SOCIAL ENGINEERING AND MANIPULATION TECHNIQUES AND METHODS

A SOCIAL ENGINEERING ÉS A MANIPULÁCIÓS TECHNIKÁK ÉS MÓDSZEREK

KOLLÁR Csaba[1], ZAKAR Ákos[2]

Abstract

In the first, theoretical part of our two-part study, we review all or most of the manipulation methods and techniques related to the human soul, psychology, and interpersonal communication, which also appear in the field of information security. In describing the techniques and methods, we present, among other things, shoulder surfing, asking for and providing help, personalization, phishing, image and video forgery, fake security applications, and fraudulent calls. In the latter case, we also point out the criminal law implications of the perpetrators 'act. Fraudsters have also taken advantage of the psychological effects of the coronavirus, as mentioned in several examples. We hope that we can contribute to the personal and organizational development of information security by reviewing the theory, presenting examples, and then presenting our research results in the next section.

Keywords

information security, social engineering, manipulation

Absztrakt

Kétrészes tanulmányunk első, elméleti részében az egészében, vagy zömében az emberi lélekhez, a pszichológiához, a személyközi kommunikációhoz köthető, manipulációs módszereket és technikákat tekintjük át, melyek az információbiztonság területén is megjelennek. A technikák és módszerek ismertetésénél a humán, illetve IT alapú felosztás mentén mutatjuk be többek között a váll feletti leskelődést, a segítségkérést, illetve -nyújtást, a megszemélyesítést, az adathalászatot, a kép- és videohamisítást, a hamis biztonsági alkalmazásokat, a csaló hívásokat. Ez utóbbinál rámutatunk az elkövetők cselekményének büntetőtörvénykönyvi vonatkozásaira is. A csalók kihasználták a koronavírus pszichés hatásait is, ahogy arra több példa kapcsán is utaltunk. Reményeink szerint az elmélet áttekintésével, a példák bemutatásával, majd a következő részben kutatási eredményeink ismertetésével egyaránt hozzá tudunk járulni az információbiztonság személyi és szervezeti fejlesztéséhez.

Kulcsszavak

információbiztonság, social engineering, manipuláció

[1] kollar.csaba@phd.uni-obuda.hu | ORCID: 0000-0002-0981-2385 | PhD student / doktorandusz | Obuda University Doctoral School of Safety and Security Sciences / Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] zakarakos85@gmail.com | ORCID: 0000-0002-3919-4098 | detective / nyomozó | Rapid Response and Special Police, Services National Bureau of Investigation, Cybercrime Department / Készenléti Rendőrség, Nemzeti Nyomozó Iroda, Kiberbűnözés Elleni Főosztály

BEVEZETÉS

Tanulmányunk első, elméleti részében a social engineering módszereiről kívánunk egy átfogó képet adni. Szerteágazó technikák gyűjteményéről van szó, hiszen a kibertérben elkövetett támadások 98%-a social engineering technikára támaszkodik [1]. Jelen tanulmányunkban ezek közül a fontosabbakat tekintjük át, alapul véve a kettős felbontást (humán és számítógép alapú) [2]. Ahogy arra Kevin Mitnick [3] is utal, a befolyásolás és rábeszélés módszerét alkalmazva, a technológia használatával vagy a nélkül éri el célját a támadó. Mivel bizonyos módszerekben átfedés tapasztalható, így az „első lépés" jellege alapján soroltuk be az adott kategóriába a támadásokat (1. táblázat), alapul véve a EC-Council CEH [4, p.959-1028] oktatási anyagát.

Humán alapú	**IT alapú (mediatizált)**	
	Számítógép használattal	*Telefon használattal*
1. Váll feletti leskelődés	1. Elhagyott adathordozó	1. SMS
2. Hallgatózás	2. Billentyűzet naplózó	2. Kártékony alkalmazás
3. Segítségkérés	3. Adathalászat	3. Hamis biztonsági alkalmazás
4. Segítségnyújtás	4. Kéretlen e-mail	4. Újracsomagolt alkalmazás
5. Fordított social engineering	5. Álvírusírtó	5. Instant üzenetküldő
6. Megszemélyesítés	6. Zsarolóvírus	6. Csaló hívás
7. Épületbe való bejutás	7. Trójai program	
8. Kukabúvárkodás	8. Hamis szoftver telepítő	
9. Jelszavak kitalálása	9. Hálózatfigyelés	
	10. Felugró ablak	
	11. Üzleti e-mail kompromittálás	
	12. Kép és videó hamisítás	

1. Táblázat: A fontosabb social engineering technikák csoportosítása (saját szerkesztés)

HUMÁN MÓDSZERREL VÉGREHAJTOTT TECHNIKÁK

Mint ahogy a kategória neve is mutatja, a támadónak ez esetben nem kell műszaki eszközöket igénybe vennie, mivel az ember kommunikációs és pszichológiai képességeire, gyengeségeire épít. Pszichológiai és kommunikációs szempontból ez igényli a legmagasabb fokú felkészültséget a támadó részéről, ugyanakkor a lebukás veszélye is itt a legnagyobb, hiszen – pár kivételtől eltekintve – közvetlen kontaktust létesít a célszeméllyel. Sok esetben kevesebb idő- és energiaráfordítást igényel végrehajtásuk, mint egy technológiai módszernek. További előnyük, hogy olyan jellegű információk birtokába juthatunk, melyekkel más jellegű támadások kivitelezését meg lehet könnyíteni, illetve a célszemélyt rá tudjuk venni arra is, hogy helyettünk hajtson végre valamilyen támadást (pl. adatbázishoz hozzáférés). Ebbe a kategóriába sorolhatók azon módszerek, melyek végrehajtásához nincs szükség az informatika, szűkebb értelemben véve a számítógép használatára. Itt csak a célszemély felkészültsége és tudatossága szabhat gátat a támadás sikerének, ugyanis semmiféle – klasszikus értelemben vett – IT technológiai védelem (pl. tűzfalak, spam szűrők) ez esetben nem működik. [5, p.88] Az alábbiakban ezeket vesszük sorra.

Váll feletti leskelődés

Avagy angol terminológiában „shoulder surfing", melyet váll-szörfnek is fordíthatunk, de a kifigyelés, leskelődés találóbb kifejezések rá. Ez egy viszonylag könnyen kivitelezhető technika, aminek célja az előttünk álló, vagy számítógépnél ülő személy hitelesítő adatainak megszerzése, miközben azokat ő begépeli az adott eszközön. Itt ki lehet használni az áldozat bizalmát (pl. közvetlen kollégák esetén) vagy amennyiben erre nincs mód az adott szituációban, akkor mindezt észrevétlenül kell végrehajtani, úgy, hogy se a célszemély se mások ne vegyék észre. Ezt utóbbi kockázatra megoldást jelenthet, ha úgynevezett hatásfok növelő eszközöket vesznek igénybe (pl. távcső, vagy speciális kamerák), amik képesek a távoli mozdulatokat, információkat közelebb hozni vagy rögzíteni. Ez utóbbi példa azonban már túlmutat a kategória keretein, de például egy rejtett kamerás megfigyelés is innen eredeztethető.

