CARNET

Uvod u socijalni inženjering

NCERT-PUBDOC-2017-11-349

CERT.hr

Sadržaj

Dokument je izradio Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

1 Uvod

U uvodu knjige *The art of deception: Controlling the human element of security*, autori Mitnick i Simon kažu:

> *„Neka tvrtka je možda kupila **najbolje sigurnosne tehnologije** koje novac može kupiti, obučila svoje ljude toliko dobro da **zaključavaju sve svoje tajne** prije vraćanja kući noću i unajmila zaštitare od najboljih sigurnosnih tvrtki.*
>
> *Ta tvrtka je i dalje **u potpunosti ranjiva**." (1)*

U području informacijske sigurnosti postoji velik fokus na to kako zaštititi računalne sustave ili kako fizički zaštititi organizaciju – no najslabija karika u lancu sigurnosti je često **ljudski faktor**.

Sljedeće dvije definicije daju dobar uvodni dojam o socijalnom inženjeringu:

*„dobivanje željenih informacija (primjerice lozinke) **od osobe** umjesto provaljivanja u sustav"* (2)

*„**socijalni/psihološki proces** kojim pojedinac može dobiti informacije od pojedinca o ciljanoj organizaciji"* (3)

Najjednostavnije rečeno, socijalni inženjering je prevara. Postupak kojim se metu nagovara da napadaču da informaciju ili učini nešto što ta osoba nikada ne bi napravila kada bi ju se otvoreno pitalo.

Na primjer, kad bi netko nazvao neku organizaciju i tražio broj privatnog mobitela gospodina Ivana Horvata, ne bi mu ga dali. Ali ako nazove i uzrujanim glasom kaže: „*Ovdje teta iz vrtića, sin gospodina Ivana Horvata je pao na glavu i sad ga vozimo u bolnicu, trebam broj njegovog mobitela da mu pošaljem sliku žile na vratu maleckog da nam kaže je li to od ranije ili je to sad nastalo*", u velikom broju slučajeva dobit će traženi broj.

Precizniji opis socijalnog inženjeringa bi bio korištenje **obmane** za **dobivanje** žrtvinih **informacija** ili **manipulaciju** žrtve da učini nešto.

Primjerice, socijalni inženjering često izgleda ovako:

- Zaposlenik neke velike tvrtke prima poziv: *„Bok, ovdje Ivan iz IT odjela – provjeravamo ispravnost nove nadogradnje sustava, trebamo provjeriti i Vaš korisnički račun – **koje je Vaše korisničko ime i lozinka**?"*.
- U pretinac elektroničke pošte stiže sljedeća poruka s dokumentom u prilogu (eng. *attachment*):
  „Poštovani,
  u prilogu se nalazi račun za prošli mjesec.
  *Molim Vas **otvorite račun** i pogledajte jesu li svi podaci ispravni.*
  Lijepi pozdrav,
  <tvrtka s kojom poslujete>"

- Ili se čak pojavljuje osoba u zgradi neke tvrtke: *„Dobar dan, ja sam iz <tvrtke za održavanje Vaše zgrade>, pozvali ste me da provjerim instalacije u sobi s poslužiteljima – molim Vas **otvorite mi vrata te sobe**."*

U sva tri slučaja, to nije bio ni Ivan iz IT odjela, ni partnerska tvrtka, ni osoba iz tvrtke za održavanje – već napadač. Ovi primjeri su pojednostavljeni i možda se na prvi pogled čini kako oni ne bi mogli uspjeti u stvarnom svijetu. No, upravo napadi slični navedenima uspješno se događaju svaki dan.

Ključno je razumjeti i što socijalni inženjering nije. Socijalni inženjering **nije** ucjena, ni fizička prijetnja, ni bilo kakav postupak u kojem je žrtva svjesna napada. Često je situacija upravo suprotna – nakon napada u kojem se koristio socijalni inženjering, žrtva zna biti toliko u zabludi da se osjeća sretno i zadovoljno jer misli kako je upravo pomogla nekome tko je zaista trebao pomoć ili kako je uspješno odradila svoj posao i slično.

Bitno je i upoznati se s ulogom i položajem socijalnog inženjeringa unutar područja informacijske sigurnosti. Socijalni inženjering razvijao se uz druge grane informacijske sigurnosti, često kao **alternativna (i lakša) metoda napada** ili kao pristup koji omogućava **nove, „hibridne" napade** koji kombiniraju tehnike socijalnog inženjerstva i drugih grana sigurnosti. Socijalni inženjeri često su **sigurnosni stručnjaci** s vještinama računalne sigurnosti, fizičke sigurnosti itd. kojima je socijalni inženjering zapravo samo jedan od alata za postizanje cilja.

2 Ciklus socijalnog inženjeringa

Kako bi potencijalne žrtve lakše uočile napad, Mitnick i Simon opisuju ciklus socijalnog inženjeringa (1). To su četiri faze kroz koje prolazi napad socijalnog inženjeringa:

1. Istraživanje
2. Razvijanje odnosa i povjerenja
3. Iskorištavanje povjerenja
4. Korištenje informacija

Osim lakšeg prepoznavanja napada, taj ciklus koristan je i za konkretnije upoznavanje s temom socijalnog inženjeringa.

2.1 Istraživanje

Kao i kod ostalih grana sigurnosti, i napadima koji se služe socijalnim inženjeringom prethodi faza istraživanja. Podaci prikupljeni u ovoj fazi olakšavaju izvođenje napada u narednim fazama.

Tehnike koje socijalni inženjeri koriste za istraživanje su iste tehnike koje se koriste i u drugim granama sigurnosti. Od konkretnih tehnika, to su obično:

- Korištenje javno dostupnih informacija (OSINT)
- Pretraga otpada (eng. *dumpster diving*)
- Gledanje preko ramena (eng. *shoulder surfing*)

Bitno je napomenuti u ovom kontekstu kako je u napadima u kojima se koristi socijalni inženjering gotovo svaka informacija korisna – npr. imena ljudi naizgled nepovezanih s metom ili žrtvom napada, informacije o relevantnim tvrtkama i novostima, čak i žargon koji se koristi u neslužbenoj komunikaciji u kontekstu mete. Sve te informacije imaju značaj u stvaranju uspješne obmane.

Korištenje javno dostupnih informacija ili **OSINT** (od eng. ***O**pen **S**ource*[1] ***INT**elligence*) je gotovo uvijek jedan od glavnih način prikupljanja informacija u informacijskoj sigurnosti. To nije ništa drugo nego prikupljanje podataka dostupnih na Web stranicama, mrežnim servisima općenito (WHOIS, DNS), u novinskim člancima, bilo kakvim javnim izvještajima, telefonskim imenicima i slično. Na taj način moguće je prikupiti mnogo informacija koje obično nisu povjerljive, ali mogu biti korisne.

[1] OSINT nije povezano sa softverom otvorenog koda, tj. eng. *open source software*

Tehnike pretrage otpada (eng. *dumpster diving*) i gledanja preko ramena (eng. *shoulder surfing*) znaju biti opisane kao tehnike socijalnog inženjeringa upravo zato jer ih socijalni inženjeri često koriste. No one su zapravo samo općenite tehnike istraživanja koje između ostalog koriste i socijalni inženjeri – to nisu konkretne tehnike socijalnog inženjeringa jer ne uključuju nikakvu obmanu.

