Socialni inženiring v spletnih socialnih omrežij

Uroš Gregorič, študent magistrskega študija, Fakulteta za varnostne vede, Univerza v Mariboru

Namen prispevka
Predstavljen bo socialni inženiring kot orodje in tehnika za pridobivanje podatkov in informacij v spletnih socialnih omrežjih. Do njih storilec (socialni inženir) ni upravičen. Predstavljene so vrste socialnega inženiringa ter dejavniki in motivi, ki omogočajo napade. Predstavljene so glavne značilnosti spletnih socialnih omrežij in socialno-psihološke značilnosti uporabnikov, ki skupaj predstavljajo vzrok, zakaj so spletna socialna omrežja tako plodno gojišče za prevare s pomočjo socialnega inženiringa. Za konec pa predstavljamo nekaj nasvetov za preventivno vedenje v spletnih socialnih omrežjih.

Metodologija
Prispevek je metodološko izveden kot deskripcija poznanih dejstev. Opravljen je pregled virov in dostopne literature s področja informacijske varnosti in psihologije. Opravljena je analiza izbranih virov in priprava pregleda bistvenih spoznanj o izvajanju socialnega inženiringa.

Ugotovitve
Socialni inženiring izkorišča dejstvo, da je človek zaradi sociooloških in psiholoških značilnosti najšibkejši člen v verigi varovanja podatkov. Za varovanje podatkov in informacij si lahko pomagamo s programsko in strojno opremo, vse premalo pa se zavedamo nevarnosti, ki jo predstavlja socialni inženiring, ki s prepričljivim manipuliranjem in prevarami napadalcu omogoča pridobitev podatkov in informacij. Novo, lahko rečemo kar neskončno polje delovanja socialnih inženirjev je zagotovo internet, še posebej spletna socialna omrežja, saj le-ta na novo definirajo pojma prijateljstvo in zaupanje ter privabljajo vse večje število uporabnikov. Kot obrambo proti napadom s pomočjo socialnega inženiringa, lahko izpostavimo le izobraževanje uporabnikov, tako zasebno kot v podjetjih.

Praktična uporabnost
Prispevek je splošen in namenjen vsem, ki so uporabniki spletnih socialnih omrežij, še posebej, če morajo pri tem upoštevati področje varovanja informacij. Seznanjanje čim širšega kroga ljudi s socialnim inženiringom in opozarjanje na nevarnosti tega pojava lahko pripomore k splošnemu dvigu nivoja zavedanja o pomembnosti varovanja podatkov in nevarnostih, ki jih pri tem predstavlja socialni inženiring.

Ključne besede: socialni inženiring, informacijska varnost, varnostna kultura, psihološki sprožilci, spletna socialna omrežja, izobraževanje

1 Uvod

Živimo v dobi informacij, obdani smo z informacijami in ekspanzija, ki jo je prinesla informacijska doba, žal ni prinesla tudi vzporednega zavedanja o občutljivosti in pomembnosti podatkov oz. informacij. Da podjetja zaščitijo svoje podatke, vlagajo velike vsote denarja v strojno in programsko opremo, le malokatero podjetje pa namenja enako, ali vsaj podobno vsoto sredstev izobraževanju in urjenju svojih zaposlenih ter nadalje tudi ustvarjanju klime in pogojev za visok nivo varnostne kulture, ki je temelj informacijske varnosti. Na področju tehnologije so nam v delno pomoč strojna in programska oprema, vse premalo pa se opozarja na nevarnost, ki jo predstavlja socialni inženiring, ki s prepričljivim manipuliranjem in prevarami napadalcu omogoča pridobitev podatkov in informacij, do katerih ni upravičen.

O socialnem inženiringu je bilo napisanega že kar nekaj in zdi se, da je skoraj težko napisati kaj povsem novega v zvezi z dejavniki in metodami. Vendar pa je v zadnjem času socialni inženiring znova pokazal, da je sposoben prilagajati se vsem oblikam tehnološkega napredka. Kljub napredku na področju zaščite posameznikov proti izkoriščanju oz. zlorabam, ostaja socialni inženiring eden od najbolj učinkovitih načinov za izvrševanje prevar in kraje podatkov. Vsakdo, ki se na kakršenkoli način ukvarja z informacijsko varnostjo, nikoli ne sme zmanjševati pomena nevarnosti, ki jo predstavljajo napadi s pomočjo socialnega inženiringa, saj ta stara in preprosta tehnika vedno znova preseneča z neverjetnimi rezultati. Novo polje za delovanje socialnega inženiringa predstavljajo spletna socialna omrežja, ki nezadržno rastejo in pridobivajo nove in nove člane, ki imajo najrazličnejše demografske značilnosti.
Če hočemo ljudi posvariti pred nevarnostmi, ki jih predstavljajo napadi s pomočjo socialnega inženiringa, moramo dobro poznati značilnosti spletnih socialnih omrežij. Analizirati je potrebno psihološke in sociološke značilnosti uporabnikov socialnih omrežij in njihovo vedenje, saj je znano, da prav t.i. psihološki sprožilci in ostale socialno-psihološke značilnosti omogočajo pridobivanje zaupanja kot enega od glavnih dejavnikov izkoriščanja nič hudega slutečih žrtev. Prav tako pa je potrebno nenehno spremljanje pojavnih oblik oz. načinov (*modus operandi*) izvajanja napadov s pomočjo socialnega inženiringa v spletnih socialnih omrežjih ter o tem v največji možni meri ozaveščati uporabnike.

