HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Socijalni inženjering

CCERT-PUBDOC-2006-10-172

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Socijalni inženjering pripada skupini napada na računalne sustave, ali i sustave u širem smislu riječi. Jezgrovita i sažeta definicija koja je raspoloživa u „*People Hacking*“ tekstu [8], slobodno prevedena glasi: „Socijalni inženjering je umjetnost i znanost nagovaranja ljudi da ispune zahtjeve napadača.“.
Radi se o načinu stjecanja informacija i podataka do kojih napadač legitimnim putem ne bi mogao doći. Pri tome se ne iskorištavaju propusti implementacija operacijskih sustava, protokola i aplikacija, nego se napad usmjerava na najslabiju kariku cjelokupnog lanca – ljudski faktor.
Jedan od slučajeva socijalnog inženjeringa dogodio se 1994. godine kada je francuski haker nazvao FBI ured u Washingtonu i lažno se predstavio kao FBI agent zaposlen u američkoj ambasadi u Parizu. Sugovornika je nagovorio da mu pojasni način na koji se može koristiti FBI račun za obavljanje telefonskih razgovora. U sedam mjeseci napravio je telefonski račun od 250 000 dolara.
Kroz ne toliko staru povijest, javljaju se jednostavni primjeri počevši od navedenog, preko pretvaranja i lažnih predstavljanja u cilju stjecanja, primjerice, zaporki za pristup sustavu, do kompleksnih prijevara koje nije jednostavno prepoznati. Za ovakve napade nije potrebno imati posebno tehničko predznanje, ali je prijeko potreban odgovarajući karakter i sposobnost uvjeravanja sugovornika u neistine koliko god one bile čudne i nelogične. Komunikacijske vještine osobe koja se bavi socijalnim inženjeringom moraju biti na zavidnoj razini jer je oslonac napada upravo čovjek.
Kod računalnih sustava neki autori čine podjelu na *hardware*, *software* i *wetware* gdje je posljednja komponenta ljudski udio u čitavom sustavu. Čak i ako su prve dvije komponente dovedene do savršenstva, uz dovoljno strpljenja i potrebnog znanja napadač može relativno jednostavno prevariti ljudsku komponentu i doći do željenih informacija. Iz ove tvrdnje vrlo se jasno vidi kako je ljudski faktor važan čimbenik u problemu računalne sigurnosti. Vještine i načini obrane od socijalnog inženjeringa vrlo se rijetko mogu naći u programima obuke djelatnika, a u nastavku dokumenta poseban je naglasak stavljen na nužnost uvođenja edukacije u svrhu obrane od opisanih napada.
U kontekstu socijalnog inženjeringa nezaobilazno je pitanje izbora žrtve napada. Da bi se mogao dati odgovor na to pitanje potrebno je ponajprije analizirati ciljeve napadača. Primarni cilj uvijek je stjecanje nedozvoljenog pristupa sustavu, najčešće, iako ne i isključivo, računalnom. Ostali ciljevi su saznavanje informacija i podataka potrebnih za izvođenje prijevara (eng. *fraud*), industrijske špijunaže, krađe identiteta ili za rušenje ugleda napadnute organizacije. Uglavnom su to velike telekomunikacijske korporacije, javno popularne te vojne i vladine organizacije. Na razini osoba i njihovih položaja u organizacijama, napadi su ponajprije usmjereni na službenike koji rade sa strankama i vrlo teško mogu uočiti sam napad. Razlozi su, između ostalih, neiskustvo i manjak obuke, ali i faktori nezainteresiranosti te nemotiviranosti zaposlenika.
Ovakvi napadi se vrlo rijetko spominju u medijima. Glavni razlog tome je zataškavanje, ponajprije od strane izravnih žrtava, operatora i službenika. Naime, uspjeh napada socijalnim inženjeringom često se, iako krivo, pripisuje nedostatku sposobnosti prevarenog zaposlenika, a takav stav dovodi do osjećaja njegove posramljenosti i izbjegavanja svakog spomena samog napada. Čak i kada zaposlenik prijavi napad nadređenima, malo je vjerojatno da će vijest biti javno obznanjena, budući da bi objava mogla dovesti do gubitka ugleda tvrtke, odnosno neželjenog negativnog publiciteta. Još jedan važan čimbenik je i nemogućnost jednostavnog uočavanja napada, sve dok se ne pojave ozbiljne posljedice. Na žalost, situacija je puno gora od one u računalnom svijetu, gdje postoje uređaji i aplikacije za detekciju napada (eng. IDS - *Intrusion Detection System*) i vrlo napredni mehanizmi obrane.

2. Filozofija socijalnog inženjeringa

Velike i ozbiljne organizacije troše gomile novca za nove tehnologije vezane uz računalnu odnosno mrežnu sigurnost. Međutim, rijetko i slabo ulažu u ljude koji su jednako tako dio sustava tih organizacija i na kojima isto tako leži veliki dio odgovornosti. Upravo je to činjenica koju koriste napadači. Pristup informacijama koje čuvaju ljudi mnogo je jednostavniji od pristupa zaporkom zaštićenim informacijama. Napadači iskorištavaju ljudsku psihologiju i na taj način uspijevaju u navođenju žrtava na ispunjavanje njihovih zahtjeva bez izazivanja nepotrebnih sumnji.
Napadač koji provodi napad zasnovan na socijalnom inženjeringu mora posjedovati osobine poput dobrog pamćenja, snalaženja u razgovorima, odgovarajućeg načina razmišljanja i slično, jer mu one donose prednost prilikom izvođenja napada.
U sljedećim poglavljima detaljnije su opisane najčešće metode prijevare korištene u socijalnom inženjeringu.

