ZAŠTITA PODATAKA INFORMACIONOG SISTEMA: STUDIJA SLUČAJA JEDNE KOMERCIJALNE BANKE U BOSNI I HERCEGOVINI

INFORMATION SYSTEM DATA SECURITY: CASE STUDY OF ONE COMMERCIAL BANK IN BOSNIA AND HERZEGOVINA

Miodrag Peranović
Univerzitet u Istočnom Sarajevu, Ekonomski fakultet Brčko
miodrag.peranovic.efb@gmail.com

Nenad Mirkov
Univerzitet u Novom Sadu, Ekonomski fakultet u Subotici
nenad.mirkov@gmail.com

Otilija Sedlak
Univerzitet u Novom Sadu, Ekonomski fakultet u Subotici
otilijas@ef.uns.ac.rs

APSTRAKT

Jedan od najvažnijih problema sa kojim se susreće svaka finansijska institucija je zaštita podataka klijenata, i drugih poslovnih informacija. U radu se vrši analiza potencijalnih rizika u sistemu upravljanja zaštitom informacija u bankarskim institucijama. Kao osnov za analizu služi studija slučaja jedne komercijalne banke, čija je centrala grupacije pretrpela DDoS napad u 2012.godini. U radu se zatim vrši dublja analiza implementiranih mera zaštite od budućih napada, navode nedostaci i predlažu mere unapređenja. Cilj ovog istraživanja je da pomogne kvalitetniju zaštitu oko informacione strukture organizacije, i spreči štetu koja može nastati prilikom DDoS napada.

Ključne reči: Distribuirano onemogućavanje usluga (DDoS), Međunarodna organizacija za standardizaciju - standard 27001, Sistem za upravljanje bezbednošću informacija, Sistem za proaktivnu zaštitu od napada

ABSTRACT

One of the major problems that every financial institution faces is the protection of client data, and other crucial business information. In this paper we analyse the potential risk in systems for managing information protection in banking institutions. As a basis for this survey we use a case study of a commercial bank which group headquarters was attacked in 2012, by DDoS breach. In-depth analyse was conducted on countermeasures which were implemented afterwards in particular bank as the protection from future DDoS attacks. We emphasize weaknesses and provide suggestions for the improvement of security measures. The goal of this survey is to provide help for potential victims, how to deploy better information security in financial institutions as well as prevent possible damage caused by DDoS attacks.

Key words: Distributed Denial of Service (DDoS), International Organization for Standardization - standard 27001, Information Security Management Systems, Introusion Prevention System

UVOD

Razvoj informacionih tehnologija uslovio je direktno oslanjanje poslovanja organizacije na informacionu strukturu i Internet kao komunikacioni kanal. Finansijske institucije poput banaka odavno koriste Internet za finansijske transakcije na međubankarskom tržištu novca, ali i kao uslugu svojim krajnjim korisnicima. Obzirom da je sama priroda Interneta takva da on predstavlja javni servis, ovo je otvorilo mnoga pitanja u domenu upravljanja rizicima koji se odnose na informacione tehnologije. U časopisima koji se bave finansijskim institucijama, tokom poslednje decenije često se susreću članci koji opisuju sajber napade na banke ili druge finansijske entitete. Hakeri su razvili veliki broj različitih metoda kojima mogu prouzrokovati veliku štetu i finansijski gubitak bankama. Neki od njih poput DDoS (Distributed Denial of Service) se mogu iznajmiti putem Interneta za manje od 20 dolara po času. Na ovaj način obaranje veb servisa ili servera postaje veoma jednostavno i dostupno pod uslovom da servisi nisu propisno zaštićeni.

Kako su rasle pretnje tako su se razvijali i sistemi koju treba da pruže kvalitetnu i bezbednu zaštitu od navedenih rizika. Organizacije koje se bave standardima su tokom poslednje decenije razvijale standarde

čijom primenom se stvara bezbednije okruženje za organizaciju. Serija standarda ISO 27000 propisuje standarde vezane za bezbednost informacija i razvijeni su od strane međunarodne organizacije za standarde (ISO) i međunarodne elektrotehničke komisije (IEC). Pored razvoja standarda, pomak se desio i na polju hardvera, pa sada postoje uređaji koji se postavljaju na mrežnu infrastrukturu i koji su u stanju da vrše prevenciju napada, a ne samo njegovu detekciju kao što je to do sada bio slučaj.

Međutim da bi se kvalitetno pristupilo rešavanju navedenih problema, neophodno je pre svega analizirati i razumeti koncepte poput kvantifikacije rizika, procene rizika i upravljanja rizikom. Rizik u domenu informacionih tehnologija, predstavlja proračun verovatnoće nastupanja neželjenih događaja, zasnovan na proceni ozbiljnosti uticaja ukoliko događaj nastane, verovatnoći da će nastati, i mogućnosti detekcije događaja ukoliko bi on nastao. Samo ukoliko se ove veličine razumeju i opišu, moguće je upravljati rizicima u IT-u i raditi na njihovoj prevenciji i sprečavanju.

Ovaj rad bavi se analizom ranjivosti informaciono-komunikacionih tehnologija, merama koje se mogu preduzeti radi njihove prevencije kroz empirijsku procenu uticaja primene standarda i hardverskih mera zaštite u bankarskom sistemu. U prvom poglavlju rada analizira se bezbednost informacija unutar sistema i analiziraju se najčešći problemi u bezbednosti koji omogućuju nastupanja neželjenih događaja (rizika). U drugom poglavlju analiziraju se aktuelni standardi na polju zaštite informacija u organizacijama i mogućnost njihove primene u bankama i drugim finansijskim institucijama. Treće poglavlje je studija slučaja jedne komercijalne banke u Bosni i Hercegovini. Na kraju, vrši se analiza anomalija dosadašnjih pristupa, i daju se sugestije za povećanje nivoa bezbednosti informacija. Zaključak je obrazložen u poslednjem poglavlju.

