FBIM Transactions
DOI 10.12709/fbim.07.07.01.03

SOCIJALNI INŽENJERING I LIČNI PODACI

SOCIAL ENGINEERING AND PERSONAL DATA

Srđan Blagojević
Visoka poslovna škola strukovnih studija „Čačak“, Beograd, Srbija

JEL Category: **C88, L86**

Apstrakt

U današnjem informacionom okruženju sve je više pretnji i opasnosti za bezbednost računarskih korisnika. Jedna od ovih pretnji koja je veoma rasprostranjena i bez izgleda da se u budućnosti umanji, je svakako krađa ličnih podataka. Da bi se do njih došlo, zlonamernici su spremni na obimnu pripremu, istraživanja pojedinaca i kompanija, čekajući pravi trenutak da napadnu i ostvare svoje ciljeve, pa je potrebno uočiti i neke od najkarakterističnijih prevara koje koriste socijalni inženjering, kao i njihovu genezu na Internetu i društvenim mrežama. Korišćenje društvenih mreža je kritično u odnosu na bezbednost i privatnost korisnika. Velika količina informacija objavljenih i često javno podeljenih na profilu korisnika, sve više privlači pažnju napadača. Umesto da napadač inicira kontakt sa žrtvom, metode obrnutog socijalnog inženjeringa se primenjuju da žrtva bude namamljena da prva kontaktira napadača što za posledicu ima ostvaren visok stepen poverenja između žrtve i napadača. Integracija socijalnog inženjeringa u ove napade predstavlja nove, složenije pretnje i pokušaje da se od korisnika Interneta uzmu lični podaci koji su za napadača moneta kojom se trguje ili koja se lako zamenjuje za novac. Da bi se ovi napadi na vreme prepoznali, pomaže nam uočavanje njihovih karakteristika, a da bi smo u potpunosti sagledali problem, neophodno je znati i pravu vrednost ličnih podataka i šta oni predstavljaju u svetu crnog Internet tržišta.

Ključne reči: *socijalni inženjering, lični podaci, prevare, bezbednost, zaštita.*

Abstract

In today's information environment, there are more threats and dangers to the security of computer users. One of these threats that is very widespread and without the chance to zoom out in the future, is certainly stealing personal data. To occur, the malicious men are ready for extensive preparation, research of individuals and companies, waiting for the right moment to invade and achieve their goals, so it is necessary to spot some of the most distinctive fraud used by social engineering and their genesis on the Internet and social networks. Usage of social networks is critical of the security and privacy of users. A large amount of information published and often publicly shared on users' profile, is increasingly drawing the attention of the attackers. Instead of the attacker initiating contact with the victim, the method of reverse social engineering is applied for the victim to be lured to the first contact with the attacker, which results in a high level of trust between the victim and the attacker. Integration of social engineering in these attacks is a new, more complex threat that attempts to take

Adresa autora:
Srđan Blagojević
srdjan@hotmail.ca

personal data from internet users that is easy to trade with or to cash in. In order to identify these attacks in time, it helps to see their characteristics, and in order to see the problem fully, it is necessary to know the true value of personal information and what they represent in the world of black Internet markets.

Keywords: *social engineering, personal data, fraud, security, protection.*

1 UVOD

Problem upravljanja bezbednošću ima više aspekata što ga čini veoma kompleksnim. Što je obimniji i kompleksniji softver koji koristi, povećava se i njegova ranjivost. Ovu činjenicu koriste hakeri, zlonamerni kompjuterski stručnjaci, te nalaze ove osetljive tačke i koriste ih u cilju lične promocije, ostvarivanja koristi ili iz puke obesti. Posledice ovih napada, nezavisno od motiva, uvek predstavljaju veliki trošak za pojedince i kompanije. Razni podaci i druge informacije, mogu biti od koristi onima kojima je cilj trka za zaradom. Stoga je poznavanje pretnji i opasnosti koje sa sobom nosi informaciona tehnologija od presudne važnosti za poslovanje i zaštitu kompanija i pojedinca.

Jedna od ovih pretnji koja je veoma rasprostranjena i bez izgleda da se u budućnosti umanji, je svakako krađa ličnih podataka. Da bi se do njih došlo, zlonamernici su spremni na obimnu pripremu, istraživanja pojedinaca i kompanija, čekajući pravi trenutak da napadnu i ostvare svoje ciljeve.