Hallgatózás

Tipikus humán alapú technika – mely szinte egyidős a váll feletti leskelődéssel, sőt lehet mondani, hogy az emberi beszéd megjelenésével – amit el lehet követni technikai eszköz használatával is. Az alkalmazás módját az adott szituáció dönti el. Itt a jogosulatlan személy valós időben privát beszélgetést „fog el", ami kettő vagy több ember közt zajlik. Könnyedén meg lehet hallani bizalmas információkat pl. kávézókban, tömegközlekedési eszközökön, rendezvényeken, várótermekben. Ilyenkor ugyanis nem tűnik fel senkinek a másik ember közelsége, mondhatni ebben a közegben ez természetes. Ha párhuzamba vonjuk a kifigyeléssel, ez az eszközös lehallgatás előszobájának tekinthető, de még mindig működő klasszikus módszer.

Segítségkérés

A segítségnek két oldalát akár egy technikának is tekinthetjük. Az egyik legkönnyebben kivitelezhető módszer, mivel a támadó egész egyszerűen segítséget kér a kiszemelt áldozattól. Bibliai hasonlattal élve „Kérjetek, és adatik nektek…" itt (is) értelmet nyer [72]. A támadó persze ezt más céllal használja úgy, hogy eredeti szándéka rejtve maradjon. Mivel az emberek nagy része segítőkész – a kiszolgáló és szolgáltató területen dolgozóktól pedig egyenesen elvárás, pl. helpdesk, recepciós, titkárnő – így könnyű sikert elérni.

Segítségnyújtás

Az előzőnek a fordítottja, vagyis a támadó idéz elő egy hibát, melyet már az elején úgy épít fel, hogy a megoldását az adott helyzetben és időben az ő személyében lássa meg az áldozat. A támadó a mesterséges kényszerhelyzet kihasználásával fog hasznot húzni pl. azáltal, hogy távolról hozzáfér az áldozat számítógépéhez, vagy nyomtató javítást, villanyszerelést imitál. De előnyhöz juthat úgy is, ha az elvégzett szívességért cserébe, fizetség helyet „viszont szívességet" kér, amivel vissza is kanyarodtunk a segítségkéréshez. [5, p.81-82] Egy jól ismert szabály a társadalmi interakcióban, hogy a szívesség szívességet szül, még akkor is, ha az eredeti szívességet kérés nélkül ajánlották fel. Ezt az eljárást hívjuk reciprocitásnak.

Fordított social engineering

Kevin Mitnick ezt a technikát „fordított szúrás”-nak nevezte el, amit már nehezebb kivitelezni, mint az előbb említett segítségnyújtást, de hasonlít hozzá [3]. Ennek oka, hogy jóval több előkészületet és speciális képességeket igényel. A támadónak ugyanis még a probléma létrejötte előtt meg kell győznie a dolgozót arról, hogy baj esetén bizalommal fordulhat hozzá. A probléma megoldására irányuló előzetes kérdések feltevésekor már eleve úgy manipulálja a kérdéseit, hogy az áldozat kimondja, elszólja magát a bizalmas információkat illetően, amik elemei lehetnek és megalapozhatnak egy komplexebb támadást.

Megszemélyesítés

Itt kifejezetten nagy jelentősége van a támadó kinézetének, mert az emberek az első benyomás alapján a fejükben bekategorizálják az idegeneket. „A humán alapú technikák nagy része alapvetően arra irányulnak, hogy a támadó egy másik személynek adja ki magát, amely lehet való vagy fiktív személy”. [7, p.9] A támadó célja, hogy elhitesse az áldozattal, hogy ő valóban az – legyen akár fiktív, akár valós személyiség – akinek kiadja magát. Mivel több alkategóriákra lehet bontani eme komplex támadási formát, így erre részletesebben a következőkben fogunk kitérni.

Épületbe való bejutás

Ezen technikának alapvetően három típusa ismert: tailgating, piggybacking, masquerading [8, p.39], s tartalmukban e három fogalom átfedést mutat, illetve a szakirodalom sem egészen következetes a használatukat illetően. A tailgating és a piggybacking egyaránt arra utalhat, hogy a támadó egy jogosultsággal rendelkező személyhez társul, beszélgetésbe elegyedik vele, s így képes bejutni bizonyos (lezárt) területekre, vagy úgy jut be, hogy nem szükséges beszédbe elegyednie mással. Ez a cselekmény nem mindig illegális, bár a belépés rendszerint jogosultsághoz és/vagy engedélyhez kötött, amivel a támadó nem rendelkezik. A támadó nem csak az emberi humánum gyengeségeit használhatja ki (amire a szoros követés, a piggybacking épül), de a biztonsági (nem csak informatikai) rendszer gyengeségeit is (a tailgating fogalma inkább ehhez köthető), például egy ajtó automatikus zárásának késleltetése kellő időt biztosít arra, hogy a támadó is bemenjen, vagy vannak olyan fizikai hátsó ajtók melyek védelmére nem fordítottak kellő figyelmet, s így a támadó minden különösebb nehézség nélkül besétálhat. A masquerading lényege, hogy a támadó meggyőzi a személyzetet arról, hogy neki joga van bizalmas, titkos információk megszerzéséhez (pl.: informatikust, vagy belső ellenőrt játszik, akit a központból küldtek ki). A hitelessége érdekében hamis belépőkártyát, hamis céges egyenruhát használhat. Határozott fellépésének köszönhetően az ellenőrzésért/beléptetésért felelős személy(eke)t viszonylag könnyen meg tudja téveszteni.

Kukabúvárkodás

Ahogy a módszer neve is mutatja, nem túl kifinomult, kommunikációt nem igénylő technikáról van szó, ugyanakkor fontos, hiszen megalapozhat egy későbbi komplex támadást. A támadónak először meg kell szerveznie, hogy milyen módszerrel juthat a kukához úgy, hogy az ne keltsen gyanakvást abban, aki ezt észreveszi. Ezt követően egy nyugodt helyen alaposan át tudja vizsgálni annak tartalmát. Ehhez információt kell gyűjteni a kukák

tárolásáról, elszállításáról is. [5] Beszélhetünk akár vállalati, akár privát szféráról, a felelőtlen emberek rengeteg olyan információt tartalmazó dolgokat dobnak ki a szemetesbe, melyről úgy gondolják, hogy az szinte egyből meg is semmisül. [8, p.39]. Sokan lebecsülik ennek a módszernek a használatát, pedig megannyi értékes dokumentumot tartalmazhat a munkahelyi szemetes:

- Szervezeti ábrákat, helyszínrajzokat: felfedik a részletes struktúráját a cégnek, fizikai felépítését, tiltott területeket (pl. szerver szobák).
- Nyomtatott e-maileket, jelentéseket, faxokat: felfednek személyes információkat dolgozóról, a jelszavak, szerződések, belső utasítások mellett.
- Belső kézikönyveket, utasításokat: felfednek foglalkoztatási adatokkal vagy az alkalmazott IT rendszer használatával kapcsolatos információkat.
- Esemény feljegyzéseket, naptárakat vagy nyomtatott számítógépes logokat: felfednek olyan információkat, amik a felhasználói be- és kijelentkezésekre vonatkoznak, így segíteni fogják a támadót a támadás megfelelő időpontjának kiválasztásában.
- Telefonszám listákat: felfedik a dolgozók neveit és belső telefonszámaikat.

