

UNIVERZITET SINGIDUNUM
DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE I
MEĐUNARODNU SARADNJU

Studijski program:
SAVREMENE INFORMACIONE TEHNOLOGIJE

MASTER RAD

**Tema: Zaštita i bezbednost podataka na internetu na primeru
home-banking rešenja jedne banke**

Mentor:
Prof. dr. Mladen Veinović

Student:
Aleksandar Stančević
Br. indeksa:400245/2014

Beograd, jun 2016.

SADRŽAJ

1. Metodologija.....	4
1.1. Uvodne napomene.....	4
1.2. Predmet istraživanja	4
1.3. Hipoteza	5
1.4. Ciljevi istraživanja	5
1.5. Naučne metode	5
2. Bezbednost podataka na internetu	6
2.1. Pretnje bezbednosti podataka	6
2.2. Namerne pretnje podacima.....	7
2.3. On-line krađa identiteta	7
2.4. Privatnost i elektronska komunikacija (Direktiva EU)	9
2.5. Vidovi krađa on-line identiteta	10
2.5.1. Phishing e-mail.....	10
2.5.2. Trojanci	12
2.5.3. Botnets i kompromitovani PC	13
2.5.4. Čovek u sredini napada	14
2.5.5. Jednostavna lozinka (eng. password)	15
2.6. Mogućnosti korisnika da zaštiti svoj on-line identitet	16
2.7. Komercijalna rešenja.....	18
2.7.1. FLEXIm	19
2.7.2. HASP	21
2.7.3. PC Guard	22
2.7.4. SyncroSoft MCFACT	22
2.8. Metode za ukidanje zaštite	23
2.8.1. Ispravljanje grešaka.....	24
2.8.2. Disasembleri i dekompileteri.....	24
3. Zaštita podataka u računarskim mrežama	26
3.1. Fizičke mere zaštite.....	26
3.2. Kontrola pristupa	26
3.3. Firewall	31
3.3.1. Packet-filtering firewall.....	34
3.3.2. Circuit-level gateway	34
3.3.3. Application-level Gateway.....	35
3.3.4. Stateful Inspection Firewall	35
3.4. Računarski programi	36
3.5. Pretnje sigurnosti podataka.....	38

4. Korisničke metode nadgledanja bankarskih transakcija	41
4.1. Hakerisanje (hacking)	42
4.2. Virusi	43
4.3. Bezbednost.....	44
4.4. Mere koje preduzimaju ISP, banke, trgovci na malo i prodavci softvera radi pomaganja i zaštite krajnjih potrošača.....	45
5. Zaštita podataka na internetu na primeru “Banca Intesa” d.o.o.	47
5.1. Bezbednost transakcija na Internetu.....	47
5.1.1. Zaštita podataka u Banca Intesa a.d.	53
5.1.2. Pristup mrežnim resursima.....	54
5.1.3. Pristup operativnom sistemu	55
5.1.4. ISMS zone	56
5.2. Bezbednosne preporuke banke u vezi sa platnim karticama i bankomatima	57
Zaključak	59
Literatura	61

1. Metodologija

1.1. Uvodne napomene

U ovom istraživanju obuhvaćene su metodologije koje se koriste prilikom zaštite i bezbednog funkcionisanja računarskog sistema. U istraživanju ćemo se baviti zaštitom i bezbednošću podataka na internetu od zloupotrebe ili ugrožavanja privatnosti.

U današnje vreme, internet je stalan alat koji se koristi u redovnom poslovanju. On je poslovne infrastrukture svakog preduzeća. Poslovni subjekti sve veću pažnju poklanjaju obezbeđenju kvaliteta i bezbednosti poslovanja u tehnološkom okruženju interneta. Sagledavajući značaj novih tehnoloških mogućnosti, u svetu se pristupanju tom problemu poklanja izuzetno velika pažnja. Ovi problemi, kao i njihova moguća rešenja, su obrađeni u ovom radu.

1.2. Predmet istraživanja

Predmet ovog istraživanja su zaštita i bezbednost podataka na internetu, a posebno u bankama, izazovi sa kojima se banke suočavaju prilikom rešavanja ovih problema i moguća rešenja. U istraživanju ćemo teorijski objasniti probleme koji se javljaju prilikom zaštite i bezbednosti podataka na internetu, opisaćemo teorijski kako je u nekim zemljama uređena ova oblast (Australija i Velika Britanija), bavićemo se zaštitom od napada na smart kartice i objasnićemo kako Banca Intesa a.d. Beograd svoje klijente štiti i savetuje u vezi zaštite i bezbednosti podataka na svojim platnim karticama..

1.3. Hipoteza

Opšta hipoteza: Danas se među stručnjacima vode ozbiljne diskusije koje su vezane za kontrolu pristupa važnim informacijama koje se nalaze u datotekama računara. Iskristalisala su se dva prioriteta u tim diskusijama, a oni se tiču sigurnosti podataka i njihovoj tajnosti.

Posebna/radna hipoteza: Pod sigurnošću podataka se podrazumeva zaštita podataka i njihovo neovlašćeno korišćenje, modifikacija, ograničavanje u korišćenju ili uništenju istih. Danas imamo mnoge slučajeve zloupotrebe tuđih podataka i krađe identiteta, posebno u bankarskom poslovanju.

1.4. Ciljevi istraživanja

Naučni cilj: Istraživanje i definisanje problema zaštite i bezbednosti podataka u računarskim sistemima, posebno banaka, i istraživanje, definisanje, analiza i predlaganje potencijalnih rešenja za ovaj problem.

Društveni ciljevi: Edukacija zaposlenih u organizaciji radi adekvatnog informisanja o ovom problemu. Definisanje potencijalnih pretnji po zaštitu i bezbednost funkcionisanja računarskih sistema i podataka, posebno u bankama, kao i o mogućim rešenjima.

1.5. Naučne metode

Pri izradi ovog rada korišćene su osnovne naučne metode deskripcije, indukcije, dedukcije, analize, sinteze i generalizacije. Metoda deskripcije je korišćena pri objašnjavanju osnovnih pojmova i sistema funkcionisanja. U teorijskim segmentima su primenjene metode indukcije, dedukcije i analize, a u izvođenju zaključaka metode sinteze i generalizacije.

2. Bezbednost podataka na internetu

Podaci u računarskim mrežama mogu da se nalaze u dva stanja:

- Na fizičkim memorijskim medijima, kao što je hard disk, ili
- Da se prenose preko kablova u obliku paketa.

Oba ova stanja pružaju mnoštvo prilika za napade kako na samu fizičku mrežu tako i za napade sa Interneta. Zbog toga moraju da postoje sigurnosni mehanizmi koji će zaštititi poverljive podatke, kako unutar računarske mreže tako i u fazi prenosa preko Interneta.

2.1. Pretnje bezbednosti podataka

Pretnje bezbednosti podataka mogu se podeliti po više osnova. Najjednostavnija podela je na nenamerne i namerne pretnje. Pretnje možemo da podelimo na one koje dolaze izvan organizacije, prvenstveno preko Interneta u vidu softverskih napada, i na one koje dolaze iznutra, od zaposlenih, hardverske ili softverske greške. Pretnje takođe možemo podeliti na one koje dolaze od prirodnih sila, kao što su poplava ili požar, na pretnje od ljudi i na tehničke pretnje.

U nenamerne pretnje spadaju ljudske greške, elementarne nepogode i greške u radu računarskih sistema. Ljudske greške mogu se desiti kod projektovanja mreže, programiranja, testiranja i prikupljanja podataka, kod unosa podataka, autorizacije, procedura itd. Više od pola sigurnosnih problema otpada na ljudske greške. U elementarne nepogode spadaju zemljotres, požar, oluja, lavina, poplava, jake strujne oscilacije ili greške, kvar na sistemu za hlađenje, eksplozije itd. Greške u radu računarskih sistema mogu da se jave kao posledica slabog kvaliteta hardvera, loše istestiranog hardvera itd. (Urošević, Z., 2012, str. 137)

2.2. Namerne pretnje podacima

Namerne pretnje su u osnovi kriminalne prirode. Kriminal koji se odvija posredstvom računara i Interneta naziva se sajber kriminal (Cybercrimes). Sajber kriminal može da se izvede spolja ili iznutra. Osobe koje spolja probiju u računarski sistem označavamo imenima haker (hacker) i kreker (cracker). Haker je osoba koja probija u sistem bez namere da nanese štetu. Kreker, ili obijač, je zlonameran haker. Podaci mogu biti ugroženi na više načina. Putem softverskih napada, krađe opreme, krađe identiteta, sabotaze, špijunaže itd. Socijalni inženjering je posebna vrsta napada iznutra gde se zaposleni u preduzeću vrbuju u cilju dolaska do osetljivih informacija, kao što su korisnička imena i lozinke. (Urošević, Z., 2012, str. 138)

2.3. On-line krađa identiteta

Svaki put kad neko koristi internet on koristi jednu on-line identifikaciju, najčešće komplikovanu lozinku, bilo da je to jedna e-mail adresa, on-line bankarski račun, on-line maloprodajni račun ili neku trenutnu drugu poruku. Off-line krađa identiteta je često posao koji se odvija po delovima, lopov potkrada sakupljene male delove informacija i postepeno kreira potrebne informacije o nekoj osobi ili preduzeću. On-line krađa identiteta je mnogo veća i mnogo brža pretnja koju može da izvrši bilo koji kriminalac bilo gde u svetu.

Anonimnost interneta znači da kriminalci mogu prevariti korisnika van korisničkih direktnih ličnih detalja i bez saznanja o tome ko je realno to uradio, odnosno učestvovao u krađi. Povećanjem informacija o pojedinačnom korišćenju interneta, kao što su korisničke e-mail adrese, bankarski računi i detalji vezani za prijavljivanje (eng. log in details), kriminalni elementi mogu uslovno rečeno postati ta osoba u on-line režimu rada, a da niko kasnije neće znati ko je zapravo to bio. Kriminalci mogu takođe da koriste tehnologiju u svoju korist, puštanjem određenih kompjuterskih virusa ili slanja phishing e-mail-ova, tako da oni svojim delovanjem vrlo brzo mogu pogoditi, odnosno uslovno rečeno "obraditi" milione internet korisnika. Međutim, kriminalci ne mogu istovremeno da drže visoku stopu

uspešnosti jer moraju brzo prekinuti takav posao, pošto bi u suprotnom to bio unosan način za stalnu krađu informacija.

Ako su se kriminalci dokopali identifikacionih detalja koji su bitni za specifičan bankarski račun, ili uslugu, tada, na primer, kriminalci mogu koristiti dobijene informacije da prenesu novac, otvore novi bankarski račun ili račun kreditne kartice, da zaključe kredit ili povećaju linije kredita ili ostvare dobijanje novih servisa za mobilne telefone preko interneta.

Često „žrtva“ neće da prihvati da je neko ukrao njen on-line identitet zbog toga što kriminalci u radu ne koriste home adresu za obračun. Kriminalci će takođe pokušati da osiguraju da "žrtva" ne dobija bilo kakvu informaciju koja se odnosi na njihovo otimanje para sa računa, direktno ili indirektno, dokle god je to moguće. Identifikovane on-line prevare su danas hit neposrednih novinarskih naslova, posle izveštavanja da kriminalni gang krađe milione od države kroz prevare u porezima korišćenjem krađe identiteta uključujući u to i ministarstvo za rad i penziono osiguranje Velike Britanije kao i mrežu železnice. Međutim, individualci su jednako u riziku i postali su meta kriminalaca širom sveta. (Bjelica, M., 2013, str. 108)

Žrtve u incidentima sa ministarstvom za rad i penziono osiguranje Velike Britanije nisu imale ideju da su njihovi personalni detalji ukradeni i da su zatim korišćeni da bi se primenili u korist prevaranata. Velika skala prevara, kao u ovom slučaju, predstavlja osobe koje dobijaju pažnju štampe, ali na svaku veliku prevaru postoji mnogo više osoba koje nikada nisu stigli u novine, a svaka od njih predstavlja primer određenog rizika. Neke od posledica krađa identiteta uključuju sledeće:

- trošak, vreme i neprilike uključene u rešavanje ishoda problema,
- pojavu lošeg kreditnog rejtinga i/ili odbijanje kreditiranja žrtve,
- definitivni zahtev za proizvod ili uslugu koja nije kupljena od strane žrtve,
- nepravedna optužba za kriminalne aktivnosti koje žrtva nije počinila,
- teškoća u sticanju hipoteke,
- neopravdan prijem sudskih poziva, parničke aktivnosti i okružna parnička presuda,
- teškoće u otvaranju novog korisničkog računa. (Ilić, O., 2015, str. 44)

2.4. Privatnost i elektronska komunikacija (Direktiva EU)

Zakonska regulativa u Velikoj Britaniji je izvedena od Direktive Evropske Unije i dizajnirana je da zaštiti potrošače i poslovanje od netraženih elektronskih komunikacija najčešće poznate kao "spam". Marketing preko elektronske pošte i SMS tekstualnih poruka je sada dozvoljen samo ako je primalac dao prethodnu saglasnost ili "izabrao" da prima informacije preko tih kanala informisanja. To stavlja dopunski "teret" za pošiljaoca elektronske pošte.

Zakonska regulacija eksplicitno formuliše da za prvo vreme, dozvola mora da bude dobijena od potrošača informacija, pre njegovog kontaktiranja preko elektronske pošte ili SMS poruka. Zakonska regulativa ne omogućava kompaniji da kontaktira postojeće potrošače - kupce koji su već dali svoju e-mail adresu ili broj mobilnog telefona. Takođe je kontakt zabranjen i onim potrošačima koji su se raspitivali oko proizvoda ili usluga preko e-mail-a ili SMS-a. U dosadašnjoj praksi, kroz prikazivanje samo jednog prolaznog interesa na web sajtu, kompanije su smatrale da imaju dozvolu da te posetioce web sajta ponova kontaktiraju u budućnosti.