Pretraga otpada (eng. ***dumpster diving***) je tehnika pretraživanja metinog otpada/smeća (osobe ili organizacije) kako bi se pronašle korisne i povjerljive informacije. Žrtve često zaboravljaju ili ne shvaćaju važnost ispravnog **uništavanja podataka** prije odlaganja – uništavanja papira (eng. *paper shredding*), sigurnog brisanja podataka s digitalnih medija i slično. Upravo zbog toga na ovaj je način moguće pronaći razne dokumente, bilješke, medije za pohranu podataka i slično koji sadrže ne samo korisne, već i **povjerljive** informacije.

„Surfanje preko ramena" (eng. ***shoulder surfing***) je točno to: stajanje iza osobe i gledanje dok ona upisuje primjerice lozinku ili PIN. Iako na prvi pogled ova tehnika zvuči banalno, to je stvarna prijetnja i socijalni inženjeri upravo tako često znaju doći do informacija. Cilj ne mora nužno biti lozinka ili PIN – napadač na ovaj način može dobiti razne korisne informacije. Primjerice, napadač može promatrati dok žrtva čita povjerljivi izvještaj ili elektroničku poštu na svom pametnom telefonu, tabletu ili laptopu u javnosti. Isto vrijedi i za čitanje tiskanih dokumenata. Slika 1 prikazuje kako gledanje preko ramena u javnosti može izgledati.

Slika 1 - Primjer gledanja preko ramena u javnosti (izvor)

2.2 Razvijanje odnosa i povjerenja

Srž napada socijalnog inženjeringa je upravo ova faza. U njoj je cilj napadača razviti odnos sa žrtvom i dobiti njeno povjerenje koje je kasnije moguće iskoristiti.

U sklopu ove faze, napadač stvara izmišljenu, ali uvjerljivu priču (eng. *pretext*) koju zatim koristi za **obmanu**. Priča obično uključuje lažni identitet napadača, razlog zašto stupa u kontakt sa žrtvom i brojne druge detalje koji čine tu priču uvjerljivijom i opravdavaju kasnije

zahtjeve. Napadač u ovom trenutku koristi brojne informacije prikupljene iz faze istraživanja kako bi priča bila što uvjerljivija.

Ovu fazu najlakše je razumjeti kroz primjer. Pretpostavimo da je situacija sljedeća – napadač želi dobiti korisničko ime i lozinku Marka koji radi u odjelu marketinga neke velike tvrtke. Napadač je u fazi istraživanja saznao da u IT odjelu tvrtke radi Ivan i da je tvrtka nedavno imala probleme s vezom na Internet. Naoružan tim informacijama, napadač zove Marka:

*„Bok, ovdje **Ivan iz IT odjela** – pokušavamo otkloniti **probleme s vezom na Internet**.*

Koliko vidim, danas od 10:30 ujutro ti Internet veza opet sporije radi? […]

Imaš li možda i nekih drugih problema s računalom – otvara li računalo sporo programe? […]"

Kroz ovakav razgovor napadač postepeno gradi odnos i razvija povjerenje, a zbog prikupljenih informacija njegova lažna priča zvuči uvjerljivo. Jednom kada napadač razvije odnos do te razine da mu žrtva vjeruje, najteži dio napada je gotov.

2.3 Iskorištavanje povjerenja

Jednom kada je povjerenje razvijeno i time najzahtjevniji dio procesa gotov, slijedi iskorištavanje tog povjerenja za postizanje cilja. Napadač u pravilu to postiže postavljanjem pitanja ili zahtjevom da žrtva nešto učini.

U kontekstu primjera iz prošle faze u kojemu napadač glumi Ivana iz IT odjela, to može izgledati ovako – napadač nastavlja razgovor u pozivu:

„Potrebno je promijeniti postavke tvog korisnika da riješimo problem – vidiš li u postavkama opciju „isprazni DNS spremnik"? […]

*Nema je? Kod tebe je vjerojatno i dalje instalirana stara verzija programa, mogu ti ja to promijeniti – **koje je tvoje korisničko ime i lozinka**?"*

Cilj je da napad u ovom trenutku uspije na temelju uvjerljive lažne priče i izgrađenog odnosa i povjerenja. Ovisno o konkretnom napadu, on se može oslanjati na zahvalnost žrtve, na njenoj želji za pomoć drugima, strahu, osjećaju krivnje i sličnome.

2.4 Korištenje informacija

U posljednjoj fazi napadač treba iskoristiti informacije do kojih je došao u prethodnoj fazi. Rezultat prethodne faze su često korisnička imena i lozinke, razne tajne i ostale povjerljive informacije – to su informacije s kojima napadač može izravno postići cilj ili su to čak ciljevi sami po sebi.

Ponekad je ova faza, ali i cijeli njen ciklus, samo jedan dio većeg procesa. Radnja koju je žrtva učinila može otvoriti vrata daljnjim napadima ili informacije koje su dobivene mogu biti materijal za prvu fazu (istraživanje) u sljedećem ciklusu.

Primjerice, ako je rezultat jednog ciklusa napada informacija o tome kako se zove direktor tvrtke i kada je na službenom putu, to može omogućiti sljedeći napad. U njemu bi napadač mogao za vrijeme tog službenog puta nazvati tvrtku i lažno se predstaviti kao direktor koji zove s puta te zatim tražiti žrtvu da učini nešto ili preda neke povjerljive informacije.

3 Pregled tehnika socijalnog inženjeringa

Socijalni inženjeri koriste brojne tehnike u svojim napadima – bitno je razlikovati konkretne tehnike socijalnog inženjeringa od općenitih tehnika koje koriste i drugi, a koje, pored ostalih tehnika, koriste i socijalni inženjeri.

Općenite tehnike koje koriste i socijalni inženjeri su u pravilu sve tehnike vezane za pasivno prikupljanje informacija (korištenje javno dostupnih informacija, pretraga otpada, „surfanje preko ramena"…) i tehnike napada ostalih grana sigurnosti (iskorištavanje ranjivosti računalnih sustava, korištenje zlonamjernog softvera, obijanje brava, svladavanje protuprovalnih sustava…). Kao što je spomenuto u uvodu, socijalni inženjeri su često sigurnosni stručnjaci s raznolikim vještinama, tako da im navedene tehnike nisu strane u postizanju cilja.

Za razliku od tih tehnika, **tehnike socijalnog inženjeringa** su zapravo **tehnike obmane** – one omogućuju stvaranje uvjerljive lažne priče i razvijanje odnosa i povjerenja koje je zatim moguće iskoristiti. No, kako se socijalni inženjering razvijao uz bok drugim granama informacije sigurnosti, i te tehnike znaju biti usko povezane, ako ne i neodvojive od tehnika napada na računalne sustave, fizičku sigurnost i sl.

S obzirom na to da se socijalni inženjering u suštini svodi na prevaru ljudi, nije moguće jednostavno nabrojiti sve tehnike – postoji ih previše, i kako se ljudska psihologija i socijalna dinamika mijenja, tako se mijenjaju postojeće tehnike, ali se stvaraju i nove. Primjerice, ljudi danas na društvenim mrežama otkrivaju osobne podatke koje ranije nikad ne bi nikome dali, barem ne u pisanom obliku. Ono što je moguće je popisivanje i opisivanje najčešće korištenih tehnika i njihovih zajedničkih elemenata. Ovo poglavlje daje upravo takav pregled tehnika socijalnog inženjeringa.