2 Socialni inženiring

Na svetovnem spletu in tudi v drugih pisnih virih obstaja vrsta definicij, kaj je socialni inženiring. Definicije so se skozi čas spreminjale, saj socialni inženiring ni izum sodobnega časa, ampak se je v najrazličnejših formah pojavljal skozi vso človeško zgodovino. Za lažje razumevanje poglejmo nekaj definicij, ki se pojavljajo na spletu in v pisni literaturi:

- Socialni inženiring je upravljanje ljudi v skladu z njihovim položajem in funkcijo v družbi (Meriam Webster Online Dictionary, 2009).
- Socialni inženir uporablja prevaro, da bi vplival na osebo na drugi strani vrat, da bi jih ta zanj odprla. Socialni inženir uporablja vpliv in prepričevanje, da bi prevaral ljudi s tem, da se jih prepriča, da je socialni inženir nekdo, ki to ni, ali z manipulacijo. Rezultat tega je, da je socialni inženir zmožen izkoristiti ljudi, za pridobitev informacij, z ali brez uporabe tehnologije (Mitnick, 2002).
- Socialni inženiring je tehnika, s katero z uporabo poznavanja psihologije ljudi, poznavanja delovanja računalniških sistemov in terminologije ter z uporabo majhnih in »verjetnih laži« pripravimo ciljne osebe, da storijo ali opustijo stvari, katere običajno ne bi storili ali opustili za tujce ali nepoznane osebe (Radulj, 2003).

Katerokoli definicijo vzamemo, strokovno ali laično, lahko kot skupni imenovalec izpostavimo, da gre za metodo, ki ji poenostavljeno lahko rečemo manipulacija. Čeprav se socialni inženiring tesno povezuje z napadi na informacijske sisteme, je treba poudariti, da je cilj napada s pomočjo socialnega inženiringa pridobitev podatka ali informacije, ki je lahko v najrazličnejših oblikah (ne nujno v digitalni obliki), kot npr.: pisano besedilo, ustni podatek, slikovni material itd. »Odlika« socialnega inženiringa je, da se pojavlja v nešteto oblikah in da vedno uporablja vse dosežke človeške družbe, spoznanja o človekovih psiholoških in sociološkihznačilnostih, prav tako pa znajo socialni inženirji spretno izkoristiti dosežke, ki jih je prinesla informacijska tehnologija, še posebej razvoj oz. dostopnost osebnih računalnikov in interneta. Napade s pomočjo socialnega inženiringa danes prav zaradi uporabe tehnoloških dosežkov lahko razdelimo na dve kategoriji:

- napadi s pomočjo računalniške tehnologije (t.i. *computer based* napadi)
  Za način, ki temelji na računalniški tehnologiji, je značilno, da komunikacija med napadalcem in napadenim poteka s pomočjo računalniške opreme in interneta. Tudi napadi s pomočjo računalniške tehnologije se neprestano spreminjajo, pojavljajo se vedno nove oblike, nekaj najbolj znanih pa je: ribarjenje (*phishing*), zvabljanje (*pharming*), pojavna okna (*pop-up windows*), trojanski konji (*Trojan horses*). Za te napade bi lahko rekli, da ne gre za »klasične« hekerske napade, temveč za t.i. hibridne

napade, saj se storilci poslužujejo tako klasičnega socialnega inženiringa kot uporabe tradicionalnih hekerskih metod.

- napadi, ki temeljijo na človeški interakciji (t.i. *human based* napadi)
  Napadi, ki temeljijo na človeški interakciji (t.i. *human based* napadi) izkoriščajo temeljni kulturni ustroj družbe in osnovne vedenjske značilnosti človeka – vse to z namenom doseganja določenega cilja, ki si ga je zadal napadalec. Za to vrsto socialnega inženiringa oz. ljudi, ki se ukvarjajo s socialnim inženiringom je značilno, da so izvrstni poznavalci psihologije, človeške interakcije, so odlični igralci vlog, retoriki, se spretno znajdejo v nepredvidenih situacijah, so vztrajni, predvsem pa znajo pridobiti zaupanje svoje žrtve. Vse te značilnosti so najboljši med njimi izpilili do perfekcije.

V začetku pojavljanja računalniške tehnologije je veliko ljudi, ki jih danes imenujemo hekerji, pridobivalo informacije do katerih niso bili upravičeni prav s pristopom, ki je temeljil na človeški interakciji. Šele z dostopnostjo interneta in osebnih računalnikov so v svoje delovanje vključili tudi poznavanje informacijske tehnologije in postali t.i. *socialni inženirji iz fotelja*. V primerih poskusa napada s pomočjo *computer based* socialnega inženiringa so nam v pomoč obrambni sistemi, ki temeljijo na programski in strojni opremi, kot so npr. anti-virusni programi, ki vključujejo npr. *anti-phishing* in *anti-pharming* tehnologije, *anti-spyware* programe, *anti-spam* programe ter požarne zidove. Menim, da so napadi, ki temeljijo na človeški interakciji bolj prikriti in jih je še težje zaznati. Gre za napade, ki temeljijo na poznavanju človeškega vedenja in psihologije in edini požarni zid, ki brani podjetje ali posameznika pred takimi napadi je človek sam.