2.1. Uvjeravanje

Nagovaranje ili uvjeravanje je akcija poduzeta od strane napadača kojoj je konačan cilj potaknuti žrtvu na izvršavanje željenih postupaka. Primjeri iz svakodnevnog života su političke kampanje. Na izborima glasači u stvari slijede želje socijalnih inženjera - političara. Vjerojatno još zorniji primjer predstavljaju propagandne poruke koje potrošače „tjeraju“ na kupovanje nečega što im često i nije potrebno niti su imali namjeru na to potrošiti novac. Sposobnost uvjeravanja jedna je od najvažnijih karakteristika koju socijalni inženjer mora posjedovati ili razviti.

2.2. Lažno predstavljanje

Ovisno o situaciji, napadač se mora maskirati odnosno pretvarati da je netko tko nije kako bi prikupio željene informacije od žrtve. Ovo je najčešće korištena metoda napada. Odabir lažne uloge ovisi o konkretnoj situaciji i željenom cilju.
Predstavljanje u svojstvu nadređene osobe najučestaliji je odabir lažnog predstavljenog socijalnog inženjera. Razlog tomu je želja zaposlenika za dokazivanjem i podrazumijevano poštivanje autoriteta. Napadač poziva djelatnika i nadređenim mu tonom zapovijeda što treba činiti. Prethodno napadač mora proučiti opis posla, odnos prema nadređenom i slične osobine osobe koju koristi za žrtvu pa stoga ovim pristupom relativno jednostavno može doći do osjetljivih informacija poput korisničkog imena i zaporke zaposlenika.
Napadač se može predstavljati i kao službenik pa na taj način doći do informacija od, primjerice, službenika na istoj razini u nekoj drugoj poslovnici tvrtke. Poznato je da je ljudi, pogotovo kada su u istom položaju, najčešće žele pomoći jedan drugome. Međutim, solidarnost u ovom slučaju može značiti i obznanu tajnih informacija napadačima.
Najopasniji je slučaj kada se napadač predstavi kao osoba iz podrške, primjerice tehničke. Službenicima na taj način ulije dozu povjerenja i uvjetuje da mu, bez ikakvih sumnji, navode podatke koji inače nisu dostupni javnosti.
Jedan od često korištenih načina lažnog predstavljanja je izigravanje novog zaposlenika. Ljudi su skloni pomoći početnicima, što socijalni inženjeri često koriste za saznavanje detalja o radu organizacije koju žele napasti. Nije moguće, a ni dobro, zaposlenicima zabraniti međusobnu pomoć, ali je zato prijeko potrebno zaposlenike educirati kako bi znali prepoznati napad i sukladno tome reagirati.

2.3. Stvaranje odgovarajuće situacije

Ovdje se radi o sposobnosti stvaranja situacije u kojoj je žrtva primorana donositi brze i važne odluke pod velikim psihološkim pritiskom s jedne strane, i brojnim zahtjevima napadača s druge. Najčešće su žrtve same krive za nastalu situaciju pa je donošenje pogrešnih zaključaka nužan ishod pokušaja ispravljanja postojećeg stanja, odnosno otklanjanja zastoja. Ponekad i više napadača može sudjelovati u stvaranju prilika pogodnih za saznavanje nedozvoljenih informacija ili odvlačenja pozornosti radi napada na nekom drugom području koje tada preopterećeni zaposlenik ne može pratiti.

Jedan od najboljih načina napadanja je zbližavanje s ljudima koji su dio sustava na koga se želi izvršiti napad. Kako su te osobe najčešće posvećene poslu te im nedostaje doticaja s okolinom, napadaču je ovo gotovo siguran način dolaženja do željenih informacija. Najčešći načini stjecanja povjerenja su postupno stvaranje odnosa između napadača i žrtve i navođenje žrtve na vjerovanje u buduću korist od napadača.
Jedan od načina zlouporabe stvaranjem odgovarajuće situacije je i dokazivanje postojanja boljeg načina za rješavanje problema u ciljnom sustavu. Takvim pristupom može se doći do detalja o djelovanju sustava koga se želi napasti.
Možda je najzahtjevniji način napadanja koji obuhvaća stvaranje situacije u kojoj ljudi misle da su u pravu, ali su pri zaključivanju načinili određene pogreške.

2.4. Moralna odgovornost

Radi se o ljudskom ponašanju u kojem žrtve pokušavaju pomoći napadaču jer osjećaju da je to njihova moralna obveza. Dakako, žrtve pri tome ne znaju da je njihova suradnja u stvari odavanje podataka zlonamjernoj osobi.
Dobar primjer ovakvog ponašanja je slučaj u kome je napadač iz iste zemlje kao i neki inozemni zaposlenik te on, koristeći osjećaj moralne dužnosti zaposlenika, dolazi do potencijalno osjetljivih informacija. Napadači koji se koriste opisanom tehnikom najčešće su vrlo bistre osobe, a svoje žrtve promatraju i upoznaju kroz dulje vrijeme te s njima uspostavljaju blizak osoban odnos.

