Mjere procjene sigurnosti i zaštite poslovnog korisnika

Urankar, Danijel

Master's thesis / Diplomski rad

2015

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:855086

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-28**



Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository







SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

Danijel Urankar

MJERE PROCJENE SIGURNOSTI I ZAŠTITE POSLOVNOG KORISNIKA

DIPLOMSKI RAD

Zagreb, 2015.

Sveučilište u Zagrebu
Fakultet prometnih znanosti

DIPLOMSKI RAD

MJERE PROCJENE SIGURNOSTI I ZAŠTITE POSLOVNOG KORISNIKA
SECURITY EVALUATION MEASURES AND USER PROTECTION

Mentor: prof. dr. sc. Dragan Peraković
Student: Danijel Urankar, 0135201127

Zagreb, 2015.

Sažetak

Informacijska sigurnost podrazumijeva očuvanje povjerljivosti, tj. tajnosti i privatnosti podataka, te integriteta i raspoloživosti informacijskih sustava. Na temelju istraživanja dobiveni su konkretni rezultati sigurnosti informacijskog sustava, te njegova otpornost na napade i nepravilnosti. U istraživanju poslovnog korisnika pronađeni su nedostaci u sustavu te predložene smjernice za poboljšanje zatečenog stanja. Svrha istraživanja je prikazati na koji način je moguće očuvati podatke i cjelokupni sustav, te procjeniti rizike kojima se izlažu informacijski sustavi. Nadalje cilj istraživanja je na primjeru poslovnog korisnika pokušati što detaljnije i bolje prikazati način zaštite i prijedloge poboljšanja informacijskog sustava.

KLJUČNE RIJEČI: informacijska sigurnost; rizičnost; prijetnje; ranjivosti

Information safety means preservation of confidentiality as well as secreacy and privacy of data, integrity and availability of information system. Based on the research, concrete results were given on safety of information system, and it's resiliance on attacks and irregulations. During the research of bussines users irregulations were found in the system and guidelines for improvements were suggested. Purpose of the research was to show the means of data preservation, preservation of the whole system and estimation of risks information systems were exposed. Furthermore, the goal of the research in bussines users was to show, in as much detail as possible, ways of protection and suggestions of improvements of information system.

KEY WORDS: information safety; risk; threats; vulnerability

SADRŽAJ

1. Uvod 1

2. Sigurnost i zaštita informacijskog sustava 3

2.1. Informacija 3

2.2. Sigurnost i zaštita 5

2. 3. Računalni kriminal 8

2.4. Arhitektura sigurnosnog sustava 10

2.4.1. Model informacijske sigurnosti 10

2.4.2. Osnova sigurnosnog sustava 11

2.5. Sigurnost i zaštita programa i operacijskih sustava 12

2.5.1. Virusi i drugi zloćudni kod 12

2.5.2. Sprječavanje od virusne infekcije 15

2.5.3. Namjerni, ciljani zloćudni kod (specifičan kod) 18

2.6. Digitalna identifikacija i autentifikacija 18

2.6.1. Identifikacija 19

2.6.2. Autentifikacija 20

2.7. Sigurnost baza podataka 28

3. Rizik informacijskog sustava 31

3.1. Norme za informacijsku sigurnost 34

3.2. ISO/IEC 17799 34

3.3. ISO/IEC 27001:2005 35

3.3. ISO/IEC 17799:2005 36

4. Ocjena rizičnosti poduzeća 42

4.1. Prijetnje 45

4.2. Ranjivost 46

4.3. Rizik 48

4.4. Prijedlog poboljšanja 49

5. Zaključak 52

Popis literature 53
Popis ilustracija 54
Popis tablica 55
Popis kratica 56
Metapodaci 57
Izjava o akademskoj čestitosti i suglasnosti 58

1. Uvod

Sigurnost informacijskog sustava čini niz mjera i postupaka koji se poduzimaju kako bi se osiguralo normalno funkcioniranje informacijskog sustava bez narušavanja njegovog integriteta. Implementirane mjere sigurnosti cjenovno ne smiju premašiti vrijednost štete koja bi nastala gubitkom cjelokupnog ili većeg dijela sadržaja. Da bi se moglo isplanirati nivo sigurnosti treba biti u stanju procijeniti razinu rizika. Cilj implementiranog sustava sigurnosti je optimiziranje rada informacijskog sustava s obzirom na rizik kojem je izložen. Rizik se procjenjuje s obzirom na:

- značaj podataka i sadržaja koji se pohranjuju ili distribuiraju
- procjenu izvora i oblika prijetnji tim sadržajima.

Najpoznatije metode izrade sigurnosnih kopija su: potpuni backup, diferencijalni backup, inkrementalni backup. U najčešće programske mjere zaštite spadaju: zaštita na razini operacijskog sustava, zaštita na razini korisničke programske podrške, kriptiranje podataka u komunikaciji, antivirus alati, antispyware alati, zaštitni zid („Firewall“). U ovom radu detaljno će biti analiziran svaki segment mogućeg rizika. To uključuje analiza kvalitete računalne opreme, analiza kvalitete softvera u kojem poduzeće radi, analiza zaštićenosti mreže od vanjskih utjecaja, testiranje osviještenosti osoblja o rizicima i prijetnjama, ispitivanje sigurnosti baze podataka i backup-a, te ispitati organizacijske procedure tj. jesu li svakom pojedincu ispravno dodijeljena prava, te dali postoji mogućnost nelegitimnog korištenja istih.

Svrha istraživanja je prikazati načine očuvanja podataka i cjelokupnog sustava, procijeniti rizik kojem je izložen informacijski sustav te ponuditi smjernice za poboljšanje. Procijeniti koliko su sigurne zaporke, dali postoji mogućnost krađe identiteta, dali se računala redovno održavaju/čiste od „virusa“, jesu li prava ispravno dodijeljena te koliko je mreža sigurna. Naposljetku svrha je analizirati sustav kako bi se osigurali kritični i vitalni poslovni procesi u zahtjevanom vremenu. Ograničiti i smanjiti gubitke koji mogu nastati kao posljedica prekida poslovnih procesa, te odabrati najdjelotvornije mjere za smanjenje rizika i prijetnji.

Cilj je na primjeru realnog informacijskog sustava pokušati što detaljnije i bolje prikazati načine zaštite te moguće poboljšanje informacijskog sustava. Ispitati sigurnosni rizik u

informacijskom sustavu, razmotriti raspoložive mjere zaštite i kontrole, otkriti ranjivosti i prijetnje te identificirati područja u kojima je potrebno više rada na postizanju bolje sigurnosti. Dati realnu ocjenu rizika poduzeća za svaki element informacijskog sustava. Analizirati sve segmente od uredske opreme, softvera, mreže, baze podataka, osviještenosti zaposlenih o rizicima ePoslovanja i organizacijskog djela kako bi se na posljetku mogle dati smjernice za povećanje otpornosti sustava te smanjenje mogućih rizika.

Tema diplomskog rada je **Mjere procjene sigurnosti i zaštite poslovnog korisnika.** Materija je izložena u 6 pogavlja:

1. Uvod
2. Sigurnost i zaštita informacijskog sustava
3. Rizik informacijskog sustava
4. Ocjene rizičnosti poduzeća
5. Prijedlog poboljšanja
6. Zaključak

U drugom poglavlju opisano je općenito što je to informacija, aspekti informacijske sigurnosti o kojima poslovni proces treba voditi računa. Nadalje opisuje se arhitektura sigurnosnog sustava te prijetnje i načini zaštite i sprječavanje od virusne infekcije.

U trećem poglavlju opisani su rizici informacijskog sustava i norme koje definiraju informacijsku sigurnost. Norme koje su opisane u ovom poglavlju su ISO/IEC 17799, ISO/IEC 27001:2005 i ISO/IEC 17799:2005. ISO/IEC 17799 norma se odnosi na područje upravljanja informacijskom sigurnošću, ISO/IEC 27001:2005 norma se odnosi na kvalitetu uspostave sustava upravljanja sigurnošću informacija i ISO/IEC 17799:2005 norma se odnosi na područje koje nas upoznaje s procjenom rizika.

Četvrto poglavlje se odnosi na ocjenu rizičnosti poduzeća i u ovom poglavlju će se analizirati sustav kroz sve elemente informacijskog sustava. Isto tako objašnjene su prijetnje, ranjivosti i rizici informacijskog sustava.

Isto tako četvrto poglavlje se odnosi na prijedlog poboljšanja sustava, odnosno tu su navedeni prijedlozi poboljšanja sustava poslovnog korisnika.

2. Sigurnost i zaštita informacijskog sustava

Informacija je imovina i kao takvu ju je potrebno prikladno zaštititi, kako bi se omogućilo normalno poslovanje organizacije. Taj zahtjev postaje sve važniji zbog distribuiranosti poslovne okoline, jer su u takvom okruženju informacije izložene većem broju prijetnji i ranjivosti, [1].

2.1. Informacija

Informacije se javljaju u više oblika. Mogu biti zapisane na papiru, pohranjene u elektroničkom obliku, sačuvane na filmu, mogu se prenositi poštom ili elektroničkim putem. Bez obzira u kojem je obliku pohranjena informacija, ona uvijek mora biti prikladno zaštićena, [1].

Informacija je rezultat obrade, manipulacija i organiziranja podataka na način koji dodaje znanje primatelju. Za kvalitetan rad potrebno je informacije zaštititi od neovlaštenih izmjena tj. osigurati integritet od objavljivanja tajnih informacija. Nadalje potrebno je osigurati povjerljivost i uskraćivanja dostupnosti informacija neovlaštenim korisnicima.

Tri su temeljna principa uspostave integriteta:

- Dodjela samo nužnih prava pristupa - korisnicima treba dodijeliti pravo pristupa samo na one datoteke i programe koji su im potrebni da bi obavljali svoju poslovnu funkciju u organizaciji.
- Odvajanje dužnosti – dobro je osigurati da nijedan zaposlenik nema kontrolu nad transakcijom od početka do kraja.
- Rotacija dužnosti – poslovni zadaci trebali bi se mijenjati periodički tako da korisnicima bude otežano zlonamjerno preuzimanje kontrole nad transakcijom.

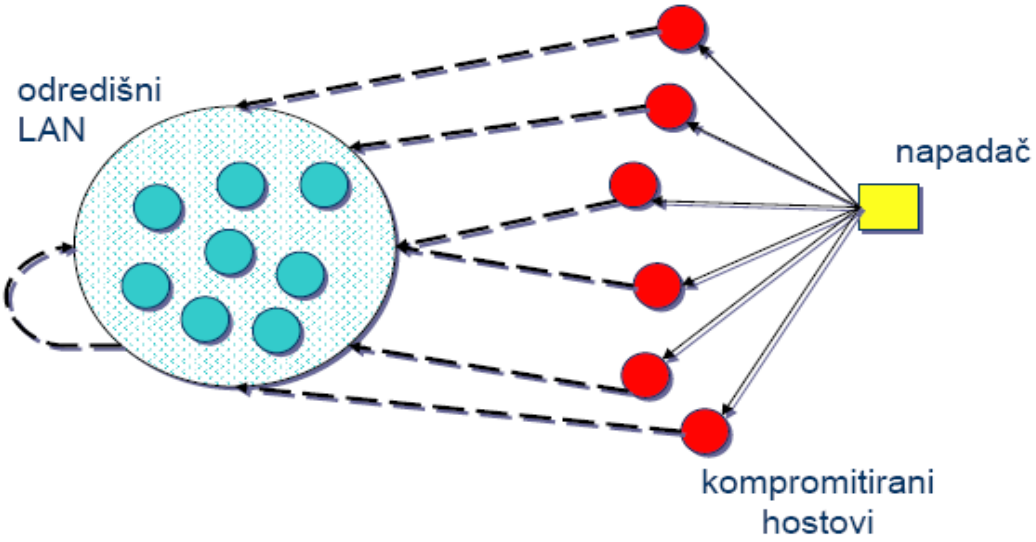
Tri su cilja integriteta, koje različiti modeli postižu na različite načine a to su sprječavanje neovlaštenih korisnika da modificiraju podatke ili programe, sprječavanja ovlaštenih korisnika da modificiraju podatke ili programe na nepropisan i neovlašten način te održavanja unutarnje i vanjske konzistentnosti podataka i programa.

Ključni aspekti povjerljivosti su korisnička identifikacija, autentifikacija i uspjela identifikacija koja je nužna kako bi se osigurala učinkovitost politika koje specificiraju koji korisnici imaju pravo pristupa pojedinim podacima.

Najčešće prijetnje povjerljivosti su:

- Hakiranje - haker je netko tko preuzima kontrolu nad sustavom iskorištavajuci sigurnosne slabosti koje postoje u sustavu.
- Maskiranje - maskiranje je proces kojim ovlašteni korisnik pristupa sustavu, ali pomoću lozinki drugih korisnika.
- Neovlaštena korisnička aktivnost - ovaj tip aktivnosti se pojavljuje kad autorizirani korisnik dobije pristup datotekama kojima nema pravo pristupa.
- Nezaštićeno preuzimanje *(*engl. *download)* datoteka - preuzimanje datoteka može kompromitirati povjerljive informacije.
- Lokalne mreže *(*engl. *Local Area Networks)* - lokalne mreže predstavljaju posebnu prijetnju povjerljivosti informacija jer podaci koji putuju mrežom mogu biti kompromitirani u svakom čvoru mreže.
- Trojanski konji - trojanski konji mogu kopirati povjerljive datoteke u neovlaštena područja sustava, ukoliko korisnik koji ima pravo pristupa tim datotekama, ne znajući, izvrši takav program.

Pod prijetnjom dostupnosti postoji uskraćivanje usluge (engl. *Denial of service - DoS*) i tu se radi se o vrsti napada u kojem se obično namjernim generiranjem velike količine mrežnog prometa nastoji zagušiti mrežna oprema i poslužitelji, te distribuirano uskraćivanje usluge (engl. *Distributed Denial of Service*) što predstavlja oblik napada uskraćivanjem usluga u kojem su izvori zagušujućeg mrežnog prometa distribuirani na više mjesta po Internetu (slika 1).



Slika 1. Uskraćivanje usluge, [1]

2.2. Sigurnost i zaštita

Sigurnost je proces smanjenja rizika ili vjerojatnosti nastajanja štete.
Neki od aspekata informacijske sigurnosti o kojima treba voditi računa ovaj poslovni proces su:

- Pristup
- Identifikacija
- Autentifikacija
- Autorizacija, [2].

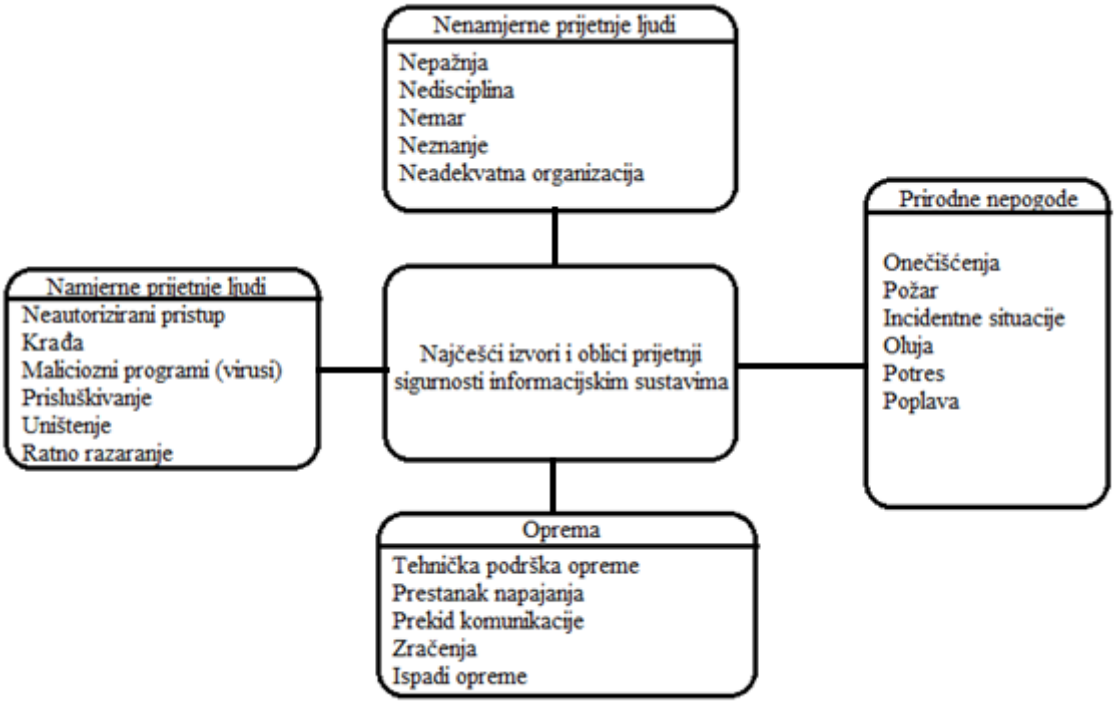
Sigurnost informacijskih sustava obuhvaća primjenu mjera za zaštitu podataka koji su u obradi, ili su pohranjeni, ili je u tijeku njihov prijenos, od gubitaka povjerljivost, cjelovitosti i raspoloživosti, te radi sprječavanja gubitaka cjelovitosti ili raspoloživosti samih sustava, [2].

Glavni ciljevi u istraživanju računalne sigurnosti su ispitivanje sigurnosnih rizika u računalstvu, razmatranje raspoloživih zaštitnih mjera i kontrola, stimuliranje razmišljanja o neotkrivenim ranjivostima i prijetnjama, identifikacija područja u kojima se zahtjeva više rada na postizanju bolje sigurnosti, [2].

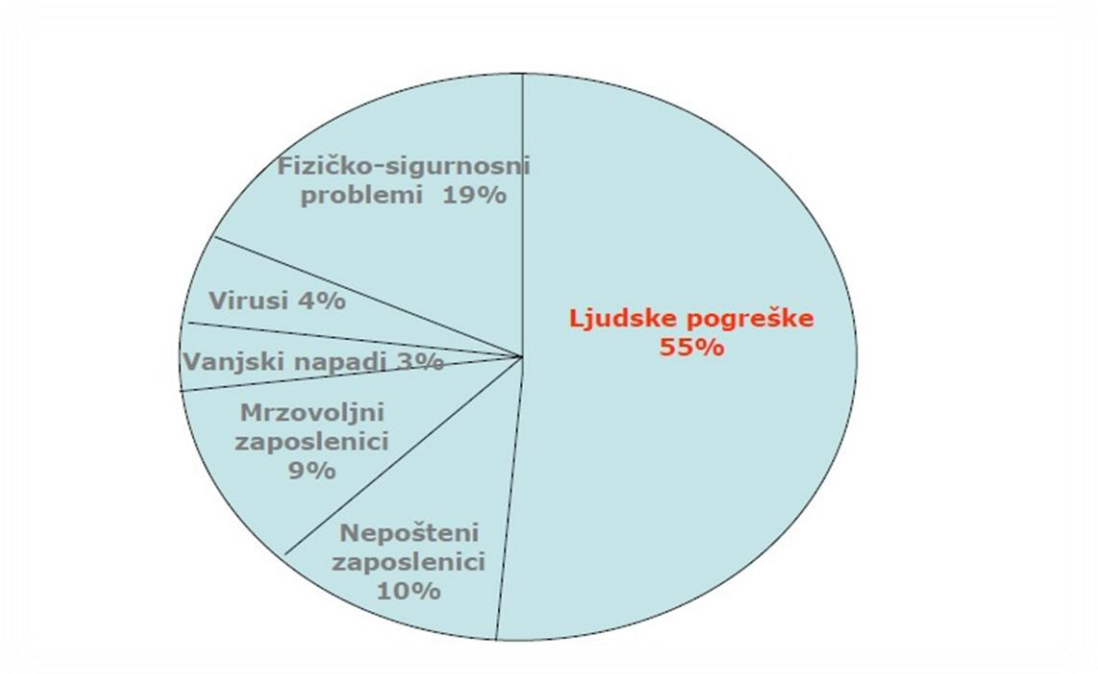
Pod pojmom informacijske sigurnosti podrazumijeva se zaštita informacija od velikog broja prijetnji, kako bi se osigurao poslovni kontinuitet, smanjio rizik, te povećao broj poslovnih prilika i povrat od investicija.

