Bezbednost društvenih mreža sa osvrtom na Twitter

Andreja Samčović
Saobraćajni fakultet u Beogradu
andrej@sf.bg.ac.rs

Sadržaj — **Društvene mreže imaju svoje prednosti i nedostatke. Prednosti se ogledaju u zabavi koju pružaju korisnicima kao i u mogućnosti održavanja kontakta sa velikim brojem ljudi bez obzira na fizičku udaljenost. Nedostaci su rizici kojima se korisnik izlaže prilikom korišćenja društvenih mreža. Jedan od glavnih problema informacionog društva je problem bezbednosti podataka koje korisnici ostavljaju na sajtovima društvenih mreža. U ovom radu biće reči o politici privatnosti, kao i rizicima po bezbednost informacija na društvenoj mreži Twitter. Takođe, biće reči i o mogućim načinima zaštite privatnosti.**

Ključne reči – društvene mreže, bezbednost podataka, Twitter

I. UVOD

Socijalna ili društvena mreža predstavlja oblik ljudske interakcije pri kojoj se pomoću postojećih poznanika ostvaruje virtuelni kontakt sa novim osobama radi ostvarivanja društvenih ili poslovnih aktivnosti. Sajtovi društvenih mreža omogućuju korisnicima upoznavanje pojedinaca sa bilo kog kraja sveta i to bez potrebe za fizičkim kontaktom [1].

Na internetu se mogu pronaći različite društvene mreže koje korisnicima nude raznovrsne načine interakcije korisnicima. Raznovrsnost načina interakcije uglavnom zavisi od količine podataka koje je korisnik spreman da otkrije. Da bi pristupio željenoj društvenoj mreži korisnik mora da kreira profil (korisnički nalog) u koji mora da upiše informacije o sebi od kojih su neke lične a neke mogu biti čak i poverljive.

Sa aspekta bezbednosti, najvažnija odlika društvenih mreža je činjenica da korisnik sam bira koje će informacije o sebi da ostavi na sajtu mreže kao i kome će te informacije biti vidljive. Korisnik može da ograniči vidljivost svojih informacija odnosno može podesiti da informacije sa profila budu dostupne samo korisnicima sa liste prijatelja ili da budu vidljive samo vlasniku profila. Većina korisnika ne vodi mnogo računa o privatnosti informacija jer nisu svesni rizika kojem se izlažu [2].

Osim fizičkih lica, naloge na mreži ove vrste mogu da kreiraju i pravna lica i to u cilju promovisanja svoje firme ili proizvoda. Najveći prihod društvenih mreža potiče upravo od oglašavanja. Kreiranje naloga na društvenim mrežama je besplatno ali materijalna vrednost mreže raste srazmerno broju korisnika. Razlog tome je činjenica da što više korisnika mreža ima više će kompanija biti zainteresovano za oglašavanje na njoj. Osim oglašavanja dosta je popularna i prodaja putem društvenih mreža.

Biti korisnik društvenih mreža nosi sa sobom čitav spektar rizika ali takođe ima i dosta prednosti. Neke od prednosti su osećaj povezanosti sa drugim korisnicima, upoznavanje istomišljenika, komunikacija sa drugim korisnicima bez obzira na fizičku udaljenost, mogućnost razmene životnih i poslovnih iskustava i druge. Nedostaci društvenih mreža najviše utiču na privatnost podataka korisnika. Pored rizika po bezbednost kojima se korisnik izlaže pri upisivanju svojih podataka na sajt društvene mreže postoje i drugi nedostaci. Jedan od nedostataka je mogućnost da se korisnik vremenom toliko navikne na virtuelni svet koji društvene mreže stvaraju i da se totalno otuđi od stvarnog sveta.

Postojanjem rizika se ne smanjuju prednosti i koristi društvenih mreža, već je cilj korisnike upozoriti na moguće napade i posledice istih. U nastavku rada će biti opisana društvena mreža *Twitter*, politika privatnosti na toj mreži, rizici kojima se korisnici izlažu otkrivanjem ličnih i poverljivih podataka, kao i načini moguće zaštite podataka.