2.5. Želja za pomaganjem

Čest je ljudski osjećaj želje za nesebičnom pomoći drugima. Taj je osjećaj još više izražen kada se u čovjeku pobudi strah da će gotovo sigurno i on sam u nekom trenutku trebati tuđu pomoć. Takav stav iskorištavaju napadači - socijalni inženjeri. Kao jednostavan primjer može poslužiti situacija u kojoj napadač zatraži pomoć od žrtve koja mu odbija pomoći jer traži neke nedostupne informacije. Međutim, lijepim razgovorom napadač pobudi osjećaj djelomične krivnje i potakne žrtvu na razmišljanje o tomu kako će i njoj vjerojatno zatrebati pomoć kada se nađe u jednakoj situaciji kao i on u tom trenutku. Žrtva najčešće pomisli kako se radi o sitnim informacijama i kako nikomu neće škoditi ukoliko pomogne čovjeku i izvan protokola. Tako otkriva potencijalno osjetljive informacije. Napadač odlazi zadovoljan jer je dobio što je htio, a žrtva ostaje relativno zadovoljna jer je pomogla nekomu.

2.6. Iskorištavanje starih veza i kooperacije

U ovom načinu socijalnog napadanja, napadač obnavlja stare ili stvara nove veze sa žrtvama. Napadač će stvoriti odnos koji je dovoljan za stjecanje povjerenja. Ovakav pristup kod socijalnog inženjeringa ima vrlo velik stupanj uspješnosti, što je posebno izraženo ukoliko je žrtva spremna za ostvarivanje suradnje sa napadačem. Na taj način je prijeđena početna barijera i prikupljanje željenih informacija kreće lakšim tokom.

3. Načini izvršavanja napada

Socijalni inženjering nije uvijek usmjeren izravno na čovjeka. U stvarnosti on može poprimiti vrlo velik spektar oblika, počevši s uspostavljanjem telefonskog kontakta s potencijalnim žrtvama, preko uvjeravanja žrtava u potrebu razgovora s odgovornim osobama pa sve do pretraživanja otpada. U ovom poglavlju su navedeni neki od važnijih oblika napada.

3.1. Telefonski inženjering

Jedan od najčešćih i najlakših načina izvršavanja socijalnog inženjeringa ide u smjeru telefoniranja. Napadači nazivaju bilo koga iz organizacije koju napadaju, od običnih radnika do administratora. Budući da napadač ima izrazito dobre vještine govora, lako stiče povjerenje od strane djelatnika. Široka rasprostranjenost telefonske mreže čini ovu tehniku napada vrlo često korištenom te umanjuje mogućnost otkrivanja napadačevog identiteta.

3.2. Pretraživanje otpada

U ranim danima socijalnog inženjeringa najlakši način napada uključivao je sakupljanje informacija iz otpadnih materijala osoba ili organizacija koje napadač želi napasti. Ovakav pristup omogućuje pronalaženje materijala kao što su pisana korespondencija, telefonski imenici, detalji različitih dnevnika, izvorni kodovi i slično. Korištenjem podataka pohranjenih u njima, napadač upoznaje strukturu organizacije, saznaje imena i osobne podatke odgovornih osoba. Ukratko, saznaje mnogo informacija korisnih za izvođenje napada.

3.3. Socijalni inženjering korištenjem Interneta

Internet napadačima nudi pregršt mogućnosti. Ponekad niti velik oprez nije dovoljan da bi se sustav u potpunosti zaštitio. U nastavku je opisano nekoliko tehnika kojima se napadači najčešće koriste.
Nažalost, mnoge osobe nisu upoznate sa sigurnosnim problemima i prijevarama koje se izvode korištenjem Interneta. Većina osoba ima naviku upotrebljavanja istih zaporki na različitim korisničkim računima, ne vodeći pri tome računa o sigurnosti sustava na kojima su im računi otvoreni.
Kako bi se dokopali zaporki napadači često koriste lažne poruke (eng. *scam*) koje oglašavaju različite krivotvorene ponude i upozorenja. Tako žrtvu navode na unos osobnih podataka i zaporke. Čest primjer je poruka u kojoj je kao pošiljatelj navedena određena banka. Njena tehnička služba obraća se klijentu poradi određenih tehničkih preinaka koje zahtijevaju korisnikove osobne podatke. Njih se prilaže korištenjem web obrazaca o kojima će biti više riječi u nastavku. Na slici ispod može se vidjeti primjer takve poruke:

Fifth Third Bank

Dear **Fifth Third Bank client**,
The Fifth Third Bank Technical Department is performing a scheduled software upgrade to improve the quality of the banking services.
By clicking on the link below you will begin the procedure of the user details confirmation.

http://www.53.com/wps/portal/contenttype/secure/confirm_context.id

These instructions are to be sent to and followed by all Fifth Third Bank clients.
We apologize for any inconvenience and thank you for cooperation.

