

PLAN INFORMACIJSKE SIGURNOSTI PODUZEĆA

1. UVOD

Vojni zapovjednici i vladari odavno su uočili važnost zaštite informacija o njihovim vojnim kapacitetima, sposobnostima, broju vojnika i njihovim pokretima. Ukoliko bi takve informacije pale u ruke neprijatelja, posljedice bi mogle biti katastrofalne. U današnje doba, vlade, vojska, finansijske institucije, bolnice i privatna poduzeća prikupljaju velike količine povjerljivih informacija o svojim zaposlenicima, komitentima, proizvodima, istraživanjima i finansijskoj poziciji. Većina takvih informacija se pribavlja, obrađuje i sprema u računalnim sustavima i prenosi mrežom do drugih računala.

U slučaju povrede povjerljivosti takvih informacija moglo bi doći do propuštene dobiti, tužbi ili čak bankrota poduzeća. Zaštita povjerljivih informacija je osnovni zahtjev poslovnog svijeta današnjice a u mnogim slučajevima i zakonska obveza. Za pojedince zaštita informacija ima značajan utjecaj na privatnost na koju se različito gleda u različitim kulturama.

Svako poduzeće trebalo bi imati funkcionalne makar osnovne elemente podsustava za zaštitu informacijskih sustava koji bi trebao biti implementiran u okviru informacijskog sustava tvrtke. Jači naglasak treba biti stavljen na organizacijske i proceduralne čimbenike informacijske sigurnosti nego na tehničke čimbenike. Razlog ovakvome pristupu je činjenica da se najčešće podcjenjuju organizacijski i ljudski čimbenici sigurnosti nauštrb tehničkom aspektu, što u praksi često rezultira manjkavostima i neadekvatnim sustavima zaštite informacijskih sustava.

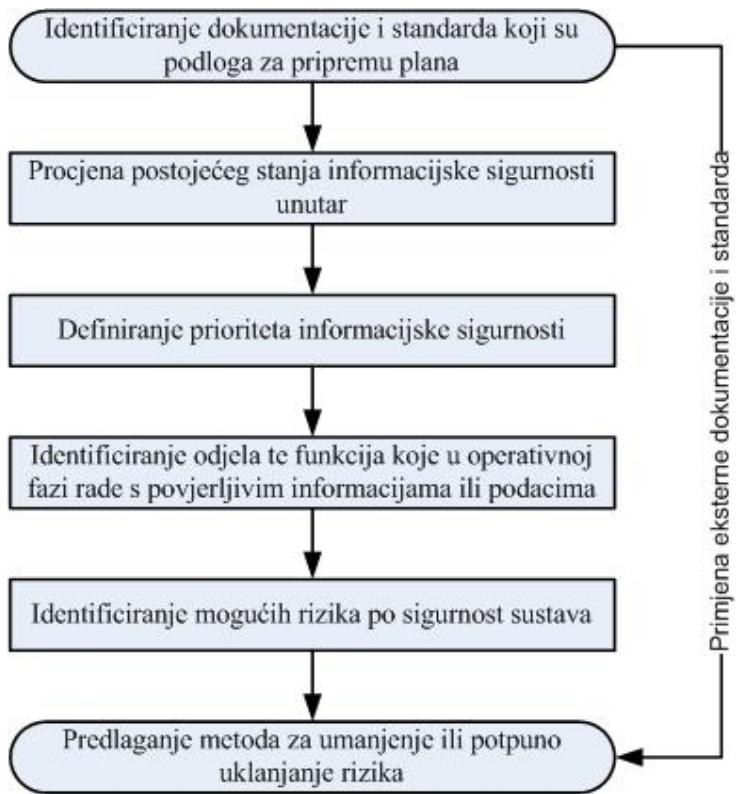
2. PLAN INFORMACIJSKE SIGURNOSTI

U današnje doba nužno je da uprava poduzeća prepozna važnost upravljanja informacijskom sigurnosti kao odlučujućim čimbenikom odvijanja poslovne aktivnosti. U tom smislu, nužno je producirati niz dokumenata koji će na jasan način definirati generalne kriterije, uloge, rizike, funkcije te odgovornosti za osiguranje sigurnosti informacija i podataka koji se prikupljaju i obrađuju tijekom odvijanja poslovne aktivnosti. Kako bi uprava poduzeća mogla ispuniti ove zadaće, moraju se primijeniti razne sigurnosne procedure koje će zaštititi povjerljivost podataka i informacija i na taj način pridonijeti kontinuitetu odvijanja poslovne aktivnosti.