BEZBEDNOST INFORMACIJA U BANCI

Informacioni sistem igra veoma važnu ulogu u poslovanju svake banke. Njegovo pravilno funkcionisanje predstavlja srž upravljanja informacijama i omogućuje efikasno funkcionisanje organizacije kao i njenu konkurentnost na tržištu. Neadekvatna podrška informacionih sistema, strategijskim ciljevima, poslovnim operacijama i potrebama menadžmenta organizacije može ozbiljno ugroziti njen opstanak i uspeh. Kompanije kvalitetnim informacijama i njihovom upotrebom u bržem i boljem donošenju strateških odluka mogu steći značajnu prednost u odnosu na konkurenciju. Konačno, informacioni sistemi koji su zasnovani na IKT tehnologijama omogućuju bankama da se izbore sa nestabilnošću poslovnog okruženja.

Neophodnost uvođenja informacionih sistema zasnovanih na IKT tehnologijama je pored prednosti koje su naveli pomenuti autori, uneo i nedostatke, koji se manifestuju u vidu rizika na polju bezbednosti informacija. Ovi rizici mogu nastati usled nekog od sledećih faktora:
- tehničkih problema (otkazivanje nekog dela sistema);
- ljudske greške;
- sistemskih propusta;
- prevara, odnosno hakerskih napada;
- spoljnih faktora.

Svest o rastućem potencijalu napada sa neželjenim posledicama uticao je na sve veće investicije i ulaganja na polju bezbednosti informacija u bankama. Prevare i hakerski napadi na informacioni sistem banke, mogu strahovito uticati na imovinske gubitke banke. Pored bankarske imovine, žrtve mogu biti i krajnji korisnici, odnosno komitenti banke. Naravno banka je dužna nadoknaditi finansijsku štetu, tako da se ekonomski gledano sav gubitak prenosi na banku (Gates and Jacob, 2009), ali je gubitak mnogo veći ako se u obzir uzme poljuljano poverenje komitenata u bezbednost informacija i novca koje banka servisira. Shodno tome, ukoliko banka dokaže da poseduje kompetencije za sprečavanje prevara, i da konstantno radi na povećanju bezbednosti informacionog sistema, ona će ne samo zadržati postojeće klijente, već može i privući nove [Hoffmann and Birnbrich, 2012].

Vrste i tehnike koje se koriste u bankarskim prevarama

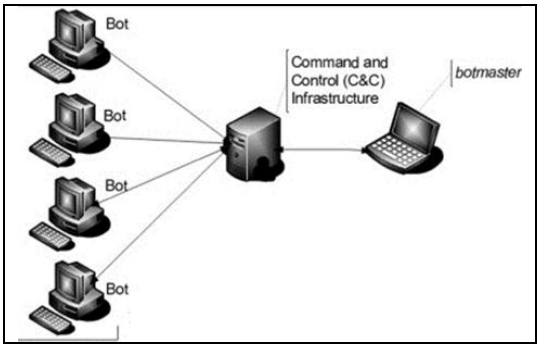
Razvoj Interneta i elektronske trgovine, pružio je sajber kriminalcima novo oružje kojim vrše svoja zlonamerna dela. Pravna regulativa je započeta u Americi, kada je 1986. godine američki kongres izglasao zakon o Internet kompjuterskoj prevari i zloupotrebi i zakon o privatnosti elektronskih komunikacija

[Marshall & Bailie, 2010]. Važno je napomenuti da su i u Srbiji, koja se smatra tehnološki zaostalom zemljom, prisutni svi oblici visokotehnološkog kriminala. Po podacima američkih službi nalazimo se čak na visokom trećem mestu u svetu po prevarama putem Interneta. Država je 2005. godine donela Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala [Lilić i Prlja, 2008] kao odgovor na ovaj problem.

Tehnike koje se najčešće koriste u napadima na računare i računarske mreže se mogu podeliti u tri grupe:
- kompjuterski virusi;
- DDoS napadi (Distributed denial of service);
- melveri (malwer - malicious software).

DDoS napadi predstavljaju pokušaje da se ciljani računar – server ili veb aplikacija u potpunosti zaguši tako da više nije u mogućnosti da izvršava zadatke za koje je predodređen/a. Najčešći ciljevi napadača su veb serveri banaka, ili sistema za plaćanje kreditnim karticama na Internetu. Nakon afere WikiLeaks-a i hapšenja Žulijana Asanža, došlo je do masovnih DDoS napada od strane Anonimusa (svetske hakerske mreže), koje Ričard Stalman (Stallman, 2010) naziva nekom formom Internet uličnih protesta.

Reč distribuirani u definiciji ove vrste napada podrazumeva napad u kojem učestvuje ogroman broj računara povezanih na Internet, i kojima upravlja napadač – *botmaster*, koristeći mrežne programe – *botnets*, koji se nalaze na svim računarima koji učestvuju u napadu i C&C (command and controll) server preko kojeg se vrši komunikacija sa botnetovima i sinhronizacija napada. Korisnici Interneta čiji računari su zaraženi botnet melverima nazivaju se zombijima i nesvesno učestvuju u napadima na ciljani server tako što šalju gomilu SYN ili UDP paketa na računar žrtve gušeći njegove resurse. Pored ove tehnike, uočena je i tehnika upotrebe BitTorrent servisa kao oružja za sprovođenje DDoS napada. Naime ovaj P2P (peer-to-peer) sistem za razmenu fajlova je izuzetno eksploatisan od Internet populacije, pa je samim ti postao veoma pogodan kao alat koji bi napadači mogli iskoristiti. Obzirom da sistem funkcioniše pomoću liste adresa na koju se šalju preuzeti paketi (trakera), dovoljno je izmeniti IP adrese i izvršiti određena vremenska podešavanja da bi se izveo masovni napad na targetiranu adresu [El Defrawy et al, 2007]. Na slici 1. dat je shematski prikaz DDoS napada.