Informacije i pripadni procesi, sustavi i mreže su važan dio poslovne imovine. Definiranje, implementacija, održavanje i poboljšavanje informacijske sigurnosti može biti od presudne važnosti kako bi se ostvarila i zadržala konkurentnost, osigurao dotok novca i profitabilnost, kako bi se zadovoljile zakonske norme i osigurao poslovni ugled, [1].

Sigurnost informacijskih sustava može biti ugrožena na više načina. Prijetnje možemo podijeliti prema različitim izvorima (slika 2, slika 3), a izvori su prvenstveno ljudi kroz namjerne i nenamjerne prijetnje, zatim oprema te prirodne nepogode [1].



Slika 2. Najčešći izvori i oblici prijetnji sigurnosti informacijskim sustavima, [1]



Slika 3. Prijetnje sigurnosti sustava, [1]

Organizacija za ekonomsku suradnju i razvoj (engl. *The Organisation for Economic Cooperation and Development - OEDC*) je ustanovila 9 principa sigurnosti informacijskih sustava. Prvi princip je svijest o informacijskoj sigurnosti kao prvi korak u sigurnosti. Važno je biti svjestan svih prijetnji i potrebe za sigurnošću informacijskih sustava i zaštitnih mjera. Na svijest se nadovezuje odgovornost svih članova organizacije za sigurnost informacijskih sustava. Treći princip je odziv što predstavlja da svi članovi organizacije trebaju pravovremeno i kooperativno sudjelovati u sprječavanju, detekciji i rješavanju sigurnosnih incidenata. Sljedeća dva principa su etika i demokracija. Nakon toga dolazi procjena rizika koju je potrebno provesti prije dizajna i implementacije sigurnosnih mjera kao sedmog principa sigurnosti informacijskih sustava. Organizacija treba uspostaviti jasan pristup upravljanju sigurnošću i na kraju kao zadnji princip dolaze promjene u redovnoj modifikaciji sigurnosnih politika, mjera, procedura i sl.

2. 3. Računalni kriminal

Postoje različite definicije i objašnjenja računalnog kriminala. Svatko od osoba vezanih za ovu temu posjeduje svoje viđenje i objašnjenje računalnog kriminala pa je tako gospodin D. Parker rekao da je računalni kriminal "opća forma kroz koju se ispunjava različiti oblik kriminalne aktivnosti, forma koja će u budućnosti postati dominantna", dok Taber ima svoju definiciju i govori kako je računalni kriminal: "računalni delikt koji uključuje visokostručne operacije na računalu u okolnostima gdje do povrede ne bi moglo doći na drugi način" (krađa, uništenje, oštećenje)". Također tu su i dvije definicije dvojice gospodina koje možemo vidjeti u nastavku teksta.

Krapac: "računalni kriminal označava sve slučajeve zloupotrebe elektronskog računala koji su pravno određeni kao kaznena djela"….

Dragičević: računalni kriminal je ukupnost kaznenih djela, učinjenih na određenom području kroz određeno vrijeme, kojima se neovlašteno utječe na korištenje, cjelovitost i dostupnost, programske ili podatkovne osnovice računalnog sustava ili tajnost digitalnih podataka"…, [1].

Kao suma i zaključak svih definicija računalni kriminal zapravo nije zasebna vrsta kriminala, već je to zajednički naziv za "tradicionalan" kriminal počinjen pomoću računala ili nekog drugog elektroničkog medija i za kriminalne radnje specifične računalima i elektroničkim medijima.

Uvriježeno je mišljenje da je računalni kriminal kriminalna radnja počinjena računalom, dok zapravo računalo može imati različite uloge bilo mete bilo alata. Po Donn Parkeru uloga računala može biti kao objekta, subjekta, oruđa te simbola. Uloga računala kao objekta u slučajevima računala i računalne mreže kao meta fizičke ili softverske sabotaže ili preuzimanja kontrole, krađe hardvera ili softvera, uništavanja ili krađe podataka. Zatim postoji slučaj računala kao subjekta u slučaju da je računalo oružje u kojem je kriminalna radnja počinjena kao što su napadi virusima, crvima i trojancima. Računalo kao oruđe u slučaju da se kriminalna radnja čini uz pomoć računala. Ovdje spadaju svi oblici krivotvorenja, pronevjera, prijevara, krađa podataka ili hakiranje.

Računala i internet su okruženje u kojem računalni kriminalci odabiru žrtvu, uvlače u prijevaru ili neku drugu kriminalnu radnju i u tom slučaju uloga računala u kriminalu je kao simbol. Ovdje spadaju razni oblici e-mail prijevare, phishing, spamming, nagovaranje na kriminalnu radnju ili iznuda.

Nadalje, računalni kriminal možemo podijeliti u 3 kategorije a to su kao prvo protuzakonito korištenje računala kao što su kriminalne radnje krađe računalnih resursa, preuzimanje nadzora nad računalom i podataka na njemu, distribucija ilegalnog sadržaja, krađa identiteta i podataka, krivotvorenje, pronevjere te svi oblici "hakiranja".

Nakon toga imamo kreiranje ilegalnog softwarea i piratstvo, a to su svi oblici stvaranja i distribucije virusa, crva i trojanaca, neovlašteno korištenje i umnožavanje foto, video i audio materijala.

Treća kategorija predstavlja uhođenje, uznemiravanje i poticanje na kriminalnu radnju kao svi oblici prisluškivanja, nadgledanja i "špijuniranja", spamming i phishing, e-mail prijevare i piramidalne sheme, nagovaranje i dogovaranje kriminalnih radnji, [3].

U postupanju s računalnim kriminalom postoje tri najvažnija postupka prevencija, otkrivanje i kažnjavanje. Kod prevencije se govori o procjeni rizika i analizi prijetnji, o fizičkoj sigurnosti, sigurnosti osoblja, komunikacijskoj sigurnosti, operacijskoj sigurnosti te planiranju borbe protiv računalnog kriminala. Moraju se provesti mjere otkrivanja računalnog kriminala, oformiti tim za rukovođenje kriznim situacijama, zatim obrada i praćenje upada, istaga i pravosudni progon, bilježenje tragova i prikupljanje svih dokaza za provođenje zadnjeg postupka, postupka kažnjavanja. Tu se provodi rukovanje sa svim prikupljenim dokazima, vještačenje eksperata, prezentacija na sudu te aktivnosti nakon presude [1].

2.4. Arhitektura sigurnosnog sustava

Namjena uspostave svake arhitekture jest osiguranje konzistentnosti u dizajnu složenih sustava. Tako je i zadatak ispravne sigurnosne arhitekture uspostava konzistentnog sustava sigurnosti složenog informacijskog sustava organizacije. Kroz sigurnosnu arhitekturu uspostavlja se slojeviti pristup čime se pojednostavnjuje složenost sustava sigurnosti.

2.4.1. Model informacijske sigurnosti

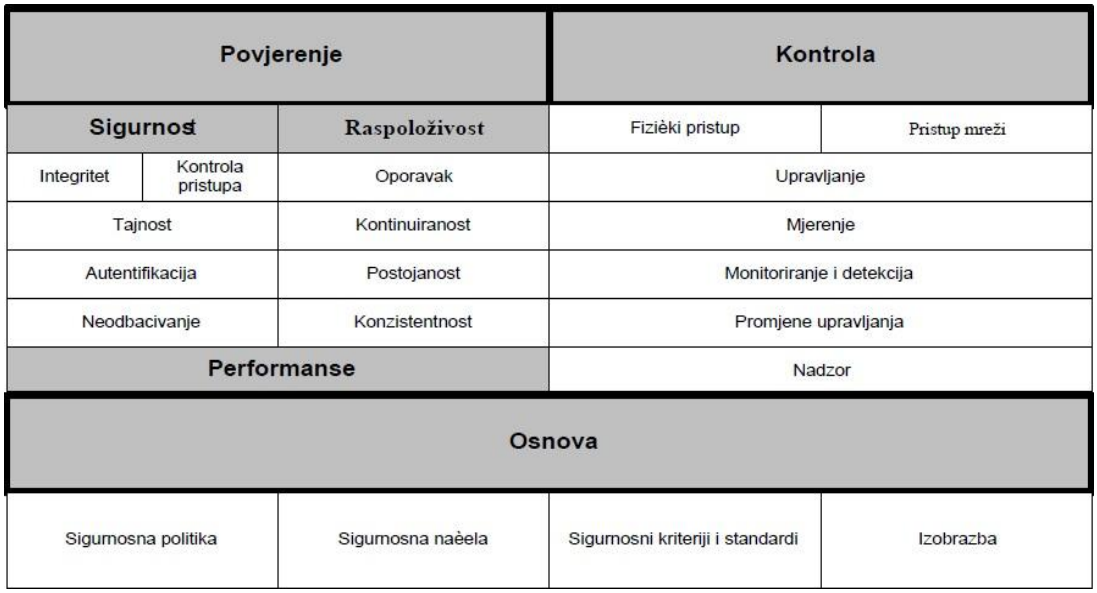
Potpuni model sigurnosnog sustava, kao što je vidljivo i sa slike 4 sastoji se od tri cjeline:

- Organizacijskog sustava,
- Sustava upravljanja,
- Tehnološkog sustava, [2].

<table>
<tr><td colspan="3">Poslovna strategija i ciljevi</td></tr>
<tr><td colspan="3">Sigurnosni zahtjevi</td></tr>
<tr><td colspan="3">Sigurnosna strategija i ciljevi</td></tr>
<tr><td colspan="2">Organizacijaska struktura</td><td rowspan="3">Organizacijski sustav</td></tr>
<tr><td colspan="2">Podjela posla -role</td></tr>
<tr><td colspan="2">Edukacija korisnika</td></tr>
<tr><td colspan="2">Upravljanje propisima</td><td rowspan="4">Sustav upravljanja</td></tr>
<tr><td colspan="2">Upravljanje sredstvima</td></tr>
<tr><td colspan="2">Upravljanje rizikom</td></tr>
<tr><td colspan="2">Upravljanjem tehnologijom</td></tr>
<tr><td colspan="2">Ocjena funkcionalnosti</td><td rowspan="8">Tehnološki sustav</td></tr>
<tr><td>Validacija i autentifikacija</td><td rowspan="5">Zaštitna funkcionalnost
(Sigurnosni servisi)</td></tr>
<tr><td>Kontrola pristupa</td></tr>
<tr><td>Integritet podataka</td></tr>
<tr><td>Povjerljivost podataka</td></tr>
<tr><td>Anti DoS</td></tr>
<tr><td colspan="2">Funkcionalnost detekcije</td></tr>
<tr><td colspan="2">Funkcionalnost odgovora</td></tr>
<tr><td colspan="2">Funkcionalnost oporavaka</td></tr>
<tr><td colspan="3">Vrednovanje sigurnosnog sustava</td></tr>
</table>

Slika 4. Potpuni model sigurnosnog sustava, [2]

Sigurnosna arhitektura sustava, koji implementira gore navedeni model, sastoji se od nekoliko osnovnih blokova, prikazanih na slici 5.



Slika 5. Model sigurnosne arhitekture, [2]

Model informacijske sigurnosti je podijeljen na osnovu, povjerenje i kontrolu.

2.4.2. Osnova sigurnosnog sustava

Osnova sigurnosnog sustava određena je strategijom ili sigurnosnom politikom organizacije, principima, definiranom sigurnosnim kriterijima i odabranim standardima sigurnosnog sustava.

Sigurnosna politika ili strategija organizacije mora i trebala bi postaviti pravce obavljanja sigurnosne politike, dati potpun vodič organizacije sigurnosnog sustava te demonstrirati potporu uprave i odanost sigurnosnom načinu rada.

Ciljevi sigurnosne politike je učinkovito upravljanje i nadzor rizika, definiranje odgovornosti svih djelatnika za zaštitu informatičkih sredstava, postavljanje osnove za stabilne uvjete rada, osiguravanje podudarnosti sa primijenjenim zakonima i propisima te mogućnost očuvanja, u slučaju zloupotrebe, gubitka ili neovlaštenog otkrivanja sredstava sustava.

Za svaku organizaciju jedna od bitnijih stavki je sigurnost i kako je uvesti. Tako postoje inheretno povjerljivi korisnici i inheretno nepovjerljivi korisnici. Potrebno se držati kriterija i standarda kod sigurnosti informacijskih sustava. Sigurnosni kriterij kao definiran referentni

standard (TCSEC) primjenjen na sigurnosnu komponentnu i tehnologiju. Vrlo važna stavka je i edukacija, odnosno formalni program edukacije i ona je obavezna komponentna sigurnosne arhitekture.

Komponentne sigurnosti su integritet, kontrola pristupa ili autorizacija, tajnost, autentifikacija i ne odbacivanje. Mehanizam kontrole kod integriteta treba omogućiti detekciju problema, ispravak ili obilježavanje namjerno ili slučajno nedopuštenih izmjena podataka, programa i sklopova. Kod kontrole pristupa, odnosno autorizacije osnovu čine identifikacija i autentifikacija. Autentifikacija ovisi o vremenskj ovisnosti, klasifikaciji podataka, ulozi i funkciji korisnika, sistemskoj adresi, vrsti transakcije te vrsti zahtjevane usluge. Važno je svaku važnu informaciju održati u tajnosti, a osnovna metoda kojom se informacija održava tajnom je kroz kriptiranje podataka.

2.5. Sigurnost i zaštita programa i operacijskih sustava

Kod sigurnosti i zaštita programa i operacijskih sustava postoje dvije vrste greške:

- nenamjerne ljudske greške,
- namjerne greške - zloćudni kod

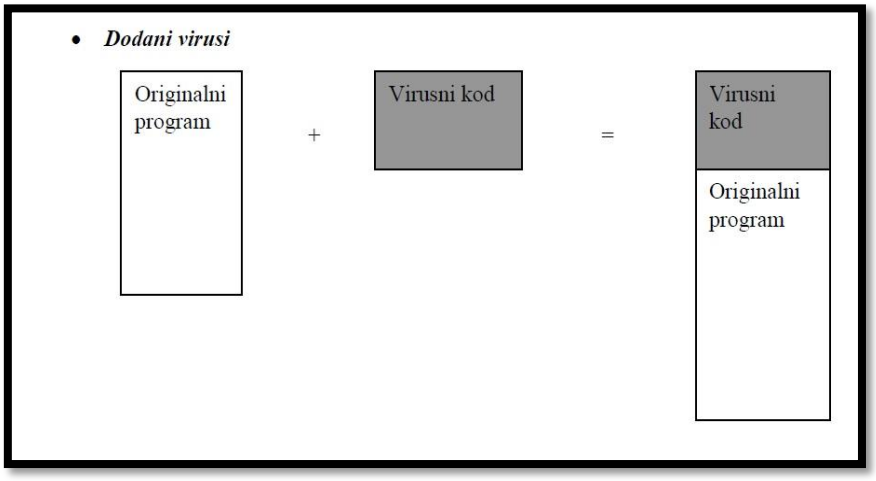
Sve programske greške ne možemo izbjeći, i za to postoje dva razloga. Jedan od razloga je što se kontrola programa još uvijek provodi na razini pojedinačnog programa i programera. Uvijek se dogode nepredvidive greške, isto tako često puta i programer može neke greške sakriti. Drugi razlog je taj da se programiranje i programsko inženjerstvo mijenjaju i razvijaju puno brže nego tehnike u računalnoj sigurnosti.

2.5.1. Virusi i drugi zloćudni kod

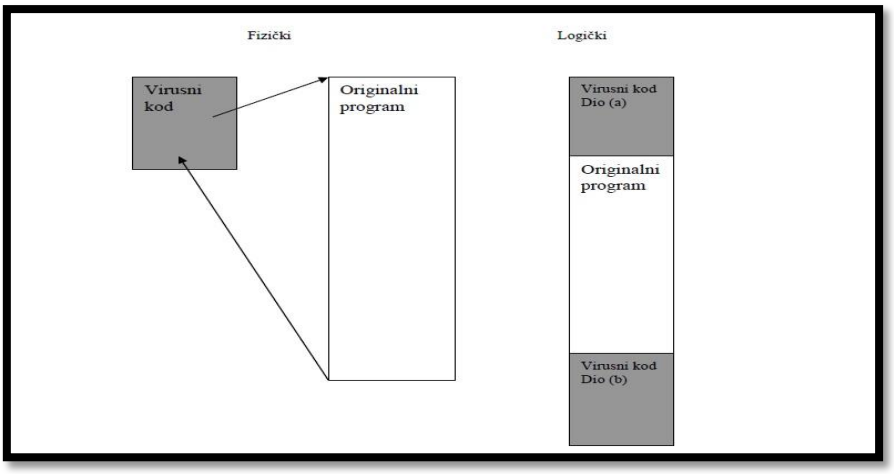
Imamo dvije vrste virusa:

- tranzitni virus
- rezidentni virus

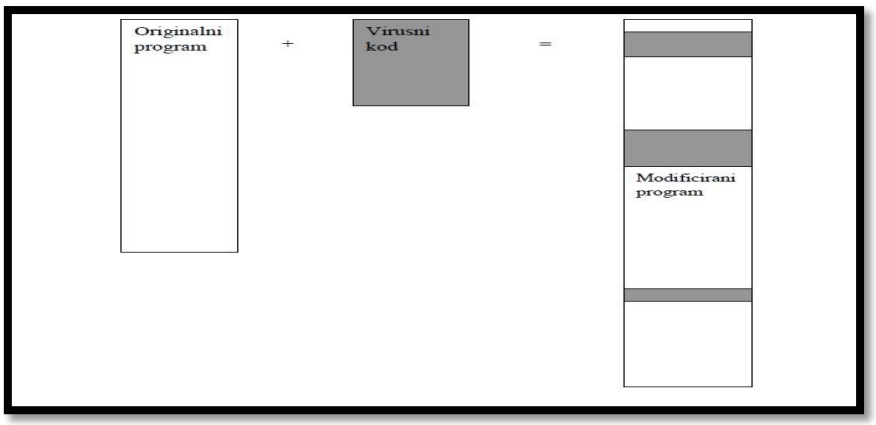
Na sljedeće tri slike možemo vidjeti na koji način se virus priključuje na program, odnosno veže i dodaje na program, na koji način virus okružuje program, te kako je virus integriran u program (slika 6, slika 7, slika 8).



