Sveučilište u Zagrebu

Fakultet organizacije i informatike

Varaždin

Kostanjevec Alen

Mjere i kontrole za smanjenje rizika

Mentor:

mag. inf. Tonimir Kišasondi

Varaždin 2014.

SADRŽAJ:

1. Uvod

Rizik predstavlja prognozu štete u budućnosti koja će se pojaviti s nekim neželjenim događajem. Budući da se svaka šteta koja nastaje gleda iz vrlo negativnog aspekta jer dolazi do oštećenja imovine, prava, ljudi itd., u prirodi čovjeka je da napravi sve kako šeteta nebi nastala. Upravo iz tog razloga kad govorimo o poslovnim sustavima je važno upravljati s rizicima, pokušati prepoznati koji su to rizici i odrediti načine na koje ćemo smanjiti utjecaj rizika i neželjenih događaja na naše poslovanje.

Ako gledamo na rizik iz aspekta informacijske sgirunosti, onda govorimo o jako širokom području koje je podležno različitim rizicima a koji su u najvećoj mjeri vezani uz gubitak imovine, ugrožavanje cjelovitosti imovine, zlouporaba imovine, i ostale aktivnosti koje ugrožavaju imovinu poduzeća a koja je vezana uz određene podatke i informacije.

S razvojem računala i sve većom upotrebom računala u poslovnom svijetu i korištenje informacijskih sustava, kao i različitih mrežnih sustava, omogučio se ljudima koji imaju namjeru iskorištenja informacija, a posjeduju znanja da preko novih tehnologija pristupe takvim informacija, da vrlo lako mogu čitati, mijenjati, prodavati i izvršavati druge akcije nad podacima koje poduzeće smatra povjerljivim podacima. U početku se ovakvim napadima nije pridodavala velika važnost, ali s vremenom su se počeli uočavati veliki gubitci koji su bili posljedica ovakvih napada. Ako gledamo na poslovni sustav kao organizaciju ljudi i poslova koji se obavljaju s ciljem stjecanja novčane dobiti, ovakvi gubici su počeli dobivati na velikom značaju i krenulo se sa sustavnim razvijanjem mjera zaštite kako bi se umanjili takvi gubici, te kako bi se umanjila mogućnost da dođe do akcije koje će proizvesti gubitke. Danas postoji niz mjera i kontrola koje se preporučuju poslovnim sustavima kako bi smanjili rizike. U ovoj temi ćemo prikazati kontrole i mjere iz aneksa A ISO norme 27001 te preporuke za implementaciju tih normi u poslovni sustav. Kako ovaj rad ne bi bio šturo prepisivanje mjera i kontrola iz aneksa A ISO norme 27001 i prikaz najbolje prakse iz ISO norme 27002, za svaku mjeru i kontrolu koja je prikazana u aneksu A ISO norme 27001, biti će prikazan i praktičan primjer na koji način su određena poduzeća realizirala i uvelu tu mjeru s ciljem smanjenja rizika, te će za pojedine biti i prikazane negativne posljedice do kojih je došlo ne obraćanjem pažnje na moguće rizike.

2. Upravljanje rizikom

Kako bi lakše razumjeli rizik i upravljanje rizikom bitno je razumijeti pojmove, rizik i upravljanje rizikom.

Rizik je u literaturi definiran kao funkcija razine prijetnje, ranjivosti i vrijednosti informacijske imovine. [1]

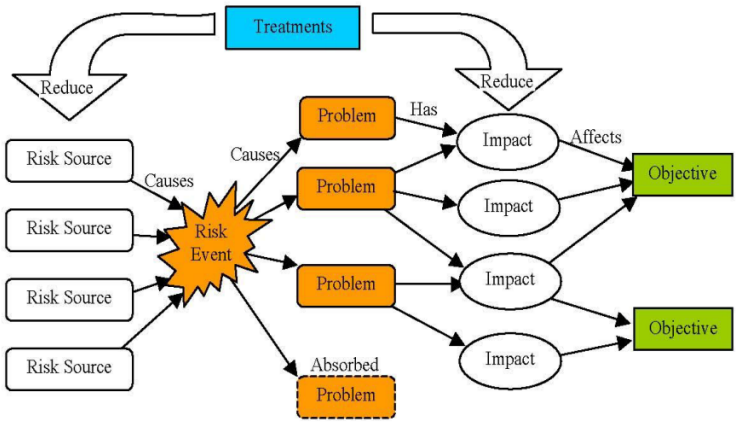
Da bi se dakle nešto moglo smatrati rizikom moraju biti prisutne sve tri komponente:

- Prijetnja
- Ranjivost
- Vrijednost imovine

Rizik se jasnije može opisati kao vjerojatnost prijetnje da iskoristi neku ranjivost imovine te time ugrozi imovinu. S obzirom na navedene definicije rizik je moguće prikazati matematičkom formulom:

RIZIK = PRIJETNJA * RANJIVOST * VRIJEDNOST IMOVINE

Na slici 2.1. [1], prikazati ćemo na koji način rizik djeluje i gdje treba djelovati kako bi se smanjio utjecaj rizika i pojavljivanja rizika uopće.



Slika 2.1. Odnos rizika i utjecaj na ostvarenje ciljeva

Na slici 2.1 se jasno može vidjeti na koji način rizik djeluje na određene poslovne ciljeve, ako govorimo iz aspekta sigurnosti IS-a, onda možemo za primjer kao izvor rizika uzeti bilo koji rizik koji odgovara tom području. Za potrebe analiziranja slike i objašnjenja na koji način zapravo rizik utječe na ciljeve, govoriti ćemo na primjeru požara u server sali. Ako pogledamo lijevu stranu slike, jasno možemo vidjeti da piše „Risk Source“ odnosno izvor rizika, izvor rizika u ovom slučaju može biti čovjek, kvar na instalacijama, stare i

neodgovarajuće mjere zaštite. Zbog ovih mogućih izvora rizika dolazi do „Risk Event“ odnosno događaja kad se pojavljuje ono što je bilo okaratkerizirano kao rizik. Sad više ne govorimo o riziku nego o neželjenom događaju koji nam je uzrokovao problem i troškove. Problem uz kvalitetnu zaštitu i jasno definirane mjere postupanja u slučaju nastupanja rizika možemo smanjiti ili otkloniti. Ukoliko ne uspijemo otkloniti problem taj problem ima utjecaj na ostavrenje ciljeve. Ako pogledamo gornji dio slike jasno se može vidjeti da upravljanje rizikom te pokušaj da se smanji utjecaj neželjenog događaj ide na dvije razine, odnosno pokušava se djelovati na dvije razine. Prva razina je pokušaj da se naprave sve predradnje kako bi se otklonio izvor rizika ili barem smanjila mogućnost pojavljivanja, ovu razinu bi mogli nazvati preventivna razina. Druga razina djelovanja je kad se rizik pojavi i uzrokuje neki neželjeni događaj a s tim događajem i problem, naš zadatak je definirati na koji način će se reagirati kad se pojavi rizik kako bi u što kraćem roku i sa što manjim troškovima otklonili problem i smanjili utjecaj rizika na naše poslovanje.

2.1. Procjena rizika

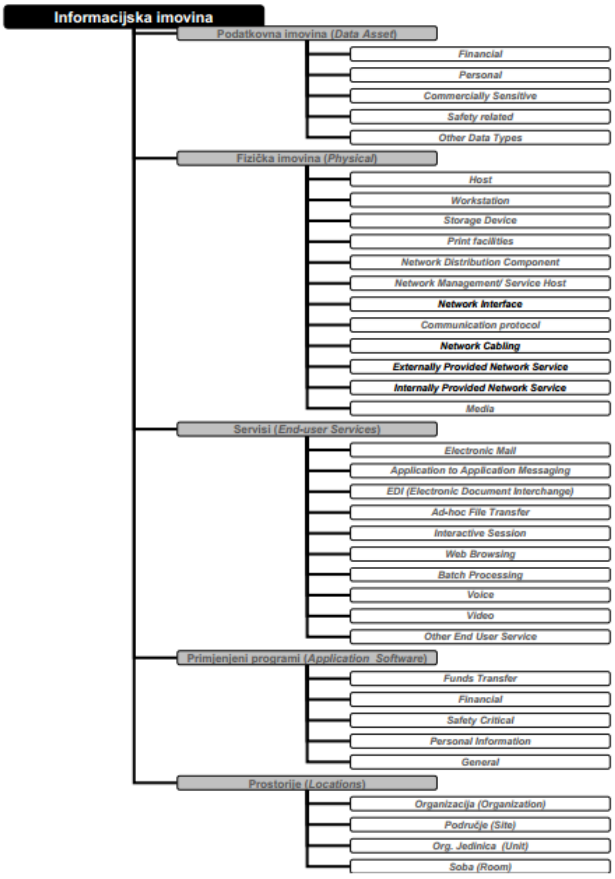
Nakon što smo općenito prikazali rizike i utjecaj rizika na poslovanje i ostvarenje ciljeva preko slike 2.1. sad će mo polako krenuti razvijati temu kroz rizike i sigurnost informacijskog sustava. Procjena rizika je jedna od važnijih aktivnosti u procesu upravljanja rizicima jer pokazuje koji rizici se mogu pojavljivati, pokušava se odrediti izvor rizika, koliki je značaj imovine na koju će rizik sa svojim pojavljivanjem utjecati, postoji li mogućnost ponovnog pojavljivanja rizika te na kraju slijedi izračun rizika.

Procjena rizika koji mogu djelovati na informacijski sustav i to ne samo informacijski sustav u smislu programskog rješenja, nego cjelokupni informacijski sustav koji sadrži sve dokumente, informacije i podatke koji predstavljaju imovinu poduzeća i kao takvi su podložni rizicima. Procjena rizika se provodi sa svrhom očuvanja i zaštite informacijske imovine te cjelovitosti infomracijskog sustava. Svako poduzeće posjeduje imovinu koja je od „vitalne“ važnosti za poslovanje i takvu imovinu je potrebno zaštititi. Kako bi se imovina zaštitila potrebno je definirati tko je vlasnik imovine, odnosno tko sve ima pristup određenoj imovini poduzeća, na koji način se određena imovina smije i mora koristiti kako ne bi došlo do pojavljivanja neželjenih događaja, te gubitka imovine, ili zlouporabe imovine. Ukoliko govorimo o podatkovnom sadržaju kao imovini poduzeća potrebno je odrediti značaj tog podatkovnog sadržaja i to prema vanjskim i unutarnjim čimbenicima[2]. Na temelju ovog do sad viđenog procjenu rizika mogli bi podjeliti u 4 podkategorije i to[4]:-

- Identifikacija imovine
- Analiza rizika
- Izlaganje riziku
- Prioritetizacija rizika

2.1.1. Identifikacija imovine

Identifikacija imovine je postupak kojim se pokušava odrediti sva imovina poduzeća, ali isto tako i vlasništvo nad tom imovinom. Kako bi uspješno napravili identifikaciju imovine potrebno je napraviti inventuru imovine odnosno popis imovine koju poduzeće posjeduje. Naravno imovina osim materijalne imovine može biti i nematerijalna. Nematerijalna imovina [2] su informacije, komunikacija, procedure i druge stvari koje nemaju materijlani oblik ali s gubitkom, krađom ili izmjenom te imovine poduzeće može ostvariti gubitke. Na slici 2.1.1.1[4] je prikazan popis informacijske imovine i moguća podjela te imovine.



