“DRUGA STRANA” SOCIJALNIH MREŽA

Jasmin Ćosić*, Zoran Ćosić**

*MUP Unsko-sanskog kantona, Bihać, Bosna I Hercegovina

** STATHEROS,d.o.o, Kaštel Stari, Hrvatska

jascosic@bih.net.ba

zoran.cosic@statheros.hr

Sažetak

Socijalne mreže kao što su Facebook, Twitter, MySpace, FriendFinder, Classmates su postale planetarno popularne, a projektirane i dizajnirane su kako bi pomogle ljudima da „budu i ostanu u kontatku“. Broj korisnika interneta je još poodavno premašio cifru od 1 milijarde, a barata se podacima da je danas čak svaki drugi korisnik unutar svoga cyber života čest gost ili član i neke od socijalnih mreža. U radu je prikazana „druga strana“ medalje i opasnosti koje sobom nosi nekotrolisan pristup socijalnim mrežama.

1. On-line socijalizacija

Ideja socijalnih mreža je nastala rastom i popularizacijom interneta, te masovnijim korištenjem od strane tzv. nadolazeće mlađe generacije. Danas je na internetu prisutno preko 200-tinjak socijalnih web site-ov. Facebook danas broji preko 400 miliona aktivih korisnika, od kojih 50% svaki dan posjećuje svoj profil, prosječan broj prijatelja (da ima i ta mjera) je 130, 6 milijardi minuta se svaki dan provede na facebooku [1] . Slična situacija je sa MySpace koji broji preko 300 miliona korisnika [2]. Twitter ima mnogo manji broj korisnika ali je u 2009.godini je proglašen kao sajt sa nabržim rastom, dok je broj članova porastao za preko 1800 % [3] . Više od 2/3 korisnika interneta je registrirano na neki od ovih servisa. Od nekakvih prvih verzija mreža, koje su prvenstveno bile namjenjeno za on-line druženja, ponovno uspostavljanje ranije prekinutih veza te socijalizaciju, danas je njihova nakana dobila jednu sasvim drugu dimenziju. Da li ste ikada razmišljali o tome koliki je vaš stepen privatnosti (ukoliko je uopće imate) od kada ste se registrirali na neki od ovih servisa, dodali nekoliko desetina (pa i stotina) tzv. „prijatelja“, razvili mrežu do besvijesti. Ovdje ne treba zaboraviti činjenicu da „*prijatelj moga prijatelja meni može biti i neprijatelj*“.

2. Opasnosti koje sobom nose socijalne mreže [4]

Pored opasnosti kao što su gubljenje identiteta, klasične internet prijevare, pljačke, socijalni inženjering i sl. problem sa kojim se danas susreću stručnjaci za sigurnost informacijskih sustava je tzv. nekontrolisan pristup uposlenika ovim web servisima. Porazno zvuči podatak da su na serverima Facebook-a, Twittera, MySpace-a često logirani ne samo mladi ljudi željni druženja, upoznavanja i avantura, nego i uposlenici u korporacijama i to u radno vrijeme ! Prema nekim istraživanjima, uposlenici u javnim korporacija se itekako uključuju u ovakve mreže, i čak svaki 7-mi korisnik je konstantno *logiran* na ovakav jedan server tokom radnog