Slika 6. Virus koji se dodaje na program, [2]



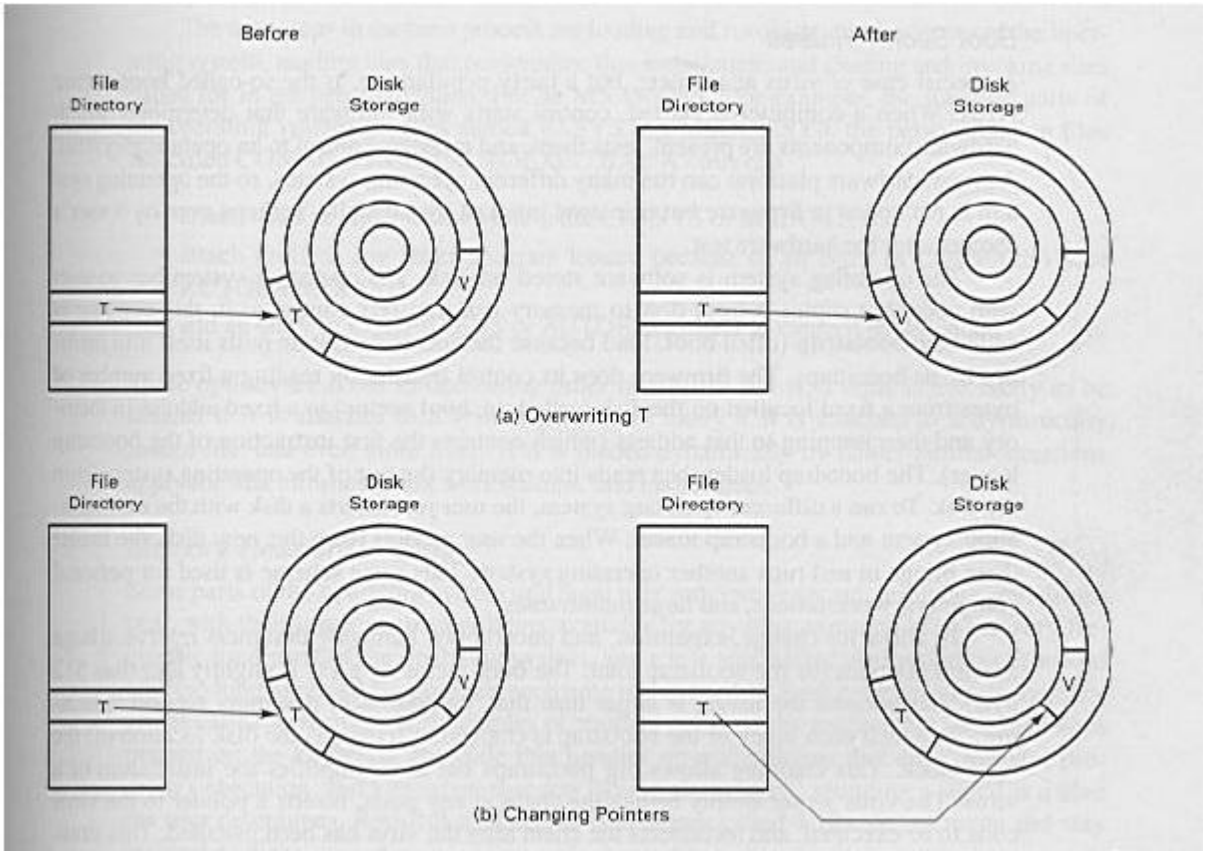
Slika 7. Virus okružuje program, [2]



Slika 8. Virus integriran u program, [2]

Virusi dobivaju kontrolu nad programom (slika 9):

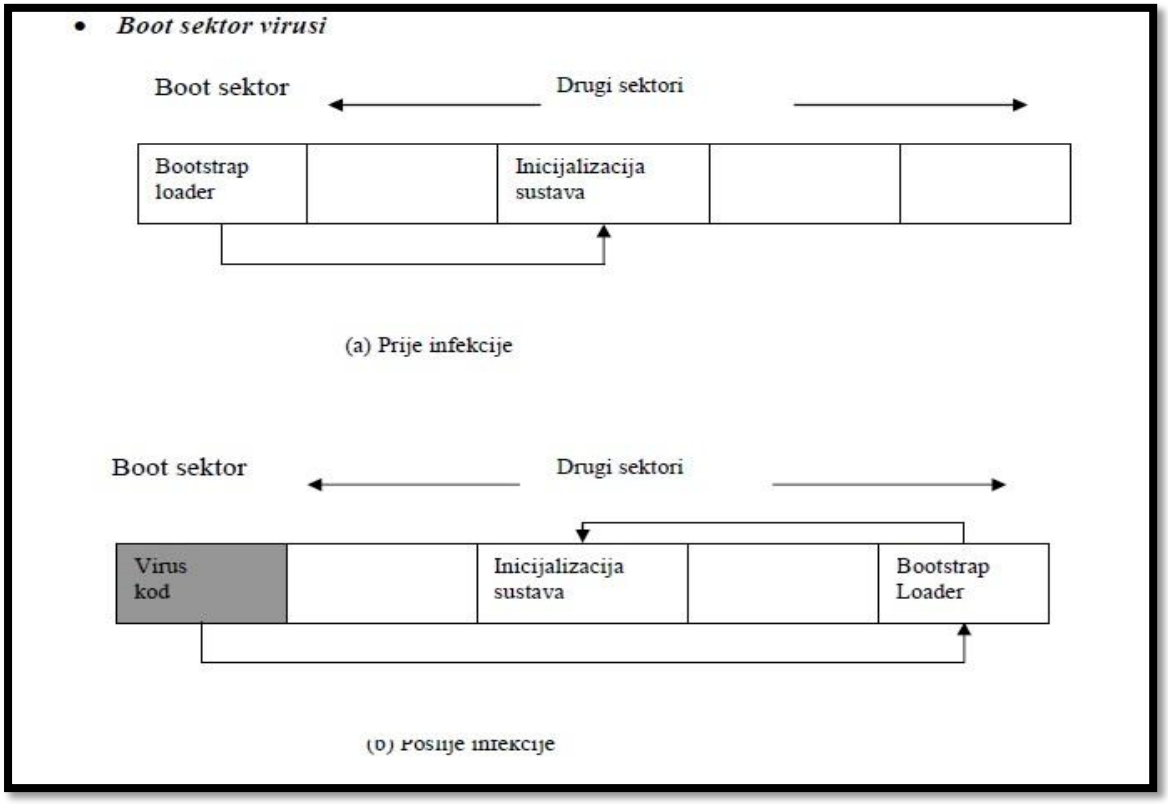
- jednostavnom zamjenom programa T na disku sa virusom V
- primjenom pokazivača u tablici datoteka tako da se locira V umjesto T



Slika 9. Virus potpuno zamjenjuje program, [2]

Kvalitetu virusa pokazuju čimbenici koji pokazuju dali je virus težak za detekciju, težak za uništenje ili deaktiviranje, koliko mu je široko područje širenja te mogućnost reinfekcije, te dali ga je lako kreirati i koliko je i dali je strojno neovisan (neovisan i od OS-a) [9].

Kada se govori o smještaju virusa, odnosno domu virusa postoji podjela na „Boot“ sektor viruse kao što se može vidjeti na slici 10, zatim postoje memorijski rezidentni virusi te ostala domišta za viruse kao što su aplikacijski programi, biblioteke programa, kompilatori, laoderi, linkeri, debugeri [9].



Slika 10. Boot sektor prije i poslije infekcije, [2]

2.5.2. Sprječavanje od virusne infekcije

U sprječavanju od virusne infekcije služe anti-virusni software, fizičke i administrativne kontrole,kriptografska kontrola suma i scanneri.

Napadi virusa koriste (exploit) nedostatak kontrola integriteta informacijskog sustava. Kako bi se obranili moramo sami uključiti te kontrole. Neki od raspoloživih zaštitnih mehanizama su specifični za viruse, ali oni općenito adresiraju integritet.

Strategija obrane treba imati sljedeće komponente:

- Prevenciju: zaustavljanje infekcije sustava.
- Detekciju: detektiranje virusa koji su inficirali sustav.
- Reakciju: restauriranje sustava do čistog stanja.

Administrativne mjere i briga korisnika su važne za uspješnu zaštitu od virusa, [9].

Fizičke i administrativne kontrole su izvrstan put za sprečavanje ulazaka virusa u sustav. Neke od tih mjera su iznenađujući jednostavne. Ako ne želite pisanje na flopy disk postavite zaštitu pisanja, pa niti jedan virus neće moći inficirati disketu. Ako operacijski sustav ima kontrolu pristupa, treba je ispravno iskoristiti. Na primjer treba postaviti skup dozvola za pristup datotekama s aplikacijama na mrežnom serveru samo za čitanje i izvođenje.

Postaviti sigurnosne mjere na mjesta gdje virusi mogu ući u sustav. Testirati novi software na izoliranim računalima gdje je instaliran anti-virusni software. Testirati s računom koji ima samo neka moguća prava, kao što je Gost. Još bolje koristiti prospojeno računalo (gateway) za izvođenje virusnog scanera, ispitati sve diskete koje ulaze u sustav. Ako je floppy disk čisti, on dobiva oznaku te je tada spreman za korištenje unutar organizacije. Ako je oznaka (stiker) na disku, tada je to briga korisnika da detektira neovlašteni disk unutar organizacije. Ako je oznaka elektronička zapisana na disk, tada računalo unutar organizacije može kontrolirati prisutnost oznake i odbaciti neovlašteni disk. Danas su vatro-zidovi (firewall) opremljeni virusnim scanerima za pregled virusa koji dolaze s mreže.

Treba provoditi regularnu (redovitu) kontrolu i držati anti-virusni software ažurnim. Antivirusni software treba uključiti u svaku login skriptu korisnika. Sistemski programi mogu automatski provesti kontrolu u unaprijed određeno vrijeme. Na primjer, u Unixu sistemski administrator može reći cron programu da izvede programe za kontrolu integriteta. Ne treba se oslanjati na samo jednu kontrolu, treba koristiti kombinacije kontrola.

Treba postojati plan za izvanredne situacije (contigency plan), tj. kako reagirati na pojavu virusnog incidenta. Često se događa da neadekvatna reakcija može izazvati više štete nego sam virus. Jasno je, da su čisti back-up-ovi neobično vani za restauraciju IS-a nakon virusnog

napada. Ipak, nije rijetko da se u vrijeme kad je detektiran virus, da je on već nađen na svim backup-ovima koji se čuvaju, [9].

Kriptografska kontrolna suma je standardna tehnika zaštite integriteta. Kontrolna suma se računa za čistu verziju datoteke koju treba zaštititi . Ta se vrijednost sprema na sigurno mjesto, idealno bi bilo u ROM, npr. na CD. Kad god se ta datoteka koristi trenutno izračunata kontrolna suma datoteke se uspoređuje sa usklađenom vrijednošću (VACINE). Bilo koja promjena u originalu će biti detektirana. Tu je jasno da kontrolor kontrolne sume ne mora znati ništa o virusima kako bi detektirao njihovu prisutnost.

Generatori kontrolnih suma su ranjivi kad god se treba ponovno izračunati kontrolna suma ,npr. kada se mijenja datoteka , ili kada se izgubi kontrolna suma. Zato su oni pogodni za korištenje tamo gdje se u organizaciji koriste standardni, već razvijeni programi, a ne tamo gdje se programi razvijaju. Isto tako kontrolori kontrolne sume ne otkrivaju prisutnost određenog virusa koji je izazvao infekciju, to otežava uspostavu plana daljnjih akcija nakon što je infekcija detektirana, [9].

Scanneri pretražuju datoteke za postojanje uzoraka (*virusnih potpisa*) koji identificiraju označeni računalni virus. Evidentno je da oni moraju poznavati virus koji detektiraju, pa prema tome oni se moraju kontinuirano ažurirati na postojanje novih virusa. Scanneri su još uvijek najpopularniji anti-virusni software. Oni se mogu koristiti bez ikakve pripreme, dok se kontrolori kontrolne sume mogu koristiti samo nakon što je kontrolna suma generirana, a scanneri mogu reći točno koji se je virus pojavio, kako bi se mogle poduzeti odgovarajuće akcije.

Posebno je važno da scanneri raspolažu tehnikama za brzo pretraživanje, kako bi bili djelotvorni. Tako da oni mogu kontrolirati samo početak ili kraj datoteke, pa virusi raspršeni kroz kod mogu proći, [9].

Kod zaštite od virusa najbolje koristiti samo komercijalne programe iz pouzdanih i dobro poznatih dobavljača, testirati sve nove programe na izoliranim računalima, nabaviti boot disketu i spremiti podatke na sigurno, napraviti i zadržati kopije sistemskih datoteka za izvođenje, koristiti razne online datoteke za spremanje podataka te redovno korištenje programa za skeniranje virusa i svih datoteka na računalu.

2.5.3. Namjerni, ciljani zloćudni kod (specifičan kod)

Vrata upada (trapdoor) nenamjernih, ciljanih zloćudnih kodova ili kako se znaju nazivati specifični kodovi su kroz zaborav odstranjivanja, namjernog ostavljanja zbog testiranja, namjernog ostavljanja zbog održavanja završenih programa, namjernog ostavljanja u programu kao tajni način pristupa programima nakon što su oni prihvaćeni za produkciju.

U računalu postoje tajni kanali (covert channels), koji ispuštaju informacije a to su memorijski (file lock) kao tajni kanal te vremenski (CPU) tajni kanal [9].

Kod namjernog, ciljanog zloćudnog koda imamo kontrolu, zaštitu od programskih prijetnji, kontrolu putem operacijskih sustava i administrativne procedure. Kontrola, zaštita od programskih prijetnji provodi se kroz modularnost, nezavisno testiranje, zatvorenost, skrivanje informacije, upravljanje konfiguracijom, dokaz ispravnosti programa, verifikacija, pridržavanje standarda ISO9000 i dr.,[9].

Kontrole putem operacijskih sustava se provode povjerljivim operacijskim sustavima, međusobnom zaštitom programa tako da se svaki program posebno zaštiti, ograničavanjem programa s obzirom na pristup sredstvima, zapisima o pristupu sredstvima i dr..

Administrativne procedure su standardi za razvoj programa i njihovo provođenje, sigurnosni nadzor, odvajanje dužnosti (projektant, programer, operater i sl.), [9].

2.6. Digitalna identifikacija i autentifikacija

Identifikacija je osnova za sve aspekte sigurnosti. Svi korisnici, bilo to informacijska sredstva ili korisnici IS-a moraju imati jedinstveni identifikator. Autentifikacija je postupak verifikacije identiteta korisnika. Korisnici uključuju pojedine osobe, računalne uređaje i sredstva.

2.6.1. Identifikacija

Identifikacije unutar tvrtke su vrlo važne. Vrsta identifikacije koju koristi tvrtka uvjetuje sve ostale sigurnosne procese. U globalnoj tvrtki postoji određen broj stvari na koje se treba osvrnuti.

Zbog velikog broja stavki za primjenu identifikatora uvodi se pojam upravljanja imenima,a to su jednoznačnost, univerzalnost, provjerljivost (verifikacija), nekrivotvorljivost, prenosivost (trans portabilnost), lakoća korištenja.

Kod jednoznačnosti je bitno da identifikatori moraju biti jednoznačni kako bi se korisnik mogao pozitivno identificirati. Ista vrsta ili tip identifikatora treba biti raspoloživa za sve korisnike, za pojedince, sustave ili programe. Vrlo važna je povjerljivost, odnosno verifikacija podataka, te treba postojati jednostavan i standardiziran postupak provjere identifikatora radi jednostavnosti arhitekture standardnog sučelja.

Identifikator mora biti težak za krivotvorenje kako bi se spriječilo krivo predstavljanje te mora biti prenosiv sa lokacije na lokaciju, s kojih korisnik treba pristup. Važno je i da identifikator mora biti jednostavan za korištenje u svim transakcijama koje ga zahtijevaju, [2].

Postoje dvije vrste izdavanja identifikatora:

- **Privatno izdavanje -** privatno izdavanje identifikatora daje organizaciji najvišu razinu kontrole.
- **Javno izdavanje -** javno izdavanje zahtjeva razinu povjerenja u organizaciju koja izdaje identifikaciju, [2].

Područje upotrebe identifikatora pokazuje kako široko će se koristiti identifikator, a prema tome koliko široko će on biti prihvaćen. Stoga postoji usko područje korištenja identifikatora koje općenito daje više kontrole lokalnom administriranju sustava te veliko područje koje smanjuje broj potreba za identifikacijom i autentifikacijom. Koncept jedne prijave (single-sign-on SSO) se zasniva na području koje uključuje sve što bi korisnik mogao trebati.

Administriranje identifikatora uključuje kreiranje i opoziv identifikatora, proces distribucije identifikatora, te integraciju identifikatora u autentifikaciju, autorizaciju i administraciju sustava. Postoji centralizirana administracija te distribuirana administracija.

Identifikacija mora biti raspoloživa svim pristupnim metodama. Standardi imenovanja su izgrađeni na X.500, OSI standardu za usluge imenika (directory service: Active directory, LDAP).

Smart kartice se mogu koristiti kako za fizičku identifikaciju tako i za elektroničku (digitalnu) identifikaciju. Fizička identifikacija se zahtjeva kako bi se osigurala fizička sigurnost. Elektronička (digitalna) identifikacija se koristi za svaki elektronički pristup, [2].

Upute (vodič) za izbor identifikatora (Check list) su kao prvo odrediti što će se koristiti za identifikatore, odlučiti tko će izdavati identifikatore, zatim postaviti zahtjeve neophodne za izdavanje identifikatora, odrediti zahtjeve na identifikaciju za svaku klasu transakcija, odrediti kako će se identifikacija administrirati, izlistati zahtjeve za izdavanje, odrediti razloge za izdavanje, odrediti razloge za opoziv te odlučiti kako će se informacija o identifikatorima implementirati i koristiti, [2].

2.6.2. Autentifikacija

Faktori koji se mogu koristiti za autentifikaciju identiteta nekog entiteta su oni faktori koji su jedinstveni za taj specifični entitet. Postoje osnovni, implicitni i višestruki faktori.

Osnovni faktori:

- Nešto što znate – dijeljena tajna, lozinka, nešto što korisnik i autentifikator znaju.
- Nešto što imate – fizički ID (npr. identifikacijska kartica, token, smart kartica)
- Nešto što jeste – mjerljiva svojstva (otisak prsta, facijalne karakteristike, boja glasa..)

Implicitni faktori su atributi entiteta koji se mogu odrediti bez interakcije sa entitetom.

- Fizička lokacija
- Logička lokacija.

Višestruki faktori predstavlja općenito korištenje više faktora u autentifikaciji transakcija daje jaču autentifikaciju, [2].

Autentifikacija je verifikacija identiteta kako bi se spriječila impersonalizacija (krivo predstavljanje), te kako bi se osigurala razina povjerenja koja je nužna za korištenje ovlaštenja (autorizacija). Vrsta zahtijevane autentifikacije zavisit će od kvalitete identifikatora, pristupne metode, i zahtijevanih ovlaštenja (privilegija).

U modelu višestruke autentifikacije svaka aplikacija ima potpunu kontrolu korištenog identifikatora za entitet i metode za autentifikaciju. Jednostruka autentifikacija (SSO) po sjednici, single sign-on (SSO), velika je prednost za korisnike.Višerazinska autentifikacija je proces koji zahtjeva različite vrsta autentifikacije koje ovise o metodi pristupa, zahtijevanim sredstvima, te zahtijevanim dozvolama, [2].

Razina i vrsta autentifikacije zavisi od vrste identifikatora, pristupne metode, zahtijevane autorizacije, te područja koje je pokriveno autentifikacijom tako da imamo:

a) Dvostrana autentifikacija

Dvostrana autentifikacija može imati jednosmjernu i dvosmjernu shemu.

