



UNIVERZITET SINGIDUNUM
DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE
-MASTER STUDIJSKI PROGRAM-
SAVREMENE INFORMACIONE TEHNOLOGIJE

Bojan Ikić

**Organizacija zaštite
savremenih informacionih sistema**

- Master rad -

Mentor:
Prof dr Mladen Veinović

Student:
Bojan Ikić
Br. indeksa: 410088/2009

Organizacija zaštite savremenih informacionih sistema

Sažetak

U ovom radu opisana je organizacija zaštite informacionih sistema. Organizacija zaštite ima svoje osobenosti koje se odnose na preuzimanje odgovornosti za specijalizovane programe što će kroz ovaj rad detaljno biti objašnjeno. Organizacija zaštite opisana je kroz njenu primenu u virtualnim privatnim mrežama.

Virtualna privatna mreža engleski Virtual Private Networking (VPN), obezbeđuje mehanizme za bezbednu komunikaciju i prenos podataka i drugih informacija kroz javnu mrežu kao što je Internet, a takođe predstavlja i jeftinu alternativu za iznajmljene telekomunikacione linije između kompanija i njihovih udaljenih organizacionih jedinica. Pored velikog broja pogodnosti koje pruža, VPN omogućava zaposlenima da mogu sa bilo koje tačke na svetu da bezbedno pristupaju podacima na kompanijskim serverima na isti način kao što to čine iz svoje kancelarije.

Ključne reči: Organizacija zaštite, bezbednost informacija, VPN, IPsec, SSL VPN, kontrola pristupa, namenski uređaji, PKI

Abstract

This paper describes the Management of information security. Because information security management is charged with taking responsibility for a specialized program, certain characteristics of its management are unique to this community of interest. Management of information security is described thru the Virtual Private Networks.

Virtual Private Network provides mechanisms for safe communication and transfer of data and other information through public network, like Internet, and it also represents cheap alternative for rented telecommunication lines between companies and their remote organizational units. Among various privileges it provides, VPN gives possibilities to its employees to safely access from any spot in the world to data within company servers at the same way as they do that from their offices.

Key words: Security management , information security, VPN, IPsec, SSL VPN, access control, appliance, PKI

SADRŽAJ

Uvod.....	5
1. Metodologija istraživačkog projekta.....	7
1.1. Uvodne napomene i obrazloženje rada.....	7
1.2. Predmet istraživanja	7
1.3. Ciljevi i zadaci istraživanja	8
1.4. Istraživačke hipoteze.....	9
1.5. Metodi istraživanja i tok istraživačkog procesa	10
2. Savremeno poslovanje i informacioni sistemi	12
2.1. Korisnici.....	12
2.2. Prevencija neautorizovanog prisupa	12
2.3. Dostupnost podataka.....	13
2.4. Backup i export podataka	13
3. Organizacija i upravljanje zaštitom	14
3.1. Bezbednost informacija.....	14
3.2. Istorijat	15
3.3. Osnovni principi	16
3.3.1. Poverljivost	17
3.3.2. Integritet	17
3.3.3. Dostupnost	17
3.3.4. Autentičnost	18
3.3.5. Neporicanje.....	18
3.4. Principi organizacije zaštite informacionih sistema.....	18
3.4.1. Planiranje (Planning)	19
3.4.2. Polise (Policy).....	19
3.4.3. Programi (Programs)	21
3.4.4. Zaštita (Protection).....	22
3.4.5. Ljudi (People)	23
3.4.6. Project Management.....	24
4. Računarske mreže.....	25
4.1. OSI model	25
4.1.1. Sloj aplikacije.....	27
4.1.2. Sloj prezentacije.....	27
4.1.3. Sloj sesije.....	28
4.1.4. Sloj transporta	28
4.1.5. Sloj mreže.....	29
4.1.6. Sloje veze.....	29
4.1.7. Fizički sloj	29
4.2. IPsec bezbednosni protokol.....	29
4.2.1. Tunelovanje	30
4.2.2. Transportni mod.....	30
4.2.3. Tunelski mod	31
4.3. SSL protokol za zaštitu virtualne privatne mreže.....	31
4.3.1. SSL rekord protokol (SSL Record Protocol).....	32
4.3.2. Protokol za uspostavljanje sigurne veze (Handshake Protocol)	32
4.3.3. Protokol za promenu ključa (Change Cipher Spec).....	33
4.3.4. Protokol za upozorenja (Alert messages).....	33
5. Organizacija savremenih računarskih mreža.....	34

5.1. Lokalna mrežna infrastruktura	34
5.1.1. Nova organizacija lokalne mreže	35
5.2. Virtualne privatne mreže	37
5.2.1. LAN-to-LAN virtualne privatne mreže	38
5.2.2. Remote access virtualne privatne mreže.....	38
6. Mrežna infrastruktura izmeštena kod provajdera	40
6.1. Namenski serveri	41
6.2. Cloud computing	41
6.3. Prednosti hostinga na namenskim ili Cloud serverima.....	42
7. Upravljanje digitalnim identitetom	44
7.1. Socijalni inženjering	45
7.2. Autentifikacija	46
7.3. Projektovanje PKI infrastrukture	47
8. Bezbedna komunikacija	50
8.1. SSL VPN uređaj	51
8.1.1. SSL portal VPN	53
8.1.2. SSL tunnel VPN	53
9. Zaštita kao servis.....	55
9.1. Osnovne karakteristike	55
9.2. Zaštita na serverskoj strani.....	56
9.3. Zaštita na klijentskoj strani	57
10. Zaštita udaljenih servisa	59
10.1. Poslovni informacioni sistem.....	59
10.2. Edukacija	60
10.3. Document Management System.....	60
10.4. Dodatna zaštita	61
Zaključak	63
Literatura	65

Uvod

Kada se govori o zaštiti informacionih sistema pre svega se misli na hardverske uređaje ili softverska rešenja koja se koriste za zaštitu. Takođe, sve češće se nude usluge koje proveravaju ranjivost Web sajtova, Web aplikacija pa i same lokalne mreže. Bezbednost informacionih sistema predstavlja međutim nešto više od puke komercijalizacije kada su u pitanju hardverska i softverska rešenja odnosno senzacionalizma kada je reč o opasnostima koja vrebaju preko Interneta. Takođe niko od njih bilo da je reč o kompaniji ili stručnom konsultantu ne sagledava bezbednost informacionog sistema kao celovit proces već svako smatra da je za zaštitu dovoljan samo segment kojim se on bavi.

Ovaj rad će se baviti organizacijom zaštite koja podrazumeva sagledavanje konkretnih potreba kompanije, definisanje bezbednosnih politika i procedura, kreiranje polisa, ljudske resurse i naravno konkretna hardverska i softverska rešenja. Kao što je već rečeno na tržištu usluga u oblasti zaštite informacionih sistema trenutno su dominantne kompanije koje se bave samo jednim aspektom bezbednosti i koje često nude svoje proizvode ne obraćajući pažnju na realne potrebe klijenta. Tu su takođe i pojedinci koji obično rade kao konsultanti za zaštitu u velikim kompanijama ili bankama koji zbog prirode svog posla sagledavaju celovitost zaštite ali nude rešenja koja se primenjuju u velikim sistemima što za manje kompanije predstavlja problem jer su njihovi budžeti za zaštitu informacionih sistema obično minimalni.

Što se tiče ljudskih resursa, primetno je da se kompanije sve više odlučuju za smanjenje broja zaposlenih IT stručnjaka. U zavisnosti od broja zaposlenih u kompanijama ostaju samo IT menadžeri koji treba da koordiniraju rad IT sektora sa outsourcing kompanijama. Takođe, sve je popularnije radno mesto IT menadžera za bezbednost koje zahteva specifične obuke i sertifikate o čemu će u ovom radu takođe biti reči.

Za sada na tržištu usluga bezbednosti informacionih sistema ne postoje specijalizovane kompanije koje bi se bavile isključivo organizacijom zaštite. Ove kompanije bi trebalo da budu u stanju da pre svega objektivno sagledaju potrebe kupaca kao i da mu pomognu u izboru neophodne opreme i ostalog što je kupcu neophodno za kvalitetnu zaštitu. Pored toga, one bi pružale usluge izrade bezbednosnih politika i procedura kao i pisanje polisa. Održavanje sistema zaštite kao i edukacija takođe bi mogli da bude u nadležnosti ovih kompanija.

Organizacija zaštite prikazana je kroz virtualne privatne mreže koje savremene kompanije sve više koriste da bi unapredile svoje poslovanje. Virtualna privatna mreža (Virtual Private Network – VPN) je privatna komunikaciona mreža koja se koristi za komunikaciju u okviru javne mreže. Transport VPN paketa podataka odvija se preko javne mreže (npr. Internet) korišćenjem standardnih komunikacionih protokola. VPN omogućava korisnicima na razdvojenim lokacijama da preko javne mreže jednostavno održavaju zaštićenu komunikaciju.

Brzina kojom se razvija Internet kao i globalizacija poslovanja dovela je do neophodnosti pristupa informacijama koje se nalaze u kompaniji sa bilo kog mesta u svetu i u bilo koje doba dana ili noći nezavisno od vremenske zone. Moderno poslovanje prepoznaje novu kategoriju zaposlenih engl. teleworker, koji proizvode ili usluge svoje kompanije nude širom sveta. Da bi bili konkurentni, oni do važne informacije moraju da dođu brzo i lako. Današnji širokopojasni Internet to omogućava ali potrebno je i resurse jedne kompanije, a tu se pre svega misli na virtualne privatne mreže prilagoditi modernim trendovima poslovanja.

Zbog ovakvog načina pristupa poverljivim informacijama neke kompanije mora se ozbiljno voditi računa o zaštiti. Ovde će se govoriti o nekoliko aspekata zaštite, a pre svega o fizičkoj i kriptološkoj organizaciji zaštite virtualne privatne mreže.

Fizička zaštita se odnosi na organizaciju hardverskih resursa u virtualnoj privatnoj mreži. Predložena su rešenja za smeštanje i održavanje serverskih kapaciteta i ona se kreću u dijapazonu od sopstvenog hostinga pa sve do cloud computinga.

Kriptozaštita¹ pored kriptanalize čini jednu od dve osnovne oblasti kriptologije. Kriptozaštita je posebna delatnost vojnih, državnih (diplomatskih, bezbednosnih, ekonomskih) i drugih organa i organizacija u cilju obezbeđenja zaštite tajnosti poruka pri prenošenju kanalima veze. Kriptozaštita obuhvata:

- naučnoistraživački rad za pronalaženje kriptoloških postupaka i sredstava
- organizaciju kriptozaštite
- primenu kriptozaštite u praksi

U ovom radu naglasak će pre svega biti na organizaciji i primeni kriptozaštite u virtualnim privatnim mrežama što podrazumeva sledeće:

- Definisanje elemenata kriptozaštite koji su neophodni
- Nabavka neophodnih elemenata kriptozaštite
- Implementacija rešenja
- Obuka korisnika
- Održavanje

Za obavljanje poslova kriptozaštite se, načelno, formiraju posebni stručni organi. Zbog značaja koji imaju, sve delatnosti kriptozaštite se svrstavaju u red vrhunskih tajni i obavezno se uređuju zakonima.

¹ Vojna enciklopedija, drugo izdanje, knjiga 4, strana 714. Vojnoizdavački zavod Beograd, 1972.

1. Metodologija istraživačkog projekta

1.1. Uvodne napomene i obrazloženje rada

Projektni zadatak ima za cilj da definiše pojam organizacije zaštite koja podrazumeva sagledavanje konkretnih potreba kompanije, definisanje bezbednosnih politika i procedura, kreiranje bezbednosnih polisa, ljudske resurse zadužene za bezbednost i naravno konkretna hardverska i softverska rešenja.

U ovom radu se pre svega sagledava odnos između savremenih poslovnih tendencija i informacionih sistema koji treba da funkcionišu u novom okruženju. Takođe detaljno je opisana struktura upravljanja zaštitom koju čine: planiranje, polise, programi, zaštita, ljudski resursi i project menadžment. Kroz opis organizacije savremene lokalne mreže prikazana su neka praktična rešenja kao i pregled troškova za implementaciju tih rešenja. Mrežna infrastruktura izmeštena kod provajdera prikazuje prednosti koje se dobijaju korišćenjem namenskih servera i Cloud computing-a korišćenjem pre svega usluge koja se zove Software as a Service. Neophodno je bilo naglasiti i potrebu za novim vidom kompanija koje bi bile specijalizovane za projektovanje organizacije zaštite informacionih sistema, njenu implementaciju i održavanje.

Kao što je već rečeno organizacija zaštite prikazana je kroz virtualne privatne mreže odnosno kroz arhitekturu, protokole i bezbednosne aspekte vezane za ovu vrstu mreža. Rad se pored organizacionih bavi i tehničkim aspektima virtualnih privatnih mreža. Prikazana su tehnološka rešenja koja su trenutno aktuelna ali i ona koja će u bliskoj budućnosti biti preovlađujuća. Takođe, treba reći da je težište rada uglavnom okrenuto na bezbednost, a manje na potencijalne pretnje.

Ovaj rad je nastao korišćenjem teoretskih i praktičnih znanja iz domena upravljanja zaštitom informacionih sistema, računarskih mreža kao i hardverskih i softverskih rešenja koja se koriste za zaštitu.

1.2. Predmet istraživanja

Predmet istraživanja je bio usmeren na više segmenata s obzirom da se radi u kompleksnoj i sveobuhvatnoj materiji što organizacija zaštite svakako jeste. Iako je kao literatura za ovu oblast korišćena knjiga koja predstavlja Bibliju kada je reč o upravljanju zaštitom, nije se išlo samo na puko prevođenje već na komentare pre svega o tome koliko se u pojedinim segmentima stiglo kod nas. Takođe u poglavlju o upravljanju zaštitom govori se i o edukaciji IT stručnjaka koji se bave zaštitom informacionih sistema kao i edukacijom zaposlenih primereno njihovim potrebama. Evo nekih pitanja na koje su se tržili odgovori prilikom istraživanja:

- Visina budžeta koji je korisnik spreman da izdvoji za zaštitu
- Prepoznavanje stvarnih potreba korisnika
- Definisane bezbednosnih politika i procedura prilagođenih korisniku
- Predlog obuke IT menadžera i zaposlenih u kompaniji

Pored upravljanja zaštitom čija struktura je detaljno opisna na početku rada najveći deo istraživanja bio je usmeren na pronalaženje optimalnih tehnoloških rešenja koja predstavljaju okosnicu čitavog sistema zaštite. Rešenja su prikazana kroz konkretne predloge kao što su na primer: nova organizacija savremenih lokalnih mreža, izmeštanje mrežne infrastrukture na namenske ili cloud servere, neophodnost stvaranja kompanija koje bi bile security provajderi. Ova tehnološka rešenja posmatrana su kroz prizmu višenamenskih uređaja za zaštitu koji se sve više koriste zbog svojih performansi, jednostavnog rukovanja i sve pristupačnije cene. Kao praktična rešenja nisu prikazivane tehničke karakteristike pojedinih uređaja već njihova optimalna primena u organizacionoj strukturi. Nije reč samo o SSL VPN uređajima koji predstavljaju nezaobilazan činilac zaštite u savremenim informacionim sistemima već je reč i o drugim specijalizovanim uređajima koji pokrivaju ostale segmente bezbednosti kao što je na primer antivirusna zaštita. Projektni rad se nije bavio tehničkim karakteristikama svakog pojedinačnog uređaja već se težilo tome da se pronađu odgovori na pitanja koja su interesantna samom korisniku kao što su na primer:

- Izbor hardverskih uređaja i softverskih rešenja shodno potrebama korisnika
- Izbor funkcionalnosti hardverskih uređaja koje su korisniku zaista neophodne

Pored istraživanja koje se odnosilo na sam pojam zaštite informacionih sistema, predmet istraživanja su takođe bile virtualne privatne mreže odnosno organizacioni aspekti zaštite u njima. Pored poglavlja koje se odnosi na klasične virtualne privatne mreže zasnovane na IPsec protokolu, veći deo istraživanja posvećen je SSL VPN tehnologiji. Za obe vrste mreža prikazani su prednosti i nedostaci kao i mogućnosti njihovog kombinovanja kako bi se od svake izvukle najbolje performanse, a smanjio uticaj slabosti koju svaka od njih poseduje. Može se sa sigurnošću reći da izbor protokola i tehnologija za razvoj virtualne privatne mreže zavisi pre svega od organizacionih potreba kompanije, a takođe i od finansijskih sredstava sa kojima kompanija raspolaže. Evo nekih pitanja na koje su se tržili odgovori prilikom istraživanja:

- Kako rade virtualne privatne mreže i kako mogu da se implementiraju u postojeću mrežnu infrastrukturu kompanije
- Planiranje implementacije virtualne privatne mreže u poslovanje kompanije
- Evaluacija benefita koje organizacija dobija uvođenjem virtualne privatne mreže
- Razumevanje onoga što treba tražiti od kompanije koja prodaje rešenje
- Skretanje pažnje korisnicima na bezbednosne aspekte virtualne privatne mreže
- Strategija kontrole pristupa aplikacijama koje se nalaze u virtualnoj privatnoj mreži
- Ukazivanje na važeće trendove u ovoj oblasti kao i na razvoj virtualnih privatnih mreža u budućnosti

1.3. Ciljevi i zadaci istraživanja

Ovaj rad je namenjen pre svega profesionalcima koji vode računa o bezbednosti informacionih sistema, kao i IT menadžerima koji treba da osmisle organizaciju zaštite informacionog sistema u svojoj kompaniji. Pored dobrog poznavanja računarskih mreža IT menadžeri bi trebalo da se edukuju i u oblasti upravljanja zaštitom odnosno u oblasti Security menadžmenta o čemu će detaljno biti reči u ovom radu. U radu će biti navedeni i neki od konkretnih problema do kojih se došlo prilikom istraživanja, a sa kojima će se to je sasvim sigurno susresti kompanije koje budu želele da zaštite svoj informacioni sistem.

Cilj istraživanja bio da se kompanije koje prodaju računarsku opremu za zaštitu i koji su ujedno i sistem integratori nekih sigurnosnih rešenja potaknu na razmišljanje da postanu

security provajderi odnosno kompanije koje nude security kao servis za veliki broj malih korisnika. Gotovo je nemoguće zamisliti da svaka od njih može da kreira sopstveni sistem za bezbednost pre svega zbog ograničenih finansijskih sredstava pa je ovakva inicijativa više nego korisna. Na ovaj način bi i kompanije koje deo svog poslovanja obavljaju preko Interneta, a koje nemaju velike budžete mogle sebi da priušte zaštitu pod povoljnim uslovima. Najvažnije je istaći da je ovakva inicijativa realno izvodljiva i da ne zahteva prevelika finansijska ulaganja.

Iako je u to teško poverovati prodavci iz pojedinih kompanija, iako tehnički obrazovani pokazuju određene slabosti prilikom procene potreba kompanije koja kupuje neko IT rešenje. Najčešće se dešava da prodavci nude tehnologije i gotova rešenja koja su već razvili za neke druge potrebe. U jednom konkretnom slučaju, nudili su kao rešenje Kerberos protokol za autentifikaciju iako to ni na koji način nije odgovaralo stvarnim potrebama organizacije gde je sistem za zaštitu trebalo da bude uveden. Prioritet prodavaca što je donekle i opravdano je na prodaji proizvoda ili rešenja bez preteranog udublivanja kako će se to rešenje uklopiti u realne potrebe kompanije. Uloga IT menadžera je da prepozna realne potrebe svoje kompanije i ukaže prodavcu na njih. Ovaj profil zaposlenih treba da poseduje širok spektar znanja iz raznih oblasti informacionih tehnologija jer kompanije, često i one veće nisu spremne da dobro plate više stručnjaka u ovoj oblasti.

1.4. Istraživačke hipoteze

Opšta hipoteza

Težište istraživanja je bilo na tome da se pokaže da na tržištu usluga u domenu informatičke bezbednosti ne postoje kompanije koje sagledavaju zaštitu kao sveobuhvatan problem već to čine parcijalno favorizujući one segmenti kojima se oni bave kao što su na primer kriptografija, komercijalna hardverska rešenja ili softver koji se koristi za zaštitu. Sledeći problem je taj što su neka rešenja iako na izgled sveobuhvatna bila vezana za jednu platformu odnosno konkretno na Windows. Kompanije koja nude ovakva rešenja imaju zaposlene inženjere koji su bez daljnijeg veoma stručni u svom poslu i veoma dobro poznaju Microsoft tehnologiju vezanu za zaštitu. Oni međutim nisu spremni na kompromisna rešenja odnosno rešenja u kojima neki od servisa nije nužno podignut na Windows platformi. Takav način razmišljanja predstavlja ozbiljno ograničenje za ove kompanije pre svega zbog činjenice da se Cloud computing razvija velikom brzinom i da se sve manje vodi računa o tome na kojoj se platformi radi. Pored ovih postoje i kompanije koje problem zaštite posmatraju pojednostavljeno odnosno pre svega kroz prizmu opasnosti koje vrebaju preko Interneta nudeći pri tom usluge penetration testova kojima proveravaju ranjivost Web aplikacija ili računarskih mreža. Da ne bude zabune, pronalaženje nedostataka u nekom informacionom sistemu je bitan segment zaštite ali ove kompanije se uglavnom zadržavaju na tome. Ukoliko neka od njih čak i ponudi neko rešenje ono je neprecizno i nedefinisano i nikada se unapred ne zna koliko će da košta. Uglavnom se ide na to da se korisnik zbuni i zastraši da bi uslugu oporavka i kasnijeg održavanja platio više nego što je neophodno.

U početku je težište istraživanja bilo na klasičnim virtualnim privatnim mrežama u kojima se međusobno povezuje više udaljenih lokacija jedne kompanije. Tokom istraživanja pokazalo se da kompanije sve više imaju potrebu za povezivanjem svojih zaposlenih koji se u određenom trenutku nalaze ili na putu ili pristupaju resursima od svojih kuća. Klasičan način VPN umrežavanja ovde se pokazao kao loš iz više razloga.

Najvažnija zamerka su komplikovana instalacija i održavanje programa koji se instaliraju na klijentskim računarima i služe za komunikaciju sa VPN koncentratorima na serverskoj strani. Ovi programi se nazivaju VPN klijenti. Veliki problemi sa VPN klijentima je to što su oni veoma osetljivi na promene parametra odnosno dodatna podešavanja bilo na VPN koncentratoru ili na njima samima. Ovi problemi uočeni su čak i kod rešenja kompanije Cisco inače lidera u ovoj oblasti.

Drugi problem, tiče se direktno bezbednosti. VPN klijenti imaju problem da se povežu sa digitalnim sertifikatima i tokom istraživanja nije pronađeno rešenje za koje pouzdano može da se kaže da neće praviti problem prilikom povezivanja VPN klijenta i digitalnog sertifikata. Digitalni sertifikati imaju odlične bezbednosne karakteristike i zato je trebalo pronaći rešenje gde će to biti iskorišćeno u punoj meri.

Radna hipoteza

Istraživanje je dovelo do zaključka da je na tržištu usluga iz oblasti zaštite informacionih sistema neophodno stvoriti kompanije koje će biti specijalizovane isključivo za poslove organizacije i implementacije rešenja iz ove oblasti. Ovakva usluga koja bi mogla da se zove security kao servis bi bila nezavisna kako od operativnog sistema tako i od drugih servisa sa kojima kompanija radi. Glavna prednost security servisa je u tome što on ne mora da se hostuje kod istog provajdera kao i ostali servisi neke kompanije. Ovo je veoma važno zbog sve bržeg razvoja virtualizacije i Cloud computing-a. Zbog svoje osetljivosti ovi servisi bi trebalo da budu konfigurisani kroz High Availability cluster odnosno da stalno budu dostupni korisnicima čak i u slučaju otkazivanja jednog od uređaja. Takođe security provajderi bi kroz security servise nudili usluge definisanja bezbednosnih politika i procedura, pisanje polisa kao i obuku IT menadžera i ostalog informatičkog kadra zaposlenog u kompaniji.

