Da li ste bezbedni na Internetu?

Seminarski rad u okviru kursa
Metodologija stručnog i naučnog rada
Matematički fakultet

Nevena Ajvaz, Natalija Jovanović, Marija Milićević, Tijana Nikčević
nevena.ajvaz@hotmail.com, natalija.jovanovic996@gmail.com,
marija.milicevic.10.23@gmail.com, tijana.nikcevic1@gmail.com

April 2019.

Sažetak

Internet je jedno od najmoćnijih oružja današnjice koji nudi mnoge pogodnosti ako se koristi u prave svrhe. Bezbednost na Internetu je jako veliki problem i u vezi sa tim upoznaćemo se sa najčešćim vrstama sajber napada, kriminala i pojmom glasanja putem Interneta. Videćemo zašto je naša bezbednost ugrožena i kroz primere poznatih napada opisati načine na koje se ona narušava.

Sadržaj

1 Uvod

U ovom radu ćemo se na početku upoznati sa pojmom sajber kriminala, kao i problemom rasprostranjenosti sajber napada. Dalje će biti prikazane 3 najčešće vrste napada - fišing, SQL injekcija [1] i DoS. Sajber kriminal brzo napreduje, što prouzrokuje razvoj i nastanak novih vrsta napada. U petom poglavlju, koje se odnosi na primere napada, biće prikazani problemi najvećih svetskih kompanija i država, i kako su se one suočavale sa tim. Nakon ovoga, pozabavićemo se temom glasanja putem Interneta.

2 Pojam sajber kriminala

Visokotehnološki ili sajber kriminal (eng. *cyber criminal*) predstavlja moderni vid kriminala, tačnije, putem računara. Sajber kriminalci su osobe ili grupe ljudi koji koriste tehnologiju kako bi izveli zlonamerne aktivnosti putem mreže sa ciljem da ukradu osetljive podatke neke firme, lične informacije ili da profitiraju [4].
Zakoni koji se odnose na ovu vrstu kriminala se dopunjuju i razvijaju u zemljama širom sveta. Nerazvijene zemlje su najizloženije sajber napadima. U takvim zemljama je zakon o ovoj oblasti slabo definisan, a u nekim ni ne postoji. Takođe, veoma je teško pronaći i uhapsiti zločinca u sajber kriminalu jer su dokazi često nepostojeći.

Treba napraviti razliku između sajber kriminalca i hakera. Sajber kriminalci sa lošim namerama vrše upad u računare, dok hakeri traže inovativne načine da koriste sistem, bili ti načini loši ili dobri.

3 Vrste sajber napada

U mnogim zemljama, Internet odvija ključnu ulogu u svakodnevnom životu ljudi. Olakšava virtuelnu komunikaciju među ljudima, podstiče razvoj novih poslovnih modela i kompanija, menja način na koji ljudi kupuju. U 2018. godini, transfer novca koji uključuje prodaju i kupovinu putem Interneta, iznosila je oko $2800 milijardi. Prema statističkim studijama [8], smatra se da će u 2021. ta vrednost iznositi oko $4.88 biliona. Iz ovih razloga, nije neobično da je sa porastom popularnosti Interneta porasla i stopa kriminala na njemu. U ovom poglavlju otkrivamo tri vrste napada putem Interneta.

3.1 Fišing (eng. *phishing*)

Fišing je vrsta društvenog inženjeringa (eng. *social engineering*)[1] gde se napadač pomoću elektronske pošte ili zlonamernih veb sajtova lažno predstavlja kao pouzdana organizacija ili kompanija kako bi prikupio lične podatke od pojedinca ili kompanije [3]. Engleski termin *phishing* je prvi put korišćen 1996. a nazvan je po pecanju jer mejlovi služe kao mamac kojim se ljudi navode da daju svoje podatke. „Ph“ umesto „f“ u zapisu reči je aluzija na termin *phreaks* koji označava ljude koji su eksploatisali telekomunikacije, a neki ih smatraju i prvim hakerima [5]. Napadi fišinga se često sastoje od slanja korisnicima mejlova koji izgledaju kao da su iz

[1] Obmana kojom se manipuliše ljudima da daju poverljive informacije.

bankarske ili finansijske institucije ili veb servisa preko kojeg pojedinac ima račun. Cilj fišinga je da prevari primaoca da da svoje podatke za prijavljivanje ili druge osetljive informacije. Na primer, napadač može da pošalje milione mejlova sa botnet-a[2]. Poruke obaveštavaju primaoce da je njihov nalog za elektronsku trgovinu bio kompromitovan i upućuju ih na veb lokaciju gde bi rešili problem. Korisnici koji kliknu na link dođu do veb stranice koja je napravljena tako da podseća na originalni sajt za elektronsku trgovinu. Kada se nađu na sajtu, od njih se traži korisničko ime, lozinka i druge privatne informacije. Te informacije mogu da se iskoriste za krađu identiteta.