Slika 1. Shematski prikaz DDoS napada korišćenjem Botneta [Silva et al, 2012]

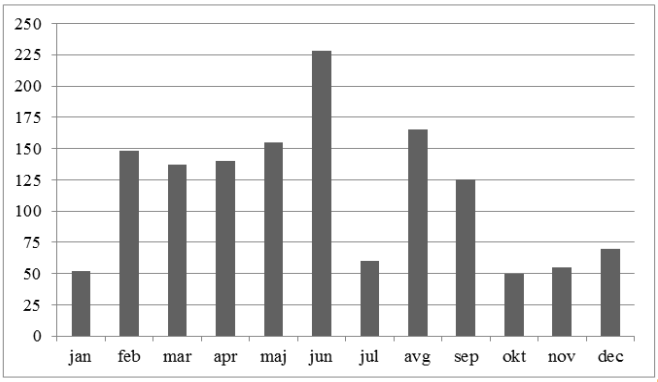
Veoma je interesantna a isto toliko i zabrinjavajuća činjenica da se DDoS napadi, mogu veoma jednostavno „iznajmiti“ na Internetu na određeno vreme (najčešće u časovima). Kriminalne organizacije se čak otvoreno reklamiraju na Internetu pod izgovorom usluge za stres testiranja [Kassner, 2013].

Motivi ovih napad mogu biti ucenjivanje, ometanje konkurencije, politički motivi i slično. Međutim septembra 2012. godine FBI je izdao upozorenje finansijskim institucijama da su neki DDoS napadi imali za cilj skretanje pažnje sa napada koje su istovremeno sajber kriminalci izvršili radi neautorizovanih transakcija i čime su u stvari želeli sprečiti njihovo otkrivanje i sprečavanje [Symantec Corporation, 2013].

Učestalost napada na korporativne računarske sisteme je u stalnom porastu. U svom govoru na TED konferenciji James Lyne [2013] daje zapanjujuće podatke o tome kako se svakog dana pojavi 250.000 novih kompjuterskih virusa, i bude zaraženo oko 30.000 veb sajtova od čega je 80% u vlasništvu poslovnih organizacija. U izveštaju kompanije Symantec za 2012. godinu pominje se slučaj jedne velike bankarske organizacije koja se obratila za pomoć ovoj kompaniji jer je u aprilu 2012. bila žrtva velikog broja napada u samo jednom danu. Čak i nakon eliminacije problema, Symantec je utvrdio da su talasi napada nastavljeni

(međutim ovaj put uspešno odbijeni). Na slici 2. dat je grafikon sa prikazom prosečnog broja napada po danu u 2012. godini.

Oko 15% svih zlonamernih softvera (melvera) su melveri koji napadaju finansijske institucije. Statistika pokazuje i da antivirusni softveri uspevaju da smanje ovaj procenat, međutim napadi na banke se ne vrše samo distribucijom finansijskih melvera, već i drugim tehnikama poput fišinga i upotrebom trojanaca koji kasnije stvaraju rupe u sistemu za preuzimanje finansijskih melvera koje onda antivirusni softveri ne detektuju. Danas se koriste veoma sofisticirani trojanci koji su programirani na samouništenje nakon izvršenog preuzimanja malicioznog koda.



Slika 2. Targetirani napadi po danu u 2012. godini [Symantec Corporation, 2013]

Iako antivirusne kompanije svakodnevno izbacuju ažuriranja za baze virusa, problem predstavljaju algoritmi koji se nalaze na udaljenim serverima a služe za izmenu malicioznog koda tako da ga antivirusni programi ne detektuju. Ovaj metod se naziva serverskim polimorfizmom [Schouwenberg, 2008]. Naravno, dok god finansijski melver postoji na računaru, njegov kreator može lako doći do poverljivih podataka koje banka koristi u svakodnevnom poslovanju.

Tehnike koje se koriste u bankarskim prevarama su: angažovanje posrednika za transfer ukradenog novca, fišing, automatizovani napadi, preusmeravanje saobraćaja, MitM napadi (Man in the middle) i druge.

Angažovanje posrednika za transfer se koristi kada je finansijski melver već infiltriran u bankarski informacioni sistem. Međutim, banke imaju instalirane okidače koji blokiraju automatske veće transfere novca, ili transfere u zemlje koje su na listi sumnjivih transfera. Tada sajber kriminalci legalno angažuju lica u zemlji gde se nalazi banka, kao finansijske menadžere, i koji obično nisu svesni da su upleteni u sajber kriminal. Na njihove račune se vrše manji transferi od čega oni zadržavaju proviziju, a ostatak se prebacuje na račun kriminalaca putem servisa poput MoneyGram.com i sličnih koji garantuju poverljivost podataka.

Fišing (*phishing*) je sada već prilično zastareo metod za pribavljanje identifikacionih parametara korisnika, podataka sa kreditne kartice i slično. Zasniva se na masovnom slanju mejl poruka koje navodno stižu od strane banke ili druge organizacije. Cilj je da se korisnik najčešće uputi na lažnu veb stranicu, koja po izgledu nalikuje originalu, na kojoj korisnik pokušava login i time šalje svoje podatke sajber kriminalcu.

Redirekcija saobraćaja i MitM napadi, se zasnivaju na preusmeravanju korisnika na lažnu veb stranu, kada on pokuša da otvori sajt banke za elektronsko plaćanje ili slično. Preusmeravanje se obično vrši modifikacijom vindovsovog hosts fajla, u kojem se mogu i ručno pomoću bilo kog editora uneti redirekcije. Hosts fajl će biti kontaktiran pre DNS-a (*domain name server*).

Većina malicioznih softvera koristi i *HTML injection* za infiltraciju tako što se veb strana banke modifikuje tako da korisniku prikaže jednostavan *pop-up* prozor u kojem se iz bezbednosnih razloga traži unos zaštićenih podataka. Obzirom da banke često putem iskačućih prozora zaista traže promenu lozinke iz bezbednosnih razloga, mnogim korisnicima ovo ne bude sumnjivo i jednostavno unesu podatke, koji su u stvari direktno prosleđeni napadaču. Treba napomenuti da je uspeh ovih prevara direktno baziran na psihološkoj osnovi, odnosno zavisan je od karaktera osobe, da li će ili ne, poverovati lažnoj strani i brzopleto uneti podatke.

AKTUELNE MERE ZAŠTITE BEZBEDNOSTI INFORMACIJA U BANKAMA

Bezbednost sistema podrazumeva primenu procesa zaštite od eventualnih anomalija i oštećenja koje mogu nastati nekim prirodnim putem, ili namernim delovanjem pojedinca ili grupe. Pod oštećenjima se podrazumeva narušavanje svojstava sistema kao što su integritet, dostupnost i poverljivost [Schechter, 2004].