II. DRUŠTVENA MREŽA TWITTER

Twitter je društvena mreža koja je besplatna za korišćenje a koju je kreirao Džek Dorsi u martu 2006. godine. Mreža je počela sa radom jula 2006. godine. Ova mreža korisnicima omogućava slanje i primanje poruka, pisanje beleški u obliku bloga, postavljanje fotografija na profil itd. Korisnik može da kreira poruke odnosno tvitove koji sadrže najviše 140 karaktera i koji se prikazuju na početnim stranama svih korisnika koji su odlučili da prate kreatora datog tvita [3].

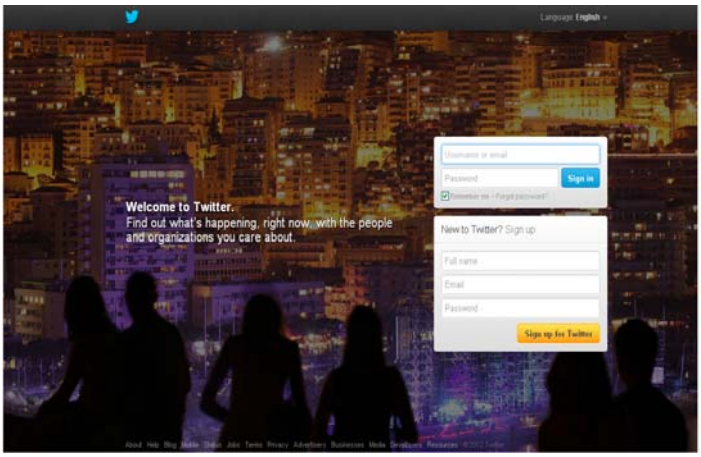
Tvitovi mogu da sadrže oznake ili da budu replike na nečiji tvit. Ako u tvitu ispred nekog dela teksta postoji prefiks # (npr. #jahorina) to znači da je u tom tvitu pomenuta određena tema i takve oznake omogućavaju pronalaženje tvitova na označenu temu. Ako u tvitu postoji znak @ ispred korisničkog imena onda je taj tvit upotrebljen za upućivanje replike korisniku ispred čijeg imena stoji znak. Ako korisnik želi da nekom korisniku pošalje poruku putem tvita onda je potrebno staviti oznaku *d* ispred korisničkog imena. Korisnik koji kreira tvit je u mogućnosti da ograniči vidljivost svog tvita samo na određenu grupu korisnika. Ako korisnik ne podesi vidljivost svog tvita on će se automatski prikazati na početnim stranama svih korisnika koji su sledbenici kreatora tvita.

Tvitove je moguće objavljivati preko sajta www.twitter.com, preko SMS (SMS - *Short Message Service*) poruka ili putem aplikacija kao što su *Tweetie*, *Twitterrific*, *Twitterfon*, *TweetDeck*. Iako je ova mreža besplatna za korišćenje objavljivanje tvitova preko SMS poruka naplaćuje se preko operatora mobilne telefonije. Nalog na *Twitter*-u je

moguće povezati sa nalogom na *Facebook*-u pa se na taj način poruke objavljene na *Twitter*-u pojavljuju i na *Facebook* profilu korisnika. Na ovoj mreži korisnik ne može da postane prijatelj nekom drugom korisniku već se može pretplatiti na njegove objave pa tako na *Twitter*-u ne postoje prijatelji nego sledbenici [1].

Ova socijalna mreža se uglavnom koristi za izražavanje mišljenja o raznim događajima u zemlji i svetu kao i za praćenje vesti, kompanija, poznatih ličnosti i slično. Poznate ličnosti, političari i razne vrste medija uglavnom koriste *Twitter* u cilju promocije svog rada i alat za sticanje popularnosti.

Prema poslednjim istraživanjima ova društvena mreža ima preko 500.000.000 korisnika u svetu a u Srbiji postoji oko 21.500 naloga na *Twitter*-u. Na Slici 1 prikazan je izgled web strane za prijavu na socijalnu mrežu *Twitter*.



