Kako se odbraniti od napada hakera?

Ni najbolji ni najefikasniji zaštitni softver ne može mnogo toga da uradi po pitanju opasnosti najveće od svih – samog korisnika. Kaže se da je zaštita onoliko dobra koliko je dobra njena najslabija karika. A najslabija karika svakog sistema je najčešće čovjek.

Socijalni inžinjering predstavlja vještinu varanja i ubjeđivanja drugih ljudi da daju informacije, novac ili neka druga dobra, koja inače nikako ne bi dali, ili, jednostavno, da urade nešto što haker želi, a što oni u normalnim okolnostima nikada ne bi učinili. Suština ove vještine je u lažnom predstavljanju, bilo da se ono odvija u ličnom kontaktu ili putem telefona, faksa, interneta ili nekog drugog elektronskog sredstva.
Cilj napadača uglavnom nije žrtva sama, već neki resursi koji su napadaču interesantni, kao što je, na primjer, mogućnost pristupa nekom serveru sa podacima . Staro je pravilo da je u bilo kom sistemu bezbjednosti čovjek, i samo čovjek, najslabija tačka. A to je upravo ono mjesto gde se socijalnim inžinjeringom djeluje, tako da primjena čisto tehničkih sredstava za zaštitu ne pomaže.

Napad socijalnim inženjeringom priprema se strpljivo, često jako dugo. Kao i u klasičnim oblicima hakerskih napada, priprema započinje istraživanjem. Naime, u napad se ulazi s jasnim motivom, napadač dobro poznaje kakvu informaciju treba. Kako bi tačno odredio mjesto gdje se nalazi takva informacija, napadač mora prikupiti što je moguće više podataka o firmi, njenim odjelima, internom ustroju, internim telefonskim brojevima, godišnjim odmorima, osobama koje bi se mogle iskoristiti u napadu.

Priprema napada rijetko obuhvaća i fizički pristup napadača u prostore žrtve. Napadač će takve izuzetke upotrijebiti samo da bi po ladicama ili monitorima pronašao zapisane lozinke koje će zatim iskoristiti na neki drugi način. Napadač će češće obilaziti otpadne kontejnere i po nepažljivo odbačenim listama, korisničkim priručnicima, uputama o radu i sličnoj dokumentaciji pronaći podatke koji ga zanimaju ili barem podatke koji će mu pomoći u nastavku napada.

Glavni dio napada socijalnim inženjeringom vodi se telefonom. Napadač će veoma rijetko direktno nazvati žrtvu napada i samo uz jedan poziv zatražiti potrebnu informaciju - korisničko ime i lozinku. Napadač će prije toga pažljivo izgraditi identitet kojim će se predstaviti žrtvi napada. Cilj je postići uvjerljivost i bliskost. Napadač će veoma dobro iskoristiti činjenicu da je većina ljudi sklona pružiti pomoć osobi u nevolji, naročito kada osjete sažaljenje prema situaciji u kojoj su i sami nekad bili ili u kojoj bi se mogli naći. U takvim situacijama napadač će se predstaviti kao službenik iz drugog odjela kojem sistem ne radi, a mora hitno obaviti neki posao, pa će žrtvu zamoliti da potraži određenu informaciju u bazi podataka Ili će napadač zamoliti žrtvu da određeni dokument pošalje faksom, jer se nalazi izvan kancelarije Ili će zamoliti za lozinku za pristup serveru, jer je na putu a važna ponuda mora biti ujutro gotova.

Evo par jednostavnih koraka kojih bi svako trebao da se pridržava da ne postane žrtva online prevare:

1. Nikada nemojte otvarati attachmente u mailu od nepoznatih izvora.
2. Nikada nemojte pokretati program ako nemate poverenja u njegov izvor pogotovo ako je downloadovan sa interneta.
3. Pravilno koristite i čuvajte svoje lozinke, i nemojte ih nikad ostavljati na papirićima oko stola ili zaljepljene na monitoru.
4. Uvijek postupajte oprezno kod poziva od nepoznatih lica, i nikad ne dajte pristupne šifre preko telefona.