Slika 2.1.1.1 Popis informacijske imovine

Sa slike 2.1.1.1 se jasno može vidjeti popis informacijske imovine te što sve jedan takav popis može sadržavati. Ono što se nemože isčitati iz ovog popisa je tko je ovlašten da koristi određenu imovinu, odnosno tko je vlasnik imovine. Dodjela vlasnika imovine je druga faza u

identifikaciji imovine. Dodjela vlasništva je izrazito bitna faza kod identifikacije imovine[5], jer je to prvi korak ka smanjenju ili povećanju rizika. Osobe kojima se dodjeljuje vlasništvo nad određenom imovine, a osobito nad imovinom od velikog značaja, trebaju proći različite testove kako bi pokazali sposobnost korištenja takve imovine ali i kako bi se provjerile namjere određene osobe koja dobiva vlasništvo nad imovine, kako kasnije ne bi došlo do krađe, iskorištavanja imovine ili preprodaje informacija i podatkovnog sadržaja koje poduzeće nastoji zaštititi. Možemo reći da dodjela vlasništva nad imovinom je prvi korak u smanjenju rizika, ako se imovina povjeri stručnoj, savjesnoj i odgovornoj osobi. Važna stavka svakog dijela procjene rizika, upravljanja rizikom i cijelog menadžmenta vezanog uz rizik je dokumentarnost. Odnosno potrebno je dokumentirati sve važnije radnje i aktivnosti, kako kasnije u slučaju pojavljivanja neželjenog događaja možemo utvrditi greške te jednostavno pronaći način na koji će se djelovati u budućnosti kako bi smanjli vjerojatnost pojavljivanja rizika.

2.1.2. Analiza rizika

Analiza rizika predstavlja skup aktivnosti koje se provode s ciljem kako bi se dobio uvid u potencijalne rizike, ranjivosti sustava na koje rizici mogu djelovati, na kvalitetu mjera i kontrola za postupanje s rizicima. Analiza rizika je cjelokupni proces od uočavanja rizika i prijetnji sustavi do analize kakav će utjecaj pojavljivanje rizika imati za poslovanje. Analizu rizika možemo podjeliti na[6]:

- Identifikacija prijetnji
- Identifikacija ranjivosti
- Analiza kontrole
- Analiza utjecaja

Identifikacija prijetnji predstavlja prepoznavanje prijetnji koje mogu utjecati na sustav. Važno je reći da osim prepoznavanja koje to prijetnje mogu utjecati na naš sustav se isto tako mora odrediti kolika je vjerojatnost pojavljivanja određene prijetnje i na kraju sve treba dokumentirati. Izvori prijetnji mogu biti različiti(čovjek, priroda, okolina) ali ipak u najvećoj mjeri danas je čovjek najveća prijetnja sigurnosti informacijskog sustava i to namjerno ili nenamjerno. 60% prijetnji dolazi od čovjeka[2]. Postoje različiti načini kako bi se smanjila prijetnja od strane čovjeka ali o tome će biti više riječi kad se krene s mjerama za smanjenje rizika. Rezultat indentifikacije prijetnji je[6] izvještaj o prijetnjama što predstavlja popis prijetnji koje mogu utjecati na ranjivost sustava.

Identifikacija ranjivosti uvelike ovisi o fazi razvoja IS-a pa tako[6]:

- U fazi analize i dizajna IS-a potraga za ranjivošću sustava je fokusirana na sigurnosnu politiku poduzeća, planirane procedure sigurnosti i definiciju korisničkih zahtjeva.
- Kod implementacije IS-a identifikacija ranjivosti sustava nastoji uključiti više specifičnih informacija koje su planirane i opisane u dokumentaciji o sigurnosti, te kod provjere i testiranja sustava.
- Kada je sustav u upotrebi proces identifikacije ranjivosti uključuje analizu sadržaja i kontrole sigurnosti, tehničke komponente i procedure koje se koriste u zaštiti sustava.

Cilj ovog koraka je sastaviti popis ranjivosti sustava koje mogu biti iskorištene od strane potencijalnih izvora prijetnji. Preporučene metoda za određivanje ranjivosti sustava su testiranje sustava i izrada kontrolnih listi zahtjeva za sigurnošću sustava. Kontrolna lista sadrži osnovne standarde za sistematiziranu procjenu i identifikaciju ranjivosti imovine.

Analiza kontrole je korak u kojem se pokušava odrediti koje kontrole su razvijene ili prihvaćene iz ISO standarda kako bi se osigurala sigurnost informacijskog sustava. Već prije je navedeno da se područjem kontrola bavi ISO 27001 standard koji definira niz kontrola i mjera koje bi poduzeće ukoliko uoči potrebu za uvođenje te kontrole trebalo provesti. Upravo u ovom koraku se pokuašava odrediti koja kontrola je odgovarajuća da se uvede kako bi se smanjio utjecaj i pojavljivanje prijetnji. Rezultat ovog koraka je lista tekućih ili planiranih kontrola koje će se koristiti u sustavu da bi se ublažila mogućnost prijetnji i smanjio utjecaj tog štetnog događaja.

Kako bi proveli analizu utjecaja potrebno je odrediti pasivni utjecaj uspješno izvšene prijetnje na ranjivost sustava. Analizu utjecaja možemo gledati i kroz sigurnosne ciljeve a to su očuvanje integriteta, uporabljivosti, povjerljivosti. Očuvanja integriteta je zaštita podataka od neželjenih promjena koje dovode do pogrešnih zaključaka i odluka i s tim mogu utjecati u velikoj mjeri na prosperitet poduzeća. Gubitak upotrebljivosti pretpostavlja ispad sustava i nemogućnost korištenja cijelog ili dijela sustava. Ako promatramo sustav u produkcijskim uvjetima to može dovesti do velikih troškova i problema u poslovanju. Gubitak povjerljivosti označava da neka treća strana neovlašteno pristupa određenim podacima, što dovodi do gubitka, krađe ili promjene informacija.

2.1.3. Izlaganje riziku

Važna odluka svake uprave i visokog menadžmenta je odluka o tome kako će se postupati s određenim rizicima, tj. hoće li rizik ići na daljnju procjenu(što iziskuje određene troškove) ili će se taj rizik zanemariti. Važno je napomenuti da se danas u velikom broju poduzeća ne posvećuje dovoljno velika pažnja na utjecaj rizika na poslovanje i da se dobar dio rizika zanemaruje što s pojavom rizika donosi nepotrebne troškove. Važno je odmjeriti koliki utjecaj će različiti rizici imati na poslovanje ako se oni pojave. Izlaganje riziku je nažalost jedan od najčešćih načina upravljanju rizicima a predstavlja ništa drugo nego dodatni rizik. Ono zbog čega je ovo nevedeno prije samog izračuna rizika i prioritizacije rizika je da se dobije uvid u stvarno stanje i pokuša osvijestiti visoki menadžment na važnost upravljanja rizicima i to osobito u području informacijske sigurnosti.

2.1.4. Prioritetizacija rizika

Svaki rizik koji je uočen i postoji potreba za upravljanje tim rizikom ima određeni prioritet ovisno o svom području djelovanja i informacijskoj imovini na koju djeluje. Kako bi lakše postavili prioritet u području upravljanja rizicima koristimo različite metode izračuna rizika koje nam pokazuju koliki utjecaj će imati koji rizik sa svojim pojavljivanjem. Danas su najčešće dvije metode izračuna rizika koje će biti prikazane na slikama 2.1.4.1.[7] i 2.1.4.2[7].

Vrijednost imovine	Razina prijetnje								
	Mala			Srednja			Velika		
	Razina ranjivosti								
	M	S	V	M	S	V	M	S	V
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8

Slika 2.1.4.1 Imovina*Prijetnja*Ranjivost

Vjerojatnost ostvarivanja prijetnje	Utjecaj			
	Vrlo veliki (100)	Umjereno veliki (60)	Srednji do mali (30)	Vrlo mali (10)
Vrlo velika (1)	Vrlo visok (100)	Vrlo visok (60)	Visok (30)	Srednji (10)
Umjereno velika (0,6)	Vrlo visok (60)	Visok (36)	Srednji (18)	Nizak (6)
Srednja do mala (0,3)	Visok (30)	Srednji (18)	Nizak (9)	Nizak (3)
Vrlo mala (0,1)	Srednji (10)	Nizak (6)	Nizak (3)	Nizak (1)

Slika 2.1.4.2 Vjerojatnost*Utjecaj

Na temelju slika 2.1.4.1 i 2.1.4.2 možemo vidjeti na koje načine se može izračunati rizik. Isto tako na temelju tih slika jasno se može vidjeti kako se stavljaju prioriteti na određeni rizik. Možemo reći da se na temelju slike 2.1.4.1 jasno vidi na koji način je dodijeljena vrijednost imovine, vrijednost razina prijetnje i razina ranjivosti, te prema dobivenim koeficijentima na koji način su postavljeni prioriteti. Vidimo da rizik koji ima koeficijent 1-2 predstavlja niski prioritet, rizik koji ima koeficijent 3-5 predstavlja srednji prioritet, a rizik koji ima koeficijent 6-8 predstavlja visoki proiritet. Slika 2.1.4.2 daje drugačiji pristup izračunu rizika ali kao rezultata isto daje matricu s koeficijentima koje predstavljaju prioritetne ili manje prioritetne rizike. Ove dvije matrice predstavljaju primjer izračuna rizika i nisu standard, ovisno od poduzeća do poduzeća se mjenja veličina matrice i vrijednosti u matrici ali ono što je bitno je ideja po kojoj se izračunava rizik i stavlja prioritet, te što taj prioritet predstavlja. Rizik visokog prioriteta zahtjeva brzu reakciju i kvalitetne mjere koje će smanjiti vjerojatnost pojavljivanja ili ako se nemože utjecati na vjerojatnost pojavljivanja treba pokušati smanjiti utjecaj rizika. Ako uspiješno smanjimo rizik od pojavljivanja i utjecaj tog rizika on gubi na vrijednosti i smanjuje mu se proiritet, važno je za reći da iako smo uspješno otklonili veći dio rizika ostaje još jedan dio koji se naziva rezidualni rizik, odnosno preostali rizik nakon postupanja s rizikom. Takav rizik nebi trebao imati veći utjecaj na poslovanje i stvoriti dodatne troškove za poduzeće, ali je bitno da uprava bude upoznata s takvim rizikom u slučaju da se prioritet tog rizika ponovno poveća zbog nekih promjenjenih okolnosti[2]. Uprava poduzeća je ta koja donosi odluku hoće li se s određenim rizikom postupati u cilju smanjenja pojavljivanja i utjecaja tog rizika ili će se određeni rizik zanemariti. Na ljudima koji se bave informacijskom sigurnošću je da upoznaju upravu s rizicima i podignu razinu svijesti o nepotrebnim troškovima koje određeni rizik sa svojom pojavom donosi.

