül letölti a frissítést, amely következtében a kártékony program már települ is a számítógépére.[9]

További IT módszerek közé sorolhatók a trójai programok. Ezek olyan rosszindulatú programok, amelyek az információs rendszerbe jóindulatú programba rejtve kerülnek be, látszólag vagy akár valójában is hasznos, illetve szórakoztató funkciókat látnak el, de emellett rejtett funkcióval is rendelkeznek, végrehajtanak olyan nem kívánt műveleteket is, amelyek adatvesztéssel járnak, például adatokat módosítanak, könyvtárakat, vagy akár adatállományokat törölnek vagy szereznek meg, vagy éppen vírust telepítenek. [10] A trójai programok érkezhetnek levelek csatolmányaként, amikor a támadó valamilyen figyelemfelkeltő, érdekes tárgyat (szexuális tartalom, akciós ajánlatok, játék, sport) ír az üzenetbe, hogy a felhasználó biztosan megnyissa az üzenetet és a mellékletet egyaránt, de lehet az egy baráti, munkatársi üzenet, egy ünnepi képeslap vagy esetleg valamilyen csalogató e-mail is, amelyben közlik velünk, hogy valamit nyertünk. A trójai program eljuthat a felhasználókhoz különböző kétes eredetű letöltő oldalakon keresztül is. Ezek az oldalak általában ingyenesen kínálnak vonzó tartalmat (videókat, képeket, zenét, filmet stb.) a felhasználó számára, amely letöltésével a trójai program is feltelepül.[11]

Az IT alapú támadások egyik legjellemzőbb színterei a WiFi hálózatok. Mindennapjaink szerves részét az interneten töltjük, levelezéseket folytatunk, híreket olvasunk, a közösségi oldalakat használjuk, a különböző ügyeink intézését (banki utalás, adóbevallás stb.) az interneten folytatjuk, illetve munkaeszközként is használjuk. A mobilinternet még mindig drága, – Európában az egyik legdrágább – így sokan ezért csatlakoznak a különböző nyílt hálózatokhoz. A kényelmes, illetve ingyenes használat és számos más előnye mellett azért az egyik legfontosabb hátrányát mindenféleképpen meg kell említeni. A nyílt hozzáférésű WiFi hálózatok gyakran adathalász célokat szolgálnak, éppen ezért ha ilyen hálózathoz kapcsolódunk például egy közösségi helyen (kávézó, könyvtár, bevásárlóközpont, tömegközlekedési eszköz stb.) érdemes megkérdezni a hálózat üzemeltetőjét, hogy valóban az adott helyhez tartozik-e a hálózat, hiszen egy ismeretlen hotspothoz kapcsolódva könnyen megfigyelhetik a tevékenységünket, vagy esetleg bizalmas adatainkat is megszerezhetik.Ezen kívül olyan eset is előfordulhat, amikor a támadó a közösségi helyünk WiFi hálózatát töri fel, ezzel szerezve meg a bizalmas információinkat.

[9] Sörös Tamás et al. i.m. p. 20.
[10] Haig 2015, i. m. p. 131.
[11] Oroszi 2008, i. m. p. 50.