Fifth Third Bank Technical Service

Slika 1: Primjer *scam* poruke

Upotrebljavanje elektroničke pošte sa ciljem saznavanja osjetljivih informacija čest je primjer socijalnog inženjeringa. Napadač se može predstaviti kao administrator mreže ili neka osoba sličnog položaja te tako steći naklonost žrtava. Ova tehnika nije vezana isključivo za socijalni inženjering već je uobičajena i na području zlouporabe sigurnosnih nedostataka programske potpore. Postupak zlouporabe u ovom slučaju uključuje slanje poruka koji sadrže štetne kodove poput virusa, trojanskih konja, crva ili nekih drugih opasnih programa. Pokretanjem štetnog programa na računalu žrtve, napadač dolazi do željenih zaporki i informacija koje su mu potrebne za daljnji napad.
Ponekad napadači mogu upravljati situacijom traženjem ponovnog unosa podataka kako bi nastavili s korištenjem usluge. Jedan od poznatih napada te vrste bile su zlonamjerno oblikovane web stranice. Kad ih žrtva posjeti pred njom se automatski otvori upozorenje o ponovnom spajanju na Internet. Postoji veći broj zlouporaba koje koriste opisani princip. Zbog toga je Microsoft posve onemogućio skriptne jezike u svojim klijentima za rukovanje elektroničkom poštom.
Osim elektroničke pošte prikladan medij za izvođenje prethodno opisanih zlouporaba predstavljaju i trenutne poruke (eng. *Instant Messaging*). U posljednje vrijeme one se sve više koriste jer omogućuju komuniciranje korisnika u realnom vremenu. U skupinu programa koji nude ovu uslugu pripadaju klijenti MSN (eng. *Microsoft Network*), ICQ (eng. *I Seek You*), IRC (eng. *Internet Relayed Chat*) te neki

manje poznati. Temeljni protokol koga koristi ICQ je poznat kao slabo zaštićen protokol koga je lako iskoristiti za neovlašteno dobivanje zaporki. Mnogo je implementacija IRC klijenata s pogreškama, a ta boljka ne zaobilazi ni MSN klijent. Usprkos svemu, pažljivijim je korištenjem moguće uvelike ublažiti kako mogućnost samo zlouporabe, tako i posljedice njenog eventualnog uspjeha.

3.4. Zavirivanje

Zavirivanje je jednostavan tip socijalnog inženjeringa u kojem napadači pokušavaju vidjeti pokrete žrtava kako bi dobili željene podatke. Tipični primjeri ove tehnike je gledanje preko ramena osobe koja upisuje primjerice PIN na bankomatu i praćenje pokreta ruke osobe kod upisa zaporke prilikom prijavljivanja na sustav.

3.5. Forenzička analiza

Do korisnih informacija može se doći analizom odbačene opreme poput starih računala, različitih medija (CD, DVD, *floppy*), USB memorijskih kartica i slične opreme.

3.6. Reverzni socijalni inženjering

Obrat socijalnog inženjeringa jedna je od najopasnijih metoda zlouporabe. Napadač-reverzni socijalni inženjer stvara situaciju u kojoj se prikazuje izvorom informacija za osobe kojima su one potrebne. Kako bi ovakva prijevara uspjela potrebno je puno predznanja i strpljenja u izvedbi. Napadaču je cilj stvoriti situaciju koju nitko u organizaciji, osim njega, ne može riješiti. Prilikom rješavanja kreiranog problema dolazi do željenih informacija, nakon čega žrtvi vraća popravljen uređaj bez ikakvih tragova o napadu.

4. Zaštita od socijalnog inženjeringa

Iz prijašnjih poglavlja je razvidan nedostatak odgovarajućih tehnika automatske detekcije, bilježenja i suprotstavljanja opisanim napadima. U biti, jedinom mogućnosti djelovanja pokazuje se ljudska intervencija. Stoga je vrlo važno posvetiti dovoljnu pažnju kreiranju odgovarajućih sigurnosnih protokola kojih se svi članovi neke organizacije trebaju pridržavati. Neki od tipičnih su opisani u nastavku ovog poglavlja

4.1. Sigurnosna politika

U svakoj od organizacija je jedan od najvažnijih koraka postizanja sigurnosti stvaranje sigurnosnih pravila (eng. *Security policy*). Nažalost, organizacije troše mnogo novca u sigurnost sklopovlja (eng. *hardware*) i programske potpore (eng. *software*), ali ne obraćaju u dovoljnoj mjeri pozornost na ljudski čimbenik. Kako bi problem sigurnosti bio riješen, odgovorna osoba mora razumjeti važnost razvijanja i primjene kvalitetnih sigurnosnih pravila, smjernica i procedura. Efikasnost sigurnosnih pravila podrazumijeva potpunu podršku svih članova organizacije.

4.2. Edukacija zaposlenika

Pri zapošljavanju osoba ne bi trebalo u obzir uzimati samo akademsko obrazovanje već i kriminalnu prošlost kandidata. Oni bi trebali biti upućeni u tajnost posla (eng. NDA - *Non-Disclosure Agreements*) te u svoja prava privatnosti. Trebali bi se provoditi ne samo tehnički, već i psihički testovi kako bi se stekao dojam o osobnosti kandidata. Sa stajališta sigurnosti optimalnim se izborom smatraju bistre i samopouzdane osobe s izraženom svojstvima kreativnosti i odgovornosti. Međutim, takve osobe nemaju povjerenja u ljude iz svoje okoline, što može predstavljati nedostatak u obavljanju osnovnog zanimanja.

Iskustvo je pokazalo da je edukacija najbolji način obrane od većine sigurnosnih prijetnji. Korisnici i upravitelji moraju biti upoznati s vrstama napada, a tijekom školovanja zaposlenicima treba dati do znanja kako ne smiju odavati zaporke ili bilo kakve druge osjetljive informacije.