Ciljano orijentisan fišing (eng. *spear phishing*) je varijanta fišinga u kojoj napadač bira adrese elektonske pošte tako da cilja jednog ili određenu grupu primalaca. Na primer, napadač može ciljati starije osobe kao osobe koje se smatraju lakovernijima ili članove grupa koji imaju pristup vrednim informacijama. Ciljano orijentisan fišing može biti veoma delotvoran jer omogućava napadaču da uobliči napad tako da žrtva zbog hitnosti ili poverenja određenim osobama bude manje oprezna. Za ovo je potrebno da napadač prikupi lične podatke o žrtvi, kao što su imena prijatelja, poslodavac, rodni grad, lokacije koje posećuje, šta je nedavno kupila na mreži itd. Na primer, napadač može da pošalje mejl ka nekoliko ljudi koji izgleda kao da je od njihovog direktora, gde im je poslat poziv na sastanak putem Gmail-a, a link u poruci navodi primaoce da se prijave na Gmail da prisustvuju sastanku.

Fišing se pojavio negde oko 1995., ali je postao čest tek nakon 10 godina. Prvi napadi bili su vezani za AOL (eng. *America Online*), u to vreme najpopularniji internet provajder[7]. 2000ih godina su napadi prešli na platne sisteme poput E-Gold, eBay i PayPal. Zanimljivo je povećanje napada na kinesku elektronsku trgovinu, što ukazuje na povećanje važnosti kineske ekonomije [6]. U tabeli 1 je prikazana količina sajtova za fišing koje je otkrila APWG (eng. *Anti-Phishing Working Group*) tokom godina [2].

Tabela 1: Količina sajtova za fišing tokom godina

godina	2015	2016	2017	2018
br. otkrivenih sajtova	789 068	1 397 553	662 795	785 920

3.2 SQL injekcija

SQL[3] injekcija je umetanje dela ili celog SQL upita obično preko polja za unos na veb stranici. Ukoliko ovako nešto uspe može se pristupiti osetljivim podacima iz baze, mogu se modifikovati podaci, izvršiti administrativne operacije nad bazom itd.

Primer 3.1

```
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users WHERE UserId = " +
    txtUserId;
```

[2]Mreža privatnih računara, zaraženih zlonamernim softverom, koji se kontrolišu kao grupa bez znanja vlasnika, npr. za slanje spama.

[3]Standardni jezik za skladištenje, manipulaciju i dohvatanje podataka u bazama podataka.

U primeru 3.1 kreira se SELECT upit dodavanjem sadržaja promenljive txtUserId na select string. Sadržaj promenljive je sadržaj polja za unos korisničkog id-a.

Jedan od načina upotrebe SQL injekcije zasniva se na činjenici da je `1=1` uvek istinito. Pod pretpostavkom da je korisnik u polje za unos uneo `105 OR 1=1`, SQL upit iz primera 3.1 bi izgledao ovako:

```
SELECT * FROM Users WHERE UserId = 105 OR 1=1;
```

Ovakav upit vratiće sve redove tabele „Users“. Šta ako tabela „Users“ sadrži imena i šifre? Može se pristupiti svim imenima i šiframa iz baze jednostavno dodavajući `105 OR 1=1` u polje za unos korisničkog imena.

`""=""` je uvek istinito.Ovo je još jedan način upotrebe SQL injekcije.

Primer 3.2

```
uName = getRequestString("username");
uPass = getRequestString("userpassword");

sql = 'SELECT * FROM Users WHERE Name ="' + uName + '"
    AND Pass ="' + uPass + '"'
```

Ukoliko naš kôd izgleda kao u primeru 3.2 može se pristupiti korisničkim imenima i šiframa u bazi unoseći `" OR ""="` u polje za šifru i u polje za korisničko ime. Kôd na serveru će kreirati ispravan SQL upit:

```
SELECT * FROM Users WHERE Name ="" OR ""="" AND Pass =""
    OR ""="";
```

Ovakav upit vratiće sve redove iz tabele „Users“.

Mnoge baze podržavaju grupu SQL upita razdvojenih ; simbolom. Ukoliko bi korisnik u polje za korisnički id uneo `105; DROP TABLE Suppliers`, SQL upit iz primera 3.1 izgledao bi ovako:

```
SELECT * FROM Users WHERE UserId = 105; DROP TABLE
    Suppliers;
```

Zaštita od ovakvih napada je moguća korišćenjem SQL parametara. To su vredosti koje su dodate SQL upitu u vreme izvršavanja na kontrolisan način.