Jelszavak kitalálása

Szándékosan a kitalálás szót használjuk és tesszük a humán alapú technikák közé, mivel itt szó sincs adathalászat útján, vagy különböző jelszó feltörő szoftverek segítségével megszerezhető hitelesítő adatokról. Jelenleg is megállja a helyét Jeff Crume mondása, miszerint „napjainkban, az informatikai rendszerekben a hitelesítés legelterjedtebb formája a jelszó”. [9, p.114] Mint ahogy arra a kutatási jelentést tartalmazó második részben még ki fogunk térni, itt a felhasználó által használt gyenge jelszavak megválasztásában kell keresni a gyengeséget, amit a támadó ki tud használni. A jelszavak nagy része ugyanis bizonyos fokú személyes ismeretség vagy információszerzést követően viszonylag könnyen kitalálható. A jelszavak egy jelentős részénél pedig – ahogy az az alábbi ábrán látható – még a személyes alaposabb ismerete sem szükséges.

1. Ábra: A leggyakrabban használt gyenge jelszavak [10]

Bizonyos munkahelyeken – a „túlzott" bizalom és a baráti légkör miatt – nem ritka, hogy a felhasználók megadják egymásnak a jelszavaikat, ezzel öntudatlanul súlyos kockázatnak kitéve az adott rendszerbeli fiókjuk saját felügyeletét. Egy 785 szervezetet tanulmányozó kutatás [11] a dolgozók jelszóhasználati szokásait elemezte. A vizsgált cégek 61%-nál találtak olyan felhasználókat, akiknek jelszavai nem járnak le. 40%-nál fordultak elő olyan engedélyezett felhasználói fiókok, melyek már elavultnak számítottak, azaz már nem aktív dolgozókhoz tartoztak. Összevetve, átlagosan minden második fiók ebbe a kategóriába tartozott. A felelőtlen magatartás által ez a statisztika is rámutat a jelszó kitalálás módszerében lévő lehetőségekre, melyre kutatási jelentésünkben mi is ki fogunk térni.

IT ALAPÚ MÓDSZERREL VÉGREHAJTOTT TECHNIKÁK

Ide azok a technikák tartoznak, melyek informatikai eszközök – jellemzően számítógépek és okostelefonok – segítségével próbálják meg átejteni a gyanútlan felhasználót, azonban itt is az emberi mulasztást, hiszékenységet használja ki a támadó. „Ezen technikák jellemzője, hogy a social engineer azt hiteti el az áldozatokkal, hogy egy valódi rendszerrel kommunikálnak, s nem veszik észre, hogy csalás áldozataivá válnak" [8, p.39]. Nagy előnye a humán alapú módszerrel szemben, hogy a személyes kontaktus elkerülésével a lebukás kockázata minimalizálható.

Számítógépes technikák

Elhagyott adathordozó. Alapvetően a kártékony programok terjesztésének egyik módszere. A technika ismert angol neve a baiting, ami csalogatást, beetetést jelent, de „Road Apple" támadásnak is nevezik[12]. Kiindulásként a támadó egy kártékony szoftvert telepít egy, de inkább minél több tetszőleges adathordozóra – többnyire pendrive-ra, SD kártyára, régebben optikai, illetve ploppy lemezekre – majd azokat a célszemélyhez közeli helyeken (pl. mosdó, konyha, tárgyaló, recepció, folyosó, nyomtató, iroda, parkoló) elhelyezi, szétszórja. Kiváló csali lehet egy figyelemfelkeltő felirat pl. „bizalmas" elhelyezése az eszközön. Az emberi kíváncsiságból eredően előbb-utóbb valaki meg be fogja tenni – remélhetőleg – a vállalati számítógépbe és a rajta lévő program már meg is kezdi a működését. Megemlítjük még a kártékony kód terjesztésének egyéb módjait, mint pl. postai úton/futárral beküldött, reprezentációs ajándékként osztogatott vagy újság mellékleteként eljuttatott adathordozót, e-mail melléklet csatolmányát, weboldal látogatását, azonban ezek bővebb bemutatására tartalmi korlátok miatt nem bocsátkozunk [5, p.105-106].

Billentyűzet naplózó. A Keyloggerek/Key stroke loggerek lehetnek szoftveres alkalmazások vagy hardveres eszközök is. Működésüket tekintve a felhasználó tudta nélkül rögzítik a billentyűzet leütéseket, beállítástól és típustól függően pedig elküldik a támadónak. A hardveres megoldás választása esetén, mint a baitingnél is, szintén szükséges az ember általi céleszköz elhelyezése. Ez a lebukás veszélye miatt kockázatos is lehet, azonban a telepítés hatékonyabb, mivel semmiféle gyanús szoftvert, weboldalt nem kell igénybe venni a kezdeti működéshez az áldozatnak. Az elhelyezés során felmerült kockázat nagyszerűen csökkenthető pl. takarító, karbantartó személyzet közbenjárásával, akik nem keltenek gyanút egy irodai dolgozóban.

Adathalászat. Az adathalászatot, vagyis a phishing-et jelszóhalászatnak is fordíthatjuk, azonban nem csupán jelszavak, hanem banki adatok, bizalmas információk stb. megszerzése is cél lehet. Amennyiben nem tömegszerűen indítanak „phishing kampányt" az elkövetők, megcélozhatnak a szervezeten belül egy adott személyt (spear pishing) vagy egy felsővezetőt (bálnavadászat/whaling) is. Az adathalász e-mailek általános jellemzői közé tartozik az általános megszólítás, helyesírási hibák használata, sürgetés, számlazárolásra/szolgáltatásból való kizárásra figyelmeztetés, személyes információkra vonatkozó kérés. A phishing levelek óriási mennyiségét az RSA 2019. IV. negyedéves jelentése [13] mutatja be a legjobban, miszerint 2019-ben a phishing levelek 60%-át tették ki éves szinten a csaló szándékú támadásoknak. Előző negyedévhez viszonyítva itt volt tapasztalható a legnagyobb arányú növekedés. A CERT-GIB jelentésében [14] 2020.02.13. és 2020.04.01. között több száz koronavírussal kapcsolatos phishing e-mail analizálásáról számol be. Az e-mailekben 65%-ban különböző típusú kémprogramokat (spyware), 31%-ban hátsó ajtókat (backdoor) és 4%-ban zsarolóvírusokat (ransomware) találtak, melyek a csatolmányban voltak megtalálhatóak. Az adathalászok a tömeges e-mail üzenetek küldésén felül további módszerekkel is átejthetik áldozatukat, adataik bekérése érdekében. Ezek közül a három leggyakoribbat az alábbiakban ismertetjük.