VPN tehnologija koja nudi prevazilaženje ovih problema zove SSL VPN, a podržavaju je najveće svetske kompanije koje rade u ovoj oblasti kao što su Cisco, SonicWall ili Baracuda Networks. U osnovi ova tehnologija nudi pristup resursima kompanije preko bilo kog poznatijeg Web pretraživača, tako da se problem sa VPN klijentima veoma jednostavno prevazilazi. Što se tiče digitalnih sertifikata, o tome takođe vodi računa Web pretraživač, a podešavanje je lako čak i za korisnike koji su početnici.

Takođe u radu je detaljno opisana organizacija kontrole pristupa resursima virtualne privatne mreže. Ovo je najosetljiviji deo VPN mreže i mnogi napadi zlonamernih korisnika usmereni su baš na to mesto. Razmotrena su hardverska i softverska rešenja za zaštitu kontrole pristupa uz pomoć SSL VPN tehnologije, kao što su SSL VPN gateway i smart kartice ili tokeni sa digitalnim sertifikatima za autentifikaciju.

1.5. Metodi istraživanja i tok istraživačkog procesa

Metodologija istraživanja svela se na korišćenje pre svega Interneta ali i na korišćenje ozbiljnih kljiga koje se bave oblastima organizacije zaštite i virtualnih privatnih mreža. Takođe informacije su dobijene i od eminentnih kompanija u ovoj oblasti, a koje u našoj zemlji imaju svoja predstavništva kao što su Cisco, SonicWall, Citrix ili Stonesoft, kao i pojedinaca koji su priznati eksperti u ovoj oblasti.

Na Internetu, a i u literaturi uopšte mnogo je manje informacija koje se tiču upravljanja zaštitom nego informacija o tehnologijama koje se za to koriste. Zbog toga je istraživanje bilo teže i kompleksnije ali i mnogo interesantnije. Svaka od informacija koja se nalazi u ovom

radu proverena je obavezno na više mesta u literaturi da bi se dokazalo da je relevantna. Takođe informacije o ovoj oblasti teško su dostupne i trebalo je puno truda da se pronađu ljudi koji o organizaciji zaštite imaju znanje i iskustvo. U radu se nalaze stavovi i razmišljanja koja na potpuno nov način govore o nekim već poznatim pojmovima, tehnologijama ili daju kritički osvrt na njih. Ovakvi stavovi pozivaju na otvorenu polemiku koja bi pomogla još bolju implementaciju ovog rada u praksi. Ideja je da ovaj rad pomogne IT menadžerima, kao i drugim stručnjacima iz domena informacionih tehnologija da dobiju jasniju sliku o ovoj oblasti kao i da im se ukaže gde mogu da pronađu dodatne informacije koje su im potrebne. Neka praktična rešenja prikazana u ovom radu svako će im biti od koristi prilikom uvođenja zaštite informacionih sistema u njihovim organizacijama.

2. Savremeno poslovanje i informacioni sistemi

Sve veći broj kompanija nudi svoje usluge kao Cloud – based servise. Bilo da se radi o Web aplikacijama u koje spadaju poslovne aplikacije, Document Management System ili aplikacije za e-learning sve one se nude kao servis na udaljenim serverima kojima korisnici mogu da pristupe sa bilo kog mesta. Za pristup ovakvim aplikacijama veoma je važna bezbednost zato što se celokupna komunikacija obavlja preko Interneta.

2.1. Korisnici

Kao što je već rečeno ovaj rad treba da posluži projektantima Web aplikacija, security provajderima kao i IT menadžerima koji treba da uvedu zaštitu informacionih sistema u manje kompanije ili organizacije bilo da su sami u njima zaposleni ili da to rade u outsourcing-u. Najteža stvar koju treba da urade jeste da ubede vlasnike ili druga odgovorna lica u menadžmentu kompanije da bezbednost podataka ne zavisi od lokacije na kojoj se oni čuvaju. Ovaj fenomen naročito je izražen u manjim kompanijama u kojima obično njihovi vlasnici žele da server na kome drže podatke imaju u svom vidokrugu naivno verujući da su na taj način osigurani od bilo kakve zloupotrebe. U ovom radu će biti detaljnije objašnjene tehnologije bezbedne komunikacije koje bi trebalo da pomognu da odgovorni menadžeri u kompanijama steknu neophodno poverenje u savremene informatičke koncepte. Suština bezbednosti podataka sažeta je u pitanjima koja će korisnici svakako postaviti. Svaki korisnik pitaće sledeće:

- Da li neautorizovani korisnici mogu da vide moje podatke?
- Da li su podaci dostupni uvek kada su mi potrebni?
- Da li mogu da uradim backup svojih podataka?

Ukoliko uspešno može da odgovori na ove postavljene zahteve smatra se da provajder Web aplikacije zajedno sa security provajderom može da obezbedi potrebne uslove za udaljeni pristup podacima.

2.2. Prevencija neautorizovanog pristupa

Zaštita podataka od neautorizovanog pristupa² je najvažnija stvar koju security provajder treba da obezbedi svojim korisnicima. Takođe korisnici koji iznajmljuju takvu vrstu usluge trebalo bi da se informišu o tehnologiji koju provajder koristi kada nudi ovakvu vrstu usluge.

1. Java EE – Aplikacije razvijene u Javi imaju dobru reputaciju kada se radi o bezbednosti. Za razliku od drugih tehnologija za razvoj Web aplikacija kao što je na primer PHP, Java poseduje veliku biblioteku funkcija koje se mogu iskoristiti za pisanje stabilnog i bezbednog koda.
2. SSL je tehnologija koja obezbeđuje šifrovanu komunikaciju između korisnikovog Web pretraživača i Web aplikacije koja se nalazi na serveru. Korišćenje digitalnih sertifikata kao dodatnog vida zaštite u SSL komunikaciji hakerima oduzima bukvalno

² Clarity accounting, Security bookkeeping, <https://www.clarityaccounting.com/help/index.php/tag/security/>

bilo kakvu mogućnost da izvrše upad u komunikacioni kanal i tako dođu do poverljivih informacija.

3. Security skeneri koji nadgledaju Web aplikacije koje kompanija koristi i preko kojih ima pristup do svojih podataka.
4. Web aplikacije koje rade sa poverljivim podacima moraju da se čuvaju ili na posebnim namenskim serverima ili u cloud-u, a nikako na deljenim serverima ili na namenskom serveru na kome provajder Web aplikacije hostuje nebezbedne sadržaje kao što su Web sajt, blog ili forum.
5. Firewall koji sprečava upade hakera na servere na kojima se nalaze podaci i Web aplikacije.

2.3. Dostupnost podataka

Ono što korisnike takođe veoma zanima jeste i dostupnost njihovih podataka. Dostupnost podataka mogu da im obezbede specijalizovani provajderi preko data centara i grid tehnologije.

1. Data centri – provajderi osetljivih Web aplikacija treba da poseduju data centre koji zadovoljavaju visoke security standarde, a takođe da imaju i neophodne sertifikate kao što je na primer SAS70. Ovakvi data centri imaju video nadzor, redundantno napajanje, redundantne internet konekcije, redundantne ruter, a ulazak u njih obezbeđen je najčešće biometrijskom autentifikacijom. Praktično je nemoguće da ovakve uslove korisnik obezbedi čak i u svojoj sopstvenoj kompaniji.
2. Grid tehnologija podrazumeva da je Web aplikacija distribuirana na više servera što u slučaju otkaza jednog od njih omogućava da aplikacija bude i dalje dostupna za korisnika, a da on ne primeti da je do otkaza došlo.

2.4. Backup i export podataka

Potrebno je da provajder obezbedi redovan backup podataka. Treba takođe razmotriti mogućnost exportovanja podataka na Windows ili NAS server koji se nalazi kod korisnika. Ovo je važno zbog nepouzdanosti Internet konekcija u našoj zemlji.

Prevenција neautorizovanog pristupa je jedna od najvažnijih stvar koju treba obezbediti da bi se korisnici uverili da su njihovi podaci u cloud-u sigurni. Izbor tehnologija koje su ovde nabrojane predstavlja nezaobilazan zahtev za bezbedno poslovanje.

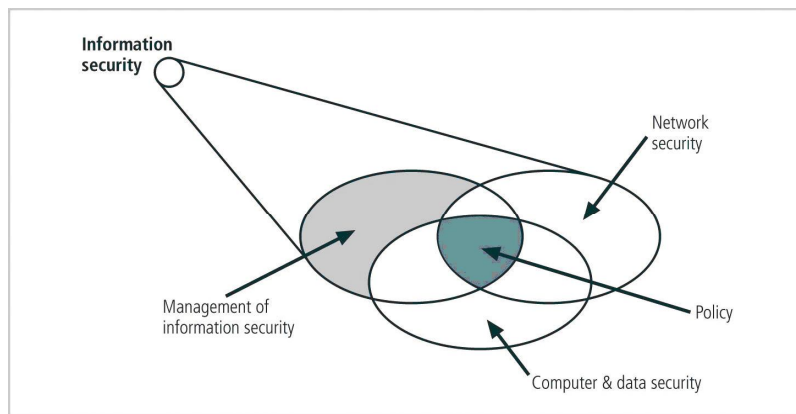
3. Organizacija i upravljanje zaštitom

3.1. Bezbednost informacija

Razumevanje tehničkih aspekata bezbednosti informacija zahteva poznavanje definicija određenih termina i koncepata u oblasti informacionih tehnologija. Uopšteno, bezbednost se definiše kao “kvalitet ili stanje bezbednosti, odnosno biti bezbedan znači ne biti u opasnosti”³. Bezbednost se često postiže putem nekoliko strategija koje se obično preduzimaju istovremeno ili se koriste u kombinaciji jedna sa drugom. Bezbednost takođe podrazumeva i čitav niz specijalizovanih oblasti o kojima će u ovom radu takođe biti reči. Specijalizovane oblasti bezbednosti su sledeće:

- Fizička bezbednost koja podrazumeva zaštitu ljudi, fizičkih aktiva, radnog okruženja od neželjenih događaja kao što su vatra, neautorizovan pristup podacima ili prirodne katastrofe
- Lična bezbednost koja se poklapa sa fizičkom bezbednošću u zaštiti zaposlenih unutar organizacije
- Operaciona bezbednost koja je fokusirana na sposobnost organizacije da bude u stanju da vodi računa o tome da ne dolazi do prekida ili kompromitovanja njenog poslovanja
- Bezbednost komunikacije koja obuhvata zaštitu medijuma, tehnologije i sadržaja koji učestvuju u procesu komunikacije i mogućnost da se ti alati koriste za pristup ciljevima organizacije
- Mrežna bezbednost koja se odnosi na zaštitu mrežnih uređaja unutar organizacije, bezbednu konekciju kao i mogućnost da se mreža koristi za proveru komunikacionih funkcija

Informatička bezbednost uključuje širok spektar aktivnosti iz oblasti informatičke bezbednosti što podrazumeva pored ostalog bezbednost računara, bezbednost podataka kao i bezbednost mreže. U srcu informatičke bezbednosti nalazi se koncept polisa. Polise, osvešćivanje, edukacija i tehnologija su vitalni koncepti zaštite informacija kao i zaštite celokupnog informacionog sistema.



Slika 1 Komponente informatičke bezbednosti

³ Michael E. Whitman and Herbert J. Mattord, Management of Information Security, Course Technology, 2008.

Bezbednost informacija predstavlja zaštitu informacija i informacionih sistema od neautorizovanog pristupa, korišćenja, razotkrivanja, remećenja, izmene ili uništenja. Termini, koji su predmet ovog rada kao što su: bezbednost informacija, računarska bezbednost i osiguranje informacija često se mešaju iako se u suštini radi o različitim stvarima. Ove oblasti su međusobno povezane i imaju sličnu namenu. Iako je za ove oblasti zajedničko to da definišu načine na koji se štiti poverljivost, integritet i dostupnost informacija kao i drugi aspekti bezbednosti među njima postoje i ozbiljne razlike.

Ove razlike leže pre svega u pristupu subjektu, metodologiji korišćenja i temama koje pokrivaju. Bezbednost informacija je povezana sa pojmovima kao što su poverljivost integritet i dostupnost podataka bez obzira na formu u kojoj se ti podaci nalaze: elektronska, štampana ili neka druga forma dok je računarska bezbednost fokusirana na osiguravanje dostupnosti i ispravno funkcionisanje računarskog sistema bez osvrta na informacije koje se skladište ili obrađuju na računaru.

Vlade, vojska, korporacije, finansijske institucije, bolnice i privatni biznis poseduju veliku količinu poverljivih informacija o svojim zaposlenima, kupcima, proizvodima, istraživanjima i finansijskoj situaciji. Veliki broj ovih informacija se sada uz pomoć računara prikupljaju, obrađuju i skladište a zatim se tako pripremljeni šalju preko mreže prema drugim računarima.

Ukoliko poverljive informacije o kupcima, finansijama ili liniji novih proizvoda padnu u ruke konkurenciji zbog probijanja bezbednosnih mera to bi moglo da dovede do propasti posla, sudskog postupka ili čak i stečaja kompanije. Zaštita poverljivih informacija je na prvom mestu poslovna ali takođe i etička kao i pravna stvar. Za pojedinca, bezbednost informacija može da ima bitne posledice na privatnost na koju se veoma različito gleda u različitim kulturama.

Oblast bezbednosti informacija značajno je rasla i razvijala se u novije vreme. Ova oblast takođe pruža niz mogućnosti za razvoj uspešne karijere, jer zahteva razne vrste specijalizacija. Specijalnosti kao što su obezbeđivanje mreže odnosno mreža i sličnih infrastruktura, obezbeđivanje aplikacija i baza podataka, testiranje bezbednosti, revizija informacionih sistema, digitalna forenzika samo su neka od zanimanja koja se mogu sresti u ovoj oblasti.

3.2. Istorijat

Još od najranijih dana korišćenja pisma državne vođe i vojni komandanti razumeli su neophodnost pronalaženja nekih od mehanizama za zaštitu poverljivosti pisanih dokumenata i sposobnost otkrivanja sertifikata. Osobe koje su želele bezbednu komunikaciju koristili su pečat od voska i druge načine pečačenja da potvrde autentičnost dokumenta, spreče falsifikovanje i obezbede poverljivost korespondencije. Julije Cezar je stekao ugled sa izumom "Cezarove šifre" 50-te godine p.n.e. koja je stvorena sa ciljem da predupredi da njegove tajne poruke budu pročitane ukoliko dospeju u pogrešne ruke.

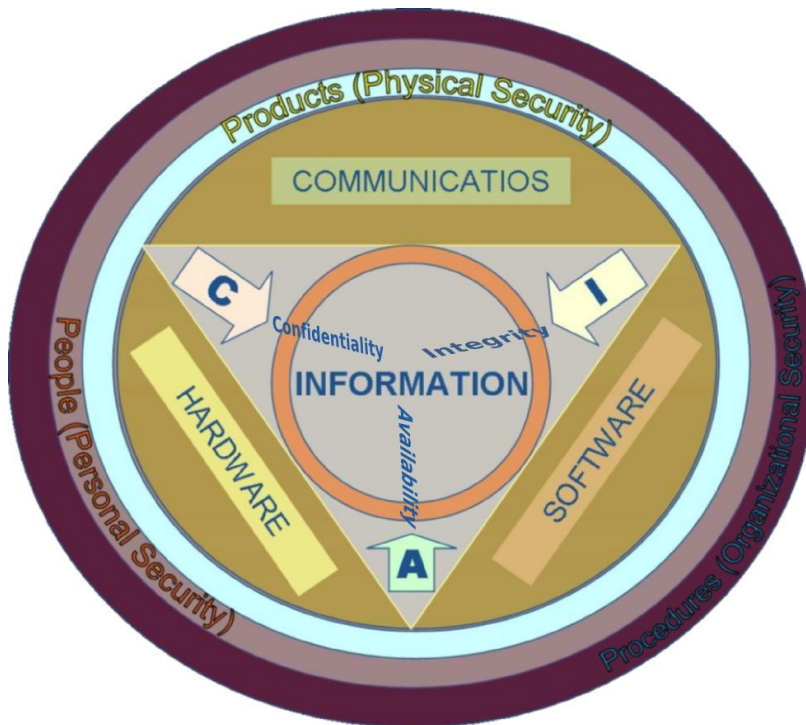
Drugi svetski rat je doneo mnoge novine u oblasti bezbednosti informacija i označio je početak profesionalnog bavljenja ovom oblašću. Uočene su prednosti fizičke zaštite informacija sa barikadama i naoružanim stražama koje kontrolišu pristup u informatičke centre. Takođe je uvedena klasifikacija podataka bazirana na njihovoj osetljivosti kao i identifikacija osoba koje mogu da pristupe informaciji. Tokom Drugog svetskog rata takođe se sprovodila provera porekla pre dobijanja prava na klasifikovanje informacija.

Kraj 20-og i početak 21-og veka povezan je sa brzim razvojem telekomunikacija, računarskog hardvera i softvera i šifrovanjem podataka. Manje, snažnije i dostupnije računarske komponente učinile su elektronsku obradu podataka bližom malim i srednjim preduzećima kao i kućnim korisnicima. Ubrzo su ovi računari postali povezani unutar mreže koja se naziva Internet ili World Wide Web.

Brz porast i široka upotreba elektronske obrade podataka i elektronskog poslovanja koje se sprovodi preko Interneta, među sve brojnijim pojavama međunarodnog terorizma, zahteva bolje metode zaštite računara i informacija koje su na njima uskladištene, obrađene i prosledene. Akademske discipline računarske bezbednosti, bezbednosti informacija i informatička sigurnost izdvajaju se među brojnim profesionalnim organizacijama koje dele isti cilj obezbeđivanja sigurnosti i pouzdanosti informacionih sistema.

3.3. Osnovni principi

Bezbednost informacija održava poverljivost, integritet i dostupnost poznatiju kao CIA trojstvo (confidentiality, integrity and availability)⁴, kao svoje osnovne principe. Informacione sisteme možemo da raščlanimo na tri osnovna dela hardver, softver i komunikacije sa ciljem da identifikujemo i primenimo industrijske standarde za bezbednost informacija kao mehanizme za zaštitu i prevenciju u tri sloja i to: fizički sloj, personalni sloj i organizacioni sloj. Ukratko, procedure i politike su implementirane da objasne zaposlenima (administratorima, korisnicima i operaterima) kako da koriste proizvode da bi obezbedili sigurnost informacija unutar organizacije.



Slika 2 Komponente koje obezbeđuju bezbednosti informacija

⁴ Wikipedia, Information Security, http://en.wikipedia.org/wiki/Information_security

3.3.1. Poverljivost

Poverljivost podrazumeva sprečavanje razotkrivanja informacija neautorizovanom pojedincu ili sistemima. Na primer transakcije kreditnim karticama preko Interneta zahtevaju da kupac svoj broj kreditne kartice treba da prezentuje trgovcu, nakon čega trgovac prenosi broj kreditne kartice banci koja će da izvrši autorizaciju. Poverljivost se štiti enkripcijom broja kreditne kartice tokom prenosa, ograničavanjem broja mesta gde može da se pojavi (baze podataka log fajlovi, backup, štampani izveštaji i slično), kao i ograničavanjem pristupa mestima gde se skladište. Ako neko ko nije autorizovan dobije broj kreditne kartice, na bilo koji način, dolazi do narušavanja poverljivosti.

Narušavanje poverljivosti se može realizovati na više načina. Dopustivši nekome pogled preko ramena na monitor vašeg računara dok su na njemu prikazane osetljive informacije predstavlja narušavanje poverljivosti. Krađe ili prodaja laptopa koji sadrži poverljive podatke o zaposlenima iz kompanije može rezultirati narušavanjem poverljivosti. Izdavanje poverljivih informacija putem telefona je takođe narušavanje poverljivosti ukoliko poziv dolazi od osobe koja nije autorizovana da primi te informacije. Poverljivost je neophodna za očuvanje privatnosti osoba čiji se lični podaci čuvaju na sistemu.

3.3.2. Integritet

U okviru bezbednosti informacija, integritet podrazumeva da se podaci ne mogu menjati bez procesa autorizacije, što ne treba mešati sa referencijalnim integritetom kod baza podataka. Integritet je narušen kada zaposleni nenamerno ili zlonamerno izbriše važne podatke, kada virus inficira računar, kada je zaposleni u mogućnosti da menja sopstvenu zaradu u bazi podataka platnih spiskova, kada neautorizovani korisnik uništi Web sajt, kada neko može da odbaci veliki broj glasova prilikom online glasanja i tako dalje.

Postoji mnogo načina u kojima je integritet ugrožen bez zle namere. Najjednostavniji primer je kada korisnik prilikom unosa podataka nepravilno unese nečiju adresu. Nešto kompleksniji je slučaj kada automatizovani proces nije pravilno napisan i testiran, pa proces ažuriranja baze podataka može da izmeni podatke na neodgovarajući način ugrožavajući time integritet podataka. Profesoinalci koji se bave ovom oblašću pokušavaju da pronađu načine za implementaciju kontrola koje će predupređiti ugrožavanje integriteta.

3.3.3. Dostupnost

U svakom informacionom sistemu informacija mora da bude dostupna kada se za njom ukaže potreba. To zapravo znači da računarski sistemi skladište i obrađuju podatke, bezbednosni sistemi ih štite, a funkcionalni komunikacioni kanali omogućavaju pristup. Visoko dostupni sistemi imaju za cilj da budu dostupni sve vreme sprečavajući prekid usluge koju računar pruža čak i u slučaju gubitka napajanja, kvara na hardveru ili nadogradnje sistema. Osiguranje dostupnosti takođe uključuje sprečavanje denial-of-service napada.

2002. godine Donn Parker predlaže alternativni model za klasično CIA trojstvo koji je nazvao "Šest atomskih elemenata informacija". Ovi elementi su poverljivost, posedovanje, integritet, autentičnost, dostupnost i upotrebljivost. Vrednost Parkerove heksade je predmet rasprave među profesionalcima koji se bave bezbednošću sistema.

3.3.4. Autentičnost

U računarstvu, e-poslovanju i bezbednosti informacija neophodno je da se obezbedi da podaci, transakcije, komunikacije ili dokumenti (elektronski ili materijalni) ostanu izvorni. Za autentičnost je takođe važna validacija koja omogućava da obe uključene strane treba da dokažu da su ono što tvrde da jesu.

3.3.5. Neporicanje

U pravnim naukama, neporicanje povlači nečiju nameru da izvrši svoju obavezu prema ugovoru. To takođe implicira da jedna strana u transakciji ne može da porekne prijem transakcije niti druga strana može da porekne slanje transakcije. Elektronska trgovina koristi tehnologiju digitalnog potpisa i šifrovane komunikacije kojima postiže autentičnost i neporicanje.

3.4. Principi organizacije zaštite informacionih sistema

Dobra organizacija zaštite informacionih sistema zasniva se na dobrom upravljanju zaštitom (Security management). Upravljanje ili menadžment predstavlja proces u kome se dolazi do nekog cilja korišćenjem određenog skupa resursa⁵. Da bi proces informatičke bezbednosti postao efikasniji, neophodno je da se dobro razumeju osnovni principi upravljanja. Rukovodilac ili menadžer je neko ko radi sa ili preko drugih zaposlenih u organizaciji koordinirajući njihove radne aktivnosti u cilju postizanja što boljih rezultata organizacije. On ima mnoštvo uloga u organizaciji uključujući i sledeće:

- Uloga informisanja podrazumeva prikupljanje, obradu i korišćenje informacija koje mogu da ugroze ispunjenje planiranog cilja
- Interpersonalna uloga podrazumeva interakciju sa nadređenima, potčinjenima, spoljnim saradnicima i drugim činiocima koji su uključeni u izvršenje nekog zadatka
- Uloga u odlučivanju podrazumeva odabir između alternativnih pristupa, kao i razrešavanje konflikata, dilema ili izazova

Organizacija zaštite koja se kao što je rečeno zasniva na kvalitetnom upravljanju zaštitom podrazumeva neke od sledećih aktivnosti:

- Definisanje procesa zaštite
- Definisanje politika, standarda procedura i uputstava
- Upravljanje rizicima
- Kontrole
- Tehnologije
- Dokumentaciju
- IT kulturu
- Edukaciju

Zbog činjenice da je upravljanje zaštitom opterećeno preuzimanjem odgovornosti za specijalizovane programe određeni aspekti ove vrste menadžmenta imaju svoje osobenosti. Glavne karakteristike po kojima se odlikuje informatička bezbednost su poznate kao šest P.

