1.08 Objavljen znanstveni prispevek na konferenci
1.08 Published Scientific Conference Contribution

Marko POTOKAR[*]*, Sanja ANDROIĆ*[**]

SOCIALNI INŽENIRING – ČLOVEK KOT DEL VARNOSTNEGA SISTEMA

Izvleček:

Kot za večino pojmov obstaja tudi za pojem socialni inženiring več definicij. Gre za žargonski izraz, pomeni pa vzpodbujanje nezavednega aktivnega sodelovanja, s prepričevanjem ciljnih oseb (žrtev), da posredujejo določene informacije. Napadalci uporabljajo ta termin za tehnike vdorov v sistem, ki temeljijo na izkoriščanju lastnosti (slabosti) človeške nravi. Lahko rečemo, da je socialni inženiring tehnika, s katero storilec pripravi žrtev, da stori ali opusti dejanja, ki jih običajno ne bi storila ali opustila. Sicer pa metode socialnega inženiringa niso nič novega. Razvite so bile s strani vojske, obveščevalnih služb in varnostnih agencij, izvedencev za industrijsko vohunjenje.

V prispevku bo predstavljen pojav socialnega inženiringa kot ene izmed najbolj podcenjevanih, hkrati pa najnevarnejših metod zlorabe človekovega zaupanja. Odkrili bomo, kakšni mehanizmi botrujejo temu pojavu in zakaj smo ljudje glede njega tako ranljivi. Spoznali bomo metode socialnih inženirjev in si pogledali, kako socialni inženiring s pridom izkorišča razširjenost socialnih omrežij. Predstavili bomo tudi, kako bi lahko socialni inženirji škodljivo vplivali na dokumentarno ali arhivsko gradivo v elektronski ali papirni obliki ali ga celo resno ogrozili.

Ključne besede:

socialni inženiring, napadalci, žrtve, dokumentarno gradivo, arhivsko gradivo

Abstract:

Social Engineering – A Man as Part of the Security System

As for most concepts, there are also several definitions of the social engineering concept. It is a jargon term, which stands for encouraging unconscious active cooperation by persuading target persons (victims) to deliver certain information. This term is used for system invasion techniques, based on taking advantage of the features (weaknesses) of human nature. We can say that social engineering is a technique used by the perpetrator to make the victim do or give up actions they would normally not do or give up. The methods of social engineering are nothing new. They were developed by the army, intelligence services, security agencies and industrial espionage experts.

This article presents the phenomenon of social engineering as one of the most underrated and at the same time the most dangerous methods of the abuse of human confidence. The authors will describe mechanisms responsible for this phenomenon and why people are so vulnerable to it. The methods of a social engineer will be presented and the article will show how social engineering uses the widespread phenomenon of social networks to its profit. We will also show how social engineers could harmfully influence records or archives in electronic or paper form, or even seriously endanger it.

Key words:

social engineering, attackers, victims, records, archives

[*] *Mag. Marko Potokar, Inštitut za varnostno kulturo, Tržaška cesta 132, 1000 Ljubljana, Slovenija, kontakt: marko.potokar@institut-ivk.si.*

[**] *Sanja Androić, vodja sprejemne pisarne, Mariborski vodovod, javno podjetje, d. d., Jadranska cesta 24, 2000 Maribor, Slovenija, kontakt: sanja.androic@mb-vodovod.si.*

1 UVOD

V prispevku bomo s pomočjo sekundarnih podatkov iz domače in tuje strokovne literature predstavili pojav socialnega inženiringa kot ene izmed najbolj podcenjevanih, hkrati pa najnevarnejših metod zlorabe človekovega zaupanja. Odkrili bomo, kakšni mehanizmi botrujejo temu pojavu in zakaj smo ljudje glede njega tako ranljivi. Predstavili bomo tudi metode socialnih inženirjev in načine, kako socialni inženiring s pridom izkorišča razširjenost socialnih omrežij. Z metodo deskripcije bomo opisali osnove, z metodo kompilacije pa bodo predstavljena teoretična izhodišča različnih avtorjev. Slednjim bodo dodane še lastne izkušnje iz prakse. Na koncu prispevka bomo predstavili tudi nekaj praktičnih primerov, med njimi so tudi primeri, ki kažejo, na kakšen način bi lahko socialni inženirji škodljivo vplivali na dokumentarno ali arhivsko gradivo v elektronski in v papirni obliki ali ga celo resno ogrozili. Z našim raziskovanjem smo želeli pridobiti odgovor na vprašanje, ali je človek med najšibkejšimi členi varnostnega sistema v primeru napadov socialnih inženirjev. Odgovor na zastavljeno vprašanje bomo pridobili s proučitvijo teoretičnih izhodišč, ki jih bomo povezali z izkušnjami iz prakse.

2 ČLOVEK KOT DEL VARNOSTNEGA SISTEMA

Pogosto v strokovni literaturi pri definiciji varnostnega sistema naletimo na navedbo, da varnostni sistem sestavljajo naslednje komponente: pravila in postopki, tehnologija in človek (ljudje). Pravila predstavljajo okvir sistema, postopki opišejo procese, tehnologija zagotavlja (podpira) skladnost s pravili, človek pa postopke izvaja. Kot primer je lahko v podjetju sprejeto ***pravilo***, da morajo zaposleni ob odsotnosti z delovnega mesta zakleniti zaslon računalnika. Kako se izvede ***postopek***, je opisano v pripadajočem navodilu (hkratni pritisk določenih tipk na tipkovnici itd.). ***Človek*** postopek izvaja - ali pa tudi ne. Zato se za zagotavljanje skladnosti s pravili uporablja ***informacijska tehnologija***, ki omogoča avtomatsko zaklepanje zaslona po preteku določenega časa.

