

Da li ste žrtva tzv. Socijalnog inženjeringa (Social Engineering)?

Pojam Social Engineering je hakerski izraz za postupak navođenja žrtve da oda poverljive podatke (različita korisnička imena, šifre, mail adrese...) koji mogu biti kasnije iskorišćeni za razne vrste prevara i zloupotreba.

Nijedna postojeća softverska tehnologija nije u stanju da Vas zaštiti od prevara ove vrste, zato što „loši momci“ igraju na kartu ljudske nemarnosti, nepažnje ili poverenja kako bi ih namamili da odaju poverljive podatke. Jedan od starih i dugo prisutnih trikova ove vrste u svetu je kada kvazi korisnik pozove oficijelnu službu za tehničku pomoć, recimo u svojoj banci, i pretvarajući se da je legitiman korisnik zatraži da mu se ponovo saopšti šifra za pristup sistemu koju je nehотиčno zaboravio. Današnje službe za tehničku pomoć već odavno ne padaju na ovakve trikove i sa te strane možete biti sigurni. Da bi ste se zaštitili danas morate biti oprezni na tzv. SPIM (Spam Over Instant Messaging) kao i na tzv. "Pecanje" (*hakera termin – Phishing [fish'ing] (n.) The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. Phishing, also referred to as brand spoofing or carding, is a variation on "fishing", the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting).*

Pecanje i SPIM

Loši momci koji se bave "Pecanjem" su veoma talentovani u kreiranju mail poruka koje podsećaju na oficijelne poruke vašeg internet provajdera, banke, osiguravajućeg društva ili neke druge kompanije od poverenja. Mail poruka je vešto sastavljena da podseća na zahtev odabranoj žrtvi da potvrdi ponovnim unosom, svoje podatke o parametrima za pristup sistemu (korisničko ime, šifra itd) jer je došlo do tehničkih problema ili nečega još mističnijeg. Varijacije na ovu temu su da se žrtva eventualno preusmerava na neku Web adresu na kojoj treba da popuni formular u skladu sa zahtevom i kada na kraju popunjavanja formulara klikne na predviđeno dugme za slanje podataka obično je dočeka poruka o grešci tipa (Server Error i sl.) i mogućnost da se vrati na pravu oficijelnu stranicu kompanije koja je korišćena za prevanu. U međuvremenu vredne informacije su se prosledile "Pecarošu" a poruka o grešci je namerno poslata.

SPIM napadi su slični "Pecanju" ali se upućuju preko IM (Internet Messaging). Ovakav metod je takođe veoma opasan jer je obuhvaćena grupa potencijalnih žrtava veoma velika i prema matematici velikih brojeva garantovano donosi rezultate. Mail poruke mogu biti veoma raznolike pa čak i da sadrže istinite informacije o nekom opasnom virusu koji se nezadrživo širi Internetom. Ključni detalj u ovakvim mailovima je savet da obavezno kliknete na navedeni link ako biste proverili da li je vaša radna stanica bezbedna od najnovijeg virusa. Tu se vraćamo na već poznati scenario o sakupljanju važnih informacija o korisnicima i njihovim kompanijama i potencijalnom nesvesnom preuzimanju programčića koji automatski podešavaju određene parametre na vašoj mašini i dozvoljavaju anoniman pristup napadaču. Ovakvi programčići su poznati kao Trojan Horse Downloader.

Povećanje svesti kod korisnika

Za uspešnu borbu protiv Socijalnog inženjeringa, ključna stvar je eliminacija ljudskog faktora ili njihova edukacija. Najčešće, eliminacija ljudskog faktora nije moguća zbog specifičnosti IT resursa pa je faktor edukacije jedino i ključno rešenje. Naprimer, veliki broj kompanija koriste razne samostalno kreirane aplikacije koje resetuju šifre koje su u opticaju i dodeljuju nove, što je jedan od vidova borbe protiv gore pomenutih metoda krađe poverljivih podataka, ili organizuju prezentacije gde se korisnici edukuju kako da utvrde tačan izvor linka na koji žele da kliknu ili da vide pravi izvor maila koji žele da pročitaju.

Edukacija IT osoblja

Edukacija IT osoblja je isto toliko važna kao i edukacija korisnika i ključna je stvar za temeljnu borbu protiv malicioznih pojava. U razvijenom IT svetu formirane su specijalne ustanove koje se bave ovom problematikom i koje donose propise čiji je cilj povećanje sigurnosti podataka. Ove propise moraju da sprovedu svi koji su uključeni u sistem osiguranja informacija kao jedini način da se predupredi šteta nastala zloupotrebom poverljivih informacija saljupljenih kroz maliciozne aktivnosti u Internet komunikacijama. Daćemo primer SAD koje su najdalje otišle na ovom planu kroz funkcionisanje ustanova kao što su Federal Financial Institutions Examination Council (FFIEC), Federal Deposit Insurance Corporation (FDIC) koje su ključne za bezbednost nacionalnog bankarskog sistema.