U svakom poslovnom entitetu, informacija igra ključnu ulogu u uspešnom poslovanju, a nekada i samom opstanku kompanije, i kao takva mora biti propisno zaštićena i bezbedna. Informacije se čuvaju u različitim oblicima poput digitalnog, materijalnog (papir) ali i nematerijalnog u vidu znanja koje poseduju zaposleni.

U naučnoj javnosti postoji veliki broj istraživanja i radova na polju upravljanja rizikom i sistemom bezbednosti informacija. Komitet koji čine eksperti u ovoj oblasti posvetio se razvoju standarda koji bi važili na međunarodnom nivou u oblasti zaštite i bezbednosti informacija. Serija ovih standarda nazvana je Sistem upravljanja bezbednosti informacija (Information Security Management Systems – ISMS) i objavljena pod serijom standarda ISO/IEC 27000. U okviru standarda ISO/IEC 27001:2005 i ISO/IEC 27001:2013 (prvi je nastao u 2005. godine a drugi predstavlja reviziju istog standarda i objavljen je 2013. godine) propisuju se zahtevi za uspostavljanje upravljanja bezbednošću informacija. Međunarodni standard ISO 27001 posebno je pogodan za banke i finansijske institucije. Njegovom pravilnom implementacijom stvara se okruženje u kojem se rizici pravovremeno identifikuju i omogućuje se njihova eliminacija ili svođenje na prihvatljiv nivo. Standard omogućuje i kontinuirano praćenje i informacione bezbednosti u organizaciji.

Istraživanja koja je sprovela kompanija Certification Europe pokazuju na trend sve većeg prihvatanja standarda za sistem upravljanja bezbednosti informacija. Takođe je interesantan pokazatelj, da su organizacije koje su već ranije implementirale neke od međunarodnih standarda poput ISO 9001 mnogo lakše i brže implementirale i ISO 27001. Svakako, nije začuđujući podatak da su IT sektori u organizacija bili prvi koji su prihvatili standard. Ipak, stiče se utisak da i pored velike dobrobiti za organizaciju, prihvatanje ISO 27001 standarda nije na očekivanom nivou. Razlozi se nalaze u kompleksnosti pristupa, i njegovoj ceni. Mnogi autori su se bavili ovim pitanjem, i razvili originalne pristupe koji se sastoje od koraka koje treba preuzeti pre početka implementacije standarda. Alan Gillies preporučuje da se čelnici organizacije motivišu izradom plana koji će, između ostalog, sagledati i posledice nepreduzimanja mera, kvantifikacijom rizika i posledica i drugim [Gillies, 2011]. Korisnosti uvođenja standarda ISO 27001 mogu se taksativno nabrojati:

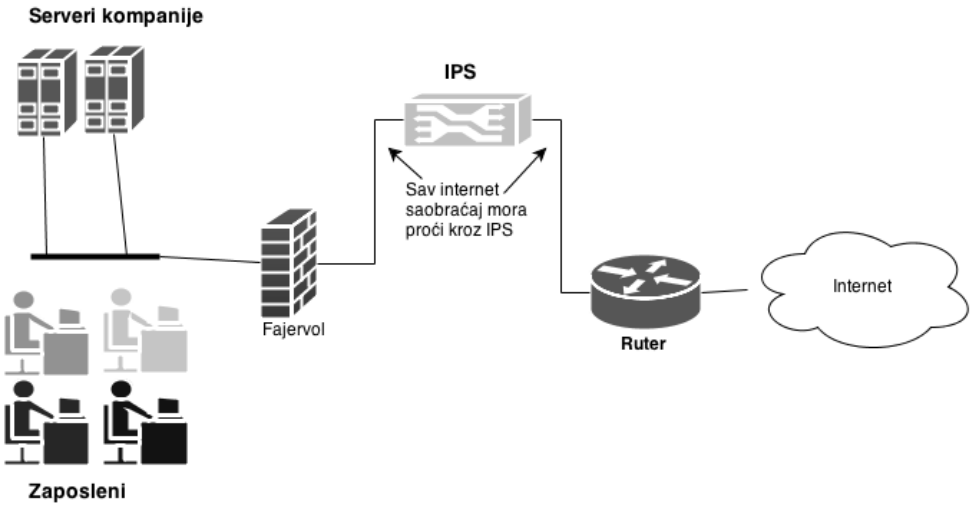
- standardizacija sistema za upravljanje bezbednošću informacija u celoj organizaciji;
- kvalitetnije ispunjenje zahteva klijenata za bezbednost informacija;
- smanjenje rizika od hakerskih napada i prevara;
- smanjenje rizika od gubitka klijenata;
- veće šanse za nove poslovne aranžmane;
- smanjenje rizika regulatornih kazni;
- smanjenje rizika od narušavanja reputacije organizacije;
- podizanje svesti o bezbednosti informacija unutar organizacije;
- omogućavanje lakše komunikacije između odeljenja u kojima su primenjeni standardi ISO 27001;
- bolje upravljanje IT imovinom i rizicima vezanim za tu imovinu.

Zapravo implementacijom ovog standarda kompanija ima bolju kontrolu nad protokom informacija, koje su elementarna čestica svih poslova. U mogućnosti je prezentovati svojim klijentima da je usvojila jak stav o usklađenosti na polju informacione bezbednosti.

Pored uvođenja standarda na polju upravljanja bezbednosti informacija, preporuka je da se za prevenciju napada koriste sistemi za proaktivnu zaštitu od napada (*Intrusion Prevention System – IPS*). Mnogi smatraju da su IPS-ovi proširena verzija IDS sistema (*Intrusion Detection System*) koji služe za monitoring mrežnog saobraćaja i šalju obaveštenja administratoru mreže u slučaju sumnje na neko zlonamerno ili neočekivano ponašanje na mreži. Međutim, sistemi za prevenciju napada (IPS) koriste drugačiji oblik kontrole pristupa u obliku aplikativnog sloja fajervola, pa se zbog toga to mišljenje smatra pogrešnim.