Osnovni dokument koji definira kritične čimbenike upravljanja informacijskom sigurnošću naziva se Plan informacijske sigurnosti. Taj plan mora biti prilagođen organizaciji na koju se primjenjuje i stoga može posjedovati različite razine kompleksnosti. U okviru njega se istražuju rizici koji se mogu pojaviti a imaju utjecaj na poslovni sustav te predložiti određene akcije koje se mogu poduzeti kako bi se oni minimizirali ili u potpunosti izbjegli. Plan informacijske sigurnosti razvija se u skladu s internom dokumentacijom organizacije ili poduzeća koja je identificirana kao osnova za pripremu Plana i relevantna je za odvijanje poslovnih procesa. Temeljno upravljanje informacijskom sigurnošću definirano je standardom ISO 17799.

Koraci koje treba poduzeti kod pripreme Plana informacijske sigurnosti prikazani su na sljedećem dijagramu.

Dijagram: Koraci pripreme plana informacijske sigurnosti



Izvor: izradio autor

2.1 Privatnost, povjerljivost i sigurnost informacija

Privatnost podataka je sposobnost zaposlenika ili odgovornog za određeni poslovni proces da kontrolira uporabu i širenje informacija koje se odnose na njega ili poslovni poduhvat.

Povjerljivost čini skup alata koji se primjenjuju za zaštitu privatnosti. Osjetljivim informacijama se dodjeljuje status povjerljivosti koji za sobom povlači specifične kontrole, uključujući striktna ograničenja pristupa i otkrivanja podataka. Te kontrole moraju poštivati svi oni koji se koriste takvim informacijama. Sigurnost u biti predstavlja sve moguće implementirane zaštite u klasičnim i kompjutorskim informacijskim sustavima. Ona štiti i sistem i informacije sadržane u njemu od neovlaštenog pristupa, slučajnog oštećenja ili korištenja na nedozvoljen način.

Svi uključeni u korištenje informacija moraju održati povjerljivost informacija koje su im povjerene, osim ukoliko je odavanje informacija odobreno od strane relevantnog tijela, odnosno Uprave, ukoliko je to predloženo od strane identificiranih ključnih korisnika ili ako to zahtijevaju lokalni zakoni i propisi. Povjerljive informacije uključuju sve privatne informacije koje bi mogle biti od koristi konkurenциji ili štetne po organizaciju koja ih štiti. One također uključuju informacije koje dobavljači, komitenti, zaposlenici i eventualne treće strane u poslovnom odnosu povjeravaju organizaciji koja podatke štiti. Obaveza zaštite povjerljivih informacija mora se definirati i unutar ugovora o radu koji potpisuje svaki zaposlenik.

2.2 Pravila dobrog ponašanja

Poslovni podaci i komunikacije mogu postati i javni pod već navedenim uvjetima, stoga u kolokvijalnoj, ali i pisanoj komunikaciji treba izbjegavati pretjerivanje, ponižavajuće primjedbe, prepostavljanje te neprimjerene karakterizacije ljudi i događaja koje bi se mogle krivo shvatiti. Ovo se jednako odnosi na elektroničku poštu, internu dokumentaciju, memorandume, kao i na formalne izvještaje i dokumente.

2.3 „Need to know“ princip

Poslovne organizacije, osobito one koje rade sa inovativnim tehnologijama ili su znanstveno intenzivne, često koriste osjetljive informacije. Ovaj princip se često koristi kako bi se osigurale takve informacije. On je vrlo jednostavan a temelji se na činjenici da čak i ako netko posjeduje sva službena odobrenja za pristup određenim informacijama poput pisane dozvole, pristup takvim informacijama se ne daje osim ako te osobe nemaju potrebu znati ih, odnosno ako je potrebno da ih znaju za vršenje službene dužnosti, odnosno za izvođenje određene faze poslovnog procesa.¹ Ova strategija pokušava zapravo odvratiti zaposlenike od toga da pregledavaju osjetljivi materijal ograničavajući pristup na najmanji mogući broj ljudi.

