Originalni naučni rad 343.533:004.056.5

*Dr Ljubomir Stajić, redovni profesor*
*Pravnog fakulteta u Novom Sadu*

*Mr Goran J. Mandić, asistent*
*Fakultet bezbednosti u Beogradu*

# SOCIJALNI INŽENJERING KAO OBLIK UGROŽAVANJA POVERLJIVIH POSLOVNIH INFORMACIJA

***Sažetak:*** *U mnogim poslovima, pogotovo tamo gde treba doći do poverljivih informacija u kontaktu sa drugim ljudima, prisutne su pojedine forme socijalnog inženjeringa. Socijalni inženjering je oblik govorne i gestikularne manipulacije pojedincima sa ciljem da se navedu na ispunjenje nekih zahteva postavljenih od strane napadača.*

*Problemi koji se javljaju u oblasti zaštite poverljivih informacija nalaze se u činjenici da iza svakog kompjutera, stoji čovek kao jedinka sa svim svojim dobrim i lošim osobinama. Socijalni inženjering je tehnika u kojoj se ubeđivanje i/ili obmana koriste da bi se dobio neovlašćen pristup kompjuterskim sistemima. Ovo se obično postiže razgovorom ili nekim drugim oblicima interaktivne komunikacije.*

*Protivmere u borbi protiv socijalnog inženjeringa su vrlo složene. Usložava ih činjenica da svako ko ima pristup bilo kom delu informacionog sistema predstavlja moguću metu napada socijalnim inženjeringom.*

*Za razliku od ostalih napada na kompjutere, socijalni inženjering se ne odnosi na tehnološku manipulaciju i korišćenje ranjivosti hardvera ili softvera. Pored toga i ne zahteva posebne tehničke veštine i znanja. Ova vrsta napada eksploatiše ljudske slabosti, kao što su nemarnost ili želja za kooperativnošću, kako bi se dobio pristup poverljivim dokumentima koji se nalaze na kompjuteru.*

*Cilj socijalnog inženjeringa može biti sticanje profita, sajber terorizam ili pristup internim sistemima i poverljivim informacijama. Mete napada su, najčešće, provajderi telekomunikacionih usluga, multinacionalne kompanije, finansijski ustanove, bolnice, vladine agencije, vojska i drugi.*

***Ključne reči**: socijalni inženjering, bezbednost informacija, bezbednosni sistemi, kompanije, hakeri, kompjuterski kriminal*

## 1. Pojam socijalnog inženjeringa

Istorijski posmatrano veština uveravanja suprotne strane da postupi po nečijem zahtevu nije koncept koji je svojstven samo savremenom dobu. Prve korene veštine uveravanja srećemo u formi retorike na tlu Grčke Sicilije, negde oko 485. godine pre naše ere, gde je na nastanak ove veštine presudnu ulogu imala sudska praksa. Retorika je od samog početka smatrana tehnikom uveravanja.[1] Cilj uveravanja bio je ubediti sudije i porotnike u krivicu koju je dokazivao oštećeni retorikom sa pozicije tužioca, odnosno u nevinost koju je govorom branio optuženi. Samo od veštine govora zavisila je procena verodostojnosti njihovih tvrdnji i iskaza. Pisani tragovi iz tog vremena potvrđuju značaj smišljenog uveravanja sa unapred definisanim ciljem, iako je jasno da je uveravanje oduvek bilo prisutno u komunikaciji između ljudi.

Od trenutka kad se govor pretvorio u tehniku uveravanja, postoje dva načina njegovog korišćenja. Prvi, za koji možemo reći da je opstao do danas, u kome se ističe svemoć jezika kao sredstva za uveravanje, a s druge strane (prema Aristotelu) savetuje se da upotreba tog sredstva mora biti u saglasju sa posebnom etikom, makar to dovelo do odustajanja od neprestane, često bezuspešne potrage za delotvornošću.[2] Za njega, ubeđivanje je veština. To je „veština navođenja ljudi da učine nešto što oni obično ne bi učinili ako vi to ne zatražite".[3]

Manipulacija i uveravanje, kao pretpostavka uspešnog socijalnog inženjeringa, u svom osnovnom pojavnom obliku, koristi govor sa ciljem uveravanja suprotne strane u neke činjenice, na način gde se zaobilazi istina, uz upotrebu svih raspoloživih sredstava uveravanja u izrečeno.

U mnogim poslovima, pogotovo tamo gde treba doći do poverljivih informacija u kontaktu sa drugom stranom, ili pak stići do nekog cilja, prisutne su modifikovane forme socijalnog inženjeringa. Možemo reći da policajci u svom operativnom radu skoro svakodnevno koriste socijalni inženjering sa ciljem da otkriju i uhvate izvršioce krivičnih dela. Bez obzira da li je cilj pozitivan i ispravan, ili ne, pristup je isti, manipuliše se drugom osobom da bi se postigao neki krajnji cilj. Mogli bi-

[1] Breton, F.: *Izmanipulisana reč*, Clio, Beograd, 2000, str. 56.

[2] Breton, F: *Izmanipulisana reč*, Clio, Beograd, 2000, str. 60.

[3] Borg, DŽ.: *Ubeđivanje: umetnost ubeđivanja ljudi*, IPS Media, Beograd, 2008, str. 4.

smo reći da je to jedan od najstarijih načina stizanja do nekog cilja putem interaktivnog odnosa dve ili više osoba, iako se njegova forma menjala vremenom.

Iz prethodno navedenog možemo zaključiti da skoro svako ljudsko biće poseduje potencijale za pokušaj napada socijalnim inženjeringom. Jedina razlika je u potrebi, motivaciji i nivou veštine potencijala koji se koriste.

Interesantno je napomenuti da je još 1997. godine, za ovu vrstu govorne manipulacije upotrebljen pojam socijalni inženjering gde se kaže da je on u osnovi „umetnost i nauka navođenja ljudi da vam ispune želje. To nije način kontrole uma i neće omogućiti da navedete ljude da obavljaju zadatke mnogo van njihovog normalnog ponašanja i daleko od sigurnog".[4] Najkraće rečeno, socijalni inženjering je oblik govorne i gestikularne manipulacije pojedincima sa ciljem da se navedu da urade nešto što inače ne bi uradili, a odnosi se na ispunjenje nekih zahteva postavljenih od strane napadača.

Problemi koji se javljaju u oblasti bezbednosti kompanija ili vladinih ustanova i agencija i zaštiti poverljivih informacija nalaze se u činjenici da iza svakog kompjutera, bio on samostalan deo mreže ili server stoji čovek kao jedinka sa svim svojim dobrim i lošim osobinama. Nije važno koje generacije su kompjuteri, koji je operativni sistem instaliran i koji hardver i softver se koristi za zaštitu poverljivih informacija na njemu, jer se u svom radu svi ovi sistemi oslanjaju na čoveka. Jasno je u ovom slučaju da ta jedinka predstavlja najslabiju kariku bezbednosnog lanca kojim se štite informacije.