Ál weboldal. Egy olyan weboldal készítése, mely regisztrációt követően csábító nyereményeket ígér, nem nehéz feladat, az elterjedt és könnyen kezelhető CMS rendszereknek köszönhetően. Természetesen ezek mögött valós nyereményjáték nincs. A regisztráció során begyűjtött e-mail címekkel már eleve egy adatbázishoz jut az elkövető, amit későbbi adathalászat során felhasználhat, valamint egyben jelszavakat szerez, amik köthetők lehetnek a felhasználó más webes alkalmazásaihoz is, alapot adva egy komolyabb támadáshoz.

Hamisított weboldal. Az ál weboldallal szemben annyiban különbözik, hogy ez esetben egy létező és jól ismert többnyire pénzügyi szektorban érintett vállalat weblapját másolják le. Az eredeti weblappal szemben a hamisított weboldal URL-jében minimális különbség fog jelentkezni, amit a nem kellőképpen figyelmes felhasználó nem fog észrevenni és az oldalra belépve jóhiszeműen megadja hitelesítő adatait, amik elküldésre kerülnek a támadónak. Az oldalra irányítás általában email üzenetben található linkkel történik. Egyes felmérések szerint minden tizedik URL kártékony oldalra irányít [15].

Farmolás. A pharming során a felhasználó nincs és nem is lehet tudatában annak, hogy hamisított weboldalon jár. A támadó a DNS szerverek sérülékenységét használja ki vagy az áldozat számítógépén található host fájlt módosítja, ezáltal az URL-ben nem fog különbség mutatkozni a hamisított és eredeti weboldal között. A módszerek eredménye ugyanaz, eltéríteni a felhasználót attól, hogy az általa elérni kívánt URL címen lévő weboldalt megtekinthesse, helyette más oldalra lesz átirányítva.

Kéretlen e-mail. A spam üzenetek irrelevánsak, kéretlenek és nagy tömegben érkeznek. A többnyire marketing célból érkező, termékek értékesítésének növelését célzó levelek mellett ide sorolhatók a scam típusú, azaz a tipikus átverős üzenetek, valamint a hoaxok, azaz a lánclevelek is. A scam-eknél általában meghamisítják a feladó e-mail címét és

ismert nagy cégek nevével élnek vissza, akik nyereményről értesítik a címzetteket. A láncLevelek célja főként az e-mail címek begyűjtése. De a fentiek akár kártékony csatolmányokat (pl. vírusokat) is tartalmazhatnak. Az ilyen veszély mellett közvetlen kárt is okoznak, mivel egy vállalati felhasználó idejét a produktív munka helyett, az üzenetek törlése, esetenként megnézése köti le. Gyakoriságukat mi sem mutatja jobban, mint az, hogy a Symantec szerint [16] 2018-ban a fogadott e-mailek 55%-a spam volt. Az IBM adatait alapul véve a spam üzenetek URL-jei mintegy 70%-át teszik ki a főbb fenyegetés típusnak.

Álvírusírtó. Ezeket a programokat scarewareknek is hívják, és ahogy a neve is utal rá, félelmet akarnak kelteni. Akár egy felugró ablakként megjelenő animációval is – mely szkennelést imitál – könnyen elhitetik a laikus felhasználóval, hogy a számítógépe vírussal fertőződött meg. Ezt követően felajánlják a saját terméküket, ami megoldást jelent a problémára, ami lehet ingyenes vagy fizetős szoftver is. A valóság ezzel szemben az, hogy a támadó által felkínált program telepítésekor fertőződik meg a felhasználó számítógépe. A program káros kódja információkat is szivárogtathat a készítőjének a megfertőzött gépről, ami előtte lehet, hogy mentes volt a vírusoktól. Jellemzőjük továbbá, hogy a háttérben blokkolhatják a már meglévő hiteles vírusírtónk frissítését vagy elérhetetlenné teszik a program törlését uninstall funkcióval [5, p.98]. A felhasználó az ilyen káros programok telepítésekor kettős kockázatnak is kiteszi magát. Egyrészt fizet egy olyan szoftverért, ami nem tölti be a funkcióját, vagyis nem írtja a vírust, másrészt megfertőzi a számítógépét kártékony programmal.

Zsarolóvírus. A ransomwarek, vagyis a zsarolóvírusok olyan kártékony szoftverek, melyek zárolják az eszközöket vagy titkosítják a rajtuk lévő adatokat annak érdekében, hogy bevételre – manapság jellemzően kriptovalutára – tegyenek szert a tulajdonostól. A fertőzést követően megjelenő képernyőn az elkövetők azt ígérik – természetesen bármiféle garancia nélkül –, hogy egy adott összegért cserébe visszaállítják a hozzáférést és megküldik a titkosítás feloldásához szükséges kulcsot az érintett géphez vagy adatokhoz. Általában email mellékletként, távoli asztal kapcsolat kihasználásával trójai program bejuttatásával, vagy böngészés közben linkre kattintással is terjedhetnek. Típusai közt megtalálhatóak a lemezkódoló (titkosítja az egész merevlemezt), a képernyőzáró (megakadályozza a hozzáférést az eszköz képernyőjéhez), a crypto (titkosítja a merevlemezen található bizonyos adatokat) valamint az okostelefonra szánt változata a PIN-lezáró (megváltoztatja a hozzáférési kódot) [17]. A legtöbb zsaroló vírus család célpontjai még mindig a Windows alapú számítógépek [18]. Az utóbbi idők egyik legsúlyosabb zsarolóvírus támadás sorozat a WannaCry és a Petya nevű ransomware volt 2017-ben [19]. A 2018-ban ismertté vált Ryuk zsarolóvírus 2019-ben már a legtöbb ágazati szektorban megtalálható volt [20]. Az Interpol közleményében [21] figyelmeztet, hogy napjainkban főként kórházakat valamint más egészségügyi intézményeket – melyek a koronavírus frontvonalában harcolnak – éri a legtöbb zsarolóvírus támadás.

Trójai program. Ahogy Jeff Crume is megfogalmazta a trójai faló olyan „rosszindulatú szoftver, amely funkciója alapján hasznosnak vagy érdekesnek tűnik, de az álca mögött meghúzódó szándék rossz” [9, p.291]. A programok működési elve a mitológiai Trójai falóhoz hasonlóan a megtévesztésen alapul. Mást csinálnak, mint amit valójában mutatnak,

így az egyik legmegfelelőbb módszer, amikor a támadó távolról akarja átverni áldozatát. Ismertek azonban olyan típusai is, melyek valóban végrehajtják a kínált – esetenként szórakoztató – funkciókat, viszont ezek mellett kártékony, rejtett tevékenységet is végeznek. A trójai programok működési elve különbözik a vírusokétól, ugyanis nem reprodukálják magukat és nem feltétlenül tartalmaznak olyan kártékony kódot, mely a rendszer működését leállítaná. Céljuk a számítógéphez való illetéktelen hozzáférés, kémkedés lehetőségének biztosítása [22]. Funkciójuk alapján így megkülönböztetünk billentyűzet leütést naplózó, hátsó ajtót nyitó, jelszavakat gyűjtő, reklámoldalakat megnyitó, felhasználói adatokat begyűjtő trójai programokat. Általában weboldalakon való böngészés, e-mail melléklet megnyitása, vagy elhagyott adathordozón keresztül juthatunk hozzájuk [8, p.50-51].