2.2. Kontrola rizika

2.2.1. Smanjenje rizika

Smanjenje rizika je kontinuirani posao s kojim se nastoji smanjiti vjerojatnost pojavljivanja, ranjivost i učinak rizika ako se pojavi. Smanjnje rizika se ne odnosi samo na to da primjerice postavimo protupožarnu zaštitu i u slučaju izbijanja požara brzo reagiramo, već se i odnosi na to da napravimo sve predradnje koje se zahtjevaju kako do incidentne situacije uopće nebi došlo. Kako smanjiti rizik od pojavljivanja neželjenih događaja ovisi o svakom poduzeću zasebno, ali budući je to vrlo širok posao gdje se treba sagledati jako puno mogućih rizika kojih su određena poduzeća svjesna ali i mnogo onih kojih nisu svjesna razvijen je ISO 27001 standard koji nudi popis od 134 mjera i kontrola s kojima je obuhvaćen velik dio rizika i način obnašanja prema riziku s ciljem smanjenja rizika. Područje informacijske sigurnosti kod mnogih poduzeća se veže najčešće uz pitanje softwera i rijetko je razvijena svijest koliko je to područje široko. ISO 27001 daje popis kontrola, a ISO 27002 najbolju praksu u primjeni tih kontrola, pregled ovih dvije normi jasno pokazuje širinu koju obuhvaća područje informacijske sigurnosti. Iako ISO 27001 nudi popis mjera a ISO 27002 objašnjava kako je najbolje implementirati te mjere u vlastiti poslovni sustav, nitko ne garantira da će te ukoliko implementirate sve mjere iz norme ISO 27001 imati potpuno siguran sustav i rizik će biti smanjen na razinu rezidualnog, ali zato implementacijom mjera i kontrola iz ISO norme 27001 ćete uvelike smanjiti veliki broj rizika koji spadaju u područje kritičnih. Ponekad je implementacija mjera izrazito skupa i svako poduzeće treba odmjeriti koliki mu je rizik i s pojavljivanjem njegov učinak velik, kako bi se postigao optimalan balans između smanjenja rizika i cijene implementacije mjere. Budući da će mo se mjerama i kontrolama iz ISO norme 27001 baviti naknadno nećemo previše duljiti te će smanjenje rizika kroz mjere i kontrole ISO 27001 norme biti puno bolje objašnjeno kasnije.

2.2.2. Planiranje u kriznim situacijama

Kad bi se krenulo zaključivati iz naslova dobar dio čitatelja bi mogao zaključiti da se ovo područje bavi planiranje i reakcijom kad se pojavi rizik i ostvaruju se negativni učinci rizika. Naprotiv planiranje u kriznim situacijama predstavlja planiranje koje se događa prije nego se prepoznati rizik pojavi kao neki neželjeni događaj. Važnost takvog planiranja je da se poslovni sustav, informacijski ali općenito govoreći i svi ostali sustavi s pojavljivanjem rizika u najkraćem mogućem roku oporave i uspostavi se normalno funkcioniranje cijelokupnog sustava. Važnost ovakvog planiranja se pokazuje na nekoliko realnih primjera gdje nije bio

predviđen plan „B“ jer se vjerovalo u apsolutnu sigurnost sustava. [2] WTC je prije rušenja u napadu 11.9.2001. godine doživio napad i prije gdje je postavljen kombi s bombom u garaži WTC nebodera. Budući da se kompletna informacijska tehnologija i serveri nalazili na prvih par katova katastrofalno su stradali te je stručnjacima za prikupljanje svih podataka trebalo više od mjesec dana da podignu sustav i povrate veći dio podataka i informacija. Naučeni tim primjerom postavljena je rezervna lokacija na kojoj se nalazio backup koji je omogućio da se nakon 11.9.2001., kad su oba dva nebodera WTC-a srušena, cijeli sustav podigne u tek nekoliko minuta. Ovaj primjer jasno pokazuje koliku važnost ima planiranje u kriznim situacijama i koliki su benefiti ako se dobro procjeni rizik i odredi postupanje s tim rizikom. Iako planiranje u kriznim situacijama donosi velike benefite za oporavak sustav i za brzu reakciju prilikom pojavljivanja rizika, to planiranje uvelike ovisi o procjeni menadžmenta za koje rizike će se raditi plan „B“ i koliko novaca će se izdvojiti kako bi se postiglo optimalno rješenje.

2.2.3. Praćenje rizika

Prilikom uočavanja rizika ovisno o izračunu i procjeni rizika, sa rizicima se različito postupa. Rizici koji su u kategoriji kritičnih rizika se rješavaju u najkraćem vremenu, s tim da je preostali rizik nakon smanjenja kritičnih rizika(rezidualni rizik) potrebno dokumentirati i pratiti. Srednje kritični rizici se rješavaju prema odluci uprave i te odluke se moraju dokumentirati a rizici ovisno o odluci se rješavaju odmah ili s počekom. Rizici manjeg značaja najčešće se ne rješavaju ali se moraju pratiti kako se njihov status nebi promijenio i njihovo pojavljivanje dovelo do velikih troškova. Prema ovoj kategorizaciji rizika, jasno se može reći da bez obzira koliki je značaj uočenog rizika uviđa se potreba da se svi rizici prate kako se značaj rizik nebi promijenio i kako s pojavljivanjem rizika čiji je učinak naizgled zanemariv, nebi došlo do velikih troškova jer se promjenio status imovine ili nekog drugog faktora koji utječe na štetu prilikom pojavljivanja rizika. Upravo zbog toga je poželjno kontinuirano preispitivanje i procjena rizika, kako bi se u svakom trenutku imao uvid u to koliko koji rizik sa svojim pojavljivanjem može nanijeti štete sustavu. Lakomisleno bi bilo pretpostaviti da se „vrijednost“ rizik ne mijenja, i to ponajviše zbog toga je je poslovni sustav uz koji je usko vezan i informacijski sustav podložan promijena koje diktira izrazito promijenjiva okolina i situacija na tržištu. Upravo zbog se stalno mijenja vrijednost određenih informacija i imovine a time se povećava i rizik od napada na takvu imovinu.

3. Strategije upravljanja rizikom

Postoje različite strategije upravljanja rizikom, one koje će ovdje biti obrađene su najrasprostranjenije i opće prihvaćene, te se može reći da globalno obuhvaćaju manje strategije upravljanja rizikom. Strategije upravljanja rizikom koje će u nastavku biti obrađene i opisane uvelike prikazuju odluku uprave na koji način će se postupati s rizikom. Na temelju toga razlikujemo 4 strategije:-

- Izbjegavanje rizika
- Smanjenje rizika
- Prenošenje rizika
- Prihvaćanje rizika

Strategija smanjenja rizika će biti obrađena na kraju kroz pregled mjera iz ISO normi, a preostale tri strategije će biti ukratko opisane.

3.1. Izbjegavanje rizika

Izbjegavanje rizika je najsigurnija strategija upravljanja rizikom. Izbjegavanje rizika pretpostavlja da se poduzeće neće upuštati u poslove koji za sobom nose određeni rizik[8]. Na taj način poduzeće anulira mogućnost pojavljivanja rizika. Kad bi se svaka mogućnost pojavljivanja rizika mogla rješiti jednostavnim izbjegavanjem rizika ne bi postojala nikakva potreba da se govori o rizicima, ali nažalost to nije svaki put moguće pa poduzeća i stručnjaci iz područja informacijske sigurnosti moraju tražiti druga rješenja kako ih određeni rizik ne bi usporio ili s njegovom pojavom kako ne bi ostvarili velike gubitke.

3.2. Prenošenje rizika

Prenošenje ili transfer rizik pretpostavlja da se rizik sa poduzeća prenese na neku treću stranu, najčešće su to osiguravajuće kuće koje osiguravaju različite rizike i nude mogućnost nadoknade nastale štete[9]. Osim osiguranja rizik se može prenijeti i na društva koja nisu osiguravajuća. Kad govorimo o prenošenju rizika na osiguravajuća društva postoji plaćanje premije osiguranja i dogovara se polica osiguranja koja definira koliko će novaca biti isplaćeno ako dođe do nastanka štete, te iznos premije. Preko osiguravajućih kuća se može osigurati velik broj rizika ali je upitna visina premije i isplati li se osiguravati rizike koji će povećati premiju osiguranja a nisu u kategoriji rizičnih i šteta koja će nastati s njihovim pojavljivanjem neće biti velika. Kad govorimo o prenošenju rizika na društva koja nisu

osiguravajuća, tu se najprije podrazumjevaju[10] druga dionička društva gdje se rizik raspodjeluje između dioničara i to u visina kapitala. Postavlja se pitanje zašto bi neka treća strana preuzela rizik drugog poduzeća, odgovor na to je zapravo vrlo jednostavan a leži u ideji da se rizik prenosi na treću stranu koja ima više iskustva i znanja upravljanja rizicima od poduzeća koje želi prenijeti rizik. Važno je napomenuti da su premije kod ovakvog prenošenja rizika puno manje od premija koje se plaćaju osiguravajućim kućama.

3.3. Prihvaćanje rizika

Prihvaćanje rizika je postupak u kojem se uprava poduzeća upoznaje i s rizikom, svijesna je rizika i prihvaća taj rizik. Potrebno je formalno potvrditi odnosno dokumentirati[11] prihvaćanje rizika i odrediti odgovorne za taj rizik. Prihvaćanje rizika najčešće se radi s rezidualnim rizikom, odnosno s rizikom koji je preostao nakon poduzimanja određenih mjera zaštite s kojima je smanjen prvotni obrađivani rizik. Rezultat prihvaćanja rizika je popis rizika koje prihvaća menadžment poduzeća i odgovornosti za pojedini rizik, kao i opis rizika koji su neprihvatljivi i za koje je potrebno implementirati daljnje mjere kako bi se doveo na razinu rezidualnog rizika kojeg se neće posebno obrađivati već samo pratiti. U nastavku će biti prikazan popis mjera za smanjenje rizika prema ISO 27002 normi. A Opis ovih mjera se može naći u poglavlju 4 ove knjige.

4. Popis mjera i kontrola za smanjenje rizika iz ISO 27002

Ovdje će biti naveden popis mjera i kontrola iz ISO 27002 norme, te će kasnije poslužiti kako bi se određene mjere prikazale u nastavku kroz različite mjere zaštite.