2.1 Motivi za socialni inženiring

Ker je za vsako človeško delovanje potreben določen motiv oz. težnja, si v naslednjem odstavku na kratko poglejmo glavne dejavnike, ki za svoje delovanje motivirajo socialnega inženirja.
Napadalci, ki napadejo podjetje, lahko prihajajo tako iz samega podjetja, se pravi, da gre za napad od znotraj. Druga možnost pa je, da gre za napad od zunaj, npr. iz konkurenčnega podjetja. Ne glede na to, s katere strani prihaja nevarnost, pa so najpogostejši naslednji motivi: finančni motivi, maščevanje (npr. odpuščeni delavci ali delavce, ki so bili žrtve *mobbinga*), zunanji pritisk (izsiljevanje, ustrahovanje), politični motivi (tudi oblike terorizma), kriminalni motivi, industrijsko vohunjenje, samodokazovanje (predvsem med mladimi hekerji).

2.2 Cikel socialnega inženiringa

Za napade, ki temeljijo na človeški interakciji, je še posebej značilno, da potekajo po določenem vrstnem redu oz. po določenih fazah. Te faze so:

- zbiranje osnovnih informacij:
  Zbiranje informacij poteka na različne načine in prav za to fazo socialnega inženiringa je značilno, da jo lahko razdelimo na zbiranje informacij s pomočjo tehnologije, npr. spletne strani podjetij, spletni iskalniki (Google, Yahoo...) in v zadnjem času predvsem spletna socialna omrežja. Načini brez uporabe tehnologije pa so npr.: opazovanje, gledanje čez ramo (*shoulder surfing*), igranje vlog, brskanje po smeteh (*dumpster diving*) itd.
- navezovanje kontakta s ciljno osebo:
  V tej fazi napadalec izkoristi vse pridobljene podatke, da naveže stik s ciljno osebo ter istočasno pridobi tudi določeno raven zaupanja, kar izkoristi v naslednji fazi, ki je:
- izkoriščanje žrtve:
  V tej fazi napadalec vnovči dosedanji trud in manipulira z žrtvijo tako, da mu le-ta, ne da bi se tega zavedala, izda določene podatke.
- izvedba samega napada:
  Pri tej fazi socialni inženir pridobljeno informacijo izkoristi in doseže svoj cilj, npr. vstopi v podatkovno bazo s pomočjo gesla, ki ga je pridobil v predhodni fazi.

Za manj prefinjene socialne inženirje se na tej stopnji sam napad konča, za najboljše in najbolj izurjene pa sledi še ena, zelo pomembna faza, in sicer:

- brisanje sledi:
  V tej fazi socialni inženir zabriše sledi, ki bi napadenemu dale vedeti, da so bile zmanipulirane ter si na ta način pridobi določen čas. Za najboljše socialne inženirje pa je značilno, da celoten napad izpeljejo tako, da napadeni nikoli ne ugotovi, kdaj, na kakšen način in komu je posredovala informacijo, ki ga je pripeljala do želenega cilja (Gregorič, 2008).

2.3 Psihološki sprožilci – temelj napadov s pomočjo socialnega inženiringa

Kot smo že dejali, je za napade s pomočjo socialnega inženiringa značilno, da napadalci izkoriščajo poznavanje psihologije, zato v nadaljevanju poglejmo, katere so tiste psihološke značilnosti, ki omogočajo napade. V literaturi se najpogosteje uporablja klasifikacija psiholoških sprožilcev, ki jih je definiral in s socialnim inženiringom povezal Robert B. Cialdini (Fripp, 2009; Timko, 2008):

- recipročnost: Za recipročnost je najbolj značilno, da skuša napadalec z majhnimi uslugami ali darili pri žrtvi vzbuditi občutek, da mora nekaj poplačati oz. storiti v zameno za uslugo ali prejeto darilo.
- obveza in doslednost: Ljudje se zavedajo, da družba kredibilneje dojema osebe, ki so dosledne in izpolnjujejo svoje obveze.
- konformnost: Gre za človeško značilnost, da prilagaja lastno vedenje in delovanje tako, da je le-to v skladu z družbenimi ali skupinskimi normami ali pričakovanji.
- ugajanje: Ena od človeških značilnosti je, da lažje zaupamo osebam, ki so nam simpatične ali nam kako drugače ugajajo. Ugajanje lahko razdelimo na fizično privlačnost in podobnost v prepričanju in izkušnjah.
- avtoriteta: Gre za preprosto tehniko prepričevanja, ki izkorišča človeško nagnjenost k temu, da upoštevamo tiste ljudi, ki nam predstavljajo avtoriteto.
- pomanjkanje oz. razpoložljivost: Gre za človeško značilnost, kjer pomanjkanje, časovno ali količinsko, v človeku povzroči pritisk, katerega posledica je, da so dejanja posameznika drugačna kot v primerih, kjer ni občutka omejitve razpoložljivosti.

Poleg zgoraj omenjenih psiholoških sprožilcev, omenjam še nekaj značilnosti človekove narave, ki spretnemu socialnemu inženirju olajšajo delo. Človeška radovednost zagotovo sodi v vrh teh značilnosti. Poleg radovednosti socialni inženirji spretno izrabljajo še naslednje človeške značilnosti: naravna tendenca človeka, da pomaga oz. občutek moralne dolžnosti, razpršitev odgovornosti, preobremenitev, brezbrižnost.
Posebna oblika socialnega inženiringa je t.i. *obratni socialni inženiring*, pri katerem napadalec namerno povzroči napako oz. ustvari situacijo, v kateri je napadena oseba primorana poiskati pomoč. Napadalec prepriča napadeno osebo, da je le on tisti, ki lahko pomaga, nakar spretno izrabi situacijo in preko ponujene pomoči pridobi podatek do katerega ni upravičen.