Egy másik napjainkban igen fontos szerepet játszó eszközhöz kapcsolódó támadási technika az okostelefon alkalmazások általi hozzáférés. Az okostelefonjaink már mindennapjaink részévé váltak, azonban nem árt óvatosnak lennünk, a mobil alkalmazások jelentős kockázatot rejtenek magukban, hiszen minden alkalmazás hozzáfér a telefonunk tartalmához, az azonban nem mindegy, hogy mennyihez. Az alkalmazás nem csak a készülék alapvető funkcióihoz, hanem a használatukért cserébe a felhasználó személyes adataihoz is kér, illetve kap hozzáférési engedélyt, még olyanokra is, amire nem is lenne oka. Az alkalmazások különböző bizalmas információkhoz férhetnek hozzá, ilyen például a tartózkodási hely, a névjegyek, az üzenetek (SMS, email), a hívásadatok (tartalma, hossza), a képek, a videók, a kamera, az SD kártya tartalma, a telefon memória tartalma, a hálózati hozzáférés, illetve a WiFi csatlakozási információk. Elég például, ha a támadó megszerzi a tartózkodási helyünket, az üzeneteink tartalmát, vagy például a képeinket, azok máris könnyen zsarolási alapként szolgálhatnak számára. Előfordulhat az is, hogy egy program a telefonhívásainkhoz is hozzáfér, vagy a névlistánkat szerkeszti, esetleg még tárcsázza is. A program akár SMS-eket is küldhet vagy éppen a személyes adatainkat is tovább küldheti nem anonimizált módon. Fontos, hogy sok esetben, ha egy alkalmazás hozzáfér a személyes adatainkhoz, a leveleinkhez, vagy például a tartózkodási helyünkhöz, az még nem jelenti azt, hogy ezen információkkal a program visszaél, de biztonsági kockázatot jelent, hiszen gondatlan programozás, szoftverhiba vagy sebezhetőség révén más alkalmazások, illetve személyek számára is hozzáférhetővé válhatnak anélkül, hogy erről a felhasználó tudomást szerezne. [12] A böngésző elleni támadásokra is kiemelt figyelmet kell fordítanunk, hiszen ezzel az eszközzel a támadó könnyen feltelepíthet egy kártékony programot a telefonunkra, amely segítségével képernyőmentést készíthet és a gombnyomások lementésével hozzáférhet az azonosítókhoz és a jelszavakhoz is. Továbbá az is előfordulhat, hogy például a felhasználó hiába írja be a megfelelő URL-t, a kártékony program könnyen átirányíthatja egy hamis oldalra is, ahol a beírt adatok nem a bank szerverébe kerülnek, mint az igazi oldal esetében, hanem a hacker számítógépébe, aki a bizalmas adatok birtokában már meg is kezdheti a belépést a bank igazi honlapján. Éppen ezért a böngésző beállításai között szabályozni kell, hogy mely adatainkhoz, illetve eszközeinkhez (pl. kamera, mikrofon) férhet hozzá a böngésző. Fontos, hogy a legtöbb esetben az alkalmazás letöltésekor tételesen megjelenik, hogy az adott alkalmazás a letöltés után mely adatainkhoz férhet hozzá, így ezek tudatában dönthetünk az esetleges letöltésről.

A támadási módszerek egy másik nagy csoportját az adathalász technikák alkotják. Az adathalászat, más néven phishing lényege, hogy az adathalászok a felhasználót, valamilyen elektronikus csatornán keresztül, egy látszólag teljesen eredeti, valójában pedig egy hamis weboldalra irányítják,

[12] Bodnár Ádám – Az alkalmazások negyede gyanús, 2012. Forrás: https://www.hwsw.hu/hirek/49403/bit9-google-android-okostelefon-alkalmazas-biztonsag.html (2017.02.19.)

ahol arra kérik a felhasználót, hogy adja meg jelszavait, bankkártya adatait, telefonszámát vagy egyéb bizalmas adatait. Az adathalászatnak számos válfaja van, aszerint, hogy milyen elektronikus csatornán keresztül invitálják a felhasználót a hamis weboldalra.[13]

Az adathalászat történhet hamis e-mailek és weboldalak segítségével. Ez a módszer a banki és pénzügyi szektort veszélyezteti a legjobban, a támadók fő célpontjai az esetek döntő többségében a pénzintézetek ügyfelei közül kerülnek ki. Ez esetben támadó kiválaszt egy bankot, amelynek honlapját lemásolja valamely weboldal szerkesztő, karakter felismerő vagy más egyéb programmal, a leendő áldozatok email címét pedig a webről gyűjti össze a különféle adatbázisokból.[14] Ezt követően a támadó a hamisított honlap címét az e-mailbe másolja, és mint a számlavezető bank valamilyen hamis indokkal kéri a felhasználót, hogy lépjen be a hamis oldalra. Ez az indok lehet például adatfrissítésre, az oldal szervízelését követő adategyeztetésre vagy az adatbázisból való törlés elkerülésére vonatkozó felhívás. A támadók a hamis weboldalt úgy készítik el, hogy az csak csekély mértékben különbözzön az eredetitől. Az e-mailben megadott linkre kattintva a hamis banki tranzakciót lebonyolító weboldalra irányítja a felhasználót, ahol azonosítóját, bankkártya adatait, jelszavát megadva egy hiba üzenetet kap, mely szerint a rendszer még karbantartás alatt áll, és később térjen vissza az oldalra. A korábban begépelt bizalmas információk nem a bank rendszerébe, hanem a hacker számítógépére kerülnek, aki az adatok birtokában már meg is kezdheti a belépést a bank eredeti honlapján. Innen már csak egy lépés, hogy akár egy nagyobb összegű tranzakciót hajthasson végre.[15]