Ovi sistemi deluju tako što blokiraju potencijalno loš mrežni saobraćaj, i u potpunosti onemogućuju njegovo prodiranje u mrežu organizacije. Posebno se smatraju pogodnim za prevenciju DDoS napada, napada grubom silom (*brute force attacks*), za detekciju ranjivosti mreže i anomalija u protokolima.

IPS sistemi mogu da funkcionišu u tzv. in-line modu što znači da su senzori postavljeni direktno unutar mrežnog puta tako da mogu analizirati sav mrežni saobraćaj u realnom vremenu. Senzori su u mogućnosti da obore zlonamerne pakete i time spreče pokušaj upada u organizacionu mrežu. Ova osobina ih diferencira od IDS uređaja koji samo detektuju zlonameran saobraćaj. Šema implementacije IPS-a data je na slici 4.



Slika 3. Šema implementacije IPS-a

Pored blokiranja napada, IPS uređaji mogu izvršiti izmene u konfiguraciji drugih uređaja na mreži poput fajervola, rutera i svičeva, u cilju ometanja napadača. Takođe je značajna i funkcionalnost izmene zlonamernih paketa. Naime, ukoliko se desi da u mrežu stigne mejl sa melverom kao prilogom, IPS uređaji mogu izmeniti tu poruku, eliminišući zakačen prilog omogućujući da primalac i dalje primi mejl ali bez malicioznog sadržaja.

STUDIJA SLUČAJA

Online usluge, koje su prisutne u mnogim delatnostima, omogućavaju korisnicima pristup informacijama i korisne su za pružaoce usluga, jer smanjuju operativne troškove koji su uključeni u pružanju usluga. Poseban razvoj online usluga se desio u oblasti bankarstva. Tako, usluga online bankarstva preko Interneta je postala neophodna za kupce kao i za banke. Pružanje ove usluge za korisnike obavezuje banku da vodi računa o visokom stepenu bezbednosti kako informacija korisnika tako i podataka o banci i poslovanju banke. Nažalost, u dosadašnjoj praksi postoje mnogi slučajevi koji dokazuju da bankarski sistemi često nisu u mogućnosti obezbediti potpunu zaštitu svojih informacionih sistema od zlonamernih napada. U poslednjih nekoliko godina, banke i klijenti su sve više na meti fišinga, DDoS, Tunelinga i drugih napada koji se pokreću s ciljem obavljanja nelegalnih finansijskih transakcija, krađom identiteta, onemogućavanja obavljanja poslovnih aktivnosti i sl. U ovoj studiji slučaja biće prikazane i opisane preduzete aktivnosti u jednoj od komercijalnih banaka u Bosni i Hercegovini, kao članici bankarske grupacije koja posluje u širem regionu, nakon izvršenog a najavljenog napada hakerske grupe Anonimusi u toku 2012. godine na centralu grupacije. Realizovani napad se može smestiti u grupu operativnih rizika a na osnovu kategorizacije po Bazel-u II gde se hakerski napad nalazi u grupi eksternih prevara. Navedeni podaci, obrasci, procedure i drugi navodi su tačni i prikupljeni nizom sastanaka i razgovarajući o ovoj temi sa nadležnim zaposlenikom zaduženim za bezbednost informacionog sistema banke. Zbog zakonske regulative u BiH, zaštite podataka i ne ugrožavajući bezbednost banke nije moguće precizno navođenje informacija i naziva pravnog subjekta.

Predmetna bankarska grupacija je bila meta napada u vidu povećanja broja istovremenih zahteva na veb servis banke. Prema kratkom obaveštenju na zvaničnom sajtu banke, zbog zagušenja, neko vreme, korisnicima je bilo onemogućeno korišćenje određenog broja servisa banke. Napad se dogodio od strane hakerske grupe Anonimusi i bio je u obliku DDoS (*Distributed Denial of Service*) napada. Preciznije, radilo

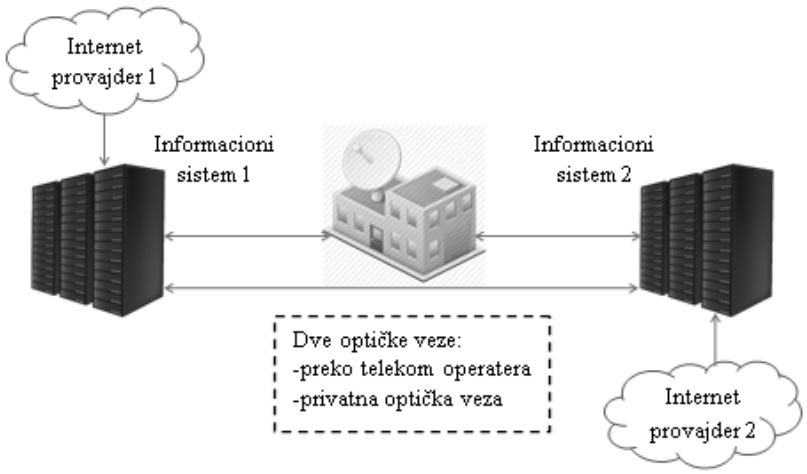
se o napadu usled koga je bio onesposobljen pristup veb servisu banke od strane komitenata. Verovatni cilj ovakvog napada je bio da zbog prestanka rada od nekoliko sati do nekoliko dana banka pretrpi određenu materijalnu štetu, na način da komitenti nisu bili u mogućnosti koristiti usluge banke. Napad se obavio sa lokalnog nivoa što može da govori koliko je bilo potrebno resursa da se napravi ozbiljan problem jednom bankarskom sistemu.

Uopšteno govoreći, za sada je jedini cilj DDoS napada bio nemogućnost korišćenja usluga elektronskog bankarstva putem sajta, i nije poznato da je bilo ikakve novčane satisfakcije za napadače, ali bi se moglo desiti da u budućnosti ovakvi napadi na neki način omoguće krađu vrednih informacija, poput onih o brojevima kreditnih kartica. Prema izveštaju Prolexic-a a [Prolexic Technologies, Inc., 2013], jedne od vodećih kompanija za zaštitu od DDoS napada, iz drugog kvartala 2013. godine, ovi napadi su se povećali za oko 79% u odnosu na isti period u 2012. godini sa značajnim učešćem, od oko 45% pri propusnom opsegu u rasponu 1-5Gb/s.