Primer 3.3

```
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users WHERE UserId = @0";
db.Execute(txtSQL,txtUserId);
```

Primer 3.3 je deo koda u ASP.NET-u u kome se koriste parametri. Parametri su predstavljeni znakom @. SQL mehanizam proverava parametre kako bi se uverio da su ispravni i da se tretiraju bukvalno a ne kao deo SQL-a koji se izvršava.

3.3 DoS napadi

https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos

DoS (eng. *Denial-of-Service*) napad je radnja napravljena tako da spreči legitimitne korisnike da koriste usluge računara, tj. napadač utiče da mašina ili mrežni resurs budu nedostupni korisnicima tako što privremeno ili neograničeno ometa usluge hosta (domacina - dodaj ref) povezanog na Internet. DoS napad moze da uključi neovlašćeni pristup jednom ili više računarskih sistema, ali cilj napada nije krađa informacija, nego remećenje sposobnosti servera da odgovori na korisničke zahteve tako što zatrpava metu mrežnim saobraćajem ili šalje informacije koje aktiviraju razne nezgode. Ometanje normalnog rada računarskih usluga može da proizvede značajnu štetu. Firma koja se bavi nekom vrstom prodaje putem Interneta može da izgubi posao, vojsci može da se prekine komunikacija, Vladi ili nekoj neprofitnoj organizaciji može da se desi da ne može da prenese svoju poruku javnosti.

DoS napad je primer "asimetričnog"napada, tj. napada u kome jedna osoba može dosta da naškodi velikoj organizaciji. Pošto se terorističke organizacije specijalizuju za asimetrične napade, neki strahuju da će DoS napadi postati važan deo terorističkog oružja.

3.3.1 DDoS napadi

Dodatni tip DoS napada je DDoS (eng. *Distributed Denial-of-Service*) napad. Glavna razlika je u tome što meta nije napadnuta sa jedne lokacije, već sa više njih odjednom. Do DDoS napada se dolazi kada višestruki sistemi vode sinhronizovani DoS napad na jednu metu. Podela hostova koji određuju DDoS daje napadaču više prednosti:

- Napadač može iskoristiti veći kapacitet resursa mašine kako bi izvršio ozbiljan razoran napad
- Domen ili resurs napadnutog objekta se teško određuje zbog slučajne podele napadačkih sistema
- Teže je ugasiti više mašina nego jednu
- Pravu napadačku grupu (eng. *attacking party*) je veoma teško identifikovati, jer se oni prikrivaju iza mnogih (uglavnom kompromitovanih) sistema

Mnoge sigurnosne tehnologije su razvile mehanizme za odbranu od mnogih vrsta DoS napada, ali, zbog jedinstvenih karakteristika, DDoS se još uvek smatra ozbiljnom pretnjom.

4 Sajber kriminal

http://docshare04.docshare.tips/files/23471/234718626.pdf
deo Advancement of Computer and Network Attack and Exploitation Methodologies (163-164)

Glavni trend koji pokreće evoluciju računarskih napada i ekspoatacija uključuje motiv rasta profita zasnovanog na zlonamernom kodu (eng. malware, malicious code). Neki napadači prodaju prilagođeni zlonamerni kod za kontrolu mašina žrtava kupcu koji je najviše ponudio. Mogu iznajmiti gomile zaraženih sistema, koji su korisni za isporuku nepoželjne pošte (spamova), fišing shema, DoS napada ili za krađu identiteta. Špijunske

kompanije i preterano agresivni oglašivači (popravi) kupuju takvu vrstu koda kako bi se ubacili (infiltrirali) i kontrolisali žrtvine mašine. Jedna zaražena mašina na kojoj iskašu reklame i prilagođavaju se rezultati pretrage može da košta svega $1 mesešno. Ključni logger (???) na zaraženoj mašini može da pomogne napadaču da skupi brojeve kreditnih kartica i ukrade $1,000 ili više od žrtve pre nego što se otkrije prevara. Ako kontroliše 10,000 mašina, napadač može solidno da profitira od sajber kriminala. Organizovane kriminalne grupe mogu okupiti grupu takvih napadaša kako bi stvorile biznis, što izaziva porast industrije zlonamernog koda. Krajem devedesetih godina proslog veka, većinu malvera su pravili entuzijasti, ali danas su profesionalni napadači stavili cenu na svoj malver. Njihovi profitni centri daju sredstva koja se mogu koristiti za istraživanje i razvoj kako bi se stvorio snažan zlonameran softver i ometali poslovni modeli, kao i finansirali drugi zločini.