Popis mjera i kontrola iz ISO 27002[18]:

1. Procjena i obrada rizika

   Procjenjivanje sigurnosnih rizika

   OBRADA SIGURNOSNIH RIZIKA

2. Politika sigurnosti

   Politika informacijske sigurnosti

   Dokument politike informacijske sigurnosti

   Provjera politike informacijske sigurnosti

3. Organizacija informacijske sigurnosti

    Unutarnja organizacija

        Obveza uprave prema informacijskoj sigurnosti

        Koordinacija informacijske sigurnosti

        Dodjeljivanje odgovornosti za informacijsku sigurnost

        Proces ovlaštenja za opremu za obradu informacija

        Sporazum o povjerljivosti

        Kontakt s nadležnim tijelima

        Kontakti s posebnim interesnim grupama

        Nezavisna provjera informacijske sigurnosti

    Vanjski suradnici

        Prepoznavanje rizika koji se odnose na vanjske suradnike

        Priprema sigurnosti u radu s klijentima

        Priprema sigurnosti u sporazumima s trećim stranama

4. Upravljanje imovinom

    Odgovornost za imovinu

        Popis imovine

        Vlasništvo nad imovinom

        Prihvatljiva uporaba imovine

    Klasifikacija informacija

        Smjernice za klasifikaciju

        Označavanje i uporaba informacija

5. Sigurnost ljudskog potencijala

Prije zaposlenja

Funkcije i odgovornosti

Odabir kandidata

Trajanje i uvjeti zaposlenja

Tijekom zaposlenja

Odgovornosti uprave

Razina svijesti o informacijskoj sigurnosti

Disciplinski proces

Prekid ili promjena zaposlenja

Odgovornosti za prekid

Povrat imovine

Ukidanje prava pristupa

6. Fizička sigurnost i sigurnost okruženja

Osigurana područja

Granice fizičkog sigurnosnog prostora

Kontrole fizičkog pristupa

Osiguranje ureda, prostorija i opreme

Zaštita od vanjskih prijetnji i nepogoda

Rad u osiguranim područjima

Područja s javnim pristupom, područja za isporuku i utovar

Sigurnost opreme

Smještaj opreme i zaštita

Prateće usluge i oprema

Sigurnost ožićenja

Održavanje opreme

Sigurnost opreme izvan prostora organizacije

Sigurno odbacivanje ili ponovno korištenje opreme

Iznošenje opreme

7. Upravljanje komunikacijama i operacijama

Operativne procedure i odgovornosti

Dokumentiranje radne procedure

Upravljanje promjenom

Odjeljivanje funkcija

Odjeljivanje razvojne, ispitne i operativne opreme

Upravljanje pružanjem usluge treće strane

Pružanje usluge

Nadzor i provjera usluga treće strane

Upravljanje promjenama usluga treće strane

Planiranje i prihvaćanje sustava

Upravljanje kapacitetom

Prihvaćanje sustava

Zaštita od zlоćudnog i prenošljivog koda

Kontrole za zaštitu od zlоćudnog koda

Kontrole za zaštitu od prenošljivog koda

Sigurnosne kopije

Sigurnosne kopije informacija

Upravljanje sigurnošću mreže

- Kontrola mreže
- Sigurnost mrežnih usluga

Rukovanje medijima

- Upravljanje uklonjivim medijima
- Odbacivanje medija
- Procedure rukovanja informacijama
- Sigurnost dokumentacije sustava

Razmjena informacija

- Politike i procedure za razmjenu informacija
- Sporazum o etici
- Prijevoz fizičkih medija
- Elektroničke poruke
- Poslovni informacijski sustavi

Usluge elektroničke trgovine

- Elektronička trgovina
- On-line transakcije
- Javno dostupne informacije

Nadzor

- Revizijski zapisi
- Nadzor uporabe sustava
- Zaštita informacija zapisa
- Zapisi administratora i operatera

Zapisi o zastojima

Sinkronizacija satova

8. Kontrola pristupa

Poslovni zahtjevi za kontrolu pristupa

Politika kontrole pristupa

Upravljanje korisničkim pristupom

Prijavljivanje korisnika

Upravljanje povlasticama

Upravljanje korisničkim zaporkama

Provjera prava korisničkog pristupa

Odgovornosti korisnika

Uporaba lozinke

Korisnička oprema bez nadzora

Politike praznog stola i praznog zaslona

Kontrola pristupa mreži

Politika uporabe mrežnih usluga

Provjera vjerodostojnosti korisnika za vanjske veze

Prepoznavanje opreme u mrežama

Zaštita priključka za daljinsku dijagnostiku i konfiguraciju

Odvajanje u mrežama

Kontrola mrežne veze

Kontrola mrežnog usmjeravanja

Kontrola pristupa operacijskom sustavu

Procedure sigurnog prijavljivanja

Identifikacija i provjera vjerodostojnosti korisnika

Sustav upravljanja zaporkama

Uporaba sistemskih uslužnih programa

Vrijeme isteka sjednice

Ograničavanje trajanja spajanja

Kontrola pristupa aplikacijama i informacijama

Ograničavanje pristupa informacijama

Izolacija osjetljivih sustava

Uporaba mobilnih uređaja i rad na daljinu

Uporaba mobilnih računala i komunikacije

Rad na daljinu

9. Nabava, razvoj i održavanje informacijskih sustava

Sigurnosni zahtjevi informacijskih sustava

Analiza ispecifikacija sigurnosnih zahtjeva

Ispravna obrada u aplikacijama

Provjera valjanosti ulaznih podataka

Kontrola interne obrade

Cjelovitost poruke

Provjera valjanosti izlaznih podataka

Kriptografske kontrole

Politika uporabe kriptografskih kontrola

Upravljanje ključevima

Sigurnost sistemskih datoteka

Kontrola operativnog softvera

Zaštita ispitnih podataka sustava

Kontrola pristupa izvornom kodu programa

Sigurnost u procesima razvoja i podrške

Procedure za kontrolu promjene

Tehnička provjera aplikacija nakon promjena operacijskog sustava

Ograničenja promjena softverskih paketa

Curenje informacija

Razvoj softvera povjeren vanjskim izvršiteljima

Upravljanje tehničkom ranjivošću

Kontrola tehničke ranjivosti

10. Upravljanje sigurnosnim incidentom

Izvještavanje o sigurnosnim događajima i slabostima

Izvještavanje o sigurnosnim događajima

Izvještavanje o sigurnosnim slabostima

Upravljanje sigurnosnim incidentima i poboljšanjima

Odgovornosti i procedure

Učenje na sigurnosnim incidentima

Prikupljanje dokaza

11. Upravljanje kontinuitetom poslovanja

Stanovišta informacijske sigurnosti pri upravljanju kontinuitetom poslovanja

Uključivanje informacijske sigurnosti u proces upravljanja kontinuitetom poslovanja

Kontinuitet poslovanja i procjena rizika

Razvoj i primjena planova kontinuiteta poslovanja koji uključuju informacijsku sigurnost

Okosnica planiranja kontinuiteta poslovanja

Ispitivanje, održavanje i ponovno procjenjivanje planova kontinuiteta poslovanja

12. Sukladnost

Sukladnost sa zakonskim propisima

Određivanje primjenjivih zakona

Prava intelektualnog vlasništva

Zaštita organizacisjkih zapisa

Zaštita podataka i privatnosti osobnih informacija

Sprječavanje zlouporabe opreme za obradu informacija

Odredbe o kriptografskim kontrolama

Sukladnost sa sigurnosnim politikama i standardima i tehnička sukladnost

Sukladnost sa sigurnosnim politikama i standardima

Provjera tehničke sukladnosti

Razmatranja revizije informacijskih sustava

Kontrole revizije informacijskim sustava

Zaštita alata za reviziju informacijskih sustava

4.1. Smanjenje rizika

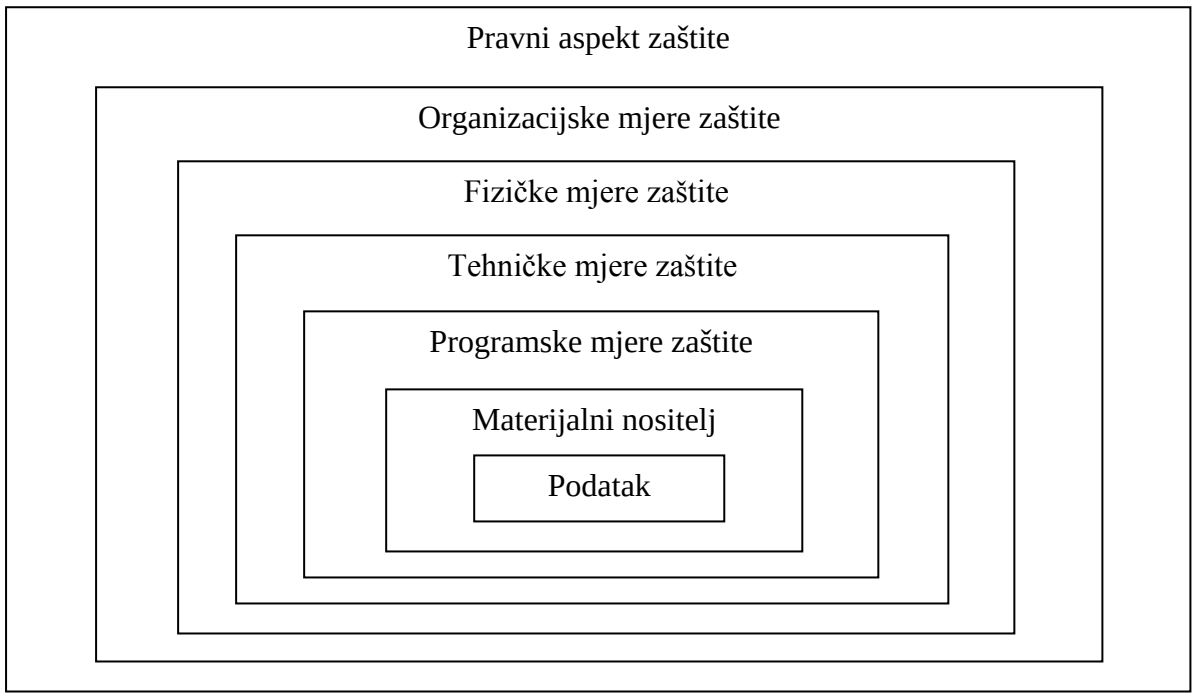
Smanjenje rizik je niz akcija i primjena različitih kontrola s ciljem smanjenja rizika na prihvatljiv rizik. Potrebno je izabrati odgovarajuće i opravdane kontrole za ispunjavanje uvjeta koji su identificirani kod procjene rizika i obrade rizika. Ovaj izbor treba uzeti u obzir kriterij prihvatljivosti rizika, kao i legalne, regulatorne i ugovorne zahtjeve. Također, izbor treba uzeti u obzir cijenu i vremenski okvir za implementaciju kontrola, odnosno tehničke, ekološke i kulturalne aspekte. Često je moguće smanjiti ukupni trošak vlasništva sustava sa pravilno odabranim kontrolama informacijske sigurnosti.