Socijalni inženjering je tehnika u kojoj se ubeđivanje i/ili obmana koriste i da bi se dobio pristup kompjuterskim sistemima.[5] Ovo se obično postiže razgovorom sa ljudima ili nekim drugim oblicima interaktivne komunikacije.

Najslabija karika u sistemu obezbeđenja uvek će biti ljudi, a najlakši način da se prodre u sistem obezbeđenja je planiranje upada koristeći se ljudima.[6] Postoji razmišljanje da je najsigurniji i jedini bezbedan kompjuter onaj koji je isključen iz izvora napajanja. Ova tvrdnja je na prvi pogled tačna, ali samo postojanje mogućnosti da nekog ubedite da ga uklju-

---

[4] *People Hacking: The Psychology of Social Engineering*, Text of Harl's Talk at Access All Areas III, 05/07/97, http://packetstormsecurity.nl/docs/social-engineering/aaatalk.html, pristupljeno 28.03.2010.

[5] Gattiker, U. E.: *The information security dictionary*, Kluwer Academic Publishers, Boston, 2004, str. 306.

[6] Rittinghouse, J.; Hancock W. M.: *Cybersecurity Operations Handbook*, Elsevier Digital Press, Oxford, str. 298.

či u izvor napajanja i potom aktivira operativni sistem, dovoljno govori da je prethodna tvrdnja iluzija.

Socijalni inženjering se definiše i kao „dobijanje poverljivih informacija sredstvima ljudske interaktivne komunikacije." (Business Wire, August 4, 1998.).[7]

Tako na primer pretvarajući se da je osoba na visokom položaju napadač može svojim zahtevom i autoritetom da zaplaši metu napada (novozaposlenu radnicu) negativnim posledicama ako ne ispuni njegov zahtev. Važan faktor koji pomaže ovom pristupu je verovanje da se autoriteti obično ne smeju proveravati. Ljudi će ispuniti neke veoma neobične zahteve za osobe za koje veruju da su na značajnoj poziciji.[8]

Kolege iz druge organizacione celine ili drugog grada, kao i novozaposleni se, takođe ne odbijaju, pogotovo ako im je potrebna neka vrsta hitne pomoći da ne bi trpeli posledice zbog neobavljenog posla. Ovu kolegijalnost veoma vešto koristi napadač da bi došao do informacija. Kevin Mitnik poznat kao „Kondor," je bio prvi haker koji je dospeo na listu najtraženijih osoba Federalnog istražnog biroa. Na ovaj način upao je u mnoge organizacije među kojima su Digital Equipment Corp, Motorola, Nokia Mobile Phones, Fujitsu, i mnoge druge.[9]

Ono što je činjenica i što usložava protivmere u borbi protiv socijalnog inženjeringa je saznanje da svako ko ima pristup bilo kom delu informacionog sistema, (fizički, ili elektronski posredstvom kompjuterske mreže) predstavlja potencijalni rizik po bezbednost informacija. Bilo koja informacija do koje se može doći predstavlja korak ka sledećoj informaciji i tako dok se ne stigne do one informacije koja je cilj napada. To ukazuje na činjenicu da i zaposleni koji se ne smatraju bezbednosno ugroženi i nisu uključeni u mere bezbednosne zaštite, mogu biti meta napada socijalnim inženjeringom.

Za razliku od ostalih napada na kompjutere, socijalni inženjering se ne odnosi na tehnološku manipulaciju i korišćenje ranjivosti hardvera ili softvera i pored toga ne zahteva posebne tehničke veštine i znanja. Ova vrsta napada eksploatiše ljudske slabosti, kao što su nemarnost ili želja za kooperativnošću, kako bi se dobio pristup legitimnim dokumentima koji se nalaze na kompjuteru.[10] Najteže je braniti se od napada socijalnim inženjeringom, jer ga ne mogu zaustaviti samo-

---

[7] Shinder, D. L.: *Scene of the Cybercrime: Computer Forensics Handbook*, Syngress Publishing, Inc., Rockland, 2002, str. 313.

[8] Gregg, M.: *Certifie Ethical Hacker Exam Prep*, Que Publishing, 2006, E-book.

[9] Gregg, M.: *Certifie Ethical Hacker Exam Prep*, Que Publishing, 2006, E-book.

[10] Shinder, D. L.: *Scene of the Cybercrime: Computer Forensics Handbook*, Syngress Publishing, Inc. 800 Hingham Street Rockland MA 02370, USA, 2002, str. 313.

stalno ni hardver ni softver.[11] Primera radi lice koje koristi socijalni inženjering za napad može ubediti operatera korisničkog servisa da mu otkrije neophodne detalje kako bi se povezao na informacioni sistem. Kasnije, napadač ponovo nazove drugog operatera žaleći se da njegova šifra iz nekog razloga ne radi i ubeđuje korisnički servis da mu promene šifru. Na taj način ta osoba dobija neovlašćeni pristup kompjuterskom informacionom sistemu.[12]

## 2. Profil lica koje izvršava socijalni inženjering

Ranije smo videli da je osnovni cilj socijalnog inženjeringa neovlašćen pristup kompjuterskim sistemima ili poverljivim informacijama i po tome on je sličan cilju hakera. Nakon što je dobilo pristup informaciji, lice koje koristi socijalni inženjering može da je koristi ili za druge napade, ili da bi poremetio sistem i izazvao štetu. Socijalni inženjering može biti organizovan zbog profita, sajber terorizma ili za pristup internim sistemima i poverljivim informacijama. Takođe može biti primenjen i radi edukacije i obuke zaposlenih korisnika za kontra mere. Najčešće se napadaju velike organizacije koje skupljaju i skladište osetljive podatke, kao što su provajderi telefonskih usluga, multinacionalne kompanije, finansijski entiteti, bolnice i vojska.[13] Naravno pored navedenih napad može biti usmeren i prema bilo kom preduzeću ili vladinoj ustanovi ili agenciji.

Određivanje precizno definisanog profila lica koja sprovode socijalni inženjering je vrlo teško. Može se samo reći da su to uglavnom lica muškog pola, mada se u praksi sreću i žene koje su bile veoma uspešne.

Tako na primer prva poznata žena haker, koja je radila pod pseudonimom Suzan Tander, bila je specijalizovana za upade u vojne kompjutere i kompjutere telefonskih kompanija. Bila je povezana sa poznatim hakerima, braćom Ronom i Kevinom Mitnikom. Posmatrajući njenu prošlost, prošla je kroz razne faze razvoja i postala vrstan telefonski i kompjuterski haker.[14]

---

[11] Thomas Mathew: *Ethical Hacking and Countermeasures [EC-Council Exam 312-50]—Student Courseware*, OSB Publisher, International Council of Electronic Commerce Consultants, New York, 2004. elektronska forma.