U praksi, sustav kontrole pristupa operativnim i dokumentacijskim sustavima može se koristiti za provođenje ovog principa. Vlasnik određene informacije ili dokumenta može odrediti da li druga osoba treba imati pristup njima. Taj princip u pravilu se primjenjuje paralelno s obveznim sustavima kontrole pristupa u kojima bi nedostatak službenog odobrenja mogao apsolutno zabraniti osobi pristup informacijama. Ovakva ugrađena kontrola u sebi sadrži element subjektivnosti.

Kao i kod većine sigurnosnih mehanizama, cilj je otežati neautoriziran pristup informacijama bez otežavanja legitimnog pristupa. U nekim situacijama poput analize informacija ili istraživanja, ovaj princip može se pokazati problematičnim jer je teško odrediti da li određena osoba treba imati pristup nekoj informaciji sve dok se informaciji ne pristupi i ne napravi se procjena.

Osnovna zamjerka ovom sustavu je da se može zlorabiti od strane onih koji žele odbiti drugima pristup informacijama nastojeći da povećaju svoju osobnu moć ili spriječe neželjeni pristup njihovom radu. Stoga primjena ovog principa mora promovirati duh pozitivne suradnje a ne samo čuvati privatnost podataka.

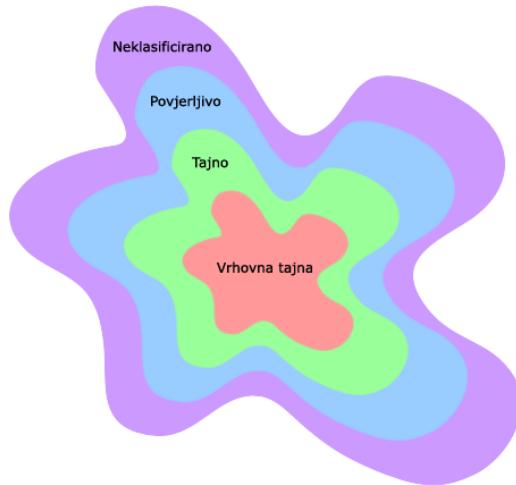
2.4 Nivoi diskrecije

Ukoliko je potrebno, ključni korisnici unutar organizacije mogu interno uvesti Bell-LaPadula² model višestupnjevane sigurnosti kako bi se formalizirali nivoi diskrecije. Ovaj jednostavni model je formalni prijelazni model koji opisuje set pristupnih pravila koja se koriste pri označavanju dokumenata i informacija, počevši od najosjetljivijih do najmanje osjetljivih. Način na koji se informacije mogu označavati može biti prilagođen organizaciji koja ga koristi.

¹ http://www.bcbst.com/code/code_confident.htm (03.06.2007)

² http://en.wikipedia.org/wiki/Bell-La_Padula_security_model (03.06.2007)

Slika: Nivoi povjerljivosti informacija



Izvor: izradio autor

Označavanje dokumenata i informacija može dodatno poboljšati način na koji se obrađuju povjerljivi podaci. Ovakve oznake mogu se koristiti i unutar sustava elektronske razmjene podataka te sustava elektronske pošte.

3. RIZIK

Rizik je koncept koji opisuje potencijalno negativan utjecaj na poslovanje poduzeća ili neku karakteristiku vrijednosti koja može proizaći iz nekog postojećeg procesa ili budućeg događaja. U svakodnevnoj uporabi, termin rizik se često koristi simultano s mogućnošću poznatog gubitka. Prema tome, rizik je u direktnoj povezanosti s ljudskim očekivanjima. Kod profesionalne procjene rizika, on kombinira vjerojatnost nastanka događaja te koliki je utjecaj tog događaja na poslovanje poduzeća. Vrlo često u poslovnom kontekstu rizik se može izraziti novčano, dakle bilo kao direktni dodani trošak ili propuštena dobit.