Bilo koja forma elektronske komunikacije poslata ka jednom pojedincu mora uvek sadržavati jasnu formulaciju opcije o neslaganju koja je besplatna za primaoca e-mail-a ili SMS-a. Poslovanje kompanije će kršiti Zakon ako nastavi da komunicira sa potrošačima koji su odustali od komunikacije. Kršenje Zakona u Velikoj Britaniji može rezultirati novčanom globom koja je veća od 5.000 funti. Regulacija takođe uvodi neka ograničenja kod korišćenja takozvanih "cookies" na web sajtu (zahtev za bazičnim informacijama o posetiocima sajta, to jest, omogućavanje da se memorišu osnovne adrese posetioca, posledice neprihvatanja toga memorisanja, kao i mogućnosti da se posetioци isključe sa tih listi). (Ljubičić, D., Franjić, A., 2012, str. 81)

Na kraju, Zakonska regulacija zabranjuje korišćenje elektronske pošte za direktne marketinške svrhe gde je ident ili adresa pošiljaoca sakrivena ili prerusena ili gde nije obezbeđena ispravna adresa za odgovor. Uticaj Zakonske regulacije je za sada ograničen zato što mnoge "spam" poruke nastaju van Evropske Unije, gde ili nema zakona ili je takav zakon manje strog. U Americi na primer, CAN - SPAM Act 2003 omogućava poslovanju

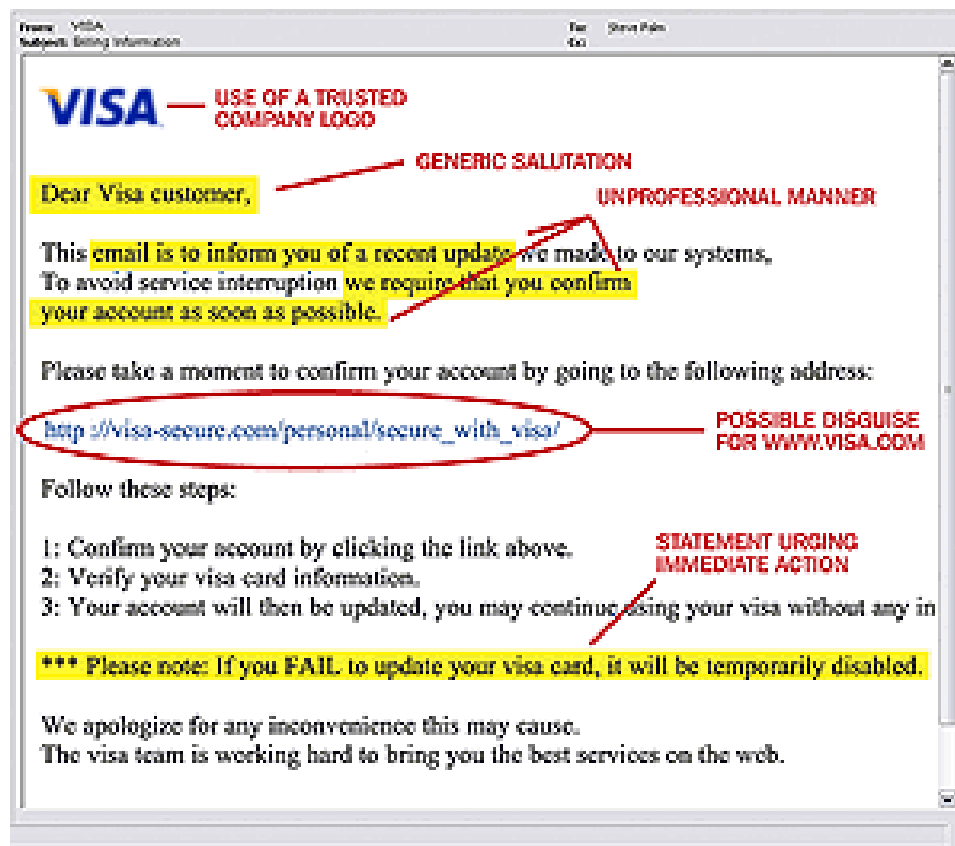
da šalje ne tražene poruke dok primalac ne uloži protest. Drugim rečima, teret je na primaocu pre nego na pošiljaocu elektronskih poruka.

2.5. Vidovi krađa on-line identiteta

2.5.1. Phishing e-mail

Kao i u offline svetu, postoje mnogi načini da se jedan identitet ili personalni detalj može ukrasti u on-line režimu rada. Najjednostavniji način je korišćenje takozvanog phishing e-mail, a to je situacija kada se napravi jedan e-mail tako da ima smisao kao da je poslat od banke ili finansijske institucije sa namerom da pita i zahteva od primaoca da unese svoje personalne detalje, takve kao što su prijavljivanje (eng. logins) i password.

Slika 1. Phishing e-mail



Izvor: <http://www.visa.ca>, pregledano 07.04.2016.

Tokom 2005. postojala je u Velikoj Britaniji serija phishing napada visokog profila sa e-mail-om sa namerom da se formira on-line sajt trgovaca na malo i sajtovi za plaćanje, zajedno sa najistaknutijim bankama u Velikoj Britaniji, skrenuvši ljude da gledaju slične websajtove koji pitaju za personalne login informacije. Ne samo da je rad tih i tako ostavljenih korisničkih informacija o računima sa velikim rizikom za finansijske napade, na takvim sajtovima ljudi ostavljaju svoj identitet za uvećanim rizikom od suštinskog korišćenja predatih informacija za proneveru od drugih kriminalnih lica.

Ako postoji jedan račun sa on-line aukcijskim sajtom, otkriveni, odnosno obelodanjeni račun i detalji prijavljivanja (log in) kroz odgovor posredstvom phishing e-maila, omogućava prevarantu pristup do računa, sa koga on može da proneveri druge korisnike. U Sjedinjenim Američkim Državama, 2.4 miliona potrošača je izvestilo o gubitku novca direktno usled phishing-a. Od tih, približno 1.2 miliona potrošača (dakle oko 50%) je izgubilo 929 miliona dolara tokom godine koja je prethodila pregledu.

Međutim, skoro 30 procenata lica koja su popunili odgovor, kaže da su se bojali nedetektovanog pristupa privatnim kreditnim izveštajima i drugim osetljivim finansijskim podacima koji su zaštićeni nasuprot phishing napada. Od njih, najzabrinutiji su u Velikoj Britaniji, skoro polovina žena i lica starosti od 16 do 24 godina, odnosno lica koja nisu znala šta je phishing. Korisnički identitet je takođe pod rizikom ako on odgovori na e-mailove koji su opšte poznati kao "akontacija takse" ili "419 prevara"⁴. Ovi e-mail-ovi su poslani kao spam velikog obima i često objavljeni primaocu kao da ima dobitak na lutriji ili zaveštanje velike sume novca.

Ako korisnik odgovori na ove e-mail-ove, sem činjenice da se od primaoca često zahteva da plati unapred, za taksu ili bilo koji drugi navodni porez, takođe se zahteva da se obezbedi pun identitet i kopija identifikacionih dokumenata. Čim se to obezbedi, prevaranti mogu tada da koriste ukraden identitet u drugim aktivnostima. (Veinović, M., Jevremović, A., 2013, str. 177)

2.5.2. Trojanci

Postoje mnogi tehnički načini sakupljanja informacija o pojedincima da bi se ukrale njihove on-line identifikacije, na primer softveri: spyware, keyloggers, ili trojanci. Slično trojanskom konju iz grčke mitologije, ovi maliciozni softveri uslovno rečeno "sede" skriveni i uspavani unutar kompjutera dok se ne aktiviraju, odnosno postanu neophodni. Čim se aktiviraju, softver može da prikuplja sve ono što je kucano u kompjuter, kao što je web sajt adresa i personalni detalji, uključujući prijavljivanje, login i password.

Maliciozni softver to radi eksploatišući bezbedonosne slabosti u operativnom sistemu i bezbedonosnom softveru, omogućavajući računaru da prosleđuje te informacije kreatoru programa, koji tada može da ga koristi da ponovo stvori ukradeni identitet.

Slika 2. Virus „trojanac“



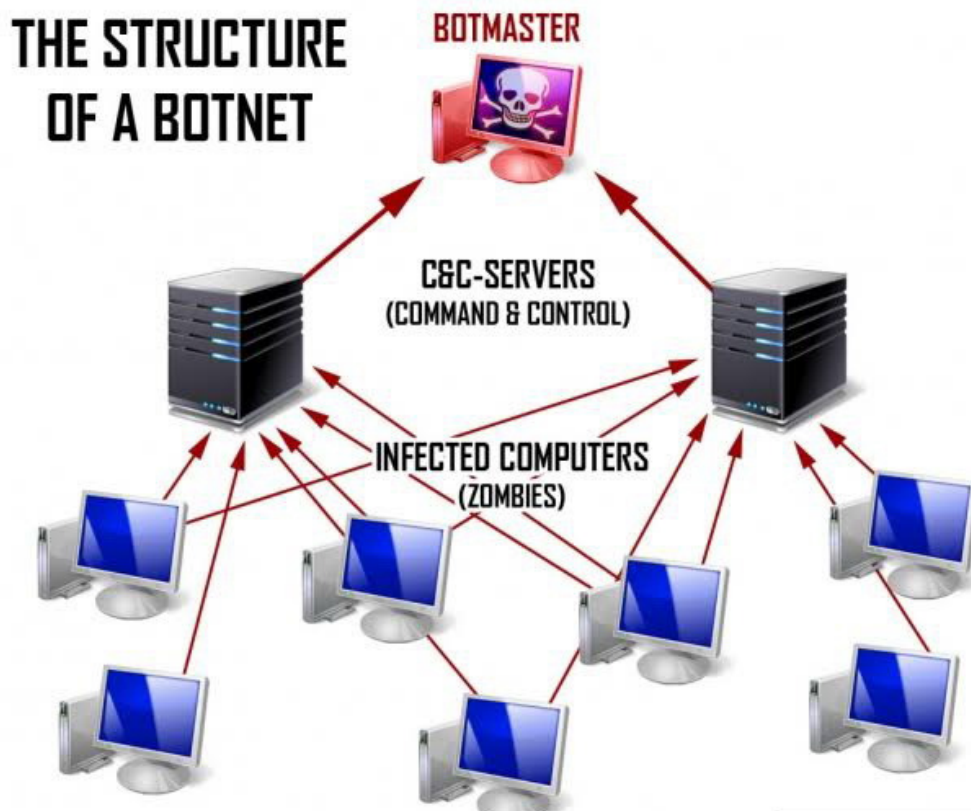
Izvor: www.emailquestions.com, pregledano 08.06.2016.

Trojanac može da se prepiše (eng. download) na bezbroj načina, ali najopštiji način je zajedno sa sadržajem iz kompromitovanog sajta ili kao e-mail dodatak (eng. attachment).

2.5.3. Botnets i kompromitovani PC

Kriminalci su sada kreirali programski kod koji pokreće inficirane kompjutere u alat koji može da se koristi za "lansiranje" napada, što znači da sem ako korisnik nije naročito zaštitio svoj PC, može da dođe u veliki rizik, ne samo u vezi sa svojim personalnim identifikacionim podacima.

Slika 3. Botnets



Izvor: [http:// www.alienvault.com](http://www.alienvault.com), pregledano 10.06.2016.

Računarska mašina može da bude deo široke mreže kompjutera koji se koriste za izvršavanje phishing-a, napada virusa u svrhu odbijanja vršenja određenih usluga. Ova pojava se naziva (bots). Razgranjavanje kompjutera suštinski uključenih u ovu vrstu aktivnosti može da bude poligon od strane internet konekcije koji je suštinski zatvorena od strane ISP, kroz potencijalno postojanje dela za ispitivanja prevara.

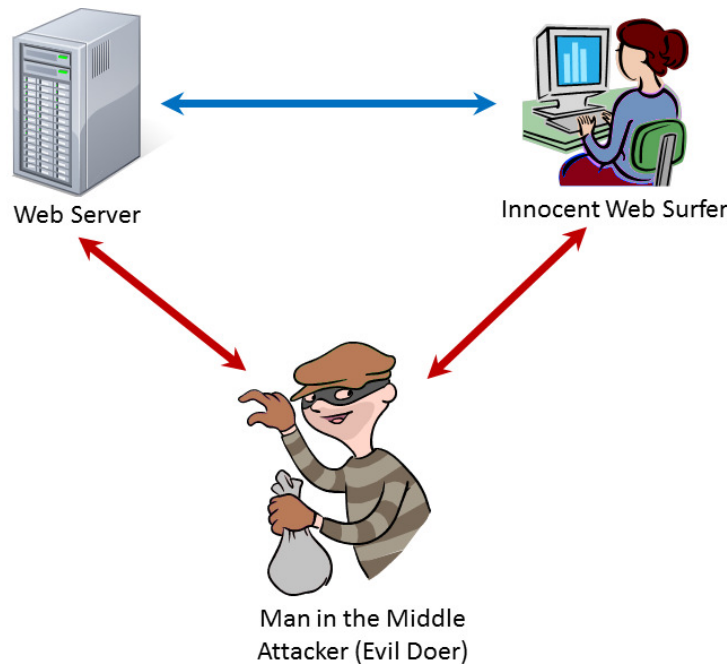
Botnet činjenice i oblici:

- Norveški internet servis provajder (ISP) - Telenor rasformirao je 10.000 čvorova botnet-a u septembru 2005. godine. Nemačka policija je našla i rastavila 100.000 čvorova botnet-a u oktobru 2005. godine,
- 172.000 novih bot inficiranih kompjutera je identifikovano svakog dana,
- Botnet od 30.000 zombija je dovoljno da obori bilo koji web sajt, Postoji oko milion bot inficiranih kompjutera širom sveta,
- Od ukupnog broja identifikovanih botnet-a širom sveta, trenutno je njih 25,5 procenata locirano u Velikoj Britaniji, a ovaj odnos prate Sjedinjene Američke Države koje imaju 24,6 procenata botnet-a. (Golden, B., 2013, str. 24)

2.5.4. Čovek u sredini napada

Čovek u sredini napada, MITM je vrsta napada pri kom je jedan napadač sposoban da čita i modifikuje pri slanju odlučivanje poruka između dveju strana u razmeni, bez znanja jedne ili druge strane da je link između njih ugrožen. Tipičan scenario je e-mail koji je poslat iz banke sa lažnim linkom na web-sajt. Kada primalac klikne mišem na link u e-mail-u, on je preuzet od sajta koji se ponaša kao štafeta prema banci, tako da je prijavljivanje normalno kroz sajt, a u sredini se može manipulirati sadržajem transakcija (Slika 4).

Slika 4. Prikaz tehnologije "čovjek u sredini napada "



Izvor: [http:// www.blog.comodo.com](http://www.blog.comodo.com), pregledano 18.06.2016.

2.5.5. Jednostavna lozinka (eng. password)

Druga bezbednosna slabost koju kriminalci eksploatišu kod korisnika je:

- korisnik bira javno dobijene podatke, kao što su početno ime pri rođenju, ili mesto rođenja kao svoju lozinku;
- neizvršavanje promene lozinke na regularnoj osnovi.

Potrošač koristi savršeno jednostavnu lozinku, uključujući i samu reč „password“. Stoga bi u lozinke trebalo uključiti slova, brojeve i specijalne simbole, na primer c3Rtly8.

Druga slabost kompjutera koja ih čini nezaštićenim od napada je korišćenje iste lozinke za bezbedan pristup brojnim on-line bankama i web-sajtovima. Skoro 61 procenat vlasnika kompjutera koristi jedan glavni password - lozinku gde god je moguće, ali to neminovno znači da, čim kriminalac stekne pristup jednom sajtu, on može tada takođe da pristupi i svim drugim sajtovima. (Vasiljević, V., 2008, str. 90)

2.6. Mogućnosti korisnika da zaštiti svoj on-line identitet

Najvažnija stvar za korisnike je da budu svesni o tome šta bi trebalo da urade on-line i o krađama koje postoje na internetu. Kroz razmatranje svojih on-line iskustava kao i u off-line iskustava, korisnik će postupiti slično licima koja ne znaju da "hodaju ulicom u velikom gradu", odnosno, prirodno će preduzeti sve potrebne mere predostrožnosti. Po pravilu, korisnik bi trebalo da se zapita zašto banka, finansijska institucija ili bilo koji drugi web sajt zahtevaju njegove lične detalje. Naročito, banke nikada putem mejla neće pitati potrošača, odnosno korisnika da se uloguje na sajt i promeni detalje putem linka u e-mail-u.

Ako korisnik to uradi dobivši jedan takav e-mail, u kom se tvrdi da ga je poslala njegova banka ili finansijska institucija, on bi trebalo da se uloguje na taj sajt isključivo ukucavanjem web adrese sajta. To može da se učini na lakši način, ako korisnici memorišu tu web adresu sajta u svoj folder sa omiljenim sajtovima (favorites) i tada pokušaju priključenje na web-sajt. Iz jedne IT perspektive, korisnik bi trebalo da ažurno u dan vrši održavanje svih bezbedonosnih softvera (uključujući antivirus, anti-spam, anti-spyware, adware odbranu i firewalls), kao i operativnog sistema, čime će znatno umanjiti potencijalni rizik.

Firewall je najznačajnija sigurnosna komponenta za sprečavanje hakinga ako je mreža u organizaciji istovremeno priključena i na internet. Firewall može da bude ili fizička "kutija" ili server koji može da ima poseban program za to, (softver) koji izvršava iste funkcije kao hardverske komponente u "kutiji".