Općenito, kontrole mogu osigurati jedan ili više tipova zaštite[11]: ispravak, eliminaciju, prevenciju, smanjenje utjecaja, odvraćanje, otkrivanje, oporavak, praćenje, opreznost. Tijekom odabira kontrole važno je izmjeriti troškove akvizicije, implementacije, administracije, rada, nadzora i održavanja kontrole protiv vrijednosti imovine koja je zaštićena. Nadalje treba uzeti u obzir, povrat od investicije u smislu smanjenja rizika i potencijala za iskorištavanje novih poslovnih prilika koje pružaju određene kontrole. Osim toga, treba razmotriti specijalizirane vještine koje će možda biti potrebne pri definiranju i implementaciji novih kontrola ili modifikaciji postojećih. ISO/IEC 27002[11] pruža detaljne informacije o kontrolama. Postoji mnogo ograničenja koja mogu imati utjecaj na odabir kontrola. Tehnička ograničenja, kao što su izvedbeni zahtjevi, upravljivost (zahtjevi operativne potpore) i pitanja kompatibilnosti, mogu spriječiti korištenje određenih kontrola ili mogu izazvati ljudske pogreške bilo da je u pitanju osporavanje kontrole, davanja lažnog osjećaja sigurnosti ili pak povećanje rizika izvan granica kontrole. Štoviše, to bi mogao biti slučaj kada kontrola utječe na performanse. Menadžeri bi trebali pokušati identificirati rješenje koje zadovoljava uvjete izvođenja, a jamči dovoljnu sigurnost informacija. Rezultat ovog koraka je lista mogućih kontrola, sa pripadajućim troškovima, koristima i prioritetima implementacije. Pri odabiru kontrole i tijekom provedbe, potrebno je uzeti u obzir razna ograničenja. Tipično, uzimaju se slijedeća ograničenja[11]:

- Vremenska ograničenja
- Financijska ograničenja
- Tehnička ograničenja
- Operativna ograničenja
- Kulturalna ograničenja
- Etička ograničenja

- Ograničenja okoliša
- Zakonska ograničenja
- Jednostavnost korištenja
- Ograničenja osoblja
- Prepreke za integraciju novih i postojećih kontrola

Naravno ova ograničenja ne znače da nije moguće smanjtiti rizik, ona pokazuju na koje stvari se treba paziti prilikom implementacije mjera za smanjenje rizika. ISO norme nude različite mjere za smanjenje rizika i upravo ova ograničenja pokazuju da nije uvijek jednostavno i moguće implementirati upravo te mjere. Nekad je potrebno izvesti vlastito rješenje koja će pružiti odgovarajuću zaštitu i smanjiti rizik na prihvatljivu razinu. Osim toga ova ograničenja upućuju upravo na veliku različitost poduzeća i činjenicu da je teško složiti mjere koje budu jedinstvene za sva poduzeća i koje budu sva poduzeća mogla implementirati u svoj ISMS. Kad govorimo o mjerama za smanjenje rizika, možemo reći da te mjere možemo podjeliti u neke logičke cijeline. Te cijeline će biti prikazane i objašnjene preko slike 3.4.1.[2] na kojoj će u centru biti prikazan podatak kao osnovna stvar koju pokušavamo zaštiti. Jer podatak je apstraktan pojam koji čini informaciju i kao takav je temelj informacijskog sustava. Svi dokumenti, datoteke, informacije se sastoje od podataka i zato je upravo preko podatka kao temelja informacijskog sustava najlakše opisati grupe mjera i prikazati na koji način je moguće smanjiti rizik.



Slika 4.1.1. Mjere za smanjenje rizika

4.1.1. Materijalni nositelj

Materijalni nositelj možda ne izgleda kao mjera zaštite ali predstavlja prvi korak zaštite podataka i o odabiru materijalnog nositelja ovisi odabir mjera i kontrola iz ostalih područja. Materijalni nositelj podataka može biti papir, magnetski disk, optički disk ili mikrofilm[11]. Ovisno o materijalnom nositelju podataka potrebno je odrediti mjere zaštite i rukovanja s materijalnim nositeljem u skladu s propisanim pravilima[2]. Trajnost dokument ovisi o potrebi za podacima koji su pohranjeni na dokumentu, ako postoji potreba za čuvanjem dokumenta na duži period od izrazite je važnosti odabrati materijalni nositelj podataka koji ima bolja tehnička i kemijska svojstva. Ako gledamo prema tehničkim i kemijskim svojstvima materijalnog nositelja u tom slučaju najdulji vijek trajanja ima mikrofilm a najkraći vijek trajanja imaju magnetski i optički disk. Papir kao materijalni nositelj ima najmanji kapacitet što stvara veliki problem s arhiviranjem ali i otežanu mogućnost pretraživanja. Uz to papir kao materijalni nositelj je izrazito podložan koroziji od strane vlage, lako je zapaljiv i iz tih razloga zahtjeva kontrolirane uvjete arhiviranja kao i velike mjere zaštite[2]. Postavlja se pitanje zašto se papir koristi. Odgovor na to se može naći u jednostavnosti korištenja papira, velikoj dostupnosti ali i u praksi koja pokazuje da papir predstavlja mogućnosti koje danas nisu u potpunosti razvijene za druge nositelje podataka, te nikakvu podložnost krađi podataka putem računalnog kriminala. Ipak radi jednostavnosti pretraživanja i korištenja podataka podaci koji su pohranjeni na papiru se digitaliziraju i pohranjuju na druge materijalne nositelje podataka. S aspekta uništenja dokumenata papir predstavlja vrlo zahvalan materijal, jer ukoliko organizacija odluči da se određeni dokumenti moraju uništiti, oni dokumenti koji su pohranjeni na papiru se mogu vrlo lako uništiti s gotovom nikakvom mogućnošću povrata podataka[2]. Magnetski disk kao materijalni nositelj podataka može biti tvrdi disk, i floppy disketa koje su danas izbačene iz upotrebe zbog vrlo malog kapaciteta. U ovu kategoriju mogli bi svrstati i magnetske kartice koje se najčešće reprezentiraju kao kartice koje omogućuju pristup određenim podacima. Ovakve kartice imaju magnetsku traku koja sadrži podatke o korisniku kartice i najčešće dolaze uz dodatnu mjeru zaštite kao što je PIN odnosno dodatni ključ koji omogućava nemogućnost korištenja kartice ukoliko se ne posjeduje ključ. Magnetski diskovi kao materijalni nositelji podataka imaju ograničen vijek trajanja na 5 do 10 godina ovisno o uvijetima korištenja, tehničkim svojstvima različitih proizvođača i gustoći zapisa. Magnetski diskovi i to tvrdi magnestki diskovi imaju vrlo veliku memoriju i kao takvi omogućuju pohranjivanje velikih količina podataka. Pristup podacima na magnetskom disku ide putem računala što predstavlja s jedne strane mogućnost zaštite ali s druge strane i veliku

prijetnju kad je računalo povezano na mrežu. Upravo zbog velikog rizika da se podacima može pristupiti dislocirano kad je računalo umreženo potrebno je uvesti različite mjere zaštite što programske, što fizičke. Potreba za tehničkim mjerama zaštite se javlja iz razloga jer postoji mogućnost kvara diska, što može dovesti do gubljenja djela podataka ili svih podataka na disku, koji se mogu vratiti forenzičkim putem što zahtjeva vrijeme i velika financijska sredstva. S aspekta uništenja podataka tvrdi disk je izrazito nepouzdan ako se želi uništiti samo dio podataka, jer svi podaci koji se jednom pospreme na tvrdi disk uz korištenje određenih tehnika mogu biti povraćeni bez obzira na način brisanja s diska. Kad govorimo o brisanju svih podataka ili uništenju diska onda se podaci mogu trajno uništiti uništavanjem diska, i to na način da se disk rastrga na velik broj djelova koje je kasnije nemoguće povezati u realnom vremenu[2]. Mikrofilm kao materijalni nositelj ima najduži vijek trajanja i kao takav koristi se za pohranjivanje podataka koji zahtjevaju čuvanje na duži vremenski period. Kao i papir, mikrofilm je analogni nositelj podataka. Podaci se na mikrofilm pospremaju slikanjem sadržaja s papira i to kao niz sličica. Upravo zbog svojih mehaničkih i kemijskih svojstava mikrofilm može izdržati i preko 100 godina a da podaci na njemu ostanu sačuvani u potpunosti. Podaci na mikrofilm se pospremaju u obliku role, kazete, košuljice, mikrofiša ili mikroplana, na kojima se nalaze slike, ton ili drugi oblik podataka. Upravo zbog velike mehaničke izdržljivosti i vijeka trajanja mikrofilm je najbolji izbor za pohranjivanje podataka na dulji period i to uz fizičke mjere zaštite koje će blokirati pristup prostorijama u kojima su pohranjeni podaci na mikrofilmu, osobama koje nemaju ovalšteni pristup.

4.1.2. Programske mjere zaštite

Programske mjere zaštite predstavlja zaštitu podatkovnog sadržaja na računalu, u komunikaciji, na mreži, zaštita od virusa i očuvanju podataka kroz multipliciranje sadržaja. Na temelju toga mogli bi programske mjere zaštite podjeliti na mjere zaštite na razini[13]:

- Operacijskog sustava
- Korisničke programske podrške
- Komunikacije
- Dupliciranja sadržaja na drugim materijalnim nositeljima
- Malicioznog koda

Na razini operacijskog sustava moramo razmatrati kakav je operacijski sustav, jednokorisnički ili višekorisnički. Na temelju toga potrebno je postaviti mjere zaštite kako

nebi došlo do ne autoriziranog korištenja računala. Potrebno je definirati vlasnika ili vlasnike računala i određenog korisničkog računa te definirati njegove pristupne podatke, ovlasti, ograničenja i obaveze. Kad govorimo o operacijskim sustavim bili jednokorisnički ili višekorisnički važno je razjasniti pojmove identifikacija i autentifikacija. Identifikacija predstavlja korisničko ime, odnosno ime koje je poznato korisniku koji koristi određeni korisnički račun ali isto tako to korisničko ime javno, pa nema ograničenja i zaštite korisičkog imena. S druge strane autentifikacija predstavlja lozinku, koja je za razliku od korisničkog imena tajna i trebala bi biti poznata samo vlasniku korisničkog računa. Prilikom dodjele vlasništva nad određenom imovinom koja zahtjeva zaštitu korisničkog računa lozinkom, svaki vlasnik takvog računa dobiva unaprijed generiranu lozinku. Zadatak svakog vlasnika korisničkog računa je da tu automatski generiranu lozinku promijeni u lozinku koju će samo on znati. Osim mjere zaštite da se lozinka odmah promijeni postoji niz pravila kako definirati lozinku da bi ona bila u najvećoj mjeri sigurna od različitih vrsta napada i pokušaja probijanja lozinke. Lozinka koja služi za autentifikaciju korisnika trebala bi imati minimalno 15 znakova i to velika i mala slova, brojke, i specijalne znakove. Kako bi se poduzeće zaštitilo može provjeravati korisnički unos i postaviti ulazne gabarite koji će definirati što lozinka mora sadržavati. Na taj način se smanjuje mogućnost ljudske pogreške u definiranju prejednostavne ili jedne od standardnog oblika lozinke, koje većina programa za probijanje lozinki s lakoćom može pronaći. U višekorisničkim operacijsim sustavima postoje dvije vrste korisnika i to administrator i korisnik. Važno je poznavati ovlasti koje su dodjeljene administratoru i ovlasti koje su dodjeljene korisniku. Administrator sustava ima pravo stvaranja novih krisničkih računa ako se ukaže potreba isto tako ima pravo definiranja lozinke i promjene lozinke ukoliko se pokaže potreba. Što u pravilu znači da će pokušaj napada prvo ići na administratora jer preko administratorskog računa je moguće pristupiti svakom drugom računu. Upravo zato administrator računala mora biti osoba koja ima određena znanja i komepetencije iz područja informacijske sigurnosti, koja je savjesna i nije podložna kriminalnim radnjama.