U tu svrhu, razvijaju se i koriste nove metode socijalnog inženjeringa i obrnutog socijalnog inženjeringa na Internetu uz često korišćenje društvenih mreža kao načina za izvođenje napada.

2 SOCIJALNI INŽENJERING

Socijalni inženjering nije nova nauka, ali sa pojavom društvenih mreža, dobija na snazi i značaju zato što su informacije o potencijalnim žrtvama lakše dostupne pa se prikupljaju brže i lakše nego ranije. Takođe, propulzivne metode i taktike, daju socijalnom inženjeringu na značaju u informatičkom okruženju, odnosno na Internetu, jer više nije neophodno sresti nekoga licem u lice, već se napadi mogu izvršiti masovno i bez ličnog kontakta.

Ovaj termin danas se koristi da opiše razne načine koje pojedinci koriste da prevare, obmanu i izmanipulišu svoje žrtve da bi od njih izvukli poverljive informacije i novac.

Kriminalci koriste poverenje ljudi da saznaju brojeve njihovih računa, kreditnih kartica, lozinke i druge lične podatke. Ove kriminalne aktivnosti se obavljaju „online“ odnosno, elektronskom poštom, preko društvenih mreža, sajtova, telefonom ili ličnim kontaktom.

Socijalni inženjering se može podeliti u dve osnovne grupe:

1. Masovni
2. Ciljani

Masovni socijalni inženjering koristi osnovne tehnike i okrenut je prema široj populaciji, kao što je na primer masovno slanje pecačkih poruka ili reklama, dok je ciljani usmeren ka vrlo specifičnim individuama i kompanijama za koje se misli da su veći „ulov“, pa je složeniji i zahteva veći nivo poznavanja funkcionisanja, potreba i okolnosti svojih meta.

Načini na koji se izvodi kriminalna aktivnost su različiti ali metodi kojima se služe kriminalci generalno prate istu matricu koja se sastoji od četiri osnovna koraka:

- Prikupljanje informacija
- Upoznavanje i razvoj poverenja
- Otkrivanje slabosti / ranjivih mesta
- Izvršenje dela.

Tipovi napada koji koriste socijalni inženjering mogu se podeliti na sledeće:

1. Poruke – Forma socijalnog inženjeringa koja koristi poruke, bilo da su poslate elektronskom poštom, SMS-om ili preko neke od multimedijalnih mreža za komunikaciju, je takva da se napadači, kroz dopisivanje, fokusiraju na stvaranje ubedljivih izmišljenih scenarija u cilju ostvarivanja materijalne koristi ili do dolaska do poverljivih informacija.
2. Pecanje sa mamcem je slično kao i obično pecanje ali sa dodatkom linka u poruci koji obećava besplatne sadržaje i/ili stvari. Može se izvršavati kroz poruke ili kroz reklame. Mamci mogu biti postavljeni i kao usluge, što predstavlja drugi oblik ovakvog pecanja.

3. Praćenje u repu je oblik napada kada se napadač približi nekome u cilju da iskoristi drugoga ko ima odobrenje za ulaz u obezbeđeno područje ili zgradu.
4. Diverzija podrazumeva pogrešno usmeravanje kurira ili transportne kompanije u cilju preusmeravanja pošiljke na drugu lokaciju. Takođe se može izvršiti i kroz preusmeravanje plaćanja na drugi račun, što se, u ovom slučaju, ostvaruje kroz pristup nalogu elektronske pošte žrtve.
5. Kidnapovanje je vrsta zlonamernog softvera koji ograničava pristup zaraženom računarskom sistemu na neki način i zahteva da korisnik plati otkup operatorima malvera, zlonamernog programa, da bi uklonio ograničenje.
6. Ronjenje u kontejneru ili, kopanje po đubretu, je tip socijalnog inženjeringa kojim se prikupljaju informacije iz odbačenih materijala kao što su: stara računarska oprema (npr. hard diskovi, disk jedinice, DVD-ovi, CD-ovi) i dokumenti pojedinaca ili preduzeća koji nisu bili bezbedno uklonjeni.
7. Pecanje, koje se može podeliti na:
   a. pecanje koja cilja na pojedinačne ili izabrane grupe
   b. pecanje harpunom gde je meta krupna riba
   c. IGS (IVR) pecanje koje koristi IGS sistem[1]
   d. kompromitovana poslovna elektronska pošta – mutacija od „pecanja harpunom“ ili „kitolovca“, gde se žrtva skenira, pretražuje, a nadzor finansira. Napadač je u ovom napadu prikriven i čeka pravi momenat da izvrši „diverziju“.