Hamis szoftver telepítő. Az elmúlt egy évtizedben jelentek meg, céljuk az anyagi haszonszerzés. A támadó ingyenesen letölthető szoftvereket tömörít be és teszi közzé különböző weboldalakon. A kicsomagolási – vagyis a hamis telepítést imitáló – művelet végén megpróbálja rávenni a felhasználót arra, hogy aktiválás címen küldjön pl. emelt díjas SMS-t vagy online fizetéssel rendezze az ellenőrző kód ellenértékét. Amennyiben a felhasználó fizet, a szoftver készen fog állni az installálásra és a használatra. A támadó lényegében egy ingyenes szoftvert nyújt a felhasználónak extra díjért cserébe, ezért is nevezik paid archive technikának [23].

Hálózat figyelés. A hálózatok figyelése, azokon való hallgatózás végrehajtása kellő fokú szakértelmet igénylő feladat. Ezért a laikusok azt is gondolhatnák, hogy inkább a hackerek, mintsem a social engineerek kompetenciájába tartozik. Az igazság azonban az, hogy nem két különálló halmazról beszélünk. Egy hackernek – legyen az jó vagy rossz szándékú – a social engineering is egy szelete a munkájának. Egy aktív MITM (közbeékelődéses) támadás végrehajtása során megtéveszthetí mindkét felet, akinek a levelezésébe beékelődik, vagyis hozzáfér az e-mailjeikhez, ezáltal akár módosíthatja is a levelek tartalmát saját érdekeinek megfelelően. Jellemző példa, amikor két pénzügyi partner esetén kicseréli a cél bankszámlaszámot a sajátjára, így a jogosult fél helyett ő fogja megkapni a pénzt. De a közbeékelődésen kívül a normál adatfolyam megszakítása, fals adat generálása és a passzív lehallgatás is ide tartozik. A hacker be tud ékelődni a felhasználó és egy webszerver közti kommunikációba is.

Wi-fi támadás. Egy nem megfelelően megválasztott, azaz túl gyenge, alapértelmezett, régóta használt jelszóval nagy veszélynek tesszük ki akár a céges, akár a magán vezeték nélküli hálózatunkat. Ugyanakkor elavult titkosítási (pl. WPA, WEP) mechanizmusok alkalmazásával szinte pár másodperc alatt törhetővé válik a hálózatunk és az eszközeink. Épp ezért tökéletes célpontjai a támadóknak az olyan helyszínek, ahol ingyenes wi-fi használat van biztosítva, vagy ki van írva a wi-fi jelszó pl. a kávézóban a bárpulton vagy egy szállodában. A támadók akár a nyílt hálózatot is kompromittálhatják vagy létrehozhatnak rouge AP-ket, ami egy rosszindulatú másolataként tűnik fel az eredeti wi-fi hozzáférési pontnak. Amennyiben a felhasználói készülékeken elmentésre került a lemásolt vezeték nélküli hálózat neve, a támadó már a saját hálózatában fogadva könnyedén ellophatja az áldozat szenzitív információit pl. netbank belépési adatait.

Felugró ablak. A felugró ablakok ráveszik a felhasználókat, hogy egy olyan hivatkozásra klikkeljenek, ami átirányítja őket egy hamis weboldalra. Itt személyes információkat kérhetnek tőlük vagy kártékony programok töltődnek le a számítógépükre úgy, mint a már említett keyloggerek, trójaiak és a vírusok is. A megjelenő pop-up ablakok általában valamilyen nem létező operációs rendszerbeli problémára és egyben megoldására hívják fel a figyelmet. Ezzel csábítják a felhasználókat és kihasználják kíváncsiságukat, hogy ráklikkeljenek az adott linkre, amivel hozzájuthatnak a szolgáltatáshoz vagy akár egy értékes nyereményhez. Ellophatnak hálózati login adatokat is azzal, hogy a hálózati kapcsolat megszakadásának színlelése miatt a megjelenő adatmezőkben újbóli bejelentkezést, hitelesítést kérnek a felhasználótól. Amikor a felhasználó követi ezeket az instrukciókat a kártékony program telepítődik a számítógépre, információkat szivárogtatva ki a támadónak.

Üzleti e-mail kompromittálás. Business Email Compromise-ként (BEC) ismert jelenség az angolszász államokban jelent meg először, majd lassan szinte az egész világon elterjedtté vált. A csalók a pénzügyi tranzakciók lebonyolításában részt vevő illetékes személyeket ejtik tévedésbe azáltal, hogy magukat a felettesüknek vagy partnercég képviselőjének adják ki és idegen bankszámlaszámra kérik az utalás teljesítését. A kivitelezés során a támadók nyílt online forrásokból (pl. cég weblapja, cég adatbázis, közbeszerzési szerződés részletei stb.) vagy akár kuka búvárkodás során megszerzett információkból megtudják az adott vállalatnál dolgozó felső vezető, valamint pénzügyi területen dolgozók nevét és email címét. A profilalkotást követően és a szükséges mennyiségű adatok birtokában, a csaló magát a partnercég képviselőjének kiadva – formailag és tartalmilag hitelesnek tűnő – e-mail üzenetben arról tájékoztatja az áldozatot, hogy a jövőben egy másik bankszámlaszámra utaljanak. Amennyiben a célpont vezetőjét kívánja megszemélyesíteni a támadó, azonnali utalásra utasítja a beosztottját. Amennyiben nem sikerül az e-mail címet teljes mértékben utánozni, az eredetihez nagymértékben hasonlító e-mail címmel és a sürgősség, fontosság látszatának keltésével többnyire sikeresen kivitelezhetőek az e fajta támadások. A magánszemélyeket célzó változatában a támadók privát postafiók felett veszik át az irányítást, ezt a típusát E-mail fiók kompromittálásnak, azaz Email Account Compromise-nak hívják (EAC). 2019-ben az FBI IC3 központja 23.775 db BEC/EAC típusú panaszról kapott bejelentést, ami több mint 1,7 milliárd $ kárt okozott a sértetteknek.