- Planiranje (Planning)
- Polise (Policy)
- Programi (Programs)
- Zaštita (Protection)

⁵ Michael E. Whitman and Herbert J. Mattord, Management of Information Security, Course Technology, 2008.

- Ljudi (People)
- Upravljanje projektom (Project Management)

3.4.1. Planiranje (Planning)

Aktivnosti koje su uključene u model planiranja informatičke bezbednosti neophodne su da bi se obezbedio dizajn, kreiranje i implementacija strategije informatičke bezbednosti kao deo planiranja celokupnog informacionog sistema. Postoji nekoliko načina na koji se može planirati informatička bezbednost:

- Planiranje odgovora na incident
- Planiranje nastavka poslovnog procesa
- Planiranje oporavka od incidenta
- Planiranje polisa
- Planiranje kadrova
- Planiranje risk menadžmenta
- Planiranje bezbednosnih programa koji uključuju edukaciju, trening i osveščivanje zaposlenih

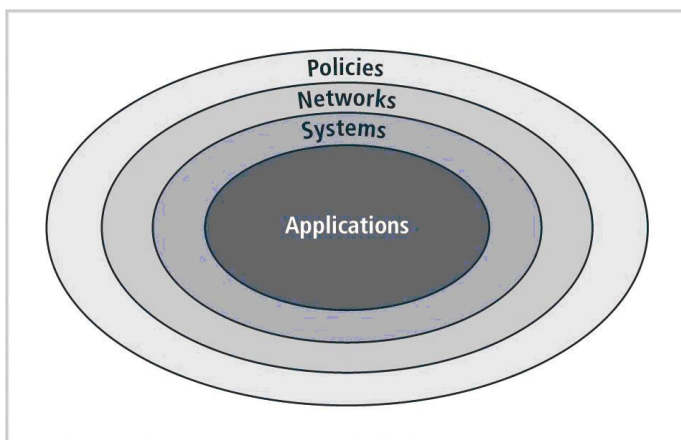
3.4.2. Polise (Policy)

Skup organizacionih uputstava koja zahtevaju odgovorno ponašanje zaposlenih u nekoj organizaciji nazivaju se polise. U informatičkoj bezbednosti postoje tri kategorije polisa:

- generalne polise (polise na nivou preduzeća)
- polise koje se odnose na specifična probleme
- polise koje se odnose na specifične sisteme

U ovom poglavlju biće detaljnije objašnjeno šta su polise, ko ih kreira, ko ih implementira i ko ih održava. Polise su osnova efikasnog programa informatičke bezbednosti. Uspeh zaštite informatičkih resursa zavisi od generisanih polisa kao i od stava rukovodstva koje definiše stepen sigurnosti informacija u automatizovanim sistemima.

Sve polise moraju da budu u službi napretka organizacije u kojoj su primenjene. Rukovodstvo kompanije mora da obzbedi adekvatnu podelu odgovornosti za pravilnu upotrebu informacionog sistema. Krajnji korisnici bi svakako trebalo da budu uključeni u onim procesima koji se odnose na formulisanje polisa. Na sledećoj slici prikazano je mesto polisa u odnosu na druge aspekte bezbednosti u nekoj organizaciji uz pomoć Bulls-eye Model-a.



Slika 3 The Bull's-Eye Model

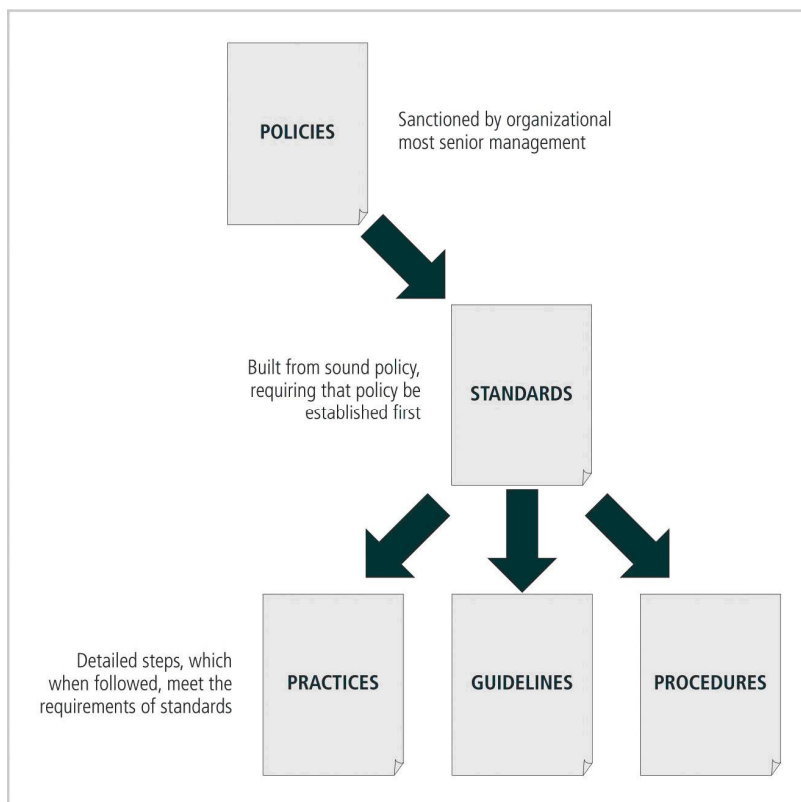
Kreatori polisa moraju konstatno da ističu kolika je važnost sigurnosti informacija unutar njihove organizacije. Njihova primarna odgovornost je da uspostave polise za korišćenje informatičkih resursa unutar organizacije sa ciljem smanjenja rizika što je povezano sa zakonskom regulativom kao i sa obezbeđivanjem kontinuiteta poslovnih procesa, integriteta i tajnosti podataka.

Kvalitet programa informatičke bezbednosti počinje i završava se polisama. Pravilno definisane i implementirane polise omogućavaju programu informatičke bezbednosti da funkcioniše skoro savršeno. Mada se čini da je polise lako primeniti u praksi često dolazi do problema prilikom implementacije. Da bi se ovo izbeglo moraju se poštovati neka pravila prilikom njihovog kreiranja:

- Polise nikada ne smeju da budu u suprotosti sa zakonom
- Polise moraju da budu održive u sudskom procesu ukoliko do njega dođe
- Polise moraju da budu podržane i administrirane na pravi način

Polise su važna referentna dokumenta za unutrašnju organizaciju i pokazuju nameru rukovodstva da želi da uvede red u oblast bezbednosti informacionih sistema u svojoj kompaniji. Iako savršeno napisana ova dokumenta mogu da budu potpuno beskorisna ukoliko nema bezrezervne podrške rukovodstva kompanije.

Pored polisa za organizaciju zaštite informacionog sistema veoma su bitna i dokumenta kao što su standardi i prakse. Sledeća slika prikazuje hijerarhijsku strukturu u kojoj treba da budu polise, standardi i prakse u nekoj organizaciji da bi zaštita koju ova dokumenta opisuju bila što efikasnija.



Slika 4 Polise, standardi, praksa

- Polise predstavljaju plan ili pravac delovanja sa ciljem da se utiče na određene odluke, akcije kao i ostale bitne aktivnosti u okviru organizacije
- Standardi su dokumenti koji detaljnije opisuju aktivnosti koje treba preduzeti u skladu sa onim što je definisano u polisama
- Prakse, procedure i uputstva objašnjavaju zaposlenima na koji način treba da se pridržavaju važećih polisa

3.4.3. Programi (Programs)

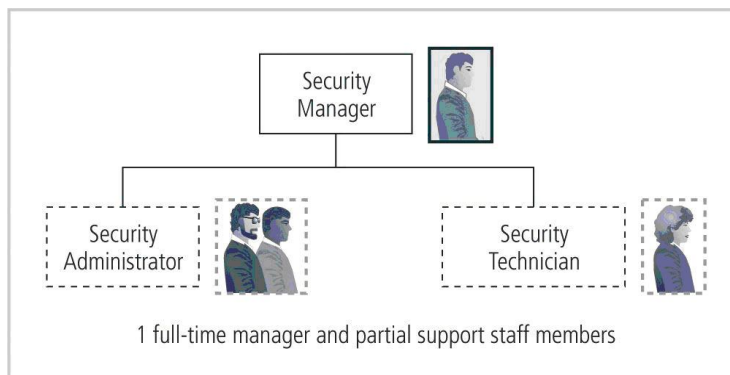
Programi podrazumevaju definisanje naziva i opis radnih mesta zaposlenih koji se bave poslovima zaštite u nekoj organizaciji. Nazivi kao i opisi radnih mesta se donekle razlikuju sa originalnom literaturom koja je korišćena u izradi ovog rada pre svega zbog lakšeg razumevanja i prilagođavanja domaćim potrebama. Da bi se zaštita informacionog sistema u nekoj kompaniji kreirala na pravi način neophodno je da se urade sledeći poslovi:

- Planiranje sigurnosnih rešenja
- Projektovanje, izrada i implementacija sigurnosnih rešenja
- Upravljanje sigurnosnim alatima, praćenje bezbednosnih funkcija i kontinuirano poboljšanje procesa

Što se tiče naziva radnih mesta zaposlenih koji se bave zaštitom oni mogu biti različiti u zavisnosti od kompanije. Međutim, s obzirom da je u ovom radu akcenat dat na organizaciju zaštite u manjim kompanijama neki od originalnih naziva iz literature kod njih jednostavno nisu primenljivi. Najveći broj poslova vezanih za zaštitu informacionih sistema može da se podvede pod neki od sledećih naziva:

- IT menadžer za bezbednost
- Administrator i analitičar za bezbednost
- Tehničar za bezbednost
- Konsultant za bezbednost
- Istražitelj za bezbednost

Nemaju sve kompanije mogućnost da otvore radna mesta za navedene profile. Ovakva radna mesta mogu da se nađu u kompanijama koje su usko specijalizovane za pružanje usluga iz oblasti zaštite. U manjim kompanijama gde je neretko zaposlen samo jedan čovek kao IT menadžer ovakve vrste poslova se realizuju angažovanjem stručnog saradnika najčešće preko projekta sa ograničenim vremenom trajanja ili na neki drugi način kao što je to prikazano i na narednoj slici.



Slika 5 Opisi poslova zaposlenih koji se bave zaštitom

Security provajderi bi trebalo permanentno da vrše edukaciju, organizuju treninge i podižu nivo svesti o neophodnosti zaštite informacionih sistema kako svojih zaposlenih tako i zaposlenih u kompanijama kojima pružaju usluge zaštite. Najbolji način da to urade jeste kroz Security Education Training Awareness (SETA) program koji je preporučen i u literaturi.

3.4.4. Zaštita (Protection)

Funkcije zaštite se odvijaju kroz dva odvojena procesa od kojih će jedan detaljnije biti objašnjen u ovom poglavlju, a drugi se odnosi na ceo rad. Procesi kroz koje se odvijaju funkcije zaštite su:

- Risk menadžment koji uključuje procenu i kontrolu rizika
- Mehanizmi za zaštitu, tehnologije i alati

Upravljanje rizicima je proces procene rizika za informacioni sistem neke organizacije i određivanje strategije kako da ti rizici budu kontrolisani i smanjeni. Upravljanje rizicima je jedna od ključnih odgovornosti svakog menadžera unutar bilo koje organizacije. Upravljanje rizicima podrazumeva sledeće procese:

- Identifikaciju i procenu rizika
- Kontrolu rizika

Poznavanje sopstvenih kapaciteta podrazumeva da menadžeri treba da budu u stanju da razumeju šta su to informacije i na koji način se obrađuju, skladište i prenose. Ukoliko poseduju neophodno znanje o tome oni mogu da iniciraju detaljan program upravljanja rizikom. Poznavanje potencijalnog neprijatelja takođe je važan deo procene rizika koji podrazumeva identifikovanje, kontrolu i razumevanje pretnji sa kojima se suočava informacioni sistem neke organizacije. Svaka organizacija mora da izabere jednu od ove četiri osnovne strategije za kontrolu rizika:

- Prevencija rizika
- Premeštanje rizika
- Ublažavanje rizika
- Prihvatanje rizika

Prevencija podrazumeva strategiju kontrole rizika kojom organizacija pokušava da spreči da neko iskoristi ranjivost njenog informacionog sistema. Prevencija se može prikazati kroz sledeće aktivnosti:

- Primena polisa
- Treninzi i edukacija
- Suprostanavljanje pretnjama
- Implementacija tehničkih kontrola za zaštitu

Premeštanje rizika je strategija kojom se pokušava da se rizik preusmeri na druge procese ili u druge organizacije. Ovo se može postići outsourcing uslugama, uzimanjem osiguranja ili sprovođenjem ugovora o uslugama sa provajderima.

Ublažavanje je strategija koja pokušava da smanji, putem planiranja i pripreme, štetu koja može da nastane usled ranjivosti informacionog sistema neke organizacije. Ovaj pristup koji se još naziva i Contingency planning (CP) sastoji se od tri osnovna plana:

- Disaster recovery plan (DRP)
- Incident response plan (IRP)
- Business continuity plan (BCP)

Prihvatanje rizika je izbor da se ne učini ništa za zaštitu informacionog sistema i da se prihvati ishod eventualnog ugrožavanja sistema. Ova strategija odnosno odsustvo kontrole, pretpostavlja da je to možda mudra poslovna odluka jer se ispitivanjem alternativnih rešenja došlo do zaključka da cena zaštite imovine ne opravdava troškove bezbednosti.

Za svaki pomenuti rizik izvršni menadžment može da prihvati rizik rukovodeći se relativno niskom vrednošću imovine, relativno malom učestalošću pojavljivanja, i relativno malom uticaju na poslovanje, a takođe može da ublaži rizik birajući i implementirajući odgovarajuće kontrolne mere. U nekim slučajevima rizik može da bude prebačen i u drugu kompaniju kupovinom osiguranja ili davanjem outsourcing usluga. Realnost pojedinih rizika može da bude diskutabilna. U takvim slučajevima rukovodstvo kompanije može da zanemari rizik, što predstavlja potencijalni rizik.

3.4.5. Ljudi (People)

Postoje razni sertifikati koji se dobijaju u oblasti zaštite ali kod nas za najbolje od njih još uvek ne postoji mogućnost obuke i polaganja ispita. Ovi kursevi zahtevaju ne samo poznavanje bezbednosnih tehnika već i široko znanje pre svega iz oblasti računarskih mreža. Dobro poznavanje računarskih mreža kao i kontrole pristupa kao jednog od njenih najvažnijih delova važno je zbog činjenice da danas verovatno ne postoji ozbiljnija kompanija koja ne koristi srazmerno svojoj veličini neki vid umrežavanja bilo da se radi o lokalnoj mreži, ili mrežnoj infrastrukturi koja se nalazi na nameskim ili cloud serverima. Evo nekih od najpoznatijih sertifikata iz oblasti računarske bezbednosti:

- CISSP
- SSCP
- GIAC
- SCP
- ICSA
- Security +
- CISM

Mnoge kompanije nude sertifikate za oblast informatičke bezbednosti ali je najpoznatija od njih svakako International Information Systems Security Certification Consortium (ISC)² koja je svakako svetski lider u edukaciji iz ove oblasti. Da se radi o ozbiljnim sertifikatima dokazuje i činjenica da za njihov najpoznatiji sertifikat koji se zove Certified Information Systems Security Professional (CISSP) može da polaže samo onaj koji ima najmanje pet godina radnog iskustva u oblasti informatičke bezbednosti. Kandidat koji želi da polaže za CISSP sertifikat mora da ima širok spektar znanja iz različitih oblasti kao što su:

- Information Security and Risk Management
- Access Control
- Security Architecture and Design
- Physical and Environmental Security
- Telecommunications and Network Security
- Cryptography
- Business Continuity and Disaster Recovery
- Legal, Regulations, Compliance, and Investigations
- Application Security
- Operations Security

Kompanija (ISC)² nudi i dodatno usavršavanje za pojedine oblasti posle dobijanja CISSP sertifikata. Evo oblasti u kojima mogu da se dobiju dodatni sertifikati:

- Architecture (CISSP-ISSAP)
- Engineering (CISSP-ISSEP)
- Management (CISSP-ISSMP)

3.4.6. Project Management

Ova komponenta koja predstavlja temeljne discipline projektnog menadžmenta odnosi se na sve elemente programa informatičke bezbednosti i veoma je važna za praćenje procesa prilikom uvođenja sistema bezbednosti u neku organizaciju. Ovaj proces podrazumeva identifikovanje i kontrolisanje sredstava koja se primenjuju na projektu, kao i merenje napretka projekta i prilagođavanje procesa kako bi se ostvario napredak u ispunjavanju cilja.

4. Računarske mreže

Funkcionisanje savremenih informacionih sistema nezamislivo je bez korišćenja računarskih mreža. Ovdje će pre svega biti reči o mrežama unutar kompanija koje one koriste da bi lakše pristupali deljenim resursima bilo da su u pitanju fajlovi ili baze podataka. Takođe biće reči i o OSI modelu kao i o zaštiti odnosno o protokolima koji se koriste da bi se obezbedila bezbedna komunikacija unutar mreže.

Konfigurisanje i administracija računarskih mreža je kompleksan posao koji zahteva stručnost kao i stalno usavršavanje i praćenje novih dostignuća u ovoj oblasti. Stručnjaci iz ove oblasti su veoma cenjeni i lako mogu da nađu dobro plaćen posao pre svega u velikim sistemima kao što su banke ili telekomunikacione kompanije. Dobro poznavanje mrežne opreme može da pomogne u optimizovanju računarske mreže što se pre svega odnosi na nabavku samo one opreme koja je korisniku zaista neophodna da bi njegova računarska mreža mogla nesmetano da funkcioniše. Savremene kompanije bez obzira na njihovu veličinu ili finansijska sredstva sa kojima raspolazu najčešće koriste dve vrste mreža i to:

- Lokalna računarska mreža (LAN)
- Virtualna privatna mreža (VPN)

Lokalna računarska mreža ili LAN (engl. Local Area Network - LAN) je skup računara koji su povezani u jednu računarsku mrežu, na relativno malom prostoru, kao što su kancelarija, više kancelarija ili zgrada. Ova mreža može da broji dva i više računara koji su povezani na određen način. Neki periferni uređaji kao što su štampači, modemi i sl., takođe se ubrajaju u ovu mrežu. Glavna karakteristika lokalnih mreža, po čemu se one razlikuju od mreža na velikim područjima (WAN) jeste mnogo veća brzina prenosa podataka (reda 10 do 1000 MB/sec) i nepostojanje potrebe za zakupljenim telekomunikacionim vodovima. Najčešći metod povezivanja računara u lokalnoj mreži jeste kablovima (Ethernet) ili bežična mreža. Lokalna mreža može, najčešće preko nekog rutera, biti povezana sa drugim mrežama u veću WAN mrežu ili direktno preko provajdera na Internet.

Virtualna privatna mreža engleski Virtual Private Networking (VPN), obezbeđuje mehanizme za bezbednu komunikaciju i prenos podataka i drugih informacija kroz javnu mrežu kao što je Internet, a takođe predstavlja i jeftinu alternativu za iznajmljene telekomunikacione linije između kompanija i njihovih udaljenih organizacionih jedinica. Pored velikog broja pogodnosti koje pruža, VPN omogućava zaposlenima da mogu sa bilo koje tačke na svetu da bezbedno pristupaju podacima na kompanijskim serverima na isti način kao što to čine iz svoje kancelarije.

4.1. OSI model

Krajem 1970-tih godina, Međunarodna organizacija za standardizaciju (Internacional Organization for Standardization, ISO), je kreirala referentni model, Open System Interconnection (OSI)⁶ da bi računari različitih proizvođača mogli da komuniciraju. OSI model je bio namenjen da pomogne proizvođačima u kreiranju kompatibilnih mrežnih uređaja i softvera u formi protokola. OSI model opisuje kako jedna aplikacija na jednom računaru, kroz mrežni medijum, saopštava podatke i mrežne informacije aplikaciji na drugom

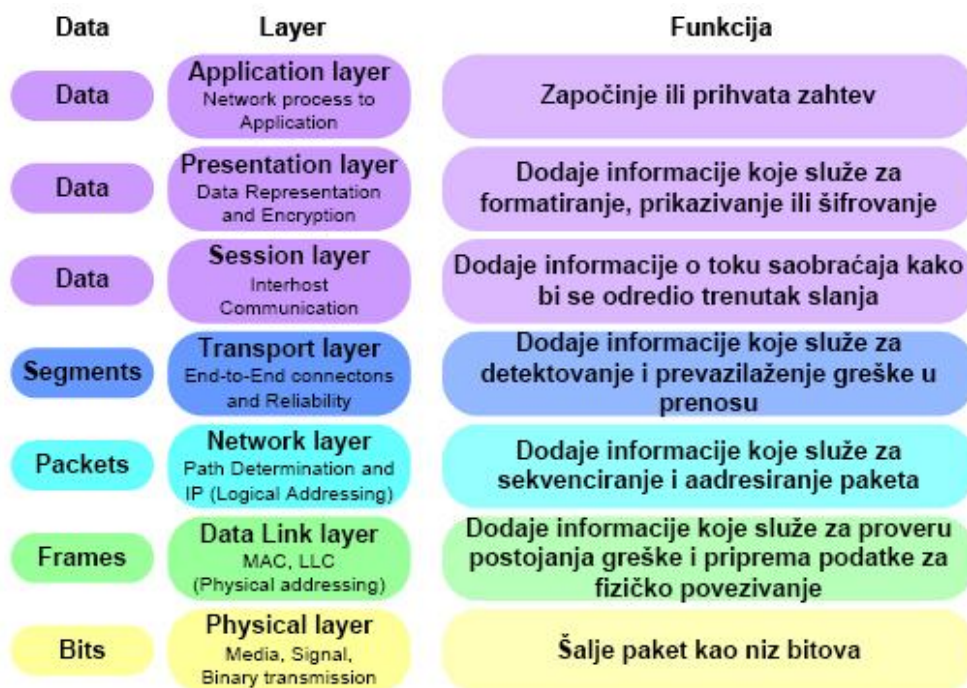
⁶ Wikipedia, OSI model, <http://sr.wikipedia.org/wiki>

računaru. Referentni model predstavlja sve procese potrebne za uspešnu komunikaciju i deli sve procese u logičke grupe – slojeve. Ovako dizajniran model se naziva slojevita arhitektura. OSI model je hijerarhijski model i treba da omogući mrežama različitih proizvođača da rade zajedno. Prednosti korišćenja OSI slojevitog modela su:

- Deli komunikacione procese u mreži na manje i jednostavne komponente
- Omogućava višeproizvođački razvoj kroz standardizaciju mrežnih komponenti
- Omogućava različitim vrstama mrežnog hardvera i softvera da rade zajedno
- Sprečava da izmene na jednom sloju utiču na druge slojeve, tako da se ne ometa razvoj

OSI model se sastoji od 7 odvojenih, ali međusobno povezanih slojeva kroz koje moraju da prođu podaci na svom putu od izvoršta preko mreže do odredišta. Čine ga sledeći slojevi:

7. sloj – sloj aplikacije (application layer)
6. sloj – sloj prezentacije (presentation layer)
5. sloj – sloj sesije (session layer)
4. sloj – sloj transporta (transport layer)
3. sloj – sloj mreže (network layer)
2. sloj – sloj veze (data link layer)
1. sloj – fizički sloj (physical layer)



Slika 6 OSI referentni model

OSI model ima 7 slojeva zbog toga što su se njegovi tvorci povelili za u to vreme, daleko najvećim proizvođačem računara, firmom IBM, koja je za svoje mreže koristila sedmoslojni protokol SNA (System Network Architecture). U OSI modelu osnovna su 3 koncepta: koncept usluge, interfejsa i koncept protokola.