4.3. Prijava incidenata

Dobra reakcija na napad obuhvaća vrlo jasne protokole prijave sumnjivih ponašanja. Jednako je važno i postojanje nedvosmislene i svestrane podrške prijavi, kako bi zaposlenici to činili bez dvojbe i odgode. Ako podrška nije dovoljno dobra tada se zaposlenici mogu obeshrabriti i nedovoljno ozbiljno shvatiti veličinu prijetnje. U suprotnoj situaciji, kada nadređeni pozitivno reagiraju na prijavu incidenta, zaposlenik je ohrabren i potaknut na pažljiviji posao i nove prijave bez okolišanja.

4.4. Kontrola pristupa

Dvije su metode koje se koriste kod određivanja kontrole pristupa. Prva uključuje omogućavanje pristupa svemu i postavljanje eksplicitne zabrane samo na određene resurse, dok je druga obratna i podrazumijeva postavljanje zabrane na sve i omogućavanje pristupa samo određenim resursima. Druga metoda je sigurnija, jer nema opasnosti da se zaboravi postaviti ograničenje pristupa na neki potencijalno osjetljiv resurs. Međutim, tom se metodom ograničava pristup resursima sve dok ga se eksplicitno ne omogući, što u određenim situacijama može predstavljati ograničenje. Optimizacija korisnosti često podrazumijeva pronalaženje odgovarajućeg odnosa između dviju opisanih metoda zabrane pristupa.

4.5. Fizička sigurnost

Budući da napadači često informacije pribavljaju iz otpadnih materijala tvrtki, a to su najčešće razni spisi, potrebno je obratiti značajnu pozornost na odlaganje otpada. Već su poznati i često korišteni uređaji poput rezača papira (eng. *paper schredder*).
Zabrane pristupa i ulaska u prostorije s važnom opremom moraju biti strogo poštivane, a pristup dozvoljen samo osobama od povjerenja. Iako opisane mjere zaštite ne garantiraju apsolutnu sigurnost, svakako su bolja opcija od nekontroliranog pristupa.

4.6. Provjera sigurnosti

Jedna od efikasnih metoda zaštite je angažiranje organizacija koje se bave testiranjem ranjivosti. Općenito, pametnije je provaliti u vlastiti sustav nego isto omogućiti zlonamjernom napadaču. Ispitivanja se mogu obavljati pod pretpostavkom potpunog nepoznavanja, djelomičnog ili opsežnog poznavanja napadanog sustava.

4.7. Višerazinska obrana

Izgradnja sustava za obranu od napada socijalnim inženjeringom vrlo je slična izgradnji bilo kojeg drugog sigurnosnog sustava. Ključno je odrediti ranjivosti i potencijalno izvedive napade te dizajnirati obrambeni mehanizam kako bi ih se onemogućio. Motiv izgradnje zaštitnog sustava u više razina polazi od spoznavanja napadačevih ograničenja. Naime, napadač koji je u doticaju samo s jednom razinom zaštite, teško može upoznati funkcionalnost slijedeće. Tako, ako i uspije zaobići jedan sloj zaštite, prije nego zaobiđe slijedeći mora proći određeno vrijeme koje se može iskoristiti za detekciju provale i poduzimanje odgovarajućih protumjera. Budući da su se napadi socijalnim inženjeringom pokazali uspješnima, razrada kvalitetne strategije obrane predstavlja slijedeći korak.
Čak se pokazuje da je uputno daleko veću pozornost posvetiti primijenjenoj strategiji nego samim metodama obrane. Pri tome strategija mora biti usmjerena prema brzom prepoznavanju napada, jer se, u protivnom, napadaču ostavlja velik prostor mogućnosti, a time i velika vjerojatnost da će zlouporaba uspjeti.
Sofisticiranija metoda borbe protiv napada je postavljanje tzv. klopki (eng. *land mines*) koja je vrlo dobar način uzvraćanja udarca. Tako je, postavljanjem stupice, moguće saznati čak i napadačeve osobne podatke.

4.7.1. Temeljna razina – sigurnosna pravila

Niti jedna utvrda ne može uspješno opstati bez jakih i stabilnih temelja. Okosnica informacijske sigurnosti su sigurnosna pravila (eng. *security policy*). Ona postavljaju standarde i razinu sigurnosti koju će sustav posjedovati te ga postavljaju u konzistentno stanje koje se može postavljati i

nadograđivati po volji. Temeljna sigurnosna pravila poprimaju još veću važnost kada štite sustav od napada temeljenih na socijalnom inženjeringu. Napadači se koncentriraju uglavnom na djelatnike koji moraju dati odgovore na pitanja i na zahtjeve različitih karakteristika. Krajnji korisnici se ne bi smjeli naći u situaciji u kojoj nisu sigurni jesu li određene informacije dostupne ili nisu. Pravila o tomu moraju biti unaprijed dobro definirana i to moraju učiniti ljudi koji se ozbiljno bave takvim problemima i koji su dobro upoznati s vrijednošću informacija čiju dostupnost definiraju.
Istraživanja su pokazala da je kod napadanja uvjeravanjem vrlo značajna svijest žrtve koja je usmjerena ka mislima i razmišljanju drugih. Iz toga je zaključeno da je izgradnja samosvijesti kod potencijalnih žrtava najbolji način obrane. Razvijanje vrlo jasnih i nedvojbenih pravila upravo povećava potrebnu samosvijest i samopouzdanje te umanjuje vjerojatnost uspjeha napada uvjeravanjem.
Sigurnosna pravila trebaju obuhvatiti široko područje kako bi bila dobar temelj zaštite. Trebala bi obuhvaćati područje pristupa informacijama, stvaranja korisničkih računa, odobravanja pristupa i izmjene zaporki. Osim navedenog, potrebno je i definirati pravila vezana uz zaključavanje, jedinstvene brojeve, uništavanje potencijalno osjetljivih pisanih informacija (eng. *paper shredding*) i pratnju posjetitelja. Pravila moraju imati ugrađenu disciplinu te, povrh svega, moraju biti poštivana od strane svih zaposlenika.
Temeljna razina obrane omogućava zaposlenicima obranu od napada zasnovanih na značajkama ljudske psihologije:

- raspršenju odgovornosti,
- poštivanju autoriteta i
- osjećaju moralne obveze.

Najvažnija njena značajka je izbjegavanje osobne odgovornosti zaposlenika za otkrivanje potencijalno osjetljivih i ostalih informacija.

4.7.2. Razina mjerila – sigurnosna osviještenost zaposlenika

Nakon uspostave sigurnosnih pravila svi bi zaposlenici trebali pohoditi odgovarajuću edukaciju vezanu uz sigurnosnu osviještenost. Pri tome su stvorena pravila smjernice koje zacrtavaju područje obučavanja za svakog zaposlenika. Dobro osmišljena pravila pojednostavljuju proces učenja i olakšavaju rad korisnicima te time bitno popravljaju kvalitetu reakciju zaposlenika na različite zahtjeve.
Svjesnost o važnosti sprečavanja socijalnog inženjeringa obuhvaća mnogo više od spoznaje zaposlenika o rizičnosti odavanja vlastitih zaporki. Poznat svjetski haker, Kevin Mitnick, izjavio je kako nikada nije izravno pitao zaporku. Njegovi napadi bili su mnogo složeniji od toga. On je stvarao osjećaj povjerenja između sebe i žrtve te ga zatim iskorištavao ovisno o potrebnom cilju.
Zaposlenici moraju biti upoznati s vrstama informacija koje su svrhovite napadačima i razgovorima koje je potrebno smatrati sumnjivima. Moraju moći razlučiti povjerljive informacije od javnih i moraju shvatiti svoju odgovornost kod njihove zaštite.
Potencijalne žrtve – zaposlenici, također bi trebali biti svjesni osnovnih značajki napada temeljenih na socijalnom inženjeringu. Pojedini uključuju odbijanje davanja informacija klijenta, užurbanost, zastrašivanje, čudna pitanja i traženje zabranjenih podataka. Zaposlenici trebaju biti svjesni činjenice kako će dobar socijalni inženjer pokušati ponajprije uspostaviti povjerljivi odnos sa žrtvom. Kasnije će to iskoristiti za dobivanje nedozvoljenih informacija kroz neobavezne razgovore, spominjanje zajednički poznatih osoba, općenitog ustrojstva organizacije i slično.
Obuka bi trebala slijediti globalna sigurnosna pravila uz nekoliko čimbenika koje bi svi zaposlenici trebali imati na umu:

- Osjećaj vrijednosti
  Često su podaci i mogućnost pristupa nekom sustavu podcijenjeni od strane zaposlenika i takvi ostaju sve dok se ne dogodi napad kojim se situacija promijeni.
- Nisu svi prijatelji pravi prijatelji
  Budući da je napadačima temeljni cilj stvoriti prijateljske odnose koje mogu iskoristiti, potrebno je obratiti posebnu pažnju na opasnost pojma prijatelj u ovom kontekstu.
- Ne odavati osobne zaporke

Zaporke namijenjene korisnicima isključivo su njihovo vlasništvo. Ni u kojoj situaciji vlasnik zaporke ne bi ju trebao dijeliti s drugom osobom.

- Ne procjenjivati na temelju radnog odijela

  Ozbiljan napadač lako će se maskirati korištenjem radnog odijela koje mu daje prividno legitiman razlog za boravak na prostoru za kojeg inače nema dozvolu. Važno je shvatiti da uniforma nije razlog za odavanje povjerljivih informacija.

4.7.3. Razina utvrde – otpor ključnog osoblja

Nije dovoljno samo osvijestiti zaposlenike u pogledu informacijske sigurnosti, nego je potrebno i educirati ključno osoblje u pogledu razvijanja otpora prema napadima. Ključno osoblje obuhvaća osoblje dostupno za pomoć korisnicima (eng. *help-desk personnel*), prodavače, poslovne pomoćnike, tajnike i recepcionare te sistemske administratore odnosno inženjere. U program obuke treba uključiti sve zaposlenike kojima je posao pomagati drugima. Kvalitetna obuka u ovom kontekstu sprečava zaposlenike od mogućnosti popuštanja pritisku napadača i od nesvjesnog davanja pristupa informacijama. Nekoliko je tehnika koje se primjenjuju u ovakvoj edukaciji. Sve one su preuzete iz socijalne psihologije:

- Cijepljenje

  Radi se o pojmu vezanom uz davanje oslabljenih argumenata u odnosu na one koje koriste socijalni inženjeri prilikom izvršavanja napada. Metoda je nazvana prema medicinskom cijepljenju koje obuhvaća izlaganje pacijenta maloj količini oslabljenih uzročnika bolesti. Time se nastoji razviti imunitet na željenu bolest. Jedini nedostatak ove tehnike je potreba za predviđanjem ponašanja napadača, što nije uvijek moguće kvalitetno učiniti.