Kada je reč o konkretnom napadu, pomenuto je da se radilo o prekidu funkcionisanja veb servisa banke koji se odnose na elektronsko poslovanje posredstvom glavnog sajta grupacije. Sagledavajući bezbednost informacionog sistema komercijalne banke iz BiH, članice grupacije, neophodno je navesti da se ovaj napad nije u velikoj meri manifestovao na poslovanje članice. Naime, informacioni sistem grupacije je decentralizovan, odnosno veza postoji samo u oblasti izveštavanja što, i da su napadom ovi procesi narušeni, ne bi dovelo do prekida u poslovanju banke u Bosni i Hercegovini. Međutim, ukoliko se napad desio na veb servis banke iz BiH, može se pretpostaviti, da bi pored zaštite koja je primenjena, moguće posledice bile slične onima nakon napad na veb servis centrale ove grupacije. Iako nije došlo do posledica po poslovanje komercijalne banke u BiH ovaj napad je shvaćen kao opomena koja je pokrenula niz izmena i poboljšanja u informacionom i telekomunikacionom sistemu banaka članica grupacije pa tako i banke koja je predmet istraživanja. U nastavku rada biće navedene određene aktivnosti preduzete s ciljem povećanja bezbednosti informacionog sistema, a time, i stabilnosti poslovanja banke. Sva poboljšanja su rezultat donesene politike grupacije nakon izvršenog napada i implementacije standarda ISO 27001.

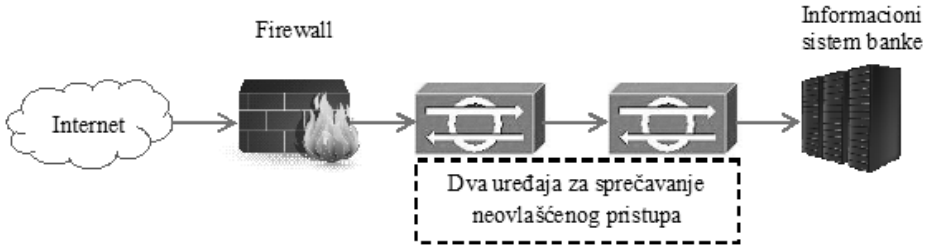
Već ranije je banka uspostavila rezervnu lokaciju čime je omogućeno postojanje dva odvojena informaciona sistema u centrali banke u BiH sa preko 90% podignutih servisa i sistema na drugoj, bezbednoj lokaciji. Veza između tih lokacija je uspostavljena preko dva odvojena optička kabla i dve nezavisne centrale Telekom operatera. Da bi obavila testiranje lokacije banka je donela odluku i uspešno provela aktivnost koja se sastojala od obavljanja svih poslova banke na *Recovery* lokaciji u trajanju od mesec dana. U toku testiranja nije došlo do problema u radu banke a nakon toga sve aktivnosti su se ponovo provodile iz glavnog informacionog sistema a da korisnici nisu primetili razliku u kvalitetu zahtevanih usluga.

Sledeće, banka je obezbedila dve odvojene Internet konekcije od dva samostalna provajdera. Dakle, ukoliko dođe do napada na informacioni sistem banke preko jednog od kanala za Internet konekciju biće omogućeno zaustavljanje preko tog i preusmeravanje saobraćaja preko drugog kanala i to je jedan od osnovnih rezultata ove aktivnosti.



Slika 4. Grafički prikaz veze informacionog sistema banke sa Internet provajderima i veza između primarnog i sekundarnog informacionog sistema banke

Nakon napada banka je donela odluku o povećanju bezbednosti na samom ulasku paketa sa podacima u informacioni sistem. Tačnije, filtriranje saobraćaja prilikom ulaska u informacioni sistem banke obavljao je fajervol i namenski server sa softverom za detaljnu inspekciju i prevenciju nepoželjnog saobraćaja (IDS/IPS). S ciljem povećanja zaštite instaliran je još jedan namenski IPS (*Intrusion Prevention System*) uređaj, nakon fajervola, a koji je povezana serijski sa prethodnim. Sistem za sprečavanje neovlašćenog pristupa je uspostavljen kao preventivni način povećanja bezbednosti mreže koji se koristi da identifikuje potencijalne pretnje i reaguju na njih brzo. Sistemi prate mrežni saobraćaj i sprečavaju upad u informacioni sistem banke na osnovu sposobnosti da preduzme hitnu akciju na prema pravilima utvrđenih od strane administratora mreže. Na primer, IPS-ovi odbacuju paket za koji utvrde da je zlonameran i blokira sav daljni saobraćaj od te IP adrese ili porta. Legitimni saobraćaj, u međuvremenu, treba da bude dostavljen primaocu bez ikakvog prekida ili odlaganja usluge. Tačnije, filtriranje saobraćaja se obavlja trostruko. Isti paketi podataka se proveravaju od strane fajervola a zatim dva IPS uređaja. Kako bi se osigurala kvalitetnija zaštita uređaji koji se koriste potiču od različitih proizvođača. Naime, svaki od uređaja ima svoje slabosti i nedostatke. Kako se može desiti da jedan od sistema za sprečavanje neovlašćenog pristupa načini grešku i propusti neželjeni sadržaj, drugi uređaj bi trebao tu grešku otkriti i ispraviti zbog različitih svojstava u odnosu na prvi uređaj.