Unutar jednog računara svaki sloj zahteva usluge od sloja ispod sebe. Procesi (entiteti) koji se nalaze u istom sloju, ali na različitim računarima nazivaju se entiteski parovi ili ravnopravni entiteti. Entiteski parovi prividno direktno komuniciraju – svaki sloj u izvorišnoj stanici prividno komunicira sa odgovarajućim slojem u odredišnoj stanici. Komunikacija između entiteskih parova obavlja se pomoću jednog ili više protokola datog sloja. Protokol je skup pravila koji upravlja načinom na koji dva entiteta razmenjuju podatke.

Virtuelna komunikacija između odgovarajućih slojeva u izvoričnom i u odredišnom računaru obavlja se pomoću njima odgovarajuće protokolske jedinice podataka (PDU – Protocol Data Unit). U stvarnosti podaci se ne prenose direktno iz sloja N jednog računara u sloj N drugog već svaki sloj šalje podatke i upravljačke informacije u sloj neposredno ispod sebe sve dok se ne dostigne najniži sloj. Ispod fizičkog sloja je medijum kroz koji se odvija stvarna komunikacija. Na prijemu, pristigli podaci ulaze u fizički sloj i sukcesivno prolaze kroz slojeve dok ne stignu u sloj aplikacije.

Jedinica podataka sloja transporta naziva se SEGMENT, sloja mreže PAKET, sloja veze RAM ili OKVIR, a jedinica fizičkog sloja je BIT.

4.1.1. Sloj aplikacije

Sloj aplikacije omogućava korisniku (čovjeku ili programu) da pristupi mreži. Zato ovaj sloj sadrži niz protokola koji su potrebni za pružanje podrške raznovrsnim uslugama: elektronska pošta, pristup fajlovima, www, diskusione grupe, pričaonica... Sloj aplikacije se ponaša kao interfejs između stvarnog aplikacionog programa, koji nije deo slojevite strukture, i sledećeg sloja ispod, pružajući načine da aplikacija pošalje informacije naniže kroz stek protokola. Npr IE se ne nalazi unutar sloja aplikacije, već komunicira sa protokolima sloja aplikacije.

Važno je da se razume da u OSI modelu aplikacija ima različito značenje od onog značenja koje ima u standardnoj računarskoj terminologiji. U OSI modelu sloj aplikacije obezbeđuje servise koje koristi korisnička aplikacija. Kada se na korisničkom računaru pokrene neka aplikacija kao što je na primer Web pretraživač ona se stvarno ne nalazi u sloju aplikacije već samo koristi servise koje joj isporučuje protokol koji radi u sloju aplikacije i koji se zove Hypertext Transfer Protocol (HTTP). Razlika između Web pretraživača i HTTP protokola je mala, ali je ipak bitna.

4.1.2. Sloj prezentacije

Ovaj sloj se bavi sintaksom i semantikom informacija koje razmenjuju dva sistema. Ovaj sloj je odgovoran za:

- Prevođenje
- Šifrovanje
- Kompresiju
- Menjanje podataka
- Šifrovanje podataka

Pre prenosa, informacija se mora pretvoriti u nizove bitova. Različiti računari koriste različite sisteme kodovanja za predstavljanje alfanumeričkih podataka (ASCII, UNICODE), celih brojeva (komplement jedinice, komplement dvojke). Da bi se omogućila komunikacija između procesa koji za predstavljanje informacija koriste različite kodove, neophodno je obaviti prevođenje kodnog sistema koji se koristi u izvorištu u kodni sistem koji se koristi u odredištu. To se postiže na sledeći način:

- U sloju prezentacije predajnika, informacija se iz formata koji se koristi unutar predajnika konvertuje u neki opšti format
- U sloju prezentacije prijemnika obavlja se inverzna operacija: opšti format se prevodi u format koji se koristi u tom prijemniku

Kada se zahteva tajnost podataka, mora se obaviti šifrovanje podataka (data encryption). Šifrovanje se obavlja u predajniku tako što on konvertuje originalnu poruku u drugačiji oblik i tek onda je šalje na mrežu. Cilj kompresije je da smanji broj bitova koji se prenose, a da se sačuva prenesena informacija.

4.1.3. Sloj sesije

Termin sesija (session) označava period komuniciranja tj vođenja dijaloga između procesa (programa). Sloj sesije ima zadatak da uspostavi, održava i sinhronizuje komunikaciju između dva sistema. Zadaci koje sloj sesije treba da obavi su sledeći:

- Upravljanje dijalogom
- Sinhronizacija

Sloj sesije koordinira komunikacijom između dva sistema i služi da organizuje njihovu komunikaciju tako što nudi tri različita režima: SIMPLEKS, POLUDUPLEKS, PUNI DUPLEKS. Ako se saobraćaj u sistemu odvija u jednom smeru, sloj sesije vodi računa o tome ko emituje u određenom trenutku.

Drugi zadatak sloja sesije je da u poruku unese sinhronizacione tačke. To su kontrolne tačke koje se unose na određenom rastojanju. Ako dođe do prekida prenosa, prenos se nastavlja od posledenje sinhronizacione tačke.

4.1.4. Sloj transporta

Sloj transporta je odgovoran za isporuku cele poruke s kraja na kraj veze tj od izvorišta do odredišta. Osnovni zadatak sloja transporta je da:

- Prihvata podatke iz sloja sesije
- Podeli ih, ako treba na manje jedinice
- Propusti ih u sloj mreže
- Osigura da svi delovi poruke stignu na drugi kraj

U sloju transporta se obavlja sledeće:

- SAP adresovanje – adresovanje tačaka pristupa uslugama ili adresovanje portova; dok sloj mreže dovodi svaki paket u odredišni računar, sloj transporta dovodi celu poruku u odredišni računar
- Rastavljanje (segmentacija) i ponovno sastavljanje: poruka se deli na segmente koji se mogu preneti i svakom segmentu se dodeljuje redni broj kako bi sloj transporta u odredištu mogao da prispele pakete identifikuje i složi po ispravnom rasporedu, zamenjujući pakete koji su se tokom prenosa zagubili njihovim ponovo poslatim kopijama
- Upravljanje konekcijom: sloj transporta može da bude konekciono orijentisan (connection-oriented) ili beskonekcioni (connectionless)
- Upravljanje protokolom
- Kontrola grešaka

4.1.5. Sloj mreže

Sloj mreže nadzire isporuku paketa, a sloj transporta nadzire isporuku cele poruke. Sloj mreže je neophodan ako su dve stanice koje se nalaze u različitim mrežama koje su povezane uređajima koji se nazivaju ruteri. On je odgovoran za:

- Logičko adresiranje: fizičko adresiranje (koje se obavlja u sloju veze) dovoljno je kada se računari nalaze u istoj mreži, u protivnom sloj mreže unosi u zaglavlje paketa logičke adrese izvorišta i odredišta
- Određivanje putanje odnosno rutiranje
- Kontrola zagušenja

4.1.6. Sloje veze

Ovaj sloj je zadužen za:

- Formiranje ramova: na otpremi dodaje paketu pristiglom iz sloja mreže zaglavlje i rep
- Fizičko adresovanje: u zaglavlje rama unosi fizičku adresu predajnika i fizičku adresu prijemnika
- Upravljanje protokom: ako je brzina kojom prijemnik prihvata podatke manja od brzine kojom predajnik šalje podatke, sloj veze aktivira mehanizam za upravljanje protokom kako bi se sprečilo da brzi predajnik zaguši spori prijemnik
- Kontrolu grešaka: pomoću informacija u repu rama, omogućava otkrivanje grešaka
- Upravljanje pristupa medijumu

4.1.7. Fizički sloj

U fizičkom sloju se ram podataka koji stiže iz sloja veze konvertuje u nestruktuiran niz bitova. Zbog toga se fizički sloj bavi mehaničkim i električnim specifikacijama interfejsa i medijuma za prenos i definiše postupke i funkcije koje fizički uređaji i interfejsi moraju da obavljaju tokom prenosa. Zadaci fizičkog sloja su:

- Mehanička pitanja vezana za pristup medijumu
- Električna pitanja vezana za pristup medijumu
- Proceduralna pitanja vezana za pristup medijumu

Fizički sloj je zadužen za:

- Definisane karakteristike interfejsa između uređaja (računara) i medijuma za prenos
- Definisane vrste medijuma za prenos
- Predstavljanje bitova pomoću električnih ili optičkih signala
- Određivanje trajanja bita tj brzina emitovanja
- Vremensku sinhronizaciju tj sinhronizaciju predajnika i prijemnika na nivou bita
- Definisane smerove prenosa (simpleks, poludupleks, dupleks)
- Način umrežavanja računara: da li se radi o topologiji u obliku magistrale, zvezde, prstena ili svako sa svakim.

4.2. IPsec bezbednosni protokol

IPSec (Internet Protocol Security) je definisan RFC-ovima 4301 i 4309. Protokol radi mrežnom sloju i implementiran je u verziji IPv6 protokola. IETF je formirao IP Security

(IPSEC) radnu grupu čiji je zadatak da definiše standarde za VPN oblast. Ova radna grupa definisala je sledeće standarde:

- definisana su dva protokola zaštićenog prenosa Authentication Header (AH) i Encapsulating Security Payload (EPS)
- definisan način komunikacije uvođenjem pojma Security Associations (SA)
- definisan je način razmene ključeva posredstvom Interneta, Internet Key Exchange (IKE)

Iako ovaj protokol sve više prepušta svoje mesto znatno fleksibilnijem SSL protokolu veliki broj kompanija još uvek ga koristi za obezbeđivanje sigurne komunikacije. On se najčešće koristi u klasičnim VPN mrežama gde se na dve lokacije nalaze specijalizovani mrežni uređaji između kojih se uspostavlja IPsec konekcija. IPsec protokol podržava dva načina rada:

- Transport mode
- Tunnel mode

4.2.1. Tunelovanje

Tunelovanje je najvažnija komponenta tehnologije virtuelnih privatnih mreža koje su zasnovane na IPsec protokolu i predstavlja prenos paketa podataka namenjenih privatnoj mreži preko javne mreže. Ruteri javne mreže nisu svesni da prenose pakete koji pripadaju privatnoj mreži i VPN pakete tretiraju kao deo normalnog saobraćaja.

Tunelovanje ili enkapsulacija je metod pri kome se koristi infrastruktura jednog protokola za prenos paketa podataka drugog protokola. Umesto da se šalju originalni paketi, oni su enkapsulirani dodatnim zaglavljem. Dodatno zaglavlje sadrži informacije potrebne za rutiranje, odnosno usmeravanje paketa kroz mrežu, tako da novodobijeni paket može slobodno putovati transportnom mrežom.

Tunel predstavlja logičku putanju paketa kojom se on rutira preko mreže. Enkapsulirani podaci su rutirani transportnom mrežom sa jednog kraja tunela na drugi. Pojam tunel uvodi se jer su podaci koju putuju tunelom razumljivi samo onima koji se nalaze na njegovom izvoru i odredištu. Ovi paketi se na mreži rutiraju kao svi ostali paketi.

Početak i kraj tunela nalaze se u VPN mrežama. Kada enkapsulirani paket stigne na odredište vrši se deenkapsulacija i prosleđivanje na konačno odredište. Ceo proces enkapsulacije, transporta i deenkapsulacije paketa naziva se tunelovanje. Tehnologija tunelovanja koristi tri vrste protokola:

- Protokol nosač
ovi protokoli služe za rutiranje paketa po mreži ka njihovom odredištu. Tunelovani paketi imaju enkapsulaciju ovih protokola. Za rutiranje paketa po Internetu koristi se IP protokol.
- Protokol za enkapsulaciju
ovi protokoli služe za enkapsulaciju originalnih podataka, i koriste se za stvaranje, održavanje i zatvaranje tunela. Najčešće korišćeni su PPTP i L2TP protokoli.
- Transportni protokol
enkapsulira originalne podatke za transport kroz tunel. Najpoznatiji su PPP i SLIP protokol.

4.2.2. Transportni mod

Transportni mod (engl. Transport Mode)

Osnovne karakteristike transportnog moda su:

- šifruje se samo korisnički deo IP datagrama

- ne menja se dužina IP datagrama
- zadržava se originalno IP zaglavlje što omogućava da se vidi ko su partneri u komunikaciji

4.2.3. Tunelski mod

Tunelski mod (engl. Tunnel Mode)

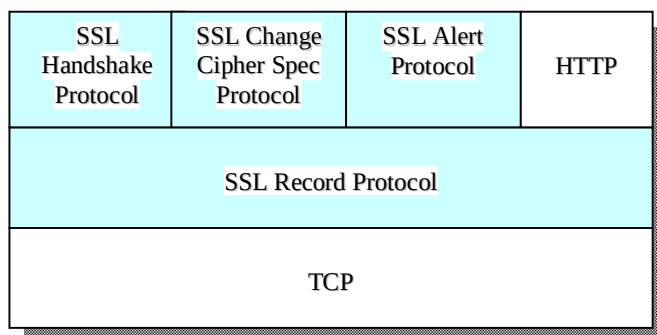
Osnovne karakteristike tunelskog moda su:

- Zajedno sa korisničkim delom IP datagrama šifruje se i originalno IP zaglavlje
- Dodaje se novo spoljno IP zaglavlje sa adresom sledećeg uređaja u mreži gde paket treba da stigne

Što se tiče IPsec protokola treba još reći da je tunelski mod znatno bezbedniji od transportnog moda. IPsec protokol se i dalje veoma često koristi za prenos zaštićenih podataka tamo gde nije neophodno da se za prebacivanje podataka sa jedne lokacije na drugu koristi Web pretraživač.

4.3. SSL protokol za zaštitu virtualne privatne mreže

Namena SSL protokola⁷ je da obezbedi sigurnu (zaštićenu) vezu između dva računara koristeći usluge transportnog TCP sloja. SSL protokol se sastoji iz više nivoa kao što je prikazano na slici



Slika 7 SSL protokol stek

SSL Rekord protokol (Record Protocol) se brine o šifrovanju–dešifrovanju informacija koje se prenose i tu uslugu pruža višim slojevima. U praksi to je obično HTTP (engl. Hypertext Transfer Protocol) preko koga Web čitači i serveri razmenjuju podatke. Tri viša protokola: Protokol za dogovaranje odnosno uspostavljanje veze (Handshake Protocol), protokol za promenu ključa (Change Cipher Spec Protocol), i protokol za upozorenje (Alert Protocol) služe za uspostavljanje veze, prelazak u režim šifrovanja simetričnim ključem i nadgledanje veze.

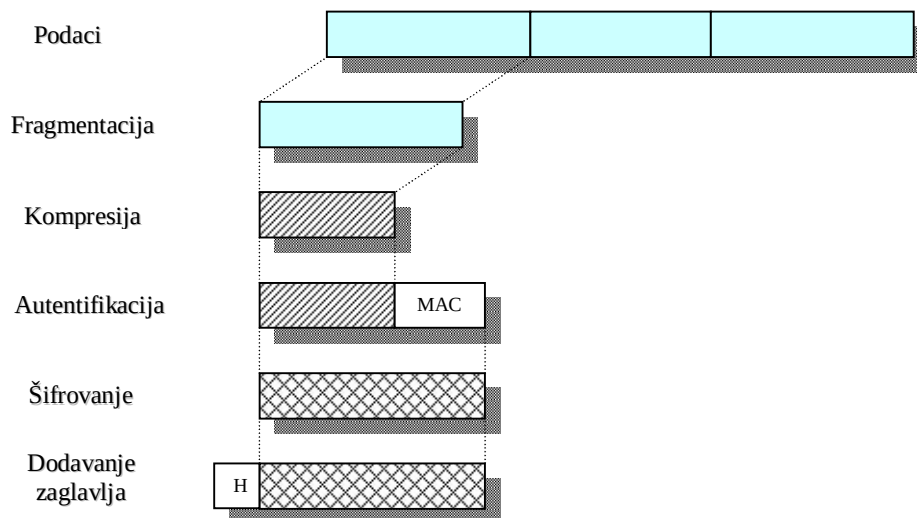
⁷ Spec.App Željko Pekić, SSL bezbednost transportnog sloja, Univerzitet Mediteran, 2009.

4.3.1. SSL rekord protokol (SSL Record Protocol)

SSL rekord protokol na predajnoj strani prihvata podatke od aplikacijskog sloja, vrši njihovu fragmentaciju u blokove, opciono komprimuje podatke, dodaje autentifikaciju (MAC - message authentication code), šifrjuje podatke, dodaje zaglavlje i predaje TCP sloju radi slanja. Na prijemnoj strani podaci se preuzimaju od TCP sloja, dešifrjuju, izračunava se i poredi MAC radi provere verodostojnosti, vrši dekompresija podataka, defragmentacija i na kraju podaci se predaju aplikacijskom nivou.

Aplikacijski podaci se dele na blokove ne veće od 2^{14} (16384) bajtova. Kompresija se opciono sprovodi i mora biti bez gubitaka. Nad kombinacijom komprimovanih podataka, parametrima kompresije i simetričnog MAC ključa izračunava se sažetak poruke po algoritmu MD5 ili SHA-1 i tako osigurava autentičnost poruke.

Komprimovani podaci i MAC se zatim šifruju dogovorenim algoritmom za šifrovanje simetričnim ključem.



Slika 8 SSL rekord protokol

4.3.2. Protokol za uspostavljanje sigurne veze (Handshake Protocol)

Najsloženiji deo SSL-a je Handshake Protocol. Ovaj protokol omogućava: proveru identiteta klijenta i servera, pregovaranje oko upotrebe algoritma za šifrovanje i izračunavanje sažetka poruke i razmenu ključeva. Koristi se u fazi uspostavljanja konekcije pre bilo kakve razmene podataka iz sloja aplikacije. Handshake Protocol se sastoji od niza poruka koje se razmenjuju između klijenta i servera.

Uspostavljanje veze između klijenta i servera odvija se razmenom poruka i može se podeliti u četiri faze:

- Prva faza- Postavljanje parametara veze
- Druga faza- Autentifikacija servera i razmena ključeva
- Treća faza- Autentifikacija klijenta i razmena ključeva

- Četvrta faza- Završetak uspostavljanja sigurne veze

4.3.3. Protokol za promenu ključa (*Change Cipher Spec*)

Ovaj protokol sastoji se od jedne poruke veličine jednog bajta i njime predajna strana obaveštava prijemnu stranu da prelazi na režim šifrovanja podataka simetričnim ključem.

4.3.4. Protokol za upozorenja (*Alert messages*)

Alert Protocol se koristi za dostavljanje SSL upozorenja do učesnika u komunikaciji. Svaka poruka sastoji se iz dva bajta. Prvi bajt može da ima vrednost warning (1) ili fatal (2), ako je vrednost fatal konekcija se trenutno raskida. Drugi bajt sadrži kod upozorenja. Kada je otkrivena greška, strana koja je otkrila grešku šalje poruku drugoj strani. U trenutku slanja i primanja takve poruke, obe strane zatvaraju sesiju (vezu). Server i klijent su u tom slučaju dužni da zaborave bilo kakve podatke o sesiji, identifikatore sesije, ključeve i ostale tajne koje su vezane uz sesiju.

5. Organizacija savremenih računarskih mreža

Tokom istraživanja vezanih za ovaj rad situacija u domenu informacionih tehnologij, a naročito u domenu računarskih mreža radikalno se izmenila. Pored nekih drugih faktora koji su tome doprineli, a o kojima će biti više reči kasnije ovde će biti rečeno nešto o korisnicima savremenih računarskih mreža. Veliki broj mrežnih administratora ne primećuje ili ignoriše činjenicu da je sve veći broj korisnika računara tehnički veoma napredovao. Tome je znatno doprinela ekspanzija mobilnih uređaja pre svega mobilnih telefona i laptop računara.

Sve češće se dešava da korisnici traže od administratora veća prava nad svojim radnim stanicama koje se nalaze u lokalnoj mreži. Ovi korisnici obično ne ugrožavaju bezbednost mreže već to po pravilu čine oni korisnici koji su pod potpunom kontrolom administratora. Problem je u tome što administratori ne mogu da ograniče ovim korisnicima nesmetano korišćenje Interneta koji im je sve više neohodan pa oni zbog svog neznanja često imaju problem. Zbog toga rešenje i nije u krutim polisama koje nameću administratori i koje korisnika sprečavaju da normalno koristi svoj računar već u tome da se korisnik edukuje da bi dobio svest o tome šta sme, a šta ne sme da radi.

5.1. Lokalna mrežna infrastruktura

Kada se danas razmišlja o konfigurisanju lokalne mreže u nekoj kompaniji moraju se imati u vidu nove tendencije razvoja IT sistema. Sve pristupačniji namenski serveri kao i ubrzani razvoj Cloud computinga dovode do toga da se kompanije sve češće odlučuju da svoje podatke kao i aplikacije pa čak i infrastrukturu izmeste izvan svoje lokalne mreže. Najveći broj lokalnih mreža koje se danas nalaze u kompanijama koristi se pre svega za razmenu fajlova, deljenje štampača i izlaz na Internet. Sve ređe, lokalne mreže se koriste za mail servis, dok se najmanje koriste za rad sa aplikacijama. U bankama i velikim korporacijama situacija je nešto drugačija ali ovde je reč o mrežama u manjim kompanijama. Iako se radi o kompanijama koje se bave različitim delatnostima način iskorišćenja mrežnih resursa, a pre svega servera je skoro identičan.

Kada se pojavio Windows 2008 operativni sistem koji zahteva mnogo moćniji hardver od onoga na kome može da radi Windows 2003 rukovodeći ljudi u kompanijama počeli su da razmišljaju o novoj opremi. Da ne bude zabune, Windows 2008 u standardnoj verziji može da radi i na serverima slabijih performansi ali takvi serveri ne mogu da se koriste za neki ozbiljniji rad. Neophodno je da kompanije moraju da imaju realnu sliku o uposlenosti kapaciteta svoje računarske mreže, a naročito servera koji se u njoj nalaze. Ovo je važno zbog toga što bi ukoliko dobro procene situaciju u budućnosti mogli da koriste alternativna rešenja uz znatno smanjenje troškova.

Kao što je već rečeno u većini računarskih mreža u manjim kompanijama Windows serveri se uglavnom koriste kao fajl serveri. Činjenica je da je novi namenski hardver koji se sve više koristi mnogo jednostavniji za konfigurisanje. Ovde se pre svega misli na Network Attach Server (NAS) server uređaj koji u potpunosti može da zameni Windows fajl server. Što se tiče mrežnih funkcija njih može uspešno da obavlja bilo koji ruter čak i efikasnije nego sam Windows server. Stalno usavršavanje i pojednostavljivanje ovakvih uređaja dovelo je do toga

da i zaposleni u kompaniji koji imaju osnovno tehničko znanje mogu da konfigurišu ove uređaje posle kraće obuke.

Sve pristupačniji namenski i cloud serveri dovode do toga da se sve više kompanija odlučuje da svoje servise izmesti iz lokalne mreže. Kada izmeste svoje podatke i aplikacije postavlja se pitanje za šta će onda lokalna mreža da služi. Da li je u takvoj mreži uopšte potreban Windows server čija kompletna konfiguracija i kasnije održavanje nisu ni malo jeftini. Međutim lokalne računarske mreže u budućnosti će i dalje postojati ali njihova uloga i organizacija mogli bi da budu bitno drugačiji.