U cilju prepoznavanja ovakvih napada na mreži, možemo prepoznati njihove karakteristike koje su prikazane u sledećoj tabeli.

Tabela karakteristika socijalnog inženjeringa (Jain, i drugi, 2016)

Karakteristike napada	**Traženje informacija**	**Potencijalne posledice**
Izgled • uglavnom dobre ili loše vesti • osećaj hitnosti • osetljiva i poverljiva stvar • pretvaranje da je neko drugi (slično ime) **Zahtevani odgovor** • da se dostave specifične informacije • da se apdejtuju lični podaci ili podaci o računu • da se klikne na link u elektronskoj poruci • da se otvori prilog uz mejl **Indikatori sumnjivosti** • Generisani pozdravi • sumnjiv kontekst • loš pravopis • neuobičajeni ili čudan pošiljalac • netačna informacija • neispravni URL-ovi u poruci	• informacije o računu • korisničkom imenu • Lozinci ili PIN-u • broju kreditne kartice • matičnom broju • broju računa • IBAN-u • adresi elektronske pošte • Broju telefona • drugim ličnim podacima	• Finansijski gubitak • krađa identiteta • krađa ličnih ili poverljivih podataka ili kritične informacije • krađa intelektualne svojine • ugroženi računar, podmetnuti virus ili zlonamerni program • podaci, softver ili hardver izmenjeni ili uništeni • naneta šteta ugledu pojedinca ili kompanije • politička šteta • odbijanje servisa

[1] IGS sistem je Interaktivni Govorni Sistem koji kroz govornu komunikaciju sa lažnim predstavnicima korisničke službe prikuplja podatke od klijenata

Primeri:

Među poznatim prevarama koje koriste metode socijalnog inženjeringa u sferi informacione tehnologije su najčešće:

„Telefonska prevara“

U ovoj situaciji, zlonamernik pronalazi broj telefona, najčešće starije osobe, predstavlja se kao član porodice ili poznanik, koji je u velikom problemu i novac mu je hitno potreban. Razlozi mogu biti predstavljeni kao problemi na putovanju, krađa novca, zelenaški dug, bolest ili neki drugi finansijski problem.

Ovu prevaru, koja zahteva znanje osnovnih podataka o osobi koja se poziva, zbog čega se nalazi u primerima socijalnog inženjeringa, treba razlikovati od sličnih prevarnih šema koje koriste SMS poruke sa sličnim sadržajem ali bez znanja kome su poslate i ne obraćaju se meti po imenu.

„Prevara elektronskom poštom ili porukama“

Ova šema počinje sa kreiranjem scenarija da se ciljana žrtva uključi u neku razmenu poruka odnosno pisanu komunikaciju. Napadač se pretvara da je menadžer banke, poreski službenik, komunalni ili policijski inspektor tražeći lične podatke kao što su brojevi računa ili lozinke. Za ovakvu kriminalnu radnju neophodno je poznavanje osnovnih ličnih podataka i okolnosti žrtve, da bi prevara uspela.

„Menadžerska prevara“

Prevarant prikuplja javno dostupne informacije o poslovnom sistemu koji namerava da napadne. Pronalazi detalje o Generalnom Direktoru ili funkcioneru na čelu sistema, kao i o osobama koje imaju ovlašćenja za prenos sredstava sa računa organizacije. Tada koristi dobijene podatke da kreira hitnu potrebu za uplatom na određeni bankovni račun.

„Hakovanje naloga elektronske pošte“

Ukoliko zlonamernik uspe da se domogne pristupa nalogu elektronske pošte žrtve, ili kontakata u mobilnom telefonu, može sa njih poslati poruke svima u listi kontakata, tvrdeći da je u nevolji, u inostranstvu, bez telefona i da mu je hitno potreban novac.

„Lutrijska prevara“

Ovu prevaru karakteriše informacija da je potencijalna žrtva dobila na lutriji, ili da je ušla u samo finale takmičenja sa ogromnim šansama za dobitak, koju moguće prati ček sa upisanim iznosom i ispisanim podacima žrtve u prilogu poruke, a samo je potrebno uplatiti troškove obrade isplate dobitka na račun. Ovde se često koriste imena poznatih kompanija kao organizatora nagradne igre da bi se ostavio utisak.

