U OVOM POGLAVLJU

- Šta je socijalni inženjering
- Kakve su posledice socijalnog inženjeringa
- Testiranje pomoću socijalnog inženjeringa
- Zaštita vaše organizacije od socijalnog inženjeringa

Poglavlje 6
Socijalni inženjering

Socijalnim inženjeringom (engl. *social engineering*) iskorišćava se jedna od najslabijih karika u odbrani bezbednosti informacija svake organizacije – ljudi. Socijalni inženjering je zapravo hakovanje osoba, jer podrazumeva zloupotrebu ljudske lakovernosti kako bi se dobile informacije za ostvarivanje lične koristi.

Socijalni inženjering spada u one vrste hakovanja koje je najteže izvršiti, jer treba da budete prilično samouvereni i vešti da bi vas potpuni stranac doživeo kao osobu od poverenja. Od takvog hakovanja ćete se najteže zaštititi, jer su njime obuhvaćena i osobe koje donose odluke o bezbednosti.

U ovom poglavlju ćemo se baviti posledicama socijalnog inženjeringa, vašim sopstvenim tehnikama za testiranje bezbednosti u ovoj oblasti i posebnim merama za odbranu od socijalnog inženjeringa.

Šta je socijalni inženjering

U scenariju socijalnog inženjeringa, zlonamerni napadači se predstavljaju kao druge osobe, kako bi došli do informacija koje bi teško dobili na neki drugi način. Informacije koje su dobili od svojih žrtava koriste za pustošenje mrežnih resursa, krađu ili brisanje datoteka, čak i za korporativnu špijunažu ili neki drugi oblik prevare organizacije koju napadaju. Socijalni inženjering se razlikuje od iskorišćavanja *fizičke bezbednosti*, kao što su špijuniranje preko ramena ili kopanje po smeću, ali ova dva tipa hakovanja su povezana i često se koriste zajedno.

Sledi nekoliko primera socijalnog inženjeringa:

- „**Osoblje za podršku“**, koje tvrdi da mora da instalira zakrpu ili novu verziju softvera na računaru korisnika, nagovara korisnika da preuzme softver i tako dobija kontrolu nad sistemom.
- **„Proizvođači“**, koji tvrde da moraju da ažuriraju računovodstveni ili telefonski sistem organizacije, traže lozinku od administratora i dobijaju neograničen pristup.
- **„Zaposleno lice“**, koje obaveštava službu obezbeđenja da je izgubilo propusnicu za centar podataka, dobija ključeve od obezbeđenja, a time i neovlašćeni pristup fizičkim i elektronskim informacijama.
- **„E-pošta za pecanje“**, koja se šalje zbog prikupljanja identifikatora i lozinki od primalaca, ili zato da bi se na njihove računare instalirao zlonamerni softver. Ovi napadi po svojoj prirodi mogu biti opšti ili ciljani – ovi drugi se ponekad nazivaju podvodni ribolov (engl. *spearphishing*). Ovlašćenja za prijavljivanje ili zlonamerni softver kriminalci koriste za pristup mreži ili intelektualnoj svojini, za šifrovanje datoteka zbog traženja otkupa i slično.

Ponekad se ovakvi napadači predstavljaju kao pouzdani i upućeni rukovodioci ili stručnjaci, a ponekad glume neobaveštene i naivne zaposlene. Mogu da nastupe i kao spoljni saradnici – na primer, IT konsultanti ili radnici službe za održavanje. Socijalni inženjeri vešto se prilagođavaju svojim ciljnim grupama. Za ovako nešto potrebna je posebna vrsta ličnosti, a u ekstremnim slučajevima reč je o sociopatama.