- Upozoravanje

  Praktična primjena ovog načina edukacije je upozoriti zaposlenike ne samo na to da će napadač pokušati uvjeriti žrtvu, nego i na varljivost i neiskrenost argumenata koje će upotrijebiti. Dakle, žarište ove tehnike je usmjereno na sadržaj napada, a ne samo na namjeru.

- Shvaćanje zbilje

  Jedan od razloga za neuspjeh edukacije je nedovoljna svijest o opasnosti. Naime, korisnici često misle kako nisu ranjivi i kako njih nije baš lako prevariti. U realnom svijetu to se pokazalo neistinitim. Stoga je cilj obuke prikazati korisnicima njihovu ranjivost na osobnom primjeru. Jednostavan i efektan način prikazivanja ranjivosti zaposlenika jest postavljanje osobe koja, primjerice, prije predavanja o ovom problemu saznaje mnoge informacije od polaznika. Tokom predavanja ista osoba dolazi i prezentira svoja saznanja. To je vrlo jasan pokazatelj koji polaznike vraća u zbilju i dokazuje da je pojam o vlastitoj neranjivosti zabluda.

4.7.4. Razina ustrajnosti - podsjetnici

Nakon obuke je svijest o važnosti i opasnosti od napada podignuta na višu razinu. Međutim, pokazalo se da ta svijest ima svoj rok trajanja. To znači da je razinu samosvijesti potrebno s vremena na vrijeme povratiti na početnu vrijednost.

Vrlo dobar primjer potrebe za navedenim je tipična policijska taktika. U redovnim vremenskim razmacima svim se zaposlenicima daju izvješća o poginulim zaposlenicima kako bi ih se podsjetilo na opasnost posla i usadio u njih neprekidan osjećaj bivanja u pripravnosti.

Na sličan način zaposlenici trebaju biti neprekidno svjesni mogućnosti pojave napadača koji preko njih pokušava pristupiti nedozvoljenim informacijama. Dobar način za izvođenje opisanog je redovno izvještavanje zaposlenika o napadima koji su se dogodili u prethodnom vremenskom razdoblju.

4.7.5. Razina hvatanja napadača – "minsko polje"

Stupice su vrlo moćno sredstvo u borbi protiv napadača, odnosno u prikupljanju podataka o zlonamjernim korisnicima. Mehanizam je logički istovjetan ideji nagaznih mina (eng. *land mines*), a cilj mu je razotkriti napadača i onemogućiti daljnje napredovanje napada. Mehanizam upozorava žrtvu da je napad u tijeku i da bi razinu obrane trebalo podići na veći stupanj. Neke ideje kojima se

spomenuto može ostvariti navedene su u nastavku, ali njihov broj je neograničen i ovisi o kreativnosti sistemskih odnosno sigurnosnih inženjera.

- Osoba koja poznaje sve zaposlenike

  Vrlo je korisno zaposliti osobu koja se bavi isključivo prepoznavanjem drugih osoba koje su zaposlene u određenom dijelu organizacije ili u čitavoj organizaciji. Ovo je isplativo samo ako se procjeni da su napadi na fizičkoj razini vjerojatni. Osoba za prepoznavanje ima zadatak upoznati sve zaposlenike i njihova zaduženja te uz dovoljan stupanj obrazovanja predstavlja odličnu zaštitu u borbi protiv napadača koji se ne ustežu od fizičkog pristupa mjestu napada.
- Središnji sigurnosni dnevnik

  Ukoliko se vodi dnevnik o potencijalnim događajima vezanim uz narušavanje informacijske sigurnosti organizacije, moguće je spriječiti daljnje napade socijalnih inženjera. Zaposlenik bi trebao svaki put kada se od njega traži neka potencijalno osjetljiva informacija, kada primi sumnjiv telefonski poziv ili kada se od njega zatraži zaporka, taj događaj zapisati u dnevnik. Tako bi se mogla uočiti pravilnost odnosno prepoznati sustavne napade. Čim se prepozna napad, potrebno je upozoriti sve zaposlenike na napadača i takvom se napadu relativno jednostavno može stati na kraj. U svrhu povećanja efikasnosti, dnevnik se može implementirati kao baza podataka ili grupna aplikacija, ovisno o potrebama i učestalosti unosa zapisa. Takav se sustav mora nadzirati iz jednog središta kako se napadač ne bi mogao neopaženo šetati od jednog odjela do drugog.
- Pravilo povratnog poziva

  Kod osoblja zaduženog za podršku korisnicima poznato je pravilo povratnog poziva. Ono se primjenjuje kada se preko telefona traže zaštićene informacije, a osoba koja ih daje mora prekinuti tekući poziv i inicirati uspostavu poziva prema strani koja je zatražila dotičnu informaciju. Ukoliko se zahtijevani telefonski broj ne nalazi u imeniku tog zaposlenika, očito je posrijedi potencijalno opasna osoba koja je zatražila informaciju i u tom slučaju se podaci ne odaju te se događaj bilježi u dnevnik.
- Ključna pitanja

  Za autentikaciju korisnika koji potražuje potencijalno osjetljiv podatak mogu se koristiti unaprijed dogovorena ključna pitanja. Na taj način se nedvojbeno može odrediti identitet takvog korisnika.