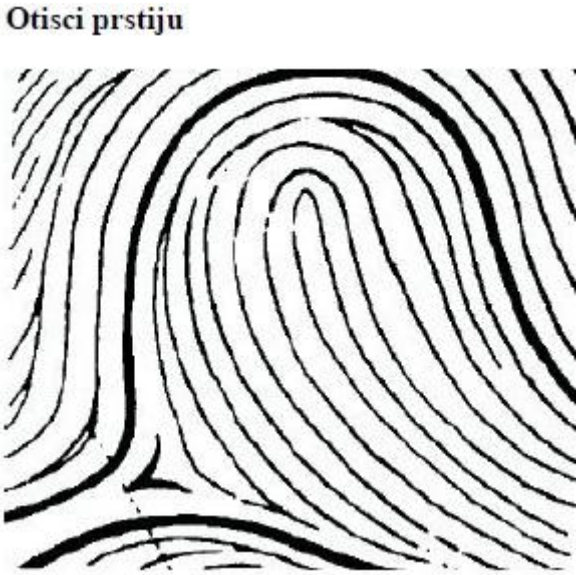
Autentifikacijska informacija može biti ili statička (npr. fiksna lozinka) ili dinamička (npr. one-time lozinka OTP). Postoje razne vrste autentifikacija koje imamo nabrojane u nastavku teksta, [2].

Lozinke su jedna vrsta autentifikacija, postoje tako ponovljive lozinke koje su najraširenija metoda za autentifikaciju danas (PAP), zatim one-time password (OTP) lozinke koje se koriste za jednu upotrebu, tako da ako i budu uhvaćene i otkrivene, više se ne koriste i svakako su dosta siguran oblik zaštite i na kraju postoje takozvane lozinke pobude-odziva (CHAP) koje su druga metoda lozinki i rješavaju problem njuškanja lozinki po mreži. Shema autentifikacije pobuda/odziv je shema zasnovana na lozinkama u kojoj server postavlja pitanje korisniku - to znači postavlja izazov (pobudu), a korisnik mora odgovoriti na odgovarajući način ili autentifikacija završava u grešci, [2].

Dok je OTP lozinka valjana samo za jednu sjednicu autentifikacije, ne prije i ne poslije.(**S/KEY**),[2]. Tu postoje token kartice kod kojih se posjeduje uređaj koji donosi lozinke. Token kartice generiraju različiti niz od osam znakova svaki puta kad se upotrijebi, pa je ona specijalni slučaj OTP sheme.

Smart kartice opisiuju komplet malog, veličine kreditne kartice, elektroničnog uređaja koji se koristi za pohranu podataka i identifikaciju. I na kraju ručni uređaji za autentifikaciju koji se skupa nazivaju HHAD, a to su prenosivi uređaji, obično po veličini kreditnih kartica, koji imaju lokalno spremište podataka i mogućnost računanja. To su kartice zasnovane na sekvenci, kartice zasnovane na vremenu, kartice zasnovane na certifikatima, [2].

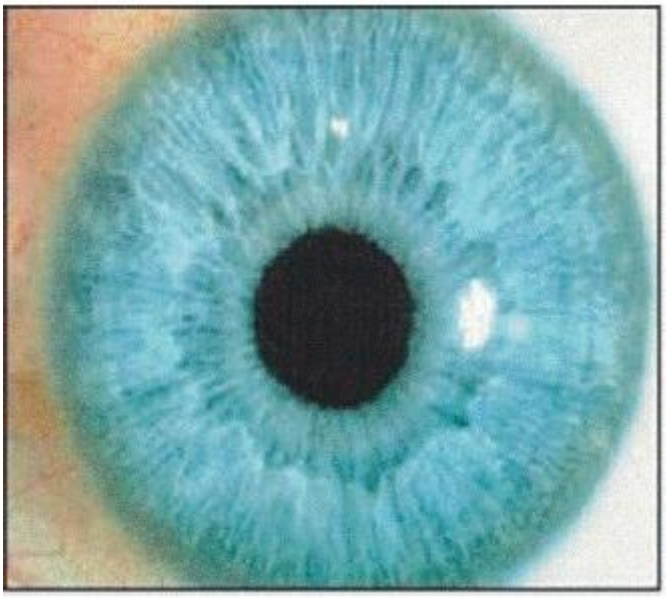
Biometrička autentifikacija koristi jedinstvenost izvjesnih fizičkih svojstava i karakteristika pojedinaca, kao što su otisci prstiju, slika rožnice oka, uzorak glasa ili facijalne karakteristike kao što je prikazano na slikama 11,12 i 13. Ta fizička svojstva ili karakteristike mogu se reprezentirati digitalno kao biometrički podatak ili biometrija, [2].



Slika 11. Otisci prstiju, [2]



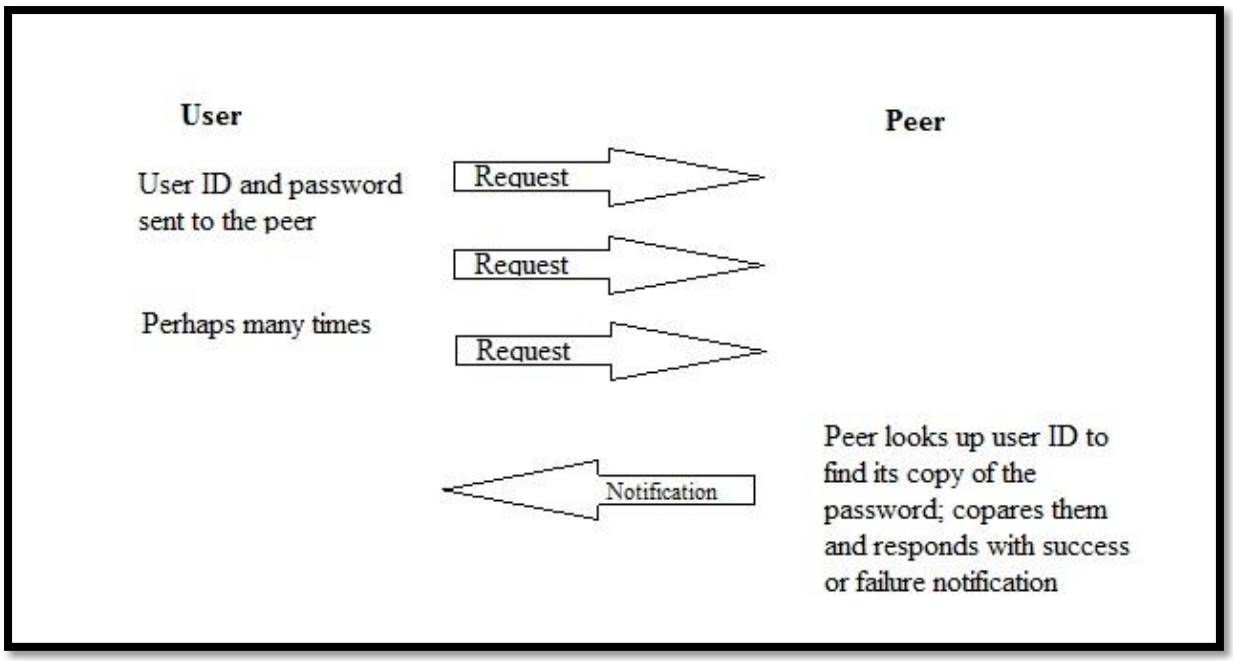
Slika 12. Skener otiska prsta, [2]



Slika 13. Skeniranje rožnice oka, [2]

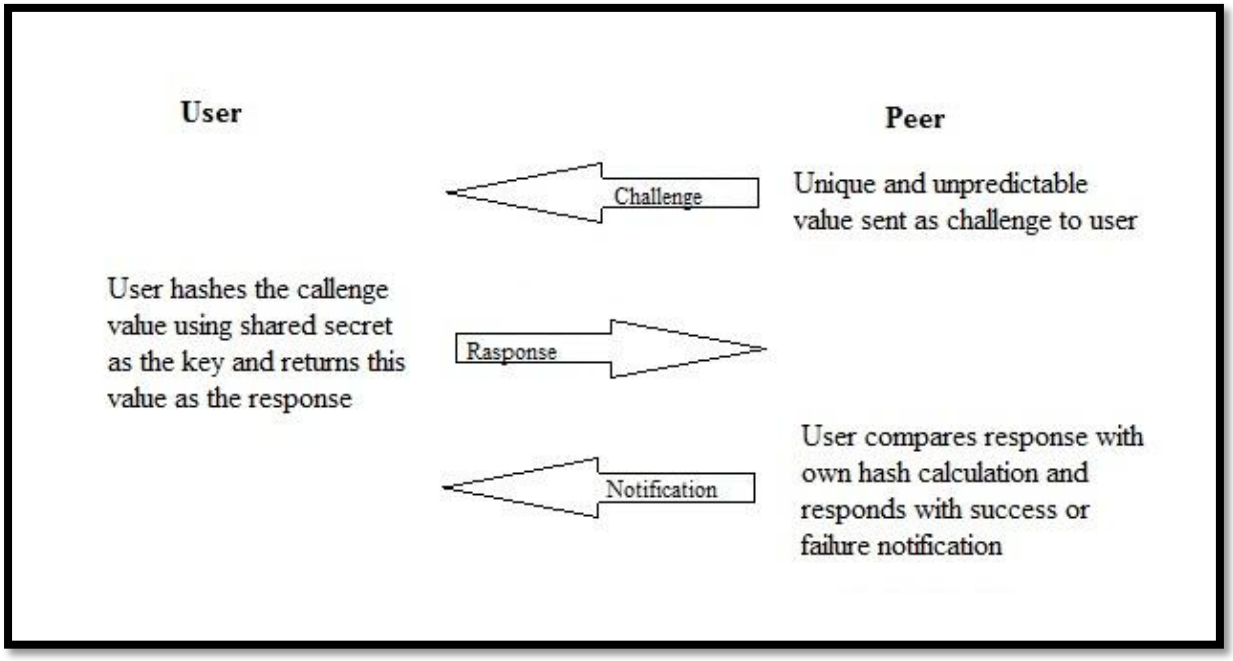
PPP autentifikacija, odnosno PPP protokol (Point-to-Point Protocol) osigurava standardnu metodu za enkapsulaciju informacije mrežnog protokola na linijama od točke-do-točke. Da bi se uspostavila veza preko komunikacijske linije, svaki kraj linije mora prvo razmijeniti Link Control Protocol (LCP) pakete kako bi dogovorio konfiguraciju veze koja će se uspostaviti. On uključuje i protokol autentifikacije, [2].

PAP, Password Autentification Protocol (RFC 1334), osigurava jednostavnu metodu za korisnika za uspostavu njegova identiteta koristeći dvosmjernu razmjenu, kako je pokazano na slici 14, [2].



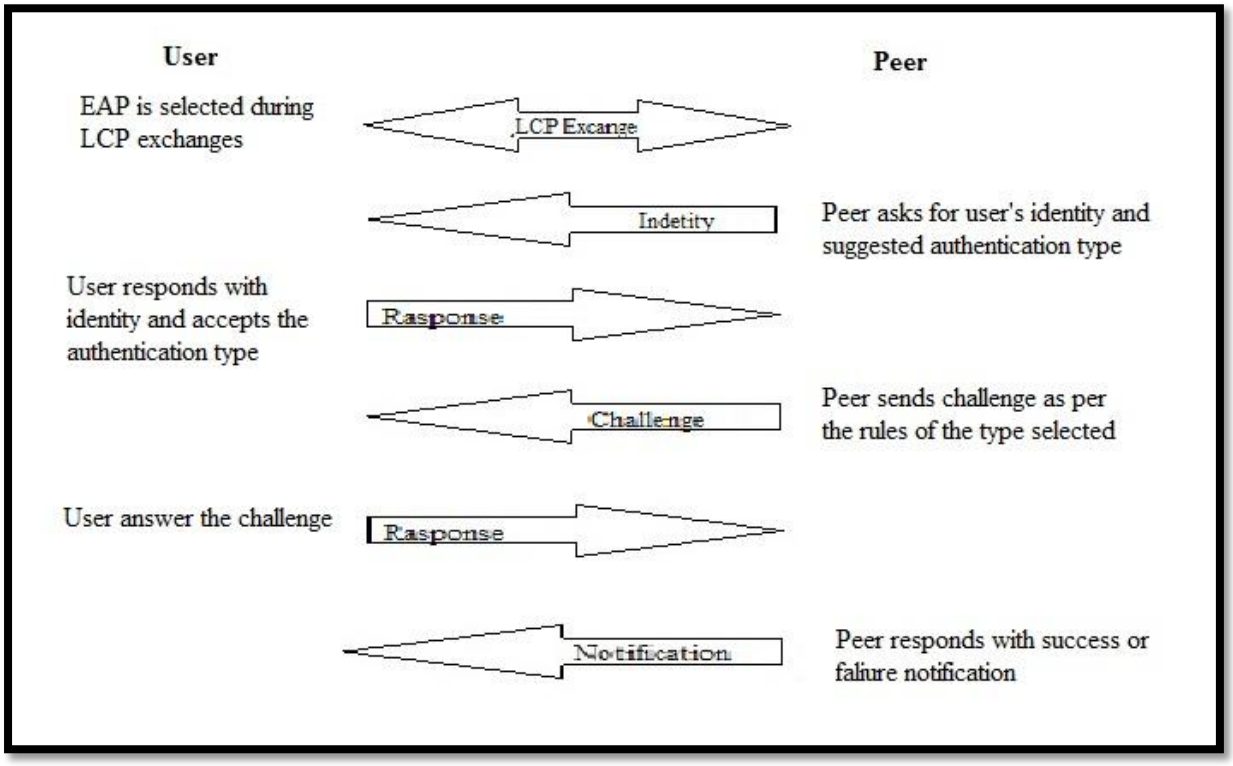
Slika 14. Dvosmjerna PAP razmjena, [2]

CHAP, Challenge Handshake Autentification Protocol (RFC 1994) je trosmjerna razmjena koja se koristi da se verificira korisnika na PPP vezi (Slika 15), [2].



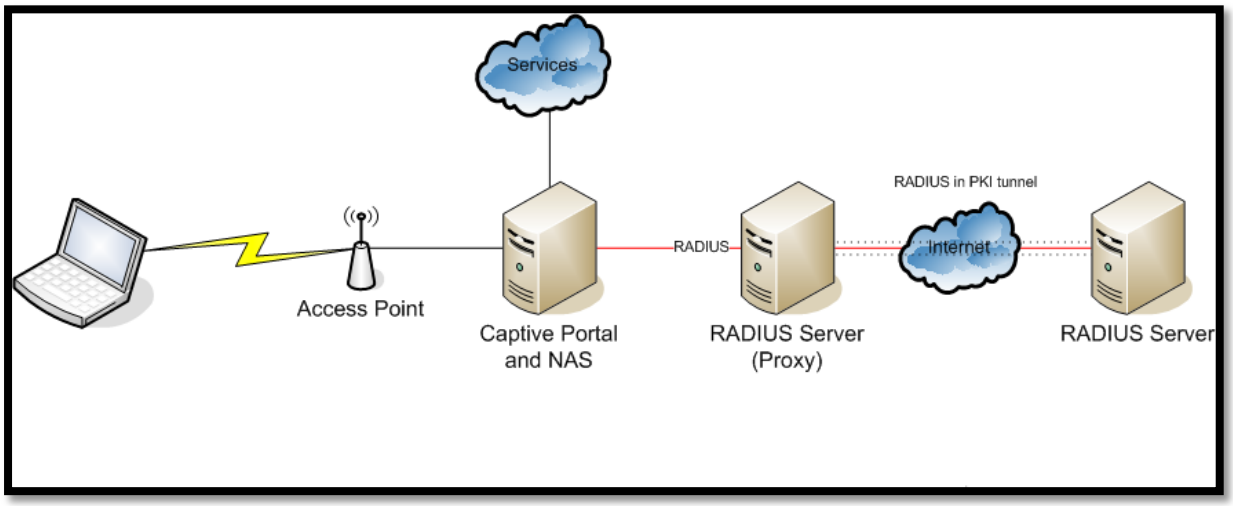
Slika 15. Trosmjerna CHAP razmjena, [2]

EAP je proširivi autentifikacijski protokol (engl. *EAP- Extensible Authetification Protocol*) (RFC 2284) je općeniti autentifikacijski protokol koji podržava višestruke autentifikacijske mehanizme. Autentifikacijska razmjena je pokazana na slici 16, [2].



Slika 16. Trosmjerna EAP razmjena, [2]

Sa RADIUS-om (engl. *Remote Access Dial In user Service* – RFC2138) autentificiraju se udaljeni korisnici, koji se spajaju preko biranih linija. Tipična RADIUS autetifikacijska sjednica u dial-in uvjetima radi kao na slici 17, [2].



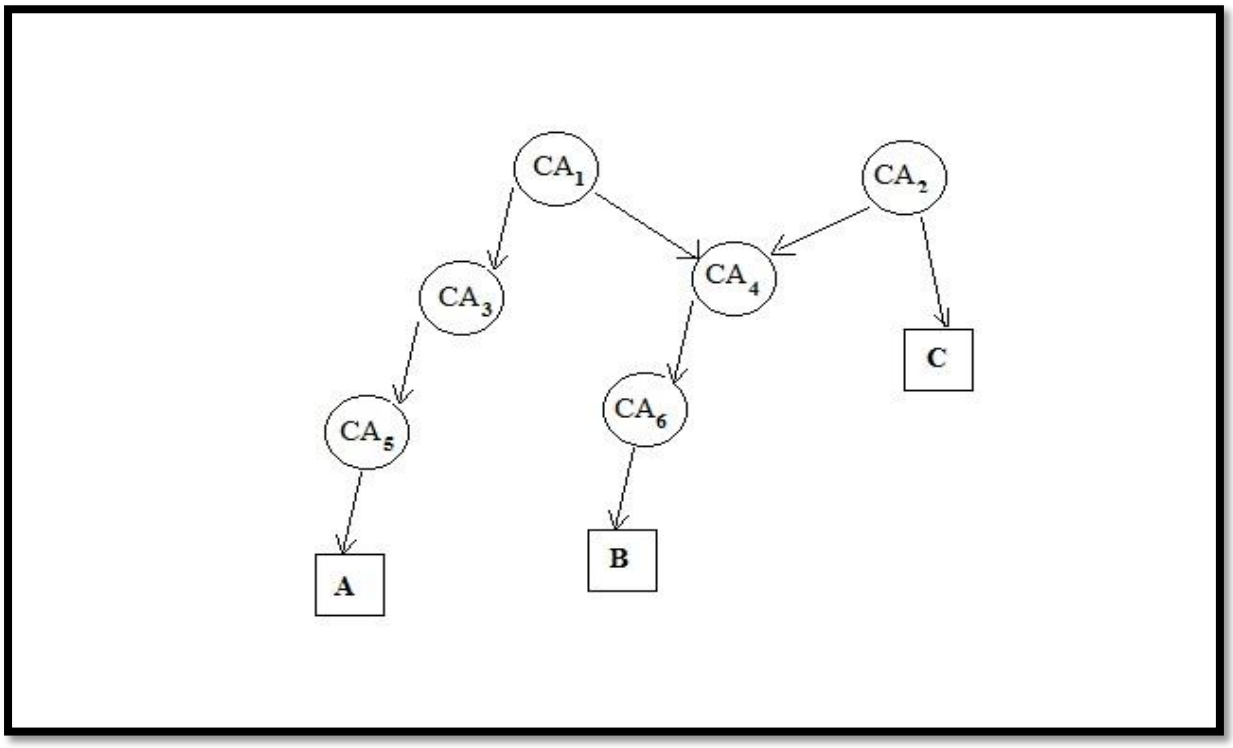
Slika 17. Radijus autetifikacijska sjednica u dial-in uvjetima, [12]

Sa S/KEY i OTP je ideja da korisnik i uslužno mjesto svako konstruira dugu listu OTP lozinki, svaka sljedeća proizašla je iz prethodne,[2].