Pregled troškova koji se javljaju prilikom korišćenja lokalne mreže, na koje mali broj kompanija obraća pažnju već po inerciji izdvaja novac za njih, pokazuju da lokalna mreža može da bude znatno jeftinija i efikasnija. Kada se uporede troškovi za hardver, odnosno troškovi za nabavku servera sa jedne ili nabavku NAS servera i rutera za mrežnu komunikaciju koji predstavljaju njegovu alternativu sa druge strane oni ne treba da budu jedini argument za izbor bilo koje od ove dve opcije. Najveći problem je u tome što odgovorni ljudi u kompanijama prilikom nabavke hardvera uopšte ne razmišljaju o dodatnim troškovima koje će imati da bi takav hardver uopšte mogli da puste u rad. Ukoliko neka kompanija želi da koristi server u svojoj lokalnoj mreži njeno rukovodstvo mora da bude svesno da će pored novca koji je neophodan za kupovinu samog servera biti neophodno da se izdvoji novac i za sledeće troškove:

- Troškovi nabavke operativnog sistema ukoliko je u pitanju Windows
- Troškovi licenciranja ukoliko je u pitanju Windows
- Troškovi instalacije
- Troškovi održavanja

Kod korišćenja namenskih uređaja potrebno je platiti jedino troškove instalacije i konfigurisanja dok permanentno održavanje kao u slučaju Windows servera nije neophodno. Kao što je već rečeno, tendencije u savremenom poslovanju potpuno će promeniti izgled i konfiguraciju lokalne mreže. Kada se razmišlja o troškovima za ulaganje u računarsku mrežu svako treba imati u vidu i to za šta će se ona u budućnosti koristiti.

5.1.1. Nova organizacija lokalne mreže

Rešenje za lokalnu mrežu jeste to da bi ona mogla da služi za backup podataka ali da bude tako konfigurisana da u slučaju da Internet iz bilo kog razloga nije dostupan korisnici koji se nalaze u lokalnoj mreži mogu nesmetano da nastave da rade. Naravno, lokalna mreža bi mogla da se koristi i za svoju prvobitnu namenu odnosno za razmenu fajlova ali sa nešto drugačijom opremom i načinom organizacije.

Za potrebe razmene fajlova u novoj organizaciji lokalne mreže Windows File server može da ima ozbiljnu alternativu u namenskom uređaju koji se zove Network Attach Server (NAS) ali pre toga evo nekoliko predloga kako bi File sistem neke kompanije mogao da bude organizovan:

- U kompaniji bi mogao da se koristi kao backup file server za file server koji se nalazi na namenskim ili cloud serverima
- Kao klasični fajl server u lokalnoj mreži ali da se umesto Windows servera koristi NAS server
- Na nekim NAS serverima koji imaju podršku za PHP i MySQL mogao bi da se instalira i Document Management System (DMS)

Network Attach Server ili skraćeno NAS server je računar za čuvanje podataka na nivou fajlova koji je povezan sa računarskom mrežom koja omogućava pristup podacima heterogenim klijentima. Od 2002. godine ovi uređaji su počeli da dobijaju na popularnosti, kao zgodan način za razmenu fajlova između više računara. Potencijalne koristi od uređaja za čuvanje koji je povezan na mrežu, u poređenju sa fajl serverima, uključuju brži pristup podacima, lakšu administraciju i jednostavnu konfiguraciju.

NAS serveri sadrže jedan ili više hard diskova koji su često poređani u logične, redundantne kontejnere za čuvanje ili RAID nizove. Iako tehnički može biti moguće pokrenuti druge softvere na NAS serveru, on nije napravljen da bude server za opštu upotrebu. Na primer, NAS serveri obično nemaju tastaturu i monitor, a kontrolišu se i konfigurišu preko mreže a za to se koristi Web pretraživač.

Kao operativni sistem na NAS serverima koristi se neko od Linux based rešenja koji je već instaliran na uređaj pa korisnik o tome ne mora da brine kao u slučaju Windows servera. NAS server podržava hard diskove velikog kapaciteta od 1TB i može se proširiti na 2TB uz pomoć ultra brzog eSATA i USB 2.0 porta. Sa svojim dizajnom koji ne pravi buku i izvanrednom tehnologijom za rasipanje toplote predstavljaju odlično rešenje za svaku lokalnu mrežu. NAS serveri imaju jednostavan interfejs za upravljanje grupnim polisama korisnika, a neki od njih su i printer serveri što ide u prilog tvrdnji da Domen kontroler i aktivni direktorijum više nisu neophodni u lokalnoj mreži.

Kada je reč o NAS serverima kao jedna od njihovih karakteristika pominje se uloga printer servera. Pored ovog rešenja na tržištu postoje i jeftini namenski uređaji koji su specijalizovani samo za ovu funkciju. Takođe ukoliko u kompaniji postoji potreba za deljenim štampačima oni jednostavno mogu da se zakače na mrežu, a drajveri za njih mogu da se instaliraju na lokalnu radnu stanicu.

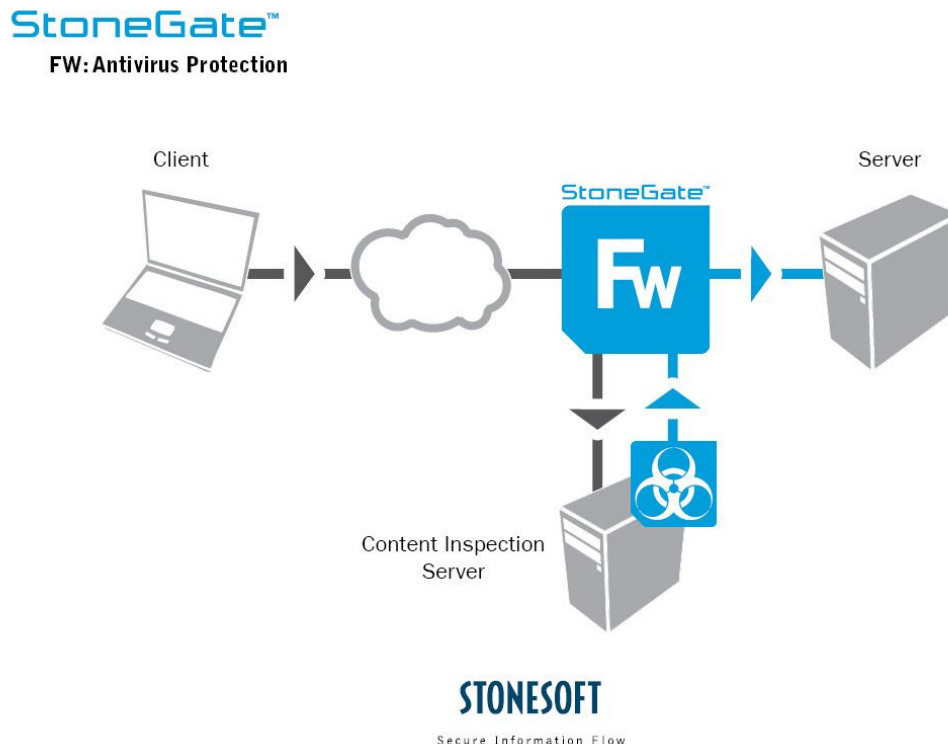
Proizvodnaja mrežnih uređaja je u velikoj ekspanziji što je dovelo do toga da se prave sve pouzdaniji višenamenski uređaji čija je glavna karakteristika pored sve pristupačnije cene i lakoća konfigurisanja. Preko ovih uređaja mnogo jednostavnije može da se konfiguriše DNS i DHCP, kao i neke funkcije rutiranja koje mogu da optimizuju rad lokalne mreže. Ukoliko se ovome dodaju i NAT funkcija VPN funkcija kao i funkcije firewall-a jasno je da ovakvi uređaji mogu u potpunosti da zamene slična podešavanja na Windows serverima.

Sve veći broj bežičnih rutera koji se koriste u kućnim uslovima ili u manjim kancelarijama dokazuje tvrdnju da su savremeni mrežni uređaji jednostavni za korišćenje i da ih čak može konfigurisati i korisnik koji nema neko specijalno tehničko znanje. Naravno za komplikovanija podešavanja potrebno je potražiti pomoć stručnjaka kojih je sve više s obzirom na činjenicu da su kursevi za rukovanje mrežnom opremom sve pristupačniji i sve popularniji.

Takođe, treba naglasiti i to da se u većini lokalnih mreža koje su bile zasnovane na Windows serverima bezbednosti tih mreža poklanjalo vrlo malo pažnje. Ovo se pre svega dešavalo zbog činjenice da je lokalna mreža sa Microsoft serverom po definiciji morla da ima i Microsoft rešenje za bezbednost. Ovo je zahtevalo investiranje u novi hardver za šta korisnici naročito u manjim mrežama nisu bili spremni. Međutim ovaj problem bi mogao da bude prevaziđen korišćenjem sve polpopularnijeg višenamenskog hardvera koji se naziva SSL VPN uređaj. Posmatrajući odnos cene i performansi ovakvi uređaji mogu da zadovolje potrebe za bezbednošću računarske mreže bilo koje velične.

Kao što je već rečeno na tržištu postoji sve veći broj kvalitetnih mrežnih uređaja, tako je primetan i porast ponude specijalizovanih UTM uređaja koji se koriste za zaštitu lokalne mreže. Ovakvi uređaji mogu da se podese za razne funkcije, a korisnički interfejs je pregledan

i jednostavan za upotrebu. Posebna pogodnost je i to što se uz kupovinu ovakvih uređaja dobijaju i licence za antivirus programe na lokalnim radnim stanicama. S obzirom na veliku konkurenciju cena ovakvih uređaja je sve pristupačnija i korisnicima koji imaju skromnije budžete predviđene za zaštitu.



Slika 9 Namenski uređaj za anti virusnu zaštitu u lokalnoj mreži

5.2. Virtualne privatne mreže

Kao što je već rečeno organizacija zaštite neće biti opisna samo teorijski već će se njena praktična implementacija prikazati kroz upotrebu u virtualnim privatnim mrežama. Sve veći broj kompanija bez ozira na njihovu veličinu koristi virtualnu privatnu mrežu kao odgovor na izazove koje pred njih postavlja savremen način poslovanja.

Treba napomenuti da VPN ne može da ukloni sve rizike koji postoje na mreži ali znatno može da ih smanji naročito u komunikaciji koja se odvija preko javne mreže. Jedan od mogućih problema je i komplikovana implementacija što se naročito odnosi na tradicionalno rešenje zasnovano na IPsec protokolu. Znatno jednostavnije rešenje je implementacija preko SSL VPN-a, novog načina na koji se konfigurišu virtualne privatne mreže. U osnovi ove vrste VPN-a je SSL protokol čija je najveća prednost u tome što obezbeđuje korisnicima da koristeći samo Web pretraživač, bez dodatnih komponenti instaliranih na klijentskoj strani kao što to zahteva IPsec protokol, mogu nesmetano da pristupaju mrežnim servisima.

Kada planira uvođenje virtualne privatne mreže u svoju informatičku infrastrukturu bilo bi dobro da se svaka kompanija odluči za tip VPN koji najviše odgovara načinu na koji je

organizovano njeno poslovanje. Planiranje i pravilan izbor nekog od postojećih tipova VPN-a veoma je važan jer pogrešna procena, bilo kompanije koja kupuje ili kompanije koja prodaje ovu uslugu, mogla bi kasnije da dovede do ozbiljnih problema u poslovanju.

Treba razmotriti pre svega koliko kompanija ima udaljenih kancelarija eng. branch office, kao i koliko ljudi je u njima zaposleno. Takođe treba uzeti u obzir koliko često su zaposleni na putu eng. teleworker dakle izvan lokalne mreže i bez mogućnosti da koriste njene resurse. Na bazi ovih procena može se konstatovati da postoje dve osnovne vrste virtualnih privatnih mreža koje u literaturi imaju različite nazive ali je ovde korišćena sledeća terminologija:

- LAN-to-LAN virtualne privatne mreže (koje se negde nazivaju i host-to-host)
- Remote access virtualne privatne mreže (koje se negde nazivaju user-to-host)

Svaki od ovih tipova virtualnih privatnih mreža ima svoje prednosti nedostatke, a kompanija treba kao što je već rečeno da se odluči za onu koja će se najbolje uklopiti u njeno poslovanje. Takođe treba istaći da se u zavisnosti od tipa virtualne privatne mreže razlikuje i organizacija i tehnologije koje se koriste za zaštitu.

5.2.1. LAN-to-LAN virtualne privatne mreže

Kada se kaže virtualna privatna mreža prvo na šta se pomisli jeste povezivanje više udaljenih kancelarija jedne kompanije u jedinstvenu logičku celinu. Inicijalna ideja za razvojem virtualnih privatnih mreža je i nastala iz ove potrebe. Korisnici u udaljenim kancelarijama su na ovaj način dobili mogućnost da bezbedno pristupaju deljenim fajlovima i drugim mrežnim resursima kompanije, imajući pri tom utisak da su lokalni korisnici. Računar koji na ovaj način pristupa lokalnoj mreži dobija IP adresu iz opsega te mreže i tretira se kao bilo koja lokalna radna stanica.

Najveći problem ove vrste virtualne privatne mreže je cena. Kompanija mora u svakoj od udaljenih kancelarija da ima specijalizovan hardverski uređaj koji će udaljenu kancelariju povezati sa VPN koncentratorom u sedištu kompanije. Ukoliko u udaljenoj kancelariji postoji veliki broj zaposlenih onda se ova investicija isplati. Međutim ukoliko u udaljenoj kancelariji sedi samo nekoliko ljudi ovo rešenje je previše skupo. U tom slučaju treba razmotriti mogućnost da zaposleni u udaljenoj kancelariji budu tretirani kao zaposleni na terenu što je moguće s obzirom na savremenu i jeftinu mrežnu opremu i nove mogućnosti za povezivanje na Internet.

Ovakva vrsta Virtualnih privatnih mreža zasnovana je isključivo na IPsec protokolu. U velikim kompanijama ovakva vrsta povezivanja udaljenih lokacija imaće svoju primenu i u budućnosti jer se zbog srazmerno velikog broja korisnika ulaganje u opremu na ovim lokacijama isplati. Međutim, ova vrsta virtualnih privatnih mreža ne može da zadovolji narastajuće potrebe kompanija da na svoju računarsku mrežu dozvole pristup korisnicima koji se iz bilo kog razloga nalaze izvan kompanije.

5.2.2. Remote access virtualne privatne mreže

Prevazilaženje problema sa pristupom udaljenih korisnika ponuđeno je korišćenje remote access virtualnih privatnih mreža. Ovu vrstu pristupa virtualnoj privatnoj mreži u zavisnosti od tehnologije koja se koristi možemo da podelimo u dve grupe:

- Virtualna privatna mreža zasnovana na IPsec protokolu
- Virtualna privatna mreža zasnovana na SSL VPN-u

Pored toga što su ova dva protokola prilično razlikuju po svojoj strukturi ono što je nesporno jeste da je komunikacija preko oba protokola veoma sigurna. Glavni nedostatak IPsec protokola je to što on ne može da se koristi kroz Web pretraživač bez koga će pristupanje podacima bilo da su u pitanju fajlovi ili baze podataka u bliskoj budućnosti biti nezamislivo. Savremeno poslovanje naročito kod kompanija koje imaju globalni biznis i čiji su zaposleni često na terenu dovelo je do potrebe za pojedinačnim pristupom lokalnoj računarskoj mreži. Obe spomenute tehnologije omogućavaju udaljenim pojedinačnim korisnicima da pristupaju lokalnoj mreži svoje kompanije. Da bi se nekom korisniku obezbedio udaljen pristup preko IPsec protokola on na svom računaru mora da ima instaliran VPN klijent o čijim nedostacima je već bilo reči.

SSL VPN tehnologija odnosno SSL protokol koji je njen glavni deo rešava problem sa udaljenim klijentskim računarom na mnogo efikasniji način. Lokalnoj mreži kompanije ne pristupa se više uz pomoć VPN klijenta već preko bilo kog Web pretraživača koga svaki klijentski računar već ima instaliranog. Ukoliko se autentifikacija vrši smart karticom ili tokenom na klijentskom računaru mora da se instalira plug-in ali je ta instalacija mnogo jednostavnija nego kada je u pitanju VPN klijent.

Sve veći broj kompanija se specijalizuje u oblasti SSL VPN tehnologija, tako da na tržištu sada postoji veliki broj kvalitetnih rešenja koja mogu da zadovolje potrebe bilo kog korisnika bez obzira na veličinu kompanije kao i na finansijska sredstva koja je spremna da uloži u zaštitu. Ovakva ekspanzija dovela je do značajnog pada cena hardverskih i softverskih komponenti koje se koriste u SSL VPN tehnologiji. O SSL VPN tehnologiji biće reči kasnije u posebnom poglavlju koje govori samo o tome.

Na kraju treba reći da SSL VPN pristup virtualnoj privatnoj mreži i znatno smanjuje troškove nabavke i implementacije potrebne opreme u odnosu na pristup preko IPsec protokola, a njegove najveće prednosti su u tome što prati savremene trendove poslovanja i što se pokazao kao znatno pouzdaniji u radu.

6. Mrežna infrastruktura izmeštena kod provajdera

Kao što je rečeno savremene tendencije u oblasti informacionih tehnologija odnose se na izmeštanje informatičke infrastrukture iz kompanija i njihovo hostovanje kod za tu svrhu specijalizovanih provajdera. Velike kompanije koje proizvode računarski hardver ponovo se okreću mainframe računarima kao rešenju koje je pouzdanije, moćnije, a kada se sagledaju svi troškovi i jeftinije. Takođe treba napomenuti da provajderi sve više pribegavaju virtuelizaciji što im uvećava resurse i omogućava da racionalnije prodaju svoje servise. Korisnik sada može da zakupi od provajdera samo onoliko procesorske snage, memorije ili prostora na hard disku koliko mu je u tom trenutku zaista neophodno što neminovno dovodi do smanjenja njegovih troškova.

Provajderi svoju opremu smeštaju u data centre koji zadovoljavaju sve potrebne uslove za nesmetan rad brojnih servera koji se u njima nalaze. Propisna temperatura, vlažnost vazduha, uvek dostupna tehnička podrška, a pre svega fizička bezbednost su glavne prednosti koje korisnicima pružaju data centri. Ovakve karakteristike data cenara omogućavaju praktično neprekidnu dostupnost servisa koji se u njima hostuju. Kada se tome doda da veliki provajderi imaju i po nekoliko lokacija na kojima imaju redundantne podatke jasno je da postoji mala verovatnoća da neki servis ne bude dostupan baš onda kada je to kompaniji neophodno. Kada se radi o dostupnosti servisima treba reći da ona ne zavisi samo od obezbeđivanja rezervnih lokacija i redundantne računarske opreme koja se na njima nalaze. Podjednako važno je da provajderi imaju stručne i osposobljene ljude za Contingency planning (CP) o kome je bilo već bilo reči u poglavlju o Organizaciji i upravljanju zaštitom, a koji se sastoji od sledećih komponenti:

- Incident response planning (IRP)
- Disaster recovery planning (DRP)
- Business continuity planning (BCP)

Sve tri komponente su veoma važan činilac koji obezbeđuje nesmetano funkcionisanje sistema što korisniku pruža komfor čije pozadine on često nije ni svestan. Jasno je da obezbeđivanje ovakvih uslova zahteva postojanje najmanje još jedne lokacije koja ima opremu kao i sve druge uslove kao i primarna lokacija. Alternativna lokacija mora da zadovoljava određene uslove, a najvažniji od njih jeste da od primarne lokacije bude udaljena određeni broj kilometara. Ovakve i slične uslove svakako ne može da obezbedi veliki broj kompanija koje imaju potrebu da se njihovo poslovanje odvija neprekidno. I kod nas je sve više provajdera koji mogu da ponude ovakvu vrstu usluga, a što je najvažnije njihova cena je sve pristupačnija čak i za manje kompanije.

Kada je reč o opremi teško je zamisliti da jedna kompanija prosečne veličine može da se utrkuje sa velikim provajderima u neprekidnom investiranju u svoje hardverske pa i softverske kapacitete. Postoji čak mogućnost da kompanija instalira svoj hardver kod provajdera što se naziva colocatred servis, ali zbog svoje visoke cene on ovde neće biti detaljnije razmatran. Zbog toga je znatno jeftinije i za kopanju isplativije iznajmljivanje opreme koja je vlasništvo provajdera. Do sada su se najčešće iznajmljivali namenski serveri ali sve više provajdera nudi iznajmljivanje virtualizovanih servera odnosno Clud computing. Kod provajdera se pre svega mogu hostovati podaci, ali je sve izraženiji trend da se od

provajdera iznajmljuju i razne vrste specijalizovanih servisa koji dodatno poboljšavaju poslovanje kompanija.

Kao što je već rečeno najveći problem za provajdera, kao i za kompaniju koja usluge provajdera nudi krajnjem korisniku, jeste u tome da ubedi krajnjeg korisnika da su njegovi podaci bezbedni. Ako se pođe od pretpostavke da se ovakvi provajderi uglavnom nalaze u Americi i da oni najveći i najpoznatiji svakako ispunjavaju rigorozne bezbednosne standarde koje na neki način i sami diktiraju, u ovom poglavlju će više biti reči o bezbednoj komunikaciji između klijenata i udaljenih servera. Bezbednost ove komunikacije samo delimično zavisi od provajdera ali u mnogo većoj meri zavisi od rešenja koje nude kompanije koje servise provajdera nude krajnjim korisnicima. S obzirom da je o bezbednosti informacionih sistema počelo da se ozbiljnije razmišlja tek od nedavno, evidentan je nedostatak pre svega konsultantskog kadra za primenu bezbednosti u realnom okruženju. Neki konkretni predlozi za rešenje ovog problema biće detaljnije opisani u poglavlju Zaštita kao servis.

6.1. Namenski serveri

Namenski serveri su računari koje korisnik može da iznajmi od provajdera za potrebe svog poslovanja. Kada se iznajmljuju namenski serveri korisnik tačno zna kakav će hardver dobiti za novac koji je uložio. Ovo i jeste najozbiljnija prednost namenskih server u odnosu na Cloud computing. Korisnik sam podešava servere počev od instalacije i konfigurisanja operativnog sistema pa sve do istaliranja neophodnih aplikacija. Serveri se zakupljuju u celosti tako da nema deljenja resursa sa drugim korisnicima što je takođe ozbiljna prednost namenskih servera. Ako govorimo o nedostacima onda bi to pored visoke cene svakako bio i problem koji korisnik može da ima ukoliko ima potrebe za nečim što se naziva high availability. Čak i uslučaju da se iznajmi backup server što dodatno povećava troškove, za prelazak na novi server u slučaju otkazivanja potrebno je neko vreme.

Namenski serveri iako veoma skupi imaju svoje kupce, mada se korisnici naročito oni sa manjim obimom poslovanja sve više odlučuju za Cloud computing, kao jeftiniji i fleksibilniji servis.

6.2. Cloud computing

Osnovna mana namenskih servera je neracionalno korišćenje hardverskih resursa. Dok kod namenskih servera korisnik iznajmljuje ceo hardver iako mu to u suštini nije potrebno Cloud computing podrazumeva zakupljivanje samo onoliko resursa koliko je korisniku zaista potrebno. Tako se može zakupiti samo deo procesorke snage, deo memorije ili deo prostora za skladištenje podataka. Ukoliko u toku poslovne godine dođe do povećanog obima poslovanja korisnik nesmetano može da iznajmi nove resurse i tako zadovolji svoje novonastale potrebe.