vremena. Ovo olakšava posao *„fisherima“*, *„hackerima*“, *„crackerima“* i ostalim prevarantima na internetu da dođu do ličnih podataka ovog profila ljudi ali i informcija o firmi u kojoj je eventualna žrtva uposlena. Pored toga što sebi možete donijeti mnogo problema i muka nekontrolisanim „aktivnsotima“ po socijalnim mrežama, sljedeći problem koji se veoma često javlja je kompromitiranje informacijskog sustava , te narušavanje sigurnosti IS-a, te time zadavanje mnogo muka administratorima i menadžerima za sigurnost u poduzećima i velikim korporacijama. Gubljenje vremena na socijalnim mrežama u radno vrijeme pored pojma koji se označava kao „*krađa procesorskog vremena*“ , utiče i na ranjivost IS-a time što se putem nekoliko stotina AJAX ili MASHUP aplikacija koje se vrte po ovim sajtovima, sustav čini ranjivim na napade. XSS, CSRF, SQL injection i ostale ranjivosti su problemi koje sigurnostne stručnjake muče već nekoliko godina [5]. Prema SOPHOS-u korporacije su žrtve *malware-a, spama, phishinga* najviše kroz socijalne mreže i posjećivanje profila koji su kreirani samo sa tim ciljem. Drugi problem je tzv. „socijalni inženjering“ koji je opasnost broj 1 u svijetu. Footprinting, istraživanja, ispitivanja uposlenika poduzeća o običajima u poduzeću,otkrivanje nekakvih poslovnih tajni o poduzeću, postala je sasvim normalna pojava na socijalnim mrežama. Stvari se dodatno kompliciraju i dobijaju novu dimenziju nastaje kada se pređe granica i kada «on-line» postane «off-line». Tada se narušava kako fizička sigurnost IS-a, tako i osobna sigurnost – privatnost . Šta to u biti znači ? Korisnici socijalnih mreža najčešće pišu šta rade, šta im je na umu, gdje planiraju i kada planiraju na putovanja, tko su im prijatelji. Novu dimenziju svemu daje i multimedija, te objavljivanje fotografija, video uradaka, sa privatnim podacima od imovine sa kojom se rapolaže, članovima obitelji , pa do slika interijera kuće ili stana i druge pokretne ili nepokretne imovine ? U ovome su šansu naravno vidjeli kriminalci, te počeli koristiti blagodeti koje im je ponudila IKT kako bi si olakšali posao. Okrivanje i praćenje žrtvi postalo je trivialno. Prate se socijalne mreže, otkrije se eventualna žrtva, pronađu potrebni podaci, putem raspoloživih web servisa (*Google Earth* npr.) pronalazi se lokacije, zatim (*Google Street* zašto da ne*)* uža lokacija sa eventualnim slikama (koje mogu biti veoma svježe), te se time omogući izrada detaljnih skica i planova. On-line kriminalci su se već duže vrijeme počeli grupirati u skupine na socijalnim mrežama i čak počeli djeliti ,razmjeljivati i prodavati ove informacije. *Cyberstalkeri* pronalaze svoje žrtve najviše putem socijalnih mreža, te im onda putem ovih mreža i zaraženih profila šalju spam, malware, uznemiravaju ih na raznorazne načine, koristeći e-mail koji je registriran na ovim mrežama. Najčešće vrše istraživanja tko ste, što radite, gdje živite, kakve su vam navike i sl. Kada ih zainteresirate , oni prelaze u off-line napade što dobija sasvim novu dimenziju, uznemiravanja se mogu nastaviti putem telefona, vandalizmima, tradicionalnom poštom i sl. Cilj je «izluditi žrtvu» i time izvući od nje određene informacije.

3. Na kraju

Facebook i socijalne mreže su postale dio naše (ne)kulture. Njima su neminovno stigle i nove potencijalne prijetnje. Naravno, blagodeti koje nam nude socijalne mreže se nemožemo (i ne želimo) odreći ali se barem možemo pridržavati nekoliko bitnih stvari:

- Nesmije se zaboraviti da je zaporka „prava crta obrane“, stoga je zaporke potrebno pravilno upotrebljavati, često mjenjati, i treba da budu duge barem 12 znakova (kombinacija slova, brojeva i specijalnih znakova- FaC3800K$$lo).

- Potrebno je definirati granice i podvući crtu gdje je granica privatnosti i sigurnosti.
- Dobro paziti što se dijeli i što piše po socijalnim mrežama. Danas je veoma teško ukloniti nešto što je objavljeno na internetu i ako se nekada uradi nešto neprikladno i to napiše na zidu, tragovi će uvijek ostati prisutni.
- Upamtite tko su vam zapravo prijatelji u stvarnom životu i činjenicu da „*prijatelji vaših prijatelja*“ veoma lako mogu biti (ili postati) vaši neprijatelji.
- Prije nego postaviti slike ili video uradke, svoje obitelji sa ljetovanja na *face*, *flickr* ili *youtube* zapitajte se da li u stvari želite i da li ima smisla da to drugi ljudi i vide ?
- Za djecu (barem ispod 12 godina) nema mjesta na ovim mrežama. Djeca u ovoj dobi neznaju rezonovati i nemogu odgovarati za svoje postupke.
- Na kraju – uvijek se sjetite koliko prijatelja imate u „stvarnom“ životu, *second life* i stotine (pa i hiljade) virtualnih prijatelja zaboravite, oni su ipak samo niz nula i jedinica !

4. Sadržaj rada

U radu je predstavljena “druga strana medalje” odnosno negativna strana socijalnih mreža I opasnosti koje sobom nosi nekontrolisan pristup socijalnim mrežama.

5. Literatura

1. Facebok Statistics, http://www.facebook.com/press/info.php?statistics (pogledano 02.07.2010.)
2. SocialMedia Statistics, http://socialmediastatistics.wikidot.com/myspace (pogledano 29.06.2010)
3. Twitter Statistics:The full pictures: http://thenextweb.com/socialmedia/2010/02/22/twitter-statistics-full-picture/ (pogledano 01.07.2010).
4. Ćosić J.,Privatnost i sigurnost na socijalnim mrežama, INFO br.142, 2009, str. 58-59
5. Ćosić J. Web 2.0 Services (Vulnerability, Threats and Protection Measures), Conference Article, CECIIS 2009 Proceedings, 23rd – 25th September, Varaždin, Croatia, 2009.