UPAMTITE

Efikasna bezbednost informacija – posebno ona koja je neophodna za zaštitu od socijalnog inženjeringa – često počinje i završava se korisnicima. Druga poglavlja ove knjige sadrže savete o tehničkoj kontroli koja vam može pomoći u borbi protiv socijalnog inženjeringa, ali nemojte zaboraviti da osnovna ljudska komunikacija i interakcija u svakom trenutku imaju veoma važan uticaj na nivo bezbednosti organizacije. Ako napravimo poređenje sa reklamama u kojima se slatkiši opisuju kao „*tvrdi i hrskavi spolja, a mekani iznutra*“, onda taj „tvrdi i hrskavi“ deo predstavlja sloj mehanizama (mrežnih barijera, sistema za sprečavanje upada, filtriranja sadržaja itd.) na koje se organizacije najčešće oslanjaju dok štite svoje informacije. „Mekani“ deo su ljudi i procesi unutar organizacije. Ako „loši momci“ prodru kroz tvrdi sloj, ugroziće unutrašnji sloj koji je najčešće bez zaštite.

Testiranje pomoću socijalnog inženjeringa

U ovom poglavlju imam drugačiji pristup metodologijama testiranja od onoga koji ću prikazati u narednim poglavljima. Socijalni inženjering je i umetnost i nauka. Potrebna je zavidna veština da se predstavite kao stručnjak za bezbednost, što u dobroj meri zavisi od vaše ličnosti i opštih znanja o organizaciji.

SAVET

Ako socijalni inženjering za vas nije prirodno, informacije iz ovog poglavlja da biste o njemu nešto naučili i pronašli najbolji način da se od njega odbranite. Ne ustručavajte se da angažujete treću stranu za ovo testiranje ako tako nešto za vas ima poslovnog smisla.

UPAMTITE

Socijalni inženjering može imati štetne posledice za poslove i reputaciju ljudi, a može da izazove i curenje informacija, naročito kod izvođenja testova pecanjem. Sve dobro isplanirajte i radite pažljivo.

Napade socijalnim inženjeringom možete izvesti na mnogo načina: od toga da uđete na neka vrata i predstavite se kao druga osoba do toga da pokrenete sveobuhvatne kampanje pecanja putem e-pošte. Sve je moguće. Iz tog razloga, a i zato što bi bilo nemoguće opisati sva specifična ponašanja u jednom poglavlju, ovde neću davati uputstva za izvođenje napada socijalnim inženjeringom. Umesto toga ću opisati posebne scenarije za socijalni inženjering koji su bili korisni meni i drugima. Možete da iskoristite neke trikove i tehnike za svoju specifičnu situaciju.

Lice koje nije zaposleno u organizaciji može uspešno da primeni određene tehnike socijalnog inženjeringa, kao što su tehnike fizičkog upada. Ukoliko ove testove sprovodite za svoju organizaciju, biće teško da se predstavljate kao spoljno lice ako vas svi poznaju. Ovaj rizik od prepoznavanja ne mora biti problem u velikim organizacijama, ali ako imate malu i spregnutu kompaniju, ljudi će sve brzo shvatiti.

UPAMTITE

Možete angažovati specijalizovanu kompaniju ili pouzdanog kolegu da izvrši napad socijalnim inžejeringom.

Zašto napadači koriste socijalni inženjering

Napadači koriste socijalni inženjering da bi provalili u sisteme i pristupali informacijama, jer je to obično najlakši način da dobiju ono što im treba. Oni više vole da im neko otvori vrata organizacije, nego da u nju fizički provaljuju i rizikuju da budu uhvaćeni na delu. Bezbednosne tehnologije, kao što su mrežne barijere i kontrole pristupa, neće zaustaviti napadače koji su čvrsto rešili da uspeju.

Mnogi socijalni inženjeri svoje napade izvode polako, da ne bi izazvali sumnju. Oni postepeno prikupljaju male količine informacija i koriste ih da bi formirali što detaljniju sliku o organizaciji koju pokušavaju da prevare. Njihovo najvažnije sredstvo za rad je – vreme. Oni nemaju ništa osim vremena i zato će se potruditi da ga sebi obezbede u dovoljnoj meri kako bi njihovi napadi bili uspešni. Ovakvi napadi mogu se izvoditi i kratkim telefonskim pozivima ili e-poštom. Korišćene metode zavise od stila i sposobnosti napadača. U svakom slučaju, vi ste u lošijoj poziciji.

Socijalni inženjeri znaju da mnoge organizacije nemaju zvanične programe za klasifikaciju podataka, sisteme za kontrolu pristupa, planove za odgovore na incidente niti programe za podizanje svesti o bezbednosti, i koriste ove slabosti.