Kép és videó hamisítás. A deep fake-nek nem kifejezetten célja a közvetlen anyagi haszonszerzés. Elsősorban reputáció csökkenést vált ki, de egyre inkább az emberek véleményének manipulálásának eszközévé vált, mint ahogy a fake news is. Ennek szerepe főleg a választási ciklusok idején éleződik ki. Kezdetben álló képeken lévő személyek arcát vagy a kezükben lévő tárgyakat, háttereket módosították. A technika fejlődésével és a célszoftverek megjelenésével az elmúlt években azonban video anyagok szereplőinek arcát és hangját is sikerült fiktív tartalommal ellátni. A módosítással elérhető hatás lehet akár megalázó (pl. szexuális tartalom esetén) vagy társadalmilag, morálisan elítélendő is. Célpontjainak tekinthetjük akár az egész online közönséget, akik az álvideókat potenciálisan megtekintik, de igazi áldozatai azok a politikusok, celebek, hírességek, akiknek visszaélnek az arcával és hangjával.

Telefonos technikák

A kiberbűncselekmények növekedésének egyik oka a mobil technológia fejlődése. A mobil alapú internetet napjainkban már telefonról, tabletről, különböző okos eszközökről is könnyedén el tudjuk érni. Szinte állandóan online lehetünk a különböző instant üzenetküldő szolgáltatásoknak köszönhetően. Ez a közvetlen hozzáférés kényelmet, egyben kockázatot is jelent a felhasználóknak. A támadók okostelefonra készült mobil alkalmazásokat is használhatnak, hogy végrehajtsanak mobil alapú social engineeringet. Ennek eredményeként sok trükk jelent meg, amivel becsaphatják az embereket.

SMS. A smishingben az SMS szöveg küldő rendszert használják csaliként a hackerek, egy olyan cselekvés kifejtésére, amivel rá tudják venni az áldozatot, hogy megnyissa az üzenetben lévő linket. Ezzel akár közvetlenül letölthetnek egy malwaret, átirányítja őket egy káros weboldalra vagy felhívhatnak egy emelt díjas telefonszámot is. Másik változata az SMS csatorna kihasználásának az adathalászat, amikor különböző ürüggyel (pl. adategyeztetés) személyes adatokat, bankkártya adatokat kérnek a csalók az ügyfelektől. A megszerzett bankkártya adatokat a bűnözők online vásárlásra is felhasználhatják vagy értékesíthetik a darkneten. Jellemző, hogy a social engineerek ezen a csatornán is igyekeznek kihasználni a pandémia okozta helyzetet. Az US Cybersecurity and Infrastructure Security Agency és a UK's National Cyber Security Centre közleményében [14] egy ilyen módszerre hívja fel a figyelmet. Itt az Egyesült Királyságban lévő állampolgároknak ígérnek pénzt, a koronavírus elleni harchoz. A linkre való kattintással a nevüket, e-mail címüket, lakcímüket és banki adataikat gyűjthetik be a csalók az áldozatoktól.

Kártékony mobilalkalmazás. A támadó először létrehozza magát a káros kódot tartalmazó alkalmazást, ami akár egy játéknak vagy más érdekes alkalmazásnak is tűnhet. Általában ezen funkciót is ellátja a valódi célja mellett. Ezt követően feltölti az alkalmazásokat kínáló webes platformokba, majd várja, hogy a felhasználó az applikáció leírása, ikonja, – esetenként manipulált – pozitív vélemények alapján letöltse az alkalmazást. Mivel a legtöbb esetben az emberek eredetinek hiszik a terméket, így letöltik, majd telepítik az eszközükre. Ezzel már kezdetét is vette az eszköz fertőzése és máris veszélyben vannak a felhasználó hitelesítő adatai (pl. login nevek, jelszavak), mivel azokat elküldheti a malware készítőjének. Vagy rosszabb esetben teljesen átvehetik a kontrollt az áldozat telefonja felett, hozzáférve névjegyzékéhez, fotóihoz, feljegyzéseihez, emailjeihez. A Symantec felmérése szerint 2018-ban minden 36. mobiltelefonon magas kockázati besorolású applikáció volt telepítve vagy rendszergazdai jogosultsággal futottak. Ez utóbbiakat rootolt vagy jailbreakelt eszközöknek nevezzük [15]. Az ilyen telefonok használata nagy biztonsági kockázattal jár. Napi aktualitás vonatkozásában megemlítendő, hogy a Checkpoint 2020. áprilisi beszámolójában [24] 16 különböző káros alkalmazásról ad hírt, melyeket a koronavírus járvánnyal összefüggésben hoztak létre a terjesztői. Ezek hivatalos alkalmazásként tüntetik fel magukat, azonban céljuk a felhasználói adatok ellopása, vagy prémium szolgáltatások generálása révén bevételhez jutni.

Hamis biztonsági alkalmazás. A támadó első lépésben megfertőzi az áldozat számítógépét egy olyan kártékony programmal, ami érzékeli a netbank belépési szándékot.

Ekkor a rendszerképernyőn megjelenő felugró ablakban jelzi a felhasználónak, hogy egy mobiltelefonos alkalmazást kell letöltenie a netbankba való bejelentkezéshez, ugyanis ott fogja megkapni a biztonsági üzenetet. Ezzel a kétfaktoros hitelesítés biztonságérzetét használja ki a támadó, elhitetve az áldozattal, hogy ez egy újabb plusz biztonsági funkció a netbank használatához. Az ajánlott alkalmazás természetesen a támadó által írt applikáció lesz. Amikor a felhasználó letölti az appot a támadó megszerzi a bizalmas információkat úgy, mint banki belépési hitelesítő adatok (felhasználónév, jelszó) és utána a valódi, második faktoros hitelesítő kódot is, amit a bank küld az áldozatnak pl. SMS-en keresztül. Felhasználva ezt az információt, egy támadó hozzáfér az áldozat bankszámlájához és anyagi kárt okozhat neki.

Újracsomagolt alkalmazás. Adott egy mobil alkalmazás, ami azt teszi, amit tennie kell mindenféle kártékony mellékhatás nélkül. A támadó egyszerűen letölti a népszerű applikációt az áruházból majd az általa írt malwaret hozzáadja, mintegy újracsomagolja az alkalmazást és ő is feltölti. Amikor a felhasználó letölti a már rosszindulatú alkalmazást, a kártékony program telepítődik a mobiljára, gyűjti a bizalmas információkat és elküldi azokat a támadónak.

Instant üzenetküldő. Egy támadó instant üzenetküldő alkalmazásokon keresztül online cseveghet a kiválasztott áldozattal. Miután a bizalmába férkőzött, megpróbál személyes információt szerezni tőle, amiket felhasználhat arra, hogy feltörje a felhasználó fiókjait. De összetettebb támadást is indíthat, – használva a korábban említett megszemélyesítéses technikát – egy hamis profilt bemutatva az áldozatnak ráveheti különböző jogcímen pénz utalásra is, abban a hiszemben, hogy ezt később busásan vissza fogja kapni. Ide sorolható még az e fajta platformokon kapott üzenetek, melyekben a közvetlen linkre rákattintva káros tartalmak töltődhetnek le a telefonunkra. A linkek címe, animált képe első ránézésre megnyerő lehet, érzelmekre, egészségre, pénzügyekre utaló címekkel ellátva nagy csábítást jelent a megtekintésre. Tartalmazhatnak továbbá csaliként kedvezményes utazáshoz, biztonsági frissítéshez vagy adathalász oldalra irányító linkeket is.