b) Autentifikacija kroz povjerljivu treću stranu

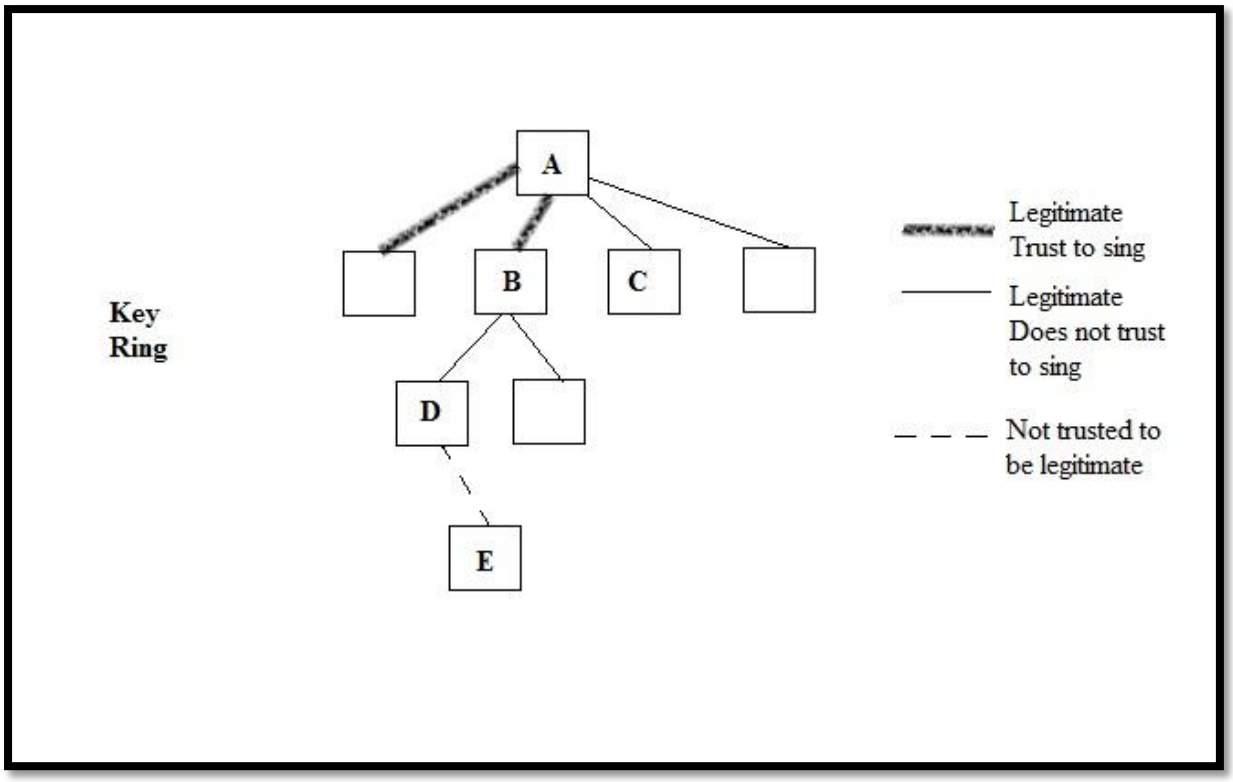
Kerberos je mrežni autentifikacijski sustav (RFC 1510) koji omogućuje verifikaciju identiteta entiteta u otvorenoj i nezaštićenoj mreži koji koristi treću povjerljivu stranu (opisan kasnije u mrežnoj sigurnosti), [2].

PKI infrastruktura specificirana je od strane ITU (International Telecommunication Union) kroz X.509 standard (slika 18) (ITU97) (prije CCITT X.509), te definira okvir za provođenje autentifikacije kroz mrežu korištenjem kriptografije javnog ključa, [2].



Slika 18. X-509 certifikacijska hijerarhija, [2]

PGP (Pretty Good Privacy) povjerljivi model (slika 19) - PGP (Zimmerman 1995) je familija softwarea koji je razvio Philip R. Zimmerman zaštitu i sigurnost elektroničke pošte, kroz enkripciju njenog sadržaja i autentificiranje njenog pošiljaoca, [2].



Slika 19. PGP mreža povjerenja, [2]

c) Autentifikacija u VPN-u

Uloga autentifikacije u VPN-u je da se verificira identitet strana uključenih u uspostavu VPN tunela. Tu onda imamo:

- Autentifikacija između prospojnika,
- Autentifikacija klijent-prospojnik.

Upravljanje autentifikacijom treba biti jednostavno i integrirano u upravljanje identifikatorima. Autentifikacijski server je sustav koji kontrolira autentifikaciju za potrebe IS tvrtke. On sadrži centralni repozitorij identifikatora, te odgovarajućih autentifikacijskih metoda za svaki identifikator koje su zasnovane na pristupnoj metodi i zahtijevanim ovlaštenjima.

Autentifikacija zahtjeva da entitet koji se autentificira šalje potvrde (vjerodajnice) entitetu koji provodi autentifikaciju, [2].

U procesu autentifikacije pojavljuju se direktni i indirektni napadi. Direktni napadi su napadi na sam proces autentifikacije, a to su pogađanje i razbijanje (cracking). Pogađanje je postupak pogađanja autentifikacijskih tokena sve dok se ne pogodi jedan ispravan, a razbijanje je proces stvarnog izračunavanja lozinki.

U indirektne napade spadaju njuškanje kao proces prisluškivanja dok se sam identitet autentificira, te prihvat autentifikacijske informacije, dohvat i odgovor kao proces dohvata autentifikacijske komunikacije i odgovor na nju, tako da autentifikator misli da se entitet reautentificira, otimanje sjednica kao krađa sjednice nakon što je provedena autentifikacija, socijalni (društveni) napadi kao napadi na pojedince u pokušaju da oni obznane token za autorizaciju, socijalni inženjering kao proces uvjeravanja nekoga da je sigurno otkriti željenu informaciju, istraživanje kao proces otkrivanja korisničke pozadine kako bi se skupilo dovoljno osobnih informacija koje bi omogućile određivanje vjerojatnih tokena, pretraživanje kao proces fizičkog pretraživanja za tokene koji pripadaju korisnicima te na kraju prisluškivanje kao proces promatranja korisnika koji unosi token, [2].

Važno je odrediti i primjeniti odgovarajuću autentifikaciju (Check list). Zbog toga postoje upute i vodiči za pravilan izbor i primjenu autentifikacije prema kojima se prvo određuje odgovarjuća metoda za autentifikaciju unutar pojedine tvrtke te se onda standardiziraju autentifikacijski postupci kroz cijelu tvrtku.

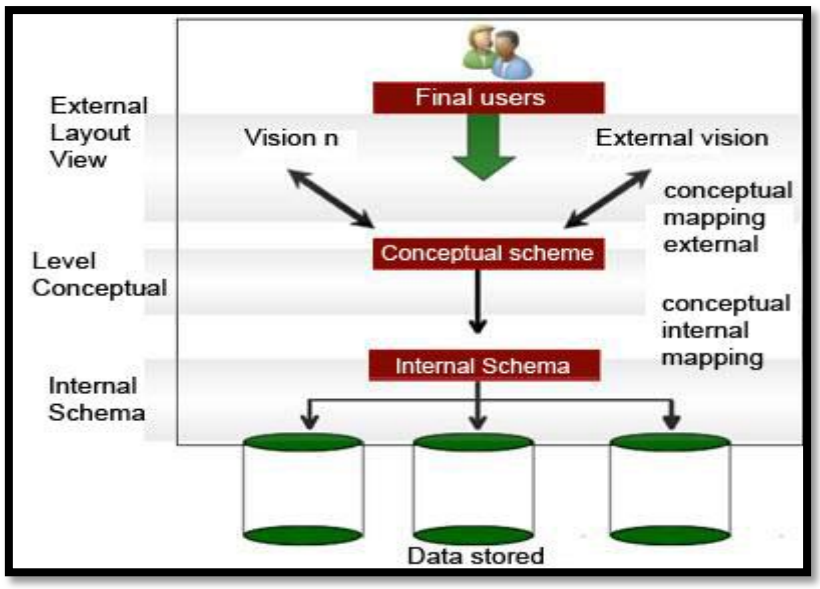
2.7. Sigurnost baza podataka

U koncepte baza podataka spadaju data base managment system (DBMS), konceptualni modeli (ER-model), logički modeli koji mogu biti hijerarhijski, mrežni, relacijski, objektni, zatim shema baze podataka (konceptualna ili logička) te jezici DDL, DML, QL), [2].

Dijelovi DBMS-a (slika 20) su DDL kompilacija, obrada DML instrukcija, upiti u bazu podataka, upravljanje bazom podataka, upravljanje datotekama, [2].

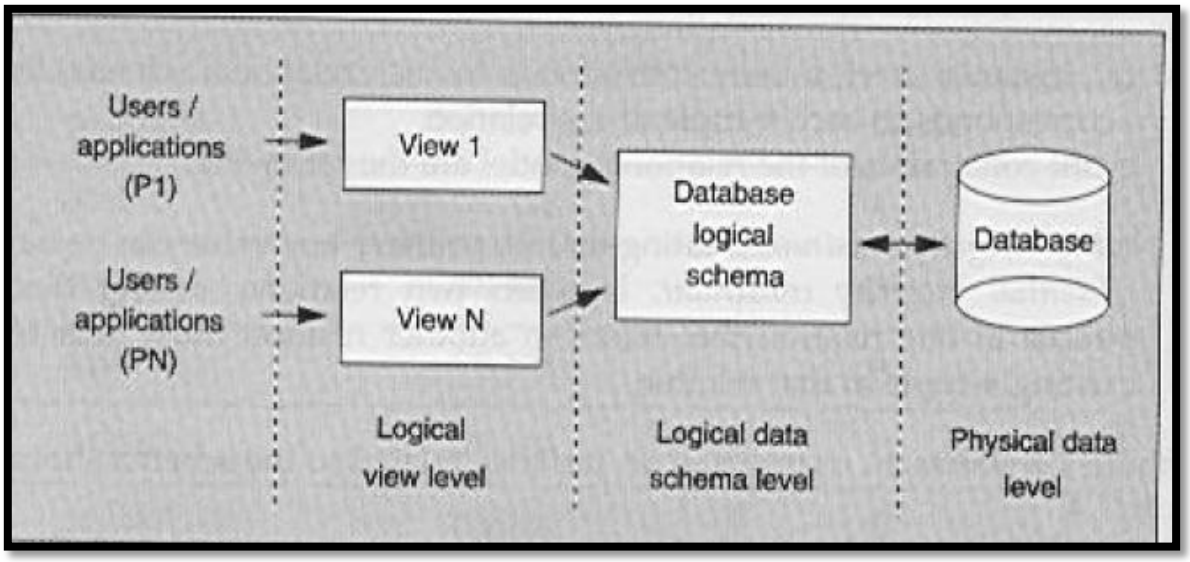
Skup tabela daje podršku funkcionalnosti ovih modula:

- Tablice opisa baze podataka
- Tablice autorizacije (ovlaštenja)
- Tablice konkurentnih (istovremenih) pristupa, [2].



Slika 20. Arhitektura DBMS-a, [4]

Razine opisa podataka (slika 21) prikazuju se kroz logičke poglede, logičke sheme podataka i fizičke sheme podataka.



Slika 21. Razine opisa podataka, [2]

Postizanje sigurnosti u uvjetima baza podataka znači identificiranje prijetnji i izbor politika (to se od sigurnosti očekuje) i mehanizama (kako će sigurnosni sustav postići sigurnosne ciljeve). To također uključuje postizanje jamstva sigurnosnog sustava (kako dobro će sigurnosni sustav ispuniti sigurnosne zahtjeve i izvršiti očekivane funkcije).

Kršenje sigurnosti baza podataka se sastoji od neodgovarajućeg (neovlaštenog) čitanja, izmjene ili brisanja podataka. Posljedice se mogu kategorizirati u tri kategorije:

- Neovlašteno oslobađanje informacija,
- Neovlaštena izmjena podataka,
- Odbacivanje usluga (DoS), [2].

Sigurnosne prijetnje se mogu klasificirati prema načinu na koji mogu nastati a to su prirodne ili slučajne nepogode, greške ili bug-ovi u HW i SW i na kraju dolaze ljudske greške kao čest slučaj nastajanja prijetnji, [2].

Kod kršenja sigurnosti postoje dvije klase korisnika. U jednu klasu spadaju ovlašteni korisnici koji zlorabe svoja prava i ovlaštenja, a u drugoj klasi su neprijateljski agenti i neovlašteni korisnici (insideri i outsideri), [2]. Mogu se podnijeti zahtjevi za zaštitu baza podataka, i to za zaštitu od neovlaštenog pristupa i zaštitu od zaključivanja (inference).
Integritet (cjelovitost) baza podataka

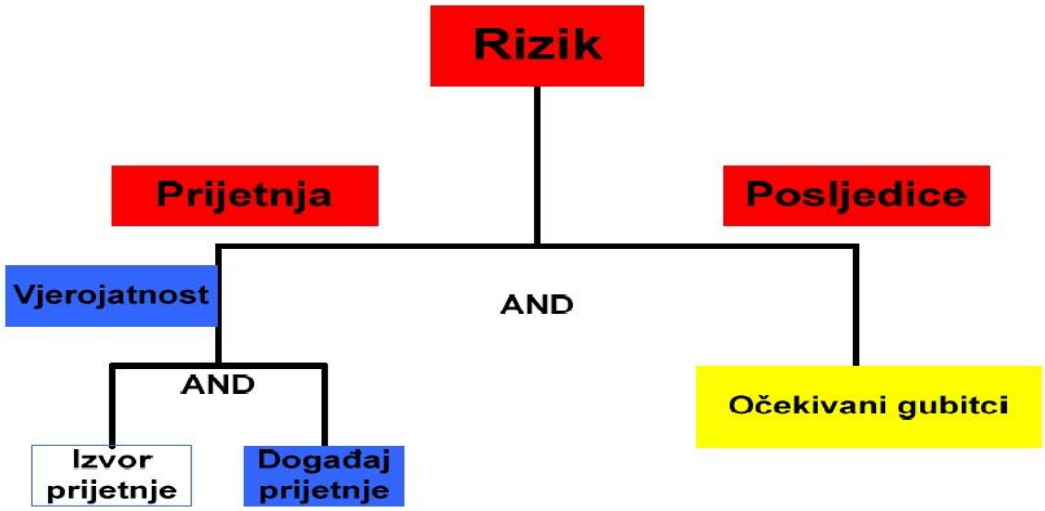
Zaštita baze podataka se postiže kroz kontrolu toka, kontrolu zaključivanja o podacima i kontrolu pristupa.

Kada se govori o kontroli toka govori se o toku između objekta X i objekta Y koji se događa kad naredba čita vrijednost iz X i upisuje vrijednost u Y. Kontrola toka provjerava da informacija koja je sadržana u nekom objektu (npr. izvješću) ne odlazi eksplicitno (kroz kopiranje) ili implicitno (preko grupe instrukcija koje uključuju među objekte) u nezaštićene objekte, [2]

Kontrola zaključivanja usmjerena je na zaštitu podataka od indirektne detekcije. Kanal zaključivanja je kanal gdje korisnici mogu naći podatak X i tada ga koriste da bi dobili Y kao Y = f(X). Glavni kanali zaključivanja u sustavu su indirektni pristup, korelacijski podaci i nepostojeći podaci. Statistički napadi mogu se spriječiti kroz dvije vrste kontrole, preturbacijom podataka i kontrolom upita. Izgradnja sigurnosti baze podataka se može provoditi na vanjskoj razini (fizička sigurnost) i na internoj razini (logička sigurnost), [2].

3. Rizik informacijskog sustava

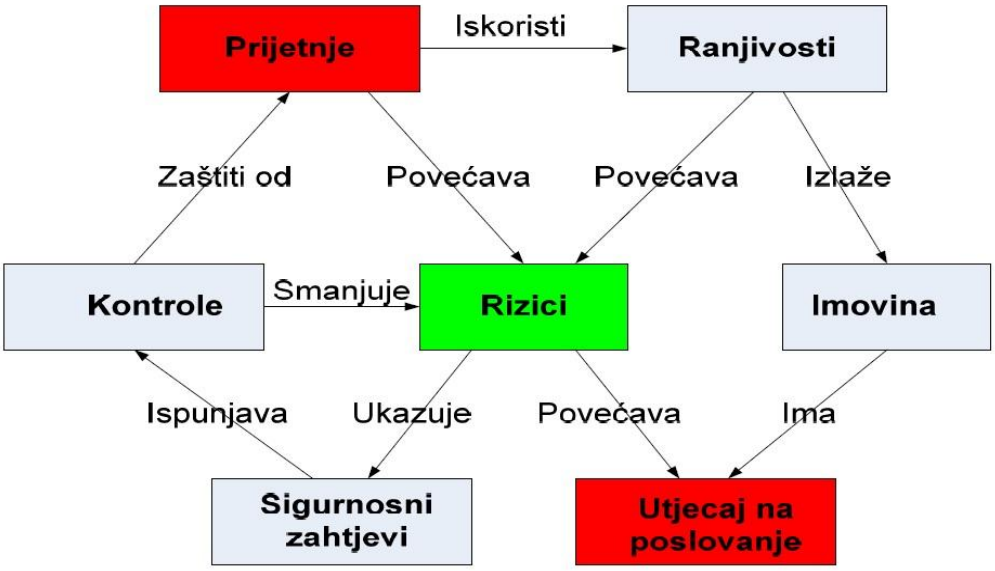
Planiranje sigurnosti informacijskog sustava uvijek počinje s analizom rizika (slika 22).



Slika 22. Grananje rizika, [2]

Sigurnosni zahtjevi se identificiraju metodičkom procjenom sigurnosnih rizika. Proširenje sigurnosnih kontrola mora biti proporcionalno šteti koju sigurnosni propusti nanose organizaciji. Rezultati procjene rizika pomažu u određivanju prioriteta i prikladnih akcija kod upravljanja sigurnosnim rizicima. Procjena rizika se mora provoditi periodički kako bi se u procjenu uključile bilo kakve promjene koje bi mogle utjecati na rizik, [1].

Rizik se pretpostavlja od strane vlasnika ili administratora sustava, a to je vjerojatnost da sustav neće biti u mogućnosti provoditi sigurnosnu politiku., uključujući i kontinuiranost kritičnih operacija u toku izvođenja napada. Rješanja su izbjegavanje, upravljanje, prihvaćanje i transfer. Pod pojmom upravljanja rizikom smatra se donošenje odluke o prihvaćanju rizika, smanjenju rizika i prijenosu rizika, [2].