2.4 Posledice napadov s pomočjo socialnega inženiringa

Posledice napadov z uporabo socialnega inženiringa so različne in lahko prizadenejo tako posameznika kot podjetje, kažejo pa se lahko kot:

- nedelovanje računalniške opreme
  Nedelovanje računalnikov se lahko odraža v izgubi časa in denarja. Za ponovno vzpostavitev normalnega stanja je potrebno zagotoviti določene človeške vire, da rešijo nastali problem. Izguba časa je pravzaprav dvojna, saj medtem ko zaposleni, ki se v podjetju ukvarjajo z informatiko, rešujejo problem, sami uporabniki ta čas ne morejo uporabljati računalniške opreme, kar se odraža v zmanjšani produktivnosti.

- izguba občutljivih informacij zaupne narave
  Pri teh informacijah ne mislimo le na izgubo osebnih podatkov, temveč gre predvsem za poslovne podatke (razvojni načrt, raziskovalno delo podjetja ipd.), ki so običajno plod dolgoletnega dela in na njih lahko temelji uspeh podjetja. Prav tako so ogrožene tudi državne institucije, ki pri svojem delu uporabljajo veliko količino osebnih podatkov državljanov ter podatkov s področja varnosti same države. Znano je namreč, da se razne teroristične organizacije in kriminalne skupine v veliki meri poslužujejo sodobne informacijske tehnologije in socialnega inženiringa, z namenom, da bi se dokopali do določenih podatkov.
- kraja identitete se nanaša na prevzem osebnih ali finančnih informacij druge osebe z namenom zlorabe finančnih transakcij in nakupov. Poznamo dve osnovni vrsti kraje identitete, in sicer:
  - kraja imena
    Gre za to, da prevarant ukradene osebne podatke uporabi za odprtje novega bančnega računa, z namenom najema posojil, ki jih ne namerava vračati, ali da koristi različne usluge na žrtvin račun, npr. telefonski pogovori.
  - prevzem bančonega računa napadenega
    Prevarant uporabi osebne podatke žrtve, da pridobi dostop njenega bančnega računa. Pogosto se zgodi, da prevarant spremeni naslov žrtve, ki je s tem bančnim računom povezana ter nato s koriščenjem sredstev oškoduje žrtev.
- kraja osebnih podatkov
  Urad informacijske pooblaščenke definira, glede na ZVOP, osebni podatek kot »katerikoli podatek, ki se nanaša na določeno ali določljivo fizično osebo, torej posameznika, na glede na obliko, v kateri je izražen« (IP RS, 2007).
- motenje zasebnosti in kraja datotek iz osebnih računalnikov:
  Velikokrat ima žrtev, ko se zave, da je napadalec vdrl v osebni računalnik, preko interneta ali direktno (npr. z ukradenim geslom), podoben občutek, kot da bi mu nekdo vlomil v stanovanje.
- finančne posledice:
  Tarče napada so lahko finančne ustanove in njihove stranke. Vsaka oseba ali podjetje, ki ima internetno povezavo, ne glede na področje svojega dela, je lahko tarča napada. Finančne ustanove lahko zagotovijo določeno stopnjo varnosti na svoji strani, nimajo pa nadzora nad računalniki svojih strank.
- izguba ugleda:
  Gledano dolgoročno je za marsikatero podjetje ali finančno ustanovo morda bolj kot finančna izguba škodljivo to, da je izgubilo ugled in da so ljudje izgubili zaupanje v poslovanje s takim podjetjem (Gregorič, 2008).

3 Spletna socialna omrežja

V človekovi naravi je prisotna tendenca po druženju, po medsebojni komunikaciji, po pripadnosti, po sklepanju novih prijateljstev. Z razvojem in razširitvijo interneta se ta del človekovega družbenega življenja vse bolj prenaša na svetovni splet. Govorimo o t.i. kibernetskem prostoru, ki je dodobra spremenil način medsebojne komunikacije. Ob pomanjkanju časa za druženje v tradicionalnem smislu, je internet enostavna, a površna alternativa, ko razdalja, čas in prostor niso ovira. Nove prijatelje iščemo kar iz naslanjača, komunikacija je brezosebna in poteka na daljavo. Spletna socialna omrežja so na novo definirala način medsebojnega sporazumevanja, drugačno je pojmovanje in dojemanje prijateljstva, prav tako tudi dojemanje zasebnosti, s tem pa se spreminjajo tudi družbeni odnosi.
Boyd in Ellison definirata spletna socialna omrežja kot: »*internetne storitve, ki omogočajo posameznikom: 1- da oblikujejo javni ali pol-javni profil znotraj zaokroženega sistema, 2- da oblikujejo seznam drugih uporabnikov, s katerimi se povezujejo, 3- vpogled na svoj seznam uporabnikov in pregledovanje seznamov drugih uporabnikov*« (Boyd in Ellison, 2007).
Zakaj se posameznik vključuje v spletna socialna omrežja? Menim, da predvsem zato, ker dajejo možnost

tako tistim, ki imajo željo po razkrivanju samega sebe in tudi tistim, ki želijo ostati anonimni, kar pomeni, da so zakriti in se predstavljajo za nekaj drugega, kar v resnici so, kljub temu pa lahko aktivno sodelujejo v kibernetski interakciji. Spletna socialna omrežja omogočajo posameznikom, da vzdržujejo stike s prijatelji in srečujejo tujce. Na ta način se oblikujejo povezave, ki se sicer ne bi, hkrati pa uporabnikom omogočajo, da svoje prijateljske povezave (seznam prijateljev) naredijo vidne drugim.