Varnostni sistem torej sestavljajo pravila in postopki, tehnologija in človek, vendar ima pri tem človek globljo in širšo vlogo. Kot izvajalec je sestavni del (element) varnostnega sistema, obenem pa je tudi tvorec pravil, postopkov in tehnologije. Je pa človek tudi zmotljivo bitje. Kdor dela, dela tudi napake. Glede na to, da je celoten varnostni sistem prežet s človekovim (ne)delovanjem, lahko trdimo, da je človek bistvena komponenta varnostnega sistema. Od zaposlenih, ki imajo dostop do informacijskih virov podjetja, se pričakuje, da bodo te vire ustrezno ščitili. Za posameznike, ki imajo dostop do občutljivih informacij, mora podjetje vpeljati ustrezne kontrolne mehanizme (Peltier, 2002). Varnostni standard ISO/IEC 27001 tako upravljanju s človeškimi viri z vidika varnosti namenja posebno poglavje, v katerem obravnava varovanje človeških virov pred in med zaposlitvijo ter po njej, s ciljem zagotoviti, da zaposleni, pogodbeniki in uporabniki tretje stranke razumejo njihove odgovornosti in so primerni za vloge, ki so jim namenjene, ter za zmanjšanje tveganja kraje, prevare ali zlorabe zmogljivosti. Pomembno je tudi, da se zaposleni, pogodbeniki in uporabniki tretje stranke zavedajo groženj in skrbi, ki ogrožajo varnost informacij, svojih odgovornosti in obveznosti, da so opremljeni za podporo politike varovanja informacij organizacije med svojim običajnim delom kakor tudi za zmanjšanje tveganja človeških napak in da zaposleni, pogodbeniki in uporabniki tretje stranke zapustijo organizacijo ali zamenjajo zaposlitev na urejen način (BSI, 2005a in b).

Prav zaradi pomembnosti človekove vloge v informacijskih sistemih sodijo tehnike socialnega inženiringa med najbolj nevarne napade na varovane sisteme.

3 SOCIALNI INŽENIRING

Kot za večino pojmov obstaja tudi za pojem socialni inženiring več definicij. Gre za žargonski izraz, pomeni pa vzpodbujanje nezavednega aktivnega sodelovanja, s prepričevanjem ciljnih oseb (žrtev), da posredujejo določene informacije. Napadalci uporabljajo ta termin za tehnike vdorov v sistem, ki temeljijo na izkoriščanju lastnosti (slabosti) človeške nravi. Informacijski pooblaščenec Republike Slovenije v svojih smernicah navaja, da »socialni inženiring po svoji naravi pomeni predvsem pridobivanje nekih koristi z zlorabo zaupanja posameznika oz. z manipulacijo« (Informacijski Pooblaščenec, 2009). Bernik in Prislan (2012) posredno definirata socialni inženiring z navedbo, da "/n/apadalec s pomočjo socialnega inženiringa prepriča uporabnika, da mu zaupa podatke, s katerimi se bo lahko prijavil v napadeni sistem«. **Lahko rečemo, da je socialni inženiring tehnika, s katero storilec pripravi žrtev, da stori ali opusti dejanja, ki jih običajno ne bi storila ali opustila.**

Pojav novodobnega socialnega inženiringa sega na področje hekerstva - vdiranja v informacijske sisteme. Izraz heker se nanaša na tiste, ki vdirajo v računalnike brez ustreznih pooblastil oziroma si te neupravičeno pridobijo (Peltier, 2002). Hekanje pa se pravzaprav ni začelo z računalniškimi hekerji, ampak s *frikerji*. Lahko bi rekli, da brez telefonskih žic hekanja ne bi bilo. Vse skupaj se je začelo s telefoni oziroma z uporabo avtomatskih telefonskih central, ki so bile krmiljene s pomočjo tonov različnih frekvenc. Telefonski hekerji so se imenovali *telefonski friki* (*angl. phone phreaks)*. Beseda *phreaking* je sestavljanka angleških besed *freak*, *phone* in *free*. Le-ti so v telefonski sistem vdirali (se lažno predstavljali) z uporabo naprav za proizvajanje tonov določene frekvence. Za to so bile sprva dovolj kar plastične piščalke, ki so jih iznajdljivi frikerji dobili v škatli za kosmiče (nekateri so namesto tega uporabljali kar svoje naravno zvočilo – ustno votlino in ustnice). Eden izmed pionirjev telefonskih frikov je bil elektroinženir John Draper alias Captain Crunch. Sčasoma se je oblikovala skrivna družba telefonskih frikov, ki so si na srečanjih zagotavljali anonimnost celo z uporabo mask. Pa manipulacija telefonskih stikal ni bila dovolj. Pričeli so tudi z manipulacijo telefonskih uslužbencev. Veščino so imenovali ***socialni inženiring***. Obdobje telefonskega frikanja so končali ameriški zvezni preiskovalci (FBI) z aretacijo najodmevnejših članov združbe, med katerimi je bil tudi Captain Crunch, ki je vsled svojih dejanj v zaporu zato presedel štiri mesece. Na pogorišču se je rodila nova generacija frikov – hekerji.

Tistemu, ki za dosego ciljev uporablja metode socialnega inženiringa, pravimo ***socialni inženir***. Delovanje socialnega inženirja temelji na (zlo)rabi posameznikovega zaupanja. Storilec se za dosego namena poslužuje majhnih (in verjetnih) laži, prevar in zvijač. Izkorišča različna čustvena in psihična stanja žrtev. Izkorišča nezadovoljstvo v službi, 'prijateljstvo' na delovnem mestu, igra vlogo 'prijazne' stranke, se lažno predstavlja itd. Dober socialni inženir tako ugaja ljudem, da mu zaupajo. Je simpatičnega videza, šarmanten, ustrežljiv, prijazen, ima dobre govorne sposobnosti, je priljubljen med ljudmi, zna pridobiti zaupanje, je dober psiholog in sociolog (raje laični kot pa diplomirani), skratka nekdo, ki bi ga, čeprav je neznanec, z veseljem spustili v svojo dnevno sobo.