Glavni cilj procjene rizika nije samo identificirati sve potencijalne rizike i prijetnje podacima i sigurnosti informacija nego i stvoriti bazu za konstantno poboljšavanje Plana informacijske sigurnosti s obzirom na najnovije rizike i prijetnje koje proizlaze iz operativnih potreba i činjenice da su informacijski sustavi dinamični te se stalno razvijaju. Po definiciji takav plan nikada nije posve primjenjen pošto se mora stalno dopunjavati.

Identificiranje rizika podrazumijeva predviđanje razumnih i predvidivih vanjskih i unutrašnjih opasnosti po informacijski sustav i integritet povjerljivih podataka koji bi mogli rezultirati u slučajnom i neautoriziranom otkrivanju, zlouporabi, promjeni, uništenju ili drugačijem načinu kompromitiranja takvih informacija.

Sve moguće rizike je izrazito teško identificirati. Pošto je rast tehnologije dinamičan a ne statičan, stalno se pojavljuju novi rizici koje u trenutku klasifikacije vjerojatno nije niti moguće obuhvatiti. Zbog pojave novih rizika i tehnologija za njihovo umanjenje, metodologiju identifikacije i obrade rizika treba stalno iznova provjeravati u periodičkim intervalima kako bi se na vrijeme prepoznali i uklonili novi rizici ili makar smanjio njihov utjecaj.

Neki najčešći rizici od kompromitiranja podataka i informacija unutar informacijskog sustava su sljedeći:

- Pristup povjerljivim informacijama od strane neovlaštene osobe
- Kompromitiranje sistemske sigurnosti kao rezultat pristupa od strane „hakera“
- Presretanje podataka tijekom transakcije
- Gubitak podataka ili povjerljivosti informacija zbog greške korisnika
- Fizički gubitak podataka uslijed katastrofe
- Nekompletност i nedokumentiranost transakcije
- Neautorizirani pristup povjerljivim informacijama od strane zaposlenika
- Neautorizirani zahtjev telefonom ili emailom za povjerljivim informacijama („phishing“)
- Neautorizirani pristup preko papirnih dokumenata i izvještaja
- Neautorizirani transfer povjerljivih informacija preko treće strane

4. KONTROLA I UPRAVLJANJE RIZIKOM

4.1 Prikupljanje informacija

Povjerljive informacije se ne prikupljaju ukoliko to nije nužno potrebno i relevantno za svrhu za koju se prikupljaju. Ukoliko je moguće, one se moraju prikupljati direktno od izvora informacija a ne iz drugih izvora. U slučaju da to nije moguće, mora se voditi evidencija o tome iz kojih izvora je dobijena povjerljiva informacija. Bitno je istaknuti da se takve informacije ne smiju prikupljati bez izričite dozvole rukovoditelja odgovarajućih odjela unutar poduzeća. U svakom slučaju, minimalan zahtjev po ovom pitanju je da kriterij prikupljanja informacija poštuje operativne potrebe i zakonsku legislativu okoline u kojoj poduzeće posluje.

4.2 Pristup informacijama

Niti jedan zaposlenik, organizacija ili vanjski entitet ne smije dobiti pristup centralnom informacijskom sustavu koji sadrži povjerljive informacije bez izričite dozvole odgovornih instanci poduzeća. Internim dokumentom (odlukom, imenovanjem) potrebno je nominirati sigurnosne funkcije unutar poduzeća. Dozvola pristupa određuje se prema procjeni rukovoditelja da određeni zaposlenik treba dobiti pristup informacijama, no pritom je potrebno da budu ispunjeni svi uvjeti iz plana zaštite podataka ali i da se zaštiti privatnost osoba na koje se odnose ti podaci, odnosno povjerljivost podataka ukoliko su općenite prirode.

Nužno je voditi adekvatne evidencije u pisanim i elektroničkim obliku prema važećim procedurama u kojima će biti evidentirano tko je, kada i zašto dobio pristup određenim povjerljivim informacijama. Kopija potpisanih formulara ove vrste mora biti sadržana u osobnoj arhivi zaposlenika. Ovakve evidencije mogu održavati i ključni korisnici te osoba zadužena za informacijsku sigurnost.