Kada kriminalci budu otkrili pouzdan nacin za zaradu novca na ovoj grani kriminala, broj incidenata ovog tipa će se neizbežno povecati. Računarski napadači su osmislili različite poslovne modele koji su niskog rizika, tako da je mala verovatnoca da će napadač biti uhvacen ukoliko pazljživo skriva svoje tragove. Tako mogu da se zarade stotine hiljada ili čak milioni dolara.

Faktor koji podstiče rast sajber napada je bot (skracenica od reci *robot*) softver. Ovaj softver dozvoljava napadaču da kontroliše neki sistem širom Interneta. Jedan napadač ili grupa napadača moze da postavi ogromne botnetove (grupe zaraženih mašina) širom sveta. Mašine koje kontrolišu botovi omogućavaju napadačima da postavljaju virtualne superračunare koji mogu da predstavljaju rivale nacionalnoj računarskoj snazi. Mogu da koriste te resurse da bi stvorili ogromnu poplavu, provale (eng. crack) kripto ključeve ili lozinke, ili da bi istražili osetljive finansijske podatke koji se koriste za krađu identiteta.

Botovi i ostali alati koji se koriste za napade su postali veoma modularni, svaki modul se sastoji iz softverskih komponenti koje omogućavaju napadačima da brzo menjaju funkcionalnost kako bi pokrenuli nove vrste napada. Obični botovi danas sadrže 50 do 100 različitih funkcionalnih modula; napadač može da ugasi ili odstrani module koji nisu potrebni za dati napad, dok lako integriše nove karakteristike (funkcije) koda. Drugi modularni napadački alati sadrže eksploatacione okvire (eng. exploitation frameworks) koji prave pakovani eksploatacioni kod koji može da se ubaci (infiltrira) u ciljnu mašinu koja je ranjiva (zato što je pogrešno konfigurisana ili nepovezana).

Ubrzavajući evoluciju, napadači se sve više oslanjaju na bot kod koji se sam preobražava, dinamički stvarajući funkcionalno ekvivalentnu verziju sa različitim skupovima osnovnog koda. Takav polimorfni kod pomaze napadačima da izbegnu alate za detekciju koje antivirusi i *antispyware* softveri[4] danas koriste. Ovaj dinamički samopodešavajući kod je teze filtrirati, s obzirom da konstantno menja svoj osnovi softver. Ova "pokretna meta"koda otežava analizu od stane branilaca. Polimorfni kod podstiče ciljeve napadača jer napadači imaju dužu kontrolu nad botnetom izbegavajući filtriranje i detekcije, tako da mogu što više novca da zarade od zaraženih sistema.

[4]Vrsta programa napravljena za sprečavanje i otkrivanje neželjenih instalacija špijunskih softvera i uklanjanje tih programa ukoliko su instalirani.

5 Sajber napadi

Sajber napad predstavlja napad od računara do računara koji povređuje poverljivost, integritet i informacije koje se nalaze na napdanutom računaru [6]. U ovom poglavlju ćemo se susresti sa nekim primerima napada na države i velike svetske gigante u poslednjih deset godina.

5.1 Primeri samostalnih napada

DŽENSON DŽJEMS ANČETA 2004. i 2005. je Dženson Džejms Ančeta, radnik u jednom Internet kafeu, napravio mrežu od oko 400,000 botova, uključujući i računare kojima upravlja Ministarstvo odbrane SAD-a. Softveri za reklame (adware companies), spameri i ostali su platili Ančeti da koriste te računare. Nakon što ga je FBI uhapsio, Ančeta se izjasnio krivim za razne optužbe, uključujući prekršavanje zakona o zlostavljanju računara kao i CAN-SPAM zakon (Computer Fraud Abuse Act and the CAN-SPAM Act). U maju 2005., federalni sudija je osudio Ančetu na 57 meseci zatvora i tražio od njega da plati $15,000 američkoj Vladi zbog napada na Ministarstvo odbrane. Zbog njegovih ilegalinih aktivnosti, vlada je Ančeti oduzela njegov 1993 BMW, više od $60,000 u kešu, kao i njegovu računarsku opremu.