Slika 1. Izgled web strane za prijavu na socijalnu mrežu Twitter

III. PRIVATNOST KOD MREŽE TWITTER

U politici privatnosti *Twitter*-a opisani su načini prikupljanja podataka i njihova upotreba [4]. Ova mreža prikuplja informacije o korisniku putem različitih *web* sajtova, aplikacija, SMS-a, *e-mail* obaveštenja i preko usluga treće strane. Kada korisnik počne sa korišćenjem *Twitter*-a on automatski daje mreži dozvolu da prikuplja podatke o njemu, skladišti ih, manipuliše njima, otkrije ih u datim slučajevima i slično. Bez obzira od lokacije korisnika sve podatke ova mreža može da koristi u SAD-u ili bilo kojoj drugoj zemlji u kojoj *Twitter* posluje.

Informacije koje korisnik mora da navede prilikom registracije na *Twitter*-u su: ime, korisničko ime, *e-mail* adresa i lozinka. Ime i korisničko ime biće prikazani na profilu kao javne informacije kao i profilna slika korisnika. Ako korisnik poželi da pregleda liste ili javne profile nije potrebno da se registruje.

Dodatne informacije koje korisnik može, po želji, da objavi su kratka biografija, lokacija i slike. Takođe, prilikom prilagođenja naloga korisnik može da ostavi broj svog mobilnog telefona da bi dobijao SMS obaveštenja sa mreže. Preko opcije za podešavanje naloga korisnik može da podesi način pretrage odnosno da li ga drugi korisnici mogu naći preko *e-mail* adrese ili preko broja mobilnog telefona. Još jedna od opcija koja je opisana u politici privatnosti ove mreže je ubacivanje kontakata iz adresara korisnika. Korisniku je tada olakšano traženje osoba iz adresara koje želi da prati. *Twitter* mreža može da koristi informacije o korisniku kako bi prilagodila poslovne ponude i usluge o kojima će mreža da obaveštava korisnika. Sa ovih obaveštenja korisnik može da se odjavi prateći uputstva koja su data na sajtu www.twitter.com.

Korisnik može da poveže svoj nalog na *Twitter*-u sa nalogom na nekoj drugoj mreži. *Twitter* će podatke tog korisnika podeliti sa tom drugom mrežom da bi bilo omogućeno unakrsno objavljivanje. Osnovna namena ove mreže je globalna razmena informacija ali korisnik može da izvrši privatizaciju svog naloga i na taj način zaštiti svoje podatke.

Pod javnim informacijama na *Twitter*-u se podrazumevaju tvitovi, liste, ljude koje korisnik prati i koji prate njega, retvitovi, omiljeni tvitovi i slično. Kada korisnik podeli informaciju kao što je fotografija, video zapis i slično ona će biti javna. Ako korisnik ne želi da takve objave budu javne on može da podesi njihovu privatnost. Ako želi, korisnik svojim tvitovima može dodati lokaciju sa koje su objavljeni. Ova funkcija je potpuno opcionalna.

Kao i mnogi drugi sajtovi i *Twitter* koristi *Cookies* tehnologiju. *Cookie* je mali fajl sa podacima koji se smešta na hard disk korisnikovog računara. Mogu se koristiti *Cookies* koje je potrebno prebacivati za svaku sesiju a postoje i trajni. Ova tehnologija se koristi da bi mreža mogla da prati *web* saobraćaj koji je rutiran ka korisnikovom računaru. Većina pretraživača automatski prihvata *Cookies* ali korisnik može da onemogući to prihvatanje ili da podesi pretraživač tako da kad god mreža pošalje ovakav fajl korisnik može da prihvati ili odbije njegov prijem. Ako korisnik onemogući prihvatanje ovih fajlova neki dodaci funkcionisati pravilno.

Log podaci su informacije o korisniku koje mogu da sadrže njegovu IP (*Internet Protocol*) adresu, tip pretraživača, domen, uređaj sa kojeg korisnik pristupa mreži, stranice koje posećuje i slično. Ove informacije se automatski snimaju na serveru mreže. Takođe, mreža prikuplja podatke iz interakcija korisnika sa mrežom, pristupanja nekim drugim sajtovima preko sajta *Twitter*-a, kliktanja na reklame i slično. Ove podatke *Twitter* koristi radi merenja saobraćaja na mreži, prilagođenja sadržaja korisniku i poboljšavanja same mreže.