3.1 Metode socialnega inženiringa

Metode socialnega inženiringa so bile razvite s strani vojske, obveščevalnih služb in varnostnih agencij ter izvedencev za industrijsko vohunjenje. Obstaja več načinov, kako socialni inženir pride do svojega cilja. Tako Verdonik in Bratuša (2005, str. 118-119) menita, da so najbolj razširjene metode socialnega inženiringa naslednje:

- »prijateljstvo (vstopna gesla se širijo na osnovi zaupanja med zaposlenimi),
- elektronska pošta (ponarejanje naslova pošiljatelja),
- pregledovanje smeti podjetja (razkrije lahko uporabne informacije),
- pregled pisarn (napadalec vohlja po odklenjenih pisarnah in kabinetih),
- zaupanje (napadalec si pridobi zaupanje zaposlenih),
- čas (je vedno na strani napadalca).«

Metode socialnega inženiringa lahko delimo tudi v dve večji skupini: metode, ki za izvedbo uporabljajo informacijsko tehnologijo (*angl.: computer based attack*), in metode, temelječe na človeški interakciji (*angl.: human based attack*). Z metodami iz prve skupine poskuša socialni inženir preslepiti tarčo s pomočjo uporabe tehnologije. Primer takega napada je pojavitev lažnega okna (*pop-up menu*), ki uporabnika obvešča, da je prišlo do prekinitve povezave in da mora zato ponovno vnesti uporabniško ime in geslo. Še vedno pa so najpopularnejše metode iz druge skupine, ki temeljijo na človekovih medsebojnih odnosih in preslepitvi (@SANS Institute, 2001).

Ena izmed metod je tudi igranje vloge nebogljenega novozaposlenega: podjetje zaposli novega delavca. Le-ta je simpatičen, uslužen, lepo vzgojen, a rahlo 'neroden'. Pravzaprav pri določenih stvareh že kar nebogljen. Ljudje pa radi pomagamo, sploh če oseba v nas prebudi določen občutek, simpatijo. Kako vendar ne bi pomagali tudi novozaposlenemu, pa čeprav za ceno izdaje gesla in drugih pomembnih informacij. ***Reverse social engineering*** predstavlja tehniko, ko socialni inženir namenoma povzroči določeno odpoved v informacijskem sistemu (npr. odpoved računalnika zaposlenega - žrtve), nato pa ponudi svojo pomoč pri odpravi 'napake' (pri tem pa ponavadi 'potrebuje' tudi geslo žrtve). ***Shoulder surfing*** je angleški izraz za *gledanje čez ramo*. Primer te uspešno uporabljene tehnike je zloraba na bankomatih, le-ta se je dogajala tudi na domačih tleh: napadalci so v režo bankomata (tisto, v katero s takim pričakovanjem vtikamo bankomatsko kartico) namestili dodaten čitalec magnetnega zapisa, ki je seveda s kartice prebrane podatke posredoval v oddaljeno napravo. Za uspešno ponareditev in uporabo kartice je bila potrebna le še osebna številka (PIN). Kako do nje? Storilec se je preprosto postavil 'v vrsto' za žrtvijo in s pogledom 'preko ramena' pridobil informacijo, kakšno osebno številko je žrtev vtipkala na tipkovnici bankomata. Ena izmed najbolj tveganih tehnik za napadalca je tako imenovan ***Direct approach***. Pri tem napadalec do žrtve pristopa z neposredno zahtevo, temelječo na lažnih pooblastilih. Poleg naštetih tehnik sta dobro poznana še dva načina: ***uporaba tehničnih sredstev*** (prisluškovalne naprave, mini fotoaparati) in ***brskanje po smeteh***.

Kevin Mitnick opredeljuje naslednja nagnjenja človeške psihe, ki jih izkorišča socialni inženir (Mitnick, 2002):

- Avtoriteta – storilec prepriča žrtev tako, da se izdaja za osebo z določenim vplivom, ki se ji je žrtev pripravljena podrediti.

- Naklonjenost – storilec pridobi naklonjenost žrtve tako, da poišče skupne točke z žrtvijo (podobne interese, mnenja, poglede itd.) in tako pri žrtvi vzbudi občutek domačnosti, kar jo pripravi do zaupanja napadalcu.
- Recipročnost – napadalec izkorišča nagnjenost ljudi do 'vračanja uslug'.
- Konsistentnost – ljudje v splošnem spoštujejo pravila in obveznosti; storilec tako prepriča žrtev v pravilnost dejanj.
- Družbena potrditev – ljudje se izogibamo dejanj, ki jih sočlani skupnosti ne sprejemajo – če so drugi že nekaj storili, nam je lažje enako ponoviti kot se upreti.
- Redkost – socialni inženir izkorišča našo naravno nagnjenost po tekmovanju.

Ravno zaradi navedenih človeških lastnosti je obramba proti metodam socialnega inženiringa izredno zahtevna. Posameznik se s pomočjo tehničnih kontrol, kot so požarni zidovi, antivirusni programi itd., lahko zavaruje le do določene mere. Sicer pa je koncept zaščite pred socialnim inženiringom enak kot pri zaščiti pred drugimi oblikami nevarnosti: ključna je določitev ranljivosti, groženj in iz njih izvedenih tveganj ter vpeljava ustreznih kontrol (@SANS Institute, 2003). Pri tem mora biti velik poudarek predvsem na nenehnem ozaveščanju in izobraževanju uporabnikov. Za učinkovito varovanje informacijskih sistemov namreč ni dovolj samo poznavanje tehničnih karakteristik, operacijskih sistemov in programske opreme, ampak moramo vedeti tudi, kaj ščitimo in katere kontrole moramo vpeljati (Potokar in Bernik, 2014).

3.2 Motivi socialnega inženiringa

Za napad s pomočjo socialnega inženiringa lahko napadalca motivira finančna korist, lasten interes, maščevanje, sovražnost, zunanji pritisk, terorizem, politično in vojaško vohunjenje, industrijsko in gospodarsko vohunjenje, intelektualni izziv in samodokazovanje. Dodatni motivator je tudi enostavnost napada zaradi neosveščenosti ljudi in relativno lahko igranje vlog pri zavajanju žrtve, pri čemer se napadalcu tudi ni potrebno posebej izpostaviti, saj lahko kot komunikacijsko sredstvo uporabi telefon, faks, internetne klepetalnice, elektronsko pošto in (trenutno najbolj popularna) socialna omrežja (Vučenović, 2010).