PHARMAMASTER Izraelska kompanija Blue Security je napravila sistem za zastrašivanje spamova kako bi pomogla ljudima koji ne žele da primaju spampve. Blue Security je prodavala svoj sistem preduzećima, dok su individualci mogli besplatno da štite svoje računare. Oko pola miliona ljudi se prijavilo za ovu besplatnu uslugu. Korisnici su na svojim računarima učitali bot po nazivu Blue Frog koji je integrisan sa Yahoo! Mail-om, Gmail-om, Hotmail-om i provera da li su dolazeći mejlovi spamovi. Kada naiđe na spam poruku, bot kontaktira Blue Security server kako bi otkrio izvor tog mejla i zatim spameru salje opt-out poruku (da prekine da salje takvu vrstu mejlova).

Spameri koji neselektivno salju mejlove na milione adresa su počeli da primaju stotine hiljada opt-out poruka, koje su ometale njihove operacije. Šest najboljih svetskih spamera se dogovorilo da koristi softver za filtriranje koji je razvio Blue Security kako bi odstranili Blue Frog korisnike sa svojih mejl lista.

Jedan spamer, čiji je nadimak bio PharmaMaster, nije se povukao. On je pretio Blue Frog korisnicima porukama kao sto je na primer sledeća: "Nažalost, zbog taktika koje koristi Blue Security, primaćete ovu poruku ili druge besmislene spamove 20-40 puta vise nego inače". On je ispoštovao svoje pretnje, pa je 1. maja 2006. počeo da šalje Blue Frog korisnicima 10 do 20 puta više spamova nego sto obično prime.

Narednog dana je počeo da napada sam Blue Security. Lansirao je DDoS napad sa desetina hiljada botova ciljajući Blue Security servere. Ogromna količina dolaznih poruka je onemogucila Blue Frog uslugu. Kasnije su se DDoS napadi fokusirali na druge kompanije koje pružaju internet usluge Blue Security-u. Na kraju su napadi ciljali preduzeća koja su placala usluge Blue Seciruty-u. Kada je Blue Security shvatio da ne može da zaštiti svoje klijente od DDoS napada i mejlova sa virusima, nevoljno je prekinuo svoju uslugu.

AVALANCHE GANG Avalanche Gang je ime dato kriminalnom preduzeću koje je odgovorno za više phishing napada nego bilo koja druga organizacija. Anti-Phishing Working Group (APWG) je procenila da je Avalanche Gang odgovoran za dve trećine svih phishing napada lansiranih u drugoj polovini 2009. U drugoj polovini 2010., APWG je zapazila da je Avalanche skoro prestao sa phishing napadima, vodeci APWG da spekuliše da je Avalanche menjao strategije i fokusirao se na širenje neželjene pošte koja ljude uvlači u preuzimanje virusa Zeus trojanca.

ALBERT GONZALEZ Albert Gonzalez je 2010. osuđen na 20 godina zatvora nakon što se izjasnio krivim za koriscenje SQL injekcija kako bi ukrao više od 130 miliona brojeva kreditnih i debitnih kartica. Neki od tih brojeva su prodati onlajn, što je dovelo do neovlašćenih kupovina i povlačenja banaka. Ciljevi napada su bili Heartland Payment Systems, 7-Eleven, Hannaford Brothers Supermarkets, TJX, DSW, Barnes & Noble, OfficeMax, and the Dave & Buster lanci restorana. Većina brojeva je ukradena od firme Heartland Payment Systems, procenjujući gubitak na $130 miliona.

5.2 Primeri napada na države

1. GRUZIJA (2008)
   Gruzija je jedna od bivših Sovjetskih republika koja je stekla nezavisnost 1991. gidine. Južna Osetija, oblast na teritoriji Gruzije koja je pripadala Rusiji do 1991, nakon kratkog rata iste godine, postaje i međunarodno priznata kao autonomna pokrajna Gruzije. Nakon provokacije separatista u Južnoj Osetiji, Gruzija šalje vojsku na ovu teritoriju 7. avgusta 2008. godine. Ruske snage su 8. avgusta ušle u Južnu Osetiju i ove dve strane su se borile četiri dana. Ovaj sukob je ostao zapamćen i iz razloga što je gruzijska vlada i pre nego što je ruska vojska došla na teritoriju Južne Osetije imala problem sa velikim DDoS napadom. Njihova vlada nije bila u mogućnosti da komunicira sa ostatkom sveta. Mnogi veb sajtovi su bili srušeni na nekoliko sati. Gruzijska vlada je bila primorana da lokacije nekih svojih veb servera prebaci na SAD. Postojale su sumnje je da je napad izvrvršila grupa kriminalaca pod nazivom "Russian Business Network", smeštenih Sent Peterburgu u Rusiji, ali je ostalo nerazlučeno da li je ova grupa imala neke veze sa ruskom vojskom.
   Na isti dan godinu dana kasnije, Tviter je bio onesposobljen u celom svetu na nekoliko sati zbog masovnih DDoS napada. Maks Keli, šef za bezbednost u kompaniji Fejsbuk, rekao je da je svrha napada bila da se spreči objavljivanje teksta gruzijskog političkog blogera, pozivajući se na činjenicu da su istovremeno pali i ostali sajtovi koje je ovaj bloger koristio. Ti sajtovi su bili Fejsbuk, LiveJournal i Gugl.