Da bi se ostvarile sve ove prevare, a i druge slične njima, u kontekstu socijalnog inženjeringa, koriste se i druge metode poput: praćenja, preusmeravanja isporuke, razmene osetljivih podataka „usled nesporazuma“, naizgled slučajnim ostavljanjem zaraženog (USB) diska, zahtevom za forenzičkom analizom inficiranih diskova, itd.

2.1 Socijalni inženjering na društvenim mrežama

Prevare na društvenim mrežama imaju svoje specifičnosti zbog načina na koji funkcionišu i kako se implementiraju. Jedna od ključnih karakteristika društvenih mreža je podrška koja se obezbeđuje za traženje novih prijatelja. Na primer, tipična tehnika sastoji se od automatskog identifikovanja zajedničkih prijatelja u slikama, a zatim promovisanju novih prijateljstva sa porukama kao što su "imate 4 uzajamna prijatelja sa „Petrom Petrovićem“. Da li biste želeli da dodate „Petra Petrovića“ za novog prijatelja? Takođe, informacije o aktivnostima korisnika se često prikupljaju, analiziraju i usmeravaju ka programima za izračunavanje verovatnoće da se dva korisnika poznaju. Ako se otkrije potencijalni poznanik, lokacija sa društvene mreže, kada se korisnik prijavi na sistem, može da prikaže novu preporuku o prijateljstvu.

Jasno je da je korišćenje društvenih mreža kritično u odnosu na bezbednost i privatnost svojih korisnika. U stvari, velika količina informacija objavljenih i često javno deljena, na profilu korisnika sve više privlači pažnju napadača. Napadi na društvenim mrežama su obično varijante tradicionalnih bezbednosnih pretnji (kao što su malver, crvi, bezvredna pošta i pecanje). Međutim, ovi napadi se izvršavaju u drugačijem kontekstu, dodavanjem društvenih

mreža kao novog medijuma za prikupljanje žrtava. Pored toga, napadači mogu da iskoriste odnose poverenja između "prijatelja" na društvenim mrežama da bi izvršili više uspešnih napada korišćenjem ličnih informacija koje su na stranicama žrtava.

2.2 Obrnuti socijalni inženjering

U obrnutom socijalnom inženjeringu, napadač ne inicira kontakt sa žrtvom. Umesto toga, žrtva je namamljena da kontaktira napadača. Kao rezultat toga, ostvaruje se visok stepen poverenja između žrtve i napadača zato što žrtva ostaje u uverenju da je prva želela da uspostavi kontakt. Jednom kada je obrnuti napad uspešan (kada je napadač uspostavio vezu sa žrtvom), on može da pokrene širok spektar napada, kao što su ubeđivanje da kliknu na zlonamerne linkove, ucenjivanje, krađu identiteta i pecanje.

Postoje tri vrste napada korišćenjem obrnutog socijalnog inženjeringa na društvenim mrežama (Irani, Balduzzi, Balzarotti, Kirda, & Pu, 2011):

- Na osnovu preporuke društvene mreže
- Predlog prijatelja za novog prijatelja
- Demografski društveni inženjering

Na samom početku ovakvog napada koriste se preporuke koje društvena mreža napravi za promociju, za svrhu prevare, napravljenog lažnog profila. Napadač želi da svoj cilj zainteresuje preporukom i da ona poželi da kontaktira profil koji je pod napadačevom kontrolom. U praksi, ovo podrazumeva da se aktivira radoznalost običnim pregledom profilne stranice. Notifikacija da je neko lajkovao žrtvinu sliku može biti dovoljna da je privuče da pregleda lažni profil.

Sugestije prijatelja za novog prijatelja mogu biti zloupotrebljene zato što se mogu vršiti sa takođe lažnih profila koje je korisnik već ranije prihvatio. Radi uverljivijeg napada, u cilju sticanja poverenja, lažni profil ostvaruje određeni broj zajedničkih prijateljstva. Često je potrebno da samo jednu osobu iz određenog kruga obmane da prihvati prijateljstvo sa lažnim profilom, da bi ostali iz istog kruga, tu osobu prihvatili po automatizmu, često misleći da samo ne mogu trenutno da je se sete i misleći da, kad su oni prethodni, koje stvarno poznaje, prihvatili zahtev, zašto to ne bih uradio i ja. Takođe, razlozi za prihvatanje nepoznatih osoba za prijatelje može biti i želja da se ima što veći broj prijateljstva da bi se time podigla „svoja važnost“.