  Jedan od jednostavnijih načina obuhvaća postavljanje triju pitanja koja se zajedno s odgovarajućim odgovorima moraju unaprijed pripremiti. Za legitimnog korisnika davanje odgovora na ta pitanja je trivijalno, ali za nekoga tko nije upoznat s detaljnijim podacima o korisniku davanje točnih odgovora je nemoguće.

  Postavljanje lažnih pitanja je isto jedan od jednostavnih načina provjere sugovornika. Potražitelju potencijalno osjetljivih informacija može se postaviti pitanje npr. vezano uz njegovog sina, a pri tomu zaposlenik posjeduje podatak o tomu da sugovornik nema djece. Ukoliko isti odgovori kako je sve u redu i slično, očito je da se radi o lažnom predstavljanju. Stoga se uočeni pokušaj napada zapisuje u dnevnik.
- Pravilo odgađanja odgovora

  Psiholozi se slažu u činjenici da je čovjeka moguće nagovoriti na izvršavanje nekog potencijalno nedozvoljenog postupka ukoliko ga se izvrgne pritisku ili ukoliko je preopterećen. Najjednostavniji način za borbu protiv ovakvog napada je uvođenje pravila koje tvrdi da za svaki sumnjiv poziv ili zahtjev za osjetljivim informacijama, zaposlenik treba sugovornika ostaviti na čekanju. To usporava razvoj događaja i pribavlja potencijalnoj žrtvi dovoljno vremena za promišljanje o postupcima koje će poduzeti. Tijekom stanke zaposlenik može zabilježiti zahtjev u dnevnik, konzultirati se sa suradnikom ili odabrati način na koji će verificirati sugovornika.

4.7.6. Razina protunapada

Posljednja razina obrane od napada socijalnog inženjeringa je prijava incidenta. Ovaj postupak je ključan budući da sprečava istog napadača u daljnjim napadima. Čim osoba uoči da je napad u tijeku, mora preuzeti inicijativu i u što većoj mjeri razotkriti napadača. Kako bi to bilo izvedivo organizacija

mora definirati pravila koja će zaposlenik primijeniti. Ukoliko nije moguće razotkriti napadača, pravila u najmanju ruku moraju osigurati upozorenje drugih zaposlenika o napadu i potencijalnom napadaču. Ukoliko ne postoji mogućnost prijave incidenta, iz zabilježenog napada se neće moći ništa naučiti i svaki zaposlenik morat će voditi svoju bitku s napadačem, često puta istu kakvu je već netko drugi vodio, a u međuvremenu napadač svakim napadom stječe sve više iskustva i postaje sve efikasniji.
Zato je vrlo važno postojanje osobe koja djeluje na razini cijele organizacije i spremna je u što kraćem roku reagirati na napade, pravovremeno upozoriti sve potencijalne žrtve te im po potrebi dati upute za daljnje reakcije.

5. Zaključak

Napadi temeljeni na socijalnom inženjeringu prisutni su u svim sferama ljudskog života, a osobito u području računalne sigurnosti. Brojni su slučajevi u kojima su napadači laganjem, od legitimnim zaposlenika različitih organizacija otkrivali sigurnosno osjetljive informacije. Nažalost, brojne organizacije ne prepoznaju u dovoljnoj mjeri važnost ljudskog faktora za ukupnu sigurnost svojih organizacija te svu sigurnost temelje samo na različitim sklopovskim i programskim rješenjima. Stoga se u ovom dokumentu nastojalo istaknuti važnost podizanja svijesti o socijalnom inženjeringu kao realnoj opasnosti.

Osim podizanja svijesti, poseban naglasak u dokumentu je postavljen i na mogućnost zaštite. Detaljno je opisan višerazinski način obrane koji, sam za sebe, nije posebno mudar. Ono što je u njemu, ali i u ostalim primjerima sasvim razvidno, a predstavlja zaključak cijele teme, može se svesti u dvije rečenice:

- Sigurnost zasigurno ne leži u metodama obrane već u sustavnom planiranju i razvoju prikladnih strategija.
- Sam proboj mjera osiguranja ne mora nužno biti loša stvar, sve dok je takav proboj predviđen u strategiji i sve dok su korisnici educirani za njeno provođenje.

Suprotno uobičajenom razmišljanju, socijalni inženjering nije isključivo vezan uz računalne sustave. On je prisutan u svim sferama osiguranja. Zbog toga bi problemi opisani u prethodnim poglavljima trebali probuditi interes i u širem krugu čitatelja.

6. Reference

[1] Social Engineering ... Mind Hacking, http://www.cissponline.com/index.php?name=News&sid=2&file=article&pageid=1, listopad 2006.

[2] Sarah Granger: Social Engineering Fundamentals, Part I: Hacker Tactics (http://www.securityfocus.com/infocus/1527) , listopad 2006.

[3] Sarah Granger: Social Engineering Fundamentals, Part II: Combat Strategies (http://www.securityfocus.com/infocus/1533) , listopad 2006.

[4] Malcolm Allen: Social Engineering, A means to violate a computer system, listopad 2006.

[5] David Gragg: A Multi-Level Defense Against Social Engineering, prosinac 2002.

[6] Yves Lafrance: Psychology - A precious security tool, 2004.

[7] Aaron Dolan: Social Engineering, 2004.

[8] Harl: People Hacking - The Psychology of Social Engineering, http://cyberpunk.barzha.com/z/se10.html, listopad 2006.