Još je bitno napomenuti da se tehnike socijalnog inženjeringa, u pravilu, velikim dijelom oslanjaju na poznavanje psihologije. Međutim, ovaj dokument neće detaljnije istraživati i opisivati tu perspektivu, već će se, što se psihologije tiče, zadržati na laičkoj razini.

3.1 Lažni identitet

Lažni identitet često je **temelj obmane** u napadu socijalnog inženjeringa. Primjerice, ako je žrtva zaposlenik i vjeruje da razgovara sa svojim šefom, zašto mu ne bi dao sve informacije koje on traži? Uspješno uspostavljanje lažnog identiteta nerijetko može biti sve što je potrebno za obmanu.

No, lažni identitet nije uvijek dovoljan, primjerice – što ako je žrtva šef, a napadač lažni zaposlenikkojemu je cilj saznati šefovo korisničko ime i lozinku? U takvim slučajevima socijalni inženjer velikim se dijelom oslanja na ostatak lažne priče, no i dalje je lažni identitet bitan prvi korak.

Lažiranje identiteta, tj. lažno predstavljanje razlikuje se ovisno o metodi komunikacije sa žrtvom. Napadač sa žrtvom može komunicirati na gotovo sve načine, primjerice:

- Elektroničkom komunikacijom (u tom slučaju napad se naziva eng. *phishing*)

    - Elektronička pošta
    - Društvene mreže
    - *Instant messaging/chat* aplikacije
- Telefonskim pozivima
- Uživo (licem u lice)
    - Primjerice, napadač se predstavi kao lažni dostavljač, majstor, inspekcija…
- SMS-om
- Telefaks-om
- Poštom

Iznenađujuće, ono što je zajedničko gotovo svim načinima je mogućnost **lažiranja izvora komunikacije**. Konkretno, moguće je:

- Lažirati telefonski broj s kojega dolazi poziv, SMS ili telefaks
- Lažirati pošiljatelja elektroničke pošte
- Lažirati povratnu adresu na pismu ili paketu koji se šalje poštom

Ti postupci razlikuju se prema tehničkoj zahtjevnosti, ali u svakom slučaju izvedivi su i socijalni inženjeri ih koriste.

Jedine situacije u kojima je nepraktično lažirati identitet proizvoljne osobe su su one u kojima se napadač nalazi licem u lice sa žrtvom – no čak i tada, napadač je samo ograničen na lažne identitete koje žrtva ne poznaje.

Pogotovo u takvim situacijama, socijalni inženjeri mogu koristiti lažiranje identifikacijskih dokumenata, kartica, znački i slično. Te tehnike mogu izlaziti iz domene socijalnog inženjeringa, ali za jedan dio njih nisu uopće potrebne nikakve posebne vještine. Primjerice, lažnu posjetnicu ili „vizitku“ (eng. *business card*) nije teško izraditi, a za toliko malo napora značajno se diže vjerodostojnost lažnog identiteta.

Ipak, socijalni inženjeri, u pravilu, jako izbjegavaju kontakt u živo, licem u lice. S obzirom na obilje elektroničkih komunikacija koje danas svakodnevno koristimo, kontakt uživo im gotovo nikad ne treba.

3.2 Povećanje uvjerljivosti lažne priče

Kao što je prethodno navedeno, napad socijalnog inženjeringa oslanja se na uvjerljivu lažnu priču.

Velik dio tehnika za podizanje uvjerljivosti lažne priče svodi se na korištenje ispravnih relevantnih informacija. Te informacije mogu se koristiti na dva načina – kada žrtva od napadača traži informacije i kada se napadač samostalno referira na njih.

Prvi slučaj odnosi se na situacije u kojima socijalni inženjer želi biti spreman na pitanja kojima se provjerava njegov lažni identitet, tvrdnje koje je iznio u lažnoj priči i slično. Primjerice, napadač zove sjedište tvrtke koju napada i lažno se predstavlja kao menadžer jedne od brojnih poslovnica te tvrtke. U tom razgovoru, ako ga osoba s druge strane telefonske linije pita, napadač želi spremno odgovoriti s ispravnim imenom i prezimenom menadžera (njegovog lažnog identiteta), ispravnim podacima o poslovnici (adresa, identifikacijski broj poslovnice…) i ostalim informacijama koje bi trebao znati.

U drugom slučaju, napadač spominje relevantne informacije i kada ih žrtva nije tražila. **Spominjanje imena** (eng. *name-dropping*) jedna je od poznatijih takvih tehnika. Primjerice, ako napadač kroz istraživanje sazna da se direktor tvrtke koju napada zove Ivan Horvat, onda u telefonskom pozivu jednom od zaposlenika može reći „[…] što prije mi trebaju financijski podaci od prošlog mjeseca – g. Horvat će biti jako ljut ako ne uspijem sastaviti izvještaj do kraja tjedna."

Korištenje relevantnog žargona još je jedna tehnika koja pripada ovoj kategoriji. Npr. ako napadač napada organizaciju u financijskom sektoru, služenje žargonom koji se u tom kontekstu koristi može puno pomoći u uspostavljanju uvjerljive priče. Također, postoje situacije u kojima neka organizacija ima svoj interni žargon – poznavanje i korištenje tog žargona u komunikaciji može napadaču biti od velike koristi. Tu je riječ o nazivima procedura, opremi, računalnim aplikacijama, nazivima lokacija na kojima organizacija posluje, odjelima ili osobama.

Osim navedenog, moguće je koristiti i bilo koje druge relevantne informacije. Ovisno o situaciji, spominjanje konkretnih informacija kao što su identifikacijski brojevi, adrese, tipovi i modeli uređaja koji se koriste i slično može značajno podići razinu uvjerljivosti.