- Hardverski firewall je najčešće mala kutija koja „leži“ između kompjutera i korisničkog modema. Poslovne mreže najverovatnije imaju hardverski firewall pošto one moraju odmah da zaštite više od jednog kompjutera.
- Softverski firewall na primer (Zone Alarm Norton Internet Security) izvodi se na korisničkom kompjuteru u pozadini. Najnoviji operativni sistemi, kao što je na primer Windows 8 ima u sebi ugrađen firewall.
- Naravno, u praksi je moguće koristiti oba sistema firewall-a istovremeno. (Pokorni, S., 2015, str. 129)

Firewall je uvek bio važan kao bezbedonosna mera u organizaciji, ali je vremenom to postao mnogo više, tako da danas sve više ljudi ima širokopojasnu konekciju - broadband na internet koja je "uvek otvorena" ka hakerima ("always on", što znači da je uvek i ranjiva, "always vulnerable").

Enkripcija, odnosno šifrovanje predstavlja model obezbeđivanja provere za povećanje mere fizičke zaštite.

Enkripcija predstavlja tehniku prerušavanja informacija, da bi se sačuvala njihova poverljivost. Enkripcija može da se izvede za vreme prenosa podataka na daljinu, kao i kod memorisanja podataka. Enkripcija se izvodi šifriranjem teksta (odnosno sadržaja) podataka sa jednostavnom šifrom, koja transformiše podatke u neprepoznatljivi oblik, rečeno na jednostavniji način, enkripcija je metoda šifrovanja podataka u poruci ili fajlu tako da podaci postaju nerazumljivi, osim za onog ko ih dešifruje ili dekriptuje u ponovo razumljiv oblik.

Proces enkripcije i dekripcije podrazumeva poseban algoritam i njegov ključ. Algoritam je funkcionalan sam po sebi, on predstavlja proces koji transformiše podatke u šifre, a ključ kontroliše algoritam. Menjajući vrednost ključa može se promeniti efekat algoritma, tako da konverzija za svaku vrednost ključa bude potpuno različita.

Kompjuteri, zbog svoje snage izračunavanja, omogućavaju primenu sofisticirane tehnike enkripcije, koja bi inače bila nerealna za praktičnu primenu. Analitičar kriptografije u organizaciji bi morao da podesi sistem rada imajući u vidu trošak dekodiranja koji je značajno visok, pre svega da bi zastrašio potencijalnog neovlašćenog dekodera ali koji mora u isto vreme, da ima nivo sofisticiranosti ne veći nego što je neophodno, posebno zato što to na određeni način usporava vreme obrade koje je dosta skupo. (Bjelica, M., 2013, str. 101)

Ključ šifre može da bude različit za svaki fajl ili poruku, ali se uvek primenjuje na grupu podataka. Često se koristi isti ključ za enkripciju i dekripciju. Tada obojica, i pošiljalac i primalac moraju da ga znaju, što povećava mogućnost da ga prepozna jedan neovlašćeni korisnik. Ako su ključevi za enkripciju i dekripciju različiti, mogu biti osmišljeni tako da potencijalni prislušivač dobije potpun uvid u proces enkripcije i ključ, ali da ipak bude u

nemogućnosti da dešifruje podatke, čak i uz pomoć sofisticirane kompjuterske opreme. Zašto? Ključ za enkripciju može da bude napravljen tako da bude opšte raspoloživ. Takav ključ u literaturi je poznat kao javni ključ. Lice koje primi poruku kodiranu javnim ključem zadržava različiti svoj privatni ključ koji mu je potreban da bi se dekriptovala poruka. Zbog toga što je privatni ključ zadržao svoju tajnost, lice koje je poslalo poruku sa javnim ključem znaće da samo očekivani primalac poruke, koji poseduje privatni ključ, može da dešifruje poruku i pročitati je.

Primenjujući ovakav metod rada, korisnik može da napravi bezbednu kupovinu preko interneta. Skoro svi prodavci će potvrditi da korisnici imaju obezbeđen bezbedan link tako da su svi detalji kreditne kartice sigurni. To znači da su svi detalji korišćene kreditne kartice enkriptovani, korišćenjem javnog ključa prodavca, a samo kupac ima pristup svom vlastitom privatnom ključu, čineći time transfer podataka vrlo sigurnim.

Naravno, može se dokazivati da je kompjuter tako brz da enkripcijski sistem može da se vrlo brzo razbije. Međutim, povećanje snage kompjutera da traga za ključem dekripcije dovodi poslednjih godina do proizvodnje ključeva kojima je potrebno značajno kompjutersko vreme da bi bili razbijeni. U svetu danas postoji više enkripcijskih sistema, a u radu ćemo se zadržati na dva, PGP i RSA. Ovi enkripcijski sistemi su marketirani preko kompanije RSA koja se bavi sigurnošću podataka. PGP i RSA su tipovi novih enkripcijskih sistema. Procenjeno je da sa sadašnjom snagom kompjuterskih sistema poruka koja je enkriptovana sa sistemom RSA ne može da bude razbijena. (Žorić, A., 2012, str. 18)

2.7. Komercijalna rešenja

Na tržištu postoje brojna rešenja namenjena zaštiti od ilegalnog korišćenja i zloupotrebe softvera.

2.7.1. FLEXlm

FLEXlm (Flex License Manager), softver kompanije Macrovision, predstavlja izuzetno komplikovan sistem nadzora nad softverskim licencama i danas je najkorišćenije komercijalno rešenje za zaštitu softvera. FLEXlm obuhvata zaštitu izvršnog koda aplikacije, kontrolu ispravnosti registracionih datoteka na disku, softver za implementaciju na serverima koji nadziru korišćenje licenci u lokalnoj mreži, sistem za lako obnavljanje licenci i centralno administriranje celog sistema. Za zaštitu samih aplikacija, FLEXlm koristi šifrovanje izvršnog koda aplikacije, šifrovanu registracionu datoteku koja zavisi od hardvera korisnikovog računara, kontrolu servera kojom se neovlašćenim korisnicima zabranjuje pokretanje mrežnih aplikacija, a u nekim verzijama primenjuje se i dongle. Sistem nadzire korišćenje softvera i ispravnost licenci, a moguće je izabrati različite metode licenciranja softvera.

Softver podržava nekoliko desetina različitih licencnih sistema, a najpoznatiji su:

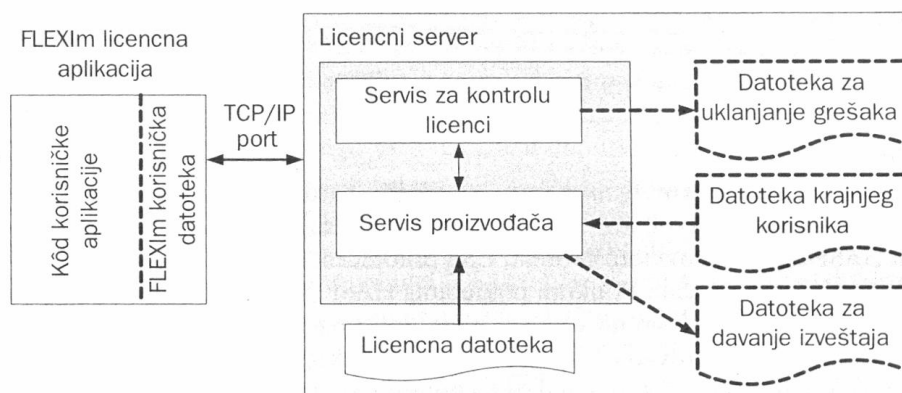
- Node locked-softver je moguće pokrenuti samo na računaru za koji je izdata licenca,
- User based - softver može pokrenuti samo korisnik koji je vlasnik licence (licenca je vezana za osobu, a ne za računar kao kod Node locked sistema),
- Site licensing - softver mogu pokrenuti svi korisnici na određenoj lokaciji i
- Floating license — softver mogu pokrenuti svi korisnici u lokalnoj mreži, ali je ograničen broj korisnika koji mogu istovremeno raditi s programom. (Bjelica, M., 2013, str. 112)

Aplikacijski softver je, u ovom kontekstu, softver koji je zaštićen FLEXlm sistemom. Softver ima ugrađene funkcije koje proveravaju postojanje i ispravnost registracione datoteke. Datoteka se mora nalaziti u određenom direktorijumu, a u datoteci je naveden naziv softvera, podaci o vlasniku licence i razdoblje u kojem je licenca važeća. U registracionoj datoteci zapisana je jedna putanja do servera za kontrolu licenci čiji je zadatak nadzor licenci u lokalnoj mreži. Aplikacija se povezuje s tim serverom i od njega saznaje lokaciju servera softverske kompanije. Server proizvođača softvera nadgleda korišćenje licenci za sve mušterije tog proizvođača.

S obzirom na to da je FLEXlm vrlo popularan softver koji koriste mnogi proizvođači softvera za zaštitu svojih aplikacija, moguće je da korisnik na svom računaru ima više

aplikacija različitih proizvođača, a sve su zaštićene FLEXlm sistemom. U tom slučaju korisnik mora instalirati FLEXlm softver samo jednom i taj sistem upravlja licencama za sve aplikacije za koje je odgovoran. Iako je ovaj sistem veoma poznat i koriste ga stotine proizvođača softvera širom sveta. Njegova komplikovana zaštita je ipak probijena i vrlo brzo su se pojavile piratske verzije softvera koji koristi ovakvu zaštitu. FLEXlm softver se instalira kao deljena DLL biblioteka funkcija, i aplikacija koja je zaštićena FLEXlm sistemom komunicira s tom bibliotekom kad god proverava ispravnost licenci. Takva implementacija olakšava probijanje zaštite.

Slika 5. Varijanta opsluživanja sa servera



Izvor: Bjelica, M. (2013) *Telekomunikacione i računarske mreže*, Akademska misao, Beograd, str. 119

Postoje dva načina za funkcionisanje FLEXlm sistema:

- Licencni server opslužuje licence.
- Licence su direktno dostupne aplikaciji.

U prvom slučaju, FLEXlm se sastoji od četiri komponente:

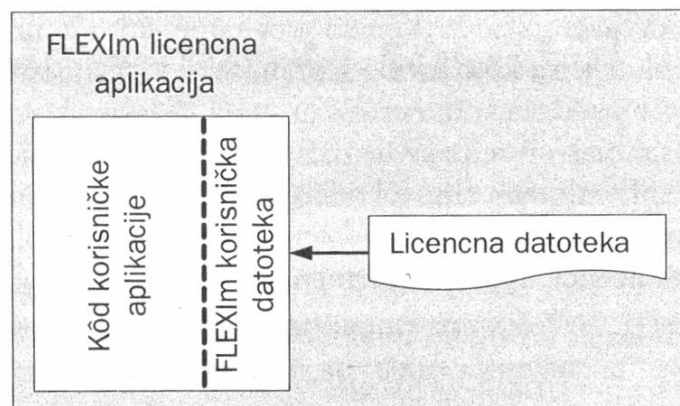
- FLEXlm licencna aplikacija (engl. FLEXlm licensed application)
- Servis za kontrolu licenci (engl. license manager daemon, LMGRD) uspostavlja početni kontakt sa FLEXlm licencnom aplikacijom i prosleđuje vezu do odgovarajućeg servisa proizvođača.
- Servis proizvođača (engl. vendor daemon) vodi evidenciju o proverenim licencama i o tome kome pripadaju.

- Licencna (registraciona) datoteka (engl. License file) sadrži informacije (u tekstualnom obliku) o serverskoj mašini i servisu proizvođača.

U slučaju licenci koje su direktno dostupne aplikaciji, FLEXlm se sastoji od dve komponente:

- FLEXlm licencna aplikacija (engl. FLEXlm licensed application)
- Licencna datoteka (engl. license file). (Ilić, O., 2015, str. 52)

Slika 6. Varijanta bez servera



Izvor: Mur-Malinos, DŽ., Mazali, G. (2014) *Bezbednost na internetu*, Pčelica, Čačak, str.

124

2.7.2. HASP

Softver HASP (Hardware Against Software Piracy) hardverski je orijentisan sistem zaštite koji se jednostavno koristi, a pri tom pruža visok stepen pouzdanosti. Moderni HASP sistemi funkcionišu preko USB priključka, dok su stariji koristili serijski ili paralelni priključak. Prilikom pokretanja HASP programa, ostvaruje se veza s hardverskim priključkom na kome se nalazi informacija neophodna za nastavak rada. HASP nudi i šifrovanje samog koda. Princip koji se koristi jeste šifrovanje podataka pomoću ključa koji se nalazi na pokretnom uređaju.

Korišćenje je jednostavno jer se svodi na instaliranje potrebnog upravljačkog programa, posle čega samo treba povezati uređaj na priključak računara. Za vreme izvršavanja programa, zaštićeni softver šalje šifrovan niz znakova priključenom uređaju koji dešifruje poruku i vraća odgovor. U ovom delu, sigurnost sistema se svodi na nemogućnost oponašanja odgovora. Ako je odgovor tačan, aplikacija će nastaviti s radom, u suprotnom, javlja se poruka o grešci usled odsustva pravog ključa. U varijanti korišćenja takozvanog ToolBoxa, automatski se generiše i kopira određeni kod koji se povezuje s kodom vaše aplikacije. „Max“ model nudi 4 kilobajta memorije s prostorom za 112 licenci. (Pokorni, S., 2015, str. 141)

2.7.3. PC Guard

PC Guard je softver kompanije Sofpro, namenjen zaštiti softvera šifrovanjem izvršnog koda i detektovanjem pokušaja analize koda. Zaštita je primenjena direktno na aplikacije (EXE, DLL), tako što se one umotavaju u sigurnosni omotač (engl. secured envelope) koji sadrži više nivoa šifrovanja i alate za sprečavanje reverznog inženjeringa. PC Guard ne koristi nikakav dodatni hardver, što bitno olakšava njegovo korišćenje. Namenjen je familiji operativnih sistema Windows. Za proveru identiteta korisnika, PC Guard koristi registracionu šifru koja zavisi od hardvera korisnikovog računara. Naprednim korisnicima je omogućeno šifrovanje u fazi izvršenja programa. Delovi koda se šifruju i tako šifrovani ostaju u memoriji. Kod se dešifruje samo u fazi izvršavanja, posle čega se odmah vraća u šifrovano stanje. Omogućeno je i IP filtriranje koje samo aplikacijama s naznačenih adresa dozvoljava pristup aplikacijama.

2.7.4. SyncroSoft MCFACT

„Sakrivanje koda“ podrazumeva njegovo transformisanje u oblik koji je čoveku praktično nečitljiv, ali je istovremeno i prilično otporan na reverzni inženjering. Na primer, strukture i promenljive su sakrivene, a tok programa je promenjen. Sigurnost ovakvog pristupa ne leži u težini rešavanja nekog matematičkog problema i ovakva zaštita ne sprečava

nelegalno kopiranje softvera. Za to je neophodan dongle uređaj ili pametna kartica (engl. smart card).

Kompanija SyncroSoft, specijalizovana za kriptografska i sigurnosna rešenja, ponudila je drugačiju mogućnost. MCFACT (Multi-Channel Finite Automata Code Transformation) tehnologija pretvara programske operacije u skup interaktivnih konačnih automata. Njihova uloga je izvršavanje šifrovanih operacija i njihovo prosleđivanje bez dešifrovanja u bilo kom trenutku. Time se uklanja mogućnost napada u trenutku u kome se podaci vraćaju u čitljivo stanje. MCFACT sigurnost je zasnovana na težini rešavanja matematičkog problema dekompozicije konačnih automata. Napadač ne može primeniti reverzni inženjering na automat jer transformacija iz konačnih automata u programski kod upravo znači da se kod dekomponuje!