U scenariju demografskog napada, napadač pokušava da dođe do svoje žrtve tako što falsifikuje lažne demografske ili lične informacije sa ciljem da privuče pažnju korisnika sa sličnim potrebama (npr. slični muzički ukusi, sličan interesi itd.). Nasuprot zdravoj pameti, istraživanja su pokazala da je dovoljno samo imati profil sa atraktivnom fotografijom da bi se regrutovao veliki broj potencijalnih žrtava. U suštini, napadač mora da obezbedi žrtvama izgovor i podsticaj za uspostavljanje kontakta.

Još jedan primer obrnutog socijalnog inženjeringa je slanje broja telefona ili adrese elektronske pošte za prijavu ili rešavanje određenog problema pre nego što se problem pojavi. Na primer, Internet servis provajder ili banka mogu da obaveste svoje klijente da, ukoliko se pojavi „takav i takav“ problem, treba da kontaktiraju sledeću adresu ili broj telefona. Kada se za nekoliko dana takav problem pojavi, stigne neki račun ili opomena, žrtva se seti informacije koju je nedavno pročitala i odluči se da kontaktira lažni kontakt. Kako je obmanuta da misli da je prva pokrenula kontakt, biće manje sumnjičava i spremna da podeli kritične informacije. (Irani, Balduzzi, Balzarotti, Kirda, & Pu, 2011)

Stotine miliona korisnika registrovano je na društvenim mrežama i redovno ih koriste da bi ostali u kontaktu sa prijateljima, komunicirali, obavljali onlajn trgovinu i delili multimedijalne sadržaje sa drugim korisnicima. Da bi bile u mogućnosti da naprave predloge i promovišu prijateljstva, društvene mreže često prikupljaju lokacije o registrovanim korisnicima. Na primer, činjenica da korisnik traži adresu nečije elektronske pošte, može da podrazumeva da korisnik zna osobu koja je vlasnik tog naloga. Na žalost, takve pretpostavke mogu da budu zloupotrebljene od strane napadača da svoju žrtvu zaintrigira lažnom porukom.

Iako je socijalni inženjering dobro proučen, njegova obrnuta verzija, na društvenim mrežama, još nije dobila dovoljno pažnje. Opasnosti koje sa sobom nosi su ogromne.

Komunikacija kroz Internet postaje svakim danom drugačija pa se metode komunikacije potencijalnih učesnika u trgovini ukradenim

podacima, korišćene do samo pre nekoliko godina zamenjuju novim, težim za otkrivanje i praćenje. Sve ovo čini da se poveća zainteresovanost za krađom podataka kompanija i pojedinaca, te se aspekti informacione bezbednosti moraju stalno ojačavati kako bi postali i ostali u skladu sa potrebama i izazovima trenutka.

3 LIČNI PODACI

Kada govorimo o ličnim podacima, govorimo, u stvari, o pojedincu koji se tim podacima može identifikovati. U današnjem svetu se prikupljaju ogromne količine ličnih podataka. Neke organizacije ih koriste za svoje potrebe a neke ih prenose trećim licima iz najrazličitijih razloga. Ovaj trend eksponencijalno raste zajedno sa razvojem složenih informacionih tehnologija za obradu i analizu velikih baza podataka.

Sa ovakvim trendom, raste i zabrinutost pojedinaca o tome ko i kako koristi njihove lične podatke. Stoga je neophodno implementirati politiku informacione bezbednosti koja će sadržati i načine zaštite ličnih podataka, odnosno njihovo prikupljanje, korišćenje i objavljivanje i cilju da se ostvari i održi poverenje pojedinaca u organizacije koje su u posedu ovih podataka.

