OUCH!

U OVOM BROJU...

- Šta je socijalni inženjering
- Detekcija i sprečavanje napada socijalnim inženjeringom

Socijalni inženjering

Uvod

Uobičajena zabluda koju većina ljudi ima o sajber napadačima je da oni koriste samo veoma napredne alate i tehnike da bi hakovali nečiji računar ili korisnički nalog. Ovo jednostavno nije tačno. Sajber napadači su naučili da je često najlakši način da ukradu vaše informacije, hakuju vaš nalog ili zaraze vaše sisteme taj da vas jednostavno zavaraju (obmanu) da napravite grešku. U ovom tekstu naučićete kako ovi napadi, poznati kao socijalni inženjering, funkcionišu i šta možete da uradite da biste se zaštitili.

Gost urednik

James Lyne (**@jameslyne**) je sertifikovani SANS instruktor i globalni rukovodilac istraživanja u kompaniji Sophos. On dekomponuje i obrnutim inženjeringom analizira najnovije i najveće prevare sajber kriminalaca. On je takođe i autor SANS-ovih obuka Metasploit (SEC580) i Social Engineering (SEC567).

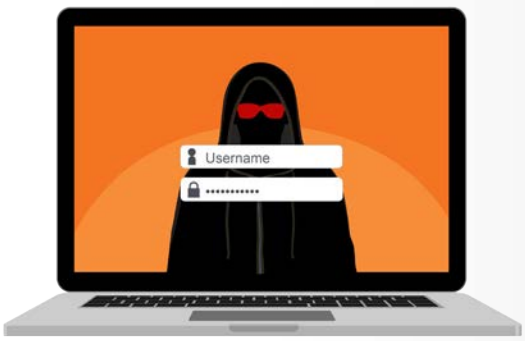
Šta je socijalni inženjering

Socijalni inženjering je psihološki napad u kojem vas napadač obmane da uradite nešto što ne bi trebalo da uradite. Koncept socijalnog inženjeringa uopšte nije nov, on postoji hiljadama godina unazad. Pomislite na razne prevarante ili varalice, to je u osnovi ista ideja. Ono što današnju tehnologiju čini mnogo efikasnijom za sajber napadače je da ne možete fizički da ih vidite, oni mogu lako da se pretvaraju da su bilo ko ili bilo šta i da ciljaju milione ljudi širom sveta, uključujući i vas. Dodatno, napadi socijalnim inženjeringom mogu da zaobiđu mnoge tehnološke mere zaštite. Najjednostavniji način da razumete kako ovi napadi funkcionišu i da se zaštitite od njih je da se upoznate sa dva primera iz stvarnog sveta.

Primili ste telefonski poziv od nekoga ko tvrdi da je iz kompanije za računarsku podršku, vašeg provajdera internet usluga ili Majkrosoftove tehničke podrške. Osoba koja vas je pozvala objašnjava vam da vaš računar aktivno skenira Internet, oni veruju da je računar zaražen i dobili su zadatak da vam pomognu da zaštitite vaš računar. Oni zatim koriste razne tehničke termine i niz zbunjujućih koraka kako bi vas ubedili da vam je računar zaražen. Na primer, mogu da vas pitaju da proverite da li imate određene fajlove na vašem računaru i da vas upute kako da ih pronađete. Kad locirate ove fajlove, pozivalac vas uverava da su ovi fajlovi dokaz da je vaš računar zaražen, dok u realnosti ovi fajlovi predstavljaju uobičajene sistemske fajlove koji se nalaze na skoro svakom računaru u svetu. Nakon što vas ubede da je vaš računar zaražen, oni vas onda pritiskaju da kupite njihov bezbednosni softver ili da im dozvolite udaljeni pristup vašem računaru kako bi mogli da ga poprave. Međutim, softver koji oni prodaju je u stvari maliciozni program. Ako kupite i instalirate ovaj softver ne samo da su

Socijalni inženjering

vas prevarili da zarazite vaš računar, već ste im i platili da to urade. U slučaju da im dozvolite da udaljeno pristupaju vašem računaru, oni će preuzeti kontrolu nad njim, ukrasti vaše podatke ili ih prodati



Zdrav razum je vaša najmoćnija odbrana za otkrivanje i zaustavljanje većine napada socijalnim inženjeringom.