4 SOCIALNI INŽENIRING IN (ZLO)RABA INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE

Z razvojem informacijsko-komunikacijske tehnologije so se nedovoljena ravnanja preselila tudi v navidezni svet interneta. Poleg neomejene možnosti informiranja, izobraževanja in komuniciranja, ki jo s svojimi storitvami omogoča internet, v njegovem svetu obstajajo tudi manj prijetne in celo nevarne stvari. Poneverbe, zlorabe, otroška pornografija in sovražni govor, to je le nekaj izmed oblik kriminalnih dejanj, ki se izvršujejo tudi s pomočjo tehnik socialnega inženiringa, ki izkorišča različne informacijsko-komunikacijske tehnologije – na internetu elektronsko pošto, forume, klepetalnice in druga družabna omrežja, lahko pa tudi mobilne telefone in druge komunikacijske naprave. Ko govorimo o internetu (splet, medmrežje), razumemo pod tem pojmom globalno omrežje, ki ga sestavljajo različna računalniška omrežja. Internet je bil razvit v akademskem okolju, da bi z njim omogočili hitrejši pretok informacij. Glede na prvotne uporabnike je internet temeljil na načelu poznavanja in medsebojnega zaupanja. Ker je bila njegova uporaba sprva omejena in

nekomercialna (uporabljale so ga akademske in vladne organizacije), za njegovo uporabo pa je bilo potrebno kar precej tehničnega znanja, tudi ni bilo potrebe po posebnih pravilih obnašanja in zaščiti izmenjave informacij. Devetdeseta leta prejšnjega stoletja pa so prinesla preobrat: razvili so se spletni brskalniki, tj. uporabnikom prijazni programski vmesniki za delo na spletu, hkrati pa je bila odstranjena omejitev glede komercialne rabe interneta. Tako je internet postal nov medij za komuniciranje. Zavedati pa se moramo, da pri uporabi interneta z vsakim korakom za seboj puščamo (elektronske) sledi. Na spletu obstajajo različni programi, ki pregledujejo spletne strani in komunikacijske poti, lovijo informacije, s kom, kdaj, kje pa tudi o čem smo komunicirali, posebni programi, imenovani *e-mail extractorji*, omogočajo pridobivanje e-naslovov iz poljubnih virov in so le ena vrsta *spletnih žanjcev*, programov-pajkov, ki pregledujejo in zbirajo informacije s spletnih strani, forumov, družabnih omrežij itd. Vedeti moramo, da je odločitev, kaj in komu bomo zaupali v našem virtualnem življenju na spletu, popolnoma naša.

4.1 Informacijsko-komunikacijske tehnologije

V tem razdelku je predstavljenih nekaj najbolj uporabljanih komunikacijskih kanalov in tehnologij na spletu ter nevarnosti pri njihovi uporabi.

Elektronska pošta (*e-mail*) je še vedno eno izmed najpomembnejših sredstev komuniciranja v virtualnem svetu. Za omogočanje storitve e-pošte so 'odgovorni' tako imenovani poštni strežniki (npr. *Yahoo, Gmail, Hotmail*), ki posameznim uporabnikom nudijo uporabo e-poštnih nabiralnikov, do katerih lahko dostopajo s pomočjo spletnega brskalnika ali pa z uporabo poštnih odjemalcev – računalniške aplikacije, postavljene na uporabnikovem računalniku (*Microsoft Office Outlook, Microsoft Outlook Express*). Pot e-pisma zna biti precej zamotana, saj ta ponavadi od pošiljatelja do prejemnika potuje preko več različnih strežnikov; tako se lahko primeri, da do naslovnika pride 'obogatena' z računalniškim virusom, črvom ali kakšno drugo obliko zlonamerne kode. Posebno primerne za nečiste namene so priponke, saj se v njih prav lahko skriva zlonamerna koda.

Pod pojmom *socialna omrežja* razumemo skupnost ljudi in tehnologijo, ki tej skupnosti omogoča medsebojno komunikacijo. Komunikacija je omogočena s pomočjo računalniškega omrežja (spleta), načini izvedbe (aplikacija) pa so različne (forumi, spletne klepetalnice itd.). Širši pojem je *virtualna skupnost* (angl. *Virtual community*), *socialna skupnost*, *e-skupnost* ali skupnost *online*. Interakcija članov tovrstnih skupnosti poteka preko komunikacijskih medijev, kot so pisma, telefon, elektronska pošta itd. Namen druženja je lahko družabne, profesionalne ali izobraževalne narave.

Forum (tudi *web forum*) je spletno mesto za izmenjavo mnenj o določeni temi.

Spletne klepetalnice so storitev interneta, ki uporabnikom omogoča medsebojno komunikacijo na spletu. Klepetalnice so vabljive predvsem zato, ker omogočajo relativno anonimnost udeleženca in navidezno reševanje problema osamljenosti posameznikov, ki poskušajo frustracijo zmanjšati s komuniciranjem preko spleta. Značilnost vsebine pogovorov na spletnih klepetalnicah je, da so le kopije tistih iz realnega življenja: sogovornike predvsem zanima, kdo smo, kaj počnemo, kako 'v resnici' izgledamo, itd. Seveda nam anonimnost omogoča, da svobodneje izražamo svoja mnenja, saj nas ne omejuje strah pred (prevelikimi) sankcijami; po drugi strani pa tudi omogoča, da se anonimnež predstavi 'boljšega', kot je v resnici – in tu se skrivajo pasti nepremišljene uporabe te storitve.

Takojšnje sporočanje (tudi *instant messaging*) je tehnologija, ki uporabniku omogoča takojšnjo dostavo sporočila uporabniku (npr. *Windows Messenger, ICQ*).

Internet Relay Chat (IRC): nevarnost uporabe tovrstne tehnologije je v tem, da so ponavadi seje med odjemalcem in strežnikom nešifrirane (le malo strežnikov IRC uporablja protokol *Secure Socket Layer*), kar pomeni, da lahko prisluškovalni programi (imenovani *snifferji*) pridobijo uporabnikovo geslo. Obstaja tudi tako imenovan *IRC takeover* – zlonamerni prevzem seje (kanala).