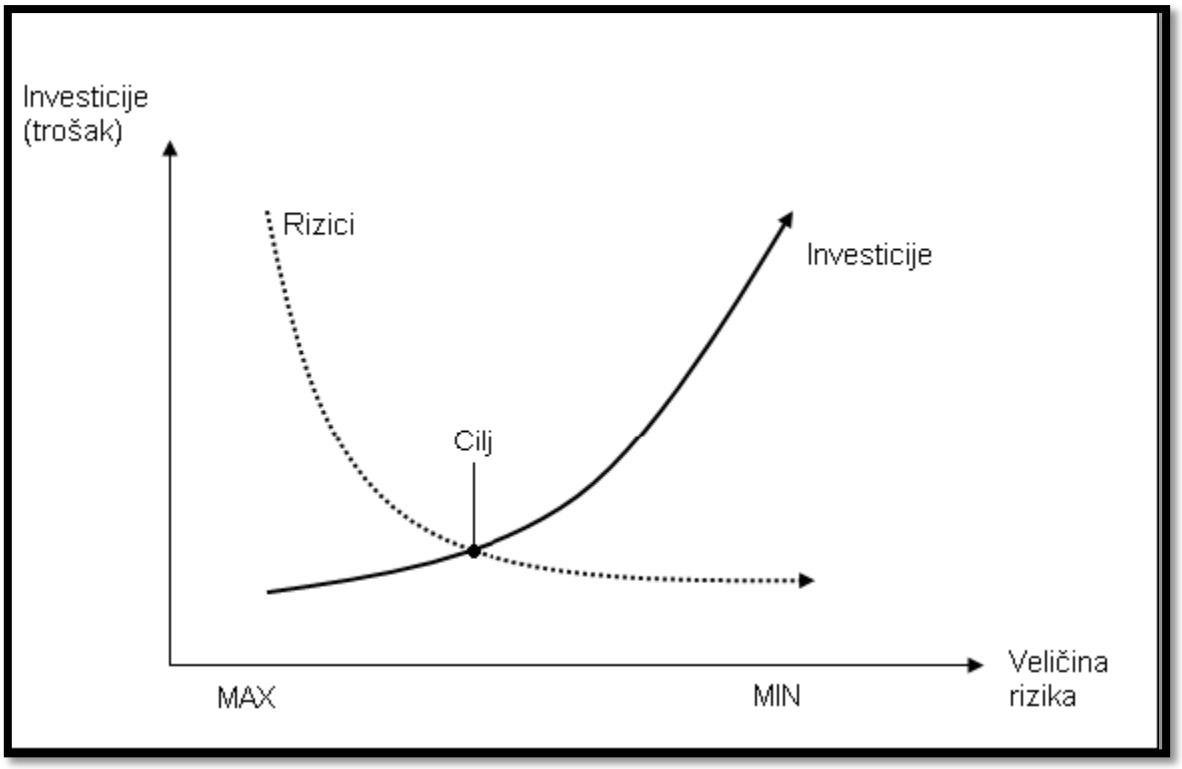


Slika 23. Proces smanjenja rizika, [2]

Koraci analize rizika:

- Identifikacija računalnih (informatičkih) sredstava.
- Određivanje ranjivosti.
- Procjena vjerojatnosti pojave i eksploatacije ranjivosti.
- Izračunavanje očekivanog godišnjeg gubitka.
- Pregled primjenjivih kontrola i njihovih cijena koštanja.
- Projekcija godišnjih ušteda prouzrokovanih uvođenjem kontrola, [2].

Pod pojmom ranjivosti smatraju se svi propusti i slabosti u sustavu sigurnosti koji omogućuje provođenje neovlaštenih aktivnosti. Ranjivost se najčešće povezuje s propustima u programskom kodu, no mogući su i mnogi drugi primjeri, kao što su površno implementirana fizička sigurnost, nedovoljno poznavanje i neprikladan izbor tehnologija i alata, propusti u dizajnu sustava, propusti u implementaciji i održavanju sustava i sl. Bez adekvatne analize ranjivosti (slika 24), gotovo je nemoguće pouzdano odrediti sigurnosni rizik. Sama logika nas navodi na to da tamo gdje nema rizika nema smisla ulagati u zaštitna sredstva, implementiraju se samo ona zaštitna sredstva koja će biti opravdana i smislena u pogledu zaštite poslovnih ciljeva organizacije, [1].



Slika 24. Graf procjene prihvatljivog rizika, [1]

Nakon što se identificiraju sigurnosni zahtjevi i napravi procjena rizika, potrebno je izabrati i implementirati prikladne kontrole kako bi se rizik sveo na prihvatljivu razinu. Izbor kontrola ovisi o organizaciji, odnosno prihvatljivosti rizika i načinu upravljanja rizikom, ali i o nacionalnim i međunarodnim zakonskim pravima i obvezama, [1].

Kontrole presudne za organizaciju postizanja informacijske sigurnosti sa zakonske točke gledišta su zaštita informacija i tajnosti osobnih podataka, čuvanje organizacijskih izvještaja te poštivanje prava intelektualnog vlasništva, [1]. Kontrole koje u praksi postižu dobre rezultate kod implementacije informacijske sigurnosti su sigurnosna politika, podjela odgovornosti informacijske sigurnosti, svijest o informacijskoj sigurnosti te edukacija i trening, zatim ispravno procesiranje podataka u aplikacijama, upravljanje ranjivostima, upravljanje poslovnih kontinuitetom i upravljanje sigurnosnim incidentima i poboljšanjima sustava, [1].

Postoje praktični razlozi za uvođenje politike i sustava osiguranja informatičke djelatnosti (ISMS Information Security Management System) sposobnih da se nezavisno

certificiraju u skladu s normama. Proces certifikacije prisiljava tvrtku da se usmjeri na neprekidno poboljšanje svojih procesa informatičke zaštite putem redovitih vanjskih nezavisnih kontrola i da omogući izgraditi od početka sustav sigurnosti kao i neprekidnu sposobnost operativnosti, [1].

Poslovne koristi od certifikata su smanjivanje sigurnosnih rizika, prepoznavanje i smanjivanje sigurnosnih rizika na željenu razinu, poboljšanje poslovnih odnosa (veće povjerenje u međusobno razmjenjivanje informacija), investicije na prava akutna mjesta, optimizirana poslovna partnerstva, upravljanje sigurnošću te upravljane procesima sigurnosti informacija. Standard sadrži strukturirani set smjernica i specifikacija za pomoć organizacijama u razvoju sustava upravljanja informacijskom sigurnošću.

3.1. Norme za informacijsku sigurnost

Norme su javno objavljene specifikacije koje u domeni informacijske sigurnosti daju metodologiju kako riješiti pojedine aspekte informacijske sigurnosti.

Danas je na tržištu prisutno mnogo normi, referenci i savjeta za uspostavu sigurnosti u informacijske sustave, no dva najpoznatija standarda zasigurno su ISO/IEC 17799 i ISO/ IEC 27001.Standardi ISO/IEC 17799 i 27001 se međusobno ne isključuju. Naprotiv, za uspostavu kvalitetnog sustava upravljanja sigurnošću informacija nužno je koristiti oba standarda. Neke od normi su nabrojane i pojašnjenje u nastavku teksta, [2].

ISO (eng. *the International Organization for Standardization*) i IEC (eng. *The International Electrotechnical Commission*) dva su tijela koji zajedno čine sustav za međunarodnu standardizaciju.

3.2. ISO/IEC 17799

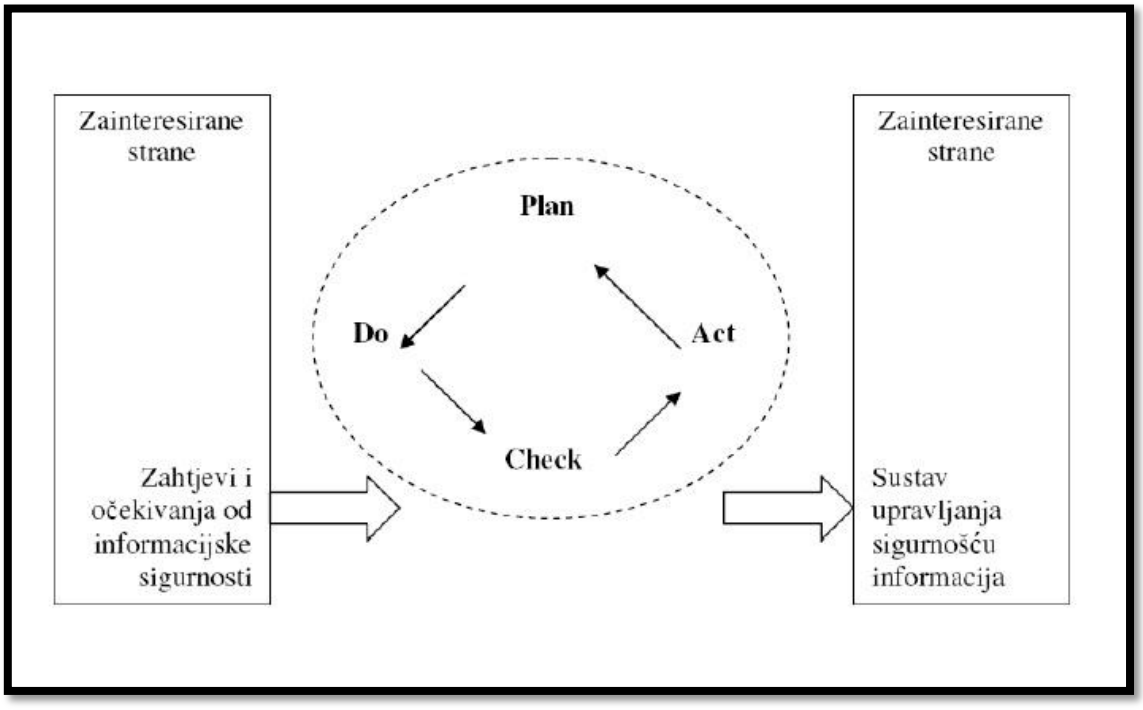
ISO/IEC 17799 je norma formulirana na mnogim postavkama BS 7799 (eng. *British Standards*) norme koja od 1995., kada je donesena, predstavlja najrašireniji pokušaj uvođenja međunarodno priznatih normi na području upravljanja informacijskom sigurnošću. ISO/IEC ističe da 17799 nije prvenstveno namijenjen certificiranju, već širenju svjesnosti o potrebi organizacije sustava zaštite informacija kroz opis najboljih već primijenjenih metoda i principa za uspostavu i održavanje takvih sustava, [1].

ISO 17799:2005 norma razlikuje provjeru sigurnosne politike, ljudskih resursa, komunikacija i operativnog sustava, nabavu, organizaciju i održavanje IT sustava, odgovor na incidente te općenito pridržavanje uobičajenih poslovnih običaja. Najveći dio dokumenta odnosi se na provjeru sustava komunikacija i ostalih informacijskih tehnologija koje se koriste u poslovnim procesima.

3.3. ISO/IEC 27001:2005

ISO/IEC 27001:2005 je standard objavljen u listopadu 2005. godine, razvijen je na temeljima BS 7799 standarda, točnije njegovog drugog dijela. Namjena ovog standarda je kvalitetna uspostava sustava upravljanja sigurnošću informacija (ISMS), a sadrži skup zahtjeva koje organizacija mora ispuniti da bi se priznao certifikat za informacijsku sigurnost. Iako standard 27001 obuhvaća izradu sigurnosne politike, njegova prvenstvena uloga je način implementacije sigurnosnih kontrola i samim time nije prikladan kao temelj pisanja sigurnosne politike, [1].

ISO/IEC 27001 upotrebljava *PDCA (engl. Plan-Do-Check-Act)* model (slika 25). Ovaj model ističe važnost pažljivog planiranja programa uspostave sustava, što rezultira efikasnim mjerama za njegovo trajno poboljšanje i pravilnu uporabu, [1].



Slika 25. PDCA model, [1]

3.3. ISO/IEC 17799:2005

ISO/IEC 17799:2005 sastoji se od 11 domena sigurnosnih kontrola koje zajedno sadrže 39 osnovnih sigurnosnih kategorija i jednu uvodnu domenu koja nas upoznaje s procjenom rizika.

Domene su:

1) Sigurnosna politika
2) Organiziranje informacijske sigurnosti
3) Upravljanje imovinom
4) Sigurnost i ljudski resursi
5) Fizička zaštita i zaštita od okoline
6) Upravljanje komunikacijama i operacijama
7) Kontrola pristupa
8) Obogaćivanje, razvoj i održavanje informacijskog sustava
9) Upravljanje incidentima informacijskog sustava
10) Upravljanje poslovnim kontinuitetom
11) Usklađivanje, [1].

Svaka glavna sigurnosna kategorija sadrži:

- kontrolni cilj koji je potrebno ostvariti,
- jednu ili više kontrola koje se mogu primijeniti kako bi se ostvario kontrolni cilj.

Sigurnosnom politikom se naglašava važnost postojanja dokumenta sigurnosne politike. Sigurnosna politika može biti dio opće politike organizacije, a ne mora nužno predstavljati poseban dokument. Cilj sigurnosne politike je dati smjernice za upravljanje informacijskom sigurnošću u skladu s poslovnim zahtjevima organizacije i relevantnim zakonima i propisima. Uprava treba definirati jasnu sigurnosnu politiku koja je usklađena s ciljevima organizacije i koja pruža potporu informacijskoj sigurnosti na svim razinama organizacije.

Dokument sigurnosne politike treba sadržavati definicije informacijske sigurnosti, njezine glavne ciljeve i opseg te važnost sigurnosti kao mehanizma koji omogućuje dijeljenje informacija, izjavu o namjerama uprave koje ce podupirati ciljeve informacijske sigurnosti u skladu s poslovnom strategijom, okvir za uvodenje kontrola, kao i strukturu procjene rizika i upravljanja rizikom, objašnjenje sigurnosne politike, principe, standarde i zahtjeve od posebnog interesa koje organizacija treba usvojiti, a to su: zakonski, pravni i ugovorni

zahtjevi, edukacija o sigurnosti, svijest o sigurnosti i sigurnosni trening, upravljanje kontinuitetom poslovanja i posljedice narušavanja sigurnosne politike, definiciju odgovornosti u procesu upravljanja sigurnošću, uključujući i prijavu sigurnosnih incidenata, referencu na dokumente koji podupiru sigurnosnu politiku, [1].

Organiziranje informacijske sigurnosti kao domena sadrži dva kontrolna cilja, a to su unutarnja organizacija i vanjski suradnici. Kontrolni cilj koji se odnosi na unutarnju organizaciju opisuje upravljanje sigurnošću unutar organizacije. Od uprave se očekuje da odobri sigurnosnu politiku, dodijeli sigurnosne uloge i koordinira implementaciju sigurnosnih mehanizama unutar organizacije. Organizacija treba zatražiti nezavisno ispitivanje sustava upravljanja sigurnošću informacija.

Za sve zaposlenike organizacije potrebno je utemeljiti odgovarajuće odgovornosti, te inicirati potpisivanje sporazuma o povjerljivosti kako bi se zaštitile kritične informacije. Kod suradnje s vanjskim strankama zahtjeva se identifikacija rizika kojeg donosi takva suradnja i usvajanje prakse i procedura za smanjenje vjerojatnosti pojave sigurnosnih incidenata. Nadalje, potrebno je zaštititi sve resurse kojima pristupaju korisnici neke od usluga organizacije. Potrebno je definirati jasne sporazume prilikom suradnje s trećom stranom, [1].

Upravljanje resursima predstavljaju ključne zahtjeve ove sigurnosne domene a to su:

- dodjela odgovornosti za resurse,
- ispravna klasifikacija informacija.

Nakon što se napravi inventura resursa zahtjeva se dodjela vlasništva nad pojedinim resursom. Vlasnik resursa postaje odgovoran za razvoj, održavanje i uporabu resursa na prikladan način. Vlasništvo se može dodijeliti nad procesom, skupom aktivnosti, aplikacijom ili skupom podataka. Za svaki resurs je dobro definirati prikladan način uporabe. Svi zaposlenici, vanjski suradnici i treće strane trebaju poštivati određeni način uporabe resursa.

Kako bi se informacija mogla zaštititi na odgovarajući način, potrebno je provesti odgovarajuću klasifikaciju informacija. Informacije se trebaju klasificirati na temelju njihove vrijednosti, zakonskih i ugovornih zahtjeva, osjetljivosti i kritičnosti za organizaciju ili neki proces. Nakon što su klasificirane informacije se trebaju označiti u skladu s klasifikacijom. Također, dobro je izraditi procedure koje definiraju način na koji će se pojedina skupina informacija pohranjivati, prenositi, koristiti i uništavati, [1].

Sigurnost i ljudski resursi pokazuju da je potrebno je utemeljiti sigurnosne zahtjeve za periode prije zaposlenja, tijekom zaposlenja i nakon zaposlenja.

Uloge i odgovornosti zaposlenika je potrebno definirati i dokumentirati u skladu sa sigurnosnom politikom. Prije primanja zaposlenika potrebno im je predstaviti uloge i odgovornosti koje podrazumijeva njihovo radno mjesto. Tijekom zaposlenja dobro je zaposlenicima pružiti edukaciju u pogledu informacijske sigurnosti i to u cilju podizanja razine svijesti o informacijskoj sigurnosti. Organizacija treba utemeljiti disciplinski proces za sankcioniranje svih sigurnosnih prekršaja, te sve zaposlenike informirati o postojanju istog. Nakon promjene radnog mjesta, odnosno premještaja unutar organizacije, ili otpusta s radnog mjesta potrebno je osigurati da zaposlenik vrati sve resurse koje je posjedovao tijekom zaposlenja. Pristupna prava se trebaju uskladiti s novim radnim mjestom ili ukinuti ukoliko se radi o prekidu zaposlenja, [1].

Fizička sigurost kao domena u kojoj se uvodi pojam sigurnosnog opsega. Zadaća sigurnosnog opsega je fizički osigurati prostor s osjetljivim resursima. Sigurnosni opseg se postiže različitim barijerama, poput zidova, rešetki ili ulaznih vrata koja se kontroliraju pametnim karticama. Organizacija bi se trebala pobrinuti da samo ovlašteni korisnici imaju pristup sigurnosnom opsegu. Potrebno je voditi računa i o zaštiti od prirodnih prijetnji, npr. požara, poplave ili potresa. Oprema treba biti smještena u prostoru zaštićenom od krađe, prašine, kemijskih efekata, vandalizma, elektromagnetske radijacije i sl. Pomoćna oprema poput grijanja, ventilacije, klimatizacije, vodovoda i sl. treba odgovarati sustavu za koji je predviđena. Svi kablovi trebaju biti zaštićeni od oštećenja. Opremu je potrebno servisirati i održavati u planiranim intervalima kako bi se smanjio rizik od kvarova. Prije premještanja opreme iz organizacijskih prostorija, zahtjeva se autorizacija, [1].

Upravljanje komunikacijama i operacijama predstavljaju operativne procedure i odgovornosti kod upravljanja komunikacijama i operacijama su vrlo bitne. Ovdje se opisuje važnost i način dokumentiranja operativnih procedura. Sve dokumentirane procedure trebaju biti dostupne korisnicima koji ih trebaju. Sve promjene u informacijskom sustavu trebaju biti identificirane kako bi se njima moglo sustavno upravljati. Kod upravljanja uslugama treće strane cilj je implementirati i održavati sigurnosne mjere kako bi se osigurala sigurnost usluga koje pruža treća strana. Zatim u planiranju i prihvaćanju sustava cilj je minimizirati rizik od pogrešaka u sustavu. Planiranje i pripremanje je potrebno kako bi se osigurala raspoloživost sustava i zadovoljavanje odgovarajućih performansi sustava. U slučaju potrebe

za novim sustavima, utemeljuju se sigurnosni i operativni zahtjevi. Izvode se projekcije zahtjeva za kapacitetom.

Zaštita od malicioznog i mobilnog koda kao mjere opreza su nužne kako bi se zaštitio integritet programske opreme i informacija. Programska oprema i informacije su osjetljivi na umetanje zloćudnog koda poput virusa, crvi, trojanskih konja i sl. Korisnici sustava trebaju biti svjesni opasnosti od zloćudnog koda. Nužno je implementirati kontrole za obranu od malicioznog koda, kao i od mobilnog koda.