Kada se od provajdera iznajmljuje Cloud computing korisnik dobija pogodnosti koje pružaju računari koji se nalaze u cluster-u ili grid-u strukturi koja obezbeđuje redundantnost odnosno mogućnost da ukoliko je jedan od servera nedostupan ostali serveri preuzimaju njegovu ulogu u realnom vremenu, tako da korisnik ne može ni da primeti da se bilo šta dogodilo. Servis nesmetano, bez prekida nastavlja da funkcinise. Ovo je pored cene velika prednost Cloud computing-a u odnosu na namenske servere. Inače infrastruktura se iznajmljuje sa već podešenom virtualnom mašinom tako da korisnik može da bira platformu na kojoj želi da instalira svoje aplikacije. Protivnici Cloud computing-a najviše zamerki imaju na to što

između Cloud provajdera ne postoji interoperabilnost, odnosno još uvek je ozbiljan problem za korisnika da servise sa jednog provajdera u nekom trenutku prebaci kod nekog drugog. Takođe, korisnik ne zna gde se fizički nalaze njegovi podaci jer se oni ne nalaze na jednom serveru što realno govoreći predstavlja više psihološki nego bezbednosni problem. Ovakva vrsta Cloud computinga gde se resursi uslovno rečeno dele sa drugim korisnicima u literaturi se sve češće naziva Public cloud. Naravno ovakav način hostinga je znatno bezbedniji od klasičnog deljenog hostinga, a postoji i mogućnost da korisnik dobije jednu ili više javnih IP adresa za pristup svom delu Cloud-a

Pored toga provajderi sve više nude Private cloud odnosno deo Cloud-a koji kompanija može da iznajmi samo za sebe da bi na njemu držala svoje poverljive podatke. Ovaj termin se u literaturi tumači na različite načine ali bitno je ono što ozbiljni provajderi nude kroz ovu uslugu. To su u stvari namenski serveri odnosno najmanje dva koji obezbeđuju redudantnost koji na sebi imaju instaliranu neophodnu platformu za Cloud computing. Tako da je pored mnogobrojnih teorija o tome šta je to Private cloud najpribližnija istini ona koja kaže da su to namenski serveri obučeni u novo ruho.

Dok je kod iznajmljivanja namenskih servera situacija više manje jasna jer korisnik iznajmljuje fizički server ili više njih, sam ih konfiguriše i jedino on ima pristup servisima koji se na njima nalaze. Što se tiče Cloud computinga tu je situacija nešto drugačija. Uz pomoć virtualizacije i grid computing-a korisnicima se pruža mogućost da rade sa svojim podacima, a da ne moraju da vode računa o tome gde se oni fizički nalaze. Korisnik može da odabere neke od sledećih servisa:

- Software as a Service
- Platform as a Service
- Infrastructure as a Service

Cloud computing odnosno tehnologije koje čine njegovu infrastrukturu ovde neće biti detaljnije razmatrane jer to i nije tema ovog rada. U ovom radu će detaljnije biti opisan Software as a Service odnosno servis koji korisnici Cloud computing-a, pa i namenskih servera najčešće koriste. Biće predložena rešenja koja treba da pokažu kako ovakva vrsta servisa može da unapredi poslovanje kompanije.

Kada se govori o bezbednosti namenskih servera i Cloud computinga pre svega se misli na bezbednu komunikaciju između klijenta i servera koji se nalaze na udaljenoj lokaciji. Podaci jedne kompanije mogu da se nalaze kod više provajdera što u isto vreme predstavlja i prednost i nedostatak ovakve vrste servisa. Za kompaniju bi bilo neisplativo da svakom od njih pristupa preko posebnog tunela koji zavisi od samog provajdera. Ideja je da se napravi nezavisan tunel kroz koji bi bio moguć pristup bilo kojoj lokaciji na kojoj se nalaze podaci kompanije. Kod nas se o ovoj temi vrlo malo govori i piše, pa je ovaj rad pokušaj da se ukaže na neke specifičnosti u sistemima zaštite koje su nametnute ovakvom vrstom servisa.

6.3. Prednosti hostinga na namenskim ili Cloud serverima

Sve brži tempo poslovanja zahteva od kompanija da brže donose važne poslovne odluke da bi na taj način bili uspešniji od svoje konkurencije. Globalizacija tržišta dovela je do toga da zaposleni sve češće moraju da putuju da bi sklapali poslove za svoju kompaniju. Prilikom sklapanja ovakvih poslova njima mogu da zatrebaju informacije koje u tom trenutku nemaju na svom laptopu.

Ovo je dovelo do toga da kompanije svoje podatke izmeste izvan lokalne mreže i učine ih dostupnim svojim zaposlenima ma gde se oni nalazili u određenom trenutku. Na taj način oni mogu da pristupaju datotekama ili nekoj aplikaciji na isti način kao kada sede u svojoj kancelariji. Pored toga što su sada podaci vidljivi sa bilo koje lokacije u svetu hostovanje na namenskim serverima ili u Cloud computing-u pruža i druge značajne pogodnosti za kompaniju kao što su značajno smanjenje troškova poslovanja i bolja dostupnost servisa o čemu je već bilo reči.

Takođe treba naglasiti da je ekspanzija mobilnih uređaja kao što su smart telefoni ili tablet računari koji će se u uskoro sve više koristiti i za poslovanje, a ne samo za zabavu govore u prilog tvrdnji da je prošlo vreme filozofije poslovanja na desktop računarima kao i statičnog okruženja u kome su oni funkcionisali.

7. Upravljanje digitalnim identitetom

Pristup zaštićenim informacijama mora da bude ograničen samo na osobe koje su autorizovane za pristup tim informacijama. Računarski programi, a u mnogim slučajevima i sami računari koji obrađuju podatke moraju takođe da budu autorizovani. Ovo zahteva postojanje mehanizama koji su u stanju da kontrolišu pristup zaštićenim informacijama. Sofisticiranost mehanizama za kontrolu pristupa treba da se uporedi sa vrednošću informacija koje se štite. Osetljivije i dragocenije informacije treba da imaju jače mehanizme zaštite. Temelji na kojima počivaju mehanizmi kontrole pristupa su identifikacija i autentifikacija.

Identifikacija je tvrdnja ko je zapravo neko i šta je u stvari nešto. Ako se osoba predstavi svojim imenom i prezimenom neko mora da potvrdi da je ta izjava istinita. Međutim, ovakva tvrdnja može biti istina ili ne. Pre nego što nekoj osobi bude dozvoljen pristup zaštićenim informacijama neophodna je verifikacija odnosno provera informacija o toj osobi.

Za svakog zaposlenog vezuje se neki kompanijski identitet. To se može dešavati spontano i stihijski, a može biti i deo organizovanog i automatizovanog procesa koji donosi boljitak poslovanju. Identitet u fizičkom okruženju možemo predstaviti kao ogroman oblak u kojem se nalazi sve što možete reći o sebi. Kako elemente identiteta možete upotrebiti? U hotelu vam, u zamenu za pasoš, daju karticu za ulazak u sobu. Isto je i u sferi informacionih sistema, samo su načini manifestovanja vašeg identiteta i njegova upotrebnost digitalni.

Informacioni sistemi velikih organizacija su izuzetno složeni. To znači da ne postoji nijedan računar na kojem radi aplikacija koja nije bitna za poslovanje. U svakom većem preduzeću postoji više servera koji mogu da budu, a često i jesu, na različitom hardveru, pod različitim operativnim sistemima. Na svakom od njih se nalazi neka aplikacija, a u složenim (npr. finansijskim) organizacijama može se naći desetak i više aplikacija koje zaposleni koriste. Poslovni partneri kompanije takođe treba da pristupaju nekim resursima, a svako od njih ima svoje potrebe i svoj nivo pristupa koji treba da bude definisan prema resursima kompanije.

Postaje teško definisati koji nivo pristupa treba da ima korisnik. Da li uopšte treba da ima pristup nekoj aplikaciji, i ako treba, do kog nivoa? Šta sme da uradi kada jednom pristupi određenom resursu? Treba voditi računa i o radnicima koji odlaze iz firme; vratiće ključeve od službenog auta, mobilni telefon i računar, ali ko će da isključi njihove naloge? To je korak koji se često preskače, a izuzetno je opasan iz bezbednosnog aspekta. Bivši zaposleni može preko Interneta da čita podatke, a može i da menja sadržaj. Nije samo urbana legenda da nezadovoljan bivši zaposleni, sa visokim nivoom pristupa, ukrade ili obriše ključne podatke.

Kada nova osoba dolazi u firmu, ona i ne zna šta joj sve treba da bi radila uspešno. O tome brinu mrežni administratori koji kreiraju naloge za pristup sistemu, određuju nivo pristupa za svakog korisnika posebno što je dugotrajan proces koji administratoru oduzima dosta vremena. Taj proces troši vreme jer uvek treba kontaktirati administratora koji zbog obaveza često nije u mogućnosti da pomogne korisniku, pa se na kraju odlučuje da popusti pa zaposlenima daje privilegije da sami mogu da održavaju svoje radne stanice. Kao što je već rečeno u manjim kompanijama to nije problem, ali u preduzećima sa više hiljada zaposlenih situacija se drastično menja. Fluktuacija osoblja je velika što zahteva automatizovane procese i potpunu kontrolu administratora.

Organizacije žele da imaju na jednom mestu sve informacije o aplikacijama i tome ko ima koji nivo pristupa, kao i ko je taj nivo odobrio. Pored toga, neophodno je da imaju mehanizam

praćenja načina na koji korisnici upotrebljavaju ovlašćenja za pristup aplikacijama u informacionom sistemu. Te želje zadovoljavaju programi za upravljanje identitetom (identity management)⁸.

Kada se jednom instalira takvo softversko rešenje, za svakog zaposlenog u kompaniji se definiše kojim delovima informacionog sistema može i treba da ima pristup. Tako se kreira organizovan kompanijski identitet. Novi zaposleni dolazi na poziciju za koju su već definisana pravila, pa se novoj osobi samo dodeli postojeći identitet. Kompanijski identitet pripada kompaniji, a korisnik ga samo zauzima dok radi na toj poziciji. Taj identitet se jednom kreira i strogo je definisan, a dodeljena mu je određena grupa resursa i određene funkcionalnosti. Kada zaposleni menja poziciju unutar kompanije, dodeljuje mu se već postojeći identitet za novu poziciju, a stari ostaje spreman za novog zaposlenog. Svaki kompanijski identitet prolazi kroz četiri faze.

Prva faza podrazumeva proces otvaranja naloga na sistemima koje zaposleni treba da koristi. To bi trebalo da se radi onda kada su definisana radna mesta, a ne onda kada se pojavi novi zaposleni. Dodeljivanje uloga (role management) je deo ove faze, a taj segment rešenja služi za grupisanje naloga kojima zaposleni sa određenom ulogom treba da ima pristup. Tako se može definisati uloga sistem administratora, koja se može dodeljivati različitim identitetima prema potrebama funkcionisanja celog sistema.

U drugoj fazi, zaposleni koristi dodeljeni korporativni identitet. Na ovom nivou se menjaju lozinke i dozvole za pristup pojedinim resursima, a prema promenama radnih procedura u kompaniji i prema definisanim bezbednosnim pravilima. U ovu fazu spada i automatizovano obaveštavanje o zaboravljenoj lozinki, kao i sve ostalo što se sa digitalnim identitetom dešava tokom rada zaposlenog.

Treća faza podrazumeva praćenje rada kreiranih identiteta, menjanje njihovih podešavanja i eventualno kreiranje dodatnih za potrebe efikasnog rada.

U četvrtoj fazi se kompanijski identiteti gase. Radi se o procesu koji ne treba raditi ručno, jer mogu ostati opasni „repovi“, već ga treba prepustiti specijalizovanom softveru i automatizovanim procedurama koje će se pobrinuti da informacioni sistem ostane bezbedan.

Rezultat kontrole i evidencije rada svih zaposlenih jeste transparentnost funkcionisanja sistema. Ako nešto krene kako ne treba administrator može da dobije izveštaj ko je za to odgovoran, što u kompaniji koja ima desetine hiljada zaposlenih i ogroman sistem koji je teško fizički predstaviti unosi sigurnost u poslovanje.

7.1. Socijalni inženjering

Phishing je tipičan primer tehnike socijalnog inženjeringa koja se koristi za obmanjivanje korisnika sa ciljem da se od njega ukradu poverljivi podaci kao što su korisničko ime, lozinka, broj računa ili broj kreditne kartice. Phishing se izvodi korišćenjem e-mail ili instant poruka u kojima se sugeriše korisnicima da unesu tražene podatke na neki Web site. Takođe, za ovakve sugestije često se koriste i telefonski pozivi. Obračun sa rastućim brojem prijavljenih phishing napada obuhvata zakonsku regulativu, obuku korisnika, javna upozorenja i tehničke mere.

Korisnik treba da zna da njegova banka ili druga kompanija čiju Web aplikaciju koristi nikada neće koristiti ovakav način da od njega zatraže poverljive ni bilo kakve druge informacije, već

⁸ Marko Herman, Upravljanje identitetom, <http://www.pcpres.rs/arhiva/tekst.asp?broj=156&tekstID=8834>

će to učiniti preko bezbednih Web formi na koje će korisnik otići dobrovoljno. Treba istaći i da verziranji Internet korisnici mogu lako da upadnu u ovo zamku.

Klijent mora unapred da bude upozoren na činjenicu da od ovakve vrste napada ne postoji praktično nikakva zaštita osim nekih opštedruštvenih mera i upozorenja, a takođe i da vlasnik Web aplikacije koja je phishingom takođe napadnuta ne snosi nikakvu odgovornost za to.

Novi vid phishinga⁹ pogađa isključivo zaposlene u velikim kompanijama i vladinim telima. Na Internetu se pojavila nova pretnja iz domena socijalnog inženjeringa – tzv. „spear phishing”. U pitanju su napadi koji su usmereni ka tačno definisanim metama – zaposlenima u pojedinim kompanijama ili vladinim telima, naročito onima koja interno imaju striktno primenjen princip subordinacije. Spear phishing se od običnog phishinga pre svega razlikuje po meti napada, što je veliki inovativni skok u odnosu na dosadašnju kriminalnu praksu koja je išla logikom velikih brojeva, u nadi da će se od miliona pokušaja „upecati” bar koja „sočna” hiljada...

Spear phishing poruka izgleda kao da je došla od kolege koji je zaposlen u istoj organizaciji, i to najčešće u odeljenju za ljudske resurse ili informacione tehnologije, i ona po svemu izgleda kao svaka druga legitimna poruka upućena zaposlenima u organizaciji. Da bi sprečile svoje službenike da postanu žrtve ovog novog, još opasnijeg vida phishinga, neke institucije su pokrenule specifičan edukativni program, u okviru kojeg na adrese e-pošte svojih zaposlenih šalju lažne phishing mamce, s namerom da se kroz praktičnu demonstraciju oni obuču kako da pravilno reaguju u slučaju susreta sa pokušajem zlonamernog socijalnog inženjeringa.

Pošto je phishing postao jedan od najvećih bezbednosnih problema za korisnike Interneta, nova pretnja nazvana pharming ima sve izgleda da je ubedljivo nadmaši, kako po intenzitetu štete koju nanosi tako i po broju žrtava koje pogađa.

Za razliku od phishinga, pharming u veoma kratkom intervalu napada ogroman broj ljudi, preusmeravajući ih s legitimnih komercijalnih sajtova koje posećuju na lažne. Konceptijski, metod prevare je jednostavan. Sajtovi na koje se korisnik upućuje bez njegovog znanja i saglasnosti izgledaju potpuno isto kao i autentični, tako da on najčešće nije u stanju ni da posumnja da se nešto loše odigrava. Međutim, onog momenta kada on otkuca svoje korisničko ime i lozinku, te informacije bivaju ukradene. Za sprovođenje mnogih manjih pharming napada koriste se posebni virusi upućeni elektronskom poštom koji prepisuju lokalne host fajlove na napadnutim kompjuterima. Host fajl pretvara URL adrese u numeričke nizove koji su razumljivi za računar, tako da ugroženi host fajl uzrokuje da korisnik bude usmeren ka pogrešnom sajtu, čak i ako korektno ukuca URL adresu legitimne Web lokacije.

7.2. Autentifikacija

Autentifikacija je čin verifikacije tvrdnje o identitetu. Kada neko ode u banku da obavi neku novčanu transakciju on se predtavlja bankarskom službeniku imenom i prezimenom (tvrdnja o identitetu). Na zahtev službenika da svoj identitet potvrdi nekim dokumentom on prezentuje ličnu kartu. Službenik zatim proverava podatke i upoređuje fotografiju iz lične karte. Ukoliko fotografija i podaci odgovaraju osobi koja ih je prezentovala službenik je izvršio autentifikaciju odnosno potvrdio je da se radi o toj konkretnoj osobi.

⁹ Svet kompjutera <http://www.sk.rs/2005/11/skin05.html>

Postoje tri različita tipa informacija koje mogu da se koriste za autentifikaciju: ono što znate, ono što imate i ono što ste. Primer za “ono što znate” je najčešće PIN ili lozinka. Primer za “ono što imate” uključuje ličnu kartu ili platnu karticu. Biometrija u stvari govori “ono što ste”. Primeri biometrije uključuju otisak dlana, otisak prsta, snimak glasa i skeniranje mrežnjače oka. Snažna autentifikacija eng. strong authentication zahteva obezbeđivanje informacija iz dva od tri različita tipa informacija. Na primer “ono što znate” i “ono što imate”. Ovo se naziva dvofaktorna autentifikacija eng. two-factor authentication.

U računarskim sistemima koji su danas u upotrebi korisničko ime je najčešći način za identifikaciju, a lozinka je najčešći način za autentifikaciju. Korisničko ime i lozinka služili su svojoj svrsi ali u savremenom svetu oni više nisu adekvatan oblik identifikacije i autentifikacije i polako bivaju zamenjeni sofisticiranijim mehanizmima kao što su smart kartice ili biometrija.

7.3. Projektovanje PKI infrastrukture

Autentifikacija uz pomoć smart kartice ili USB tokena se naziva Two Factor Authentication ili dvofaktorska autentifikacija. To znači da je pored smart kartice ili USB tokena za autentifikaciju potreban i PIN koji zna samo njegov vlasnik.

Infrastruktura javnih ključeva (Public Key Infrastructure) je skup postupaka, dokumenata, resursa i aplikacija koje formiraju specifičan okvir za uspostavljanje digitalnog identiteta osobe, kao i za njegovo administriranje, upravljanje i nadzor tokom životnog ciklusa. PKI omogućava učesnicima, koji se uobičajeno i ne moraju unapred poznavati, da međusobno uspostave elektronsku komunikaciju, zasnovanu na međusobnoj autentifikaciji, verifikaciji digitalnog potpisa i poverljivosti.

PKI je zasnovan na kriptografiji javnih ključeva – asimetričnim kriptofunkcijama, koji dozvoljavaju da jedan od ključeva (iz para) jednog učesnika bude objavljen i poznat svim ostalim učesnicima u komunikaciji. Učesnik drugi ključ čuva u tajnosti. Informacija šifrovana jednim od ključeva može se dešifrovati drugim ključem iz istog para. Ova činjenica se koristi za potpisivanje ili poverljivo komuniciranje.

Digitalni identitet je vezan za posedovanje para ključeva koje izdaje nezavisna institucija – sertifikaciono telo (Certification Authority) u koju svi učesnici imaju apsolutno poverenje. Takva institucija izdaje tajni (privatni) ključ i javni ključ svakom učesniku. Javni ključ se izdaje u formi digitalnog sertifikata koji sadrži javni ključ i dodatne podatke koji su specifični za tog učesnika. Sertifikaciono telo overava svaki izdati digitalni sertifikat sopstvenim digitalnim potpisom.

Svaki učesnik može da proveri ispravnost digitalnog sertifikata primljenog od bilo kog drugog učesnika u komunikaciji, koristeći digitalni sertifikat sertifikacionog tela koje ga je izdalo. Ako je sertifikat punovažan, učesnik ima potvrdu da su lični podaci koji se odnose na pošiljaoca zaista njegovi, odnosno da je taj pošiljalac još uvek validan pretplatnik tog CA.

Digitalni sertifikati mogu da se distribuiraju na različite načine i uglavnom se publikuju na serverima CA koji su dostupni svim učesnicima. U našoj zemlji postoji nekoliko sertifikacionih tela koja su dobila pravo od nadležne institucije da izdaju kvalifikovane digitalne sertifikate. Kao što je poznato, kvalifikovani digitalni sertifikat odnosno kvalifikovani digitalni potpis imaju pravnu snagu svojeručnog potpisa i mogu se koristiti na sudu. Postoji međutim problem interoperabilnosti između sertifikata koje izdaju ova sertifikaciona tela. Naime, u našoj zemlji ne postoji jedna Root CA koja bi obezbedila da svi

sertifikati koje izdaju CA koja se hijerarhijski nalaze ispod nje poštuju uslov interoperabilnosti. Kod nas postoji nekoliko Root CA i sigurno će se pojaviti ozbiljni problemi vezani za interoperabilnost digitalnih sertifikata kada ova tehnologija bude počela ozbiljnije da se koristi.

Kada je reč o digitalnim sertifikatima koji se koriste kod nas pre svega se misli na samopotpisane sertifikate koje izdaju pojedine kompanije za svoje potrebe. Interesantno je da čak i kompanije koje se bave zaštitom ne vide ništa loše u tome da se ovakvi sertifikati koriste u sistemima u kojima se zahteva visok stepen bezbednosti. Najveći problem kod samopotpisanih sertifikata jeste to što Web pretraživač daje upozorenje da lokacija na kojoj se koristi ovakav sertifikat nije preporučljiva za korišćenje. Ukoliko žele da budu shvaćeni ozbiljno security provajderi treba da izbegavaju ovakvu vrstu sertifikata.

Rešenje predstavlja korišćenje kvalifikovanih elektronskih sertifikata koje izdaju ovlašćena sertifikaciona tela engleski Certification Authority (CA) koja mogu biti nacionalna ili međunarodna. Elektronski sertifikat je elektronski dokument kojim se potvrđuje veza između podataka za proveru elektronskog potpisa i identiteta potpisnika. Kvalifikovani elektronski sertifikat je elektronski sertifikat koji je izdat od strane sertifikacionog tela za izdavanje kvalifikovanih elektronskih sertifikata i sadrži podatke predviđene ovim zakonom.

Kvalifikovani elektronski sertifikat¹⁰ je elektronski sertifikat koji izdaje sertifikaciono telo za izdavanje kvalifikovanih elektronskih sertifikata i koji mora da sadrži:

- oznaku o tome da se radi o kvalifikovanom elektronskom sertifikatu;
- skup podataka koji jedinstveno identifikuje pravno lice koje izdaje sertifikat;
- skup podataka koji jedinstveno identifikuje potpisnika;
- podatke za proveru elektronskog potpisa, koji odgovaraju podacima za izradu kvalifikovanog elektronskog potpisa a koji su pod kontrolom potpisnika;
- podatke o početku i kraju važenja elektronskog sertifikata;
- identifikacionu oznaku izdatog elektronskog sertifikata;
- kvalifikovani elektronski potpis sertifikacionog tela koje je izdalo kvalifikovani elektronski sertifikat;
- ograničenja vezana za upotrebu sertifikata, ako ih ima.