Peer-to-Peer (P2P): med storitve, ki jih ponuja splet, lahko štejemo tudi uporabo brezplačnih programov (aplikacij) s skupnim imenom P2P, kot so: BitTorrent, µTorrent, Azureus, BitComet, BitTornado, BitLet, eMule, Shareaza, MLDonkey, Vuze, DNA, BitLord, BitDownload, TurboMule, BitSpirit, Kazaa itd. Tovrstni programi se najpogosteje uporabljajo za (neupravičeno) distribucijo različnih avtorskih del, največkrat filmov, glasbe in računalniških programov. Uporabniki programov P2P po eni strani na svoj računalnik prenašajo različne vrste datotek, po drugi strani pa drugim uporabnikom nudijo možnost prenosa podatkov s svojega računalnika. To pomeni, da lahko vsak računalnik v omrežju ponudi v skupno rabo del ali celotno pasovno širino internetne povezave, poleg tega lahko vsak računalnik omogoči še skupno rabo poljubnega imenika, lahko pa kar celotne razdelke (particije) na trdem disku. S stališča varnosti predstavljajo zmerno visoko tveganje že P2P-programi sami, saj so bile pri mnogih že večkrat odkrite varnostne pomanjkljivosti, ki jih napadalci zaradi povezanosti programov v internet zlahka zlorabijo. Večji problem predstavljajo nevešči uporabniki, ki pomotoma v skupno rabo v omrežju P2P dodelijo tudi imenike, v katerih hranijo svoje zasebne ali celo zaupne službene podatke, kjer jih lahko dobijo in zlorabijo nepridipravi. Največjo nevarnost pa predstavlja zlonamerna koda, ki je pogosto dodana legitimnim računalniškim programom ali datotekam, ki se med prenosom 'dobre' datoteke znajde na uporabnikovem računalniku. Od tu naprej nas do hekerskega vdora loči le korak. Po končanem prenosu podatkov oziroma po zagonu datoteke se namreč zlonamerna programska koda izvede in se namesti na računalnik, pri tem pa je npr. pridobila uporabniška imena in gesla, odprla stranska vrata in o svoji namestitvi poslala sporočilo hekerju, ki je bil njen lastnik. Znani so tudi primeri, ko je bilo ime priljubljenega filma ali programske opreme zlorabljeno tako, da je uporabnik na svoj računalnik namesto vsebine, ki je ustrezala naslovu, prenesel film z otroško pornografsko vsebino. V nekaterih primerih bi lahko tak uporabnik programa P2P zaradi tega tvegal celo kazenski pregon. Niso pa to edine grožnje varni uporabi informacijskega sistema. Pri prenosu velikih količin podatkov lahko pride do poslabšane pretočnosti omrežja oziroma do slabše zmogljivosti računalniškega procesorja. Računalnik lahko zato občasno postane zelo slabo odziven oziroma se sploh ne odziva, kar onemogoči izvajanje vseh storitev (angl. *Denial Of Service – DOS)*.

4.2 Tehnike zlorabe informacijsko-komunikacijske tehnologije

Proces socialnega inženiringa poteka v več korakih, mednje sodi zbiranje informacij, pri čemer storilec pridobi potrebne informacije za razvijanje odnosa z žrtvijo, ta pa predstavlja drugi korak življenjskega cikla socialnega inženiringa. V tej fazi storilec pri žrtvi vzpostavi ustrezno zaupanje za prehod v tretji korak, tj. pridobitev željenih informacij, potrebnih za četrti korak, slednji pa obsega doseganje postavljenih ciljev oziroma osnovnega namena socialnega inženiringa, to je vdor v informacijski sistem oziroma pridobitev željenih informacij. V celotnem življenjskem ciklu socialnega inženiringa uporabljajo storilci za dosego ciljev različne tehnike. Nekaj teh bomo predstavili v nadaljevanju.

4.2.1 Lažno predstavljanje - ribarjenje

Pri lažnem predstavljanju (*angl. phishing*) napadalci pošiljajo lažna e-poštna sporočila, ki na prvi pogled delujejo kot pristna. V njih pozivajo naslovnika, naj npr. obišče spletno mesto neke banke ali plačilne ustanove, spletna povezava do nje pa je vključena v sporočilo. Obiskovalec take (lažne) spletne strani nevede sam posreduje podatke, potrebne za uspešno zlorabo.

4.2.2 Zvabljanje

Zvabljanje (*angl. pharming*) je delno podobno lažnemu predstavljanju, le da je bolj zahrbtno, saj se napad običajno zgodi brez kakršnega koli vsaj približno sumljivega sporočila. Napadalci uporabnika računalnika preusmerijo na lažno spletno stran, ne da bi se ta tega zavedal, in od njega pridobijo ustrezne podatke.

4.2.3 Vishing

Vishing (*angl. voice phishing*) izkorišča internetno telefonijo oziroma VoIP (Voice over IP). Žrtve prejmejo telefonski klic, in ko se odzovejo, zahteva avtomatski odzivnik na drugi strani linije določeno akcijo, v okviru katere mora žrtev poklicati lažni klicni center, kjer operator zahteva npr. osebne podatke, podatke o kreditni kartici itd.

4.2.4 Smishing

Smishing (*angl. SMS phishing*) je podoben vishingu, le da žrtve namesto klica prejmejo lažno sporočilo, ki zahteva določeno akcijo, v okviru katere mora žrtev poklicati lažni klicni center, kjer operator zahteva npr. osebne podatke, podatke o kreditni kartici itd.

4.2.5 Škodljiva programska oprema

Napadalci lahko s pomočjo škodljive programske opreme (trojanski konji, orodja, ki snemajo pritiske na tipke računalniške tipkovnice, itd.) in brez uporabnikove vednosti pridobijo vse podatke, ki jih potrebujejo za nelegalne oddaljene nakupe.