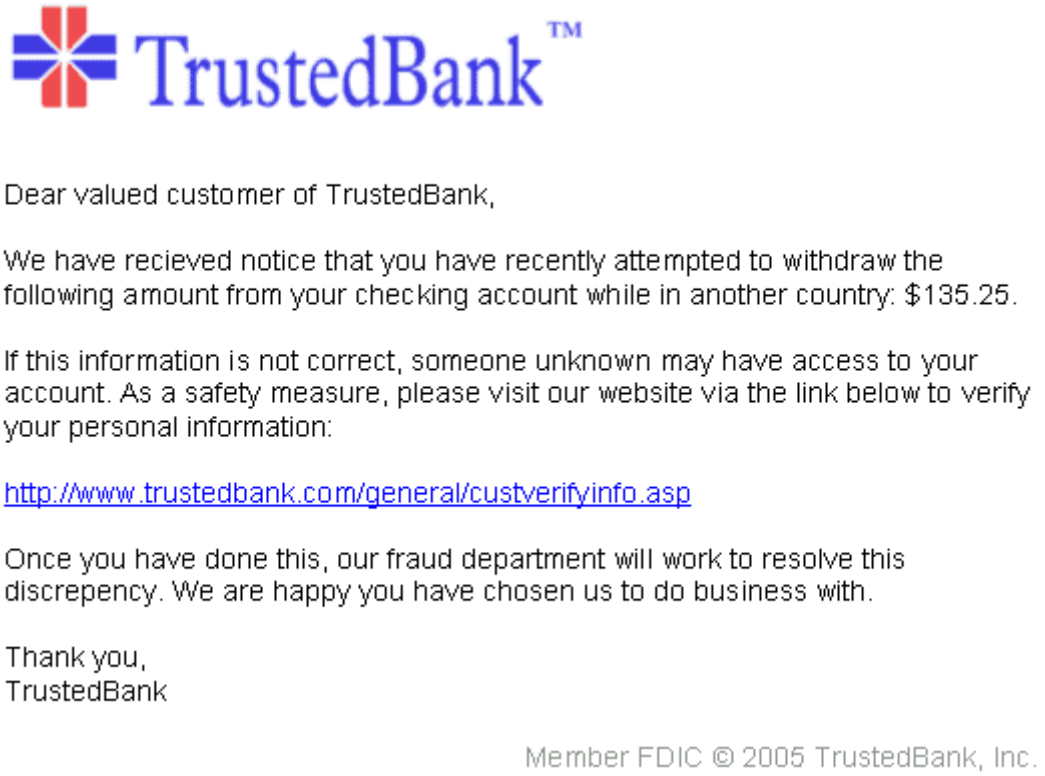
Jedan način za podizanje uvjerljivosti priče na visoku razinu je stvaranje situacije u kojoj **žrtva uspostavi kontakt s napadačem**. Primjerice, napadač pošalje žrtvi poruku elektroničkom poštom koja kaže „Novi broj tehničke podrške je <*napadačev broj*>". Zatim, napadač izazove tehničke probleme kod žrtve (npr. uspori ili onemogući joj vezu na Internet). Konačno, žrtva zove napadača (misleći da zove novi broj tehničke podrške) i traži pomoć. U ovakvoj situaciji, žrtva je naizgled inicirala komunikaciju – zašto bi sumnjala u priču i identitet napadača? Ova tehnika se još zove „reverzni socijalni inženjering".

Također, obećanje nagrade može podići vjerodostojnost priče i učiniti žrtvu manje opreznom. To je, primjerice, moguće napraviti u lažnim pričama u kojima napadač traži žrtvu da ispuni anketu/upitnik koji u nekom od pitanja traži povjerljive informacije. U takvim situacijama napadač može žrtvi ponuditi čokoladicu, kemijsku olovku, bon za dućan i slično u zamjenu za ispunjavanje upitnika. U istraživanju iz 2003. god. (4) koje je provjeravalo efikasnost ovakvog napada, 90% ispitanih uredskih radnika otkrilo je svoju lozinku u upitniku u zamjenu za jeftinu kemijsku olovku.

3.3 Phishing

Socijalni inženjering kroz elektroničku komunikaciju naziva se eng. *phishing* (od engleske riječi za pecanje – *fishing*) i jedan je od najčešćih oblika socijalnog inženjeringa danas. *Phishing* u suštini nije ništa novo što nije do sada objašnjeno u ovom dokumentu, no zaslužuje vlastiti odjeljak zbog sveprisutnosti elektroničke komunikacije u današnjem svijetu i zbog posebno učinkovite vrste *phishing* napada zvane *spear phishing*.

Općenito, *phishing* je napad u kojem se u komunikaciji putem elektroničke pošte, društvenih mreža, instant messaging/chat aplikacija koristi socijalni inženjering. Većina ljudi susrela se s pokušajima *phishing* napada putem elektroničke pošte u koje je uložen minimalan trud . Poruke iz takvih napada često smatramo običnim *spam* porukama. Primjer *phishinga* kroz elektroničku poštu prikazan je na slici 2.



Slika 2 - Primjer *phshing* napada kroz elektroničku poštu

Zbog takvih, gotovo bezopasnih pokušaja, ne smije se zanemariti opasnost od *spear phishing* napada. *Spear phishing* (od eng. *spearfishing* – pecanje kopljem) ciljani je *phishing* napad koji je izuzetno dobro prilagođen meti. Drugim riječima, to je *phishing* napad s uvjerljivom i dobro razrađenom lažnom pričom koja je relevantna u kontekstu mete.

Jedan primjer stvarnog *spear phishing* napada je poruka elektroničke pošte kojom kandidat za posao šalje svoj životopis i prijavljuje se za otvoreno radno mjesto u tvrtki. Prirodno je da će netko u tvrtki otvoriti tu poruku – na kraju krajeva, traže novog zaposlenika za to radno mjesto, redovito primaju takve poruke i ovo se čini kao da bi mogao biti odličan budući zaposlenik. Ovog puta, životopis koji se nalazio u prilogu potajno je izvršio zlonamjeran kod prilikom otvaranja i preuzeo kontrolu nad računalom.

Koliko je opasan *spear phishing* pokazuje i činjenica da je to jedna od najčešće korištenih tehnika naprednih napadača (eng. *advanced persistent threat*) (5) upravo zbog toga što je često uspješna, čak i kada se cilja metu s visokom mjerom zaštite i opreznosti.

3.4 Indirektne tehnike

Nije u svim napadima socijalnog inženjeringa potreban izravan kontakt (izravna elektronička komunikacija) između napadača i žrtve. Postoje i tehnike neizravnih napada koje su posebno korisne kada je žrtva oprezna, sumnjičava te čak i kada očekuje napad. U takvim situacijama su te tehnike uspješnije od uobičajenih tehnika jer iz perspektive žrtve praktički ni ne postoji potencijalni napadač koji bi izazvao sumnju.

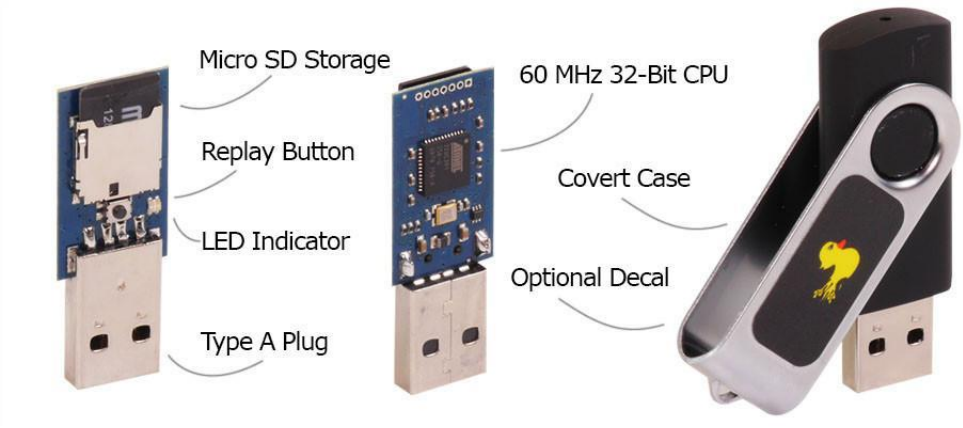
Vjerojatno najpoznatiji takav napad je ostavljanje naizgled bezopasnog uređaja (eng. *baiting*) gdje će ga žrtva pronaći, u nadi da će ga kasnije priključiti na svoje računalo. Jednom kada žrtva priključi taj uređaj na svoje računalo, napadač preuzima kontrolu nad njim.