[12] Gattiker, U. E.: *The information security dictionary*, Kluwer Academic Publishers, Boston, 2004, str.306.

[13] Janczewski, J. L.; Colarik, M. A.: *Cyber Warfare and Cyber Terrorism,* Information Science Reference, Hershey - New York, 2008, str. 184.

[14] Shinder, D. L.: *Scene of the Cybercrime: Computer Forensics Handbook*, Syngress Publishing, Inc., Rockland, 2002, str. 107.

Starosnu strukturu kao element profila počinioca, takođe je teško odrediti. Kreće se od tinejdžerskog uzrasta do zrelog doba. Može se reći, da su napadači najaktivniji u periodu od dvadesete do tridesete godine života. Lica koja ga sprovode u pozitivnoj konotaciji (da bi proverili bezbednost pravnog entiteta) pripadaju nešto starijoj životnoj dobi.

Ova lica su inače veoma inteligentne i izuzetno kreativne osobe. Poseduju dobre komunikacijske i manipulatorske veštine, dobri su poznavaoci psihologije i uglavnom imaju dovoljno tehničkog znanja. Mogu da nastupaju timski i samostalno, s tim što je timski napad mnogo opasniji jer udružuju svoja znanja i umeća poštujući se međusobno i uvažavajući hijerarhiju.

Često timski napad rezultira dozvolom za ulazak u kompaniju i na kraju sticanje željenih informacija.[15]

Postavlja se pitanje koje sve kategorije ljudi i u kojim sve prilikama, mogu da koriste socijalni inženjering. Podela može biti napravljena u odnosu na motiv koji ih pokreće i cilj koji se želi postići.

Te grupe su:

1. hakeri,
2. kradljivci identiteta,
3. lica koja se bave industrijskom špijunažom,
4. lica koja pribavljaju informacije o radu konkurencije,
5. nezadovoljni zaposleni,
6. razne vrste kriminalaca,
7. teroristi,
8. privatni detektivi,
9. lica koja proveravaju funkcionisanje sistema obezbeđenja,[16]
10. lica koja rade u obaveštajnim agencijama države i policiji,
11. građani u svojim svakodnevnim aktivnostima.

Kod svih pomenutih grupa ljudi koje koriste socijalni inženjering, zajedničko je samo to da ga koriste, dok su motivi uglavnom različiti. Sa aspekta bezbednosti treba se fokusirati na one kategorije ljudi koji ga koriste u destruktivne svrhe sa ciljem da dođu do određene koristi, bez obzira da li je ona materijalna, ili se ogleda u ostvarenju određenih ideja i želja.

---

[15] Rittinghouse, J.; Hancock W. M.: *Cybersecurity Operations Handbook,* Elsevier Digital Press, Oxford, 2003, str. 299.

[16] Lice koje proverava funkcionisanje sistema obezbeđenja korišćenjem socijalnog inženjeringa proverava integritet zaposlenih u kompaniji, kao i funkcionisanje kontrole pristupa pokušajem ulaska u restriktivni - štićeni prostor. Integritet zaposlenih se proverava pokušajima neovlašćenog dolaska do informacija koje poseduju.

U daljem tekstu prikazaćemo preduslove koje treba da ispuni osoba koja koristi socijalni inženjering. Za te preduslove možemo reći da predstavljaju kriminogene faktore u užem smislu i odnose se na motiv, spremnost i mogućnost izvršenja socijalnog inženjeringa.

Naime, da bi se neke konkretne ilegalne aktivnosti mogle realizovati, neophodno je da se u određenom vremenskom trenutku kod potencijalnog izvršioca istovremeno steknu tri preduslova:

- Motiv zbog kog bi potencijalni izvršilac preduzeo kriminalnu radnju,
- Spremnost izvršioca da zbog toga prihvati određeni rizik i
- Mogućnost da se kriminalna radnja izvrši.[17]

Pored ovako definisanih kriminogenih faktora u užem smislu, u literaturi pronalazimo navođenje i drugih preduslova kako bi napadač ostvario svoj cilj.

Ti preduslovi su:

- metod (mora imati veštine, sredstva i ostale neophodne resurse za izvršenje napada),
- mogućnost (izvršilac mora imati vreme i pristup kako bi obavio i uspeo u napadu) i
- motiv (mora postojati razlog zbog koga će izvršilac izvesti napad.).[18]

Analizom navedenih preduslova dolazimo do zaključka da je i jedna i druga klasifikacija preduslova nepotpuna kada govorimo o napadima na kompjutere. Naime, u prvoj ne postoji metod kao važan preduslov ispunjenja napada, dok se u drugoj ne pominje spremnost, bez koje nema ispunjenja kriminalne aktivnosti. Iz tog razloga prihvatljivije je reći da su preduslovi predstavljeni kroz četiri kategorije ili faktora i to:

- motiv,
- spremnost,
- mogućnost i
- metod.

*Motiv* je psihološki faktor koji se definiše kao proces koji izaziva, usmerava i održava određene aktivnosti koje lice dovode do projektovanog cilja.

Motivi mogu biti različiti. Neki izvode napade kako bi ukrali novac, ili specifične podatke. Drugi to čine kao izazov ili iz zabave.

[17] Petrović, R. S.: *Kompjuterski kriminal,* Ministarstvo unutrašnjih poslova Republike Srbije, Beograd, 2000, str. 108.

[18] Pfleeger P. C.: *Security in Computing*, Fourth Edition, Prentice Hall, Pearson Education, Inc., Upper Saddle River, 2006, elektronsko izdanje.

Ostali, pak, iz osvete.[19] Pri tome, svaki kriminalac ima svoje sopstvene motive koji se mogu menjati, mogu trajati godinama, a mogu da se jave i iznenada.[20]

Primarni projektovani motivi kod socijalnog inženjeringa su u osnovi isti, dolaženje do upotrebljivih i kvalitetnih informacija, dok sekundarni motivi mogu biti različiti u zavisnosti od profila napadača i navode se kao izazov, novac, takmičenje sa drugima i samodokazivanje i slično.

*Spremnost* predstavlja svesno prihvatanje određenog rizika po napadača, koji neminovno postoji kao posledica njegovog delovanja. Spremnost može biti inicirana različitim karakternim osobinama počinioca i uslovljena motivom.

*Mogućnost* označava kvantitet i kvalitet lakoće i izvesnosti kojom osoba može da počini štetno, zabranjeno, protivzakonito i/ili krivično delo, a da ne bude otkrivena.

Kao i sve druge pojave, prestup je sticaj prilika i okolnosti u datom vremenu i prostoru.[21] Sticaj prilika i okolnosti označava i mogućnost da se prestup izvrši.