Oni obično znaju po malo o svemu – kako unutar tako i izvan ciljnih organizacija – jer im takva znanja koriste za ono što rade. Zahvaljujući platformama

društvenih medija kao što su LinkedIn i Facebook, ali i mnogim drugim resursima na mreži o kojima sam govorio u poglavlju 5, svaka informacija potrebna ovakvim napadačima često im je i na raspolaganju. Što više informacija o organizaciji dobiju, lakše im je da se predstave kao zaposlena lica ili druge pouzdane osobe unutar organizacije. Znanje i rešenost socijalnih inženjera omogućava im prednost u odnosu na upravu i zaposlene, koji ne prepoznaju vrednost informacija za koje su ovakvi napadači zainteresovani.

Posledice

Mnoge organizacije imaju neprijatelje koji žele da im stvore probleme socijalnim inženjeringom. To mogu biti aktuelna ili bivša zaposlena lica koja žele osvetu, konkurenti koji žele prednost ili hakeri koji žele da se dokazuju.

Bez obzira na to ko predstavlja uzrok problema, svaka organizacija je izložena riziku – pogotovo ako je u većoj meri prisutna na internetu. Velike kompanije koje obuhvataju više lokacija često su ranjivije zbog svoje složenost, ali i male kompanije mogu biti mete napada. Svako – od recepcionera, preko čuvara službe obezbeđenja do IT osoblja – može biti potencijalna žrtva socijalnog inženjeringa. Osoblje službi za tehničku podršku i službi za informacije posebno je ranjivo, jer su predusretljivost i pružanje informacija sastavni deo njihovog posla.

Socijalni inženjering ima ozbiljne posledice. Budući da je u ovom slučaju cilj napadača da nekog prevari i dobije informacije za ostvarivanje lične koristi, sve je moguće. Delotvornim socijalnim inženjeringom mogu se dobiti sledeće informacije:

- Korisničke lozinke.
- Propusnice ili ključevi za objekat, čak i za sale sa računarima.
- Intelektualna svojina, kao što su specifikacije projekata, izvorni kôd i druga istraživačka i razvojna dokumentacija.
- Poverljivi finansijski izveštaji.
- Privatne i poverljive informacije o zaposlenima.
- Lični podaci za identifikaciju (PII), kao što su zdravstveni kartoni i podaci sa kreditnih kartica.
- Spisak kupaca i planovi prodaje.

Ako bilo koja od navedenih informacija procuri, može doći do finansijskih gubitaka, pada morala zaposlenih i lojalnosti klijenata, čak i problema sa zakonskom i regulatornom usklađenošću. Mogućnosti su neograničene.

Iz različitih razloga, teško je zaštititi se od napada socijalnim inženjeringom. Prvo, o njima ne postoji odgovarajuća dokumentacija. Drugo, ovakve napadače može da ograniči samo nedostatak mašte. Pored toga, teško je obezbediti oporavak i zaštitu posle napada jer postoje brojne metode, a spoljašnji zidovi mrežnih

barijera i sistema za sprečavanje upada pružaju lažni osećaj sigurnosti, čime se problem samo dodatno pogoršava.

Kad je reč o socijalnom inženjeringu, nikada se ne zna sledeća metoda napada. Najbolje što možete jeste da budete na oprezu, razumete motive ovakvih napadača i zaštitite se od najčešćih napada pomoću stalne bezbednosne budnosti u organizaciji. U nastavku ovog poglavlja govoriću o tehnikama za to.

Sticanje poverenja

Poverenje – koje je tako teško steći, a lako izgubiti – predstavlja suštinu socijalnog inženjeringa. Većina ljudi veruje drugima, sve dok zbog situacije ne bude prisiljena na suprotno. Ljudi žele da pomognu jedni drugima, pogotovo nema očiglednog razloga za nepoverenje i ako zahtev za pomoć deluje opravdano. Oni najčešće vole timski rad na poslu i ne shvataju šta se sve može desiti ako otkriju previše informacija nepouzdanom izvoru. To poverenje omogućava da socijalni inženjeri postignu svoje ciljeve. Za sticanje poverenja obično je potrebno vreme, ali veštim napadačima je dovoljno i nekoliko minuta ili sati. Kako im to uspeva?