Programske mjere zaštite na razini korisničke programske podrške mogli podjeliti na tri razine zaštite i to zaštita koja se odnosi na[13]:

- Zaporku(korisničku lozinku)
- Jednokratnu instalaciju
- Nemogućnost rada s drugog računala

Zaporka ili lozinka predstavlja autentifikaciju korisnika koji koristi određeni softwer, koji je dodjeljen tom korisniku i predstavlja njegovo vlasništvo. Autentifikacija je djelomično opisana u dijelu jednokorisničkih i višekorisničkih operacijskih sustava, dok će mo u ovom dijelu detaljno objasniti autentifikaciju i kako osigurati sigurnost lozinke. Autentifikacija je proces kojim se utvrđuje korisnički identitet onog koji ima pravo pristupa informacijskom sustavu ili pojedinom programu unutar informacijskog sustava. Postoje tri načina utvrđivanja neospornosti korisničkog identiteta i to[14]:

- Nešto što samo korisnik zna (lozinka, PIN, kriptografski ključ)
- Nešto što samo korisnik posjeduje (token, magnetska kartica, pametna kartica)
- Nešto što korisnik jest (biometrijske metode kao što su otisak prsta, skeniranje rožnice, prepoznavanje glasa...)

Jasno možemo vidjeti da je autentifikacija puno više od same lozinke i da postoje različiti mehanizmi zaštit korisničkog identiteta ali i zaštite pristupa od neovlaštenog upada. Iako postoje različite metode zaštite najrasprotranjenije je ipak još uvijek zaporka ili ti korisnička lozinka. Upravo iz toga razloga će lozinka biti detaljnije opisano kao i mehanizmi zaštite korisničke lozinke(njene jedinstvenosti, tajnosti i složenosti).

Kao što je i navedeno lozinke su danas jedan od najčešćih oblika autentifikacije korisničkog identiteta, ali zbog velike ovisnosti o ljudksoj prirodi lozinke su istovremeno i najnesigurniji način zaštite korisničkih računa i to iz više razloga. Korisnici informacijskog sustava i vlasnici određenih djelova informacijskog sustava često nisu svijesni rizika i važnosti čuvanja tajnosti lozinke pa se događaju situacije da ukoliko nisu u mogućnosti odraditi određeni zadatak nerjetko otkriju lozinku drugoj osobi kako bi ona za njih ti odradila. I drugi najveći propust vezan uz lozinke se događa kad korisnik definira „slabu“ lozinku koja se lako može pogoditi različitim mehanizimima. Najčešći napadi na informacijski sustav se događaju upravo nad lozinkama gdje se pokušavaju zaobići lozinke ili pogoditi lozinke. Zato je potrebno napraviti obratiti pažnju na sljedeće stvari[14]:

- Sve lozinke moraju biti povjerljive
- Sve lozinke se moraju čuvati u nečitljivom(kriptiranom obliku) ako se nalaze izvan adekvatno osigurane okoline

- Lozinku ne smije dijeliti više korisnika s čim se osigurava dokazivost
- Lozinku bi se trabalo mijenjati nakon određenog perioda koji se propisuje u svrhu zaštite IS-a
- Ako postoji sumnja da je integritet i povjerljivost zaporke narušena potrebno ju je mjenjati
- Potrebno je definirati oblik zaporke(broj znakova, raspon simbola...)
- Ako korisnik pogriješi više od 3 puta potrebno je zaključati taj korisnički račun zbog sumnje na napad

Preporuča se korištenje ovakve zaštite za sve zaporke koje se koriste u informacijskom sustavu, ali opet ovisno o procijeni rizika i značaju podatkovnog sadržaja koji dostupan preko određenog korisničkog računa i isplativosti postavljanja takve zaštite važno je odrediti na kojim korisničkim računima će se ovakva zaštita primjenjivati u potpunosti a na kojima će se ona primjenivati djelomično. Ukoliko ne primjenjujemo potpuno zaštitu važno je upoznati vlasnike korisničkih računa sa važnosti čuvanja povjerljivosti i integirteta lozinke i najčešćim vrstama napada na korisničke lozinke kako bi u skladu s tim sami osigurali potrebnu zaštitu i mjere sigurnosti. Neki od najčešćih napada na korisničke lozinke su[14]:

- Pokušaj pogađanja na temelju dopuštenih simbola
- Pokušaj pogađanja na temelju poznatih podataka o vlasniku
- Pokušaj neautorizirane autentifikacije pomoću standardnih zaporki koje definiraju proizvođači različite opreme i softwera
- Pokušaj neautorizirane autentifikacije zbog neadekvatne pohrane lozinke, s čime je narušena njezina povjerljivost

Osim lozinke naveli smo i druge mjere zaštite kao što su magnetske kartice, pametne kartice tokeni. Prilikom korištenja ove mjere zaštite puno je veća sigurnost da neće doći do neautoriziranog korištenja iz dva razloga:

- Za upad u sustav potrebno je imati karticu koja je u vlasništvu autoriziranog korisnika
- Uz karticu potrebno je poznavati i lozinku koja najčešće dolazi u kombinaciji s karticom

Kad govorimo o biometrijskoj zaštiti ona je najsigurnija zaštita ali izrazito skupa što predstavlja negativni aspekt. Upravo zbog visoke cijene uvođenja zaštite na biometrijskoj

razini ona se koristi samo za vlasnike onih računa i štiti ono podatke čiji je značaj od izrazite važnosti za poduzeće i gdje se procjenjuje visok rizik od gubitka takvih podataka.

Komunikacija za razliku od operacijskog sustava i korisničke programske zaštite se odvija na više razina te svako poduzeće treba razmotriti moguće razine komunikacije i donijeti mjere zaštite u odnosu na razinu. Komunikacija se odvija između dva ili više zaposlenika i to na više načina koji u velikoj mjeri ovise o odabranom komunikacijskom mediju. Komunikaciju gledamo kao razmjenu poruka između minimalno dva subjekta. Upravo zbog razmjene poruka koje mogu biti podatkovni sadržaji od velikog značaja potrebno je zaštiti komunikaciju kako sigurnost tavkih podatkovnih sadržaja nebi bila narušena, točnije kako treća strana nebi mogla pristupiti tim podatkovnim sadržajima. Napad na sigurnost poruke u komunikaciji ovisi o komunikacijskom mediju pa tako možemo govoriti o:

- Usmenoj komunikaciji
- Komunikaciji putem telefona, mobitela
- Komunikaciji putem interne mreže poduzeća
- Komunikaciji putem interneta

Važno je naglasiti da komunikacija ne predstavlja samo razgovor nego cjelokupni proces razmjene poruka. U tom kontekstu sadržaj poruke može biti razgovor(pisane poruke, usmene poruke), mogu biti dokumenti koji se razmjenjuju unutar informacijskog sustava. Zaštita komunikacije, uvođenje mjera i kontrola u komunikacij kao i kod svega ostalog ovisi procjeni rizika i procjeni podatkovnog sadržaja. Usmena komunikacija je područje koje je izrazito teško zaštiti i u kojem podaci mogu biti otkriveni namjerno, ili pak slučajno kroz nesmotrenost i ne obraćenje pažnje kome se ti podaci povjeravaju ili tko „prisluškuje razgovor“. Najvažniji aspekt zaštite u usmenoj komunikaciji je prilikom donošenja važnih odluka, i u komunikaciji prema dolje[15], odnosno od menadžmenta prema zaposlenicima, gdje je važno staviti naglasak na pozornost menadžmenta da ne otkriva informacije koje bi se kasnije mogle zlorabiti. Kad govorimo o drugim medijima za komunikaciju lakše je osigurati i zaštiti podatke u komunikaciji jer podaci u takvoj komunikaciji ne ovise samo o ljudskom faktoru već se može pomoću određenih mehanizama zaštite spriječitio otkrivanje podatkovnog sadržaja osobama koje nisu ovlaštene da imaju pristup tim sadržajima. Jedan najpopularnijih načina zaštite komunikacije je kriptiranje poruka. Kriptiranje će biti detaljno obrađeno kasnije u ovo radu a za sad je dovoljno reći da kriptiranje predstavlja postupak zaštite poruka na način da ona bude čitljiva samo onom korisniku kojem je i namjenjena.

Jedna od programskih mjera zaštite je i dupliciranje sadržaja na drugim materijalnim nositeljima[13]. U dijelu u kojem su opisani materijalni nositelji podataka je djelomično objašnjeno kako se s pojedinih materijalnih nositelja podaci mogu prebacivati na druge materijalne nositelja. Ovdje će biti opisana važnost dupliciranja sadržaja ovisno o vremenu čuvanja određenog podatkovnog sadžaja i važnosti podatkovnog sadržaja. Već prije je napomenuto da različiti materijalni nositelji predstavljaju različite rizike kod pohranjivanja podatkovnog sadržaja. Kako bi se spriječio gubitak podatkovnog sadržaja potrebno je taj sadržaj duplicirati na više materijalnih nositelja, osobito ako se radi o podatkovnom sadržaju koji će biti pohranjen i kao takav čuvan na duže vremensko razdoblje. Svrha dupliciranja nije samo pohrana podataka na različite materijalne nositelje da se podaci zaštite od propadanja već i to da se u slučaju gubitka određenih podatka tim podacima može pristupiti preko drugih izvora. Dupliciranje podataka je samo dio rješenja jer u slučaju velikog oštećenja sustava, ako su podaci pospremljeni na istoj lokaciji, može doći do gubitka podataka bez obzira na materijalni nositelj na kojem su podaci sačuvani. Potpuno rješenje leži u backupiranju podataka. Backup predstavlja postupak dupliciranja podataka i njihovu fizičku dislokaciju[2] kako bi se omogućio pristup podacima u uvijetima kad su podaci na prvotnoj lokaciji u potpunosti ili djelomično oštećeni ili uništeni. Ovisno o izboru materijalnog nositelja ovisi i vrsta zaštite ali i način dupliciranja. Ako su postojeći podaci na papiru oni se mogu pretipkavanje unijeti u računalo i pospremiti na tvrdi disk ili optički disk, ili se mogu slikanjem sličica pospremiti na mikrofilm koji kako je navedeno ranije ima najbolje mehanička i kemijska svojstva i pogodan je za čuvanje podataka na dulji vremenski period[2].

Maliciozni kod predstavlja programe koje su napisani s cilje oštećenja, izmjena dokumenata, prisluškivanja razgovora, i ostalih radnji koje mogu utjecati na poslovanje poduzeća. Maliciozni kod će detaljnije biti opisan na kraju knjige kao i mjere zaštite o malicioznog koda. Za sad je bitno prepoznati da zaštita od malicioznog koda spada u programske mjere zaštite koje predviđaju određenu programsku zaštitu na razini antivirusnih programa, postavljanja firewall-a, antispywera i drugih razina programske zaštite.