Slika 5. Prikaz filtriranja saobraćaja pomoću dva serijski povezanih IPS uređaja

Pored navedenih hardverskih rešenja koja je banka realizovala nakon hakerskog napada na drugu članicu grupe postoji i određeni niz aktivnosti i procedura koje se provode a direktno proističu iz implementiranog standarda ISO 27001. Kada je reč o zaštiti podataka, banka pored sinhrone replikacije na rezervnu lokaciju, na dnevnoj osnovi kreira bekap baze podataka i smešta ga u jednu od ekspozitura lociranu na drugoj tektonskoj ploči, na oko 60 km udaljenoj od centralne lokacije banke. Sledeća mera zaštite jeste sprečavanje eksternih pristupa servisima banke svim zaposlenicima. S druge strane, banka ima VPN tunel ka javnom organu nadležnom za izdavanje ličnih dokumenta zbog provere npr. podataka o prebivalištu u postupku naplate potraživanja. Ovakav ili sličan servis banka ima otvoren i ka većim poslovnim partnerima i nadležnim institucijama, a koji podleže tačno propisanim pravilima zaštite. Banka je, prema standardu ISO 27001, uspostavila sistem prevencije i reakcije na incidente, propisala procedure uspostavljanja i rada nadležnih tela za bezbednosti i operativne rizike. Na primer, ukoliko bi došlo do najavljenog (najavljeni incident) ili nenajavljenog nestanka struje, prema propisima koji se poštuju i u praksi izvršavaju banka realizuje niz aktivnosti s ciljem zaštite podataka i kontinuiranog obavljanja poslovnih procesa. Pored direktnih ciljeva realizovanih preduzetim aktivnostima i propisanim procedurama banka je postigla i druge uspehe. Potvrda ovom navodu može biti zvanična statistika koju vodi i objavljuje Agencija za zaštitu ličnih podataka u Bosni i Hercegovini prema kojoj komercijalna banka obuhvaćena studiji slučaja ima najveći broj odbačenih žalbi komitenata podnesenih za nepoštovanja ograničenja u korišćenju ličnih podataka.

Na kraju analize provedenih poboljšanja od operativnih rizika, prvenstveno od eksternih napada na informacioni sistem, koje je banka realizovala, može se reći da je komercijalna banka kao članica grupacije, na osnovu politike grupacije, preduzela niz aktivnosti opisanih u studiji slučaja usmerenih na minimalizaciju ponavljanja realizovanog operativnog rizika koji je bio inicijator ovih aktivnosti. Nadalje, sve preduzete aktivnosti koje su imale za cilj povećanje bezbednosti od operativnih rizika a podstaknute novom politikom banke nakon hakerskog napada na veb servise članice grupacije mogu se primeniti u drugim bankarskim informacionim i poslovnim sistemima ali i šire iz razloga što niti jedno od rešenja nije implementirano poštujući neke od specifičnih poslovnih procesa ove komercijalne banke što bi ga učinilo neprimenjivim u širem smislu. Hardverski posmatrano, korišćeni su uređaji (komponente informacionog sistema na rezervnoj lokaciji, IPS uređaji i dr.) koji po svojoj vrsti, nameni i načinu rada mogu biti korišćeni u drugim informacionim sistemima. Propisane procedure su primenjive i u drugim finansijskim institucijama jer su izrađene strogo poštujući standard ISO 27001.

Kao sledeća planirana aktivnost zaštite može se navesti instaliranje dodatnog IPS uređaja ispred baze podataka. Iako je informacioni sistem zaštićen od eksternih napada namera jeste minimizovati mogućnost zlonamernih internih napada od strane zaposlenih. Sledeće poboljšanje jeste puno uvođenje poslednje verzije PCI DSS (*The Payment Card Industry Data Security Standard*) standarda. Reč je o standardu čijom će implementacijom banka osigurati bolje bezbednosne mere u kartičnim sistemima i zaštiti krajnjih korisnika te smanjiti prevare prilikom korišćenja kreditnih kartica. U konkretnom slučaju cilj banke je uvođenjem poslednje verzije standarda, osigurala poboljšano šifrovanje podataka između korisnika i banke ali i između filijala i centrale banke.

ZAKLJUČAK

Analizom studije slučaja može se zaključiti da je banka uvođenjem standarda sistema za upravljanje bezbednosti informacija i implementacijom IPS uređaja za proaktivnu detekciju napada, smanjila rizik od DDoS napada i povećala bezbednost informacija koje predstavljaju srž bankarskog poslovanja. S obzirom na to da su i klijenti veoma zainteresovani za bezbednost, banka ovim potezom obezbeđuje konkurentnost na tržištu i omogućuje pridobijanje novih klijenata koji traže sve veći nivo bezbednosti podataka.

Slabosti uvedenih mera u pogledu adaptacije postojećih poslovnih procesa ka zahtevima ISO standarda u najvećoj meri odnose se na finansijski elemenat, odnosno često je teško uveriti rukovodstvo kompanije u isplativost finansijskog ulaganja za uvođenje ISO 27001 standarda. Stalna edukacija zaposlenih se predlaže kao moguće rešenje ovog problema. Kada se radi o IPS uređajima koji su implementirani u mrežnu arhitekturu, stvar je malo komplikovanija. Mišljenja smo da iako IPS uređaji uspevaju da sačuvaju integritet informacija unutar organizacije, neuspeh može biti na polju dostupnosti informacija i podataka. Naime, kako raste propusna moć Interneta, tako se pojavljuju DDoS napadi sve većeg protoka. Statistički podaci za tekuću godinu pokazuju drastičan porast protoka koji se koristi prilikom napada: prosek poslednjeg kvartala 2012. godine bio je 5,9 Gbps a u prvom kvartalu 2013. godine prosek je porastao na 48,25 Gbps, što je povećanje od preko 800%. IPS uređaji su strukturirani da analiziraju sav saobraćaj i odvraćaju zlonamerne pakete. Međutim, ovako masivni napadi, iako neće prodreti do informacionog sistema organizacije, uzrokovaće nedostupnost podataka bez obzira na postojanje rezervnog linka, jer saobraćaj i dalje prolazi kroz IPS analizu. Rešenje ovog problema je uvođenje inteligentnih sistema za ublažavanje DDoS napada (IDMS – Intelligent DDoS Mitigation Systems). Inteligencija ovih sistema se ogleda u tome što ne moraju pratiti stanje svake konekcije, sistem mora biti fleksibilan i skalabilan kako bi dinamički pratio porast protoka DDoS napada u budućnosti.

Arhitektura ovih sistema obezbeđuje višeslojnu odbrambenu strategiju (s obzirom na to da se i napadi razvrstavaju prema slojevima ISO-OSI modela). Predlaže se razdvajanje odbrambenog sistema na dve grane. Prva se odnosi na volumetrijske napade koji bi se sprečili u *cloud-u* na strani provajdera, dok bi se napadi na aplikativni sloj sprečavali unutar centra podataka na strani klijenta. Ovakva šema odbrane u potpunosti je primenjiva u slučaju kada se koriste *cloud* servisi i Internet centri podataka za čuvanje poverljivih informacija.