Nikakvi napadi u fazi izvršenja takođe nisu mogući jer se program sve vreme nalazi u šifrovanom stanju. Posle generisanja konačnih automata, njihova struktura je proizvoljna pa je napadaču potpuno beskorisna. Treba napomenuti da napadač - sem pokušaja da nađe nedostatak u samoj matematičkoj teoriji - može pribеći i drugim metodama i tako izbeći sudar s najjačom tačkom zaštite. Na primer, na nivou individualnih instrukcija, proces dešifrovanja i dekompresije zaštićenih podataka može se posmatrati - uz pamćenje međustanja - čak i ako se ne poznaju detalji samog procesa. (Žorić, A., 2012, str. 32)

2.8. Metode za ukidanje zaštite

Postoje dva glavna pristupa probijanju softverske zaštite. Prvi pristup je pokretanje programa unutar nekog alata za ispravljanje grešaka u kodu (engl. debugging), a drugi pristup je reverzno prevođenje programa iz izvršnog koda natrag u asemblerski kod (engl. disassembling) ili u neki od viših programskih jezika (engl. decompiling).

2.8.1. Ispravljanje grešaka

Softverska greška (engl. software bug) deo je koda koji na neki način ometa željen tok programa. Softverske greške imaju različite oblike: mogu biti očigledne ili duboko skrivene. Mogu izazvati čekanje, pogrešan izlaz ili pad sistema. U procesu nalaženja i smanjenja broja grešaka (engl. debugging) koristi se softverski alat koji se na engleskom zove debugger. On omogućava programeru da interaktivno prati izvršavanje programa korak po korak.

Program za otkrivanje grešaka može zaustaviti izvršavanje programa između svake dve instrukcije. Nakon što se program zaustavi, programer može videti u kom se delu izvornog koda programa proces trenutno nalazi. Osim dela izvornog koda, programer u svakom trenutku može videti sadržaj radne memorije, sadržaj procesorskih registara, podatke koji se zapisuju u datoteke, informacije o programskim nitima i slično. Međutim, alati za otkrivanje grešaka u kodu često rade i kao samostalne aplikacije i takvi alati su obično mnogo moćniji.

Najbolji alati za otkrivanje grešaka u kodu mogu komunicirati direktno s jezgrom operativnog sistema i zaobići pozive sistema. Na taj način rade mnogo stabilnije, mogu prepoznati više informacija o stanju sistema, pa omogućuju čak i analizu hardverskih upravljačkih programa (engl. drivers). Korišćenjem takvih alata, pirati mogu zaustaviti program u trenutku kad on zahteva autorizaciju korisnika. Nakon što se program zaustavi, moguće je videti deo koda koji je odgovoran za autorizaciju softvera i izmeniti ga tako da prihvata svaku šifru. Najpoznatiji alati za otkrivanje grešaka u kodu su Softlce i GNU Debugger (GDB).

2.8.2. Disasembleri i dekompileteri

Disasemblovanje (engl. disassembling) jeste proces vraćanja izvršnog binarnog koda u njegov asemblerski oblik. Prilikom ovog procesa, glavni problem je razlikovanje koda (instrukcija) od podataka. Kako je assembler jezik koji se direktno prevodi u binarni kod

(jedna instrukcija asemblera odgovara jednoj binarnoj instrukciji), disasembleri mogu prevesti svaku aplikaciju, bez obzira na programski jezik na kome je napisana. Takozvani „pametni“ disasembleri mogu generisati strukturiran kod koji je moguće lako pratiti i analizirati. Oni čak generišu i komentare za lakše snalaženje u programu. Najčešće korišćen alat za disasemblovanje je IDA Pro kompanije NuMega.

Dekompailiranje je proces vraćanja izvršnog binarnog koda u razumljiviji oblik - prevođenje na neki programski jezik visokog nivoa. To je vrsta reverznog inženjeringa, to jest proces suprotan prevođenju (kompajliranju). Osnovna namena mu je analiza grešaka u kodu, nalaženje virusa i slično. Pošto su jezici visokog nivoa razumljivi široj populaciji, mogućnosti dekompileiranja se često zloupotrebljavaju. (Ilić, O., 2015, str. 73)

3. Zaštita podataka u računarskim mrežama

Mere zaštite podataka preduzimaju se u skladu sa stepenom rizika koji predstavlja verovatnoću da će se određena pretnja sigurnosti podataka ostvariti. Prvo je potrebno napraviti analizu rizika. Kod analize rizika prvo se procenjuje vrednost podataka i mrežne opreme koja se štiti, zatim se procenjuje verovatnoća da će se pretnja ostvariti i, na kraju, porede se troškovi zaštite sa troškovima povrede. Na osnovu ove analize preduzimaju se kontrolne mere u cilju sprečavanja pretnji i razvijaju se planovi za oporavak ukoliko se pretnja ostvari. Preduzimaju se sledeće mere: fizička zaštita sredstava, kontrola pristupa sredstvima, zaštita podataka od slučajnog ili namernog izlaganja neautorizovanim licima ili od menjanja i uništavanja od strane neautorizovanih lica, postavljanje firewall-a na granici između mreža (obično između lokalne mreže i Interneta), instaliranje antivirusnog softvera, autentifikacija i autorizacija korisnika mreže, enkripcija, korišćenje virtualne privatne mreže za pristup lokalnoj mreži sa interneta itd.

3.1. Fizičke mere zaštite

Fizička kontrola sprečava pristup neautorizovanim osobama mrežnim resursima. Ovde se pre svega misli na servere, rutere i kablove. Potrebno je obezbediti server od namerno ili nenamerno izazvanog kvara. Potrebno je onemogućiti pristup kablovima kako ne bi mogli da se prisluškuju. Dobro je kada kablovi idu kroz plafone, podove i zidove. Primeri fizičkih kontrola su: zidovi, vrata, brave, alarmni sistemi, kamere, čuvari, portiri i slično. (Jovanović, N., 2011, str. 37)

3.2. Kontrola pristupa

Kontrole pristupa (Access controls) su mere kojima se sprečava pristup neovlašćenih lica računarskom sistemu. Prvi deo ovih mera predstavlja autentifikacija korisnika. Autentifikacija je proces kojim se identifikuje korisnik.

Generalno gledano, identifikacija može da se izvrši:

- (1) na osnovu onog što korisnik zna,
- (2) na osnovu onog što korisnik ima,
- (3) na osnovu onog što korisnik uradi i
- (4) na osnovu onog što korisnik jeste, odnosno na osnovu samo njemu svojstvenih fizičkih karakteristika.

Autentifikacija se najčešće radi na osnovu korisničkog imena (user name) lozinke (password) ili fraze (passphrase). Ovaj način identifikacije korisnika predstavlja pristup sistemu na osnovu onog što korisnik zna (something the user knows).

Pristup sistemu na osnovu onog što korisnik ima (something the user has) uključuje korišćenje ID kartica, smart kartica i tokena. Token je uređaj ko ima ugrađen čip i displej i za svako prijavljivanje na sistem generiše drugačiji broj koji korisnik treba da unese da bi pristupio sistemu. Ovi načini prijavljivanja na sistem se obično kombinuju sa prethodnim načinom prijavljivanja. (Jovanović, N., 2011, str. 43)

Pristup sistemu na osnovu onoga što korisnik uradi (something the user does) se ostvaruje tako što korisnik treba da izgovori nešto ili ispiše neki tekst. Kod identifikacije glasom korisnik treba da izgovori neke prethodno snimljene reči, npr. svoje ime i prezime, odeljenje kojem pripada, funkciju koju obavlja i slično. Kod prepoznavanja potpisa, korisnik treba da napiše neki tekst koji je ranije snimljen u računar. Prilikom pisanja, pored slično rukopisa, uzimaju se obzir parametri kao što su brzina pisanja i pritisak olovkom na podlogu po kojoj se piše. Najsigurniji način identifikacije oslanja se na ono što korisnik po prirodi jeste. Ovaj način prijavljivanja poznat je pod imenom biometrija. Biometrijske aplikacije za identifikaciju koriste fizičke karakteristike korisnika koje su jedinstvene za svakog korisnika, kao što su otisak prsta, mrežnjača, zenica lica i raspored vena na ruci. (Ljubičić, D., Franjić, A., 2012, str. 148)

Kada se korisnik autentifikuje počinje proces autorizacije. Autorizacija je proces davanja prava i dozvola autentifikovanim korisnicima nad resursima sistema. Dozvole mogu da se dodeljuju pojedinačnim korisnicima ili grupi korisnika. Kratko rečeno, autorizacijom se određuje šta korisnik može da uradi na sistemu. U višekorisničkim računarskim sistemima administratori definišu u samom sistemu kojim korisnicima je dozvoljen pristup sistemu i

koja prava imaju. Na primer može da se definiše vreme kada korisnik može da pristupa sistemu, kojim folderima i fajlovima ima pristup, koja prava ima. Pravima se upravlja kroz dozvole koje se definišu nad samim objektima, kao što su folder ili pojedinačni fajl. Svaki objekat ima pridruženu listu za kontrolu pristupa (access control list – ACL) kojom se identifikuju prava korisnika sistema. U nastavku ćemo koristiti naziv ACL. ACL sadrži spisak svih korisnika sistema i njihova prava nad tim objektom. Najčešća prava uključuju mogućnost čitanja fajla, pisanje u fajl, pokretanje fajla (kada se radi o programu) itd. Microsoft Windows operativni sistemi, Novell NetWare, Digital-ov OpenVMS i Unix bazirani operativni sistemi koriste ACL.

U Microsoft Windows operativnim sistemima svaka ACL lista sadrži jedan ili više ulaza koji se nazivaju Access control entries (ACE). ACE se sastoji od imena korisnika ili grupe i dozvola koja ima nad tim objektom (listanje, pisanje, brisanje itd.). Određena prava nad objektom se dodeljuju uključivanjem polja u koloni Allow, a zabranjuju se uključivanjem Deny. Deny uvek ima prednost nad Allow. To znači ako je korisniku na jednom data određena dozvola nad objektom (allow), a na drugom mu je zabranjena (deny), korisnik neće imati to pravo nad objektom. (Ljubičić, D., Franjić, A., 2012, str. 153)

U Microsoft Windows 8 operativnom sistemu korisnik može da ima sledeće vrste dozvola nad objektima: read, write, read and execute, full control, modify... Read dozvola predstavlja i omogućava korisniku prikazivanje sadržaja objekta. Ako se radi o folderu korisnik može da vidi sadržaj foldera. Ako se radi o korisnik može da prikaže fajl. Ako je fajl program, korisnik može da ga pokrene.

Write dozvola omogućava korisniku da kreira nove foldere u folderu nad kojim ima write dozvolu. Kada se radi o fajlu, da bi mogao da ga promeni korisnik treba da ima i read dozvolu.

Read and Execute je ista kao i dozvola read, ali dodaje i dozvolu za prolazak kroz foldere nad kojim korisnik nema dozvole.

Modify je kombinacija dozvola read and execute i write, s tim da omogućava i brisanje objekta.

Full control daje korisniku puna prava nad objektom. Korisnik koji ima ovu dozvolu automatski ima i sve prethodno pomenute dozvole, ali ima i mogućnost preuzimanja vlasništva nad objektom. Ova dozvola omogućava korisniku brisanje podfoldera i fajlova, čak i kada nema eksplicitnu dozvolu koja mu to dopušta.

List folder contents dozvola se odnosi samo na foldere i daje pravo korisniku da može da vidi sadržaj foldera. Korisnik ne može da vidi sadržaj samih fajlova koji se nalaze u folderu. (Obradović, S., Maček, N., Stanišević, I., 2010, str. 83)

Special permissions dozvola omogućava kreiranje specifičnih dozvola kada nijedna od napred navedenih dozvola ne odgovara pravima koja treba dodeliti korisniku. Ove dozvole se kreiraju preko tzv. atomskih dozvola.

Atomske dozvole su: traverse folder/execute file, list folder/read data, read attributes, read extended attributes, create files/write data, create folders/append data, write attributes, write extended attributes, delete subfolders and files, delete, read permissions, change permissions i take ownership.

Traverse folder/execute file dozvola omogućava korisniku pristup folderu koji se nalazi u folderima nad kojim on nema nikakva prava. Na taj način korisnik se direktno prebacuje u taj folder.

Listfolder/read data omogućava prikazivanje naziva fajlova i foldera (list data) u okviru datog direktorijuma i prikazivanje sadržaja fajla (read data). Ova dva prava zajedno čine osnovu prava ranije opisane dozvole read.

Read attributes daje prava korisniku da vidi atribut objekta, kao što su read-only, hidden, system i archive.

Read extended attributes omogućava korisniku da vidi dodatne atribut koje dodaju neki programi. Na primer, kod dokumenata koji su urađeni u Microsoft Wordu mogu se videti sledeći dodatni atributi: author, subject, title manager, company itd.

Create files/write data je dozvola koja omogućava postavljanje novih fajlova u okviru foldera. Ova dozvola omogućava prepisivanje postojećih podataka u fajlu, ali ne i dodavanje podataka u postojeći fajl.

Write attributes dozvola omogućava izmenu osnovnih atributa fajla (read-only, hidden, system i archive).

Write extended attributes omogućava izmenu dodatnih atributa fajla.

Delete subfolders and files je dozvola za brisanje podfoldera i fajlova, čak i kada korisnik nema dozvolu delete za određeni podfolder ili fajl. (Obradović, S., Maček, N., Stanišević, I., 2010, str. 83)

Delete dozvola omogućava brisanje objekta. Ako korisnik nema prava nad nekim fajlova u okviru foldera, a ima dozvolu delete nad tim folderom, on neće moći da obriše taj folder. Fajl ne može da se obriše ako ne postoji dozvola delete za taj fajl.

Read permissions dozvola omogućava prikazivanje svih NTFS dozvola koje su dodeljene određenom objektu. (Pokorni, S., 2015, str. 125)

Change permissions dozvola daje pravo korisniku da promeni dozvole koje su dodeljene nekom objektu.

Take ownership dozvola daje pravo korisniku da preuzme vlasništvo nad objektom. Kada se kreira određeni objekat ova dozvola se automatski dodeljuje administratoru sistema.

Kod deljenih foldera postoje tri vrste dozvola. To su full, change i read. Full dozvola daje pravo korisniku da izvršava sve funkcije nad svim folderima i fajlovima u deljenom folderu. Change dozvola daje pravo korisniku da čita, izvršava, briše i menja fajlove i direktorijume u deljenom folderu. Read dozvola omogućava korisniku listanje sadržaja foldera, čitanje fajlova i pokretanje fajla kada se radi o izvršnom programu.

Postoje i kontrole pristupa koje nisu zasnovane na identitetu korisnika. One se odnose više na uopštene mere kontrole pristupa resursu. Tu spadaju: vreme dana kada može da se

pristupi resursu, IP adresa sa koje može da se pristupi, domen sa kojeg tnože da se pristupi, vrsta enkripcije koju HTTP klijent treba da podrži, posedovanje bilo kojeg tipa hardverskog ili softverskog tokena itd.

3.3. Firewall

Firewall (mrežna barijera, zaštitni zid) predstavlja bezbednosni sistem kojim se štiti računar ili računarska mreža od neautorizovanog pristupa. Firewall može biti softverski, hardverski ili kombinacija hardvera i softvera. Obično se nalazi se na granici između lokalne i javne mreže (Interneta). Firewall vrši filtriranje mrežnog saobraćaja. Na njemu se postavljaju pravila kojima se dozvoljava ili zabranjuje određena vrsta mrežnog saobraćaja između mreža koje razdvaja.