U ovakvom napadu, uređaj može gotovo bilo što:

- Medij za pohranu podataka (CD, DVD, USB *stick*…)
- Bilo kakav uređaj sa USB priključkom (pametni telefon, slušalice…)
- Čak i uređaj kao što je grafička kartica (npr. zapakirana u naizgled originalno pakiranje)

S tehničke strane, postoje brojni načini da napadač preuzme kontrolu nad računalom jednom kada se taj uređaj priključi. Ti načini će biti opisani kasnije (3.5.4 „Hardverska strana socijalnog inženjeringa"), no bitno je znati da tehnološka složenost takvih napada pada iz dana u dan tako da oni postaju sve veća prijetnja. Danas je potrebno iznimno malo tehničkog znanja i ostalih resursa za izvedbu takvih napada jer je moguće kupiti relativno jeftine proizvode koji obavljaju sav tehnički dio napada.

Jedan poznati primjer takvog proizvoda je USB *Rubber Ducky* (6), prikazan na slici 3. To je uređaj koji izgleda kao memorijski USB *stick* koji se, jednom kada je priključen u računalo, predstavlja kao tipkovnica i „tipka" ono što je napadač zapisao u njega. Pri tome korisnikovo računalo „misli" da to tipka njegov korisnik koji se uredno prijavio za rad svojim korisničkim imenom i lozinkom. Istovremeno legitimni korisnik može raditi svoj posao i nije ni svjestan paralelne aktivnosti koja se događa: napada i preuzimanja kontrole nad računalom.



Slika 3 - USB *Rubber Ducky* (6)

Druga tehnika u ovoj kategoriji je tzv. „napad na pojilište“ (eng. *watering hole attack*). Neobično ime napada dolazi od prirodne pojave gdje grabežljivci napadaju svoj plijen oko njegovog pojilišta (mjesta gdje taj plijen dolazi piti vodu). U takvom napadu, napadač ne pokušava izravno napasti žrtvu, već prati koje Web stranice (i općenito usluge) žrtva koristi i traži priliku za napad na njih. Jednom kada njih uspješno napadne, posredno preko njih napada i korisnika.

Primjerice, napadač zna da zaposlenici organizacije koju napada čitaju vijesti s Web stranice http://www.example.com/. Zatim napada tu Web stranicu, preuzima kontrolu nad njom i modificira ju kako bi prikupljala informacije o posjetiteljima te ih inficirala. Ovakav napad često nije očekivan – „Zašto bi Web stranica s vijestima napala organizaciju?“ Također, otkrivanje napada je otežano – „Kakve veze bi Web stranica s vijestima mogla imati s ovim napadom?“ Čak i da postoji sumnja, žrtva u pravilu nema dovoljan pristup poslužitelju Web stranice kako bi dalje mogla istražiti napad.

I ovaj napad ima značajnu tehničku stranu – napadač mora na neki način dobiti (potpunu ili djelomičnu) kontrolu nad Web stranicom kako bi zatim napao i korisnike. Nešto više o tome piše kasnije u ovom poglavlju u odjeljku 3.5.1 „Socijalni inženjering na Webu“.

3.5 Socijalni inženjering i računalna sigurnost

Postoje brojne tehnike koje su velikim dijelom i dio socijalnog inženjeringa i računalne sigurnosti. Drugim riječima, brojni napadi imaju i socijalnu/psihološku i tehničku komponentu te ih nije uvijek moguće u potpunosti odvojiti.

U ovom su poglavlju ukratko opisane takve tehnike prema sljedećim kategorijama:

- Socijalni inženjering na Webu
- Socijalni inženjering i bežične mreže
- Socijalni inženjering i zlonamjerni softver (eng. *malware*)
- Hardverska strana socijalnog inženjeringa

S obzirom na to da je svaka od tih kategorija dovoljno velika za zasebnu temu, ovaj dokument neće ulaziti u detalje već će samo dati kratak pregled.

3.5.1 Socijalni inženjering na Webu

Socijalni inženjeri često iskorištavaju postojeće korisnikovo povjerenje prema Web stranicama koje koristi. To u pravilu rade na dva načina:

- Navođenjem korisnika na lažnu verziju Web stranice
- Napadanjem Web stranice kojoj korisnik vjeruje

Prilikom izrade lažne verzije postojeće Web stranice, socijalni inženjer brine da:

- Lažna stranica izgledom imitira originalnu Web stranicu
- URL (eng. *Universal Resource Locator* = mrežna adresa, hiperveza, *link*) lažne stranice izgleda što sličnije pravom URL-u

Napadi na postojeće Web stranice variraju prema složenosti, no jedna ranjivost koja je u isto vrijeme izrazito česta na Webu i korisna socijalnim inženjerima je eng. *Cross-site scripting* (XSS).

Osim iskorištavanja povjerenja koje korisnik ima prema postojećim Web stranicama, socijalni inženjer često u procesu napada navodi korisnika i na svoju Web stranicu koju je stvorio u kontekstu lažne priče.

U svim navedenim slučajevima, u nekom trenutku korisnik će otvoriti Web stranicu koju napadač djelomično ili u potpunosti kontrolira. Tada napadač na raspolaganju ima cijeli spektar tehnika ovisno o tome što mu je krajnji cilj. Te tehnike uključuju eng. *Cross-site request* forgery (CSRF), eng. *tabnabbing*, eng. *clickjacking*, iskorištavanje ranjivosti Web preglednika, prikupljanje informacija kroz JavaScript itd.

3.5.2 Socijalni inženjering i bežične mreže

Krajnji korisnici često nisu svijesni opasnosti spajanja na napadačevu Wi-Fi pristupnu točku (eng. *Wi-Fi access point*). Socijalni inženjeri to često iskorištavaju:

- Stvaranjem lažne pristupne točke (eng. *evil twin acess point/rogue access point*) koja glumi neku legitimnu za koju napadač zna da ju njegova meta koristi
- Pružanjem „besplatne veze na Internet"

Žrtvin uređaj automatski će se pokušati spojiti na napadačevu lažnu pristupnu točku ako ona ima isti naziv (tj. ESSID) kao i originalna pristupna točka na koju se korisnik inače spaja. Ovisno o konfiguraciji mreže, napadač može pokušati otkriti žrtvino korisničko ime i lozinku s kojima se spaja, a ako spajanje bude uspješno može i čitati i izmjenjivati sav nezaštićeni korisnikov mrežni promet.

Alternativno, socijalni inženjeri znaju i stvarati pristupne točke s otvorenim pristupom koje se oglašavaju kao „Besplatna veza na Internet“ ili slično. Žrtve se često spajaju na takve mreže ako nemaju pristup Internetu na svom uređaju ili ako imaju ograničenu količinu mrežnog prometa. Kada se žrtva spoji, napadač može čitati i izmjenjivati sav nezaštićeni korisnikov mrežni promet.

Uz Wi-Fi, socijalni inženjeri koriste i napade povezane s bežičnim povezivanjem Bluetooth protokolom. Postoji cijela klasa napada vezanih za Bluetooth i socijalni inženjering od kojih najozbiljniji napadi i omogućuju potpuno preuzimanje kontrole nad žrtvinim uređajem (često telefonom).

3.5.3 Socijalni inženjering i zlonamjerni softver (eng. *malware*)

Spoj socijalnog inženjeringa i zlonamjernog softvera (eng. *malware*) su trojanski konji – programi koji se korisniku predstavljaju kao uobičajeni, bezopasni alati, no u pozadini izvršavaju zlonamjeran kod.