*Metod* predstavlja način napada koji je uslovljen i determinisan veštinama, stepenom komunikacije, posebnim znanjima, potrebnom opremom (hardverom i softverom) i neophodnim pratećim resursima, koji jedino zbirno omogućavaju uspešno ostvarenje cilja napadača.

Ukoliko jedan od četiri pomenuta faktora ne postoji, napad se neće desiti. Činjenica je da se na motiv i spremnost ne može uticati jer su objektivno van kontrole lica koje štiti sistem. U funkciji proaktivnog delovanja na mogućnost se može uticati njenom eliminacijom ili umanjenjem i na taj način se može sprečiti i odvratiti lice od činjenja napada usmerenog na neovlašćeno prikupljanje i dobijanje informacija. Četvrti preduslov, metod, u današnjim uslovima predstavlja relativno lako savladivu prepreku, pogotovo ako govorimo o socijalnom inženjeringu. Problem je u tome što su informacije i znanje o sistemima i metodama napada lako dostupni na Internetu.

Tako na primer, utvrđeno je da su desetine hiljada internet stranica sadržavale softverske alate i uputstva korisna za sajber napad i da su mili-

---

[19] Pfleeger P. C.: *Security in Computing*, Fourth Edition, Prentice Hall, Pearson Education, Inc., Upper Saddle River, 2006, elektronsko izdanje.

[20] Petrović, R. S.: *Kompjuterski kriminal,* Ministarstvo unutrašnjih poslova Republike Srbije, 2000, str. 110.

[21] Krstić, O.: *Primenjena kriminalistika*, Zavod za udžbenike i nastavna sredstva, Beograd, 1997, str. 5.

on korisnika kompjutera posedovali veštine da ih iskoriste tako da prouzrokuju značajno oštećenje na internet komponentama i mehanizmima.[22]

Ako neko ima motiv i spremnost, bez većih poteškoća će naći potrebna znanja, alate u vidu softvera i načine kako napasti određene sisteme. Ako ovome dodamo i relativno lak pristup kompjuterskim mrežama preko Interneta i neznanje o socijalnom inženjeringu, jasno je da se napadačima često ukazuje prilika, odnosno da objektivno postoji mogućnost za izvršenje napada.

Kombinacija motiva, spremnosti i metoda, s jedne strane, i, s druge strane, evidentne i stalne ili trenutne slabosti u funkcionisanju i organizaciji bezbednosti i zaštite informacija, nameće eventualnim izvršiocima pitanje i dilemu kolika je verovatnoća da će uspeti, ukoliko počine (izvrše) napad, i kakve su mogućnosti da počinjeno delo ostane neotkriveno?

Veoma je važno znati da će potencijalni izvršilac inkriminisane radnje ovo pitanje postaviti sebi uvek pre nego što počini zabranjeno delo. Ukoliko su adekvatnim procedurama zaštite eliminisane mogućnosti i postoji veliki broj prepreka do cilja i ako je izuzetno veliki stepen verovatnoće otkrivanja dela, odnosno izvesno je da će izvršilac biti uhvaćen, mali broj potencijalnih napadača će pokušati da izvede inkriminisano delo.

## 3. Socijalni inženjerig kao oblik pretnje štićenim informacijama

Smanjiti ranjivosti sistema koji se štiti nije uvek lako. Prvi korak u tom procesu podrazumeva identifikovanje vrste pretnji koje mogu da se ostvare. Identifikacija protivnika, utvrđivanje njegovih osobina i karakteristika i vrsta pretnji je realna pretpostavka uspešnom suprotstavljanju kroz razvijanje sistema obezbeđenja i zaštite. Zadatak menadžmenta zaduženog za obezbeđenje i bezbednost kompanija je da shvate ko je, ili šta je njihov eventualni protivnik. Često im to i ne uspeva. Razlog je to što su nedovoljno edukovani, pogotovo kad je u pitanju socijalni inženjering, te ne mogu ispravno da identifikuju ili okarakterišu ovu vrstu pretnje.

Kada nisu u mogućnosti da identifikuju pretnje i protivnike, lica zadužena za obezbeđenje imovine i poslovanja i bezbednost generalno se umesto pomenutog usredsređuju na smanjenje ranjivosti, što je po-

[22] Parker, T.; Shaw, E.; Stroz, E.; Devost, G. M.; Sachs, H. M.: *Cyber Adversary Characterization: Auditing the Hacker Mind,* Syngress Publishing, Inc., Rockland, 2004, str. 221.

grešna logika iz razloga što je ranjivost u uzročno-posledičnoj vezi sa pretnjom.

Sa umanjenjem ili uklanjanjem pretnji i shodno tome sa smanjenom ranjivosti, pretnje se ne mogu ispoljiti same od sebe. Nakon svega, ako jedan sistem nije ranjiv na napad, onda ne može biti štete od napada. Organizacije sa odbrambenim položajima koje se orijentišu na pretnju, pre nego na ranjivost ili izloženost, orijentisane su često na neshvatanje ovog jednostavnog pravila.[23]

Iz tog razloga neophodno je utvrditi ko predstavlja pretnju po bezbednost informacija i shodno tome razviti sistem adekvatne zaštite koji uzima u obzir pretnje i ranjivosti na koje su one usmerene.

Kritične informatičke infrastrukture su ranjive na napade na mnogo načina iz mnogih uglova, uključujući i napade fizičkim pristupom i napade izvedene preko kompjuterske mreže. Međuzavisnosti između elemenata infrastrukture čine rizičnim sve elemente, tako da će uspešan napad na jedan deo sistema sigurno uticati na druge delove sistema koji nisu direktno napadnuti, ali su međusobno povezani.[24]

Kompjuterski kriminalitet predstavlja oblik kriminalnog ponašanja, kod koga se korišćenje kompjuterske tehnologije i informacionih sistema ispoljava kao način izvršenja krivičnog dela, ili se kompjuter upotrebljava kao sredstvo, ili cilj izvršenja, čime se ostvaruje neka, u krivično-pravnom smislu, posledica.[25]

Kompjuterski kriminalitet možemo klasifikovati kroz sledeće tipove koji donekle oslikavaju motive kao i mete napada i to na:

- vojne i obaveštajne napade,
- poslovne napade,
- finansijske napade,
- terorističke napade,
- osvetnički napadi i
- napadi zabave radi.[26]

U svim ovim napadima, pored ostalih tehnika, prisutan je i socijalni inženjering.

---

[23] Parker, T.; Shaw, E.; Stroz, E.; Devost, G. M.; Sachs, H. M.: *Cyber Adversary Characterization: Auditing the Hacker Mind,* Syngress Publishing, Inc., Rockland, 2004, str. 229.