Sve pakete koji ulaze u lokalnu mrežu, ili iz nje izlaze, firewall ispituje. Proverava se vrsta protokola, izvorišna i odredišna IP adresa, odredišni i izvorišni port, broj fragmentiranog paketa, tabela sa informacijama o rutiranju paketa. Ako paket prođe sve provere on se propušta, ako ne prođe blokira se. Firewall takođe može da kontroliše prava pristupa serverima, ili drugim računarima unutar same lokalne mreže. (Spasić, D., 2012, str. 111)

Firewall može da vrši kontrolu pristupa na osnovu osnovne i napredne access liste, na osnovu dinamičke i vremenski bazirane access control liste, može da vrši kontrolu pristupa na bazi određene politike ili na osnovu sadržaja, da blokira Java i ActiveX aplete, vrši prevođenje mrežnih adresa i mapiranje portova.

On može da beleži različite sumnjive događaje i da štiti mrežu od različitih napada kao što su: IP spoofing, SYN napad, Land napad, Ping smrti, napad skeniranjem portova itd.

Firewall omogućava autentifikaciju i autorizaciju korisnika i autentifikaciju rutera, šifrovanje korišćenjem algoritama za šifrovanje kao što su DES, 3DES i AES.

Firewall-i se kreću od jednostavnih, koji se koriste za kućnu upotrebu ili zaštitu jednog računara, do vrlo složenih koji se koriste za zaštitu kompanijskih računarskih mreža. Kroz firewall se implementira sigurnosna politika kompanije.

Firewall se koristi i za ograničavanje pristupa određenim sajtovima koji mogu da ugroze sigurnost ili njihovo posećivanje može da ugrozi reputaciju kompanije.

Zavisno od sloja OSI modela na kojem se odvija komunikacija, firewall-i mogu da se podele u sledeće 4 grupe:

- Firewall koji filtrira pakete (Packet-filtering firewall)
- Firewall koji radi na transportnom sloju (Circuit-level gateway)
- Firewall koji radi na aplikativnom sloju (Application-level gateway)
- Firewall sa višeslojnim ispitivanjem paketa (Stateful inspection firewall) (Stojčev, M.K., 2012, str. 153)

Packet-filtering firewall. Packet-filtering firewall je ruter koji filtrira pakete na osnovu informacija u TCP i IP zaglavlju. Većina ovih firewall-a može da prihvati ili odbije paket na osnovu:

- izvorišne adrese
- odredišne adrese
- protokola
- broja izvorišnog porta
- broja odredišnog porta (Tanenbaum, E.S., 2013, str. 225)

Za razliku od običnog rutera koji prosleđuje pakete na odgovarajuću mrežu, Packet-filtering firewall, pre nego što prosledi paket, proverava da li paket ispunjava sve uslove koji su navedeni u pravilima koja određuju koji paket propustiti, a koji odbiti.

Circuit-level gateway. Circuit-level gateway nadgleda uspostavljanje TCP end-to-end sesije između poverljivih klijenata i servera sa nepoverljivim hostovima i obrnuto. Kod filtriranja podataka na ovaj način, circuit-level gateway se oslanja na podatke iz zaglavlja paketa koji se odnose na protokole sloja sesije. Sesija se smatra legitimnom samo ako SYN i ACK zastavice (bitovi) i SEQ broj (broj sekvence) koji su uključeni u uspostavu veze putem trostrukog rukovanja (TCP handshaking) između servera (ili klijenta) kojem se veruje i hosta, kojem se ne veruje, imaju logične vrednosti. Kada se utvrdi da je konekcija

legitimna circuit-level gateway uspostavlja TCP sesiju. Od tog momenta nadalje circuit-level gateway ne vrši nikakvo filtriranje nego samo kopira i prosleđuje pakete između strana koje učestvuju u sesiji. Circuit-level gateway mapira sve lokalne IP adrese sa jednom javnom IP adresom (address translation) tako da svi odlazeći paketi imaju istu IP adresu (javna adresa gateway-a). Na taj način se sprečava direktan kontakt između lokalne mreže i nesigurne javne mreže (Interneta). (Urošević, Z., 2012, str. 154)

Slabost ovog gateway-a je što se, kada se uspostavi sesija, svaka aplikacija može da radi preko te konekcije jer se ne vrši filtriranje paketa na sloju aplikacije. Drugim rečima, circuit-level gateway ne može da vrši filtriranje sadržaja paketa na aplikativnom sloju koji razmenjuju poverljive i nepoverljive mreže. Ovo otvara mogućnost hakerima da u sesiju ubace paketi sa zlonamernim sadržajem.

Application-level Gateway. Application-level Gateway radi na aplikativnom sloju OSI modela. Radi kao proksi server i tako sprečava direktnu vezu između poverljive lokalne mreže nesigurne javne mreže (Interneta). Proverava i filtrira pojedinačne pakete na aplikativnom sloju. Mogu da prođu samo paketi za koje postoji dozvola na serveru. Na primer, ako postoje dozvole samo za FTP i HTTP servise, onda će samo moći da prolaze paketi koje su generisali ovi servisi, odnosno biće dopušten samo FTP i HTTP saobraćaj.

Gejtveji koji rade na aplikativnom sloju takođe mogu da ograniče izvršavanje određenih komandi. Na primer, moguće je zabraniti komandu PUT koja omogućava korisnicima da upisuju svoje podatke na FTP serveru.

Stateful Inspection Firewall. Stateful Inspection Firewall kombinuje karakteristike sva tri prethodno opisana firewall-a, što mu omogućava višeslojno ispitivanje paketa. Ima bolje performanse i veći stepen sigurnosti od svih prethodno navedenih firewall-a. Aplikativni gejtvej razdvaja konekciju između servera i klijenta na dve konekcije, jednu sa serverom drugu sa klijentom, a zatim razmenjuje pakete između njih, što daje određeni stepen sigurnosti, ali i usporava vezu. Stateful Inspection Firewall, s druge strane, ne zahteva dve konekcije, nego omogućava direktnu vezu između verovanog servera i hosta iz nesigurne mreže. Da bi obezbedio da ova veza bude sigurna, firewall presreće i proverava svaki paket na aplikativnom sloju. (Urošević, Z., 2012, str. 156)

3.3.1. Packet-filtering firewall

Packet-filtering firewall je ruter koji filtrira pakete na osnovu informacija u TCP i IP zaglavlju. Većina ovih firewall-a može da prihvati ili odbije paket na osnovu:

- izvorišne adrese
- odredišne adrese
- protokola
- broja izvorišnog porta
- broja odredišnog porta (Tanenbaum, E.S., 2013, str. 225)

Za razliku od običnog rutera koji prosleđuje pakete na odgovarajuću mrežu, Packet-filtering firewall, pre nego što prosledi paket, proverava da li paket ispunjava sve uslove koji su navedeni u pravilima koja određuju koji paket propustiti, a koji odbiti.

3.3.2. Circuit-level gateway

Circuit-level gateway nadgleda uspostavljanje TCP end-to-end sesije između poverljivih klijenata i servera sa nepoverljivim hostovima i obrnuto. Kod filtriranja podatak na ovaj način, circuit-level gateway se oslanja na podatke iz zaglavlja paketa koji se odnose na protokole sloja sesije. Sesija se smatra legitimnom samo ako SYN i ACK zastavice (bitovi) i SEQ broj (broj sekvence) koji su uključeni u uspostavu veze putem trostrukog rukovanja (TCP handshaking) između servera (ili klijenta) kojem se veruje i hosta, kojem se ne veruje, imaju logične vrednosti. Kada se utvrdi da je konekcija legitimna circuit-level gateway uspostavlja TCP sesiju. Od tog momenta nadalje circuit-level gateway ne vrši nikakvo filtriranje nego samo kopira i prosleđuje pakete između strana koje učestvuju u sesiji.

Circuit-level gateway mapira sve lokalne IP adrese sa jednom javnom IP adresom (address translation) tako da svi odlazeći paketi imaju istu IP adresu (javna adresa gateway-a). Na taj način se sprečava direktan kontakt između lokalne mreže i nesigurne javne mreže (Interneta). (Tanenbaum, E.S., 2013, str. 226)

Slabost ovog gateway-a je što se, kada se uspostavi sesija, svaka aplikacija može da radi preko te konekcije jer se ne vrši filtriranje paketa na sloju aplikacije. Drugim rečima, circuit-level gateway ne može da vrši filtriranje sadržaja paketa na aplikativnom sloju koji razmenjuju poverljive i nepoverljive mreže. Ovo otvara mogućnost hakerima da u sesiju ubace paketi sa zlonamernim sadržajem.

3.3.3. Application-level Gateway

Application-level Gateway radi na aplikativnom sloju OSI modela. Radi kao proksi server i tako sprečava direktnu vezu između poverljive lokalne mreže nesigurne javne mreže (Interneta). Proverava i filtrira pojedinačne pakete na aplikativnom sloju. Mogu da prođu samo paketi za koje postoji dozvola na serveru. Na primer, ako postoje dozvole samo za FTP i HTTP servise, onda će samo moći da prolaze paketi koje su generisali ovi servisi, odnosno biće dopušten samo FTP i HTTP saobraćaj.

Gejtveji koji rade na aplikativnom sloju takođe mogu da ograniče izvršavanje određenih komandi. Na primer, moguće je zabraniti komandu PUT koja omogućava korisnicima da upisuju svoje podatke na FTP serveru. (Tanenbaum, E.S., 2013, str. 227)

3.3.4. Stateful Inspection Firewall

Stateful Inspection Firewall kombinuje karakteristike sva tri prethodno opisana firewall-a, što mu omogućava višeslojno ispitivanje paketa. Ima bolje performanse i veći stepen sigurnosti od svih prethodno navedenih firewall-a. Aplikativni gejtvej razdvaja konekciju između servera i klijenta na dve konekcije, jednu sa serverom drugu sa klijentom, a zatim razmenjuje pakete između njih, što daje određeni stepen sigurnosti, ali i usporava vezu. Stateful Inspection Firewall, s druge strane, ne zahteva dve konekcije, nego omogućava direktnu vezu između verovanog servera i hosta iz nesigurne mreže. Da bi obezbedio da ova veza bude sigurna, firewall presreće i proverava svaki paket na aplikativnom sloju. (Urošević, Z., 2012, str. 156)

3.4. Računarski programi

Više ne postoji nikakva sumnja da pronalazak kompjutera i kompjuterskih programa koji njima upravljaju, predstavlja prekretnicu u istoriji savremenog čovečanstva. Kao što je pronalazak parne mašine bio ključni događaj za pojavu industrijske ere, tako nas kompjuteri danas uvode u jednu novu eru, eru informatičkog, visoko-tehnološkog društva. Njihova pojava presudno je uticala prvenstveno na tehnološki, a kao posledica toga i na opšti ekonomski i privredni razvoj pre svega najrazvijenijih svetskih ekonomija, dok je danas ovaj fenomen prisutan i na globalnom planu.

Dva osnovna sastavna dela svakog kompjutera čine hardver (elektronski uređaj, mašina) i softver, odnosno kompjuterski programi. Softver se sastoji od ljudskih komandi izraženih posebno stvorenim simbolima pretvorenim u tzv. programske jezike, kojih ima nekoliko i koji poseduju mogućnost konvertovanja jednih u druge. Kompjuterski program zapravo čini lanac informacija koji hardveru, odnosno samom uređaju daje određenu funkciju (npr. prevođenja, projektovanja, analitičkog planiranja, vođenja knjigovodstva, upravljanja nuklearnim elektranama i drugim postrojenjima itd.)

Kao novo, strateško sredstvo za zauzimanje dominantnog, odnosno preovlađujućeg položaja na različitim tržišnim strukturama, razvijanje novih kompjuterskih programa zahteva značajna finansijska sredstva, kao i angažovanje najelitnijih humanih resursa. Kompjuterski programi su se, nedugo nakon svog pojavljivanja, pokazali kao element koji igra sve značajniju ulogu u različitim industrijskim granama, pa se za tehnologiju kompjuterskih programa može slobodno reći da ima fundamentalni značaj za industrijski razvoj svakog savremenog društva.

Upravo zbog astronomskih prihoda koji rezultiraju iz ovih produkata ljudskog uma, nužno se postavilo i pitanje neophodnosti njihove zaštite putem zakonskih propisa. Adekvatna pravna zaštita postavila se kao imperativ i zbog nesagledivih posledica koje bi imalo zadržavanje u tajnosti ovakve vrste tehnologija, pa je za autore kompjuterskih programa trebalo obezbediti mogućnost zakonitog prenosa prava na druga lica, kao i ostale načine zadovoljavajućeg iskorišćavanja njihovih prava. Najzad, i kompjuterski programi predstavljaju rezultat čovekovih stvaralačkih sposobnosti, pa ih je, kao i ostale takve

proizvode, bilo nužno zaštititi od raznih vrsta zloupotreba koje su u savremenim uslovima sve više rasprostranjene. Naime, kopiranje kompjuterskih programa, bez plaćanja bilo kakve naknade njihovim autorima i bez bilo kakvog ulaganja u njihov razvoj, postalo je veoma brzo rasprostranjena svakodnevna pojava.

U pravnoj teoriji i praksi, nije postojala dilema da li ove nove tekovine ljudskog stvaralaštva treba zaštititi ili ne, već se ona javila u pogledu toga da li pravnu zaštitu treba obezbediti kroz postojeće institute ili je potrebno stvoriti novu, posebnu i specijalizovanu granu prava.

Naše pravo se, prihvatajući opšteprihvaćeno rešenje u uporednom pravu, opredelilo za mišljenje da računarski program predstavlja rezultat čovekovog stvaralaštva odnosno duhovnu tvorevinu, te da ih treba štititi u okviru postojeće grane prava - intelektualne svojine, kao generičkog pojma za disciplinu koja u sebi sadrži industrijsku svojinu i autorsko pravo. U okviru ove grane prava, rezultati ljudskog stvaralaštva mogu da uživaju pravnu zaštitu bilo na osnovu propisa patentnog prava bilo autorskog prava, a sve u zavisnosti od toga koja će se od dve osnovne koncepcije izabrati - ona da je softver, odnosno kompjuterski pojam, bliži pojmu pronalaska ili ona da je računarski program autorsko delo.

Postoje i mišljenja da je računarske programe moguće zaštititi putem primene pravila o nelojalnoj konkurenciji. Međutim, ne treba izgubiti iz vida činjenicu da ova pravila štite nosioca, odnosno vlasnika prava intelektualne svojine (koji u najvećem broju slučajeva nije tvorac autorskog dela ili pronalaska) od postupaka trećih lica koji su suprotni načelima zdrave, lojalne konkurencije, a ne samog tvorca programa kao produkta ljudskog uma.

Takođe, rasprostranjeno je i mišljenje da računarske programe treba posmatrati kao vrstu poslovne tajne, odnosno know-how-a, pri čemu se zaštita ostvaruje kako na osnovu kriterijuma tajnosti programa, odnosno činjenice da drugi učesnici na tržištu ne raspolažu takvim softverom, tako i na osnovu ugovora o transferu tehnologije, na osnovu koga se proizvođač ili imalac programa obavezuje korisniku da će čuvati tajnost programa. Ovakva mišljenja nisu zaživela u praksi, pa je u uporednom pravu najrasprostranjeniji vid zaštite, zaštita u okviru prava intelektualne svojine. (Ljubičić, D., Franjić, A., 2012, str. 108)

3.5. Pretnje sigurnosti podataka

Postoji šest grupa incidenata koji mogu ozbiljno da ugroza sigurnost podataka u računaru, a to su:

- dejstvo više sile,
- hardverske i softverske greške,
- ljudska nepažnja,
- namerna oštećenja,
- kriminal i
- atak na tajnost.

Posledice ovih incidenata se mogu realizovati kroz:

- gubitak pojedinih slogova,
- modifikaciju slogova,
- gubitak celokupne datoteke,
- uskraćivanje mogućnosti korišćenja datoteke i
- neovlašćeno čitanje i kopiranje slogova.