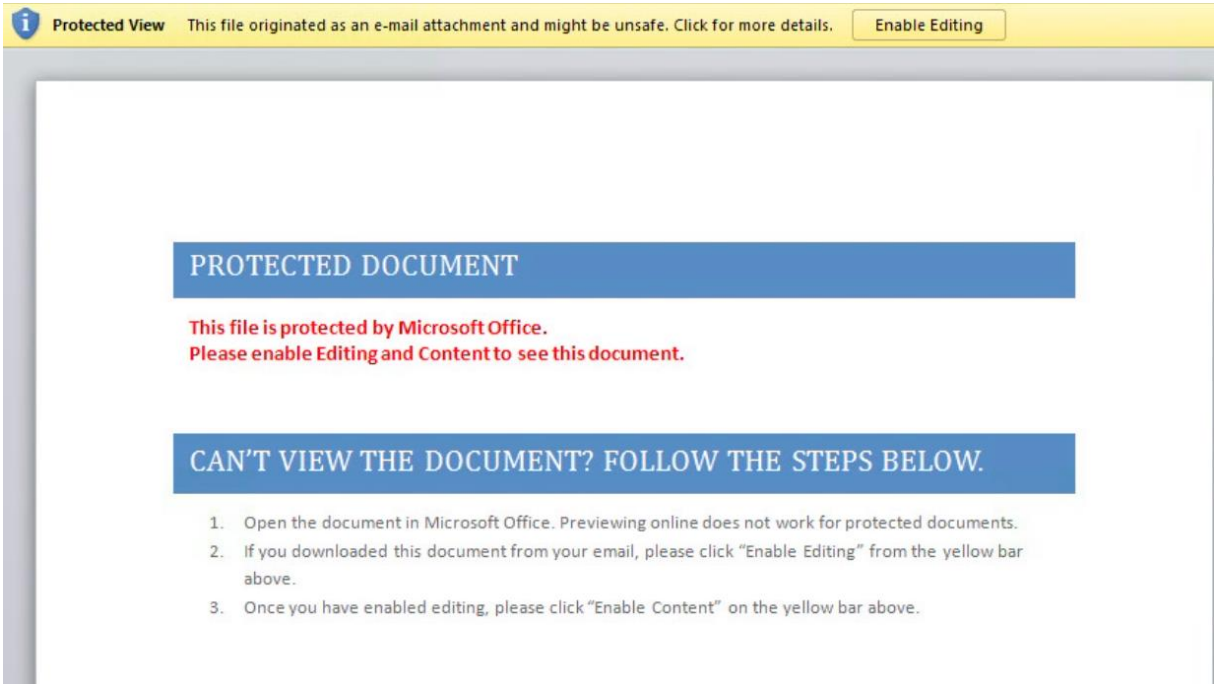
Socijalni inženjering se u takvom napadu pojavljuje na dva načina:

- Navodi korisnika da preuzme i pokrene trojanskog konja
- Zavarava korisnika da je taj program bezopasan i tako sakriva činjenicu da se događa napad

S tehničke strane, trojanski konji se najčešće pojavljuju kao jedna od dvije vrste datoteka:

- Izvršne datoteke (obično s *.exe* nastavkom)
    - S takvim datotekama su korisnici posebno oprezni, tako da je obično potrebno dobro opravdanje da žrtva preuzme i pokrene izvršnu datoteku.
- Dokumenti (datoteke s *.docx*, *.pdf* i sličnim nastavcima)
    - Žrtve često ne znaju da dokumenti mogu sadržavati kod koji se izvršava – uključujući i zlonamjerni kod. No, u većini slučajeva taj kod se izvršava tek nakon korisničke interakcije (primjerice nakon klika na „Omogući uređivanje“) te u tom slučaju napadač treba uvjeriti, opravdati, korisnika da to učini.

Slika 4 prikazuje kako izgleda jedna varijanta *Dridex* trojanskoj konja kada ga korisnik otvori. To je na prvi pogled samo nekakav zaštićeni Microsoft Word dokument. Upute („*This file is protected […] please Enable Editing*“) izgledaju kao da su dio alata Microsoft Word, ali zapravo ih je napadač napisao. Cilj napadača je da korisnik pročita upute i klikne gumb „*Enable Editing*“ („Omogući uređivanje“) čime će se zlonamjerni kod unutar dokumenta izvršiti.



Slika 4 – Jedna varijanta *Dridex* trojanskog konja – socijalnim inženjeringom pokušava se navesti korisnika da onemogući zaštitu i time dopusti izvršavanje zlonamjernog koda (izvor)

3.5.4 Hardverska strana socijalnog inženjeringa

Socijalni inženjeri se u napadima često znaju koristiti i raznim uređajima.

Prethodno je bio spomenut napad u kojem socijalni inženjer ostavi medij za pohranu podataka (CD, DVD, USB *stick*…) ili neki drugi uređaj (npr. USB slušalice) na mjestu gdje će ga žrtva pronaći i u konačnici priključiti na svoje računalo.

Postoji više načina koji su značajno različiti s tehničke strane pomoću kojih napadač preko uređaja preuzima kontrolu nad računalom:

- *Autoplay* funkcionalnost
    - Za CD, DVD, Blu-ray i slične uređaje često je uključena *autoplay* funkcionalnost koja omogućuje automatsko pokretanje programa koji u slučaju napada mogu biti napadačevi zlonamjerni programi.
    - Za USB *stickove* i slične medije, *autoplay* funkcionalnost obično je isključena upravo zbog sigurnosnih razloga pa socijalni inženjeri koriste ostale metode.
- Trojanski konj pohranjen na uređaju
    - Moguće je jednostavno pohraniti trojanskog konja na uređaj i osloniti se na to da će ga korisnik otvoriti.
- Iskorištavanje ranjivosti

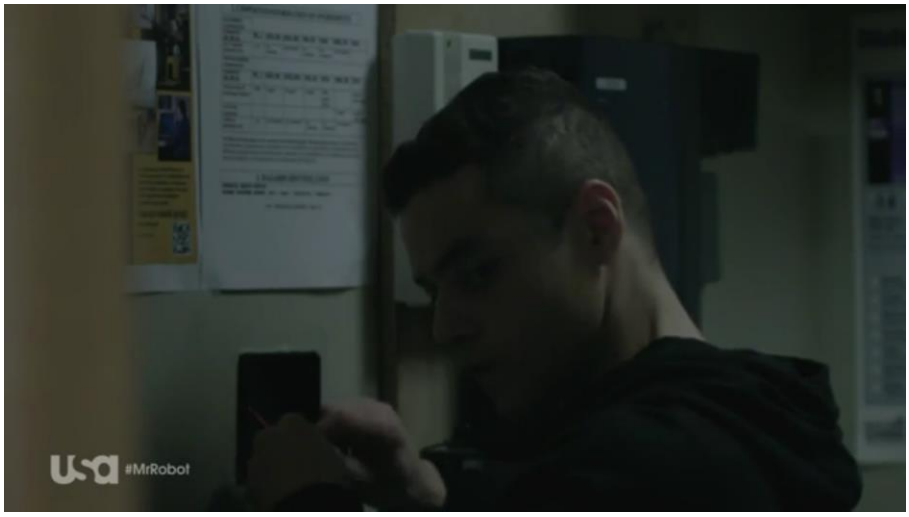
- Postoji velika količina koda koji se aktivira prilikom priključenja uređaja na računalu i otvaranja datoteka na njemu – i u bilo kojem dijelu može se nalaziti ranjivost. To uključuje upravljačke programe za komunikaciju s uređajem, za korištenje datotečnog sustava, dijelove koda koji obrađuju datoteke prije otvaranja (npr. za stvaranje slike datoteke – eng. *thumbnail*) i dijelove koda koji se pokreću prilikom otvaranja datoteke.