Twitter takođe koristi i usluge drugih sajtova koje se još nazivaju i usluge trećih strana kao što su blogovi ili *Google Analytics*. Lične podatke korisnika ova mreža može da podeli sa sajtovima usluga trećih strana ali ta razmena je samo u mreži koje je određena za obavljanje date funkcije ili pružanje usluga mreži. Sajtovi sa kojima *Twitter* deli informacije korisnika su dužni da te podatke čuvaju u tajnosti i to u skladu sa politikom privatnosti *Twitter*-a.

Što se tiče zaštite dece u politici privatnosti ove mreže je navedeno da usluge mreže nisu namenjene osobama mlađim od 13 godina odnosno da se njima ne preporučuje korišćenje ove mreže. *Twitter* apeluje na roditelje i staratelje da, ako primete da njihova deca mlađa od 13 godina otkrivaju svoje informacije na *Twitter*-u, kontaktiraju administratore mreže na privacy@twitter.com. Takođe, ako administratori mreže

postanu svesni postojanja profila osobe mlađe od 13 godina taj profil će biti uklonjen sa mreže.

Postoje i situacije u kojima *Twitter* otkriva sve informacije koje je korisnik ostavio na mreži i te situacije su opisane u politici privatnosti. U slučaju saradnje sa policijom, zahteva od strane vlade ili policije da bi se zaštitila bezbednost neke osobe ili otkrila prevara kao i da bi se zaštitila prava i imovina *Twitter*-a ova mreža će otkriti korisničke informacije [5].

IV. SIGURNOSNI PROPUSTI NA MREŽI TWITTER

Među najpoznatijim sigurnosnim propustima na mreži *Twitter* jeste propust vezan za dozvolu izvršavanja proizvoljnog programskog kôda na nečijem profilu. Ovaj sigurnosni propust je iskoristio crv pod imenom „*StalkDaily*“ (takođe ime jednog od konkurenata mreži *Twitter*). Crv „*StalkDaily*“ se vrlo brzo proširio mrežom. Korisnik je mogao da zarazi sopstveni profil jednostavno pregledajući profil drugog korisnika koji je zaražen zlonamernim programom. Naime, napadač je iskoristio propust koji je dozvoljavao izvršavanje proizvoljnog programskog kôda i preuzimanje zlonamerne datoteke na profil na *Twitter* mreži. Na Slici 2 je prikazan zlonamerni kôd kojim su zaraženi korisnički profili velikog broja korisnika.

```
<a href="http://www.stalkdaily.com"></a><script
src="hxxp://mikeysklaz.uuuq.com/x.js"
var update = urlencode("Hey everyone, join www.StalkDaily.com.
It's a site like Twitter but with pictures, videos, and so much
more! :)");
var xss = urlencode('http://www.stalkdaily.com"></a><script
src="http://mikeysklaz.uuuq.com/x.js"></script><script
src="http://mikeysklaz.uuuq.com/x.js"></script><a ');

var ajaxConn = new XHConn();
ajaxConn.connect("/status/update", "POST", "authenticity_token="+authtoken+"&status="+update+"&
tab=home&update=update");
ajaxConn1.connect("/account/settings", "POST", "authenticity_token="+authtoken+"&user[url]="+xss+"&
tab=home&update=update");
```

Slika 2. Prikaz zlonamernog koda crva StalkDaily

Crvenom bojom su označeni delovi kôda koji su zapravo načinili štetu. Crv je u svaki zaraženi profil ugradio *Javascript*. Pregledanjem zaraženog profila korisnik je učitao zlonamernu *Javascript* datoteku, pa je na taj način pokrenuo preuzimanje iste takve zlonamerne datoteke sa navedene stranice (*uuuq.com*). Svim korisnicima čiji su profili bili zaraženi ovim crvom, otuđeni su korisnički podaci za pristup mreži *Twitter* čime je ugrožena sigurnost njihovih podataka. Zaraženi korisnički profili su automatski slali spam poruke korisnicima sa liste prijatelja, usmeravajući ih na stranicu *StalkDaily* društvene mreže. Vlasnici mreže su u kratkom vremenskom roku uspeli da „zakrpe“ sigurnosni propust.

Modifikovani crv je ponovo pogodio *Twitter* mrežu, ali iskorišćavanjem drugog sigurnosnog propusta. Druga pretnja korisnicima ugrozila je znatno manji broj korisnika, pa je ispravljena u kratkom vremenskom roku.