4.2.6 Lažne spletne trgovine

S pomočjo lažnih spletnih trgovin, ki po sumljivo ugodnih cenah ponujajo različne vabljive izdelke, lahko napadalci dobijo vse podatke za izvedbo nelegalnih oddaljenih nakupov. Obiskovalec do lažnih spletnih trgovin ponavadi pride preko spletnih povezav, ki mu jih napadalec pošlje po lažni e-pošti.

4.2.7 Lažni prodajalci blaga po telefonu

Po telefonu žrtev pokliče lažnivi neznanec, ki naj bi opravljal neposredno prodajo prek telefona, v resnici pa skuša priti do podatkov, ki bi mu omogočili nelegalne oddaljene nakupe.

5 PRIMERI SOCIALNEGA INŽENIRINGA

Spletna klepetalnica. V prejšnjem poglavju smo predstavili uporabo socialnih omrežij, elektronske pošte, klepetalnic itd., ki jih za dosego svojih ciljev uporabljajo tudi socialni inženirji. Predstavljajmo si naslednji scenarij: včlanimo se v spletno klepetalnico, navežemo stike z različnimi uporabniki le-te in nekateri nam postanejo tako simpatični, da za njih sčasoma pričnemo uporabljati izraz prijatelji. In jim vedno bolj zaupamo. In smo z njimi odkriti. Pa res vemo, kdo je 'na drugi strani'? In nam nekega dne spletni 'prijatelj', tako kot že mnogokrat, pošlje zanimiv spletni naslov ali pa priponko. Seveda pogledamo, kaj zanimivega se skriva za tem 'pozivom' (človek je

med drugim tudi zvedavo bitje). Lahko da je res samo zanimiva informacija, lahko pa je tudi zlonamerna koda, ki se namesti na naš računalnik. Kaj je zlonamerna koda, pa tudi vemo.

Pomoč strokovnjakov. Enega izmed arhivov obiščeta dve osebi. Prva se predstavi za varnostnega inženirja, druga pa za svetovalca za področje informacijske tehnologije. Prišla sta, pravita, da preverita informacijsko varnost in splošno delovanje računalnikov, mreže in drugih tovrstnih naprav. Obenem bo pa njun kolega informatik, ki je v računalniškem centru, na računalnike naložil program, ki bo omogočal hitrejše delovanje le-teh. Nihče ne preveri istovetnosti oseb, dobita pa dostop do računalnika. In zaposleni ju pustijo sama (da ju ne bodo motili). In kolega 'iz centra' naloži program, skupaj ga tudi preverijo, vse se uspešno konča v slabih 15 minutah (to je sicer redek primer pri testiranju in prehodu v produkcijsko delovanje). Varnostni inženir in svetovalec se po končanem opravilu zahvalita zaposlenim za prijazen sprejem in zgledno sodelovanje. In odideta. Tokrat sta osebi res bili to, za kar sta se predstavljali. Mi si pa tudi predstavljamo, kaj bi v danem primeru naredila socialna inženirja. Arhivsko gradivo v elektronski obliki bi lahko bilo resno ogroženo, saj bi lahko ta varnostni inženir in svetovalec vdrla v informacijski sistem arhiva in spremenila ali celo izbrisala katero od arhivskih gradiv v elektronski obliki. Lahko bi tudi zlorabila kakšne osebne podatke in informacije iz gradiva, npr. v politične namene. Posledice bi bile velike in tudi vsa odgovornost bi žal najverjetneje padla na zaposlene ali na vodstvo zaradi slabih varnostnih politik.

Zloraba zaupanja. Virus, imenovan Love bug, je bil najbolj očiten napad, ki je izkoristil zaupanje ljudi. Pred tem virusom so uporabniki imeli navado odpirati vsa elektronska sporočila, ki so imela v vrstici pošiljatelja znano ime (prijatelj, sodelavec, itd.) ali so bila videti kot dobra šala (Verdonik in Bratuša, 2005, str. 119). Kot primer zlorabe zaupanja bi lahko v enem od arhivov zadolžili novozaposlenega za določen čas, npr. delavca, ki ga je eden od arhivov začasno zaposlil preko javnih del, za urejanje dokumentarnega in arhivskega gradiva podjetij v stečaju. Ta novozaposleni je tako pridobil pravico do dostopa do arhivskega skladišča in do podatkov podjetij, ki so zaključila svoje poslovanje s stečajem. Njegova naloga je izločitev dokumentarnega gradiva, ki mu je pretekel rok hrambe, in odbiranje arhivskega gradiva, ki mu je potrebno odstraniti kovinske sponke ter ga zložiti v papirne mapice, nato pa še v arhivske škatle vključno s popisom vsebine. Seveda zaposleni v arhivu ne morejo celoten delovni čas nadzorovati zaposlenega preko javnih del, pa saj so mu zaradi njegove prijaznosti, družabnosti in zmožnosti samostojnega izvajanja nalog tudi zaupali. Zaradi njegove samostojnosti in natančnega dela se mu je dodelila ureditev gradiva enega od zloglasnih gradbenih podjetij, ki je končalo svoje dolgoletno poslovanje v stečaju. V primeru, da bi omenjeni delavec bil socialni inženir, bi lahko brez težav odtujil del pomembnega arhivskega gradiva, ne da bi kdo kaj opazil in posumil. S takšnim dejanjem bi povzročil veliko škodo, ki se najverjetneje nekaj časa ne bi ugotovila. Odgovornost za škodo bi najverjetneje nosilo vodstvo arhiva ali celo kakšen od redno zaposlenih. V katerem od podjetij pa bi lahko kot najverjetnejši primer dali študenta, ki so mu predali velik rednik dokumentarnega gradiva, da ga skopira ali skenira. Če bi bil študent socialni inženir, bi lahko zlorabil podatke iz gradiva, naredil še sebi kakšno kopijo gradiva, lahko bi del gradiva tudi namerno uničil ali odtujil itd. V glavnem, možnosti je nešteto. Posledice takšnega iztoka pomembnih informacij podjetja bi lahko bile velike in bi lahko celo vplivale na konkurenčen položaj podjetja. Verjetno pa ne bi nobeden pomislil, da je lahko kriv prav študent. Prav zanimivo je, da v večini podjetij dajejo zaposleni študentom gradivo v papirni obliki za kopiranje, skeniranje ali prepisovanje kakšnih podatkov v elektronske evidence. Pa tudi za urejanje elektronskih podatkov, informacij in datotek. Verjetno pa skoraj nihče

ne pomisli na tveganje ob takšnem početju in možnosti zlorab oz. uničenja podatkov ali gradiva, saj so lahko študenti premalo skrbni ali pa imajo celo zlonamerne namene. V današnjem času je žal zelo hitro možno zlorabiti podatke in informacije, saj ima skoraj vsak posameznik mobitel, s katerim je mogoče v trenutku narediti sliko. Velika nevarnost pa so tudi USB-ključki, na katere je mogoče hitro prenesti večjo količino gradiva v elektronski obliki.