Drugi primer je napad putem elektronske pošte poznat kao „CEO prevara“, koji se najčešće događa na poslu. Ovo je situacija kada sajber napadač istraživanjem vaše organizacije na Internetu sazna imena vaših pretpostavljenih ili kolega. Napadač zatim pripremi mejl koji izgleda kao da je od te osobe i pošalje vam ga. U mejlu se traži da hitno preduzmete neku akciju, kao što je prenos novca na neki račun ili slanje osetljivih informacija o zaposlenima. Veoma često ovi mejlovi koriste navodnu hitnost situacije kao razlog za zaobilaženje standardnih bezbednosnih procedura, npr. može da se zahteva da pošaljete vrlo osetljive informacije na privatni nalog na @gmail.com. Ono što ciljane napade poput ovog čini tako opasnim je činjenica da sajber napadači unapred obave istraživanje. Pored toga, tehnološke mere zaštite kao što su antivirus programi ili fajervoli ne mogu da detektuju ili spreče ove napade jer oni ne koriste maliciozne programe ili linkove.

Imajte na umu, napadi socijalnim inženjeringom poput ovih nisu ograničeni samo na telefonske pozive ili elektronsku poštu; oni mogu da se pojave u bilo kojoj formi uključujući i tekstualne poruke na vašem telefonu, putem društvenih mreža ili čak uživo. Ključno je da znate na šta da obratite pažnju, sami ste sebi najbolja zaštita.

Detekcija i sprečavanje napada socijalnim inženjeringom

Na sreću sprečavanje ovakvih napada je jednostavnije nego što mislite – zdrav razum je vaša najbolja odbrana. Ako vam nešto izgleda sumnjivo ili vam ne deluje u redu, to može biti napad. Najčešći znakovi koji ukazuju da je u pitanju napad socijalnim inženjeringom su:

- Neko stvara izuzetan osećaj hitnosti pokušavajući da vas prevari da napravite grešku.
- Neko vam traži informaciju kojoj ne bi trebalo da ima pristup ili bi već trebalo da je zna.
- Neko vam traži vašu lozinku, nijedna legitimna organizacija vam to nikad neće tražiti.
- Neko vrši pritisak na vas da zaobiđete ili ignorišete bezbednosne procedure kojih bi trebalo da se pridržavate na poslu.

Socijalni inženjering

- Nešto je previše dobro da bi bilo istinito. Na primer, obavešteni ste da ste dobili novac ili iPad u nagradnoj igri, iako nikad niste učestvovali u toj nagradnoj igri.
- Primili ste neobičan mejl od prijatelja ili kolege koji sadrže formulacije koje uopšte nisu uobičajene za njih. Sajber napadač je možda hakovao njihov nalog i pokušava da vas prevari. Da biste se zaštitili proverite ove zahteve, tako što ćete stupiti u kontakt sa vašim prijateljima korišćenjem drugih metoda za komunikaciju, uživo ili preko telefona.

Ukoliko sumnjate da neko pokušava da vas prevari ili obmane, nemojte komunicirati više sa tom osobom. Ako je napad povezan sa poslom, obavezno ga odmah prijavite vašoj IT podršci (help desk) ili timu koji se bavi informacionom bezbednošću. Zapamtite, zdrav razum je često vaša najbolja odbrana.

Saznajte više

Prijavite se na OUCH! mesečni bilten za podizanje svesti o bezbednosti informacija namenjen svima, pročitajte prethodne brojeve OUCH!-a i saznajte više o SANS-ovim rešenjima za unapređenje svesti o bezbednosti informacija na našoj internet prezentaciji securingthehuman.sans.org/ouch/archives.

Verzija na srpskom

Telekom Srbija kao društveno odgovorna telekomunikaciona kompanija pomaže prevođenje i distribuciju ovog biltena kako bi se unapredila svest korisnika informaciono-komunikacionih tehnologija o bezbednosti informacija.

Dodatne informacije

Sajber pecanje:	https://securingthehuman.sans.org/ouch/2015#december2015
CEO prevara:	https://securingthehuman.sans.org/ouch/2016#july2016
Ransomware:	https://securingthehuman.sans.org/ouch/2016#august2016
Arhive OUCH biltena:	https://securingthehuman.sans.org/ouch/archives

Redakcija: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis Cheryl Conley
Preveli: Dragan Ristić i Gordana Živanović