2. SAD I JUŽNA KOREJA (2009)
   DDos napad na američku i južnokorejsku vladu je izvršen tokom vikenda uoči 4. jula, američkog Dana nezavisnosti. Tom prilikom zabeležen je pad više od trećine veb sajtova u ovim državama. U Americi je napadnuta Bela kuća, američki trezor, Tajna služba, njujoršku berzu i kompaniju NASDAQ. U Južnoj Koreji, DDoS napad je izvršen na Plavu kuću(predsednička palata), Ministarstvo odbrane i Narodnu skupštinu.
   Ova vrsta napada se smatra relativno malom jer je izvršen uz pomoć

botnet-a(naći referencu za botnet) koristeći između 50 i 65 hiljada računara, što se smatra malom cifrom u poređenju na velike napade gde se koristi oko milion računara. Ipak, ova vrsta napada je ostala zapamćena i po tome što su južnokorejski sajtovi ostali nedostupni do 9. jula. Pretpostavljalo se da je napad izvršen kao vid osvete jer su Ujedinjene Nacije uvele određene sankcije Severnoj Koreji u tom periodu. I do danas se još uvek ne zna ko je tačno izveo ovaj napad jer su napadači koristili računare koji su bili u posedstvu drugih ljudi.

5.3 Primeri napada na kompanije

1. Yahoo
   Yahoo je jedan od najvećih giganta na internetu. Ova kompanija je 2016. godine objavila informaciju da je bila žrtva jednog od najvećih napada u istoriji; 2013. godine je grupa hakera kompromitovala tri milijarde naloga korisnika. Pored imena, datuma rođenja, imejl adresa i šifara, zaštitna pitanja i odgvori su takođe otkriveni. Pored ovog napada, 2014. je zabeležen još jedan napad na ovu kompaniju. Tada su obelodanjena imena, imejl adrese, datumi rođenja i brojevi telefona 500 miliona korisnika. Ovoga puta su šifre ostale zaštićene.

2. eBay
   Ova kompanija se bavi prodajom proizvoda putem interneta. Bila je napadnuta u maju 2014. kada su otkrivena imena, adrese, datumi rođenja i enkriptovane šifre(naći referencu za enkripciju) od 145 miliona korisnika. Kriminalci su "upali"u bazu tako što su koristili kreditacije troje zaposlenih i imali su pristup unutrašnjosti 229 dana.U tom periodu su imali vremena da pristupe bazi podataka korisnika. Informacije koje se tiču finansija kao što su brojevi kreditnih kartica su ostale zaštićene jer se ta vrsta podataka čuva u odvojenoj bazi.

3. Uber
   Uber je američka kompanija koja se predstavlja kao mreža koja pruža uslue transporta. Ona je 2016. bila napadnuta od strane samo dva hakera koji su uspeli da dođu do imena, imejl adresa i brojeva telefona 57 miliona korisnika Uber aplikacije. Takođe, otkriveni brojevi vozačkih dozvola 600000 vozača na ovoj platformi.
   Hakeri su pristupili i Uberovom nalogu na GitHub platformi(referenca) gde su pronašli korisničko ime i lozinku kreditacije ka AWS nalogu(referenca). Uber je ovaj napad objavio godinu dana kasnije. Ova kompanija je platila 100000 američkih dolara hakerima da unište podatke.

6 Glasanje putem Interneta

Postoje mnogi načini na koje napadači mogu da naruše bezbednost umreženih računara. Međutim, praktičnost i niska cena obavljanja poslova putem interneta donose značajne prednosti, pa nije iznenađujuće da se onlajn rešenje često predlaže kada postoji problem sa tradicionalnim načinom. U ovom delu biće prikazani predlozi za sprovođenje izbora putem interneta.

6.1 Motivacija za glasanje putem interneta

Predsednički izbori 2000. godine su bili jedni od najneizvesnijih u istoriji SAD. Florida je bila država od glavnog značaja. Bez izbornih glasova na Floridi, ni demokrata Al Gor (eng. *Al Gore*), ni republikanac Džordž Buš (eng. *George V. Bush*) nisu imali većinu glasova. Posle ručnog prebrojavanja glasova u četiri veoma demokratske pokrajine, državni sekretar Floride je izjavio da je Buš pobedio sa razlikom od 537 glasova u odnosu na Al Gora. Bušova prednost bila je neverovatno mala: manje od 2 glasa na svakih 10.000 glasova.