Na elektronskim sertifikatima bilo da su kvalifikovani ili ne nalazi se elektronski potpis vlasnika sertifikata. Elektronski potpis je skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa elektronskim dokumentom i koji služe za identifikaciju potpisnika. Kvalifikovani elektronski potpis je elektronski potpis kojim se pouzdano garantuje identitet potpisnika, integritet elektronskih dokumenata, i onemogućava naknadno poricanje odgovornosti za njihov sadržaj, i koji ispunjava uslove utvrđene zakonom. Kvalifikovani elektronski potpis u odnosu na podatke u elektronskom obliku ima isto pravno dejstvo i dokaznu snagu kao i svojeručni potpis, odnosno svojeručni potpis i pečat, u odnosu na podatke u papirnom obliku. Kvalifikovani elektronski potpis, mora da zadovolji sledeće uslove:

- isključivo je povezan sa potpisnikom
- nedvosmisleno identifikuje potpisnika
- nastaje korišćenjem sredstava kojima potpisnik može samostalno da upravlja i koja su isključivo pod nadzorom potpisnika
- direktno je povezan sa podacima na koje se odnosi, i to na način koji nedvosmisleno omogućava uvid u bilo koju izmenu izvornih podataka

¹⁰ Zakon o elektronskom potpisu

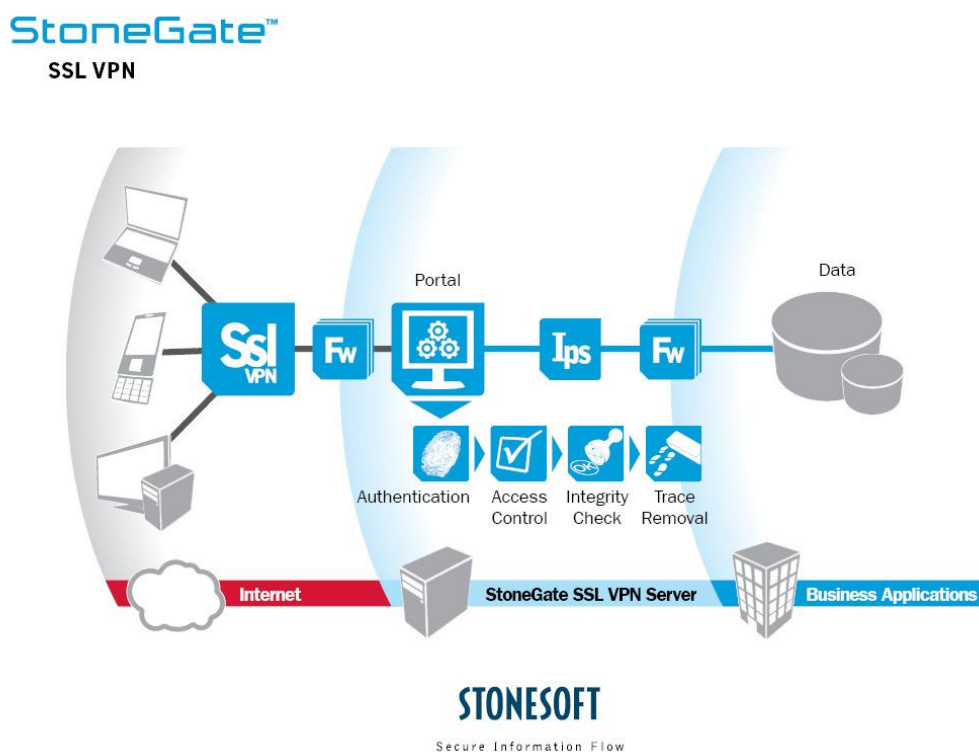
- formiran je sredstvima za formiranje kvalifikovanog elektronskog potpisa
- proverava se na osnovu kvalifikovanog elektronskog sertifikata potpisnika

Suštinska razlika između elektronskog potpisa i kvalifikovanog elektronskog potpisa je u tome što kvalifikovani elektronski potpis ima snagu svojeručnog potpis i njegova zloupotreba povlači krivičnu odgovornost. Psihološki efekat koji kvalifikovani elektronski potpis ostavlja na korisnika veoma je važan. Kada korisnik zna kakve posledice mogu da nastanu zbog zloupotrebe ili nemarnog korišćenja kartice na kojoj se nalazi kvalifikovani elektronski potpis biće mnogo oprezniji u rukovanju sa njom. Ukoliko neko korisniku ukrade karticu, ukoliko korisnik izgubi karticu ili je kompromituje na bilo koji drugi način dužan je da o tome odmah obavesti security provajdera ili izdavaoca smart kartice kao bi je oni proglasili nevažećom.

8. Bezbedna komunikacija

Kao što je već istaknuto virtualne privatne mreže obezbeđuju zaposlenima koji nisu u svojim kancelarijama da na bezbedan način pristupaju kompanijskoj mreži preko Interneta šifrujući pritom saobraćaj koji se odvija između mreže i korisničke mašine odnosno klijenta. Uređaji koji su se ranije koristili za bezbednu komunikaciju zvali su se VPN koncentratori i oni su radili sa IPsec protokolom. Ovakvi uređaji se koriste i danas a komunikacija preko njih zahteva da na klijentskom računaru bude instaliran specifičan softver koji se zove VPN klijent. Za razliku od klasičnog VPN-a zasnovanog na IPsec protokolu, SSL VPN je konstruisan tako da nema potrebe za posebnim podešavanjem korisničkih računara. Bilo koji računar koji ima Web pretraživač može bez problema da pristupa SSL VPN mreži.

Korisnici mogu bezbedno da pristupaju kompanijskoj mreži sa bilo kog računara bilo da je to računar na javnom mestu, laptop računar ili čak mobilni telefon. SSL VPN je multifunkcionalni višenamenski uređaj¹¹, a o nekim od njegovih mnogobrojnih funkcionalnosti biće više reči u ovom poglavlju. Jedna od funkcija je da bude gateway i da obezbedi korisnicima koji dolaze spolja pristup unutrašnjim servisima kao što je fajl server, e-mail server kao i Web orijentisanim aplikacijama koje su šifrovane korišćenjem SSL protokola. Mnoge poznate svetske kompanije prilagođavaju svoja rešenja zahtevima SSL VPN tehnologija koje se sve više razvijaju.



Slika 10 SSL VPN uređaj

¹¹ Joseph Steinberg and Tim Speed, Understanding SSL VPN, Packt Publishing, 2005.

U ovom poglavlju detaljnije će biti objašnjeno kako funkcionišu SSL VPN uređaji i biće prikazani njihove prednosti i nedostaci. Biće posvećena posebna pažnja i korisnicima koji predstavljaju vitalni element sigurnosti. Takođe biće reči i o strategiji za jednostavan pristup aplikacijama i fajlovima koji se nalaze u kompanijskoj mreži. Takođe ukoliko je potrebno obezbediti pristup iz udaljene kancelarije može se izbeći dodatni VPN uređaj u toj kancelariji. Korisnici, naročito ukoliko ih je manje mogu da pristupaju SSL VPN-u koristeći jeftin uređaj kao gateway ili pojedinačno koristeći pogodnosti modernog Interneta. Ne treba zanemariti troškove za radne sate administratora koji često mora da podešava nestabilnu infrastrukturu klasičnih VPN mreža. Kao predlog dobre organizacije SSL VPN mreže može se reći da ona treba da sadrži sledeću hardversku infrastrukturu:

- SSL VPN appliance
- Server za autentifikaciju (RADIUS, LDAP, Active directory)

8.1. SSL VPN uređaj

Sve više poznatih proizvođača mrežne opreme nudi specijalizovane hardverske uređaje za SSL VPN mreže. Oni su različitih performansi i karakteristika ali je zanimljivo istaći da pored osnovne uloge da zatvaraju VPN konekcije odnosno da budu VPN koncentratori imaju i mnoge dodatne pogodnosti. Te pogodnosti koje nude usko su povezane sa sve dinamičnijim razvojem računarskih mreža, virtualnih privatnih mreža, a posebno sa razvojem Interneta koji nudi dosada nezamislive mogućnosti.

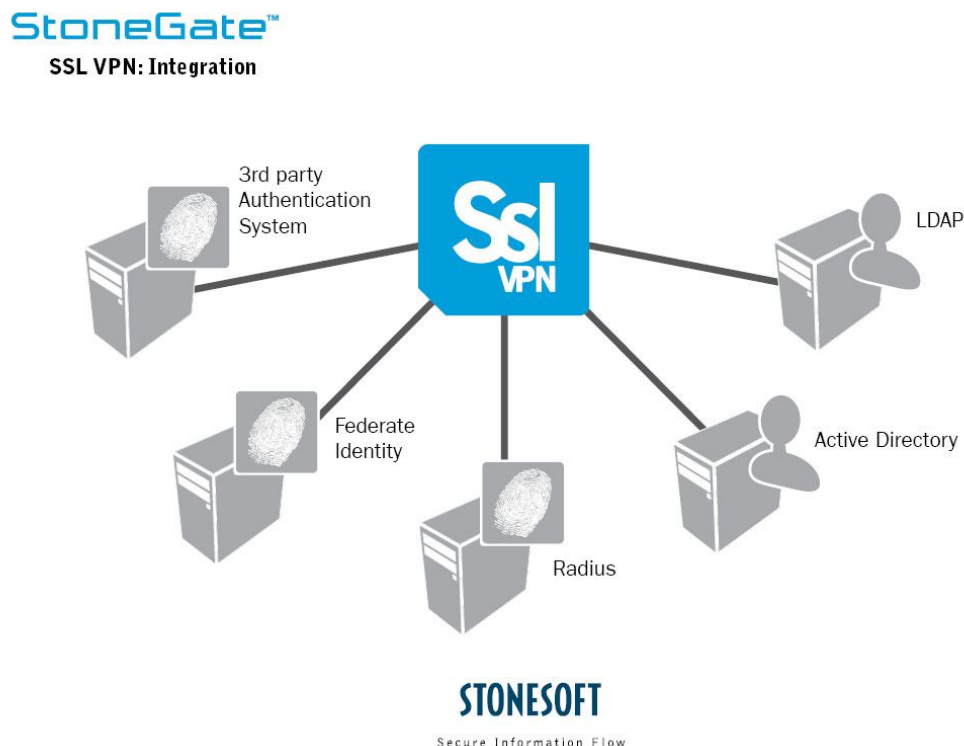
Kao što je već rečeno SSL VPN uređaj je višenamenski hardverski ili virtualni uređaj koji osigurava bezbednu kontrolu pristupa i bezbednu komunikaciju do lokalne mreže odnosno namenskog ili cloud servera. Ovi uređaji imaju sopstveni operativni sistem što im pruža mogućnost da se koriste bilo u Windows ili Linux okruženju. SSL VPN uređaj može da ima neke od sledećih funkcionalnosti:

- Rad sa digitalnim sertifikatima (samopotpisanim ili sertifikatima drugih CA)
- Revers proxy
- Split tunneling
- Mrežni firewall
- Application firewall
- Intrusion prevention system
- Ddos protection
- Load balancing
- Rad sa grupnim polisama
- Kontrola radne stanice sa koje korisnik pristupa (verzija operativnog sistema, antivirus)

Za ostvarivanje bezbedne komunikacije između klijentskih radnih stanica i udaljenih servera korišćenjem security servisa nisu potrebne sve navedene funkcionalnosti. Ono što je neophodno da bi security servis upšte mogao da funkcioniše jeste mogućnost SSL VPN uređaja da radi sa digitalnim sertifikatima. Kao što je poznato ovaj zahtev se prosleđuje sertifikacionom telu koje izdaje digitalni sertifikat koji se zatim prenosi na uređaj. Ova mogućnost pruža ozbiljnu prednost prilikom konfigurisanja virtualne privatne mreže, jer više nije potrebno da se request generiše na posebnom Web serveru već SSL VPN uređaj postaje uslovno rečeno Hardware Security Modul (HSM). To podrazumeva da se tajni ključ

serverskog sertifikata čuva na specijalizovanom hardverskom uređaju u koga napadači veoma teško mogu da uđu.

Što se tiče rada sa grupnim polisama one mogu da se čuvaju u samom uređaju mada postoji i varijanta da im se pristupa kroz LDAP, Aktivni direktorijum ili preko RADIS servera.



Slika 11 SSL VPN integracija

Antivirus, antispam, anti phishing zaštita funkcioniše tako što je SSL VPN neprekidno povezan sa podrškom kompanije čiji je proizvod u pitanju i koja redovno prati i otkriva nove definicije zlonamernog koda i generiše mehanizme za zaštitu od njih.

Web Application Firewall integrisan na ovaj uređaj obezbeđuje odbranu od najčešćih napada koji Web aplikacijama prete preko Interneta. Najčešće to podrazumeva zaštitu od DoS ili DDoS napada, SQL injection napada, CSS napada kao i mnogih drugih pretnji koje mogu da ugroze Web aplikacije. Web Application Firewall funkcioniše tako što je neprekidno povezan sa podrškom kompanije čiji je proizvod u pitanju i koja redovno prati i otkriva nove definicije zlonamernog koda i generiše mehanizme za zaštitu od njih.

Reverse proxy je proxy server koji radi u ime nekog mrežnog servera. Najčešće korišćenje reversnog proxy-ja je da se zaštiti Web server. Kada korisnik na Internetu zahteva podatke od Web servera koji je zaštićen reversnim proxy serverom, reverse proxy presreće zahtev i proverava da li su podatci sadržani u zahtevu prihvatljivi, i da ne sadrže neke ne-HTTP podatke ili neke maliciozne HTTP komande. Ovo obezbeđuje da korisnici na Internetu nikada ne pristupaju direktno Web serveru.

Postoji nekoliko tipova SSL VPN-a čije će karakteristike ovde biti detaljnije opisane. Dva glavna tipa SSL VPN-a su:

- SSL portal VPN
- SSL tunnel VPN

Takođe, postoji i treći tip koji se zove SSL gateway-to-gateway VPN koji se primenjuje u pojedinim implementacijama. On se retko koristi jer ima slične karakteristike kao IPsec VPN ali je manje fleksibilan pa se zbog toga ovde neće detaljnije opisivati.

Oba glavna tipa SSL VPN mreža se koriste da bi se obezbedio pristup za udaljene korisnike brojnim servisima koje kontroliše i kojima upravlja SSL VPN uređaj. U zavisnosti od potreba korisnika treba obezbediti optimalno rešenja jer oba pristupa imaju svoje prednosti i nedostake.

8.1.1. SSL portal VPN

SSL portal VPN dozvoljava korisnicima da koristeći standardnu SSL konekciju bezbedno pristupaju brojnim mrežnim servisima. Ovaj pristup se naziva SSL portal VPN zato što se preko jedne Web stranice pristupa svim ostalim resursima. Ova vrsta SSL VPN-a radi u transportnom sloju preko posebnog mrežnog porta čiji je pun naziv TCP port za SSL-protected HTTP (443).

Udaljeni korisnici pristupaju na SSL VPN gateway koristeći bilo koji od postojećih Web pretraživača gde se autentifikuju metodom koju taj gateway podržava. Nakon toga prikazuje im se Web stranica koja predstavlja portal prema drugim servisima. Ovi servisi mogu da budu linkovi prema Web serverima, deljenim direktorijumima sa datotekama, Web-based email sistemima, aplikacijama koje su pokrenute na zaštićenim serverima kao i svemu ostalom čemu se može pristupiti preko Web stranice.

Da bi pristupili SSL portal VPN-u korisnici unose u Web pretraživač URL portala na koji žele da se konektuju na isti način kao kada pristupaju bilo kom drugom Web sajtu. Ovaj URL najčešće koristi https šemu koja odmah startuje SSL konekciju, ali mnogi SSL VPN-ovi dozvoljavaju korisnicima da prvo pristupe portalu koristeći http URL, a da zatim budu redirektovani na bezbedan SSL port.

SSL portal VPN-ovi rade sa Web pretraživačima bez obzira na to da li Web pretraživač dozvoljava ili podržava aktivan sadržaj. Zbog toga je SSL portal VPN pogodniji za pristup većem broju korisnika nego što je to SSL tunnel VPN. Kada korisnik treba da pristupi nekoj Web aplikaciji gde se zahteva veća sigurnost SSL portal VPN nije preporučljiv.

8.1.2. SSL tunnel VPN

SSL tunnel VPN dozvoljava korisnicima da koristeći običan Web pretraživač bezbedno pristupaju brojnim servisima kroz tunel koji je pokrenut preko SSL-a. On zahteva da Web pretraživač podržava specifične tipove aktivnog sadržaja (Java, JavaScript, Flash ili ActiveX) kojima korisnik može da upravlja. Većina Web pretraživača koji podržavaju ove aplikacije takođe dozvoljavaju korisnicima ili administratorima da blokiraju njihovo izvršenje.

Kada se govori o SSL tunnel VPN-u pojam „tunnel“ ima sličnosti ali i razlike sa istim pojmom u IPsec VPN-u. Sličnost je u tome što je ceo IP saobraćaj potpuno zaštićen tunelom i na taj način korisniku je omogućeno da na bezbedan način pristupa željenim mrežnim servisima. Razlika je u tome što je SSL VPN tunel kreiran preko SSL-a i ne koristi iste protokole za tunelovanje kao IPsec. Kada se koristi SSL tunnel VPN neophodno je da se na

klijentskoj strani instalira plug-in koji omogućava uspostavljanje tunela između klijenta i SSL VPN gateway-a. Ovakav plug-in može da se instalira unapred ili prilikom povezivanja Web pretraživača sa SSL VPN uređajem. Najčešće se kao plug-in koristi ActiveX kontrola ali je problem u tome što ona može pouzdano da se koristi samo kroz Internet Explorer. Drugo rešenje predstavlja plug-in koji je napravljen kao Java Applet i koji može da radi na bilo kom Web pretraživaču.

9. Zaštita kao servis

Kao što je već rečeno bezbednost savremenih računarskih mreža nezamisliva je bez korišćenja specijalizovanih višenamnskih mrežnih uređaja koji se zovu SSL VPN uređaji. To su u najvećem broju slučajeva fizički odnosno hardverski uređaji mada se sa razvojem virtualizacije na tržištu pojavljuje sve veći broj virtualnih SSL VPN uređaja. Zbog svoje multifunkcionalnosti oni uspešno mogu da se koriste za zaštitu lokalne mreže ali i za neke druge namene o čemu će ovde biti više reči.

U svetu već postoje provajderi koji prodaju uslugu koja bi mogla da se nazove security kao servis. Većina provajdera međutim, nudi ovaj servis samo u slučaju da se i ostali servisi nalaze kod njih. Ovo je u suprotnosti sa suštinom Cloud computinga koja pretpostavlja da servisi koje koristi neka kompanija mogu da se nalaze bilo gde pa samim tim i kod različitih provajdera. Ukoliko je podela odgovornosti između provajdera precizno definisana nema razloga da se kupcu ne dozvoli mogućnost izbora. Ovo naravno ne znači da ne postoje provajderi kod kojih može da se dobije samo usluga security servisa ali ovde treba biti oprezan s obzirom da ova usluga ne spada u njihovu standardnu ponudu. Kod nas ne postoje ovakvi servisi, a ovaj rad bi trebalo da pomogne u tome da se sagledaju mogućnosti primene ovakvih rešenja.

Bezbednost informacionih sistema najrazvijenija je u velikim kompanijama i bankama. Ove institucije ulažu velika sredstva u bezbednost svojih informacionih sistema jer bi svaki propust mogao ozbiljno da kompromituje njihovo poslovanje. Međutim postoje i kompanije koje ne mogu sebi da priušte velike budžete za zaštitu svojih informacionih sistema. Rešenje bi mogli da predstavljaju security provajderi odnosno kompanije koje bi usluge bezbednosti pružale drugim kompanijama.

9.1. Osnovne karakteristike

Pre detaljnijeg opisa security sistema treba reći nekoliko reči o podeli odgovornosti s obzirom da se radi o osetljivoj stvari kao što je bezbednost. Svaki informacioni sistem pored hardvera i softvera čine i ljudi što se u praksi ponekad zaboravlja. Veoma je važno precizno definisati ulogu svakog pojedinca ili kompanije koja učestvuje u projektovanju nekog informacionog sistema. Kompanije se sve više odlučuju za outsorsing rešenja koja kupuju ili iznajmljuju od jedne ili više kompanija. Da bi se izbegli ozbiljni problemi koji mogu da nastanu prilikom eksploatacije sistema neophodno je da se definišu obaveze kompanije koja je kupac kao i da se razdvoje obaveze svake outsorsing kompanije koja učestvuje u ovom procesu. Zbog svega toga neophodno je da security servis odnosno ono što on podrazumeva bude precizno definisan i odvojen od drugih procesa. Pre svega treba odrediti granice u kojima je security servis odgovoran što nije nimalo lako s obzirom da se preko njega odvija čitav proces komunikacije.

Ovaj proces započinje još na klijentskom računaru, a ono što security provajder bezuslovno treba da zahteva jeste da se autentifikacija obavlja isključivo uz pomoć smart kartica ili tokena. Korišćenje bilo kog drugog načina autentifikacije nije bezbedan i mogao bi provajderu security servisa da stvori nepotrebne probleme. Na taj način definiše se precizna podela odgovornosti na klijentskoj strani. Posao security provajdera ne treba mešati sa poslom

administratora lokalne mreže koji bi po definiciji trebalo da vodi računa o tome da li korisnici lokalne mreže pravilno koriste svoje radne stanice. Security provajder mora da pođe od pretpostavke da je moguće da udaljenim servisima prilazi i neko čiji računar nije u lokalnoj mreži odnosno neko ko se sam stara o svom računaru iako za to nema potrebno znanje.

Kada je reč o serverskoj strani situacija je nešto drugačija. Kompanija koja pruža security servis odnosno security provajder treba pre svega da pronađe provajdera koji je pouzdan i kod koga može bez ograničenja i uslovljavanja da iznajmi hardverske resurse za instaliranje neophodne infrastrukture za svoj security servis. Kada to uradi security provajder bi usluge svog security servisa iznajmljivao drugim kompanijama, koje bi ga koristile kao siguran kanal do svojih udaljenih servisa.

Ukoliko se na udaljenom serveru nalaze Web aplikacije dobro bi bilo uključiti opciju za Web application firewall koju ima većina SSL VPN uređaja. Međutim, ukoliko se na udaljenom serveru nalazi neki fajl server ili DMS neophodno je uključiti i namenski uređaj za antivirus zaštitu. Takođe, treba reći da SSL VPN uređaji pružaju i zaštitu od Ddos napada ali se preporučuje da se za tu namenu iskorisiti zaštita koju kao servis pruža sam provajder jer se ona smatra mnogo efikasnijom. Ovde neće biti detaljnije opisivana rešenja pojedinih proizvođača SSL VPN uređaja jer svi oni nude uz svoje proizvode odlične vodiče uz pomoć kojih svako ko dobro poznaje računarske mreže može lako da ih konfiguriše i pusti u rad. Važno je još napomenuti da security servis podrazumeva postojanje redundantnih SSL VPN uređaja zbog osetljivosti servisa koji se na njima hostuju. Ovakav način hostovanja poznatiji je kao High-availability clusters.

High-availability clusters (HA Clusters ili Failover Clusters) su računarski klasteri koji se koriste za obezbeđivanje neprekidne dostupnosti servisima koji se na tom klasteru izvršavaju. Klasteri funkcionišu tako što se u njima nalaze redundantni računari ili nodovi koji služe da obezbede servis ukoliko jedan od računara u klasteru otkáže. Ukoliko se računari ne nalaze u klasteru svako otkazivanje dovodi do prekida rada sve dok se računar ponovo ne stavi u funkciju. HA klastering prevazilazi ovakve situacije tako što detektuje otkazivanje hardverskih ili softverskih komponenti i odmah pokreće servis na drugom računaru u klasteru bez bilo kakve intervencije administratora. Ovaj proces se naziva Failover. Kao deo ovog procesa softver za klasterizaciju mora da konfiguriše nod pre nego što se na njemu pokrene aplikacija.

HA klasteri se najčešće koriste za kritične baze podataka, deljenje fajlova preko mreže, poslovne aplikacije kao i za Web sajtove za elektronsku trgovinu. Korošćenje HA klasteringa za obezbeđivanje neprekidne dostupnosti security servisa je neophodno jer su ovi servisi najosetljiviji deo sistema i nikako ne bi bilo dobro da iz bilo kog razloga ne budu dostupni.

9.2. Zaštita na serverskoj strani

Komunikacija između klijenta i servera na kome se nalaze servisi korišćenjem security servisa odvija se kroz dva koraka. Prvo treba obezbediti komunikaciju između klijentske radne stanice i SSL VPN uređaja security provajdera što je lakši deo. Mnogo je komplikovanije uspostaviti bezbednu komunikaciju između SSL VPN uređaja i servera na kome se nalaze servisi kojima korisnik želi da pristupi. Kada se kaže da je komplikovanije uspostaviti komunikaciju između SSL VPN uređaja i udaljenog servera tu se ne misli na tehnički aspekt koji je u suštini veoma jednostavan. Ovde se pre svega komplikovano to što korisnici a i neki provajderi još uvek nemaju predstavu o tome na koji način ovakav servis opšte može da funkcioniše i da bude isplativ.