Takođe, jedan od napada na *Twitter* mrežu je uzrokovan nedovoljno dobrom autentifikacijom pri pristupu mreži. Haker pod imenom „*Hacker Croll*“ je uspeo da otkrije korisničko ime i lozinku jednog od administratora mreže *Twitter,* pa je bio u mogućnosti da ugrozi sigurnost miliona korisnika. Haker je provalio u e-poštu administratora i tamo pronašao korisničko ime i lozinku za mrežu *Twitter*. Haker je kao dokaz navedene radnje prikazao sliku interfejsa administratora u koju je ušao pa je upozorio vlasnike mreže *Twitter* na nedovoljno dobru autentifikaciju računara administratora. Moguća zaštita protiv ovakvih napada je korišćenje dvo ili višenivovske autentifikacije pri prijavi na računar administratora.

Jedan od napada koji je takođe prouzrokovao veliku štetu je napad kome je cilj slanje spam poruka putem korisničkih profila [6]. Do danas nije poznato na koji su način napadači uspeli da saznaju korisničke podatke korisnika. Korisnički profili automatski su slali spam poruke korisnicima sa liste prijatelja. Spam poruka je sadržala vezu ka web stranici koja prodaje proizvode za mršavljenje. Korisnicima, osim otuđivanja korisničkih podataka, nije naneta nikakva druga šteta. Vlasnici mreže *Twitter* su se pobrinuli da se otuđeni korisnički podaci vrate u normalno stanje.

V. MOGUĆNOSTI ZAŠTITE NA DRUŠTVENIM MREŽAMA

Zaštita privatnosti korisnika društvene mreže, isto kao i podataka koje je korisnik postavio na društvenu mrežu, mora biti primereno osigurana. Iako serveri ugrađuju zakrpe za propuste na društvenoj mreži, česte su situacije kada je napad izveden putem propusta u web pretraživačima koje korisnici upotrebljavaju. Međutim, korisnici često mogu i sami (nesavesnim korišćenjem) da kompromituju svoj profil ili otkriju svoje osetljive podatke. U ovom poglavlju su navedeni saveti korisnicima društvenih mreža kako bi zaštitili svoje podatke i informacije, kao i primenili odgovarajući oprez pri otkrivanju osetljivih ili poverljivih informacija.

Sigurnosne pretnje društvenih mreža moguće je podeliti u četiri grupe:

- Pretnje privatnosti;
- Pretnje mrežama i podacima;
- Pretnje identitetu;
- Društvene pretnje.

Korisnik može da primeni sledeće korake kako bi se zaštitio od zlonamernih napada:

Ograničavanje količine ličnih informacija koje su prikazane na društvenoj mreži - korisnik ne bi smeo da otkriva informacije koje ga mogu ugroziti na bilo koji način (poput adrese stanovanja ili dnevne rutine).

Internet je javni resurs - na svom profilu korisnik ne bi trebalo da prikazuje podatke ili medije koje ne želi da otkrije širem krugu ljudi (poznatih ili nepoznatih). Važno je napomenuti da jednom kada podaci budu postavljeni na web stranice društvene mreže, ne mogu se povući ili izbrisati. Iako ih korisnik izbriše sa svog profila, postoji vrlo velika verovatnoća da su ti podaci ostali sačuvani u pomoćnoj memoriji na računaru nekog drugog korisnika ili arhivi podataka društvene mreže.

Potrebno je obratiti pažnju pri komunikaciji sa strancima - internet je prilika zlonamernim korisnicima da bi lažno predstavljali sebe i svoje motive i interese. Korisnik bi trebalo

da ograniči broj ljudi koji imaju mogućnost da ga kontaktiraju putem ovakvih web servisa. Ukoliko se korisnik upoznaje sa strancima, potrebno je primeniti oprez pri otkrivanju ličnih informacija.

Skeptičnost je oprez - podatke koje korisnik pročita na društvenoj mreži potrebno je razmotriti sa oprezom. Drugi korisnici mogu da prikazuju lažne podatke o sebi (što nije nužno zlonamerno). Korisnik treba da pokuša da odredi autentičnost svake informacije.