Većina ovih okruga koristila je mašinu za glasanje u kojoj birači biraju kandidata tako što olovkom probuše rupu u kartici pored odgovarajućeg imena (slika dodati). Uočene su dve nepravilnosti u glasanju upotrebom ovih mašina. Prva nepravilnost je da ponekad olovka ne probuši glatko rupu, ostavljajući mali, pravougaoni komad kartice koji visi sa jednog ili više uglova. Takve glasove obično ne uračuna mašina za automatsko prebrojavanje glasova, pa se ručno prebrojavanje fokusiralo na identifikaciji takvih glasačkih listića. Druga nepravilnost bila je da su neki birači u okrugu Palm Beach bili zbunjeni glasačkim listićima i pogrešno probušili rupu koja odgovara kandidatu Patu Bakananu umesto rupe za demokratskog kandidata Al Gor. Ova konfuzija je možda koštala Al Gora glasova koji su mu bili potrebni za pobedu na Floridi.

6.2 Predlozi

Problemi sa izborima na Floridi doveli su do raznih akcija za poboljšanje pouzdanosti glasačkih sistema u Sjedinjenim Državama. Mnoge države su zamenile papirne sisteme elektronskim glasačkim aparatima za direktno očitavanje. Druge su predložile da se koristi glasanje putem interneta, makar radi odbacivanja korišćenja glasačkih listića. U stvari, onlajn glasanje već postoji. Korišćeno je u Aljasci 2000. godine za republikansku anketu za predsedničkog kandidata i u Arizoni za demokratsku predsedničku listu za premijera. Na predsedničkim izborima 2004. godine, 100.000 Amerikanaca u vojsci i onih koji žive u inostranstvu je trebalo da ima priliku da glasa preko interneta kao deo eksperimenta za sigurnu elektronsku registraciju i glasanje (eng. *"Secure Electronic Registration and Voting Experiment"*), ali se vlada predomislila u poslednjem trenutku. Mnoge zemlje su ispred Sjedinjenih Država po pitanju uvođenja glasanja preko interneta. Lokalni izbori u Ujedinjenom Kraljevstvu koristili su onlajn glasanje 2001. godine. Građanima koji žive u Sjedinjenim Državama bilo je dozvoljeno da koriste internet da biraju svoje predstavnike u Skupštini francuskih građana u inostranstvu. Estonija je bila prva zemlja koja je omogućila svim svojim građanima da glasaju putem interneta na lokalnim i nacionalnim izborima. Nekoliko kantona u Švajcarskoj je ustavnim promenama odobrilo internet kao zvaničnu opciju za glasanje, pored biračkih mesta i glasanja poštom.

6.3 Etička procena

U ovom poglavlju biće vršena diskusija o glasanju putem Interneta na osnovu prikazanih rizika i benefita. Diskusija podrazumeva da je glasanje sprovedeno preko interneta, implementirano preko veb pregledača, iako bi bilo slično da je korišćena neka druga tehnologija.

BENEFITI GLASANJA PREKO INTERNETA

- Glasanje preko interneta daje ljudima priliku da glasaju iz svojh domova, ukoliko nisu u mogućnosti da dođu do biračkog mesta.
- Glasovi koji se salju preko interneta mogu se prebrojati mnogo brže od glasova na papiru.
- Elektronski glasovi ne bi imali nikakvu dvosmislenost.
- Izbori koji su sprovedeni na internetu koštali bi manje nego tradicionalni izbori.
- Glasanje preko interneta eliminisalo bi rizik da neko manipuliše glasačkom kutijom u kojoj se nalaze glasački listići.
- Dok na većini izbora ljudi glasaju za jednog kandidata, drugi izbori omogucavaju da osoba glasa za više kandidata. Na primer, školski odbor može imati tri slobodna radna mesta, a od glasača se moze tražiti da glasaju za tri kandidata. Bilo bi lako isprogramirati obrazac za glasanje kako bi se sprečilo da ljudi glasaju za više ljudi nego što bi trebalo.
- Ponekad, dugi i komplikovani glasački papiri rezultiraju tome da glasač slucajno zaboravi da zaokruži kandidata za određenu poziciju. Veb forma bi mogla da se dizajnira da bude na više strana i da svaka strana ima kandidata za jednu poziciju.