Mjere zaštite iz ISO 27002 koje spadaju u programske mjere zaštite:-

1. Upravljanje komunikacijama i operacijama
2. Kontrola pristupa
3. Nabava, razvoj i održavanje informacijskih sustava

Ove mjere zaštite iz ISO norme sadrže niz kontrola koje su opisane u poglavlju ISO 27002 norma ove knjige, i dat je detaljan opis kako implementirati koju normu u ISMS. Naravno ovako gledano ovo je dosta gruba podjela iz ISO 27002, ali u ovoj knjizi već je više puta napravljen osvrt na kontrole iz norme i nema se potrebe ponavljati. Potrebno je reći da ova tri područja zaštite spadaju u programske mjere zaštite, ali ne samo isključivo u programske mjere zaštite, jer dijelovi odgovaraju i drugim mjerama zaštite.

4.1.3. Fizičke i tehničke mjere zaštite

Fizičke i tehničke mjere zaštite predstavljaju fizička odnosno tehnička rješenja s kojima se ograničava pristup neautoriziranom osoblju u prostorije s informacijskom opremom, u prostorije s povjerljivim podacima, ali i sve druge prostorije za koje postoji ograničenje pristupa na razini vlasnika[2]. Ciljevi fizičke mjere zaštite su povezani sa zaštitom fizičke imovine i to[13]:

- Objekta u kojem je smješten IS
- Osoba uposlenika i gostiju za vrijeme boravka uobjektu
- Računalne opreme
- Magnetskih nosioca podataka

Na način da[13]:

- Odvrate potencijalne provalnike s pokazivanjem jasnih barijera koje su postavljene kako bi se zaštitila imovina
- Otežavanje prodora onima koji se ipak odluče na pokušaj provale, te zadržavanje provalnika na svakoj barijeri što dulji vremenski period
- Otkrivanje ili dojava pokušaja ili proboja kroz barijere
- Odgovor u obliku raznih obrambenih aktivnosti koje trebaju zaštiti imovinu i spriječiti ostvarivanje ciljeva provalnika

Fizičke mjere obrane su primjerice postavljanje rampe na ulazu u poduzeće, zaštitar na ulazu koji provjerava i propušta samo one koji imaju pravo pristupa određenom objekti ili prostorijama unutar objekta. Neprobojno staklo, debeli zidovi i vrata koji odvajaju prostorije s povjerljivim podacima, opremom. Različite vrste sefova koji onemogućuju krađu podataka. Alarmni sustavi i sustavi automatskog zaključavanja prostorija u slučaju uključivanja alarma. Ima mnogo primjera fizičkih mjera zaštite, ali i one kao i sve drugo ovise o cijenovnoj isplativosti i procijenjenoj vrijednosti rizika i razini prijetnji.

Tehničke mjere zaštite kao i fizičke pretpostavljaju zaštitu od provale i provalnika, s razlikom da tehničke mjere zaštite predviđaju tehnička rješenja kako bi se spriječio ulazak neautoriziranog korisnika u dijelove gdje se nalazi oprema bitna za funkcioniranje informacijskog sustava te informacije koje su pohranjene na određenim materijanim nositeljima podataka. Prema tome tehničke mjere zaštite bi mogli podjeliti na[13]:

- elektroničke mjere zaštite
- zaštita od elektro-magnetskog zračenja
- protupožarna i protupoplavna zaštita

Elektroničke mjere zaštite mogu biti[17]:

- Detekcija pokreta(primjer):
  - Passive infrared
  - Ultrasonic
  - Microwave
  - Laser
  - Mikrovalne ograde
  - Sezmički
  - Tomographic / Radio network
- Video nadzor(primjer):
  - CCTV
  - IR Iluminacija
  - Thermal
- Tehnička zaštita(primjer):
  - CO senzori
  - Dim
  - Toplina
- Alarm(primjer):
  - Magnetski prekidači
  - Glass break senzori
  - HF/RF polja
  - Taut wire / Tripwire senzori za ograde
- Brave(primjer):
  - Cilindar
  - Dimple

- Biaxial
- Sefovi
- Elektronički – PIN
- Ključ
- Rotacija
- Glass relocker
- HSS-CO / Thermal Lance

U ovoj podjeli možemo s lakoćom vidjeti široku lepezu proizvoda koji su proizvedeni s ciljem tehničke zaštite ali i jedan dio mjera koje se mogu implemetirati kao dio tehničke zaštite. Mjere iz ISO normi su opisane ranije pa se s njima nećemo posebno sad baviti.

Zaštita od elektromagnetsko polja potrebna je iz dva razloga, prvi razlog je očuvanje zdravlja pojedinaca koji su prisutni u okruženju gdje postoji elektromagnetsko zračenje, a drugi razlog je zaštita podataka na magnetskim diskovima koji se usred dijelovanja jakog elektro magnetskog polja mogu promijeniti i kasnije biti nečitljivi ili nepotpuni. Danas postoji razvijeni cijeli niz proizvoda koji omogućuju izolaciju od elektromagnetskog polja ali i niz mjerenja koja mogu pokazati koliko je jako elektromagnetsko polje i njegov učinak na magnetske diskove. Ukoliko se procjenom rizika pokaže da je potrebno zaštiti određene dijelove IS-a kako nebi došlo do gubitka podataka, takvi dijelovi se trebaju izolirati s ciljem smanjenja učinka elektromagnetskog polja, ili ukoliko se pokaže da je djelovanje elektromagnetskog polja izrazito jako treba se pokušati pronaći izvor tog polja i smanjiti djelovanje izvora s ciljem smanjenja jakosti elektromagnetskog polja.

Protupožarna zaštita predviđa poduzimanje mjera s ciljem otklanjanja mogućnosti pojavljivanja požara ili ukoliko dođe do požara smanjenje učinka požara na informacijski sustav. Postoji niz rješenja za protupožarnu zaštitu a ta rješenja se mogu primjenjivati prilikom izgradnje objekta s ciljem smanjenja mogućnosti pojavljivanja i povećanja otpornosti na požar i naknadno sa postavljanjem protupožarnih aparata, prskalica i ostalih proptupožarnih mjera. Jedna od prednosti je da se od požara može osigurati kod većine osiguravajućih kuća i na taj način se osigurati od nastale štete, ono što je bitno za napraviti kao predradnju je osigurati da su podaci backupirani i da ukoliko nastane šteta od požara se može bez velikih poteškoća nastaviti s poslovanjem.

Područja mjere zaštite iz ISO 27002 norme:

1. Fizička sigurnost i sigurnost okruženja

a. Sigurnost opreme
b. Osigurana područja

Ovo je područje fizičke mjere zaštite koje se može pronaći u ISO 27002 normi, dok područje tehničkih mjera zaštite odgovara:

1. Fizička sigurnost i sigurnost okruženja
2. Kontrola pristupa

4.1.4. Organizacijske mjere zaštite

Organizacijske mjere zaštite predstavljaju mjere zaštite koje imaju za cilj organizacijsku sigurnost koju možemo podjeliti na[13]:

- Infrastruktura informacijske sigurnosti
  - Tim za upravljanje informacijskom sigurnošću
  - Koordinacija rada informacijske sigurnosti
  - Dodjela odgovornosti za informacijsku sigurnost
  - Proces autorizacije organizacijskih cjelina koje sudjeluju u obradi
  - Savjeti specijalista o informacijskoj sigurnosti
  - Suradnja između organizacija
  - Neovisni pregledi efikasnosti informacijske sigurnosti
- Sigurnost pristupa treće zainteresirane strane
  - Identifikacija rizika kod pristupa trećih strana
  - Sigurnosni zahtjevi u ugovorima s trećim stranama
- Outsorsing

Potrebno je utvrditi skupinu managera koji će inicirati i kontrolirati implementaciju informacijske sigurnosti u organizaciji. Potrebno je formirati i odgovarajući tim pod vodstvom managementa, koji će odobriti politiku o sigurnosti informacija, dodjeljivati sigurnosne uloge i koordinirati implementaciju sigurnosti kroz cijelu organizaciju. Ako je potrebno, u organizaciji treba organizirati grupu specijalista za savjetovanje o informacijskoj sigurnosti. Treba i održavati veze s vanjskim specijalistima za sigurnost, kako bi se išlo u korak sa trendovima, pratilo standarde i metode procjene, te kako bi se uspostavila suradnja za slučajeve kada dođe do sigurnosnih incidenata. Nadalje, treba poticati multidisciplinarni pristup sigurnosti informacija, npr. poticanjem suradnje managera, korisnika, administratora, dizajnera

aplikacija, auditora, osoblja za sigurnost i stručnjaka u područjima poput osiguranja i upravljanja rizikom[13]. Organizacijske mjere zaštite propisuju dokumente, ovlasti, ponašanje i ugovorne obaveze treće strane, a razvijaju se prilikom izgradnje, implementacije i održavanja sustava sigurnosti u poduzeću. Postavlja se pitanje zašto riskirati i uključiti treću stranu u proces izgradnje, implementacije i praćenja sustava sigurnosti, ako njihovim ne uključivanjem izbjegavamo rizik. Odgovor leži u tome da velik broj poduzeća nema adekvatne stručnjake iz područja sigurnosti informacijskog sustava i upravo zbog toga se javlja potreba angažiranja stručnjaka iz vana, kako bi se proces implementacije ISMS-a proveo na najbolji mogući način. Uvođenje ISMS-a se može provoditi na 3 načina[2]:

- Sve sami(posao odrađuju naši stručnjaci)
- Sve drugi(posao je u potpunosti povjeren trećoj strani)
- Kombinirano(naši stručnjaci i treća strana surađuju na izgradnji ISMS)

Kad govorimo o organizacijskim mjerama zaštite važno je objasniti dio oko uvođenja ISMS-a u poslovanja i načinima uvođenja te prednostima i nedostatcima određenog načina. Ako posao odrađujemo u potpunosti sami trebamo biti svijesni kakav tim stručnjaka imamo i ukoliko će oni odraditi posao hoće li odraditi posao dobro. Ukoliko radi samo treća strana važno je ugovorno dobro definirati obaveze koje ima treća strana ali i ograničenja. Tu se javlja problem komunikacije, jer treća strana ne poznaje naš poslovni niti informacijski sustav u potpunosti pa dolazi do problema prikupljanja podataka. Najbolja opcija je da se posao odrađuju u suradnji vlastitih stručnjaka i treće strane, gdje treća strana ima kompetencije u izgradnji jednog takvog sustava a vlastiti stručnjaci dobro poznaju cjelokupni sustav i mogu u svakom trenutku treću stranu upoznati sa potrebitim informacijama.

Outsorsing predstavlja zaštitu podataka kad je njihova obrada i korištenje dodjeljeni nekoj trećoj strani. Kako bi smanjili rizik disperzije podataka, važno je ugovorno odrediti način na koji treće strana smije postupati s ustupljenim podacima. Dogovori oko outsorsinga trebaju uključiti u ugovor rizike, kontrlonemehanizme i sigurnosne postpuke za informacijske sustave te mrežna i/ili stolna okruženja[13].

