UVODNA REČ

RELJA JOVIĆ

Bezbednost, laž i socijalne mreže

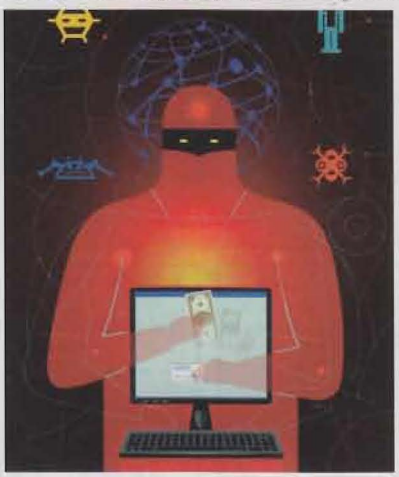
AKO JE BEZBEDNOST ljudski, procesni i tehnološki problem, onda su ljudi najslabija karika u tom lancu. To objašnjava zašto su učestali napadi takozvanim socijalnim inženjerstvom.

U obraćanju učesnicima konferencije LANDesk, održane nedavno na Floridi, Kevin Mitnik je upozorio da je u kompanijama danas prva meta napadača služba za pružanje pomoći korisnicima, koja ima pristup važnim informacijama u sistemu. Haker otkriva ime nekog radnika kompanije i poziva službu s obrazloženjem da je izgubio ili zaboravio lozinku, a pravi cilj je da sazna koje će podatke služba za pružanje pomoći zatražiti radi provere identiteta pozivaoca. Napadač potom prekida razgovor s unapred pripremljenim izgovorom i kreće u potragu za informacijama koje su od njega tražene.

Mitnik je na pomenutom skupu pozvao jednog dobrovoljca iz publike i pomoću kombinacije besplatnih i jeftinih mrežnih usluga, za nekoliko minuta uspeo da otkrije sve podatke o toj osobi. „Kompanije koje koriste ovakva pitanja za proveru identiteta svojih radnika to nipošto ne bi trebalo da čine", upozorio je on. „To bi trebalo da bude dinamičan sistem."

Poznati haker je otkrio kako je socijalnim inženjerstvom uspeo da ukrade izvorni kôd za Motorolin telefon Star Tak čim se pojavio na tržištu. Na putu od kancelarije do kuće, pozvao je centralu Motorole i zatražio da razgovara s vodećim programerom. Lažno se predstavio kao radnik odeljenja za istraživanje i razvoj te kompanije i posle dugog „šetanja" su ga ipak povezali s pomoćnicom tražene osobe. Ona je pronašla datoteke što ih je Mitnik tražio i uz njegovu pomoć i smernice, pokušala da ih protokolom za prenos datoteka (FTP) pošalje na anoniman nalog, ali je pokušaj propao zbog određenih internih bezbednosnih ograničenja.

Pre nego što je uspeo i da se pobuni, osoba s druge strane ga je zamolila da sačeka dok ona porazgovara s kolegama



zaduženim za zaštitu sistema. Dobila je uputstva za zaobilaženje posredničkog servera i uspela da pošalje datoteke – sve je trajalo dvadesetak minuta. „Ljudi su više nego spremni da pomognu", kaže Mitnik, i to je ključno u njegovom prvom predlogu za borbu protiv ovakvih hakerskih napada: radnicima se mora pokazati kako se ti napadi izvode i šta je sve izloženo opasnosti. Neophodno je tome prilagoditi i norme ljubaznosti. „Sasvim je ispravno reći 'ne' kada neko od vas zatraži osetljive ili poverljive podatke", dodao je on. Uostalom, rezultati istraživanja pokazuju da će 35 do 70 procenata osoba odati svoje korisničko ime i lozinku anonimnom pozivaocu koji tvrdi da je iz informatičkog odeljenja. Možda bi obrazovanje zaposlenih trebalo da bude vaše sledeće veliko ulaganje u oblasti bezbednosti i zaštite mada je nabavka naprednog sistema za zaštitu od curenja podataka poput sistema InfoWatch (koji se odnedavno može nabaviti i kod nas) najbolje rešenje. Kada se jednom postavi, ovaj sistem sprečava zaposlene da slučajno ili namerno pošalju ili kopiraju „osetljive" informacije.

Društvene mreže, kao virtuelne zajednice, egzistiraju u mrežama ravnopravnih računara (P2P), a pristup sredstvima, kapacitetu i građi obavlja se preuzimanjem softvera.

Već postoji mnoštvo Web lokacija koje pružaju usluge društvenog umrežavanja, između ostalih i MySpace.com, Tagworld, Technorati i Bebo. Na tim lokacijama se posetiocima nude pričaonice, odeljci za besplatno postavljanje sadržaja, prostor za prikazivanje TV programa, mrežni dnevnici i sl. To je korak napred u odnosu na samostalne pričaonice ili mrežne dnevnike, jer se omogućava veća interaktivnost – prava mesta za postavljanje ličnih fotografija, informacija, filmova i trenutnu razmenu poruka. Međutim, osnovni pristup virtuelne zajednice je u velikoj meri podložan zloupotrebi, a nisu ni sve Web lokacije dovoljno zaštićene. Korisnici koji pristanu na „pravila" virtuelne zajednice i razmenjuju datoteke, preuzimaju softver i prosleđuju informacije izlažu se nepotrebnom riziku – ono što nalikuje tehnički privlačnom i prefinjenom načinu za digitalnu interakciju predstavlja veliku potencijalnu opasnost. ■

Relja Jović je glavni i odgovorni urednik časopisa Mikro. *Njegove uvodne reči pročitajte na adresi www.mikro.co.yu/arhiva/relja.*