[24] Parker, T.; Shaw, E.; Stroz, E.; Devost, G. M.; Sachs, H. M.: *Cyber Adversary Characterization: Auditing the Hacker Mind,* Syngress Publishing, Inc., Rockland, 2004, str. 229.

[25] Kukrika, M.: *Upravljanje sigurnošću informacijama*, Infohome, Beograd, 2002, str.66.

[26] Stewart, M. J.; Tittel, E.; Chapple, M.: *CISSP - Certified Information Systems Security Professional Study Guide,* 3rd Edition, SYBEX Inc, 1151 Marina Village Parkway, Alameda, CA 94501, 2005, str. 606.

### *3.1. Vojni i obaveštajni napadi*

Motiv vojnih i obaveštajnih napada se ogleda prvenstveno u želji da se dođe do informacija koji predstavljaju tajnu od značaja za funkcionisanje vojske, policije, državnih institucija ili određenih procesa koji se sprovode pod okriljem države. Obelodanjivanje i otkrivanje ovog tipa informacija može da kompromituje određene istrage koje sprovodi policija, poremetiti funkcionisanje vojske i da predstavlja pretnju nacionalnoj bezbednosti države.

Zbog svoje osetljivosti, značaja i prirode ovih informacija, one su često atraktivna meta napada pogotovo za iskusne napadače. Ovakve napade sprovode lica koja su izuzetno motivisana, spremna i lica sposobna da istraže i pronađu mogućnost za napad i koja imaju veoma razvijene metode za ove vrste napada. Po završetku ove vrste napada iza napadača ostaje veoma malo ili nimalo dokaza koji govore da se napad uopšte i desio i možemo reći da su napadi u ovoj kategoriji veoma uspešni kada se izvedu do kraja.

### *3.2. Poslovni napadi*

Poslovni napadi su usmereni na otkrivanje i ekploataciju poverljivih informacija proizvodnih, uslužnih ili naučnoistraživačkih organizacija. Te informacije su od ključne važnosti za funkcionisanje organizacije. To su na primer: strategijski planovi razvoja i usvajanja novog proizvoda, analiza konkurencije, informacije marketinške i finansijske prirode koje nisu namenjene javnosti, uslovi poslova koji se dogovaraju i podaci o klijentima i zaposlenima. Motiv je ostvarivanje materijalne dobiti ili nanošenje štete i uništavanje reputacije mete napada.

Prikupljanje poverljivih informacija, predstavlja industrijsku špijunažu i kao pojava nije nova. Pre pojavljivanja Interneta, ovo prikupljanje informacija zahtevalo je dugotrajnu obuku pojedinaca i značajna materijalna sredstva. Danas je to promenjeno korišćenjem sofisticiranijih oblika prikupljanja informacija kao i količinom informacija dostupnih na Internetu. Ova tehnika deluje samo protiv mete napada koja aktivno skladišti i čuva svoje informacije na kompjuterima. Prikupljanje poslovnih podataka i informacija samo po sebi neće imati fizički destruktivni ili razorni efekat na kritičke infrastrukture vlasnika informacija.

Kompanije širom sveta špijuniraju jedni druge iz različitih razloga. Većina špijunskih operacija se usredsređuje na prikupljanje obaveštenja o aktivnostima konkurencije da bi se pogodio njegov sledeći potez ili za rano otkrivanje novih tehnologija. Drugi razlozi uključuju

praćenje poslovnih poteza konkurencije vezenih za ugovore sa konkurencijom na tržištu.

Institucionalizacijom zaštite informacija koje objektivno predstavljaju tajnu, kroz njihovu klasifikaciju i donošenje određenih internih akata organizacije, samo se donekle rešava ovaj problem. Ako se i zaštite informacije koje su stepenovane kao tajna i sprovedu adekvatne mere zaštite dolazimo do novog pitanja: „Da li su samo podaci proglašeni poslovnom tajnom predmet industrijske špijunaže?“ Odgovor na postavljeno pitanje je da je to samo deo interesovanja industrijske špijunaže. Ostalo se odnosi na radne navike zaposlenih, njihovu stručnost, produktivnost, interpersonalne odnose u preduzeću, vrline i slabosti rukovodilaca, spisak dobavljača, klijenata, odnosno na sve one informacije koje mogu doprineti dolaženju do informacija koje su stepenovane, ili koje mogu konkurentskom preduzeću da pomognu da ostvari bolji i uspešniji položaj na tržištu ili da preuzme najznačajnije kadrove sa gotovim znanjima u koje je ulagano godinama mnogo novca.

S obzirom da svi ovi podaci ne mogu biti poslovna tajna, zakonom i nisu zaštićeni od neovlašćenog prikupljanja. Organizaciji ostaje da sama iznađe najbolje načine i metode zaštite od industrijske špijunaže, kako od onih oblika koji su zakonom sankcionisani, tako i od onih koji nisu, ali objektivno mogu naneti štetu.

### *3.3. Finansijski napadi*

Finansijski napadi se sprovode sa ciljem direktnog nezakonitog dolaženja do novca ili nekih drugih finansijskih vrednosti ili nekih usluga. Ovi napadi su najrasprostranjeniji tip kompjuterskog kriminala i s obzirom na to da je o njima mnogo pisano nećemo ih šire eleborirati.

### *3.4. Teroristički napadi*

Oslanjanje na kompjutere i informacione sisteme u svim sferama funkcionisanja društva čini ovu infrastrukturu sve više i više privlačnom za terorističke napade. Takvi napadi se suštinski razlikuju od vojnih i obaveštajnih napada jer je svrha terorističkog napada da širenjem straha kod šireg kruga ljudi nateraju vlast da promeni ponašanje u odnosu na teroriste i da na taj način ostvari političke ciljeve terorističkih organizacija. Kod vojnih i obaveštajnih napada cilj je samo dolaženje do poverljivih informacija. Prikupljanje početnih informacija neizostavno prethodi bilo kojoj vrsti terorističkog napada. Znači da su mete fizičkog terorističkog napada po pravilu prvo bile mete napada socijalnog inžinjeringa čiji je cilj bio dolaženje do početnih informacija. Ha-

lid Ibrahim (Khalid Ibrahim) član Pakistanske terorističke grupe Harkat-UlAnsar (Harkat-UlAnsar) je poznat po tome što koristi metode socijalnog inženjeringa kako bi došao do informacija koje mu omogućavaju neovlašćen ulaz u vojnu kompjutersku mrežu Sjedinjenih Američkih Država.[27]

Kao što je Dolan rekao: „U socijalnom inženjeringu sve je u tome da se koriste drugi da bi se sakupile informacije i na taj način ostvario napad". U periodu posle 11. septembra 2001, socijalni inženjering je deo dobro organizovanog sajber napada koji je usmeren tako da izazove paniku zajedno sa fizičkim napadom na kritičnu infrastrukturu i postrojenja, kao što su razne javne strukture i kompanije za snabdevanje vodom, energijom i druge.[28]

Moguće mete napada mogu biti sistemi koji kontrolišu rad sistema proizvodnje i distribucije električne energije, sistemi telekomunikacija i veza, zdravstveni sistemi, sistemi snabdevanja vodom, kao i ostali sistemi čijim nefunkcionisanjem bi bili izazvani strah i panika.