Az adathalászat másik formája a vishing (VoIP csalás), vagyis a telefonos adathalászat, mely során a támadó valamilyen hangátviteli technikát használ. Ez esetben a támadás úgy történik, hogy e-mailben vagy sms-ben kérik a felhasználót, hogy hívja fel az üzenetbe beillesztett ingyenes telefonszámot, az adatok frissítése, pontosítása, vagy esetleg zárolása miatt. Amikor a gyanútlan áldozat felhívja a telefonszámot, kérik, hogy adja meg bank- vagy hitelkártya információit, mint például a felhasználó nevét, kártyájának számát, banki azonosítóját, illetve a régi és új PIN kódját, hogy ezzel adatait frissíteni tudják, esetleg kártyáját újra aktiválhassák. De a támadás úgy is történhet, hogy a támadó a tömeges tárcsázás módszerével végigtelefonálja egy adott körzet összes hívószámát, és ahol felveszik a telefont, ott egy előre rögzített üzenetet játszanak le. A rögzített üzenetben értesítik az áldozatot, hogy például adathalászat, karbantartás, technikai probléma vagy adatvesztés miatt zárolták a fiókját, illetve szükségük van az ügyfél adataira, így megadnak egy telefonszámot, amit ha felhívnak, könnyedén megoldhatják a problémáját. A vishing támadások

[13] Muha Lajos et al., i. m. p. 51.
[14] Nagy Zoltán András: Bűncselekmények számítógépes környezetben. Ad Librum, Budapest, 2009. pp. 261-264.
[15] Bérczes Attila, Pethő Attila: Kriptográfia. NKE Szolgáltató Kft., Budapest, 2014, pp. 42-44.

sikeressége abban rejlik, hogy az ügyfelek jobban megbíznak a telefonban, mint például egy e-mailben vagy weboldalban, illetve a telefonon keresztül történő csalások sokkal kevésbé ismertek.[16]

Az adathalászat történhet SMS-en keresztül (smishing) [17], mely során az adathalász üzenet SMS-ben érkezik. A smishing támadások jelentős része az előző két technikához hasonlóan szintén a banki és pénzügyi szektort célozza elsősorban. Ebben az esetben a támadó a számlavezető bank helyett küld egy SMS-t, melyben arra hivatkozik, hogy valamilyen probléma felmerülése miatt zárolták vagy törölték a fiókját, esetleg adatfrissítés miatt az üzenetbe beillesztett telefonszámot kell felhívnia a probléma megoldása érdekében. A smishing támadások másik részében a támadó valamilyen ingyenes szolgáltatás használatára, nyereményjátékra, ajándékok átvételére hívja fel az áldozat figyelmét, és arra kéri, hogy az üzenetben található hivatkozásra lépjen, vagy hívja fel az üzenetben megadott telefonszámot. A weboldal segítségével pedig a támadó könnyen megszerezheti bizalmas információinkat, esetleg a nyereményre szolgáló kupon letöltésével valamilyen kártékony program is települhet az eszközünkre. Abban az esetben, ha telefonszám került megadásra az SMS-ben, akkor a támadó vagy egy előre rögzített üzenet segítségével vagy saját maga kérdezi meg a bizalmas adatokat az áldozattól.

Az adathalászat egy másik válfaja a pharming, más néven eltérítéses adathalászat[18], mely során a felhasználó hiába gépeli be az eredeti oldal címét, a DNS szerver[19] egy álweboldalra irányítja a felhasználót. A technika a DNS szerver sebezhetőségeit használja ki, azáltal, hogy egy kártékony program segítségével módosítja a DNS gyorsítótár[20] tartalmát, így amikor a DNS a gyorsítótárból próbálja megnyitni az adott oldalt, az előzőleg módosított gyorsítótár szerinti álweboldalra irányítja, ahol a felhasználó a támadó megtévesztéséről mit sem sejt.[21] A DNS gyorsítótár módosítása egy kártékony program segítségével történhet, amely érkezhet e-mailek csatolmányaként, vagy az ingyenesen letölthető tartalmak által.