Na početku treba reći nekoliko reči o udaljenim servisima kojima zaposleni iz neke kompanije treba da pristupe. Ovde će se pre svega razmatrati bezbedan pristup poslovnim Web aplikacijama jer ove servise iznajmljuje najveći broj kompanija. Koristeći poslovne aplikacije kompanije treba svoje poverljive podatke kao što su podaci o zalihama ili neki finansijski podaci da preko Interneta pošalju na neku udaljenu lokaciju. Ovakav način rada predstavlja veliki rizik za kompaniju koja je vlasnik tih podataka.

Neke kompanije koje se bave razvojem Web aplikacija koje svojim klijentima prodaju kao servise nude neku vrstu zaštite svojih aplikacija. Oni garantuju pre svega stalnu dostupnost servisima kao i šifrovanu komunikaciju od klijenta do servera na kome se nalaze servisi uz pomoć SSL protokola. Naravno postoji i veliki broj onih kompanija koje svoje Web aplikacije nude kao servis bez bilo kakve zaštite bilo iz razloga da ne žele time da se bave ili da za to nemaju neophodan stručni kadar.

Za oba ova slučaja dobro bi bilo da kompanija koja kupuje Web aplikaciju kao servis pronađe security provajdera preko čijeg će zaštićenog kanala slati svoje podatke do udaljenih servera. Najbolje bi bilo da to bude lokalni provajder sa kojim može da se dogovori oko eventualnih specifičnih zahteva. Kompanije koje pružaju ovakvu vrstu usluga ne postoje kod nas ali je nekoliko njih zainteresovano da razvije ovaj servis jer i oni uviđaju da će za ovom vrstom usluga biti sve veća potražnja.

Što se tiče tehničkih karakteristika ovog servisa kao što je već rečeno one nisu preterano komplikovane za podešavanje. Korišćenjem nekih preduslova koje provajderi već nude kao uslugu SSL VPN uređaj može da se podesi za pristup udaljenim serverima. Pre svega, namenski server na kome se nalaze servisi kojima se pristupa mora da ima javnu IP adresu. Takođe, treba tražiti od provajdera da u svojim access listama omogući da ta javna IP adresa bude vidljiva samo sa IP adrese na kojoj se nalazi SSL VPN uređaj security provajdera. Na ovaj način udaljeni server postaje deo VPN mreže i može mu se bezbedno pristupati. Ovo se veoma jednostavno dogovara sa provajderom i ne iziskuje nikakve dodatne troškove za korisnika. Takođe se može definisati da se udaljenom serveru pristupa samo preko porta 443 što omogućava bezbednu komunikaciju preko SSL protokola.

Ovakav security servis pruža mogućnost pristupanja udaljenim servisima nezavisno od proizvođača ili od provajdera kod koga se ti servisi hostuju. Ekonomski interes za provajdere koji bi nudili security servis i za servere koji se ne nalaze kod njih mogao bi da bude veliki broj manjih kompanija koje bi mogle da ga koriste. Veliki broj korisnika servisa doveo bi do njegovog pojeftinjenja što svakako pokazuje da razvoj ovakvog servisa nije uzaludan posao.

9.3. Zaštita na klijentskoj strani

Što se tiče security servisa na klijentskoj strani najvažnije je da se obezbedi jednostavna instalacija neophodnog softvera i da se pojednostavi podešavanje neophodnih komponenti za pristup SSL VPN uređajima. Uz minimalnu obuku bilo koji korisnik može samostalno da uradi sve što je neophodno da bi svoj uređaj podesio za bezbednu komunikaciju.

Kao što je već rečeno osnovna prednost SSL pristupa u odnosu na IPsec pristup VPN mreži je u tome što preko SSL-a korisnik može da pristupa VPN mreži sa bilo koje lokacije. Ovo predstavlja veliki konfor za korisnika ali stvara dodatne probleme security provajderima. Prosečan korisnik računara zna veoma malo o opasnostima koje vrebaju sa Interneta tako da njegov računar može da postane meta napadača, a da on toga nije ni svestan. Za programe kao što je na primer keylogger koji je pogodan za krađu korisničkog imena i lozinke korisnici

često nisu ni čuli. Socijalni inženjering koji se ispoljava kroz phishing, spear phishing i pharming takođe predstavlja ozbiljnu pretnju za korisnike Interneta.

Security provajder mora precizno da definiše svoju odgovornost na klijentskoj strani. Ovo se pre svega odnosi na način autentifikacije klijenta na SSL VPN uređaj. Iako ovi uređaji podržavaju autentifikaciju uz pomoć korisničkog imena i lozinke security provajderi ovakvu mogućnost uopšte ne treba da razmatraju. Oni treba da insistiraju na autentifikaciji jedino uz pomoć smart kartica ili USB tokena.

10. Zaštita udaljenih servisa

Ovde će biti opisana neka zanimljiva rešenja koja bi mogla da pruže uvid kompanijama u to kakve im sve mogućnosti stoje na raspolaganju. Čak i gigant kakav je Microsoft svoje nove proizvode užurbano prilagođava novim tendencijama poslovanja. To se pre svega odnosi na Office, Microsoft-ov proizvod koji je verovatno najrasprostranjeniji u svetu. Microsoft nudi ovakav servis kao pandan za Google apps za fizička lica potpuno besplatno. Za kompanije bi moglo da bude rešenje da uz Windows server 2008 koji može da se iznajmi u Cloud-u na njega dodaju dodaju Share point foundation i Office Web app (ove komponente su besplatne ukoliko korisnik ima licencu za Windows 2008). One omogućavaju korisnicima da preko Web pretraživača pristupaju Office aplikacijama iako nemaju instaliran Office na svojim radnim stanicama. Microsoft će uskoro izaći na tržište i sa novim integrisanim proizvodom koji se zove Office 365 što pokazuje jasne namere ove kompanije da želi sve više da ulaže u ovu oblast.

Pored Office i Google apps aplikacija, koje su interesantne najvećem broju korisnika, preko Web pretraživača može na isti način da se pristupa i drugim aplikacijama bilo da ih je kompanija kreirala samo za sebe ili je iznajmila neke već postojeće. Software as a Service mogao bi da nađe primenu u sledećim oblastima:

- Poslovni informacioni sistem
- Edukacija
- Document Management System

10.1. Poslovni informacioni sistem

Kada se govori o poslovnom informacionom sistemu koji se može ponuditi kao servis pre svega se misli na aplikacije za vođenje knjigovodstva. Na tržištu postoji bezbroj dobrih ili manje dobrih rešenja. Svi ovi programi rade uglavnom pod Windows operativnim sistemom kao desktop ili client - server aplikacije. To i jeste njihov glavni nedostatak.

One su veoma komplikovane za instalaciju kod korisnika dok se za programiranje obično koristi Microsoft .NET platforma, a za pokretanje aplikacija na klijentskoj strani neophodan je .NET framework čije nove verzije Microsoft objavljuje veoma često. Neke od ovih aplikacija su napravljene tako da svaka promena verzije framework-a zahteva kompletnu reinstalaciju programa kod korisnika što podrazumeva zastoj u radu i druge probleme. Kao što je već rečeno to su uglavnom client – server aplikacije koje su spore ukoliko se radi o udaljenom serveru pa korisnici na odziv čekaju dugo što je neugodno ukoliko neki upit iz baze podataka treba da predaju klijentu koji stoji ispred njih.

U razvijenim zemljama ovakve aplikacije odavne se nude kao servis preko Interneta. Korisnik više ne mora da brine o instalaciji aplikacije, njenim verzijama ili tehničkoj podršci. Aplikacija je instalirana na Web serveru i brzo i lako joj se pristupa sa bilo koje lokacije. Njeno održavanje je jednostavno jer programer sada ima aplikaciju samo na jednom mestu što mu značajno olakšava posao. Ovakve aplikacije za sada ne postoje u Srbiji ali se njihov razvoj najavljuje.

Bezbedna komunikacija između udaljenog korisnika i ovakve aplikacije je od ključne važnosti. Ukoliko se pođe od pretpostavke da je provajder koji hostuje aplikaciju pouzdan ostaje samo da se uz pomoć SSL protokola odnosno korišćenjem digitalnog sertifikata obezbedi pre svega sigurna komunikacija, a uz pomoć digitalnog potpisa da podaci koji su uneti ne mogu biti promenjeni, što je za rad sa finansijskim podacima od ključne važnosti. Korišćenje PKI infrastrukture u Web aplikacijama za knjigovodstvo svakako bi veoma doprinelo tome da korisnici ne brinu o tome da li su njihovi podaci bezbedni iako se ne nalaze u kompaniji. Treba istaći da će ovakve aplikacije u budućnosti biti dominantne na tržištu i da je neophodno da se paralelno sa njihovim razvojem mora ulagati i u njihovu bezbednost.

10.2. Edukacija

Edukacija podrazumeva pre svega novi i sve popularniji servis koji se zove e-learning. Ovaj servis se sve više koristi i u našoj zemlji i pokazao se kao odlična alternativa tradicionalnom načinu učenja. Nastavni materijali, predavanja, online testovi i ostale pogodnosti koje pruža ovakav servis sada su postali dostupni korisnicima sa bilo koje lokacije pod uslovom da postoji brza Internet konekcija. Ideja je da pored online predavanja studenti mogu da polažu i online testove ili od svojih kuća ili u nekoj specijalizovanoj učionici. Ukoliko bi se polagali u tačno dogovoreno vreme i bili vremenski ograničeni studenti ne bi mogli međusobno da se dogovaraju čak iako ih niko ne kontroliše. Testovi koji se polažu preko Interneta trebalo bi svakako da budu digitalno potpisani od strane učenika ili studenta čime bi se izbegla svaka eventualna zloupotreba.

Zbog značajnog smanjenja troškova koje obezbeđuje proces učenja na daljinu razmatra se mogućnost širenja i na ostale aspekte obrazovnog sistema. Postojeće mogućnost, a jedan takav projekat je sada u pilot fazi, da roditelji imaju potpun uvid u ocene kao i u izostanke svoje dece iz škole. Takođe se razmatra mogućnost ocenjivanja testova preko Interneta. Ocenjivanje bi vršili pre svega nastavnici, profesori i mentori mada modernizacija nastave podrazumeva da i nastavni kadar može da bude ocenjivan od strane učenika ili studenata.

Proces ocenjivanja je svakako najosetljiviji deo ovog sistema jer bi svaka zloupotreba mogla dovesti do kompromitovanja samog sistema kao i pojedinaca koji na njemu rade. Najbolji način da se proces ocenjivanja preko Interneta učini bezbednim jeste da se koriste smart kartice za autentifikaciju i pristup sistemu. Takođe, smart kartice bi se koristile i za digitalno potpisivanje elektronskih dnevnika što bi uticalo na to da je praktično nemoguće da neko izmeni ocenu, a da to ne bude primećeno. Naravno elektronski dnevnici trebalo bi da se nalaze na dobro zaštićenim serverima, a njihovu izradu treba poveriti proverenoj kompaniji koja razume potrebu za pisanjem bezbednih Web aplikacija.

10.3. Document Management System

Document Management System (DMS) je platforma koja u osnovi predstavlja centralizovano skladište sadržaja (svih vrsta fajlova: word, excel, zvučnih i video zapisa itd.) nad kojima se mogu izvršavati radni tokovi kao deo poslovnih procesa, uz poštovanje svih internih i eksternih pravila i propisa (prava pristupa podacima, menjanja sadržaja, odobravanja, objavljivanja itd.).

Centralnom skladištu je moguće pristupiti na više načina:

- kroz web interfejs

- kao windows deljeni disk (CIFS)
- kroz namenski pisane aplikacije
- Web servise
- WebDAV
- FTP
- NFS

Pri svakom od ovih načina pristupa poštuju se ugrađena pravila za radne tokove i prava pristupa. Čuvanje sadržaja u centralnom skladištu (koje može da bude na više lokacija ali ga korisnici vide kao jedan) donosi višestruke prednosti, koje se pre svega ogledaju u bezbednosti sadržaja (kvar radne stanice ne dovodi do gubitka podataka, prava pristupa su nad celim sistemom), jednostavnog i veoma efikasnog pretraživanja sadržaja (sadržaji se ne pretražuju samo po meta podacima kao što je naziv fajla, već i po samom sadržaju, bez obzira da li je to word, excel ili powerpoint) kao i njenoj trenutnoj dostupnosti (ne mora se tražiti slanje sadržaja od korisnika koji je taj sadržaj napravio ili trenutno poseduje). Druge funkcionalnosti u vezi sa upravljanjem sadržaja koje poseduje DMS platforma su automatsko čuvanje svih verzija nekog sadržaja fajla (versioning), rad više korisnika na jednom sadržaju (colaboration), kao i mehanizam za sprečavanje slučajnog brisanja sadržaja (undelete).

Kao što je već rečeno u slučaju Web aplikacija podaci koji se unose preko Web forme na klijentskom računaru bezbednim kanalom putuju do servera. Slično je i sa fajlovima koji se nalaze na namenskim serverima ili cloud serverima. Bilo da se radi o običnim fajl serverima ili o DMS-u potrebno je da se uspostavi bezbedan kanal kroz koji će ti podaci prolaziti. Takođe, komunikacija između Web pretraživača i DMS-a obavlja se posredno što omogućava da server na kome se nalazi DMS ostane nevidljiv za korisnika.

10.4. Dodatna zaštita

Kako je već rečeno osim bezbedne komunikacije između klijentskog računara i udaljenog servera veoma je važno da se pristup aplikacijama, kao i same aplikacije osiguraju na neki način. Podaci koji se obrađuju uz pomoć ovakvih aplikacija veoma su osetljivi za kompaniju ili neku obrazovnu instituciju. Već smo rekli da se kod aplikacija za poslovni informacioni sistem radi pre svega o knjigovodstvu. Zamislimo da jedan takav podatak kao što je završni račun neke kompanije bude kompromitovan na bilo koji način. Kakav bi tek problem mogao da nastane ukoliko bi neko za drugoga polagao testove ili još gore menjao ocene u nekom online dnevniku.

Sve ovo može da se spreči korišćenjem smart kartica koje na sebi imaju kvalifikovani digitalni sertifikat čija zloupotreba za sobom povlači krivičnu odgovornost. Kada knjigovođa digitalno potpiše završni račun ili student digitalno potpiše svoj test oni su potpuno mirni jer znaju da te podatke više niko ne može da promeni. S druge strane ne postoji mogućnost poricanja da su određeni dokument potpisali baš oni.

U oba ova slučaja interesantno je da se ne radi o direktnom potpisivanju dokumenata već se to čini na posredan način. Kao što je rečeno radi se o aplikacijama odnosno o Web formama kroz koje se podaci unose. To zahteva dodatne alate koji se koriste da bi se od forme napravio PDF dokument koji se zatim lako može potpisati. Evo nekoliko primera:

- Korišćenje komercijalnih biblioteka za JavaScript koje se koriste za generisanje PDF dokumenta, a prednost ovakvog rešenja je što se ono kompletno odvija na klijentskoj strani.

- Konvertovanje na serverskoj strani uz pomoć PHP skripta ili Java aplikacije što podrazumeva da je obezbeđen pouzdan kanal koji omogućava da se Web forma bezbedno prosledi do servera, a generisani dokument bezbedno poslati do klijentskog računara na kome treba da bude potpisan
- Za konvertovanje se koristi Java Applet koji preuzimanje Web forme i njeno prevođenje u PDF dokument obavlja na klijentskoj strani ali je potrebno da se za svaku različitu Web formu napravi poseban Java Applet

Svaka od ovih varijanti ima svoje prednosti i nedostatke, a na security provajderima je da u dogovoru sa klijentom izaberu za obe strane prihvatljivo rešenje. Postoje kompanije koje prave bezbedne Web aplikacije i one koje to ne rade. Kompanija koja kupuje rešenje treba da proverí refernce prodavca softvera i da proverí bezbednosne mehanizme koje koristi u svojim aplikacijama. Oblast bezbednosti i zaštite Web aplikacija veoma je interesantna ali ona nije tema ovog rada tako da neće biti detaljnije obrađivana.

Zaključak

U ovom radu bilo je reči o organizaciji zaštite informacionih sistema. Na početku rada prikazana je metodologija po kojoj je istraživanje obavljeno što je pored ostalog podrazumevalo predmet istraživanja, ciljeve i zadatke istraživanja, istraživačke hipoteze, metode istraživanja i tok istraživačkog procesa.

Cilj ovog rada bio je da se prikaže situacija na tržištu usluga koje se pružaju u oblasti zaštite informacionih sistema. Ukoliko bi se neka kompanija odlučila na primer da osigura bezbednu komunikaciju između svojih radnih stanica koje se ne nalaze samo u lokalnoj mreži i svojih servisa koji se nalaze kod različitih provajdera imala bi poteškoća da to ostvari. Temeljno višemesečno istraživanje pokazalo je da i ovakav na izgled jednostavan zahtev nije jednostavno sprovesti u delo. U ovom radu data su rešenja i konkretni predlozi koji mogu da pomognu IT menadžerima u kompanijama da prevaziđu neke od problema prilikom implementacija bezbednosnih rešenja.

Na početku rada dat je pregled potreba koje kompanije imaju u oblasti informacionih tehnologija, a koje su uslovljene savremenim poslovanjem koje podrazumeva da informacije budu dostupne uvek bez obzira na to gde se zaposleni u kompaniji trenutno nalaze. Takođe je bilo reči i o tome da korisnici žele da se njihove informacije nalaze na sigurnim serverima, a da se komunikacija do njih odvija na bezbedan način.

Oblast kojoj je u ovom radu posvećeno dosta pažnje jeste i security management odnosno upravljanje zaštitom. O ovoj oblasti zaštite koja je veoma važna kod nas se veoma malo zna. Zbog toga će informacije koje su ovde ponuđene sasvim sigurno biti od velike pomoći sadašnjim i budućim IT menadžerima, kao i menadžerima koji vode računa o bezbednosti informacionih sistema kako bi unapredili poslovanje svojih kompanija u ovoj oblasti.

Kada se govori o računarskim mrežama svakako se mora nešto reći i o OSI modelu koji je veoma važan za razumevanje načina na koji funkcionišu računarske mreže. Pored toga ovde je bilo reči i o sigurnosnim protokolima koji se koriste za bezbednu komunikaciju odnosno o IPsec protokolu, a detaljno je opisan i SSL protokol. Ovaj protokol se sve više upotrebljava pre svega zbog svoje fleksibilnosti koja se najviše ogleda u jednostavnosti korišćenja kroz Web pretraživač koji se sve više koristi ne samo za pretraživanje već i za pokretanje Web aplikacija kao i drugih Web servisa.

Tehnički obučeni korisnici, sve češća upotreba mobilnih uređaja kao što su mobilni telefoni ili laptop računari, pojava namenskih hardverskih uređaja, a pre svega virtualizacija i razvoj Cloud computing-a doveo je toga da je postalo neophodno da se preispita opravdanost sadašnje organizacije računarskih mreža naročito manjih kompanija. Ovde je data detaljna analiza sadašnjeg stanja, kao i smeli predlozi koji podrazumevaju bolju iskorišćenost mrežnih resursa kao i znatno smanjenje troškova koje bi se time postiglo.

Neophodnosti izmeštanja podataka ili mrežne infrastrukture kod specijalizovanih provajdera uslovljena je sve povoljnijom ponudom namenskih servera kao i ekspanzijom virtualizacije koja predstavlja osnov za Cloud computing. Izmeštanje podataka i infrastrukture kod specijalizovanih provajdera pruža bolju dostupnost ovih resursa zaposlenima u kompaniji bez obzira na to gde se oni u određenom trenutku nalaze.

Kada je bilo reči o upravljanju identitetom pre svega je skrenuta pažnja na opasnosti koje vrebaju korisnike kroz metode socijalnog inženjeriga. Mnogi korisnici iako poseduju solidno

znanje o računarima mogu da upadnu u zamku zlonamernih ljudi koji krstare Internetom u potrazi za žrtvom od koje će moći da ukradu njen digitalni identitet i da ga kasnije zloupotrebe. Jedina prevencija pored stalne edukacije jeste dosledna primena PKI infrastrukture pre svega za autentifikaciju jer jedino u tom slučaju korisnik može da bude siguran da komunicira sa odgovarajućim serverom. Takođe na serverskoj strani se čuvaju podaci o digitalnom sertifikatu korisnika čijom se proverom prilikom autentifikacije sprečava bilo kakva zloupotreba.

Bezbedna komunikacija obezbeđena je pre svega preko višenamenskog specijalizovanog hardverskog ili virtualnog uređaja koji se naziva SSL VPN uređaj. Pored mogućnosti da se na njega instalira serveski sertifikat što je njegova verovatno najbolja karakteristika on takođe može da bude mrežni firewall, a sa ubrzanim razvojem Web aplikacija sve više se koristi i kao application firewall. SSL VPN uređaj može da radi kao SSL portal VPN i kao SSL tunel VPN, a svaki od njih ima svoje prednosti i nedostatke.

Zbog potrebe da se dokaže neophodnost postojanja nezavisnog servisa koji bi osigurao bezbednu komunikaciju između klijentskog računara i udaljenog servera nastao je ovaj rad. Security servis, nezavistan od provajdera koji hostuju druge servise neke kompanije pruža mogućnost da može da ga koristi veliki broj manjih kompanija za koje je do sada bezbedna komunikacija predstavljala veliki problem zbog ograničenih finansijskih sredstva izdvojenih za ovu namenu.

Praktična primena security servisa moguća je pre svega u korišćenju poslovnih Web aplikacija, kao i drugih servisa kao što su e-learning ili DMS koji se nalaze na udaljenim serverima. Takođe prikazana su i neka praktična rešenja koja su vezna za digitalno potpisivanje Web formi o čemu se do sada kod nas veoma malo znalo.

Kao što je već rečeno ovaj rad namenjen je pre svega stručnjacima iz oblasti informacionih tehnologija jer obuhvata širok dijapazon tema koje se tiču bezbednosti i svakao može da im bude od pomoći kada budu uvodili neke od elemenata zaštite u informacione sisteme u svojim kompanijama.

Literatura

- [1] Vojna enciklopedija, drugo izdanje, knjiga 4, strana 714. Vojnoizdavački zavod Beograd, 1972.
- [2] Wikipedia, Information Security, http://en.wikipedia.org/wiki/Information_security
- [3] Wikipedia, Kriptozaštita, <http://sr.wikipedia.org/wiki>
- [4] Wikipedia, OSI model, <http://sr.wikipedia.org/wiki>
- [5] Wikipedia, Lokalna računarska mreža, <http://sr.wikipedia.org/wiki>
- [6] Netset, http://wmproba.atspace.com/srpski/technology_public_key_infrastructure.html
- [7] Virtualna privatna mreža, <http://sr.wikipedia.org/wiki>
- [8] Joseph Steinberg and Tim Speed, Understanding SSL VPN, Packt Publishing, 2005.
- [9] Grupa autora, Guide to SSL VPNs, National Institute of Standards and Technology, 2008.
- [10] Spec.App Željko Pekić, SSL bezbjednost transportnog sloja, Univerzitet Mediteran, 2009.
- [11] Dr Zoran M Urosević, Uvod u računarske telekomunikacije i mreže - transportni deo, Tehnički fakultet u Čačku, 2004.
- [12] Vladan Nikačević, Prikupljanje digitalnih dokaza na računarskim mrežama, Univerzitet Singidunum, 2009.
- [13] Zakon o elektronskom potpisu
- [14] Michael E. Whitman and Herbert J. Mattord, Management of Information Security, Course Technology, 2008.
- [15] Svet kompjutera <http://www.sk.rs/2005/11/skin05.html>
- [16] Svet kompjutera <http://www.sk.rs/2005/04/skin06.html>
- [17] Stonesoft, http://www.stonesoft.com/en/press_and_media/brand_place/illustrations/
- [18] Marko Herman, Upravljanje identitetom, <http://www.pcpres.rs/arhiva/tekst.asp?broj=156&tekstID=8834>
- [19] Clarity accounting, Security bookkipping, <https://www.clarityaccounting.com/help/index.php/tag/security/>
- [20] Wikipedia, Network attached storage, http://en.wikipedia.org/wiki/Network-attached_storage