Potrebno je imati sigurnosne kopije kako bi se zaštitio integritet i raspoloživost informacija potrebno je redovito izrađivati sigurnosne kopije. Isto tako potrebno je upravljati mrežnom sigurnošću kojoj je cilj osigurati zaštitu informacija u mrežama, kao i pripadne mrežne infrastrukture. Mreže se često protežu izvan granica organizacije. Stoga je potrebno razmotriti tok podataka, legalne implikacije, nadzor i zaštitu mreža. Mora se voditi računa o rukovanju medijima i razmjeni informacija kako bi se zaštitila tajnost informacija i spriječile neautorizirane modifikacije te da bi se omogućila sigurna razmjena informacija unutar programa unutar organizacije ili s nekim vanjskim entitetom.

Informacije uključene u elektroničku trgovinu koje prolaze javnim mrežama trebaju biti zaštićene od neovlaštenih aktivnosti, osporavanja ugovora i neovlaštenog razotkrivanja ili modificiranja prilikom E-kupovine preko E-trgovina. I na kraju je važno nadziranje i bilježenje događaja koji su vezani za sigurnost. Datoteke sa zapisima o korištenju sustava i greškama sustava se upotrebljavaju kako bi se identificirali problemi informacijskog sustava.

Kontrola pristupa sadrži mnogo poddomena kao što su poslovni zahtjevi kontrole pristupa, upravljanje pristupom korisnika, obaveze korisnika, kontrola pristupa mreži, kontrola pristupa informacijskim sustavima, aplikacijska i informacijska kontrola pristupa i mobilno ručunarstvo i udaljeni rad.

Poslovni zahtjevi kontrole pristupa omogućuju pristup informacijama, kao i svim ostalim resursima, te poslovnim procesima se treba kontrolirati u skladu s poslovnim i sigurnosnim zahtjevima. Pravila kontrole pristupa trebaju uzeti u obzir politike autorizacije i pružanja informacija.

Upravljanjem pristupom korisnika potrebno je omogućiti autorizirani pristup informacijskim sustavima i spriječiti neautorizirani pristup. Da bi se to omogućilo dobro je osigurati formalne procedure za kontrolu prava pristupa informacijskim sustavima i uslugama. Procedure trebaju obrađivati cijeli ciklus pristupa korisnika, počevši od inicijalne registracije novog korisnika da ukidanja prava pristupa.

Obveze korisnika se prikazuju kao suradnja autoriziranih korisnika je ključna za učinkovito ostvarenje sigurnosti. Potrebno je utemeljiti politiku za čuvanje informacija na radnom mjestu kako bi se spriječio neautoriziran pristup informacijama i informacijskim sredstvima.

Kontrola pristupa mreži ima za cilj spriječiti neovlašten pristup mrežnim uslugama. Potrebno je kontrolirati pristup, kako unutarnjim, tako i vanjskim mrežnim uslugama. Pristup korisnika mreži i mrežnim uslugama. Kontrola pristupa operacijskim sustavima su sigurnosne kontrole trebaju ograničiti pristup neautoriziranim korisnicima. Aplikacijska i informacijska kontrola pristupa ima za cilj spriječiti neautoriziran pristup informacijama koje se nalaze u aplikacijskim sustavima. Mobilno računarstvo i udaljeni rad ima za cilj pružiti sigurnost kod uporabe mobilnih naprava i kod rada na daljinu. Zaštita treba odgovarati rizicima koje ovakav način rada uzrokuje, [1].

Nabava, razvoj i održavanje informacijskog sustava je važna kategorija ili domena sigurnosnih provjera. Sigurnosni zahtjevi informacijskih sustava pokazuju da sigurnost treba biti integralni dio informacijskih sustava. Informacijski sustavi uključuju operacijske sustave, infrastrukture, poslovne aplikacije, gotove proizvode i usluge i aplikacije razvijene unutar organizacije. Sigurnosni zahtjevi trebaju biti definirani prije razvoja i implementacije informacijskog sustava.

Ispravnom obradom informacija u aplikacijama nastoji se spriječiti greške, gubitak ili neovlaštena modifikacija informacija u aplikacijama. U aplikacije je potrebno ugraditi kontrole kako bi se osigurala ispravna obrada informacija. Kontrole trebaju validirati unesene podatke, te kontrolirati internu obradu i izlazne podatke. Kriptografske kontrole pokazuju da je potrebno razviti i implementirati kriptografske kontrole za zaštitu informacija. Upravljanje kriptografskim ključevima osigurava ispravnu uporabu kriptografskih tehnika.

Sigurnost sustavskih datoteka govori kako pristup sustavskim datotekama i izvornom tekstu programa treba biti kontroliran, a IT projekti i uz njih vezane aktivnosti trebaju biti izvedeni na siguran način. Sigurnost i razvoj programske opreme ima cilj održati sigurnost aplikacijskih programa i pripadnih informacija. Potrebno je kontrolirati razvoj programske opreme kao i pripadno razvijeno okruženje. Upravljanjem tehničkim ranjivostima potrebno je smanjiti rizik od eksploatacije objavljenih tehničkih ranjivosti. Upravljanje tehničkim ranjivostima treba biti obavljano sustavno i efikasno, [1].

Upravljanjem incidentima informacijskog sustava potrebno je osigurati da se sigurnosne slabosti i incidenti povezane s informacijskim sustavima priopće pravovremeno kako bi se na vrijeme poduzele odgovarajuće mjere. Potrebno je utemeljiti formalne procedure za prijavljivanje incidenata. Svi zaposlenici, suradnici i ostali korisnici trebaju poznavati procedure za prijavljivanje različitih tipova incidenata koji mogu imati utjecaja na sigurnost resursa organizacije. Svi zaposlenici, suradnici i treće strane trebaju prijaviti sve sigurnosne slabosti u sustavima i uslugama koje zapaze ili na koje sumnjaju.

Potrebno je utemeljiti obveze i procedure za rješavanje sigurnosnih incidenata nakon što su prijavljeni. Kao rezultat nadzora, evaluacije i upravljanja sigurnosnim incidentima dolazi do kontinuiranog poboljšavanja informacijskog sustava, [1].

Upravljanje poslovnim kontinuitetom moramo postići da ne dolazi do prekida u upravljanju. Prekidi u odvijanju poslovnih procesa, odnosno poslovanju organizaciji uzrokuju direktno mjerljive financijske gubitke. Osim tih, mjerljivih gubitaka, prekidi u poslovanju, mogu uzrokovati i druge štete kao što su gubitak kredibiliteta kod klijenata, pozicije na tržištu, ugleda organizacije koji nisu direktno mjerljivi, ali mogu imati vrlo ozbiljne posljedice na poslovanje.

Potrebno je razviti i implementirati plan poslovnog kontinuiteta kako bi se osigurao kontinuitet poslovnih operacija. Upravljanje poslovnim kontinuitetom treba uključivati kontrole za identifikaciju i smanjivanje rizika, kao dodatak općenitim procesima procjene rizika, te osigurati da su informacije potrebne za poslovne procese lako dostupne, [1].

Usklađivanjem svi važeći zakonski i ugovorni zahtjevi trebaju biti definirani, dokumentirani i ažurirani, kao i način na koji organizacija zadovoljava te zahtjeve. Potrebno je implementirati procedure za usklađivanje sa zakonskim i ugovornim uvjetima korištenja različitih materijala poštivajući prava intelektualnog vlasništva. Važne zapise je potrebno čuvati od gubitka, uništenja, krivotvorenja u skladu sa zakonskim, ugovornim i poslovnim zahtjevima.

Zaštita podataka i privatnosti treba biti osigurana u skladu s relevantnim zakonima, propisima i eventualnim uvjetima ugovora. Potrebno je osigurati da su sve sigurnosne procedure implementirane korektno, kako bi se postigla njihova usklađenost sa sigurnosnim politikama i standardima. Informacijske sustave je potrebno redovito provjeravati kako bi se utvrdila usklađenost sa sigurnosnim implementacijskim standardima, [1].

4. Ocjena rizičnosti poduzeća

U procjeni rizičnosti poduzeća proći će se kroz sve elemente informacijsko komunikacijskog sustava. Sustav koji će se analizirati kroz sve elemente je realni sustav koji će se u daljnjem tekstu nazivati „poslovni korisnik“.

Elementi informacijskog sustava su:

- Hardver
- Softver
- Orgware
- Lifeware
- Netware
- Dataware, [5].

U informacijskom sustavu hardver predstavlja fizičku komponentu sustava, opreme i ostale elemente koji čine materijalnu osnovicu sustava. Isto tako hardver poslovnih upravljačkih informacijskih sustava može se kategorizirati u tri funkcionalne skupine uređaja, a to su:

- skupina središnjih jedinica
- skupina perifernih jedinica
- skupina komunikacijskih jedinica.

Poslovni korisnik sastoji se od povećeg broja hardverske opreme, jer u suštini ta tvrtka se bavi sa prodajom i servisiranjem računala, mobitele i drugih elektroničkih uređaja. Sam prostor tvrtke podijeljen je u tri dijela. Prvi dio je trgovina koja sadržava elektroničke uređaje koji su za prodaju i izloženi na policama. Unutar prostora postoji određeni broj kamera koje su spojene sa računalom i koje bilježe svakodnevna događanja unutar prostora. Nadalje drugi dio prostora je backoffice. Taj prostor sadrži brojna računala i kamere koja su međusobno povezana i spojena na zajedničku bazu podataka. Nadalje treći prostor je prostor servisa u kojem se obavlja podizanje elektroničke opreme sa servisa, taj prostor se također sastoji od određenog dijela računalne opreme i servera. Isto tako moramo uzeti u obzir da hardverska oprema nisu samo računala koja se nalaze unutar tvrtke nego i sama zgrada, zidovi, skladište opreme itd., od kojih zapravo i počinje fizička zaštita informacijskog sustava.

Nadalje drugi element informacijskog sustava je softver, koji je zapravo nematerijalni dio informacijskog sustava, odnosno može se reći da je to skup programa koje upravljaju računalom ili se izvode na računalu. Softver se može podijeliti na operativni sustav i aplikacije. Operativni sustav koji koristi poslovni korisnik je Windows 7. Cijeli računalni sustav tvrtke koristi program „Luceed“. Program „Luceed“ obuhvaća i objedinjuje sve funkcije poslovanja koje su potrebne tvrtki. Neke od karakteristika „Luceed-a“ su:

- neograničen unos podataka, po principu „jedan unos za sve pozicije“,
- povezanost i praćenje dislociranih poslovnih jedinica (online ili sinkronizacijom podataka),
- kreiranje velikog broja izvješća i analiza uz samostalno definiranje izgleda i sadržaja istih,
- mogućnost kreiranja različitih cijena po poslovnim jedinicama (centralno i u poslovnici),
- kvalitetan izvještajni sustav (stanju zalihe, analize prodaje, potraživanja),
- omogućeno praćenje članova kroz „Loyalty“ program, [6].

Svaki od računala koje koriste radnici tvrtke sadrži antivirusnu zaštitu te je detaljno testiran prije puštanja u rad.

Orgware je organizacijski dio sustava. Sastoji se od postupaka, metoda i procedura, te načina povezivanja ostalih komponenti sustava. Poslovni korisnik je jedan veliki sustav koja osim centralne tvrtke u Zagrebu sadrži i podružnice po ostatku Hrvatske. Uzevši to u obzir može se definirati da je poslovni korisnik (centralna tvrtka) sustav koji sadrži svoje podsustave po drugim dijelovima države, a ti podsustavi imaju definiranu strukturu unutar sebe. Da bi jedan takav sustav funkcionirao potrebno je dobro definirati procese, te dobro napraviti zaštitu sustava tj., strogo definirati dozvole i mogućnosti unutar podsustava te samog centralnog sustava. Treba jasno definirati koji podsustav ima koje ovlasti i koje odluke donose sami, a za koje se moraju savjetovati sa centralnim sustavom.

Lifeware je oznaka za ljudski faktor u sustavu, što je ujedno i jedan od najbitnijih dijelova sustava jer bez ljudi ne bi većina sustava ni radila. Kod lifeware-a, mogu se identificirati operatori u IS-u, serviseri, osobe koje trebaju informaciju, projektanti IS-a, ostali uposlenici i slučajni korisnici. U primjeru koji se objašnjava također postoje različite sektori u kojim rade ljudi. Neki od njih su prodavači, serviseri, menadžeri, računovođe, direktor, čistačica. Isto

tako mora se uzeti u obzir da sudionici lifeware-a nisu samo osobe koje rade u tom sustavu nego i svi posjetioci, odnosno kupci koji dolaze s namjerom nešto kupiti, osobe koje dođu samo razgledavati po trgovini odnosno slučajni prolaznici, isto tako u sudionike lifeware-a ulaze i osobe koje donose uređaje na servis. Jedan od najvećih problema sigurnosti dakako predstavljaju ljudi koji dolaze u druge tvrtke u toj zgradi i za koje se ne obavlja autorizacija pri ulasku te imaju nesmetani prolaz kroz cijelu zgradu. Kada se govori o sigurnosti ljudskog faktora, može se reći da je za više od 80% grešaka koje se dogode u sustavu kriv čovjek. Prema tome može se podijeliti s obzirom na namjernost ljudi na ljude s atribucijom namjernosti i ljude s atribucijom nenamjernosti. U ljude s atribucijom namjernosti može se svrstati određenu konkurenciju tvrtke koja je došla i želi vidjeti ili pokušati omesti sam rad tvrtke. Nadalje u tu skupinu spadaju i hakeri koji žele nauditi sustavu tvrtke, osobe koje žele ukrasti neki proizvod iz dućana itd. Za skupinu s atribucijom nenamjernosti može se reći da su u više od 50% slučajeva krive i odgovorne same tvrtke koje omogućavaju zaposlenicima pretjerana prava korištenja odnosno omogućavaju da pojedini zaposlenici imaju pristup stvarima koje uopće ne spadaju u njihovu domenu odnosno opis posla. Isto tako mora se uzeti u obzir da dosta tvrtki uopće ne educira svoje zaposlenike.

Netware u sustavu predstavlja komunikacijsko povezivanje elemenata i dijelova sustava u cjelinu, tj. može se reći da predstavlja hardversko-softversku komponentu koja omogućava komuniciranje unutar mreže. U poslovnom korisniku pod netware spadaju svi usmjerivači unutar tvrtke, serveri i sva druga mrežna oprema koja omogućava rad sustava, tj. omogućava zaposlenicima korištenje softvera. Sigurnost netware elemenata je dosta teško omogućiti zbog mogući grešaka u prijenosu, prisluškivanja, ometanja signala, preusmjeravanje prometa itd. Neki od načina zaštite su kriptografija, elektromagnetska zračenja, zabrana pristupa.

Dataware je komponenta sustava vezana za organizaciju baze podataka i informacijskih resursa. Sigurnost dataware-a se može ugroziti neunošenjem potpunih podataka, unošenjem netočnih podataka, korištenjem administratorskih ovlasti, ukoliko neka osoba ima pretjerane ovlasti itd. Poslovni korisnik temelji svoju bazu podataka na programu „Luceed“ odnosno baza podataka se nalazi na serveru poduzeća Tomsoft d.o.o., unutar svake poslovnice (jedna ili više lokacija). Svaka od navedenih opcija kreira se na definirane lokacije:

- kao zaštitne kopije baze podataka (postoji vremenski raskorak)
- postupkom replikacije (u realnom vremenu)

Dodatnu sigurnost pruža opcija razmjene podataka. Prilikom razmjene podataka, program razmjenjuje sve promjene evidentirane u bazi i kreira identične baze podataka na ostalim lokacijama. Sukladno tome, baze u različitim poslovnim jedinicama osiguravaju dodatnu sigurnost u slučaju kvara na serverima jedne od poslovnica. Takve baze mogu poslužiti kao backup.

4.1. Prijetnje

Prijetnje u informacijskom sustavu poslovnog korisnika mogu biti, ako je čovjek taj koji ih može učiniti, slučajne, namjerne ili prirodne pojave. Namjerne prijetnje su:

- prisluškivanje,
- modifikacija informacija,
- hakiranje,
- maliciozni kod,
- krađa,[7].

Nadalje slučajne su:

- pogreške i propusti,
- nenamjerno brisanje podataka i sl.,
- pogrešno preusmjeravanje,
- nenamjerno fizičko oštećenje, [7].

Prirodne pojave su:

- potres,
- udar groma,
- poplava,
- požar, [7].

Prijetnja se može pojaviti unutar poslovnog korisnika ili izvan nje. Primjer jedne prijetnje unutar tvrtke je sabotaža jednog od zaposlenika koji nije zadovoljan sa plaćom ili neki drugi oblik zadovoljstva, te ukrade neki elektronički uređaj iz tvrtke, ukoliko ima pristup administraciji ili bazi podataka izmjeni neke podatke koji su bitni tvrtki za daljnje poslovanje te izbriše korake protoka robe kako bi prikrio krađu koja se zbog toga može otkriti tek nakon

godišnje usklade. Primjer vanjske prijetnje može biti neki zlonamjerni „haker“ ili špijunaža neke druge tvrtke kako bi došla do podataka poslovnog korisnika, te ih mogla iskoristiti u svoju korist. Isto tako mora se uzeti u obzir da postoji i nenamjerna prijetnja osoba unutar tvrtke na taj način da osobe napuste svoje radno mjesto te odu npr. zapaliti cigaretu u prostor koji se ne nalazi u prostru tvrtke te na taj način omogućavaju lopovu da uđe u prostorije i ukrade ili oštetiti imovinu tvrtke. Nadalje jedan veliki problem poslovnog korisnika je južni ulaz zgrade gdje ne postoji kontrola prilikom ulaska, jer na taj ulaz ulaze i ostali radnici drugih tvrtki u toj zgradi. Isto tako prijetnja tvrtki ne dolazi samo od ljudskog faktora nego i od prirodnih pojava koje mogu nanijeti veliku štetu.

4.2. Ranjivost

Ranjivost je slabost koju je moguće slučajno aktivirati ili namjerno iskoristiti, a posljedica toga može biti nanošenje štete informacijskom sustavu i poslovnim ciljevima. Ranjivosti koje se povezuju s resursima uključuju, između ostalog, slabosti fizičke sigurnosti, organizacije, internih akata, zaposlenika, upravljačke strukture, hardvera, softvera i informacija, [7].

Ranjivost se može podijeliti na pet dijelova. Jedna od ranjivosti je ranjivost okoliša i infrastrukture, za primjer se može uzeti taj što tvrtka nema zaštitara ili osobu koja može spriječiti lopova da ukrade iz dućana, nedostatak autorizacije, odnosno otvaranje vrata na način da se prisloni identifikacijska kartica na uređaj koji otvara vrata. Autorizacija se odnosi za vrata koja su samo za zaposlenike tvrtke. Isto tako jedna od ranjivosti je i loša i stara instalacija električnih i ostalih instalacija, koje sa svojim kvarom mogu naštetiti tvrtki. Sljedeća ranjivost je ona hardverska, kod koje dolazi ukoliko se prostorija gdje se nalaze serveri ne hladi te dolazi do pregrijavanja i prekida rada, ali isto tako ova ranjivost dosta ovisi i o ranjivosti infrastrukture jer ukoliko često dolazi do gubitka električne energije onemogućava se rad servera ali i ostatka hardverske opreme. Do softverske ranjivosti može doći ako se u računala koje koriste radnici ubaci neki novo sučelje s kojim se osoblje još do tada nije srelo, a nije prošlo neku edukaciju može slučajnom pogreškom unijeti pogrešne podatke o nekoj osobi ili doći do krive naplate odnosno ne naplate računa itd. Što se tiče komunikacijske ranjivosti ona se ne mora samo temeljiti na prisluškivanju linija nego isto tako osobe koje rade u tvrtki mogu odnijeti laptop koji koriste u tvrtki sa sobom na kavu te

se spojiti putem bežične konekcije na Internet, te mu se netko sa različitim programima može ubaciti u laptop te na taj način skinuti podatke koji su mu potrebni.