Povrede bezbednosti ličnih podataka mogu izazvati ozbiljnu štetu i patnju žrtvama zloupotrebe, pa im mogu, čak, dovesti i život u pitanje. Primeri štete nastale gubitkom ili zloupotrebom ličnih podataka ponekad povezanih sa krađom identiteta uključuju:

- Lažne transakcije kreditnim karticama;
- Lažne zahteve za poreskim kreditima tj. povraćajima poreza;
- Lažne priznanice za prijem robe, pozajmice ili dugovanja;
- Lažne testamente;
- Lažnu dokumentaciju o usvajanju;
- Hipotekarne prevare.
- Rizik za svedoke od fizičkih povreda ili zastrašivanja;
- Rizik počinilaca od vaninstitucijalne osvete oštećenih; i
- Rizik saznavanja adresa uslužnog osoblja, policije i zatvorskih službenika, žena žrtava nasilja u porodici, lekara.

Razlozi zašto su lični podaci dragoceni za kiber—kriminalce leže u činjenici da oni zapravo predstavljaju monetu sive ekonomije kojom se trguje. Vlasnici baza ličnih podataka ili oni koji te baze pribave na dozvoljene ili nedozvoljene načine, mogu ih prodati različitim kupcima, odnosno: kradljivcima identiteta, organizovanim bandama, spamerima i operaterima botnet mreža. Botnet mreža predstavlja mrežu, malverom zaraženih računara, kojom upravlja njen tvorac a koji koriste ove baze podataka da prošire svoje mreže i time pribave još više novca.

Spameri, na primer, mogu dobiti novu listu adresa elektronske pošte, na koju mogu poslati ponude za Cijalis i Vijagru. Zaradu imaju po svakom kliku na link koji su promovisali, ili po broju odgovora, ili po broju pristupa reklamiranim sajtovima. Kradljivci identiteta mogu koristiti adrese za sve oblike pecanja.

Kiber-kriminalci trguju ovim informacijama međusobno da bi kompletirali sliku pojedinca. Ideja je, da svi zajedno, prikupe više informacija o ljudima te da tako da mogu da naprave veću štetu odnosno ostvare veću dobit. Cilj im je da iz više izvora sakupe: ime, broj kreditne kartice, PIN, e-mail adresu i telefonski broj. Otkrivanje pojedinačnih podataka u različitim situacijama i na različitim mestima, možda se ne učini opasno, ali kada pojedinac ili kompanija predstavljaju ciljanu metu radi se o potpuno drugačijoj slici. (Levinson, 2012)

4 MATIČNI BROJ GRAĐANA

Krađa identiteta u Srbiji nije definisana kao krivično delo, iako je broj onih kojima su ukradena dokumenta ili na neki drugi način zloupotrebljeni lični podaci, sve veći. Ljudi uglavnom nisu svesni gde sve „seju“ matični i broj lične karte, i broj bankarske kartice, i ne znaju skoro ništa o opasnostima koje ih zbog toga vrebaju. A život u samo nekoliko minuta može da im se pretvori u pakao.

Kancelarija poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti ukazuje da su kancelariji, do sada, građani prijavili pet krađa identiteta. U MUP tvrde da ovakve podatke nemaju jer Krivični zakonik ne poznaje to krivično delo, a na slične situacije primenjuju se odredbe koje se odnose na falsifikovanje isprava i prevare. 2014. godine je, prema podacima Republičkog zavoda za statistiku, podneto je 1.256 prijava za falsifikovanje isprave, 364 za posebne slučajeve

falsifikovanja isprave i nešto više od 2.600 za prevaru, ali se ne zna koliko od toga za zloupotrebu tuđih podataka. Za falsifikovanje i zloupotrebu platnih kartica policija je podnela 262 prijave. (Crnjanski Spasojević, 2014)

Veoma je opasno davanje jedinstvenog matičnog broja.[2]

Na osnovu njega bilo ko može da uđe u bazu podataka građanina u poreskoj upravi ili u birački spisak, APR i zloupotrebi ih.

Mnogi prikupljaju podatke i bez zakonskih ovlašćenja (recimo, sportski klubovi). Ali nekada i zakon dozvoljava bespotrebno uzimanje podataka. Centralno pitanje je kako se te baze štite. Više istraživanja pokazalo je da mnogi rukovaoci podacima, kako ih zakon zove, imaju veoma slabu ili čak nemaju nikakvu zaštitu.

Da bi ukrali identitete ljudi, ili počinili prevaru sa kreditnim karticama, kiber kriminalcima treba lozinka, broj kreditne kartice ili broj socijalnog osiguranja na zapadu a kod nas matični broj. Za to se između reklama ubacuju pecačke poruke ili zlonamerni programi koji mogu da instaliraju i „key-logging“ programe.