- **Dopadljivost:** Ko može da odoli prijateljskom ponašanju? Ljubaznost prija svima. Što su ovakvi napadači pristojniji – pod uslovom da u tome ne preteruju – veće su im šanse da dobiju ono što žele. Napad socijalnim inženjeringom često počinje tako što se odnos uspostavlja na osnovu zajedničkih interesa. Napadači obično koriste informacije do kojih su došli u fazi istraživanja, kako bi utvrdili šta žrtva voli i pretvarali se da i oni vole isto. Mogu da pozovu žrtvu telefonom ili se s njom sretnu uživo i da, na osnovu informacija koje su o toj osobi otkrili, započnu razgovor o lokalnim sportskim timovima ili o tome kako je divno ponovo biti samac. Nekoliko dobro izabranih i odmerenih komentara može predstavljati početak zanimljivog novog odnosa.
- **Uverljivost:** Sposobnost uveravanja se delimično zasniva na tome koliko znanja imaju napadači koji koriste socijalni inženjering, kao i na tome koliko su dopadljivi. Oni igraju određene uloge – na primer, predstavljaju se kao novi zaposleni ili kao kolege sa posla koje žrtve još nisu srele. Mogu se čak predstavljati i kao prodavci koji posluju sa organizacijom, a često sebi daju slobodu da utiču na druge. Najčešći trik u napadima socijalnim inženjeringom jeste da se učini nešto lepo za žrtvu, kako bi ona osećala obavezu da uzvrati, ili da se učestvuje u timskom radu organizacije.

Iskorišćavanje odnosa

Kada napadači pomoću socijalniog inženjeringa dobiju informacije od svojih naivnih žrtava, oni nastavljaju da ih navode da im otkrivaju sve više. To rade u direktnom kontaktu, ili putem elektronske komunikacije koju žrtve rado koriste, odnosno tehnologije kojom se žrtva lako navodi da otkrije informacije.

Obmanjivanje rečima i delima

Lukavi socijalni inženjeri dobijaju informacije od svojih žrtava na brojne načine. Često započinju i usmeravaju konverzaciju tako da žrtve nemaju dovoljno vremena da razmisle o onome o čemu govore. Međutim, ako su napadači suviše nepažljivi ili nestrpljivi, može ih odati sledeće:

- Prenaglašeno prijateljsko ponašanje ili entuzijazam.
- Pominjanje imena istaknutih osoba u organizaciji.
- Hvalisanje sopstvenim ovlašćenjima u organizaciji.
- Ukazivanje na negativne posledice ako se njihovi zahtevi ne ispune.
- Ispoljavanje nervoze ako im se postave pitanja – grimase i vrpoljenje, a naročito nevoljni pokreti šaka i stopala (jer je teže svesno kontrolisati delove tela koja su udaljeniji od lica).
- Preterivanje u detaljima.
- Fiziološke promene, kao što su širenje zenica ili promene visine glasa.
- Užurbanost.
- Odbijanje pružanja informacija.
- Dobrovoljno davanje informacija i odgovaranje na nepostavljena pitanja.
- Poznavanje informacija kojima lice izvan organizacije ne bi trebalo da raspolaže.
- Korišćenje načina govora ili žargona zaposlenih u organizaciji, iako je poznato da osoba u njoj nije zaposlena.
- Postavljanje čudnih pitanja.
- Pogrešno napisane reči u pisanoj komunikaciji.

Dobar socijalni inženjer neće na očigledan način ispoljiti navedene reakcije, ali ovi znakovi mogu da pokažu da je reč o zlonamernom ponašanju. Naravno, ako je osoba sociopata ili psihopata, iskustvo sa njima može biti i drugačije. (*Psihologija za neupućene*, 2. izdanje autora Adama Casha [John Wiley & Sons, Inc.] dobar je izvor informacija o takvim složenostima ljudskog uma.)