RIZICI GLASANJA PREKO INTERNETA

- Glasanje preko interneta je nepravedno, jer daje predost onima koji su u finansijski boljoj situaciji tj. ljudima koji imaju računare i internet.
- Isti sistem vrsi autentifikaciju glasača i beleži glasački listić. Ovo otezava čuvanje privatnosti glasača.
- Glasanje preko interneta povećava mogućnost za kupovinu i prodaju glasova. Pretpostavimo da se osoba X slozi da glasa za kandidata Y u zamenu za isplatu od osobe Z. Ako osoba X glasa sa njegovog računara, moze da dozvoli osobi Z da gleda kako je glasao za Y, dokazujući na taj način da je ispunio svoje obećanje. Ovo je mnogo manje verovatno na zvaničnom biračkom mestu koje nadgledaju izborni zvaničnici.
- Veb lokacija koja održava izbore očigledna je meta DDos napada. Za razliku od korporativnih veb stranica, koje privlače pažnju tinejdzera hakera, veb stranica za nacionalne izbore mogla bi privući pažnju stranih vlada ili terorista koji pokušavaju poremetiti izborni proces.
- Virus bi mogao da promeni glas neke osobe, a da ta osoba čak i ne posumnja u ono što se desilo. Mnogi ljudi imaju fizički pristup računarima drugih ljudi, i to im daje mogućnost instaliranja aplikacija za obmanu glasača u nedeljama koje prethode izborima.
- *Trojanac* koji vreba na računaru glasača bi mogao da omogući da glasač bude posmatran. *Trojanac* bi čak mogao da omogući da neko drugi glasa umesto pravog glasača.
- Napadač moze da prevari korisnika da misli da je povezan sa serverom za glasanje kada je u stvari povezan sa lažnim serverom za glasanje koji je kontrolisan od strane napadača. Na primer, napadač moze da pošalje mejl u kojem se glasači pozivaju da kliknu na link da bi došli do mesta glasanja. Učinivši to, oni bi bili povezani sa lažnim glasačkim mestom. Napadač može tražiti potrebne informacije birača, a zatim koristiti te informacije da se poveže sa pravim biračkim mestom i glasa za kandidata za koga želi.

ZAKLJUČAK

„Siguran sistem za glasanje preko interneta je teorijski moguć, ali to bi bila prva sigurna umrežena aplikacija ikada stvorena u istoriji računarstva.“, napisao je Bruce Schneier.

Već postoji dokaz da je došlo sumnjivih radnji na izborima preko interneta. U aprilu 2001. Vivendi Universal, pariski medijski konglomerat, održao je glasanje preko interneta za svoje akcionare. Hakeri su napravili da se glasovi nekih velikih akcionara racunaju kao uzdržani. Ako ovakvi privatni izbori mogu privući pažnju hakera, pretpostavlja se da bi neki veći izbori bili atraktivnija meta.

Svaki izborni sistem koji se oslanja na bezbednost ličnih računara kojim upravljaju obični građani biće osetljiv na prevare. Samo iz tog razloga, postoji jak argument zašto vlada ne bi dozvolila da se na taj način sprovede glasanje.

7 Zaključak

Iz svega priloženog, korišćenje Interenta bi trebalo da bude odgovono. Videli smo da ni ozbiljne organizacije nisu uspele da se odbrane od zlonamernih napada. Stoga, svako od nas treba biti svestan ozbiljnosti napada kojim može biti izložen i oprezan prilikom ostavljanja ličnih i poverljivih informacija.

Literatura

[1] SQL Injection. https://www.w3schools.com/sql/sql_injection.asp.

[2] APWG.org. APWG News. https://www.apwg.org//apwg-news-center/.

[3] US-CERT (eng. *The United States Computer Emergency Readiness Team*). What Is Phishing? https://www.us-cert.gov/report-phishing.

[4] Trend Micro. Cybercriminals, 2019. https://www.trendmicro.com/vinfo/us/security/definition/cybercriminals.

[5] Phishing.org. History of Phishing. https://www.phishing.org/history-of-phishing.

[6] Michael J. Quinn. *Ethics for the information age*. Pearson Education, One Lake Street, Upper Saddle River, New Jersey 07458, 2015.

[7] Koceilah Rekouche. Early Phishing. https://arxiv.org/abs/1106.4692.

[8] Statista. Retail e-commerce worldwide. https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/.

1. https://www.trendmicro.com/vinfo/us/security/definition/cybercriminals
2. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
3. https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos
4. https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html
5. http://docshare04.docshare.tips/files/23471/234718626.pdf str 163-164