Csaló hívás. A telefonon keresztül elkövetett cselekmények közül a csalások igénylik a legkevesebb technikai ismeretet a támadó részéről. Itt viszont annál inkább szüksége van a már korábban említett manipulációs módszerek igénybevételére, ugyanis csak pár perc áll rendelkezésre, hogy végrehajtsa a műveletet. Nehézsége, hogy kizárólag a verbális kommunikációs csatornát használhatja. A telefonos technikákról szóló rész zárásaként három jellegzetes módszer végrehajtását szeretnénk a humán aspektus oldaláról részletesebben bemutatni.

A Büntetőtörvénykönyvről szóló 2012. évi C. törvény 373. § (1) bekezdése kimondja, hogy aki jogtalan haszonszerzés végett mást tévedésbe ejt vagy tévedésben tart és ezzel kárt okoz, csalást követ el [25]. Az utóbbi időkben elszaporodott úgynevezett „unokázós csalások” is ezen alapulnak. A támadó az esti órákban felhívja az idős, jellemzően egyedülálló áldozatát, majd olyan rövid történetet hitet el vele, melyben az érzelmi ráhatásnak nagy szerepe van. Felderítő tevékenységük során a telefonkönyvekben főként az „özv.” előtaggal vagy a hagyományos „-né” utótaggal szereplő személyeket célozzák meg, akikről feltételezik, hogy egyedül élhetnek. A célszemélyeket néha közösségi portálon vagy

lakóhelyük megfigyelése útján is feltérképezik. A hívó magát valamilyen hatóság munkatársának adja ki és azzal keríti hatalmába az aggódó nagyszülőt, hogy elhiteti vele azt, hogy súlyos közlekedési balesetet okozott a gyereke, unokája. A megfelelő egészségügyi ellátás és a rugalmasabb jogi ügyintézés végett hozzátartozójának azonnali készpénzre van szüksége. Itt kihasználják még a sürgetést (pl. mindjárt viszik a rabkórházba), mint időtényezőt, valamint a kitalált életveszélyes helyzetet (pl. a bordája átszúrta a tüdejét). De olyan is előfordul, hogy kifejezetten megkéri a csaló a sértettet, hogy másnak ne mondja el, mert bajba kerülhet. A készpénzért, vagy ennek hiányában ékszerért már személyesen küldi el a csaló az egyik társát, aki adott esetben rendőrnek adja ki magát, ezzel a hitelesség látszatát keltve a rémült áldozatban. Az érték átadásnál már át is lépett a támadó társa a humán technika megszemélyesítés módszerének a használatához, melyben különböző kellékek (pl. Rendőrség feliratos póló, jelvény, stb.) segítenek szerepe eljátszásában. Az aktualitását ennek a módszernek mi sem mutatja jobban, minthogy a csalók alkalmazkodtak a jelenlegi járványügyi helyzethez: „próbálkoznak telefonon is, egy kórház munkatársának kiadva magukat felhívnak valakit, majd azt hazudják, hogy az egyik rokonuk megfertőződött a koronavírussal, és ki kell fizetni az orvosi költségeket" [26].

Az elmúlt években ütötték fel fejüket a „feltöltőkártyás csalások", ahol az elkövetők általában valamelyik telefonszolgáltató nevével élnek vissza. Jellemzően az emberek hiszékenységére, kapzsiságára utaznak. Felderítő tevékenységük nem túl kifinomult, teljesen véletlenszerűen vagy folyamatos növekvő sorrendbe tárcsázva, naponta akár több száz hívást is lebonyolítanak. ATM-en, POS terminálon vagy SMS küldés útján különböző telefonszámok egyenlegeit töltetik fel a gyanútlan sértettel. Az áldozat ezalatt abban a hiszemben van, hogy eközben gyarapodik a begépelt összeggel a számlája vagy éppen a nyerő kódot üti be, mely a nyeremény utalásához szükséges. A valóságban azonban az elkövetők vagy hozzátartozóik használatában lévő telefonszámainak az egyenleg feltöltését hajtják végre. A tévedésbeejtő szöveg általában sorsoláson nyert pénznyeremény, amit esetenként kombinálni szoktak az elkövetők nagyértékű televízió vagy telefonkészülék ajándékkal is. A sértettek általában a következő havi számlakivonaton értesülnek a csalásról, vagy amikor hívás után felhívták a valós telefonszolgáltatójukat, mert mégis gyanakodni kezdenek. Az áldozatok közül szinte senkinek nem tűnik fel, hogy ha nem regisztráltak semmiféle nyereményjátékban, így nem is nyerhettek azon. De olyan tévedésbe ejtő szöveg is ismert, amiben csak egyszerűen kötelező előfizetői adategyeztetésre, központi rendszer újraindítása miatti ellenőrzésre, mobilkészülék vírusírtásra vagy biztonsági ellenőrzésre hivatkoznak. Ez esetben a személyes adatok megszerzése a cél, melyet későbbi social engineering támadásokban felhasználnak. Fenti módszer továbbfejlesztett változatában az elkövetők különböző ürüggyel (pl. adóvisszatérítés átutalása) magát a hatóság munkatársának kiadva elkérik a sértettektől a bankkártyájuk adatait, mellyel internetes tranzakciókat bonyolítanak le. Ezek jellemzően webáruházból való vásárlások, valamint telefonkártya egyenleg feltöltések. Mivel ez esetben már konkrét felhasználása történik a bizalmas adatoknak (bankkártya adatok), így az elkövető cselekményével a Btk. 375.§ (1) bekezdésébe ütköző információs rendszer felhasználásával elkövetett csalás bűncselekményét valósítja meg [25]. Információs rendszer vonatkozásában adatbevitelnek, megváltoztatásnak, hozzáférhetetlenné tételnek kell történnie vagy olyan műveletnek, ami a rendszer működését befolyásolja. Ennél a bűncselekménynél jellemzően adatbevitelről beszélhetünk, ami a jogos felhasználó tudta és beleegyezése nélkül zajlik.

Végezetül érdemes megemlíteni a klasszikus „telefon betyárkodás”-t, amit akár az utcai fülkés telefonkészülékkel, akár hagyományos mobiltelefonok felhasználásával is végre lehet hajtani. A Btk. 338.§ (1) bekezdésébe ütköző közveszéllyel fenyegetést követ el, aki a köznyugalom megzavarására alkalmas olyan valótlan tényt állít, híresztel, vagy azt a látszatot kelti, hogy közveszéllyel járó esemény bekövetkezése fenyeget, bűncselekményt követ el [25]. Ami a telefonálónak adott esetben vicces vagy szándékosan szabotáló célú (pl. bírósági tárgyalás elhalasztása), az a rendvédelmi szerveknek erő, eszköz és nagy anyagi ráfordítással járó rendkívüli feladatot jelent. Itt jellemzően bombariadóra kell gondolni, amit elkövettek már pénzintézetek, bíróságok, iskolák ellen is. A hívást fogadó diszpécsert ez esetben nem lehet áldozatnak tekinteni, hiszen belső szabályzatok sokasága írja elő az ilyenkor szükséges halaszthatatlan intézkedések megtételét. Nem mérlegelhet a hívás valódiságát illetően az ügyeletes, még ha – tapasztalatai és a háttérzajok alapján – előre sejthető is a hívás komolytalansága.