Klasično oz. tradicionalno prijateljstvo je odnos, ki vključuje delitev skupnih interesov, obojestranskost, zaupanje, razkrivanje intimnejših podrobnosti skozi čas in v specifičnih socialno-kulturnih kontekstih. Tako prijateljstvo se oblikuje, krepi in vzdržuje v okviru zasebnosti, torej stran od ostalega sveta. Prav nasprotno pa je pojem prijateljstvo v spletnih socialnih omrežjih javno, spremenljivo oz. gibljivo, pomešano. V virtualnem svetu gre za zbiranje, upravljanje ter rangiranje ljudi in to počnemo javno (Rosen, 2007). Če pogledamo z očmi uporabnika spleta, ki ni pristaš socialnih omrežij, bi lahko rekli, da se ves smisel teh omrežij vrti okrog nabiranja čim večjega števila »prijateljev«. Gre za tekmovanje, kdo bo zbral daljši seznam prijateljev. Princip zbiranja prijateljev je: *prijateljev prijatelj je avtomatično moj najboljši prijatelj*. Vse o prijateljih mojih prijateljev lahko izvemo preko interneta, ne da bi te ljudi v resnici kdaj srečali. »*Življenje brez stotine on-line prijateljev je virtualna smrt*« (Rosen, 2007: 26).

V realnem življenju ni pogosto, da bi spoznali veliko število prijateljevih prijateljev in z njimi ohranjali stike na enakem nivoju oz. zgradili enak nivo zaupanja kot s prvotnimi prijatelji. Za spletna socialna omrežja lahko rečemo, da pride posameznik v situacijo, ko se znajde obdan z neobvladljivo množico in prav vsak v tej množici je njegov prijatelj. Ne morem si predstavljati, kako ima lahko posameznik 280 prijateljev, z njimi vzdržuje kvalitetne stike in z njimi deli podrobnosti o svojem vsakdanjem življenju. V resnici se kvalitetno prijateljstvo nadomešča s kvantiteto, kar pomeni razvrednotenje pojma prijateljstva, s tem pa tudi pojma zaupanja, ki je s prijateljstvom tesno povezano. Iz tega sledi, da je tudi zaupanje z razmahom socialnih omrežij dobilo drugačno pojmovanje. SSKJ (2005) definira zaupanje kot: »*prepričanje, da je kdo sposoben, voljen narediti, kar se pričakuje; prepričanje, da je kdo pošten, iskren; prepričanje, da je kaj dobro in da bo dobro vplivalo na uresničitev določenih pričakovanj*«.

Praktično je nemogoče, da bi po tej definiciji človek lahko zaupal vsem spletnim prijateljem v enaki meri kot prijateljem v realnem svetu, pa čeprav se v interakciji preko spletnih socialnih omrežij največkrat tako obnašamo. Edina logična posledica je, da pri sodelovanju v spletnih socialnih omrežjih prekomerno znižamo nivo samovarovanja, in sicer se zniža raven pozornosti, hkrati s tem pa neupravičeno narašča nivo zaupanja. Posameznik na podlagi dolgega seznama »prijateljev« dobi občutek, da je obkrožen s pravimi prijatelji, torej ljudmi, ki jim lahko zaupa.

Le zato, da bomo imeli enega prijatelja več, pa čeprav je to v resnici popoln neznanec, ga želimo uvrstiti na svoj seznam prijateljev. Zastrašujoče je, da t.i. »prijatelju v tretjem kolenu« razkrivamo enake podatke kot resničnemu prijatelju. Še več: celotni množici ljudi posredujemo svoje podatke o zaposlitvi in sodelavcih, zdravstvenem stanju, intimi, sorodnikih itd. Nagnjenje, da v spletnih socialnih omrežjih zbiramo tako množico prijateljev, ne izhaja iz človekove potrebe po druženju, temveč potrebe po statusu. Rosenova uporabnike socialnih omrežij imenuje *iskalci statusa* (Rosen, 2007).

Spletna socialna omrežja združujejo na milijone uporabnikov, njihovo širjenje pa je še v porastu, saj je bilo februarja 2010 samo na Facebooku 400 milijonov aktivnih uporabnikov, v MySpace je bilo vključenih 66 milijonov. Za ponazoritev s kakšno hitrostjo se posamezna spletna socialna omrežja širijo, si poglejmo nekaj zgovornih podatkov:

- Facebook je bil ustanovljen februarja 2004, februarja letos je bila presežena številka 400 milijonov aktivnih uporabnikov, ki še narašča. S tem je Facebook za Googlom postala druga najbolj obiskana spletna stran na svetu.
- 50 % uporabnikov Facebooka se prijavi vsak dan in na njem prebije 55 minut dnevno.
- Povprečni uporabnik Facebooka ima 130 prijateljev.
- Približno 70 % uporabnikov Facebooka živi izven ZDA (Facebook, 2010).