Program zaštite se pravi s ciljem da zaštiti instalaciju i to, kroz krupne događaje koji se retko dešavaju, kao što je vatra ili velika pronevera, tako i sitna oštećenja pojedinih slogova koja se mogu desiti više puta nedeljno. Postavljaju se tri pravca delovanja i to:

1. Minimiziranje verovatnoće da se pretnja uopšte ostvari, preventivnim delovanjem.
2. Minimiziranje štete, ukoliko se pretnja ostvari.
3. Projektovanje metoda oporavka od štete nastale ostvarenjem neke pretnje, bilo kako ozbiljna bila, pri čemu se pretpostavlja da vitalni slogovi, (npr. stanje računara), ne smeju ni u kom slučaju biti uništeni.

Korisno je za svaku instalaciju napraviti tabelu procene verovatnoće dešavanja pojedinih pretnji. Tabela br. 1 je jedan takav primer koji pokazuje kako to može biti urađeno, pri čemu brojevi u tabeli predstavljaju verovatnoću dešavanja pojedinog događaja prema ključu datom u tabeli 1. (Đorđević, B., Đorđević, M., 2010, str. 129)

Tabela 1.

P	Verovatnoća da se neki događaj desi
0	praktično nemoguće
1	može se desiti jednom u 400 godina
2	može se desiti jednom u 40 godina
3	može se desiti jednom u 4 godine (1000 dana)
4	može se desiti jednom u 100 radnih dana
5	može se desiti jednom u 10 radnih dana
6	može se desiti jednom dnevno
7	može se desiti deset puta dnevno

Izvor: Bjelica, M. (2013) *Telekomunikacione i računarske mreže*, Akademska misao, Beograd, str. 101

Na osnovu procene verovatnoće događanja određene pretnje, izračunava se izloženost sistema pretnji. Ona zavisi od štete koju bi pretnja uzrokovala ako bi se u praksi ostvarila. Procena štete se određuje na osnovu sledeće šeme:

Tabela 2.

D	Šteta nastala ukoliko se neka pretnja ostvari
0	zanemarljiva (reda 1 DM)
1	reda 10 DM
2	reda 100 DM
3	reda 1000 DM
4	reda 10 000 DM
5	reda 100 000 DM
6	reda 1 000 000 DM
7	reda 10 000 000 DM

Izvor: Bjelica, M. (2013) *Telekomunikacione i računarske mreže*, Akademska misao, Beograd, str. 103

Korišćenjem navedenih oznaka može se izračunati izloženost sistema (E) pojedinoj pretnji, prema formuli:

$$E = \frac{10^{(P+D-1)}}{4} \text{ DM godišnje}$$

Računanjem procene izloženosti sistema pojedinim pretnjama može se doći do zaključka da je, na primer, ugroženost od događaja koji se češće dešava sa malom štetom veća od onog koji pravi veću štetu, ali je verovatnoća njegovog događanja mala. Tako se na osnovu izračunatih procena pretnji mogu pravilno usmeriti naponi da se određene pretnje preduprede. Osim toga, obezbeđenjem zaštite od određene pretnje na više nezavisnih načina, verovatnoća njenog događanja se značajno smanjuje, pa time i izloženost datoj pretnji.

Najvažnija pretnja za elektronski prenos novca je pretnja od pronevere. Dok sa jedne strane računar omogućava da se raznim proverama, koje se pomoću njega mogu efikasnije izvoditi, spreče klasični načini pronevere, sa druge strane se otvara niz drugih mogućnosti za proneveru. Zahvaljujući pre svega velikoj koncentraciji podataka u računaru, kontroli je mnogo teže da pronade modifikovani slog, jer se on modifikuje u računaru. Programi koji bi napravili modifikaciju mogu se pojaviti samo na kratko i odmah nestati. Pri tome se ne ostavlja otisak prsta niti bilo koji drugi trag koji bi doveo do prekršioaca. Da se prikrije šta se desilo nije potrebno spaljivati knjige - evidencija o tome se uništava brisanjem traka ili diskova. (Pokorni, S., 2015, str. 161)

4. Korisničke metode nadgledanja bankarskih transakcija

Internet korisnici bi trebalo da osiguraju svoju normalnu proveru obračuna bankarske i kreditne kartice od neovlašćenih transakcija. Pored toga, korisnik može povremeno da izvrši ličnu kreditnu proveru sa priznatom akreditovanom kreditnom agencijom da bi video da li je bilo kakvih neovlašćenih korišćenja njegovog korisničkog imena i ličnih podataka za dobijanje kredita od bilo koje finansijske institucije.

Ako je korisnik otkrio bilo kakvu finansijsku zloupotrebu, trebalo bi odmah da obavesti finansijsku instituciju i da to potvrdi i pismeno. Takođe bi trebalo da registruje činjenicu da je njegov identitet kompromitovan sa CIFAS ili kod jedne od priznatih kreditnih agencija, da bi sprečio buduće neovlašćeno korišćenje svojih ličnih podataka.

Deset tačaka kao priručnik za zaštitu on-line korisničkog identiteta:

1. **Držite sve vreme razboritost o vama.** Potrebno je razumeti rizik i funkcionisanje na internetu na isti način kao i u off-line svetu, sa oprežnošću i neophodnim skepticizmom. Ali ne treba biti bez straha sa jednostavnim merama predostrožnosti jer je to sigurno za korišćenje u on-line bankarstvu i elektronskoj trgovini.
2. **Zapitajte se zašto je neki web-sajt tražio informacije o vama.** Mislite o tome da li postoji negde ili neko ko želi da uzme vaše identifikacione detalje. Samo koristite bezbedne web-sajtove, a takođe koristite vaš opšti osećaj kada dolazi do phishing e-mail-ova i web sajtova.
3. **Nikad nemojte davati bilo koji on-line bezbedonosni detalj, bilo kome, osim ako nije krajnje neophodno.** Budite podesno oprezni ako vi delite vaše podešavanje sa drugim ljudima. Razmotrite način postavljanja lozinki na vašem kompjuteru da bi izbegli nepotreban pristup.
4. **Pazite na vašu lozinku – password.** Menjajte vašu lozinku redovno i izbegavajte standardne lozinke slične imenima članova porodice ili reči iz rečnika. Kada kreirate lozinku, ako je moguće, koristite kombinaciju slova, brojeva i specijalnih znakova, slično stvaranju exclamation. To će učiniti vašu lozinku jakom. Ne koristiti iste lozinke za svaki bezbedan sajt na koji ste registrovani.

5. **Nikad nemojte da kliknete na link iz e-mail-a.** Uvek kucajte web-sajt adresu (www) za banke, finansijske institucije i sajtove za nabavku u browser adresu liniju ili zapamtite takvu adresu u internet explorer funkciju "favorites", u okviru browser funkcije.
6. **Držite ažurne - aktuelne podatke.** Ažurirajte vaše bezbedonosne softvere kako bi bili aktuelni, (anti-virus, anti-spam, anti-spyware i firewall), operativni sistem i aplikacije kao što su Microsoft Office i to radite uvek.
7. **Udaljeno špijuniranje.** Proverite sve fajlove u svakom kompjuteru koji su priključeni na internet bar svake nedelje korišćenjem aplikacija anti-spyware i adware.
8. **Osigurajte vašu konekciju.** Budite sigurni da svako ko koristi kompjuter razume mere predostrožnosti koje su potrebne da se održavaju kada se korisnik nalazi u on-line režimu rada. Nemojte ostavljati vašu broadband konekciju uključenu ako je ne koristite, a ako koristite bežični modem osigurajte da bude podešen na poslednju 128-bitnu enkripciju, ako ste registrovani za on-line bankarsko poslovanje.
9. **Ako izgleda suviše dobro da bi bilo istinito, verovatno i jeste problematično.** Ne otvarajte e-mail i ne idite na sajt koji obećava dobijanje nagrade ako unesete specifične kompetencije. Ako jedan e-mail izgleda sumnjiv i nije traženo da bude izbrisan, ne otvarajte ga.
10. **Treba znati gde potražiti pomoć ako ste žrtva on-line krađe identiteta.** Postoji širok rang organizacija i grupa tako da ljudi mogu da se obrate za savet kada su žrtve krađe on-line identifikacije. U nastavku je dat kratak pregled, koji bi uključio policiju, tela pojedinih delatnosti i dobavljače sa on-line uslugama. (Žorić, A., 2012, str. 48)

4.1. Hakerisanje (hacking)

Pošto je donet nov zakon o zaštiti podataka u Velikoj Britaniji, trebalo bi se podsetiti šta je to "hakerisanje". Hakerisanje je sticanje bespravnog, neovlašćenog pristupa kompjuterskom sistemu, a često taj proces može da dovede i do promene određenih sadržaja u računaru. Hakerisanje može da bude urađeno praćenjem određenih kriminalnih aktivnosti, ali to može da bude i hobi, na osnovu kojeg haker radi sam, ili šalje informacije drugima. Hakerisanje je često neškodljiva aktivnost, sa učesnicima koji uživaju u izazovima da prekinu deo sistema odbrane, ali ozbiljna šteta može biti uzrokovana na kompjuterskom sistemu vlasnika, ako je to cilj hakera. Iako je kompjutersko hakerisanje u

najopštijem slučaju povezano sa spoljnim upadom u kompjuterski informacioni sistem, novi zakon u Velikoj Britaniji se jednako primenjuje i na neovlašćeni pristup u jedan kompanijski kompjuterski informacioni sistem od strane sopstvenih zaposlenih radnika.

Postalo je ilegalno da se dobije pristup ili pokušaj da se dobije pristup u kompjuterski informacioni sistem bez preciznog ovlašćenja. Nije neophodno da se uspe u dobijanju pristupa da bi se osudilo za ovo krivično delo. Maksimalna kazna za ovo delo je šest meseci zatvora i/ili novčana kazna.

Na primer, radnik kompanije može dobiti neovlašćen pristup slogovima zarada, možda korišćenjem lozinke jednog autorizovanog korisnika i gledati zarade isplaćene kompanijskim direktorima. To je prekršaj koji se sada sankcioniše.

Maksimalna kazna za ovaj prekršaj odnosno zločin je značajno veća nego predviđena kazna za neovlašćeni pristup:

- u kratkoj osudi jednog prekršioca obavezna je kazna od šest meseci zatvora i/ili ekvivalentna novčana globa;
- u osudi ili optužnici jedan prekršilac može biti zatvoren na pet godina zatvora i/ili neograničenu novčanu kaznu. (Pokorni, S., 2015, str. 164)

Na primer, radnik kompanije može dobiti neovlašćen pristup slogovima zaposlenih i naći informacije o zaposlenima koje može iskoristiti za ucenu. Ovaj prekršaj vrši osoba koja je kriva za pokušaj takvog zakonskog prekršaja, ako njena namera nije sprečena, već je ostvaren nevidljiv pristup bilo kom programu ili podatku ili je ugrožena pouzdanost podataka ili programa u kompjuterskom sistemu. Kazna za ovaj prekršaj je ista kao za prekršaj neovlašćenog pristupa sa namerom da se preda drugom prekršiocu.

4.2. Virusi

Virusi su delovi softvera čiji je zadatak da inficiraju kompjuterski sistem, najčešće nevidljivo. Oni se automatski šire na druge informacione sisteme ako dobiju tu mogućnost.

Mnogi kompjuterski virusi imaju tri funkcije - izbegavanje detekcije, samostalnu reprodukciju i izazivanje štete u kompjuterskom sistemu.

Izazvana šteta može biti relativno neškodljiva i zabavna (najbolji primer za to je: "kaskada", izazvana pismom da "pada" na ekranu). Međutim, u praksi smo često suočeni i sa ozbiljnijim štetama. Poslednjih godina, dva virusa, osobito ("Mellisa" i "I Love You") koji su se raširili posredstvom adresa elektronske pošte širom sveta (e-mail-a), su unutar vrlo kratkog vremena, naneli znatnu štetu informacionim sistemima i poslovanju koje je zavisilo od njih. (Veinović, M., Adamović, S., 2012, str. 76)

4.3. Bezbednost

Bezbednost može da se definiše kao:

- zaštita podataka od neovlašćenog pristupa, promene ili modifikacije podataka,
- zaštita programa od neovlašćene izmene,
- obezbeđenje da informacioni sistem funkcioniše kao što je osmišljen i da korisnici nastavljaju da dobijaju usluge koje su im potrebne,
- zaštita hardvera od oštećenja,
- zaštita ljudi od povreda i nezgoda. (Mur-Malinos, Dž., Mazali, G., 2014, str. 73)

Štete na podacima, hardveru i softveru mogu da budu uzrokovane promišljenim akcijama ili slučajno, a mogu biti uzrokovane božijom voljom, ljudskim zlonamernim delovanjem ili greškama. Osiguranje da informacioni sistem funkcioniše kao što je definisano u specifikaciji korisničkih zahteva implicira da se sistemske greške takođe nalaze unutar opštih definicija bezbedonosnih problema. Bezbednost je stoga širok pojam i važan deo menadžmenta informacionih tehnologija i mora se uzeti u razmatranje veoma ozbiljno. Politika bezbednosti bi trebalo da se razmatra u okviru menadžmenta kompanije, da bi se izbegle ili minimizovale pretnje, predviđanje i detekcija problema i obnavljanje informacionog sistema, posle nastalih problema.

4.4. Mere koje preduzimaju ISP, banke, trgovci na malo i prodavci softvera radi pomaganja i zaštite krajnjih potrošača

Sve strane koje imaju interes u on-line bezbednosti, iz ranga oblasti raznih delatnosti, vlade i zakonske primene su povećali rad zajedno u inicijativi za obe svrhe, da bi edukovali i zaštitili ljude kada su u on-line režimu rada i uhvatili kriminalce koji koriste internet kao sredstvo dolaska do novca. Najnovija Get Safe Online inicijativa je doneta zajedno sa vladom i zakonskom primenom sa kompanijama BT, eBay, HSBC, Lloyds TSB, Microsoft, bezbedne trgovine i laboratorije poruka (Message Labs) da obezbedi lako razumevanje ekspertnog saveta oko on-line krađa i kako da se sami potrošači zaštite.

Ministarstvo unutrašnjih poslova Velike Britanije je proizvelo informacije u vezi sa tim kako da se zaštititi korisnički identitet i kako da se otkrije ako ga je neko koristio zlonamerno u cilju obmane i zakonsko primenjivanje agencija kao što su Metropolitan Police koje imaju inicijativu vezanu za prevare, koja omogućava ljudima da pošalju zahtev za e-mail savet. Agencija dobija oko 400 e-mail-ova dnevno zbog prevara, sa mnogo navodnih napada koji su nastali on-line.

Banke i organizacije za finansijski servis su takođe gledale na koji način da spreče potrošače da zapadnu u prekršaj zbog malicioznih e-mail-ova i hacking-a, uključujući probe dveju vrsta bezbednosnih sistema od strane Lloyds TSB. Tu je ključ prstenasta veličina jedinice bezbednosti koja generiše šest digitalnih kodova svakih 30 sekundi i koja se koristi u paru sa standardnim korisničkim imenom i lozinkom.

U vezi sa tim je rad koji je Uprava finansijskog servisa "FSA" uradila povodom on-line bezbednosti. Ona je obelodanila da je više od 50 procenata ljudi izuzetno zabrinuto zbog rizika od on-line prevara, a manje nego skoro četvrtina ne zna kada su poslednji put ažurirali svoj softver za bezbednost.