Ako se dokopaju samo 4 zadnje cifre broja kreditne kartice, mogu to da iskoriste za promenu lozinke na nekim prodajnim sajtovima, zato što neki od njih koriste te cifre kao PIN kod korisnika. Jednom kada promene lozinku mogu promeniti i druge podatke i naručivati robu mimo znanja vlasnika kartice. Takođe, nakon svojih napada, mogu da prodaju ovu informaciju i nekom drugom, ko može da izvrši još neku drugu vrstu napada na ovog korisnika. (Levinson, 2012)

Neke baze podataka imaju zaštitu, ali je pitanje da li je ona dovoljna i srazmera vrednosti zaštićenih podataka. Naročito su opasni upadi u velike elektronske baze kakve imaju banke, sistemi koji se bave trgovinom preko interneta, zdravstvene službe ili PIO fond. Više od 300.000 institucija rukuje ličnim podacima građana, a procene su da su one napravile milion baza podataka. Najviše evidencija ima MUP, Vojska, bezbednosne službe, Carina, poreznici, pravosuđe, banke, firme, socijalne ustanove, opštine, izborne komisije...

Svi koji rukuju ličnim podacima građana trebalo bi da prijave svoje baze podataka u Centralni registar, kako bi poverenik mogao da kontroliše ko i kako obrađuje nečiji jedinstven matični broj, ime i prezime, adresu... Međutim, u centralni registar je upisano tek 317 rukovaoca ličnim podacima, i oko 1.600 evidencija o zbirkama koje vode. To nije ni 0,5 odsto onoga što se očekuje. (Crnjanski Spasojević, 2014)

Svrha registra je ne samo da se evidentira svaka zbirka, već i da se omogući svakome da sazna ko obrađuje podatke o ličnosti, u koje svrhe i kome su podaci dostupni.

Inače, krađa identiteta je već godinama, prema Američkoj federalnoj komisiji za trgovinu, prva na listi „naj-prevara“.

5 VREDNOST LIČNIH PODATAKA

Vrednost ličnih podataka pojedinačno nije velika. Kreće se od delića centa do jednog dolara u zavisnosti od svežine prikupljenih podataka i njihovog kvaliteta. Čak i brojevi kreditnih kartica koštaju manje od jednog dolara iz razloga velike ponude.

Ovo možda ne izgleda kao nešto sa čime bi se pojedinac mogao da se obogati, ali kada se pomnoži sa milionima podataka, cifre postaju ogromne. Na primeru provale poznate pod imenom „Zappos“, u kojoj je su ukradeni podaci o 24 miliona korisnika, može se izračunati da, ako se proda samo 5 miliona zapisa po 5 centi, dolazi se do cifre od 250,000 dolara za samo jedan

[2] Jedinstveni matični broj građana (JMBG) je identifikaciji broj dat svim novorođenim građanima SFRJ (Socijalističke Federativne Republike Jugoslavije) od 1976. godine. Svi građani rođeni pre 1976. godine su dobili broj u zavisnosti od regija u kojim su tada živeli. Broj je još uvek u upotrebi u novonastalim državama.
Broj je napravljen od 13 cifara u formi „DD MM GGG RR BBB K“ (bez razmaka), gde su:
DD – dan rođenja
MM – mesec rođenja
GGG – poslednje tri cifre godine rođenja
RR – regija rođenja (za građane rođene pre 1976. godine regija gde su trenutno živeli)
BBB – jedinstveni broj, 000-499 – muški, 500-999 – ženski
K - kontrolna cifra

hakerski napad. Operateri mreže botova mogu da zarade enormne sume novca. Ako se mreža sastoji od recimo 100,000 bot računara, može da se iznajmi za 1000 dolara po satu.

Pravljenje botnet mreže je izuzetno isplativ posao. Kada neko ukrade 24 miliona imejl adresa, kao što se to dogodilo u slučaju „Zappos"-a, i pošalje malver na njih, ako uspe da zarazi 20 procenata onih koji prime i otvore njegov e-mejl, čime postaju deo njegove botnet mreže, uspeće da izgradi mrežu kapaciteta 5 miliona računara koju onda može da izda za 5000 dolara po satu uz vrlo malo truda.