Prema ISO normi 27002 zaštitne mjere koje spadaju u organizacijske zaštitne mjere su:

1. Procjena i obrada rizika
2. Politika sigurnosti
3. Organizacija informacijske sigurnosti
4. Upravljanje imovinom

5. Sigurnost ljudskog potencijala
6. Upravljanje sigurnosnim incidentom
7. Upravljanje kontinuitetom poslovanja

4.1.5. Pravni aspekt zaštite

Pravni aspekt zaštite predviđa da je sustav sigurnost IS u poduzeću potrebno uskladiti sa zakonima i pravnim politikama poduzeća. Ovakav način nam omogućava pravno terećenje osoba koje se zlorabile informacije te kazneni postupak protiv njih. Pravni aspekt zaštite nam uvelike pomaže da ukoliko dođe do ispada jednog dijela sustava prema zakonima i pravnim politikama poduzeća možemo tražiti krivca i ne odgovarati pred zakonom zbog pogreške jednog ili više pojedinaca u poduzeću.

Pravni aspekt zaštite u ISO normi 27002 možemo naći u području:

1. Sukladnost

5. Zaštitne mjere

Prilikom opisivanja mjera za smanjenje rizika govorili smo o programiskim mjerama, fizičkim, tehničkim i organizacijskim mjerama, ali nismo opisali što su to mjere i što one znače, di naći pomoć za primjenu tih mjera, kako implementirati mjere. Zaštitne mjere su mjere koje se poduzimaju s ciljem smanjenja ili uklanjanja rizika. One nam omogućuju:

- Zaštitu resursa
- Smanjenje ranjivosti
- Ograničavanje učinka neželjenih događaja
- Otkrivanje neželjenih događaja
- Oporavak od incidenta

Zaštitne mjere su kroz godine proučavanja rizika i ranjivosti svedene u različite norme koje se bave područjem informacijske sigurnosti. Danas zasigurno najznačajnija norma koja donosi popis mjera i kontrola za smanjenje rizika je ISO 27001 norma. ISO 27001 predstavlja popis mjera i kontrola koje mogu biti uvedene u poduzeće s ciljem smanjenja rizik, a istovremeno omogućava certifikaciju ukoliko je na temelju rizika koji se pojavljuju u poslovanju poduzeća prema mjerama i kontrolama koje su propisane u normi izgrađen sustav sigurnost. Kako bi se u što većoj mjeri smanjila mogućnost pogreške u implementaciji mjera iz norme ISO 27001

napravljena je ISO 27002 norma koja govori o najboljoj praksi prilikom implementacije mjera iz norme ISO 27001. Obje norme su detaljno opisane u prvom dijelu knjige i zato se nećemo posebno baviti mjerama i kontrolama te implementacijom mjera i kontrola koje bi do sad trebale biti poznate čitatelju, nego ćemo napraviti kratak osvrt koraka koje ISO 27001 nudi te dio dokumenata koje propisuje.

5.1. Koraci u smanjenju rizika prema ISO 27001

Kako smo već i prije naveli ISO 27001 norma nudi korak kako organizirati i uvesti sustav za upravljanje informacijskom sigurnošću(ISMS). Koraci[2]:

1. Definirati politiku sigurnosti(Rješenje uprave o razvoju sustava sigurnosti i njegovo financiranje, dokument o granicama koje obuhvaća ISMS)
    a. Krovni dokument(predstavlja upute)
    b. Operativna razina(daje način realizacije kontrola, što se smije, a što se nesmije te što se preporuča)
2. Procjena rizika
    a. Identifikacija informacijske imovine i dojdela vlasništva
    b. Procjena značaja podatkovnog sadržaja
    c. Procjena oblika i učetalosti prijetnji
    d. Izračun rizika(kvalitativni, kvantitativni, kombinirani)
3. Postupanje s rizikom
    a. Odluka uprave o prihvaćanju i primjeni ISMS-a
    b. Dokument o prihvaćanju rezidualnog rizika
4. Dopuna sustava sigurnosti
5. Certifikacija
    a. Priprema za certifikaciju
    b. Certifikacija

Ovdje je prikazan najkraći mogući popis koraka koje nudi ISO 27001 norma, te na temelju tog popisa koraka se jasno može vidjeti smjer koji se želi postići kako bi se smanjili rizici. Posebno interesantan je zadnji korak a to je certifikacija. Certifikacija predstavlja dobivanje certifikata za uspješno implementiran sustav sigurnosti po normi ISO 27001. Posjedovanje ovakvog certifikata omoguću poduzeću lakšu suradnju s drugim poduzećima koja posjeduju certifikat i koja su uspješno implementirala sustav sigurnosti IS-a u svoje poslovanje. Ovaj certifikat jamči razvijen sustav sigurnost i otvara nove mogućnosti povezivanja različith

poduzeća. Ukoliko ne posjedujemo takav certifikat to nemora značiti mnogo ali znači manju mogućnost povezivanja sa stranim poduzećima koja posjeduju certifikat jer takva poduzeća neće riskirati povezivanje sa „nesigurnim“ poduzećem koje ne posjeduje formalni dokaz da je uspješno implementiran sustav sigurnosti. Sam postupak certifikacije je dosta skup i zato je potrebna priprema za certifikaciju odnosno poželjno je da se pozove treća strana koja će analizirati sustav i predložiti promjene ili nas usmjeriti na certifikaciju.

5.2. Dokumentacija u ISO 27001

Dokumentacija može sadržavati samo jedan dokument (tzv. ISMS manual) ili skup dokumenata koji najčešće imaju određenu hijerarhiju (krovna politika, organizacijske/procesne politike, standardi, procedure). ISO 27001:2005 u pogledu dokumentacije izričito zahtjeva nekoliko dokumenata/poglavlja[17]

- ISMS politiku,
- Opseg ISMS-a,
- Procedure i kontrole koje podupiru ISMS,
- Opis metodologije procjene rizika,
- Izvještaj procjene rizika,
- Plan obrade rizika,
- Dokumentirane procedure za učinkovito planiranje, rad i kontrolu ISMS-a,
- Zapise i
- Izjavu o primjenjivosti (eng. *Statement of Applicability*)

Ova dokumentacija pruža uvid u to kako organizacija radi, kakva je organizacijska struktura, koji su joj ključni poslovni procesi, detaljnost kojom se pristupa ISMS-u i sl.

6. Literatura

[1] Ines Sutić, Ekonomski fakultet, Zagreb, 2013, Sustav upravljanja poslovnim rizicima ISO 31000, http://web.efzg.hr/dok/TRG/isutic/Upravljanje%20poslovnim%20rizicima_ISO-31000.pdf Dostupno, 27.12.2013.

[2] Željko Hutinski, Fakultet organizacije i informatike, Varaždin, 2013, Sigurnost informacijskih sustava: Predavanja.

[3] Fakultet elektronike i računarstva, Zagreb, 2013, Metodologija procjene rizika , Dostupno, http://www.fer.unizg.hr/_download/repository/Metodologija_procjene_rizika.pdf 27.12.2013.

[4] Suzana Stojaković-Čelustka, Hrvatska banka za obnovu i razvoj, Zagreb, 2013, Osnove upravljanja rizikom informacijskog sustava, Dostupno, http://www.cis.hr/files/Celuska-Osnove_upravljanja_rizikom.pdf , 27.12.2013.

[5] Hrvatska narodna banka, Zagreb, 2006, Smjernice za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika, Dostupno http://www.hnb.hr/supervizija/h-smjernice-za-upravljanje-informacijskim-sustavom.pdf 28.12.2013.

[6] Karmen Klarin, Fakultet elektrotehnike i računarstva, Zagreb, 2008, Upravljanje rizicima, Dostupno, http://www.zpr.fer.hr/zpr/Portals/0/Predmeti/UIS/Upravljanje%20rizicima.pdf 28.12.2013.

[7] Dalibor Uremović, alterinfo, Split, 2012, Rizici virtualnih okruženja, Dostupno, http://www.alterinfo.hr/userfiles/Media/Rizici%20virtualnih%20okruzenja%20-%20Mreza%2005%202012.pdf 28.12.2013.

[8] Raska Točagić, Univerzitet u Tuzli, Tuzla, 2011, Upravljanje rizicima: Izbjegavanje rizika, Dostupno http://upravljanjerizicima.com/izbjegavanje-rizika/2.4.1 30.12.2013.

[9] Raska Točagić, Univerzitet u Tuzli, Tuzla, 2011, Upravljanje rizicima: Transfer rizika, Dostupno http://upravljanjerizicima.com/izbjegavanje-rizika/2.4.1#!/transfer-rizika/2.4.2 30.12.2013. 30.12.2013.

[10] Raska Točagić, Univerzitet u Tuzli, Tuzla, 2011, Upravljanje rizicima: Transfer rizika na neosiguravajuća društva, Dostupno http://upravljanjerizicima.com/izbjegavanje-rizika/2.4.1#!/osiguranje/2.4.2.1 30.12.2013.

[11] Šantalab, Vitez, Zjakić, Fakultet organizacije i informatike, Varaždin, 2011, ISO 27005 Upravljanje rizicima, Dostupno http://security.foi.hr/wiki/index.php/ISO_27005_-_Upravljanje_rizicima#VIII._Prihva.C4.87anje_rizika_informacijske_sigurnosti 2.1.2014.

[12] Željko Hutinski, Fakultet organizacije i informatike, Varaždin, 1991, Journal of information organizational science, Metodologija izrade modela generiranja karakteristika dokumentacije,
Dostupno http://hrcak.srce.hr/index.php?show=clanak&id_clanak_jezik=118833 3.1.2014.

[13]Željko Hutinski, Fakultet organizacije i informatike, Varaždin, 2010, Sigurnost informacijskih sustava, Dostupno http://www.scribd.com/doc/17094401/Sigurnost-informacijskih-sustava 3.1.2014.

[14]Hrvatska narona banka, HNB, 2006, Smjernice za upravljanjem informacijskim sustavom u cilju smanjenja operativnog rizika, Dostupno http://www.hnb.hr/supervizija/h-smjernice-za-upravljanje-informacijskim-sustavom.pdf 3.1.2014.

[15] Kenan Sapho, Kvalis, 2012, Komunikacija kao način upravljanja u kompaniji, Dostupno http://www.kvalis.com/o-portalu/item/693-komunikacija-kao-na%C4%8Din-upravljanja-u-kompaniji 3.1.2014

[16] Fakultet organizacije i informatike, FOI, Varaždin 2012, Sis wiki: Tehničke mjere zaštite,
Dostupno,http://security.foi.hr/wiki/index.php/Tehni%C4%8Dke_mjere_za%C5%A1tite 3.1.2

[17] Dalibor Uremović, Fakultet organizacije i informatike, Varaždin, 2008, Revizija (audit) sustava upravljanja informacijskom sigurnošću prema normi ISO/IEC 27001:2005

[18] ISO/IEC 27002: 2005