3.1 Socialni inženiring in spletna socialna omrežja

Iz zgoraj povedanega, lahko na kratko strnemo naslednja dejstva, ki so značilna za spletna socialna omrežja: množičnost uporabnikov (razširjenost), naivno pojmovanje prijateljstva in zaupanja, tekmovanje za pridobitev čim večjega števila prijateljev, preobilje stikov (ki so površni), objavljanje velikega števila podatkov (družina, zaposlitev, socialno okolje itd.), drugačen način komunikacije (spletna socialna omrežja favorizirajo kvantiteto interakcije, posledično je manjša kvaliteta interakcije), znižana raven samovarovanja.
Za socialni inženiring je znano, da izkorišča človekove socialno-psihološke značilnosti, kot npr.: psihološki sprožilci (avtoriteta, recipročnost, obveza in doslednost, naklonjenost in privlačnost ter podobnost, razpoložljivost, konformnost), naravna tendenca človeka, da pomaga in zaupa, moralna dolžnost, razpršitev odgovornosti, prekomeren vpliv, preobremenitev, radovednost, brezbrižnost. Ko združimo zgoraj omenjene značilnosti spletnih socialnih omrežij in socialnega inženiringa, dobimo idealno okolje za izvajanje socialnega inženiringa. Zaradi svojih specifičnih značilnosti so spletna socialna omrežja idealno polje za tovrstne napade, saj lahko napadalec uporabi tako *computer based* kot tudi mutacijo klasičnih *human based* napadov, katerih temelj je neposredna človeška interakcija, le-ta pa se je v tem primeru preselila v internetno okolje. Prav to omogoča, da se izvajanja prevar s pomočjo socialnega inženiringa lahko lotijo tudi osebe, ki pri izvajanju klasičnega *human based* socialnega inženiringa ne bi bile uspešne. Zakaj ne? Za izvajanje klasičnega socialnega inženiringa so potrebne določene kvalitete, ki jih mora tak človek v medosebni komunikaciji nujno imeti. Naj jih naštejem nekaj: biti mora vztrajen in potrpežljiv, imeti mora odlične retorične sposobnosti, imeti mora privlačno osebnost, biti mora odličen opazovalec ljudi in okolice ter odličen igralec vlog, biti mora samozavesten (Gregorič, 2008).
Nekatere od naštetih lastnosti uspešnega socialnega inženirja pri zgoraj omenjeni mutaciji klasičnih *human based* napadov, v katerega sodi tudi socialni inženiring v spletnih socialnih omrežjih, so nepotrebne oz. so lahko izražene v manjši meri, saj je komunikacija iz oči v oči za socialnega inženirja veliko zahtevnejša kot pa komunikacija v virtualnem okolju. V spletnih socialnih omrežjih je vsak lahko kdorkoli. Ustvarjanje profila namreč nudi idealno krinko oz. možnost, da napadalec ustvari profil, za katerega ve, da bo v žrtvi vzbujal zaupanje, kar se v realnem življenju morda ne bi nikoli zgodilo. Če vsemu temu dodamo še naivnost, lahkomiselnost in brezbrižnost uporabnikov ter prepričanje, da ne more biti nič narobe, če informacije in podatke objavijo na svojih profilih, potem vidimo, da socialni inženir z na videz nepomembnimi podatki, ki so mu na razpolago na profilu napadenega, kot mozaik sestavlja posamezne informacije v celotno sliko, ki mu omogoča izvedbo napada. Navidezno nepomembni podatki kot so npr. rojstni datumi, imena domačih ljubljenčkov, imena sorodnikov, prelomni dogodki v življenju posameznika, so za spretnega socialnega inženirja smernice, s katerimi plete mrežo okoli svoje žrtve.
Kot rečeno, v spletnih socialnih omrežjih uspevajo tako *computer based* napadi, s katerimi poskušajo napadalci pretentati svojo žrtev tako, da le-ta nevede namesti na svoj računalnik določeno obliko škodljive programske kode, kot tudi mutacija klasičnih *human based* napadov, ki temeljijo na navezovanju stikov, zbiranju podatkov o določeni osebi in zlonamerno izkoriščanje le-teh. Eden od primerov klasičnega *computer based* napada je, ko žrtev dobi spletno povezavo do datoteke, ki naj bi bila njej zanimiva, v resnici pa ta povezava povzroči, da na svoj računalnik nevede namesti zlonamerno programsko kodo. Drugi primer pa lahko povežemo z mutacijo klasičnega *human based* napada, kjer napadalec z lažno ustvarjenim profilom in preko seznama žrtvinih prijateljev plete mrežo, s ciljem, da pridobi zaupanje ciljne osebe, kar mu bo omogočilo vpogled oz. dostop do zasebnega profila napadenega.

4 Nasveti za preventivno vedenje spletnih socialnih omrežij

Prišli smo v obdobje, ko je v spletnih socialnih omrežjih *spam* že povsem normalen pojav, socialni inženiring pa je v vzponu. Izobraževanju o varnosti oz. nevarnosti v spletnih socialnih omrežjih, ki je povezana z objavljanjem raznovrstnih podatkov na njih, bi morali posvečati veliko pozornosti tako v zasebnem življenju kot tudi v podjetjih.
Da je problem resen in da so zaradi socialnega inženiringa in spletnih socialnih omrežij ogrožena podjetja