Prvi nivo informacija koji je potreban hakerima da bi počeli svoj posao su adrese elektronske pošte. Sa njima, počinje spamovanje, odnosno zatrpavanje sandučića elektronske pošte raznim komercijalnim porukama.

6 ZAKLJUČAK

Nemaju svi napadi samo finansijske posledice. Mnogi izazivaju posledice druge vrste, kao što su na primer, osramoćenje i neprijatnosti.

Napredak u tehnologiji omogućio je organizacijama da obrađuju sve više ličnih podataka i da lakše razmenjuju informacije. To ima očigledne prednosti ukoliko prikupljaju i dele lične podatke u skladu sa principima zaštite podataka, ali takođe podjednako sadrže i očigledne bezbednosne rizike. Što je veći broj popunjenih baza podataka, i što se više informacija u njima razmenjuje, to je veći je rizik da će informacije biti izgubljene, oštećene ili pogrešno iskorišćene.

Veliki broj poznatih slučajeva gubitaka ličnih podataka je privukao pažnju prema problemu bezbednosti informacija. Međutim, ovi incidenti su takođe jasno dali do znanja da je bezbednost informacija zadatak društva, ali i da postoji i problem tehničke neusaglašenosti. Ako lični podaci nisu propisno čuvani, to može ozbiljno da ošteti reputaciju i prosperitet organizacije i može da ugrozi bezbednost pojedinaca.

CITIRANA DELA

Crnjanski Spasojević, V. (2014, 07 27). Matične brojeve ostavljamo "na izvol'te". *Večernje novosti online*. Preuzeto sa http://www.novosti.rs/%D0%B2%D0%B5%D1%81%D1%82%D0%B8/%D0%BD%D0%B0%D1%81%D0%BB%D0%BE%D0%B2%D0%BD%D0%B0/%D0%B4%D1%80%D1%83%D1%88%D1%82%D0%B2%D0%BE.395.html:502763-%D0%9C%D0%B0%D1%82%D0%B8%D1%87%D0%BD%D0%B5-%D0%B1%D1%80%D0%BE%D1%98%D0%B5%D0%B2%D0%B5-%D0%BE%D

Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E., & Pu, C. (2011, 05 16). *Reverse Social Engineering Attacks in Online Social Networks.* Preuzeto sa SysSec: http://www.syssec-project.eu/m/page-media/3/irani-dimva11.pdf

Jain, A., Tailang, H., Goswami, H., Dutta, S., Mahipal, S. S., & Kumar, R. (2016). Social Engineering: Hacking a Human Being through Technology. *Journal of Computer Engineering (IOSR-JCE)*, 94-100. doi:10.9790/0661-18050594100

Levinson, M. (2012, 01 26). *Are You at Risk? What Cybercriminals Do With Your Personal Data.* Preuzeto sa CIO from IDG: https://www.cio.com/article/2400064/security0/are-you-at-risk--what-cybercriminals-do-with-your-personal-data.html

Datum prve prijave: 02.09.2018.
Datum prijema korigovanog članka: 11.03.2018.
Datum prihvatanja članka: 27.03.2019.

Kako citirati ovaj rad? / How to cite this article?

*Style – **APA** Sixth Edition:*

Blagojević, S. (2019, 04 15). Socijalni inženjering i lični podaci. (Z. Čekerevac, Ed.) *FBIM Transactions, 7*(1), 20-28. doi:10.12709/fbim.07.07.01.03

*Style – **Chicago** Sixteenth Edition:*

Blagojević, Srđan. 2019. "Socijalni inženjering i lični podaci." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (1): 20-28. doi:10.12709/fbim.07.07.01.03.

*Style – **GOST** Name Sort:*

Blagojević Srđan Socijalni inženjering i lični podaci [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Beograd : MESTE, 04 15, 2019. - 1 : Vol. 7. - pp. 20-28.

*Style – **Harvard** Anglia:*

Blagojević, S., 2019. Socijalni inženjering i lični podaci. *FBIM Transactions,* 15 04, 7(1), pp. 20-28.

Style – **ISO 690** Numerical Reference:

Socijalni inženjering i lični podaci. **Blagojević, Srđan.** [ed.] Zoran Čekerevac. 1, Beograd : MESTE, 04 15, 2019, FBIM Transactions, Vol. 7, pp. 20-28