Čak i ako se ne sprovedu ovakvi destruktivni napadi ostaje problem koji se ogleda u tome da terorističke grupe iskorišćuju kompleksnost Interneta za prikupljanje sredstava i pranje novca, kao i razmenu informacija i koordiniranje napada.

### *3.5. Osvetnički napadi*

Osvetnički napadi se po pravilu sprovode na štetu neke organizacije vladinih agencija ili pojedinih osoba. Šteta se može ogledati u gubitku informacija, nemogućnosti njihove dalje obrade ili uništavanju ugleda određenih osoba. Motiv koji stoji iza ovih napada obično je osećaj ljutnje i besa i napadač bi mogao da bude sadašnji ili bivši zaposleni ili neko od konkurencije.

### *3.6. Napadi iz zabave*

Osnovni pokretački motiv ovog napada je lično zadovoljstvo i uzbuđenje ostvarivanjem upada u štićeni sistem. Ovi napadači po pravilu preuzimaju gotove programe sa Interneta koji im koriste u ovim napadima. Žrtve ovih napada uglavnom imaju problem pristupa svojim servisima i podacima. Iako napadač koji koristi ovu vrstu napada može da uništi po-

[27] Colarik, A,.M.: *Cyber Terrorism: Political and Economic Implications*, Hershey, PA, USA: Idea Group Publishing, 2006, str. 35.

[28] Janczewski, J. L.; Colarik, M. A.: *Cyber Warfare and Cyber Terrorism,* Information Science Reference, Hershey - New York, 2008, str. 183.

datke, njegov osnovni motiv je da kompromituje sistem zaštite, a samim tim i organizaciju koja ga je postavila, kao i da upad iskoristi za pokretanje napada na druge žrtve.

Klasifikacija pretnji usmerenih ka kompjuterima može se izvršiti i prema tome ko stoji iza napada i gde je usmeren napad. Napad može biti usmeren na makro planu gde je predmet napada država sa institucijama koje je predstavljaju i resursima koji su značajni za njeno funkcionisanje. Druga vrsta napada je pretnja usmerena ka mikro planu prema pojedinim privrednim društvima, kompanijama, bankama ili institucijama.

Interesantni su podaci navedeni u SAD, gde su proučavane i analizirane specifične vrste grupa ili organizacija koje bi mogle da izvrše napad na kritične infrastrukture države ili vladine kompjuterske mreže. Utvrđeno je da preko 100 zemalja ima tehnološke i informacione preduslove za ovu vrstu napada. Najmanje 20 zemalja ima SAD kao metu, a nekoliko njih je ima iste mogućnosti informacionih tehnologija i znanja kao i SAD.[29]

Po toj klasifikaciji kao pretnje su označene sledeće grupe:

- Nacionalne države (najređa pretnja, ali u slučaju ostvarenja mogućnost najveće štete),
- Teroristi,
- Špijuni, uključujući i korporativnu špijunažu,
- Organizovani kriminal,
- Insajderi[30] i
- Hakeri (najčešća pretnja, ali najmanja mogućnost za oštećenje).

Tehnike i alati koje koriste svih ovih šest grupa su obično iste, ali motivacije i namere uveliko variraju.[31] Iz tog razloga i kada se utvrdi napad, ne može se sa sigurnošću reći ko stoji iza njega dok se ne uhvati izvršilac, što je veoma često neizvodljivo. Ovo ukazuje na značaj shvatanja borbe protiv socijalnog inženjeringa koji se koristi kod svih pomenutih napada, jer se uglavnom ne zna ko stoji iza pretnje.

Hakeri predstavljaju stalnu pretnju usmerenu ka kompjuterskim sistemima. U početku motiv je bio proširivanje znanja i pokazivanje ranjivosti si-

---

[29] Parker, T.; Shaw, E.; Stroz, E.; Devost, G. M.; Sachs, H. M.: *Cyber Adversary Characterization: Auditing the Hacker Mind,* Syngress Publishing, Inc., Rockland, 2004, str. 220.

[30] Po ovoj klasifikaciji insajder je lice koje nije nužno zaposleno u pravnom entitetu koji je meta napada. U kontekstu ovih pretnji, insajderi su svi oni koji imaju pristup računarima i računarskim mrežama i imaju znanje o vrednosti informacija koje se nalaze u pravnom entitetu. Ovoj grupi pripada većina zaposlenih, ali takođe mogu da pripadaju i članovi porodice zaposlenih, poslovni partneri, kupci, dobavljači i u retkim slučajevima konkurencija.

[31] Parker, T.; Shaw, E.; Stroz, E.; Devost, G. M.; Sachs, H. M.: *Cyber Adversary Characterization: Auditing the Hacker Mind,* Syngress Publishing, Inc., Rockland, 2004, str. 221.

stema. U sledećoj fazi cilj je bio prikupljanje informacija, a u fazi u kojoj smo danas cilj je uglavnom neki oblik finansijske dobiti. Promena ciljeva takođe je značila promenu izvršioca. Rodžers je dao svoju klasifikaciju 2000. godine, a ona je dopunjena kod Vilsona (Tim Wilson) 2007. godine, gde on pisuje osam kategorija hakera.[32]

1. *Novajlija*: često nazvan i skript klinac. (script kiddies). Pripadnici ove grupe su mlađe osobe, ograničenih sposobnosti. Njihova primarna motivacija je potraga za uzbuđenjem i podizanje sopstvenog ega. U želji da dokažu svoje vrednosti upadom u sisteme, uglavnom koriste softver koji je neko drugi razvio.

2. *Sajber sledžija* (cyber punk): najbliži su tradicionalnom izgledu hakera. Mladi, obično muškog pola, sa određenim sposobnostima i znanjima u programiranju. Motiv im je, uglavnom, želja da skrenu pažnju na sebe, a ponekad i materijalna korist. Obično biraju visoko profilisane mete i obično se opredeljuju za vandalizam umesto krađe informacija.

3. *Interni* (internal): zaposleni koji koriste svoje interne mogućnosti pristupa informacijama, korišćenjem privilegija koje imaju. Mogu se klasifikovati u dve kategorije. U prvu ulaze oni koji su nezadovoljni iz bilo kog razloga i na ovaj način se svete i drugu oni koji imaju finansijski motiv.