Industrija je udružila snage i radila zajedno da bi promovisala poruke koje su se same uništavale, ali te mere nisu bile dovoljne da bi zaštitile potrošače. Organizacije kao što je CPP su takođe istraživale način na koji kriminalci krađu identifikaciju i koriste je da bi izvršili prevare. Internet servis provajderi ISP imaju širok opseg inicijative da bi pomogli

potrošačima u on-line bezbednosti. Mnogi obezbeđuju softver da bi se zaštitili protiv virusa, isto tako dobro kao i filtere za zaštitu e-mail poruka od spama i virusa pre nego što dopru do korisnika kako bi minimizovali rizik od trojanaca i drugih malicioznih kodova koji se instaliraju na mašini.

ISP je razvio inicijativu za edukaciju vezanu za rizike i predostrožnost korisnika. Ova inicijativa bi trebalo da bude zadržana kada korisnik radi on-line, pošto mnogi nisu svesni da su izloženi pretnjama, kao što su phishing i hacking. Provajderi elektronske pošte, kao što je na primer Yahoo Mail su takođe razvili tehnologiju kao što je ključ domena DomainKeys da bi pomogli u borbi sa on-line pretnjama. DomainKeys razvijen od strane Yahoo nudi kriptografiju zasnovanu na rešenjima koja rešavaju probleme vezane za phishing i e-mail falsifikate, tako što proverava poreklo e-mail poruke. On je takođe nedavno udružio snage sa Cisco Sistemom da bi kreirao kombinovano tehnološko rešenje poznato kao DKIM koje je izloženo na internetu IETF za razmatranje kao jedan industrijski standard.

Na kraju, ISP softverski provajderi i vladina tela su počeli zajedno da rade u posebnoj tehničkoj grupi, sa radnim nazivom "Radna grupa protiv zloupotreba u porukama" da bi obezbedili da internet korisnici imaju najbezbedniji mogući on-line doživljaj. (Veinović, M., Jevremović, A., 2013, str. 197)

5. Zaštita podataka na internetu na primeru “Banca Intesa” d.o.o.

Slika 7. Logo Banca Intesa a.d. Beograd



Izvor: <http://www.bancaintesa.rs> (pregledano, 05.04.2016.)

5.1. Bezbednost transakcija na Internetu

Potrošači koriste Web-browser da bi naručili robu i poslali informacije o načinu plaćanja. Plaćanje može da se izvrši pomoću kreditne kartice, digitalnog keša, ili elektronskim čekom. Softver na serveru treba da izvrši transakciju verifikujući narudžbinu i obavljaajući autorizaciju radi transfera- sredstava iz banke izdavaoca kreditne kartice. Uobičajeno je da se ovaj poslednji korak obavlja uz pomoć gatewaya koji komunicira sa bankom bilo preko Interneta ili preko bančine privatne mreže. (<http://www.bancaintesa.rs>, pregledano, 05.04.2016.)

Slika 8. Ekspozitura banke

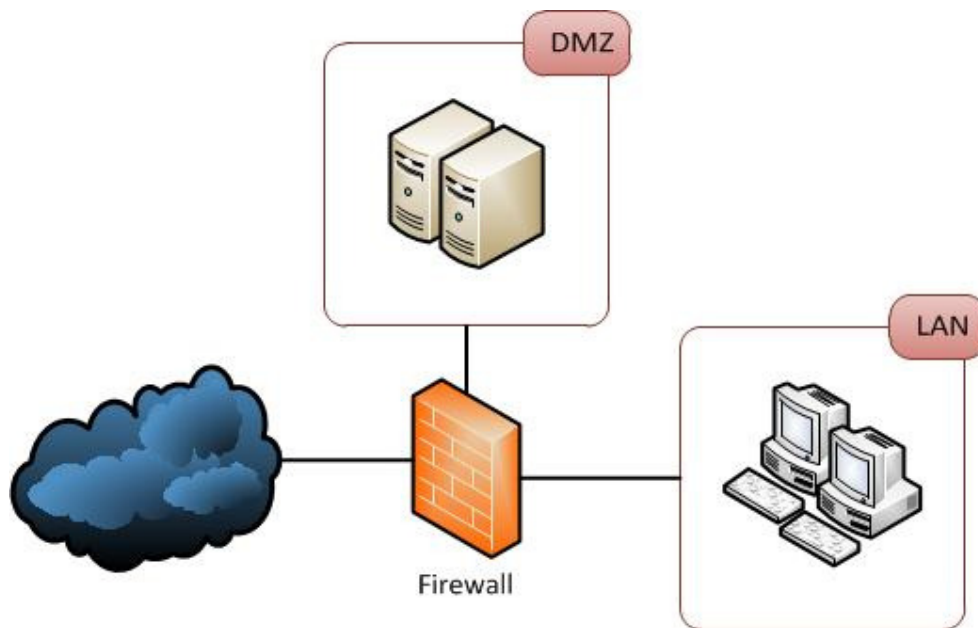


Izvor: <http://www.bancaintesa.rs> (pregledano, 05.04.2016.)

Sigurnost se obezbeđuje na sledeće načine:

- Firewall barijere služe da spreče licu da neovlašćeno pristupi određenom podatku, jer dozvoljava korisnicima da pristupe intranetu samo ako su autorizovani. Njega koriste organizacije i pogodaj je za primenu zato što se sa njima lakše sakrivaju određene informacije o članovima. S druge strane, firewall barijere su nedovoljne za celokupno obezbeđenje sigurnosti podataka i zbog toga predstavljaju njihov prvi korak u procesu obezbeđivanja sigurnosti.

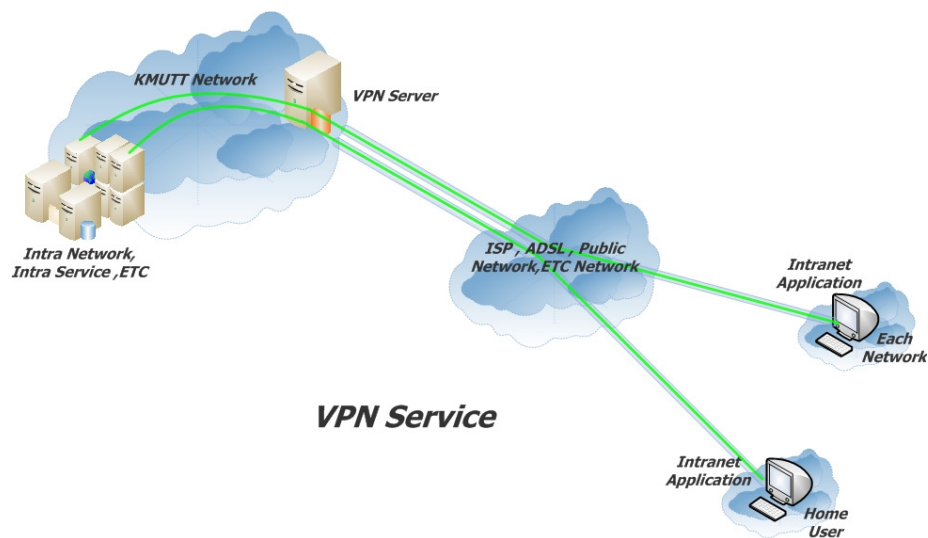
Slika 9. Funkcionisanje Firewall-a



Izvor: <http://www.security.stackexchange.com>, pregledano, 17.06.2016.

- Virtuelne privatne mreže, VPN (Virtual Private Network) imaju za cilj da obezbede vidljivost i privatnost podataka i time omogućavaju siguran prenos transakcija. Oni koji učestvuju u trgovini vrše proces komuniciranja preko virtuelne privatne mreže koja nije vidljiva za javnost. Na taj način čuvaju poverljivost transakcija na internetu.

Slika 10. VPN mreža



Izvor: <http://www.avesina.org>, pregledano 15.06.2016.

- Zatim, imamo tehnologiju enkripcije koja predstavlja šifrovanje podataka, digitalnih potpisa i sertifikata. Oni su mehanizmi koji vrše identifikaciju kupca i prodavca. Većina sistema elektronskog plaćanja bazira na nekim formama enkripcije i korišćenja digitalnih sertifikata.

Slika11. Šifrovanje podataka



Izvor: <http://www.go4it.ro>, pregledano 15.06.2016.

Postoje dve vrste kriptosistema za enkripciju podataka: simetrični i asimetrični. Simetrični kriptosistemi koriste isti ključ, tajni ključ, za enkripciju i dekripciju poruke. Pošiljalac i primalac imaju isti ključ, što znači da obe strane mogu šifrovati i dešifrovati podatke sa istim ključem, pri čemu prethodno moraju da se dogovore u pogledu zajedničkog tajnog ključa. Ovaj metod je brži, međutim, problem simetričnih kriptosistema je u tome što identitet pošiljaoca poruke ne može biti dokazan (na ovaj način samo se štiti tajnost i integritet informacija). Asimetrični kriptosistemi se zasnivaju na konceptu para ključeva: javnog ključa i tajnog ili privatnog ključa. Jedan ključ se koristi za enkripciju poruke, a drugi za njeno dekriptovanje. Bilo koji ključ iz para može biti korišćen za enkriptovanje podataka, dok se dekriptovanje može izvršiti samo sa drugim ključem iz para. (<http://www.bancaintesa.rs>, pregledano, 05.04.2016.)

Ako pošiljalac koristi javni ključ za enkriptovanje poruke obezbeđena je poverljivost poruke sve dok je primalac ne dekodira privatnim ključem. S druge strane, ako se koristi privatni ključ za kodiranje poruke, obezbeđen je dokaz autentičnosti pošiljaoca. Međutim, u ovom slučaju nema garancije da neko drugi već nije pročitao poruku, jer nije osigurana poverljivost kao u prethodnom slučaju gde dekodiranje može da izvrši samo vlasnik privatnog ključa. Najčešće korišćen asimetrični kriptografski algoritam je RSA algoritam, koji je dobio naziv po autorima koji su ga dizajnirali, Rivest, Shamir i Adelman. Ovaj algoritam najčešće koristi ključeve dužine 1024 bita u cilju postizanja zadovoljavajuće kriptografske zaštite.

Korišćenje asimetričnih kriptosistema za enkriptovanje poruka je sporo, pa su kriptografi došli na ideju da generišu kratku jedinstvenu reprezentaciju poruke, tzv. digest, odnosno ekstrakt poruke, koji može biti enkriptovan privatnim ključem i nakon toga korišćen kao digitalni potpis. Ovaj digitalni potpis ne može biti falsifikovan. Popularni, brzi kriptografski algoritam za generisanje digesta poruke poznat je kao jednostrana hash funkcija.

Hash funkcija je formula koja prevodi poruku u string, koji predstavlja digest poruke. Ovaj digest se enkriptuje privatnim ključem i kao digitalni potpis "lepi" na kraj poruke. Problem koji nije rešen korišćenjem digitalnog potpisa je problem privatnosti. Ovaj problem može biti rešen dodatnim korišćenjem simetričnog algoritma za enkriptovanje samog teksta poruke. Pošiljalac koristi simetrični ključ za enkriptovanje poruke, digitalnog potpisa i sertifikata pošiljaoca. Kao rezultat dobija se enkriptovana poruka. Pošiljalac šalje svoj sertifikat jer sadrži javni ključ pomoću koga primalac dešifruje digitalni potpis, i simetrični ključ koji je korišćen za enkriptovanje poruke.

U cilju očuvanja privatnosti ovog ključa pošiljalac koristi javni ključ primaoca, koji se nalazi u njegovom digitalnom sertifikatu, i rezultat, koji se naziva digitalni koverat, šalje zajedno sa enkriptovanom porukom primaocu. Primalac pomoću svog tajnog ključa dešifruje digitalni koverat da bi dobio simetrični ključ koji koristi za dekripciju poruke. Dešifrovana poruka sadrži poruku sa digitalnim potpisom i digitalni sertifikat pošiljaoca sa njegovim javnim ključem. Primalac poruke koristi javni ključ pošiljaoca za dešifrovanje digitalnog potpisa i dobija digest poruke. Zatim koristi istu hash funkciju, koja je prethodno dogovorena između njih, i primenjuje je na tekst poruke. Ako je izračunata

vrednost jednaka digestu poruke dobijenom dekodiranjem digitalnog potpisa, primalac može biti siguran da je digitalni potpis autentičan i da poruka nije neovlašćeno izmenjena. (<http://www.bancaintesa.rs>, pregledano, 05.04.2016.)

Jedna od ključnih aplikacija u kriptografiji za obezbeđenje autentifikacije, kao procesa verifikacije ljudi i entiteta, je digitalni sertifikat. Sertifikat je kolekcija informacija na koje je stavljen digitalni potpis izdavaoca, odnosno CA (Certificate Authority) koji garantuje njegovu verodostojnost. Funkcije koje vrši CA su:

- proveravanje identiteta korisnika,
- izdavanje digitalnih sertifikata i
- provera ispravnosti digitalnih sertifikata.

Slika 12. Digitalni sertifikat



56

Izvor: <http://www.slideshare.net>, pregledano 12.06.2016.

Tipičan digitalni sertifikat predstavlja skup informacija, koje su digitalno potpisale sertifikacione ustanove, kao što su npr. VeriSign, Cybertrust, Nortel, i enkriptovale RSA algoritmom.

Digitalni sertifikat sadrži:

- ime korisnika i druge identifikacione informacije, kao što je npr. e-mail adresa,
- ime izdavaoca sertifikata,
- digitalni potpis izdavaoca sertifikata,
- javni ključ vlasnika sertifikata koji može biti korišćen za proveru digitalnog potpisa pošiljaoca poruke,
- vremensko ograničenje za korišćenje sertifikata,
- klasu sertifikata, koja ukazuje na stepen izvršene provere korisnika, pri čemu viša klasa povlači i višu cenu za dobijanje sertifikata,
- identifikacioni broj sertifikata. (<http://www.bancaintesa.rs>, pregledano, 05.04.2016.)

Velika je verovatnoća da Web browser koji ima primalac poruke već sadrži javni ključ CA, jer su Netscape i Microsoft procenili kojim se CA može najviše verovati, pa su njihove javne ključeve uključili u svoje browsere. Da bi CA izdala digitalni sertifikat osobi ili entitetu koji ga zahteva neophodno je lično prisustvo i davanje na uvid identifikacionih dokumenata. Digitalni sertifikati mogu biti distribuirani i on-line zahvaljujući samozaštiti koju poseduju.

CA održavaju i obezbeđuju pristup listama za opoziv sertifikata CRL (Certificate Revocation List), na osnovu kojih se može videti koji su sertifikati validni. Na CRL se ne nalaze sertifikati kojima je istekao rok važnosti, jer svaki sertifikat ima ugrađeno vremensko ograničenje za korišćenje. Sertifikat može biti opozvan zbog gubitka, krađe ili npr. u slučaju kada zaposleni napusti firmu. Odluka o opozivu sertifikata odgovornost je ustanove koja ga je izdala. Zbog dodatne sigurnosti CA vrši autentifikaciju izvora koji je zatražio opoziv sertifikata.

5.1.1. Zaštita podataka u Banca Intesa a.d.

Banka je duboko privržena zaštiti i čuvanju tri bitne karakteristike informacije, poverljivosti, integriteta i dostupnosti. Kao bitan korak se nameće definisanje pravila koja bi odredila pristup zaposlenih svih resursima koji postoje implementirani u infrastrukturi

banke. Namera ovog uputstva je da utvrdi pravila pristupa kako mrežnim resursima, tako i resursima sa aspekta operativnog sistema, bez obzira da li se odnosi na pristup folderima i fajlovima na lokalnoj mašini ili se odnosi na pristup deljenim resursima na mreži. Pored toga deo uputstva se i bavi fizičkim aspektima bezbednosti i definiše ISMS zone i njihovo prostiranje i označavanje.