- Lažiranje svrhe uređaja s USB priključkom

  - Žrtva na računalo priključi memorijski USB *stick*, slušalice ili neki drugi naizgled bezopasan uređaj. No, prilikom priključenja, uređaj se računalu zapravo predstavi kao tipkovnica i preuzme kontrolu nad njim „utipkavajući" naredbe. Alternativno, uređaj se predstavi kao USB mrežno sučelje i izvrši mrežni napad na računalo.

Nepoznati uređaji koje žrtva pronađe nisu jedini rizik – ukoliko napadač ima pristup žrtvinom računalu, ponekad može i inficirati spojene uređaje kao što su memorijski USB *stickovi*. Taj napad je poznat kao BadUSB[2] (7) i u kontekstu socijalnog inženjeringa može uređaje kojima žrtva najviše vjeruje – njezine vlastite uređaje – pretvoriti u alat napadača.

Osim korištenja naizgled bezopasnih uređaja za preuzimanje kontrole nad žrtvinim računalom, postoji niz uređaja koji imaju posebnu vrijednost u napadima socijalnim inženjeringom u kojima socijalni inženjer može dobiti fizički pristup prostorijama do kojih drugi ne mogu doći. Slika 5 prikazuje scenu iz serije Mr. Robot koja je dobar primjer upravo takve situacije – u sceni napadač pomoću socijalnog inženjeringa ostvaruje fizički pristup tvrtki, nakon čega ugrađuje i spaja na mrežu vlastiti uređaj (modificirano Raspberry Pi računalo).



Slika 5 - Scena iz serije Mr. Robot u kojoj napadač socijalnim inženjeringom ostvaruje fizički pristup tvrtki te ugrađuje i spaja na mrežu svoje modificirano Rasberry Pi računalo

[2] predstavljen 2014. godine na konferenciji BlackHat)

4 Osnovne zaštite

S obzirom na to da je socijalni inženjering samo jedno područje unutar informacijske sigurnosti, za njega vrijede i općeniti koncepti kao i za ostale grane sigurnosti. Kao prvo, potrebna je dubinska, slojevita obrana (eng. *defense in depth*) – gotovo uvijek je neprihvatljivo da sigurnost sustava ovisi samo o jednom zaštitnom mehanizmu. Isto tako, ne postoji potpuna sigurnost – moguće je učiniti napade izrazito skupima za napadača i malo vjerojatnima, ali nikada nije moguće potpuno ukloniti vjerojatnost uspješnog napada.

Glavna lekcija sa socijalnim inženjeringom je to da sigurnost ne staje s tehnologijom. Kao što piše u citatu u uvodu ovog dokumenta, moguće je imati najjače zaštite računalne i fizičke sigurnosti, no to ništa ne govori o sveukupnoj jačini sigurnosnog lanca gdje je najslabija karika često **ljudski faktor**.

Zaštita od socijalnog inženjeringa je kompleksna tema koja se iz dana u dan razvija i, kao sigurnost općenito, to nije problem koji će ikada u potpunosti biti riješen. No, postoje neke konkretne mjere koje se često preporučaju kao dobre početne točke za zaštitu od socijalnog inženjeringa.

Iz perspektive organizacije, korisno je (1) (8):

- Jasno **označiti tajnost** podataka
    - Jesu li neki podaci javni? Samo za internu uporabu? Povjerljivi?
- Uspostaviti **jasna pravila**
    - Maknuti **ljudsku procjenu** iz procesa odlučivanja. Zaposlenici ne bi smjeli imati nikakve sumnje smiju li ili ne dijeliti neke informacije s potencijalnim napadačem
- **Podići svijest** o socijalnom inženjeringu, redovito **obrazovati**
    - Objasniti zaposlenicima kako informacije koje posjeduju mogu imati veliku vrijednost za napadača
    - Posebno obrazovanje za ključno osoblje koje ima najveći rizik za izloženost napadu (npr. korisnička podrška)

Za krajnje korisnike (unutar organizacije i u kontekstu osobne sigurnosti) korisno je upoznati se s temom socijalnog inženjeringa, razumjeti kako se napadi odvijaju i zašto uspijevaju te upoznati se s čestim znakovima napada socijalnog inženjeringa. U pravilu, isto što bi i zaposlenici u organizaciji trebali proći kroz obrazovanje vezano za obranu od socijalnog inženjeringa.

5 Zaključak

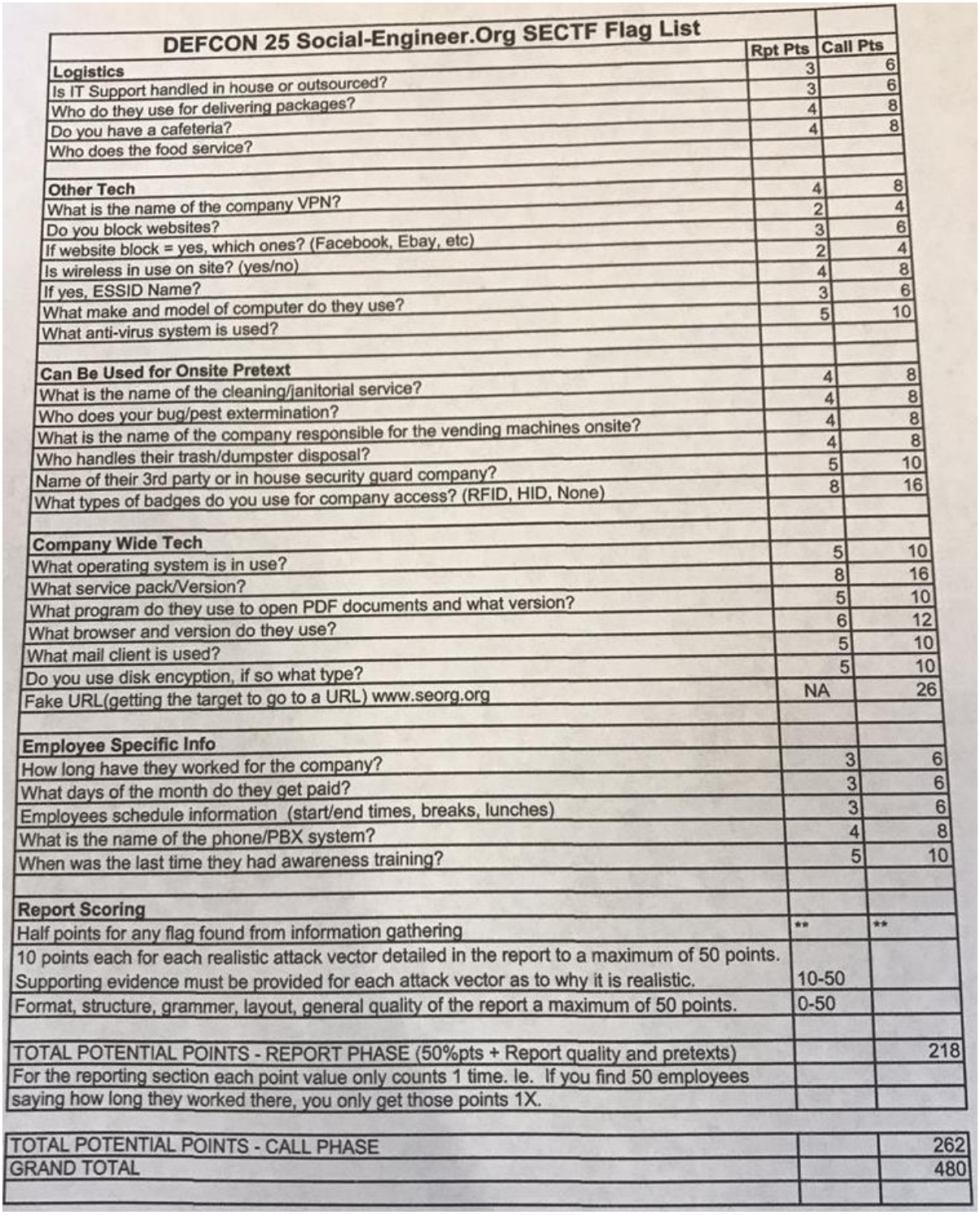
U konačnici, socijalni inženjering široka je tema i ovaj dokument samo je uvod u nju. U ovom dokumentu socijalni inženjering opisan je kroz ciklus napada, pregled tehnika i osnovne zaštite. No, i ovo osnovno znanje o socijalnom inženjeringu već je izrazito korisno za razumijevanje rizika te prepoznavanje i zaustavljanje napada. Glavna pouka dokumenta trebala bi biti da sigurnost nisu samo tehnički sustavi: vatrozidi, protuprovalni sustavi i slično, već je potrebno posvetiti značajnu pažnju i ljudskom faktoru sigurnosti.