4. *Mali lopov* (petty thief): klasični kriminalci koji u sklopu svoje kriminalne karijere pokušaju da ovladaju napadima na kompjuterske sisteme da bi proširili polje svog kriminalnog delovanja. U početku nisu dovoljno sposobni, ali vremenom postaju kvalifikovani. Osnovni motiv im je finansijska dobit.

5. *Stari čuvar* (old guard): Ova kategorija vidi hakerstvo kao mentalni izazov i veoma su radoznali. Često su vrlo sposobni i imaju potrebna znanja za pisanje kompjuterskih programa. Prihvataju ideologiju prve generacije hakera i obično nemaju kriminalne namere. Dele sa drugima svoje iskustvo, odnosno programe koje su razvili i napisali.

6. *Pisac virusa*: uglavnom mlađe osobe muškog pola, motivisani pre radoznalošću ili osvetom, nego ozlojeđenošću.

7. *Profesionalni kriminalac*: u ovu kategoriju se ubrajaju visoko obučeni IT stručnjaci koji koriste svoje veštine i znanja za sticanje finansijske dobiti. Oni nikada ne žele da skreću pažnju na sebe. Rade za organizovane kriminalne grupe.

8. *Informatički ratnik*: motivisani su patriotizmom, koriste svoje veštine da poremete sisteme „neprijateljskih zemalja". Obično su do-

[32] Wilson, T.: *Eight Faces of a Hacker*, 2007. http://www.darkreading.com/security/perimeter/showArticle.jhtml?pgno=1&articleID=208804443, preuzeto sa sajta 21.09.2010.

bro obučeni i visoko kvalifikovani po znanjima i veštinama kojima raspolažu.

Najčešća i najvidljivija pretnja za kompjutere i kompjuterske mreže povezane na internet je zlonamerna hakerska subkultura. Nažalost, administratori sistema i napredni korisnici kompjutera smatraju sebe članovima opšte hakerske scene. Zbog toga ih je teško razlikovati od onih koji imaju zle namere i onih koji to nemaju. Alatke koje koriste „beli šešir" (nezlonamerni), „crni šešir" (zlonamerni) identične su. Na primer, hakeri belih šešira koriste skenere ranjivosti da pronađu ili poprave bezbednosne rupe da bi sprečili neovlašćen pristup, dok hakeri crnih šešira koriste iste alatke da pronađu i iskoriste bezbednosne rupe da dobiju neovlašćen pristup.[33]

Sledeći korak u zaštiti od socijalnog inžinjeringa je identifikacija izvora pretnji, koje mogu da koriste socijalni inženjering kao način dolaženja do informacija i podataka i da na taj način ugroze bezbednost informacionih sistema. Dele se na *unutrašnje, spoljašnje, i kombinovane pretnje.*

*Unutrašnja pretnja* - insajderi predstavljaju lica koja su zaposlena u preduzeću, kompaniji i instituciji bez obzira na njihov radni status. Unutrašnja pretnja je pretnja koja ima izvor unutar kompanije, vladine agencije ili institucije i obično predstavlja nezadovoljnog zaposlenog koji nije unapređen ili je obavešten o otkazu. Napad socijalnim inženjeringom može da pokrene i napadač koji je tražio privremeno zaposlenje.[34]

Pretnje izazvane insajderom su ili namerne ili nenamerne, a unutar ove dve grupe one mogu (ali ne moraju uvek) biti destruktivne. Primer nenamerne i potencijalno destruktivne pretnje je kada zaposleni prosleđuje osetljivu elektronsku poštu na kućni nalog da bi radio na njoj. Normalno da ovi zaposleni ne izgledaju kao da mogu da naškode, ali im niko nije objasnio koliki je rizik po gubitak informacija koji oni stvaraju prosleđivanjem unutrašnje elektronske pošte sami sebi, putem javnog i nezaštićenog sistema, korišćenjem Interneta.

Nenamerne i potencijalno destruktivne pretnje insajdera uključuju zaposlene koji instaliraju neki softver na kompjuterima kompanije iako znaju da je to protivno politici kompanije.

Namerni i destruktivni insajder može biti, na primer, nezadovoljni administrator sistema koji briše važne podatke sa servera neposredno pre nego što prekine radni odnos.

---

[33] Parker, T.; Shaw, E.; Stroz, E.; Devost, G. M.; Sachs, H. M.: *Cyber Adversary Characterization: Auditing the Hacker Mind,* Syngress Publishing Inc., Rockland, 2004, str. 226.

[34] Schell, B.; Martin, C.: *Webster's New World Hacker Dictionary*, Wiley Publishing, Inc., Indianapolis, 2006, str. 169.

Nekoliko nedavnih istraživanja sajber kriminala ukazuje na insajdera kao pretnju broj jedan sa kojom se suočavaju organizacije koje koriste kompjutere i kompjuterske mreže. S obzirom na kompleksnost kompjuterskih mreža i obično mali broj osoblja koje daje podršku korisnicima, insajderi imaju mnogo mogućnosti da izazovu ozbiljna oštećenja. Zlonamerni insajderi jesu, a i ostaće, najveća pretnja za pouzdan rad kritičnih infrastruktura.[35]

*Spoljašnju pretnju* predstavljaju lica koja nemaju zasnovan radni status sa metom napada. Motivi koji pokreću spoljašnje pretnje su različiti i zavise od toga koji je razlog napada i prema čemu je usmeren. U ovu grupu možemo uključiti kategorije u koju se ubrajaju poslovni partneri, članovi porodice, kupci, dobavljači i konkurencija, kao i totalno nepoznata lica, sa kojima organizacija nije imala zvaničnih kontakata, ali zbog onoga čime raspolaže, predstavlja interesantnu metu napada.

Socijalni inženjering pomaže zlonamernim licima da dobiju unutrašnji pristup poverljivim podacima kod organizacija sa sofisticiranim tehničkim bezbednosnim sistemima. Pretvarajući se da su legitimno zaposlena ili da imaju ovlašćeni pristup, lica koja sprovode socijalni inženjering koriste ranjivost u ljudskim običajima i učtivosti prijateljskog pomaganja nekome ko ima neki problem očekujući za uzvrat isto tako ponašanje kada to njima zatreba. Ako su sposobni da ubede legitimnog zaposlenog neke organizacije da im se omogući fizički pristup kompjuterskim resursima ili pristup preko mreže, oni su tada podignuti na status insajdera, jer sada imaju dve ključne stvari - pristup i znanje.[36]

*Kombinovana pretnja* se ostvaruje zajedničkim i koordiniranim napadom na informacije, koju svesno i sa namerom sprovode lica koja su zaposlena u nekom pravnom entitetu, bez obzira na oblik pravno-radnog odnosa, zajedno sa licima koja nisu zaposlena. Po kategorizaciji stepena opasnosti može se reći da je ova pretnja najopasnija, s tim što, po dosadašnjim iskustvima, nije često ostvarivana.