Rešenja realizovana u komercijalnoj banci prikazana su u studiji slučaja. Zaposleni zaduženi za zaštitu informacionog sistema banke i donosioci odluka su, u periodu nakon napada Anonimusa na drugu članicu grupacije, odabrali i implementirali niz poboljšanja s ciljem sprečavanja neovlašćenih pristupa informacijama od kojih bi, kao jedan od najznačajnijih izdvojili instaliranje IPS uređaja. Na osnovu toga, može se zaključiti da je banka pokrenula delatnosti redovnog i detaljnog praćenja rizika kao i prevencije istih. U duhu instaliranja novih IPS uređaje, o čemu je govoreno u prethodnom delu, nezaobilazno je pomenuti tekstove kompanije Arbour Networks (Arbour Networks, Inc., 2013) u kojima se navodi da fajervol i IPS uređaj ne mogu efikasno blokirati DDoS napad. Prema njima, IPS uređaj radi na bazi detekcije poznatih pretnji dok obično propuste novu pretnju jer nemaju informaciju o njoj ili definisano pravilo od administratora kako postupiti u tom slučaju. Oni uređaji koji su zasnovani na mreži takođe koriste detekciju poznatih anomalija prateći protokole na bazi detekcije, koja nije efikasna u otkrivanju i zaustavljanju DDoS napada. To je zato što ovaj metod otkrivanja ne dozvoljava IPS uređajima da analiziraju saobraćaj istovremeno na više linkova. Na kraju, pošto se IPS uređaji obično instaliraju serijski, oni mogu dovesti do neprihvatljivog kašnjenje u mrežama sa velikim protokom saobraćaja. Složeni algoritmi u IPS uređajima

mogu značajno da dovedu do kašnjenja jer mogu biti preplavljeni velikim paketima prilikom DDoS napada. Osim toga, takva latentnost je neprihvatljiva u mrežama visokog propusnog opsega. Pored toga u objavljenom tekstu kompanije Arbour Networks se navodi da fajervol uređaji nemaju unutrašnjih sposobnost da otkriju ili zaustave DDoS napad, jer se on izvršava kroz otvorene portove i protokole. Zaštitni zidovi su skloni da postanu prve žrtve DDoS napada i njihova sposobnost da prate veze s ciljem detektovanja i sprečavanja napada je zanemariva. U nastavku rada kompanija predlaže uvođenje novih inteligentnih sistema za ublažavanje DDoS napada (*IDMS – Intelligent DDoS Mitigation Systems*). Ovaj članak je izazvao oprečna mišljenja. Stručnjaci se kreću od teze da su navodi iz teksta argumentovani do toga da je ovo marketinški potez kompanije koja se bavi zaštitom od DDoS napada. U svakom slučaju, nastavak ovog istraživanja može se usmeriti u pravcu provere ovih navoda i ukoliko se dokaže da su osnovani, banka treba uzeti u razmatranje uvođenje sličnih sistema za zaštitu i sprečavanje potencijalnih i ublažavanje konkretnih hakerskih napada.

LITERATURA

[1] Arbor Networks (2013). Why IPS Devices and Firewalls Fail to Stop DDoS Threats [White Paper].

[2] El Defrawy, K., Gjoka, M., & Markopoulou, A. (2007). *BotTorrent: misusing BitTorrent to launch DDoS attacks*. In Proceedings of the 3rd USENIX workshop on Steps to reducing unwanted traffic on the Internet (pp. 1-6). USENIX Association.

[3] Gates, T., & Jacob, K. (2009). *Payments Fraud: Perception Versus Reality—A conference summary*. Economic Perspectives, 33(1), 7-15.

[4] Gillies, A. (2011). *Improving the quality of information security management systems with ISO27000*. The TQM Journal, 23(4), 367-376.

[5] Hoffmann, A. O., & Birnbrich, C. (2012). *The impact of fraud prevention on bank-customer relationships: An empirical investigation in retail banking*. International Journal of Bank Marketing, 30(5), 390-407.

[6] ISO/IEC 27000:2009 (2009). *Information Security Management Systems: Overview and Vocabulary.* ISO/IEC 2009.

[7] Kassner M. (16. September 2013). *TechRepublic. What's better than creating your own DDoS? Renting one.* Preuzeto 19.09.2013, sa http://www.techrepublic.com/blog/it-security/whats-better-than-creating-your-own-ddos-renting-one/

[8] Lilić S., i Prlja D. (2008). *Pravna informatika – veština*. Lavdem i Dosije Beograd, ISBN 978-86-7738-089-2

[9] Lyne J. (2013). *James Lyne: Everyday cybercrime -- and what you can do about it* [Video file]. Preuzeto sa http://www.ted.com/talks, 18.09.2013.

[10] Marshall J.H. & Bailie, M. W. (2010). *"Prosecution of Computer Crimes*". Office of Legal Education Executive Office for United States Attorneys.

[11] Prolexic (2013). Prolexic Quarterly Global DDoS Attack Report Q2 2013 [White Paper].

[12] Schechter, S. E. (2004). *Computer security strength & risk: A quantitative approach* (Doctoral dissertation, Harvard University Cambridge, Massachusetts).

[13] Schouwenberg R. (2008). Securelist. *Attacks on banks*. Retrieved 10.9.2013, from http://www.securelist.com/en/analysis/204792037/Attacks_on_banks.

[14] Silva, S. S., Silva, R. M., Pinto, R. C., & Salles, R. M. (2012*). Botnets: A survey*. Computer Networks.

[15] Stallman R. (2010). *The Guardian. The Anonymous WikiLeaks protests are a mass demo against control.* Preuzeto 20.09.2013, sa http://www.theguardian.com/commentisfree/2010/dec/17/anonymous-wikileaks-protest-amazon-mastercard

[16] Symantec Corporation (2013). Internet Security Threat Report 2013. Vol. 18, Published April 2013

[17] What is IPS and how Intrusion Prevention System Works. Preuzeto: 13.09.2013, sa http://www.aboutonlinetips.com/what-is-ips-and-how-intrusion-prevention-system-works/