in njihovi poslovni rezultati, so že spoznala tudi nekatera večja podjetja (Intel, IBM, Dell, Cisco, GM, BBC) in Evropska komisija, ki je leta 2009 s sedemnajstimi internetnimi ponudniki spletišč za socialno mreženje podpisala sporazum varnejšega socialnega mreženja, ki se osredotoča na varnost mladoletnikov, ki uporabljajo spletna socialna omrežja.
Podjetja so za svoje zaposlene izdelale smernice (politiko) za sodelovanje v spletnih socialnih omrežjih. Zavedajo se, da to ogrožanje ne izvira iz dejstva, da ljudje porabljajo delovni čas na spletnih socialnih omrežjih, temveč iz dejstva, da skozi ta medij za socialno interakcijo zaposleni nevede izdajajo poslovne skrivnosti ali druge podatke, za katere podjetje ne želi, da so javni oz. lahko s svojim vedenjem v spletnih socialnih omrežjih kompromitirajo podjetja.
Za uvajanje pravilnikov za uporabo spletnih socialnih omrežij v podjetjih ne obstaja enotno navodilo oz. postopek, saj je vsako podjetje specifično glede svojega področja delovanja in zaposlenih. Kljub temu pa lahko navedem nekaj splošnih vzrokov za implementacijo zgoraj omenjenih pravilnikov v podjetjih:

- ko govorimo o spletnih socialnih omrežjih, morajo imeti zaposleni jasno predstavo o tem, kakšno je stališče podjetja; to jim bo pomagalo pri njihovi komunikaciji na teh omrežjih,
- podjetja bodo delovala bolj inovativno ter usmerjeno v prihodnost in bodo svoje zaposlene ozaveščala o tem, kako so se spletna socialna omrežja integrirala v naša življenja,
- podjetje bo pravno zaščiteno pred morebitno zlorabo ali izgovorom o nevednosti, ki se nanašajo na kršitve politike o sodelovanju v spletnih socialnih omrežjih,
- zaposleni bodo imeli nabor dobrih praks in smernice, ko bodo uporabljali spletna socialna omrežja,
- zaposleni se bodo na ta način čutili opogumljene, da lahko s sodelovanjem v spletnih socialnih omrežjih pozitivno vplivajo na svojo vlogo in kariero (Schawbel, 2009),
- zaposleni se bodo bolj zavedali pomembnosti in vrednosti informacij ter dobili jasno sliko, katere informacije ni dovoljeno objavljati v spletnih socialnih omrežjih,
- z uvajanjem politike o sodelovanju v spletnih socialnih omrežjih se ustvari pozitiven psihološki pritisk, ki pripomore k razmišljanju o delovanju v spletnem socialnem omrežju in posledicah le-tega, kar pripelje do višje ravni ozaveščenosti.

Menim, da mora vsako podjetje vpeljati politiko delovanja v spletnih socialnih omrežjih ter določiti, kaj vse mora biti v to politiko vključeno. Pri tem je ključnega pomena, da se pogosto opravlja revizija ustreznosti in učinkovitosti uvedene politike ter se jo po potrebi prilagodi spremembam v podjetju in spremembam v spletnih socialnih omrežjih. Pomembno pa je, da se o nevarnostih in zlorabah v spletnih socialnih omrežjih, ki so v veliki meri posledica socialnega inženiringa, zavedamo tudi v zasebnem življenju. Še posebej pomembno pa je, da o pasteh sodelovanja v spletnih socialnih omrežjih starši izobražujejo svoje otroke.
Za konec navajam enajst priporočil, ki jih predlaga podjetje Microsoft:

- bodite previdni pri odpiranju spletnih povezav (*link*), ki ste jih dobili v sporočilih od svojih prijateljev,
- zavedajte se, kaj ste objavili o sebi – podatki kot so: rojstno mesto, datum rojstva, srednja šola ipd., lahko v primeru možnosti za obnovitev izgubljenega gesla (F*orgot your password?*), ki jo ponujajo nekatera spletna mesta, in sicer s t.i. tajnim vprašanjem oz. namigom za geslo, spretnemu socialnemu inženirju omogočijo, da s podatki, ki jih je pridobil na spletnem socialnem omrežju, vdre v vaše finančne ali druge spletne račune,
- ne zaupajte, da sporočilo v resnici prihaja od osebe, za katero se pošiljatelj izdaja (identiteta pošiljatelja je lahko ukradena),
- v izogib nepooblaščenemu izdajanju naslovov spletne elektronske pošte ljudi, ki jih imate na seznamu prijateljev, onemogočite aplikacijam spletnih socialnih omrežij, da skenirajo vaš elektronski imenik naslovov,
- internetni naslov vašega spletnega socialnega omrežja vpišite direktno v vaš brskalnik oz. uporabljajte samo osebne zaznamke, da se izognete možnosti kraje vašega imena računa in gesla na ponarejenih spletnih straneh,
- bodite selektivni in previdni, koga sprejmete na listo prijateljev; spletni prevaranti, ki kradejo

identitete, redno prakticirajo socialni inženiring tako, da ustvarjajo ponarejene spletne profile z namenom pridobitve nepooblaščenih informacij,
- previdno izberite spletno socialno omrežje, ki ga boste uporabljali in se dobro seznanite z njihovo politiko zasebnosti,
- zavedajte se, da vse, kar napišete v spletnih socialnih omrežjih, tam ostane za vedno,
- bodite previdni pri nameščanju dodatkov na vaši strani, kriminalci lahko uporabijo te aplikacije za krajo vaših osebnih informacij,
- dvakrat premislite, ko uporabljate spletna socialna omrežja na delovnem mestu,
- pogovorite se z vašim otrokom o spletnih socialnih omrežjih in bodite prepričani, da jih uporabljajo varno (Microsoft, 2010).