Svrha datog uputstva je da utvrdi, definiše i propiše kontrolu pristupa svim vrednostima koji postoje u Informacionom Sistemu, kako bi se obezbedio adekvatan nivo pristupa svim zaposlenima, a da pritom nema ugrožavanja njihove funkcije posla s jedne strane, a da se sa druge obezbedi i zadovolje svi bezbednosni aspekti. (<http://www.bancaintesa.rs>, pregledano, 05.04.2016.)

5.1.2. Pristup mrežnim resursima

Banka će za pristup mrežnim resursima koristiti sledeći postupak, koji će obezbediti adekvatan i ispravan pristup svim mrežnim uređajima i to ruterima, svičevima, i svim ostalim uređajima koji su prisutni u Informacionom Sistemu.

Postupak je sledeći:

- Pristup mrežnim uređajima je dozvoljen samo zaposlenima u Sistemsko tehničkom odeljenju i to sistem inženjerima, direktoru odeljenja, kao i menadžeru za bezbednost
- Pristup mrežnim uređajima je definisan shodno zahtevu direktoru Sistemsko tehničke podrške, a nakon odobravanja od strane Izvršnog direktora IT-a, dodeljuje se adekvatan pristup bilo novozaposlenom bilo zaposlenom nakon sticanja rešenja za stalno zaposlenje ili se pak vrši promena ovlašćenja
- Novozaposleni dobija na Cisco uređajima ovlašćenja najnižeg nivoa, koja mu zabranjuju bilo koje izvršne komande, a sa druge strane omogućavaju osnovno nadgledanje
- Zaposleni u Sistemskom odeljenju nakon sticanja statusa zaposlenog na neodređeno vreme i ukoliko njegov opis posla zahteva pristup mrežnim uređajima dobijaju potpun pristup uređajima

- Korisnička imena i lozinke se kontrolišu pomoću softvera za monitoring koji održavaju sistem inženjeri, pri čemu se treba pridržavati svih dobrih praksi za generisanje lozinki (<http://www.bancaintesa.rs>, pregledano, 05.04.2016.)

Sva aktivnost na uređajima se redovno proverava i prati, kako bi se utvrdili eventualni bezbedonosni prekršaji.

Slika 13. Zaštita podataka u banci



Izvor: <http://www.bancaintesa.rs> (pregledano, 05.04.2016.)

5.1.3. Pristup operativnom sistemu

Banka takođe uspostavlja posebnu kontrolu koja se odnosi na pristup korisnika folderima i fajlovima na operativnom sistemu, kao i svim ostalim bitnim resursima na operativnom sistemu.

Treba da bude primenjeno sledeće:

- Administrativnu funkciju (Administrators) nad operativnim sistemom obavljaju samo autorizovana lica koja brinu o funkcionalnosti operativnog sistema, data funkcija se uspostavlja činom zaposlenja i odgovarajućim opisom posla
- Grupi Administrators na operativnim sistemima pripadaju zaposleni u odeljenju za Sistemsko tehničke poslove i produkciju, pomenuta grupa ima nerestriktivan pristup folderima i fajlovima na operativnom sistemu
- Ostali zaposleni, nakon kreiranja korisničkog naloga i dodeljivanja lozinke od strane IT sektora, a u skladu sa opisom njihovog radnog mesta, na operativnim sistemima banke imaju restriktivan pristup (users), koji je izabran u skladu sa najboljom praksom proizvođača operativnog softvera
- Korisnici mogu imati više ovlašćenja nad operativnim sistemom ili pak odgovarajućim aplikacijama, ako to izričito zahteva svrha posla
- Sve aktivnosti nad operativnim sistemom se prate i kontrolišu, kako bi se uočili eventualni bezbednosni prekršaji. (<http://www.bancaintesa.rs>, pregledano, 05.04.2016.)

5.1.4. ISMS zone

U banci su prisutne četiri bezbednosne zone. Podela na bezbedonosne zone je izvršena da bi se jasno identifikovala oprema u skladu sa svojom poslovnom funkcionalnošću, i zaštita podataka i informacija. Zone su označene brojevima od 1-4, gde 1 predstavlja najniži nivo bezbednosti, a 4 veoma visok nivo bezbednosti i odgovarajućim bojama. Zone su obeležene nalepnicama u boji prema stepenu bezbednosti, postavljenim na vidnom mestu na ulazu u bezbedonosnu zonu. Pristup svim zonama ima Predsednik Banke, i članovi IO, zaposleni sa ovlašćenjem na ID kartici. Visoko poverljive informacije trebaju da budu enkriptovane korišćenjem ključeva i infrastrukture koja je prisutna u banci. Menadžment određuje potrebu za enkriptovanjem.

U slučaju prenosa informacija navedenim sredstvima komunikacije, onaj koji saopštava informacije treba uzeti u razmatranje kojoj kategoriji informacija pripada, tako javne i interne informacije se mogu saopštavati unutar interne mreže Banca Intese bez ikakvih posebnih predostrožnosti. Za osetljive i visoko osetljive informacije korišćenje lokalne

komunikacije je prijemčivo u slučaju kada ne postoji mogućnost fizičkog prisluškivanja ili nema mogućnosti da informacija dospe do osoba bez ovlašćenja “treba da zna”. Kako je prenos visoko osetljivih informacija nefrekventan i njih je dozvoljeno prenositi u okviru privatne mreže banke. Pored toga u zavisnosti od procene dozvoljeno je i prenositi informacije preko javne mreže.

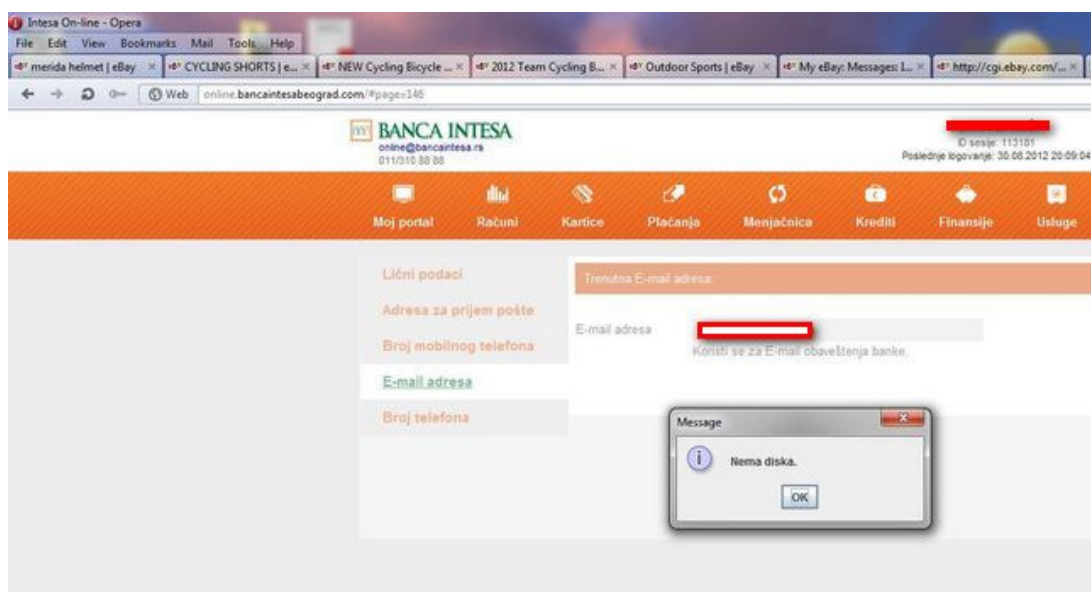
Javne informacije se mogu prenositi bez ikakvih kontrola u okviru linkova koje je Banka zakupila od treće strane. Pošto je saobraćaj poverljivih i visoko poverljivih informacija slučajan, tako da je mogućnost prisluškivanja mala, dozvoljeno je njihovo prenošenje unutar Banke.

5.2. Bezbednosne preporuke banke u vezi sa platnim karticama i bankomatima

Platne kartice su vremenom postale deo svakodnevnice svih poslovnih ljudi. Iz tog razloga banka posebnu pažnju posvećuje pitanjima bezbednosti korišćenja platnih kartica. Banka svojim klijentima na web sajtu skreće pažnju na važnost bezbednosti plaćanja platnim karticama, kroz objavljivanje preporuka kojih se klijenti moraju držati.

Da bi se podigao novac sa bankomata, prvo je potrebno ubaciti platnu karticu u bankomat. Posle toga bira se jezik i unosi se PIN broj kartice. Posle toga, izlaze uputstva na ekranu šta dalje raditi u vezi sa transakcijom. Kod bankomata Banca Intesa, transakcija se obavlja tako što se prvo isporuči novac, a tek posle toga platna kartica. Da bi se preuzeo novac, klijent ima na raspolaganju 30 sekundi. Ukoliko se u tom vremenskom periodu ne podigne novac, bankomat će zadržati karticu. Ako klijent dođe u ovu situaciju, potrebno je da se obrati zaposlenima u ekspozituri ili da pozove kontakt centar banke.

Slika 14. Bezbedonosne preporuke na sajtu banke



Izvor: <http://www.bancaintesa.rs> (pregledano, 05.04.2016.)

Zaključak

Na internetu se javlja poseban stepen identifikacije, od toga da ga održavaju sami trgovci, posebne podrške potrošačkim transakcijama, do njihovog uspostavljanja za zaposlene unutar preduzeća. Ti sistemi identifikacije nisu generalno interoperabilni, odnosno, informacije o identitetu koje su držane u jednom sistemu nisu generalno primenljive u drugom. Učiniti federalnim upravljanje adresama identiteta ishod je ove interoperabilnosti koja omogućava organizacijama da dele poverenje i identitet kroz granice koje ga dele. To dozvoljava ljudima da koriste isto korisničko ime (eng. user name), lozinku ili druge lične identifikacije, da bi se prijavili u više od jedne organizacije i da stvaraju transakcije, pojednostavljujući on-line događaj. Detalji i složenost svakog sistema identifikacije nevidljivi su za druge posredstvom standarda za izradu XML poruka. Pažljivo povezan predmet je autentičnost - to je proces koji dokazuje da je osoba ili drugi entitet stvarno taj ili ta za koju tvrdi da jeste.

Tokom sledećih pet godina videćemo ličnu autentičnost koja se prenosi od tradicionalnog passworda-lozinke ili PIN-a na mnoge druge opcije biometrije, kao što su glas, otisak prsta ili skeniranje retine (zenice), "u svoje vreme passworde" generisani od strane simbola hardvera, slično onim koji su probani od strane Lloyds TSB, i korišćenih od strane drugih personalnih jedinica, kartica i "dongles" kao dokaz identiteta. "Dva faktora autentičnosti" u kojima su dva po dva nezavisna znači da se zahteva da se dokaže identitet koji će postati norma. Mi ćemo takođe videti jedno povećanje korišćenja dva načina autentičnosti, gde vlasnici web sajta, kao što su banke, će imati dokaz njihove identifikacije za potrošače, isto toliko dobro kao drugi načini koji postoje okolo u okruženju.

Kriptografija, digitalni sertifikat i tehnike sa tim u vezi će biti korišćene mnogo šire, da bi se zaštitila poverljivost integriteta informacija i obezbedile pouzdane revizorske pretrage. Ovi postupci će takođe biti korišćeni da dozvole kompjuterima da jasno prave razliku između autentičnih i dubioznih softvera i stoga smanje pretnje od "loše robe". Razmnožavanje dokaza koji ne mogu pokvariti hardverske module uklopljene u kompjutere i druge jedinice će takođe moći tu da pomogne.

Poboljšanje metoda i alata korišćenih od strane ljudi koji razvijaju softver će smanjiti broj grešaka i drugih ranjivih situacija u operativnim sistemima i aplikacionim programima, iako će to da bude postepen proces. Ranjivost neće nikada da bude sasvim eliminisana, ali tehnike za detekciju i reagovanje na napade i druge probleme će postati mnogo više automatizovani i efikasniji. Jedna linija istraživanja inspirisana kroz imitaciju prirode pomaže da se načine IT da su samo odbranljive i samo popravljive.

Dok će tehnološki razvoj stalno povećavati bezbednost interneta, individualni korisnici mogu da urade mnogo više da sami zaštite svoje računare. Čineći tako, oni će takođe pomoći da internet bude mnogo sigurniji i za druge. Tehnologije i servisi koji su obezbeđeni teže da načine internet sigurnim mestom, ali bezbednost nije samo tehnološka odluka. Internet je neverovatan alat, ali bez pogodnih mera predostrožnosti, on izlaže potrošačke živote i identitet rizicima na isti način kao nezaključana vrata.

Literatura

1. Bjelica, M. (2013) *Telekomunikacione i računarske mreže*, Akademski misao, Beograd
2. Đorđević, B., Đorđević, M. (2010) *Zaštita podataka na 'intranetu' i 'ekstranetu' posredstvom digitalnog potpisa*, Bankarstvo, Beograd
3. Golden, B. (2013) *Amazon Web Services For Dummies*, Prentice Hall, New York
4. Ilić, O. (2015) *Računarski integrisana proizvodnja*, Fakultet organizacionih nauka, Beograd
5. Jovanović, N. (2011) *Računarske mreže : edukacioni sistem za računarske mreže zasnovan na web-u*, Viša poslovna škola, Beograd
6. Ljubičić, D., Franjić, A. (2012) *Računarske mreže*, Beogradska poslovna škola, Beograd
7. Mur-Malinos, Dž., Mazali, G. (2014) *Bezbednost na internetu*, Pčelica, Čačak
8. Obradović, S., Maček, N., Stanišević, I. (2010) *Računarske mreže*, Visoka poslovna škola strukovnih studija, Valjevo
9. Pokorni, S. (2015) *Računarske mreže*, Visoka škola strukovnih studija za informacione tehnologije, Beograd
10. Spasić, D. (2012) *Postnet računarska mreža i Internet servisi*, Zadužbina Andrejević, Beograd
11. Stojčev, M.K. (2012) *Računarske mreže i prenos podataka*, Elektronski fakultet, Niš
12. Šarkić, N., Prlja, D., Damjanović, K., Marić, V., Živković, V., Vodinelić, V., Mrvić-Petrović, N. (2011) *Pravo informacionih tehnologija*, Pravni fakultet Univerziteta Union, Beograd
13. Tanenbaum, E.S. (2013) *Računarske mreže*, Mikro knjiga, Beograd
14. Urošević, Z. (2012) *Računarske mreže i komunikacije*, Zavod za udžbenike, Beograd
15. Veinović, M., Jevremović, A. (2013) *Uvod u računarske mreže*, Univerzitet Singidunum, Beograd
16. Veinović, M., Adamović, S. (2012) *Kriptologija I: osnove za analizu i sintezu šifarskih sistema*, Univerzitet Singidsunum, Beograd
17. Žorić, A. (2012) *Integrisani računarski sistemi*, Fakultet tehničkih nauka, Kosovska Mitrovica

Internet izvori:

<http://www.visa.ca>, pregledano 07.04.2016.
internetsecurity101.net, pregledano 08.04.2016.
<http://www.howtogeek.com>, pregledano 10.04.2016.
<http://www.bancaintesa.rs> (pregledano, 05.04.2016.)
<http://www.slideshare.net>, pregledano 12.06.2016.
<http://www.slideshare.net>, pregledano 12.06.2016.
<http://www.go4it.ro>, pregledano 15.06.2016.
<http://www.avesina.org>, pregledano 15.06.2016.
<http://www.avesina.org>, pregledano 15.06.2016.
<http://www.security.stackexchange.com>, pregledano, 17.06.2016.
[http:// www.blog.comodo.com](http://www.blog.comodo.com), pregledano 18.06.2016.
[http:// www.alienvault.com](http://www.alienvault.com), pregledano 10.06.2016.
www.emailquestions.com, pregledano 08.06.2016.