ZÁRÓ GONDOLATOK

Az informatikai rendszerek, eszközök és alkalmazások használatánál nem a technika, hanem az azt használó ember a leggyengébb láncszem, aki többek között pszichikumából, társas lény voltából, szocializációjából és a társadalmi elvárásoknak való megfelelési kényszerből adódóan viszonylag könnyen és meglehetősen változatos módon manipulálható. Ezt használják ki azok a social engineerek, akik vagy a humán, vagy az IT alapú technikák használatával (de ez utóbbinál is az emberi gyengeségre, hiszékenységre alapozva) információkat szereznek meg áldozatuktól, visszaélnek azzal, vagy az általuk elvárt viselkedésre bírnak rá gyanútlan (és gyakran az elkényelmesedés miatt felelőtlen) felhasználókat. Jelen tanulmányunkban a fontosabb módszereket mutattuk be, s ezen elméleti részszel, valamint a kapcsolódó példákkal alapoztuk meg tanulmányunk következő részét, amelyikben elsősorban az információbiztonság humán oldalával foglalkozó nagymintás kutatásunk fontosabb eredményeit, valamint az ezekből levonható következtetéseket ismertetjük.

FELHASZNÁLT FORRÁSOK

Irodalom

[1] PurpleSec’s Cyber Security Experts, The Ultimate List Of Cyber Security Statistics For 2019, (letöltve: 2020.04.12.) [online] https://purplesec.us/resources/cyber-security-statistics/#SocialEngineering
[2] M. Guenther, *„Social Engineer - Security awareness series”*, M. Guenther LLC., 2001. [online]
https://www.coursehero.com/file/38974373/ (letöltve: 2020.05.14.)
[3] K. D. Mitnick, W. L. Simon, *„A legendás hacker – a megtévesztés művészete”*, Budapest: Perfact Pro Kft., 2003.
[4] EC-Council, Certified Ethical Hacker v10 – Social Engineering Module 09. [online] https://www.eccouncil.org
[5] E. D. Oroszi, „Social engineering technikák”, in.: V. Deák, Ed., *Célzott kibertámadások*, Budapest: NKE, 2018.
[6] Biblia, Máté 7:7, Budapest: Magyarországi Ref. Egyház Kálvin János Kiadója, 1990.

[7] T. Sörös Tamás, D. Váczi, *„Social engineering a biztonságtechnika tükrében”*, bemutatva XXXI. OTDK Had- és Rendészettudományi Szekció, Budapest, 2013.
[8] E. D. Oroszi, *„Social Engineering – Az emberi erőforrás, mint az információbiztonság kritikus tényezője,”* B.S. szakdolgozat, Budapesti Corvinus Egyetem, Budapest, 2008.
[9] J. Crume, *„Az internetes biztonság belülről – amit a hekkerek titkolnak,”* Bicske: Szabad Tér Kiadó, 2003.
[10] D. Krishnaswamy „World's Worst (Most Common) Passwords,” Security Scorecard.com
https://securityscorecard.com/blog/worlds-worst-passwords (letöltve: 2020.04.17.)
[11] Varonis, 2019 Data Risk Report Stats and Tips You Won’t Want to Miss (letöltve: 2020.04.17.) [online] https://www.varonis.com/blog/data-risk-report-highlights-2019
[12] A. O'Donnell „What Is a Road Apple Social Engineering Attack?” Lifewire.com, https://www.lifewire.com/what-is-a-road-apple-social-engineering-attack-2487194 (letöltve: 2020.03.12.)
[13] RSA Quarterly Fraud Report Vol. 2, Issue 4, Q4 2019. (letöltve: 2020.04.17.) [online] https://www.rsa.com/en-us/offers/rsa-fraud-report-q4-2019
[14] US DHS CISA and the UK NCSC, Alert (AA20-099A) COVID-19 Exploited by Malicious Cyber Actors [online] https://www.us-cert.gov/ncas/alerts/aa20-099a (letöltve: 2020.04.19.)
[15] Symantec Internet Security Threat Report Volume 24, 2019. február [online] symantec.com
[16] IBM Security X-force Threat Intelligence Index 2020. (letöltve: 2020.03.12.), [online] ibm.com/security/data breach/threath intelligence index
[17] ESET, Zsarolóvírus, (letöltve: 2020.03.12.), [online]
https://www.eset.com/hu/zsarolovirus/
[18] F. Mouton, L. Leenen, M. M. Malan and H.S. Venter, „Towards an Ontological Model Defining theSocial Engineering Domain”, In: K. Kimppa et al., Eds. *ICT and Society.* HCC 2014. IFIP Advances in Information and Communication Technology, vol 431. Berlin, Heidelberg: Springer, 2014.
[19] Kitekintés az elmúlt évek legsúlyosabb kiberbotrányaira, Securinfo.hu
https://www.securinfo.hu/termekek/it-biztonsag/8403-kitekintes-az-elmult-evek-legsulyosabb-kiberbotranyaira.html (letöltve: 2020.03.12.)
[20] Crowdstrike 2020 Global Threat Report, (letöltve: 2020.03.12.), [online]
crowdstrike.com/reports
[21] Interpol, Cybercriminals targeting critical healthcare institutions with ransomware, Interpol.int https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware (letöltve: 2020.04.19.)
[22] G. Szappanos, *„Kirándulás a számítástechnika sötét oldalára”*, Budapest: VirusBuster Kft., 2003.
[23] S. Chernyshev, D. Chipiristeanu, *„Less aggressive, more effective: social engineering with paid archives,”* VB2012, Dallas [online] Elérhető:https://www.virusbulletin.com/uploads/pdf/conference_slides/2012/ChernyshevChipiristeanu-VB2012.pdf
[24] A. Hazum, O. Mana, I. Wernik, B. Melnykov and C. Efrati „COVID-19 goes mobile: Coronavirus malicious applications discovered,” Check Point, 2020.04.09, (letöltve:

2020.04.19.) [online] Elérhető:https://research.checkpoint.com/2020/covid-19-goes-mobile-coronavirus-malicious-applications-discovered/
[25] 2012. évi C. törvény a Büntető törvénykönyvről
[26] Origo, A rendkívüli időszakban még inkább az idősekre vadásznak a csalók, Origo.hu [online] https://www.origo.hu/itthon/20200318-unokazos-modszerrel-a-koronavirusra-hivatkozva-keresik-a-csalok-az-idosebbeket.html (letöltve: 2020.04.19.)
[27] C. Hadnagy, *„Unmasking the Social Engineer – The human element of security”*, Hoboken: Wiley, 2014.