Povabilo v družabno omrežje Google+. V času uvajanja družabnega spletnega omrežja *Google+* je podjetje *Kaspersky Lab* opozarjalo, da so mnogi spletni uporabniki v svoje elektronske nabiralnike dobili vabilo, da se pridružijo družabnemu spletnemu omrežju Google+. Vendar pa taka sporočila niso vsebovala povezave na omenjeno omrežje, temveč povezavo do zlonamernih programov oz. - natančneje - do tako imenovanih bančnih trojancev. Tako je *Kaspersky Lab* zaznal tako sporočilo, ki cilja na portugalsko govoreče uporabnike. Lažno vabilo je vsebovalo povezavo, ki je vodila na domeno *google****.redirectme.net*. Ko je uporabnik vstopil na omenjeno domeno, je bil preusmerjen do zelo pogoste datoteke *.cmd* brazilskega bančnega trojanca, ki je gostoval na družabnem omrežju *Dropbox*. Druga povezava v sporočilu pa je vodila do aplikacije (programa) za vabila, ki je gostovala v Googlovih dokumentih. Sporočilo je vsebovalo povezavo '*pošlji vabilo svojim prijateljem*', v resnici pa je šlo za lažno aplikacijo, ki je zbirala imena in elektronske poštne naslove novih žrtev.

6 ZAKLJUČEK

Kot za večino pojmov obstaja tudi za pojem socialni inženiring več definicij. Lahko rečemo, da je socialni inženiring tehnika, s katero storilec pripravi žrtev, da stori ali opusti dejanja, ki jih običajno ne bi storila ali opustila. V prispevku smo predstavili pojav socialnega inženiringa kot ene izmed najbolj podcenjevanih, hkrati pa najnevarnejših metod zlorabe človekovega zaupanja. Odkrili smo tudi, kakšni mehanizmi botrujejo temu pojavu in zakaj smo ljudje glede njega tako ranljivi. Spoznali smo tudi metode socialnih inženirjev in si pogledali, kako socialni inženiring s pridom izkorišča razširjenost socialnih omrežij. Na koncu prispevka smo predstavili tudi nekaj praktičnih primerov, med njimi take, ki kažejo, na kakšen način bi lahko socialni inženirji škodljivo vplivali na dokumentarno ali arhivsko gradivo v elektronski in v papirni obliki ali ga celo resno ogrozili. Za napad s pomočjo socialnega inženiringa lahko napadalca motivira finančna korist, lasten interes, maščevanje, sovražnost, zunanji pritisk, terorizem, politično in vojaško vohunjenje, industrijsko in gospodarsko vohunjenje, intelektualni izziv in samodokazovanje.

Z našim raziskovanjem smo želeli pridobiti odgovor na vprašanje, ali je človek v primeru napadov socialnih inženirjev med najšibkejšimi členi varnostnega sistema (slednji je sestavljen iz pravil, postopkov oziroma procesov, tehnologije in človeka (ljudi)). Za odgovor na to raziskovalno vprašanje smo proučili teoretična izhodišča, ki kažejo, da je človek res med šibkejšimi členi varnostnega sistema. Človek namreč sodeluje v prav vseh delih varnostnega sistema, saj postavlja pravila, jih izvaja v procesih ter tudi vpliva na uporabo same tehnologije. Teoretična izhodišča smo povezali tudi z izkušnjami iz prakse, kjer smo srečali ogromno primerov, ko je bil človek najšibkejši člen različnih tehnik napadov socialnih inženirjev zaradi svoje nravi. Izkazalo se je, da je večina ljudi zaupljive narave. Dobri socialni inženirji znajo ugajati ljudem, da jim ti zaupajo. Za dosego svojih ciljev izkoriščajo različna čustvena in psihična stanja žrtev. Metode socialnega inženiringa lahko delimo v dve večji skupini: metode, ki za izvedbo uporabljajo informacijsko tehnologijo (npr. pojavitev lažnega računalniškega okna), in metode, temelječe na človeški interakciji, ki temeljijo na

človekovih medsebojnih odnosih in preslepitvi (npr. igranje vloge nebogljenega novozaposlenega). Z razvojem informacijsko-komunikacijske tehnologije so se nedovoljena ravnanja preselila tudi v navidezni svet interneta. Poneverbe, zlorabe, otroška pornografija in sovražni govor, to je le nekaj oblik kriminalnih dejanj, ki se izvršujejo tudi s pomočjo tehnik socialnega inženiringa, ki izkorišča različne informacijsko-komunikacijske tehnologije – na internetu elektronsko pošto, forume, klepetalnice in druga družabna omrežja, lahko pa tudi mobilne telefone in druge komunikacijske naprave. Najbolj pogoste tehnike zlorab informacijsko-komunikacijske tehnologije, ki jih za dosego svojih ciljev uporabljajo socialni inženirji, so lažno predstavljanje oziroma ribarjenje s pomočjo e-pošte, zvabljanje na lažno spletno stran, napadi s pomočjo internetne telefonije (vishing), napad s pomočjo SMS-sporočil (smishing), napadi s škodljivo programsko opremo, napadi s pomočjo lažne spletne trgovine in napadi s pomočjo lažne prodaje preko telefona. Na podlagi našega raziskovanja lahko zaključimo, da je za napade socialnih inženirjev najšibkejši člen prav človek, saj se tudi napadi na tehnologijo in komunikacijske kanale vršijo preko njega ali z njegovo nezavedno pomočjo.