Primena odgovarajućih postavki za privatnost - većina korisnika ne iskorišćava puni potencijal postavki za privatnost na društvenim mrežama. Podrazumevane postavke na nekim društvenim mrežama omogućuju svim korisnicima da vide profil. U postavkama je moguće postaviti vrstu profila na privatni kako bi ga videli samo korisnici sa liste prijatelja. Međutim, i uz primenu postavki za privatnost, neke informacije o korisniku mogu da budu otkrivene.

Korišćenje jakih lozinki - korisnički profil je potrebno zaštititi sa jakom lozinkom koju nije moguće pogoditi (ne sme da sadrži ime ili prezime, datum rođenja, niti bilo koju informaciju koja je kasnije navedena na profilu). Ukoliko se dogodi da neko otkrije lozinku, mogao bi se lažno predstavljati, otkriti osetljive informacije, zavarati druge korisnike, itd..

Provera politike privatnosti - važno je saznati koje informacije serveri društvenih mreža dele sa drugim organizacijama. Ukoliko se radi o slučaju da serveri dele adrese e-pošte svojih korisnika sa drugim organizacijama, moguće je da korisnik počne da prima velik broj spam poruka. U ovom slučaju bilo bi korisno proveriti politiku privatnosti svake mreže.

Korišćenje i održavanje antivirusnih programa - antivirusni programi automatski prepoznaju većinu zlonamernih programa i štite korisnika od gubitka podataka. Napadači neprestano stvaraju nove oblike zlonamernih programa, stoga je potrebno redovno ažurirati antivirusne programe.

VI. ZAKLJUČAK

Društvene mreže su, u vrlo kratkom vremenskom periodu, postale vrlo popularne. Većina korisnika ne može da zamisli jedan dan bez posete sajta neke od društvenih mreža. Korisnici postavljaju razne podatke, od slika, interesovanja do brojeva mobilnih telefona i kreditinih kartica. Malo je onih korisnika koji su potpuno upoznati sa rizicima koje nosi upisivanje podataka na društvenoj mreži. Takođe, dosta korisnika ne zna ili ne želi da podesi privatnost podataka na svojim profilima. Može se doći do zaključka da bi trebalo izvršiti kolektivno podizanje svesti korisnika društvenih mreža i da u tom postupku treba da učestvuju i mediji i policija ali i sami korisnici.

Popularnost ovih mreža će u u budućnosti rasti pa je potrebno, osim podizanja svesti o rizicima, korisnike upoznati i sa merama koje treba da preduzmu da bi poboljšali bezbednost svojih podataka.

ZAHVALNICA

Ovaj rad je deo istraživanja na projektima pod brojevima 32025 i 32048, koje finansira Ministarstvo za prosvetu, nauku i tehnološki razvoj Republike Srbije.

LITERATURA

[1] Hrvatska akademija i istraživačka mreža Croatian Academic and Reaserch Network CARNet, „Sigurnosni rizici društvenih mreža“, *CERT.ht*, Zagreb, Hrvatska, 2009.

[2] N.Tomić, D.Petrović: „Društveno umrežavanje i zaštita korisnika interneta“, *Zbornik radova PosTel 2009*, Beograd, Srbija, str. 95-104, 2009.

[3] B.Huberman, D.M.Romero, F.Wu: „Social networks that matter: Twitter under the microscope“, available at SSRN 1313405, 2008.

[4] http://www.twitter.com/privacy, /septembar 2012./

[5] V.Maletić, J.Dakić: „Internet, socijalne mreže i ljudska prava“, *Zbornik radova INFOTEH Jahorina,* Vol. 11, str. 771-776, mart 2012.

[6] A.H.Wang: „Don't follow me: spam detection in twitter”, Proceedings of the IEEE International Conference on security and cryptography SECRYPT 2010.

ABSTRACT

Social networks have their advantages and drawbacks. The advantages are reflected in the entertainment provided for users as well as the opportunity to maintain contacts with many people, regardless on physical distance. Drawbacks are the risks to which the user is exposed by using social networks. One of the main problems of information society is the security of data that users leave on the social networking sites. In this paper we will discuss about security policy and the risks of information security on the social network Twitter. Also, it will also be said about possible ways of privacy protection.

SOCIAL NETWORKS SECURITY WITH AN EMPHASIZE ON TWITTER

Andreja Samčović