Napotek vseh napotkov, ki bi ga morali uporabniki spletnih socialnih omrežij upoštevati vedno in povsod, pa se glasi: »*Premisli dvakrat, preden objaviš*!«.

5 Zaključek

Na kratko lahko rečemo, da je socialni inženiring pridobivanje informacij s pomočjo manipulacije ljudi. Oblik socialnega inženiringa je pravzaprav nešteto in so v največji meri odvisne od iznajdljivosti, spretnosti in znanja socialnega inženirja. Novo, lahko rečemo kar neskončno polje delovanja socialnih inženirjev je zagotovo internet, še posebej spletna socialna omrežja, ki privabljajo nove in nove uporabnike. Zgovoren je podatek, da ima samo Facebook več kot 400 milijonov uporabnikov, kjer posamezniki objavljajo svoje podatke, fotografije, podatke o bližnjih, o zaposlitvi in sodelavcih itd. Spletna socialna omrežja na novo definirajo pojma prijateljstvo in zaupanje. Zato je treba dobro spoznati način delovanja spletnih socialnih omrežij in socialno-psihološke značilnosti vedenja ljudi na teh omrežjih, saj bomo na ta način lahko razumeli napade s pomočjo socialnega inženiringa, ki izkoriščajo prav te socialno-psihološke značilnosti. Prav ta nova definicija pojmov prijateljstva in zaupanja ter več ali manj nekontrolirano razkrivanje raznovrstnih podatkov predstavljajo grožnjo tako posameznikom kot podjetjem. Spreten socialni inženir je sposoben, iz množice na videz neškodljivih informacij, pridobiti podatke in informacije, s katerimi lahko izvede napad s pomočjo socialnega inženiringa in s prevaro pridobi najrazličnejše koristi, od finančnih, kraje poslovnih in osebnih podatkov itd. Da ne smemo podcenjevati nevarnosti, ki jo v spletnih socialnih omrežjih predstavlja socialni inženiring, se zaveda vse več strokovnjakov, ki se ukvarjajo z informacijsko varnostjo in prav opozorila teh strokovnjakov napovedujejo, da bo v prihodnosti socialni inženiring še naprej predstavljal eno največjih nevarnosti informacijske varnosti, tako za posameznika kot za podjetja, saj je s spletnimi socialnimi omrežji ta pojav dobil nov zagon. Potrebno je neprekinjeno spremljanje oblik izvajanja socialnega inženiringa ter o tem obveščati in izobraževati ljudi, tako v zasebnem življenju kot na delovnem mestu. V podjetjih pa je pomembno, da odgovorni spoznajo, poleg nekaterih koristi spletnih socialnih omrežij, tudi nevarnosti, ki jih le-ta prinašajo ter namenijo primerno količino časa in finančnih sredstev za vpeljavo politik in izobraževanja, ki bodo zaposlene in podjetje obvarovala pred nevarnostmi, ki prežijo v spletnih socialnih omrežjih.

6 Literatura

Boyd, M. D. in Ellison, B. N. (2007). *Social Network Sites: Definition, History, and Scholarship***.** Članek dobljen 15.3.2010 na: http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html

Europa press releases (2009). *Socialno mreženje: sporazum Komisije za varnejšo spletno uporabo med največjimi internetnimi podjetji*. Članek dobljen 25.3.2010 na: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/232&format=HTML&aged=0&language=SL&guiLanguage=en

http://www.facebook.com/press/info.php?factsheet

Fripp, Patricia. *Why Do People Say "Yes?" The "6 Weapons of Influence"***.** Članek dobljen 12.12.2009 na http://www.fripp.com/art.of_influence.html

Gregorič, U. (2008). *Socialni inženiring: prepoznava, obramba in njegova pravna kategorizacija***.** (Diplomsko delo). Ljubljana: Fakulteta za varnostne vede.

IP RS – Informacijski pooblaščenec RS. *Pogosta vprašanja. Varstvo osebnih podatkov*. Dobljeno 25.12.2007 na http://www.iprs.si/pogosta-vprasanja/varstvo-osebnih-podatkov/

Meriam Webster Online Dictionary. Dobljeno 9.12.2009 na http://www.m-w.com/home.htm

Microsoft (2010). *Microsoft Online Safety. 11 Tips for Social Networking Safety***.** Članek je dobljen 23.2.2010 na http://www.microsoft.com/protect/parents/social/socialnet.aspx

Mitnick, K. D. & Simon, W. L. (2002). *The Art of Deception: controllling the human elements of security*. Indianapolis: Wiley.

Radulj, B. (2003). *Socialni inženiring - vpliv na informacijsko varnost***.** *(Diplomsko delo)*. Ljubljana: Fakulteta za varnostne vede.

Rosen, C. (2007). *Virtual Friendship and the New Narcissism***.** Članek dobljen 20.2.2010 na: http://www.thenewatlantis.com/publications/virtual-friendship-and-the-new-narcissism

Schawbel, D. (2009). *Implement Social Media Guidelines, Now***.** Članek dobljen 15.1.2010 na http://www.briansolis.com/2009/09/implement-social-media-guidelines-now/

SSKJ, elektronska izdaja, v1.1. (2005). Ljubljana: DZS.

Timko, D. (2008). *The Social Engineering Threat***.** *ISSA Journal*. Članek je dobljen 10.12.2009 na https://www.issa.org/Library/Journals/2008/January/Timko-The%20Social%20Engineering%20Threat.pdf