Socijalni inženjeri često nekome učine uslugu, a odmah zatim tu osobu mole da pomogne njima. Ovakvi trikovi iz oblasti socijalnog inženjeringa veoma dobro funkcionišu. Ovi napadači koriste i nešto što se naziva *obratni socijalni inženjering* (engl. *reverse social engineering*). Često nude pomoć u slučaju da nastane neki problem, a kada problem nakon izvesnog vremena zaista i nastane (često tako što ga izazovu sami napadači), oni pomažu žrtvi da ga reši. Može se desiti da ispadnu i heroji, što im dodatno poboljšava poziciju – mogu odmah da traže protivuslugu od naivnog zaposlenog, što će sigurno i učiniti. Mnogi ljudi padaju u takve zamke.

Igranje uloge zaposlenog je lako. Socijalni inženjer može da nosi sličnu uniformu, lažnu identifikacionu oznaku ili se naprosto oblači kao pravi zaposleni, jer zna da će zbog toga ostali prirodno pomisliti da je i on jedan od njih. Ovakvi napadači se mogu pretvarati i kao zaposleni koji zovu sa spoljne telefonske linije, što

je posebno popularan način za iskorišćavanje osoblja tehničke podrške i pozivnih centara. Napadači znaju da ovi zaposleni rutinski obavljaju zadatke i izgovaraju rečenice koje se ponavljaju.

Obmanjivanje pomoću tehnologije

Tehnologija može mnogo da olakša posao ili ga učini zabavnijim socijalnom inženjeru. Zlonamerni zahtev za informacije često stiže sa računara ili drugih elektronskih uređaja za koje žrtve veruju da mogu da ih identifikuju. Lažiranje imena računara, e-adrese, broja faks uređaja ili mrežne adrese nije teško. U sledećem odeljku biće opisano nekoliko merama protiv ovakvih tipova napada.

Hakeri mogu da vas prevare preko tehnologije slanjem e-poruke u kojoj se od žrtava traže važne informacije. Takvom e-poštom najčešće se šalje hiperveza koja žrtve usmerava na profesionalne veb lokacije, koje izgledaju kao prave i na kojima se „ažuriraju“ informacije o nalogu, kao što su korisnički identifikator, lozinka i broj socijalnog osiguranja. Ovo može da se izvodi i na lokacijama društvenih mreža, kao što su Facebook i Twitter.

Ovaj trik se koristi i u mnogim neželjenim e-porukama i e-porukama za pecanje. Većina korisnika preplavljena je neželjenom poštom do te mere da oni često spuštaju gard i otvaraju e-poruke i priloge koje ne bi trebalo da otvaraju. Ove e-poruke često izgledaju profesionalno i uverljivo, a primaoce navode da – u zamenu za neki poklon – otkriju osetljive informacije. Ovako nešto se može primeniti kada haker, koji je već provalio u mrežu, šalje poruke ili pravi lažne iskačuće prozore na internetu. Isti trikovi se primenjuju u trenutnom razmenjivanju poruka ili razmeni poruka preko pametnih telefona.

U nekim poznatim incidentima, hakeri su svojim žrtvama slali e-poruke sa zakrpom za koju se tvrdilo da ju je napravio Microsoft ili neki drugi poznati proizvođač. Međutim, takva poruka nije ono što korisnik misli – poslao ju je haker koji želi da korisnik instalira zakrpu, a sa njom i trojanski program koji krade lozinke ili pravi tajna vrata za računare i mreže. Ova tajna vrata hakeri koriste za hakovanje sistemâ organizacije, ili da bi računare žrtava (poznate pod nazivom *zombiji*) koristili kao odskočnu dasku za napade na druge sisteme. Čak i virusi i crvi mogu da izvode napade socijalnim inženjeringom. Na primer, crv LoveBug uverava korisnike da imaju tajne obožavaoce. Kada žrtve otvore e-poruku, već je prekasno za sve – računari su im zaraženi, a od tajnih obožavalaca ni traga ni glasa.

Mnoge računarske taktike socijalnog inženjeringa mogu se sprovoditi anonimno sa interneta preko proksi servera, anonimizatora, anonimnih servera za prosleđivanje pošte i osnovnih SMTP servera koji imaju otvoren relej. Kada se ljudi odazovu na zahtev za pružanje poverljivih ličnih ili korporativnih informacija, izvorima ovih napada socijalnog inženjeringa nemoguće je ući u trag.