VIRI IN LITERATURA

- Bernik, I. in Prislan, K. (2012): *Kibernetska kriminaliteta, informacijsko bojevanje in kibernetski terorizem*. Ljubljana: Fakulteta za varnostne vede.
- BSI (2005a). *Informacijska tehnologija - Varnostne tehnike - Sistemi za upravljanje varovanja informacij - Zahteve (BS ISO/IEC 27001:2005 BS 7799-2:2005*). Velika Britanija: BSI.
- BSI (2005b). *Informacijska tehnologija - Varnostne tehnike - Kodeks za upravljanje varovanja informacij (BS ISO/IEC 27002:2005)*. Velika Britanija: BSI.
- Informacijski pooblaščenec. (2009): *Socialni inženiring in kako se pred njim ubraniti?* Pridobljeno 21. 12. 2014 s spletne strani: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/socialni-inzeniring-in-kako-se-pred-njim-ubraniti.pdf.
- Mitnick, K. (2002). *The art of deception. Controling the human element of society*. Indianapolis: Wiley Publishing.
- Peltier, Thomas R. (2002): *Information Security, Policies, Procedures and Standards: Guidelines for Effective Information Security Management*. CRC Press LLC.
- Potokar, M. in Bernik, I. (2014): *Vzpostavitev Sistema upravljanja varovanja informacij za project e-arhiviranja v skladu z ZVDAGA in ZVOP-1*. V N. Gostenčnik (ur.), *Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja [Elektronski vir] : Arhivi v globalni informacijski družbi : zbornik mednarodne konference, Radenci, 2. - 4. april 2014,* URL: http://www.pokarh-mb.si/uploaded/datoteke/radenci2014/03_potokar_2014.pdf. Maribor: Pokrajinski arhiv Maribor.
- Verdonik, I. in Bratuša, T. (2005): *Hekerski vdori in zaščita*. Ljubljana: Pasadena.
- Vučenović, M. (2010): *Nevarnosti socialnega inženiringa za organizacije* (diplomsko delo). Kranj: Univerza v Mariboru, Fakulteta za organizacijske vede.
- @SANS Institute (2001): *A Proactive Defence to Social Engineering*. Pridobljeno 19. 12. 2014 s spletne strani: http://www.sans.org/reading-room/whitepapers/engineering/proactive-defence-social-engineering-511.
- @SANS Institute (2003): *A Proactive Defence to Social Engineering*. Pridobljeno 19. 12. 2014 s spletne strani: http://www.sans.org/reading-room/whitepapers/engineering/multi-level-defense-social-engineering-920?show=multi-level-defense-social-engineering-920&cat=engineering.

SUMMARY

Marko POTOKAR[*]*, Sanja ANDROIĆ*[**]

SOCIAL ENGINEERING – A MAN AS PART OF THE SECURITY SYSTEM

As for most concepts, there are also several definitions of the social engineering concept. It is a jargon term, which stands for encouraging involuntary active cooperation by persuading target persons (victims) to deliver certain information. This term is used for system invasion techniques, based on taking advantage of the features (weaknesses) of human nature. We can say that social engineering is a technique used by the perpetrator to make the victims do or give up actions they would normally not do or give up.

The methods of social engineering are nothing new. They were developed by the army, intelligence services, security agencies and industrial espionage experts. The article shows the phenomenon of social engineering as one of the most underrated and at the same time the most dangerous methods of abuse of human confidence. The authors also discovered what mechanisms are responsible for this phenomenon and why people are so vulnerable to it. They were acquainted with the methods of social engineers and saw how social engineering uses the widespread phenomenon of social networks to its advantage.

At the end of the article some practical examples are presented, including one that shows how social engineers could harmfully influence records or archives in electronic and in paper form, or even seriously endanger it. For a social engineering attack , the attacker can be motivated by financial benefit, personal interest, revenge, hostility, external pressure, terrorism, political and military espionage, industrial and economic espionage, intellectual challenge and self-affirmation.

The aim of this research was to answer the following question: Is man the weakest link of the security system in case of an attack by social engineers? To answer this research question, the authors studied the theoretical basis showing that man is among the weaker links of the security system, which consists of rules, procedures or processes, technology and man (people). Man is involved in all parts of the security system, since he makes the rules, follows them in the processes and also influences the use of technology. The theoretical basis was linked with practical experience, where the authors encountered a lot of cases where man – confronted by various attack techniques of social engineers – was the weakest link due to his nature. It was found that most people are trustful by nature. Thus, good social engineers please people to gain their trust. In order to reach their goals, they exploit various emotional and mental conditions of their victims. The methods of social engineering can be divided into two large groups: methods based on information technology (e.g. emergence of a fake computer window) and methods based on human relations and fraud (e.g. playing the role of a helpless new employee). With the development of information and communication technology, illicit activities moved to the virtual world of the Internet. Embezzlement, abuse, child pornography, and hate speech are only some forms of

[*] *Marko Potokar, M. Phil., Institute for Safety Culture, Tržaška cesta 132, 1000 Ljubljana, Slovenia, contact: marko.potokar@institut-ivk.si.*

[**] *Sanja Androić, head of reception office, Mariborski vodovod, javno podjetje, d. d., Jadranska cesta 24, SI-2000 Maribor, Slovenia, contact: sanja.androic@mb-vodovod.si.*

criminal acts also performed by means of social engineering techniques, using different information and communication technologies: on the Internet electronic mail, forums, chat rooms and other social networks, but also mobile phones and other communication devices. The most common techniques of information and communication technology abuse that social engineers use to reach their goals, are false identification – phishing by means of e-mail, luring to a fake website, attack by means of internet telephony (vishing), attack by means of text messages (smishing), attacks with harmful software, attacks by means of fake online shops and attacks by means of fake telephone sales. Based on the research, we can conclude that for social engineers' attacks, man is the weakest link, since attacks on technology and communication channels are performed through him or with his involuntary assistance.