Podizanje svijesti i obrazovanje glavno su oruđe u toj borbi i oni se moraju trajno provoditi za sve sudionike u informacijskim sustavima: proizvođače, vlasnike, korisnike i sve koji s tim sustavima dolaze u dodir. Pored toga potrebni su sustavi podrške kojima se korisnici mogu javiti, kako u organizaciji tako i na nacionalnoj razini. U Hrvatskoj takva točka je Nacionalni CERT.

Za kraj, zanimljivo je znati da slično natjecanjima u računalnoj sigurnosti (tzv. eng. *Capture The Flag* natjecanja), postoje i natjecanja u socijalnom inženjeringu. Najpoznatije takvo natjecanje je SECTF (eng. *Social Engineering Capture the Flag*) koje se redovito održava na sigurnosnoj konferenciji DEF CON. Na tim natjecanjima sudionici pokušavaju prikupiti što više zadanih informacija (eng. *flags*) o određenoj organizaciji u dva dijela. U prvom dijelu (prije konferencije) rade fazu istraživanja, gdje primarno kroz javno dostupne podatke prikupljaju informacije i pišu izvještaj. Zatim, u drugom dijelu (na samoj konferenciji), natjecatelji imaju 20-ak minuta da kroz telefonske pozive saznaju što je više moguće zadanih informacija o ciljnoj organizaciji.

Slika 6 prikazuje natjecatelja na konferenciji DEF CON 23 kako pokušava pozivom prikupiti zadane informacije, a slika 7 prikazuje popis informacija koje su natjecatelji pokušavali saznati na SECTF natjecanju na konferenciji DEF CON 25.

Slika 6 - SECTF (natjecanje u socijalnom inženjeringu) na konferenciji DEF CON 23 (izvor)



DEFCON 25 Social-Engineer.Org SECTF Flag List	Rpt Pts	Call Pts
Logistics	3	6
Is IT Support handled in house or outsourced?	3	6
Who do they use for delivering packages?	4	8
Do you have a cafeteria?	4	8
Who does the food service?		
Other Tech	4	8
What is the name of the company VPN?	2	4
Do you block websites?	3	6
If website block = yes, which ones? (Facebook, Ebay, etc)	2	4
Is wireless in use on site? (yes/no)	4	8
If yes, ESSID Name?	3	6
What make and model of computer do they use?	5	10
What anti-virus system is used?		
Can Be Used for Onsite Pretext	4	8
What is the name of the cleaning/janitorial service?	4	8
Who does your bug/pest extermination?	4	8
What is the name of the company responsible for the vending machines onsite?	4	8
Who handles their trash/dumpster disposal?	5	10
Name of their 3rd party or in house security guard company?	8	16
What types of badges do you use for company access? (RFID, HID, None)		
Company Wide Tech	5	10
What operating system is in use?	8	16
What service pack/Version?	5	10
What program do they use to open PDF documents and what version?	6	12
What browser and version do they use?	5	10
What mail client is used?	5	10
Do you use disk encyption, if so what type?	NA	26
Fake URL(getting the target to go to a URL) www.seorg.org		
Employee Specific Info	3	6
How long have they worked for the company?	3	6
What days of the month do they get paid?	3	6
Employees schedule information (start/end times, breaks, lunches)	4	8
What is the name of the phone/PBX system?	5	10
When was the last time they had awareness training?		
Report Scoring	**	**
Half points for any flag found from information gathering		
10 points each for each realistic attack vector detailed in the report to a maximum of 50 points. Supporting evidence must be provided for each attack vector as to why it is realistic.	10-50	
Format, structure, grammer, layout, general quality of the report a maximum of 50 points.	0-50	
TOTAL POTENTIAL POINTS - REPORT PHASE (50%pts + Report quality and pretexts)		218
For the reporting section each point value only counts 1 time. Ie. If you find 50 employees saying how long they worked there, you only get those points 1X.		

TOTAL POTENTIAL POINTS - CALL PHASE		262
GRAND TOTAL		480

Slika 7 - Popis zadanih informacija (eng. *flags*) koje su natjecatelji u SECTF-u na konferenciji DEF CON 25 pokušavali prikupiti (izvor)

6 Literatura

1. **Mitnick, Kevin D. i Simon, William L.** *The art of deception: Controlling the human element of security.* s.l. : John Wiley & Sons, 2011.
2. **Berg, Al.** *Cracking a Social Engineer*. s.l. : LAN Times, 1995.
3. **Thornburgh, Tim.** *Social engineering: the dark art.* s.l. : ACM, 2004.
4. **Leyden, John.** Office workers give away passwords for a cheap pen. *The Register.* [Mrežno] 18. travanj 2003. [Citirano: 20. studeni 2017.] https://www.theregister.co.uk/2003/04/18/office_workers_give_away_passwords/.
5. **Trend Micro.** Spear-Phishing Email: Most Favored APT Attack Bait. [Mrežno] 2012. [Citirano: 17. studeni 2017.] https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf.
6. **Hak5.** USB Rubber Ducky. [Mrežno] [Citirano: 16. studeni 2017.] https://hakshop.com/products/usb-rubber-ducky-deluxe.
7. **Security Research Labs.** USB peripherals can turn against their users. [Mrežno] [Citirano: 16. studeni 2017.] https://srlabs.de/bites/usb-peripherals-turn/.
8. **Gragg, David.** *A multi-level defense against social engineering.* s.l. : SANS Reading Room, 2003.