Korisnik u fokusu cybernapada

Prema predviđanjima, tržište računalno-sigurnosnog softvera u 2007. godini iznosit će oko 9,1 milijardu dolara. Samo u regiji EMEA (Europa, Srednji Istok, Afrika) tržište je vrijedno oko 2,4 milijarde eura. Dodajmo ovim brojkama vrijednost raznoraznih hardverskih rješenja i sijaset računalnoj sigurnosti orijentiranih usluga (primjerice: security monitoring, device management, vulnerability scanning, active response, log management, email and web scanning, DDoS prevention, security consulting) i ukupna vrijednost industrije računalne sigurnosti dostiže iznos i do 100 milijardi dolara. Usprkos tome, ekonomski gubici od cyberkriminala u rapidnom su porastu. Štoviše, prema nekim statistikama, cyberkriminal postaje jedna od najprofitabilnijih grana organiziranog zločina, bok uz bok ilegalnoj trgovini drogom. S druge strane, sve više djelatnosti ovisi o računalima, pa tako postaje nemoguće posuditi knjigu u knjižnici ili podići film u videoteci u slučaju tzv. „pada sustava“, a o nekakvom plaćanju računa u banci da i ne govorimo.

Postavlja se pitanje: ako je industrija računalne sigurnosti toliko napredovala, zašto su korisnici i dalje u iznimno velikoj opasnosti? Odgovor leži u tzv. najslabijoj karici u lancu računalne sigurnosti, a to je sam korisnik. Osim što je čovjek kao prosječni korisnik računala u računalno-sigurnosnom smislu napredovao bitno manje od napretka koji su iskazala osnovna računalno-sigurnosna rješenja poput antivirusnih alata, vatrozidova i sl., današnja je sveopća prisutnost računala uz maksimalnu jednostavnost korištenja uzrokovala i to da se računalima koriste i oni koji za to definitivno nisu adekvatno obrazovani i osposobljeni. Kvalitetan softver i napredna računalno-sigurnosna rješenja postaju sve veća prepreka u ostvarivanju kriminalnih ciljeva i cyberkriminalci sve češće posežu za dobrim staromodnim prijevarama koje prenešene iz realnog svijeta nimalo ne gube na učinkovitosti; dapače, mnogi aspekti tih staromodnih prijevara čak su jednostavniji i efikasniji nego prije.

Ovakve vrste napada skupnim imenom nazivamo socijalni inženjering. Socijalni inženjering obuhvaća pojmove poput phishinga, pharminga, hoaxa, krađe identiteta, online prijevara, scama i sl., a interes korisnika pobuđuje se obećanjima o brzom mršavljenju, besplatnoj pornografiji, jeftinim lijekovima, velikim dobicima na lutriji, povoljnim kupovinama dionica itd. Jedan od najpoznatijih hakera današnjice, Kevin Mitnick, izjavio je da je u svojim pothvatima koristio tehničke, kao i netehničke metode za ostvarivanje neovlaštenog pristupa, ali danas drži seminare o socijalnom inženjeringu po Americi i autor je knjige „The Art of Deception: Controlling the Human Element of Security“ čime jasno daje do znanja koji je vektor napada atraktivniji. Štoviše, postoji konkretna prednost napada koji se temelje na socijalnom inženjeringu, a to je da funkcioniraju jednako bez obzira na operacijski sustav, hardversku platformu ili primijenjena računalno-sigurnosna rješenja, što znači da su primjenjivi na najveći mogući broj korisnika.

Cilj je ovog predavanja pokazati neke od metoda kojima se cyberkriminalci sve više okreću u potrazi za lakom zaradom, a koje u fokusu imaju upravo korisnika računala kao danas najlakši i najjednostavniji način za ostvarivanje uspješnog napada, odnosno pokazati da je danas upravo čovjek najslabija karika u lancu računalne sigurnosti. Iako ove vrste napada u Hrvatskoj još nisu poprimile zabrinjavajuće razmjere, izolirani primjeri dokazuju da je priključak svjetskim trendovima tek pitanje dana. Za razliku od tradicionalnih računalno-sigurnosnih prijetnji protiv kojih se uspješno braniti možemo adekvatnim tehnološkim mjerama, zaštita od socijalnog inženjeringa u softverskom ili hardverskom obliku ne postoji, te je jedini pravilan put do zaštite edukacija korisnika kroz upoznavanje s postojećim

prijetnjama, prikaz načina na koji one funkcioniraju i primjenu metoda kojima se možemo obraniti od tih prijetnji.