Isto tako moguće je preko SQL (engl. *Structured Query Language*) injection tehnike koja iskorištava sigurnosnu ranjivost prilikom pristupa web aplikacije bazi podataka iskoristiti za zlonamjerno korištenje. Ranjivost nastaje kad web aplikacija prikazuje korisniku dinamički generirane web stranice za koje podatke dobiva SQL upitom, a kojeg formira ugrađujući u njega podatke koje unosi sam korisnik. Javlja se zato što aplikacija ne filtrira znakove posebne namjene od kojih se kreira SQL upit ako ih (zlonamjerni) korisnik upiše u polje za pretragu. Ukoliko napadač uspije po volji izmijeniti SQL upit, kojeg će aplikacija proslijediti internoj, skrivenoj bazi podataka, aplikacija će u ime (zlonamjernog) korisnika pretraživati cjelokupan sadržaj baze, uključujući i one podatke koji nisu namijenjeni vanjskim korisnicima. Posljedica napada je preuzimanje kontrole nad bazom podataka i izvršavanje naredbi nad ranjivim sustavom. Neki od nizova znakova koje napadač može unijeti su: • ' OR "=' • ' OR 1=1— • 1 AND 1=1 • 1'1. Na primjer, ukoliko se od korisnika traži unos korisničkog imena i zaporke na web stranici, napadač može upisati jedan od prethodno spomenutih nizova znakova. Rezultat konstruirane SQL izjave je uvijek istinit i napadač će se uspjeti prijaviti na sustav kao prvi korisnik u korisničkoj tablici. Primjer izbjegavanja upisivanja korisničkog imena i lozinke pomoću SQL naredbi: Korisničko ime: ' OR "=' Lozinka: ' OR "=' Na ovaj način će se umjesto uspoređivanja korisnički unesenih podataka s podacima o korisnicima, uspoređivati " (prazan niz) s " (prazan niz). Stoga će rezultat ove SQL izjave uvijek biti istinit i napadač će se uspjet ulogirat u sustav kao legitiman korisnik, [8].

4.3. Rizik

Utvrđivanje rizika izloženosti određenoj kombinaciji prijetnje i ranjivosti može se izraziti kao funkcija:

- vjerojatnosti da će identificirani izvor prijetnje iskoristiti određenu ranjivost,
- jačine (razine) učinka ako izvor prijetnji uspješno iskoristi ranjivost, [7].

Jedan od načina smanjenja rizika je izrada matrice i ljestvice rizika.

U matrici, razina rizika utvrđuje se množenjem ocjene koja je dodijeljena vjerojatnosti da izvor prijetnje iskoristi ranjivost s ocjenom učinka neželjenog događaj, pri čemu se uzima u obzir prikladnost planiranih ili postojećih kontrola, [7].

Tablica 1. Matrica razine rizika, [7]

Vjerojatnost da izvor prijetnje iskoristi ranjivost	Učinak		
	Mali (10)	Srednji (50)	Veliki (100)
Velika (1,0)	10 x 1,0 = 10	50 x 1,0 = 50	100 x 1,0 = 100
Srednja (0,5)	10 x 0,5 = 5	50 x 0,5 = 25	100 x 0,5 = 50
Mala (0,1)	10 x 0,1 = 1	50 x 0,1 = 5	100 x 01, = 10

Tablica 1 prikazuje primjer kako se mogu odrediti rizici na temelju podataka o vjerojatnosti da izvor prijetnje iskoristi ranjivost i o učinku. U tablici 1 prikazan je primjer kako se računa ukupna razina rizika. Ocjena vjerojatnosti da izvor prijetnje iskoristi ranjivost koja se prepisuje svakoj razini vjerojatnosti prijetnje je 1,0 za veliku, 0,5 za srednju i 0,1 za malu. Ocjena učinka koja se dodjeljuje svakoj razini jačine učinka je 100 za veliku, 50 za srednju i 10 za malu, [7].

Tablica 2. Ljestvica rizika i aktivnosti koje je potrebno poduzeti, [7]

Razina rizika	**Opis rizika i aktivnosti koje je potrebno poduzeti**
Veliki rizik (veći od 51)	Ako je rizik procijenjen kao veliki, nužno je hitno provođenje mjera za smanjenje rizika. Postojeći sustav može nastaviti raditi, ali nužno je u što kraćem roku sastaviti plan provođenja mjera te odrediti prioritete i rokove.
Srednji rizik (11 do 50)	Ako je rizik procijenjen kao srednji, nužno je provođenje mjera za smanjenje rizika. Potrebno je sastaviti plan provođenja mjera kako bi se one provele u razumnom vremenu.
Malen rizik (1 do 10)	Ako je rizik procijenjen kao malen, potrebno je utvrditi je li nužno provođenje mjera za smanjenje rizika ili se rizik može prihvatiti.

Tablica 2 opisuje razine koje su prikazane u tablici 1. Ljestvica rizika s pripadajućim ocjenama predstavlja stupanj rizika kojima su izloženi resursi informacijskog sustava ako je iskorištena određena ranjivost. Stupanj rizika određuje aktivnosti koje bi se trebale poduzeti.

Svaki informacijski sustav susreće se svakodnevno sa rizicima pa tako i poslovni korisnik.. Određene rizike moguće je izbjeći, kao što je nestanak struje na način da se napravi pomoćni generator koji će omogućiti nastavak rada i dok struje nema, za razliku od nekih kojima se moramo prilagoditi jer je nemoguće predvidjeti u kojem trenutku će se dogoditi potres ili neka druga prirodna pojava koja može ugroziti tvrtku.

4.4. Prijedlog poboljšanja

Da bi se mogao napraviti prijedlog poboljšanja, potrebno je znati da prijetnje sustavu mogu biti ljudi, stvari i događaji iz sutava ili okoline. Nekada djelovanje prijetnji može biti predvidljivo te za takve prijetnje je moguće unaprijed postaviti zaštitu. Sama zaštita informacijskog sustava kao što je već objašnjeno prije, obuhvaća sve logičke i fizičke mjere potrebne za osiguranje integriteta sustava, ali isto tako i dostupnost sustavu jedino ovlaštenim osobama.

Poboljšanje sustava poslovnog korisnika kreće od okoline odnosno od samog fizičkog okuženja. Za početak potrebno je provjeriti sve kamere koje snimaju područje oko poslovnog korisnika i ako je potrebno dodati još koju da se pokrije čitav prostor oko poslovnog

korisnika. Nadalje, ulazna vrata i vrata sa južne strane zgrade potrebno je nakon isteka radnog vremena zatvoriti i sa nekim oblikom rešetkastih vrata koja će biti još jedna dodatna zaštita, uz trenutnu. U podrumu zgrade zbog mogućnosti poplave koja se znala događati potrebno je napraviti redizajn prostora (elektroničke uređaje koje dolaze dostavom stavljati na povišene police) te u slučaju poplave neće biti u kontaktu sa vodom. Za vrijeme trajanja radnog vremena poslovnog korisnika potrebno je staviti jednog zaštitara na ulaz koji će onemogućiti bijeg u slučaju krađe. Kod ulaska na južni ulaz potrebno je omogućiti korisnicima (osobama koje dolaze popravit elektronički uređaj) kretanje na taj način da im se omogući pristup samo do pulta i predvorja. Ostala vrata u koja se može ulaziti iz predvorja ograničiti na ovlaštene osobe na način da se pri ulasku mora osoba identificirati karticom te nakon potvrde identifikacije vrata mu se otvaraju. Korisnicima ne dopuštati prolazak do WC-a jer ako imaju pristup do WC-a imaju u pravilu pristup i otići na bilo koji kat poslovnog korisnika.

Isto tako veliki problem kod zaštite sustava je i ljudski faktor. Osoba svoje radno mjesto ne bi trebala napuštati ukoliko je neće zamjeniti druga osoba (kolega). Ukoliko je to nužno potrebno je napraviti logout iz sustava te neomogućiti korisnicima neovlašteno kretanje. Također treba zabraniti pristup osobama koje ne rade u određenom odjelu, bilo da se radi o korisnicima ili zaposlenicima ukoliko nemaju ovlaštenje. Dnevni promet potrebno je stavljati u sef kojem imaju pristup samo ovlaštene osobe.

Što se tiče trgovine gdje je izložena elektronička oprema, svu opremu potrebno je spojiti na alarmne sustave i po mogućnosti ne gasiti alarme jer na taj način se omogućava lopovu da bez problema ukrade uređaj i izađe iz trgovine. Održavanje pulteva i gašenje alarma omogućiti isključivo van radnog vreemena ili uz nadzor zaštitara. Nadalje potrebno je ukoliko nastane velika koncentracija ljudi u trgovini pozvati osobu iz drugog odjela da. nadgleda trgovinu dok se gužva ne raščisti. Na kraju svakog radnog vremena potrebno je provjeriti sve ulaze u zgradu poslovnog korisnika i uključiti alarme.

Što se tiče računala i pristupu računalima unutar poslovnog korisnika, potrebno je definirati da svaki zaposlenik ima samo pravo na one privilegije koje su u funkciji njegovog radnog zaduženja. Svaki zaposlenik koji koristi računalo mora dobiti korisničko ime i lozinku koja mu omogućava pristup računalu. Isto tako ta lozinka i korisničko ime ne smiju biti napisani na nekom vidljivom mjestu na kojem će ga moći pročitati bilo tko i ući na računalo. Po mogućnosti u roku od dva dana nakon dobivanja korisničkog imena i lozinke uništiti

papirić na kojem je bilo napisano. Isto tako pristup zaposlenicima se mora ograničiti i nad bazom podataka jer nema potrebe da osoba koja radi u servisu ima pristup godišnjim prihodima ili nekim drugim podacima koji nisu unutar njegove domene posla.

Nakon što su se postavila ograničenja na računala, potrebno je ograničiti i pristup internetskim stranicama što zbog sigurnosti tj. mogućnosti da se računalo zarazi virusom, ali i iz razloga da ne dođe do zagušenja mrže, te sustav neće dovoljno brzo raditi. Također potrebno je definirati i vatreni zid između Interneta i lokalne mreže poslovnog korisnika i na taj način sprječiti neovlašteni pristup podacima i sustavima komunikacijskim kanalima. Nakon što je prijenos podataka i komunikacije zaštićena potrebno je te iste podatke koji su potrebni za daljnji rad sustava pohraniti odnosno napraviti sigurnosnu kopiju koja se ne mora nalaziti u zgradi poslovnog korisnika nego može biti na drugoj lokaciji.

Veliki problem u zaštiti kao što je već navedeno i prije u tekstu odnosi se na ljude i mogućnost korištenja njihovih osobnih prijenosnih tvrdih diskova i usb-ova za prebacivanje određenih podataka sa računala od poslovnog korisnika. Da bi se to spriječilo potrebno je ili antivirusnim programom pretražiti prijenosi disk prije pokretanja ili prvo provjeriti prijenosni medij na nekom računalu koje nije spojeno na sustav poslovnog korisnika nego samo služi za razna testiranja.

Poslovni korisnik bi također trebao donijeti politiku sigurnosti i upoznati korisnike informacijskog sustava s njom, te imenovati osobu koja će biti nadležna za nadzor i kontrolu procesa upravljanja informacijskim sustavom, kako bi se prijedlozi mogli ostvariti i poboljšati zaštitu sustava. Također bitne stavke kod poslovnog korisnika su upravljanje rizikom i proces provođenja mjera za smanjivanje rizika koje je potrebno postaviti kao kontinuirani proces. Proces procjene rizika omogućio bi smanjenje rizika na prihvatiljivu razinu te bi olakšao samo održavanje. Operativni i sistemski zapisi moraju biti adekvatno zaštićeni od neovlaštenog pristupa, izmjena i brisanja. Isto tako poslovni korisnik bi trebao uspostaviti sustav koji će upravljati korisničkim pravima pristupa i na taj način definirati procese evidentiranja, identifikacije, autentifikacije i nadzora.

Poslovni korisnik bi trebao definirati način, kriterije, postupke i standarde razvoja informacijskih sustava, imajući u vidu funckionalne i sigurnosne aspekte.

5. Zaključak

Ubrzani razvoj informacijskih mreža u posljednjim godinama zahtjevao je od privatnih i državnih organizacija ugradnju učinkovitih mjera informacijske sigurnosti kako bi unaprijedile svoj kredibilitet i konkurentnost na tržištu. Današnji zahtjevi za informacijskom sigurnosti su bitno drugačiji od onih prije dvadeset i više godina. Opća umreženost te sve prisutnost informacijske i komunikacijske tehnologije u svim porama društva nameće potrebu jakih i jasnih zahtjeva na sigurnost. Informacijska sigurnost podrazumijeva očuvanje povjerljivosti, tj. tajnosti i privatnosti podataka, te integriteta i raspoloživosti informacijskih sustava. Povreda povjerljivosti, oštećenje podataka i prekidi u uslugama imaju svoju cijenu kako za poslovanje u javnom i privatnom sektoru, tako i za korisnike i društvo u cjelini.

Visoka ovisnost o informacijskoj tehnologiji (programi, mreže računala, baze podataka) za kritične infrastrukturne sustave jedne zemlje te visoki troškovi koji nastaju zbog napada na takve sustave, sve veća vrijednost informacija u poslovanju, zakonske i regulatorne obveze u RH te obveze od članstva u EU i NATO postavljaju hitne zahtjeve za uspostavu i mjerenje informacijske sigurnosti svake zemlje. Informacijski prostor je neupitno ugrožen. Ne samo u RH nego i šire. Stanje u RH je još i teže jer nije uspostavljena odgovarajuća tehnička i semantička infrastruktura, te su mnogi problemi za sada još i slabo vidljivi. Cijeli informacijski prostor je pod velikim rizikom povrede informacijske sigurnosti posebno zbog toga što se donose i primjenjuju kratkoročne mjere za uklanjanje sigurnosnih propusta, radije nego dugoročno planirane i koordinirane mjere.

Na temelju istraživanja raspisane su mjere zaštite kojima se štite resursi informacijskog sustava, smanjuje ranjivost informacijskog sustava, ograničava učinak neželjenih događaja, otkrivaju neželjeni događaji te pospješuje oporavak. Očekuje se podizanje razine znanja i svijesti zaposlenih vezanih za sigurnost i funkcionalnost informacijskog sustav, te na kraju osvješćivanje upravljačke strukture o svim rizicima i njihovom mogućem utjecaju te vjerojatnosti pojave negativnih događaju kako bi donijeli odluku o prihvaćanju rizika kojima je izložen informacijski sustav ili o prevenciji, odvraćanju te smanjenju ranjivosti sustava.

Popis literature

[1] Vukelić B.: Sigurnost informacijskih sustava (skripta sa predavanja), Fakultet prometnih znanosti Zagreb

[2] Hadjina N.: Zaštita i sigurnost informacijskih sustava (nastavni materijali sa zbirkom zadataka), Fakultet elektrotehnike i računalstva Zagreb, Zagreb,2009.

[3] Donn Parker: "Fighting Computer Crime", 2000.

[4] Internet stranica: http://mrbool.com, (05.07.2015.)

[5] Sigurnost i zaštita informacijsko komunikacijskih sustava, predavanja 2012.

[6] Internet stranica: http://www.tomsoft.hr/index.cgi?menu_id=556, (09.07.2015.)

[7] Smjernice za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika, Hrvatska narodna banka, ožujak 2006.

[8] Internet stranica: http://security.lss.hr/documents/LinkedDocuments/CCERT-PUBDOC-2008-05-228.pdf, (13.07.2015)

[9] Gledec G., Mikuc M., Kos M.: Sigurnost u privatnim komunikacijskim mrežama, Sveučilište u Zagrebu, Fakultet elektrotehnike i računalstva Zagreb, Zagreb, travanj 2008.

[10] Mark Rhodes-Ousley: „Information Security, The Cmplete Reference, Second Edition“, 2013.

[11] Theodore Parker: „Security Concepts“, 2009.

[12] Internet stranica: https://en.wikipedia.org/wiki/RADIUS (15.07.2015)

Popis ilustracija

Slika 1. Uskraćivanje usluge, [1] 5
Slika 2. Najčešći izvori i oblici prijetnji sigurnosti informacijskim sustavima, [1] 6
Slika 3. Prijetnje sigurnosti sustava, [1] 7
Slika 4. Potpuni model sigurnosnog sustava, [2] 10
Slika 5. Model sigurnosne arhitekture, [2] 11
Slika 6. Virus koji se dodaje na program, [2] 13
Slika 7. Virus okružuje program, [2] 13
Slika 8. Virus integriran u program, [2] 14
Slika 9. Virus potpuno zamjenjuje program, [2] 14
Slika 10. Boot sektor prije i poslije infekcije, [2] 15
Slika 11. Otisci prstiju, [2] 22
Slika 12. Skener otiska prsta, [2] 22
Slika 13. Skeniranje rožnice oka, [2] 23
Slika 14. Dvosmjerna PAP razmjena, [2] 24
Slika 15. Trosmjerna CHAP razmjena, [2] 24
Slika 16. Trosmjerna EAP razmjena, [2] 25
Slika 17. Radijus autetifikacijska sjednica u dial-in uvjetima, [2] 25
Slika 18. X-509 certifikacijska hijerarhija, [2] 26
Slika 19. PGP mreža povjerenja, [2] 27
Slika 20. Arhitektura DBMS-a, [4] 29
Slika 21. Razine opisa podataka, [2] 29
Slika 22. Grananje rizika, [2] 31
Slika 23. Proces smanjenja rizika, [2] 32
Slika 24. Graf procjene prihvatljivog rizika, [1] 33
Slika 25. PDCA model, [1] 35

Popis tablica

Tablica 1. Matrica razine rizika, [7].....48
Tablica 2. Ljestvica rizika i aktivnosti koje je potrebno poduzeti, [7] 49

Popis kratica

CHAP- Challenge Handshake Autentification Protocol

DBMS- Database Management System

DDL- Data Definition Language

DDoS- Distributed Denial of Service

DML- Data Manipulation Language

DoS- Denial of service

EAP- Extensible Authetification Protocol

IEC- International Electrotechnical Commission

ISMS- Information security management system

ISO- International Organization for Standardization

LCP- Link Control Protocol

OEDC- The Organisation for Economic Cooperation and Development

OTP- One-Time Password

PAP- Password Autentification Protocol

PDCA- Plan-Do-Check-Act

PPP- Point-to-Point Protocol

RADIUS- Remote Access Dial In user Service

SQL- Structured Query Language

Metapodaci

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000
Zagreb
Vukelićeva
4

METAPODACI

Naslov rada: Mjere procjene sigurnosti i zaštite poslovnog korisnika

Autor: Urankar Danijel

Mentor: prof. dr. sc. Dragan Peraković

Naslov na drugom jeziku (engleski):

Security evaluation measures and user protection

Povjerenstvo za obranu:

- prof. dr. sc. Slavko Šarić , predsjednik
- prof. dr. sc. Dragan Peraković ,mentor
- dipl. ing. Ivan Jovović , član
- prof. dr. sc. Zvonko Kavran , zamjena

Ustanova koja je dodjelila akademski stupanj: Fakultet prometnih znanosti Sveučilišta u Zagrebu

Zavod: Zavod za informacijsko komunikacijski promet

Vrsta studija: sveučilišni

Naziv studijskog programa: Promet

Stupanj: diplomski

Akademski naziv: mag. ing. traff.

Datum obrane završnog rada:

Izjava o akademskoj čestitosti i suglasnosti

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu diplomskog rada pod naslovom **Mjere procjene sigurnosti i zaštite poslovnog korisnika**

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

Student/ica:

U Zagrebu, _____ _____

(potpis)