Az adathalászat egy speciális formája a whaling, vagyis bálnavadászat, amely a „nagy halakat”, a vezetői réteget, a cégvezetőket, középvezetőket célozza. A technika előnye, hogy sok esetben a vezetők e-mail fiókjába érkező leveleket a titkárság előzetesen megszűri, esetleg továbbítja is azt egy másik osztály, intézmény felé.

---

[16] Muha Lajos et al., i. m. p. 51.
[17] Oroszi 2008, i. m. p. 46.
[18] Muha Lajos et al., i. m. p. 51.
[19] A DNS-kiszolgáló egy olyan szolgáltató oldali szerver, amely az internetes címek fordításáért felelős. Ezen szerver segítségével tudunk az interneten keresztül weboldalakon böngészni, e-maileket küldeni és fogadni.
[20] A számítógép a korábban meglátogatott weboldalak DNS találataiból saját másolatot őriz meg.
[21] Pharming": adathalászat mesterfokon, észrevétlenül (**http://securityresponse.symantec.com/hu/hu/norton/library/familyresource/article.jsp?aid=article1_08_06)** (2017.02.29.)

Az adathalászat egy másik formája a különböző nyereményjátékokat, ajándékokat vagy ingyenes szolgáltatásokat hirdető áloldalak. Különösen veszélyes módszernek tekinthető, hiszen a felhasználók jelentős része annyira vágyik a különféle ingyenes ajánlatokra vagy ajándékokra, hogy sok esetben nem gondolnak bele, hogy az ingyenes ajánlatok és nyereményjátékok mögött valójában a felhasználók bizalmas adatainak megszerzése áll.

Összességében elmondható, hogy függetlenül attól, hogy a felhasználó használ-e számítógépet vagy sem, az adott támadás IT vagy humán alapú, a biztonságtudatosság és a támadási formák ismerete elengedhetetlen a megfelelő és hatékony védelem kialakításához. A különböző támadások módszereit megismerve jelentősen tudjuk csökkenteni a ránk bízott információk kiszivárgását, és illetéktelen felhasználását, valamint ezzel együtt növelni az állami és nem állami szervek működésének stabilitását, valamint a társadalom és a gazdaság részvevőinek biztonságát.

Felhasznált irodalom

- Bérczes Attila, Pethő Attila: Kriptográfia. NKE Szolgáltató Kft., Budapest, 2014
- Bodnár Ádám – Az alkalmazások negyede gyanús, 2012. Forrás: https://www.hwsw.hu/hirek/49403/bit9-google-android-okostelefon-alkalmazas-biztonsag.html (2017.02.19.)
- Deák Veronika: A social engineering humán alapú támadási technikái, Biztonsagpolitika.hu 2017.04.10., Forrás: http://biztonsagpolitika.hu/publikaciok-2017/deak-veronika-a-social-engineering-human-alapu-tamadasi-technikai, (2017. 04. 16.)
- Fekete Csanád: Információ és hadviselés: háború a kognitív hadszíntéren II., Szakmai Szemle 2016/4. szám, Forrás: http://knbsz.gov.hu/hu/letoltes/szsz/2016_4_szam.pdf (2017.02.17.)
- Haig Zsolt: Információ – társadalom – biztonság. NKE Szolgáltató Kft., Budapest, 2015.
- Muha Lajos, Krasznay Csaba: Az elektronikus információs rendszerek biztonságának menedzselése. Nke Szolgáltató Kft., 2014
- Nagy Zoltán András: Bűncselekmények számítógépes környezetben. Ad Librum, Budapest, 2009.
- Oroszi Eszter: Social Engineering, 2008. http://krasznay.hu/presentation/diploma_oroszi.pdf (2017.02.25.)
- Oroszi Eszter: Kártékony programok terjedése social engineer szemmel, Dunakavics 2015/VIII. szám in: http://dunakavics.uniduna.hu/online_1508.pdf
- (2017.02.21.)
- Sörös Tamás et al.: Social engineering a biztonságtechnika tükrében, 2013. http://www.uni-obuda.hu/users/horvath.zsolt.laszlo/_szakirodalom/Inform%C3%A1ci%C3%B3biztons%C3%A1g/TDK-Social_Engineering-Soros-Vaci_orszagos.pdf (2017.03.02.)
- http://securityresponse.symantec.com/hu/hu/norton/library/familyresource/article.jsp?aid=article1_08_06 (2017.02.29.)