## 4. Zaključak

Najslabija karika u sistemu obezbeđenja uvek su ljudi, a najlakši način da se prodre u zaštićeni sistem je planiranje upada koristeći se ljudima i njihovim slabostima. Tvrdnja da je jedino bezbedan kompjuter onaj koji je isključen iz izvora napajanja samo je delimično tačna.

---

[35] Parker, T.; Shaw, E.; Stroz, E.; Devost, G. M.; Sachs, H. M.: *Cyber Adversary Characterization: Auditing the Hacker Mind*, Syngress Publishing, Inc., Rockland, 2004, str. 225.

[36] Parker, T.; Shaw, E.; Stroz, E.; Devost, G. M.; Sachs, H. M.: *Cyber Adversary Characterization: Auditing the Hacker Mind,* Syngress Publishing, Inc., Rockland, 2004, str. 225.

Postojanje mogućnosti da nekog ubedite da ga uključi u izvor napajanja i potom aktivira operativni sistem, dovoljno govori o značaju socijalnog inženjeringa.

Socijalni inženjering je tehnika u kojoj se ubeđivanje i/ili obmana koriste da bi se dobio pristup kompjuterskim sistemima.

Ono što usložava protivmere u borbi protiv socijalnog inženjeringa je saznanje da svako ko ima pristup bilo kom delu informacionog sistema predstavlja potencijalni rizik po bezbednost informacija. Bilo koja informacija do koje se može doći predstavlja korak ka sledećoj informaciji i tako dok se ne stigne do one informacije koja je cilj napada. To ukazuje na činjenicu da i zaposleni koji se ne smatraju bezbednosno ugroženim i nisu uključeni u mere zaštite, mogu biti meta napada socijalnim inženjeringom.

Za razliku od ostalih napada na kompjutere, socijalni inženjering se ne odnosi na tehnološku manipulaciju i korišćenje ranjivosti hardvera ili softvera i pored toga ne zahteva posebne tehničke veštine i znanja. Ova vrsta napada eksploatiše ljudske slabosti, kao što su nemarnost ili želja za kooperativnošću, kako bi se dobio pristup legitimnim dokumentima koji se nalaze na kompjuteru.

Socijalni inženjering može biti sproveden zbog profita, sajber terorizma ili za pristup internim sistemima i poverljivim informacijama. Najčešće se napadaju velike organizacije koje obrađuju i skladište osetljive podatke, kao što su provajderi telekomunikacionih usluga, multinacionalne kompanije, finansijski ustanove, bolnice i vojska ili vladine ustanove ili agencije. Naravno, pored navedenih napad može biti usmeren i prema bilo kom preduzeću.

Lica koja sprovode socijalni inženjering su veoma inteligentne i izuzetno kreativne osobe. Poseduju dobre komunikacijske i manipulatorske veštine, dobri su poznavaoci psihologije i uglavnom imaju dovoljno tehničkog znanja. Mogu da nastupaju timski i samostalno, s tim što je timski napad mnogo opasniji jer udružuju svoja znanja i umeća poštujući se međusobno i uvažavajući hijerarhiju.

Iz tog razloga prihvatljivije je reći da su preduslovi predstavljeni kroz četiri kategorije ili faktora i to: 1) motiv, 2) spremnost, 3) mogućnost i 4) metod. Ukoliko jedan od četiri pomenuta faktora ne postoji, napad se neće desiti.

Kritične informatičke infrastrukture su ranjive na napade na mnogo načina uključujući i napade fizičkim pristupom i napade izvedene preko kompjuterske mreže. Međuzavisnost elemenata infrastrukture čine rizičnim sve elemente, tako da će uspešan napad na jedan deo sistema sigurno uticati na druge delove sistema koji nisu direktno napadnuti.

Tehnike i alati koji se koriste obično su isti, ali motivacije i namere uveliko variraju. Iz tog razloga i kada se utvrdi napad, ne može se sa sigurnošću reći ko stoji iza njega dok se ne uhvati izvršilac, što je veoma često neizvodljivo. Ovo ukazuje na značaj shvatanja borbe protiv socijalnog inženjeringa koji se koristi kod svih pomenutih napada, jer se uglavnom ne zna ko stoji iza pretnje.

Insajderi se navode kao pretnja broj jedan sa kojom se suočavaju organizacije koje koriste kompjutere i kompjuterske mreže. S obzirom na kompleksnost kompjuterskih mreža i obično mali broj osoblja koji daju podršku korisnicima, insajderi imaju mnogo mogućnosti za izazivanje ozbiljnih oštećenja. Zlonamerni insajderi jesu, a i ostaće, najveća pretnja za pouzdan rad kritičnih infrastruktura.

Socijalni inženjering pomaže zlonamernim licima da dobiju unutrašnji pristup poverljivim podacima kod organizacija sa sofisticiranim tehničkim bezbednosnim sistemima. Pretvarajući se da su legitimno zaposleni ili da imaju ovlašćeni pristup, lica koja sprovode socijalni inženjering koriste slabosti u kolegijalnim običajima i učtivosti. Sposobni su da lako ubede zaposlenog neke organizacije da im se omogući fizički pristup kompjuterskim resursima ili pristup preko mreže i tada imaju dve ključne stvari - pristup i znanje.

*Ljubomir Stajić, Ph.D., Full Professor*
*Faculty of Law Novi Sad*

*Goran Mandić, LL.M.,Instructor*
*Faculty of Security Studies University of Belgrade*

# Social Eengeneering as the Form of Endangering Confidential Business Information

***Abstract***

In many jobs, especially the ones where you need to get some confidential information in contact with other people, there are some forms of social engineering. Social engineering is the form of oral and gesture manipulation with individuals, aiming to impose them fulfill a kind of demands, made by the attacker.

The existing problems in the confidential information protection sphere appear in the fact that behind each computer, there is a human being, as an individual, with own good and bad characteristics. Social engineering is a technique where persuading and/or delusion are used for getting the access to the computer systems. This is usually accomplished by conversation or some other forms of interactive communication.

Countermeasures in fighting against social engineering are getting more complicated due to the fact that anyone who has the access to any part of the information system represents a potential risk to information security.

Unlike other attacks on computers, social engineering does not refer to technological manipulation or the use of hardware and software vulnerability. Besides that, it does not demand any special technical skills and knowledge. This kind of attack exploits human weaknesses, as negligence or cooperation wish, in order to get an access to the confidential documents existing in the computer.

Social engineering can be organized for the sake of profit and cyber terrorism or for the access to internal systems and confidential information. Big organizations that process and save sensitive data are the most often attacked and among them are telephone services providers, multinational companies, financial entities, hospitals, Government agencies, military service and others.

Key words: social engineering, information security, security systems, companies, hackers, computer crime.