4.3 Obrazovanje

Novi zaposlenici obično ne posjeduju specifična znanja potrebna za održavanje i poboljšanje informacijske sigurnosti sustava poduzeća. Iz tog razloga osoba zadužena za informacijsku sigurnost poduzeća bi trebala napraviti plan internog obrazovanja kadrova, odnosno angažirati vanjsku tvrtku ukoliko se za to ukaže potreba. Informacije o obrazovanju zaposlenih vezano uz informacijsku sigurnost su osobito važne u slučaju identificiranih sigurnosnih propusta te kod provođenja unutrašnje ili vanjske revizije.

4.4 Čuvanje i uništavanje dokumenata

Svi tiskani materijali koji sadrže povjerljive informacije moraju biti štićeni od uništenja ili gubitka te mogućih katastrofa poput požara, izljeva vode, na način koji je određen od strane odjela za zaštitu na radu i važećih zakonskih propisa. Posebnu pažnju treba posvetiti ograničavanju fizičkog pristupa takvim informacijama korištenjem sustava prepoznavanja korisnika, ali i zaključavanjem osjetljivih materijalnih dokumenata te definiranjem liste onih koji imaju ključeve te korištenjem principa selektivne distribucije informacija.

Čuvanje dokumenata i osjetljivih podataka dulje od potrebnog roka koji definiraju zakonski propisi ili operativne potrebe poduzeća predstavlja značajan sigurnosni rizik. Zbog prostornog ograničenja, povijesne dokumente moguće je čuvati na udaljenim lokacijama ili za to angažirati tvrtke koje pružaju takve usluge, uz periodičke provjere da li je doista osigura na sigurnost podataka. Ukoliko ne postoje posebni zahtjevi, dokumenti koji sadrže povjerljive informacije trebaju se uništiti najkasnije tri mjeseca nakon što je istekao traženi rok zadržavanja dokumenata.

Uništavanje dokumenata je odgovornost ključnih korisnika uključenih u odgovarajuće procese u poduzeću, odnosno vlasnike tih procesa. Sav tiskani materijal koji sadrži povjerljive informacije treba biti uništen kada je istekao rok zadržavanja. Uništavanje se mora izvesti tako da se spriječi neautorizirani pristup povjerljivim informacijama, npr. rezanjem u specijaliziranim rezačima papira i magnetoptičkih medija. Prije predaje računalne opreme u proces recikliranja ili prije doniranja rashodovane računalne opreme, odnosno prije redistribucije računalne opreme od jednog korisnika drugom korisniku, originalni korisnik je odgovoran za brisanje i snimanje vlastitih sadržaja s tvrdog diska računala.

4.5 Odjelni planovi čuvanja privatnosti podataka

Odgovornost je i pravo svakog ključnog korisnika da razvije i primjenjuje vlastiti plan čuvanja povjerljivih informacija i dokumenata. Iako ne postoji propisani format odjelnog plana, minimalni zahtjev je da je dokument potpisana od strane rukovoditelja odjela, da sadrži datum donošenja, te definira sljedeće zahtjeve:

- naziv ureda, odjela, projekta ili organizacijske jedinice koja manipulira povjerljivim podacima
- imena osoba koje imaju pristup povjerljivim podacima
- administrativne kontrole koje su poduzete kako bi se minimizirao broj ljudi koji imaju pristup povjerljivim informacijama
- opis metoda fizičke zaštite informacija
- opis roka trajanja zadržavanja povjerljivih informacija
- opis načina uništavanja povjerljivih dokumenata
- opis sadržaja treninga o informacijskoj sigurnosti, učestalosti te način dostave povjerljivih informacija

4.6 Zahtjevi prema trećim stranama

Zbog specijaliziranih znanja koja su potrebna da bi se dizajnirale, primjenile te servisirale nove tehnologije, te zbog kratkog roka na raspolaaganju za njihovu primjenu, poduzeća vrlo često ne posjeduju obrazovani kadar koji može obaviti taj posao sam. Iz tog razloga poduzeća ponekad moraju angažirati vanjske specijaliste u određenim područjima,

odnosno konzultante. Isto tako, vanjske službe ponekad se angažiraju da bi pomogli u uništavanju dokumentacije koja se nalazi u papirnatom obliku, te na magnetnim ili optičkim medijima a koja nastaje tijekom odvijanja poslovne aktivnosti poduzeća.

Zbog osiguranja od slučajnog ili namjernog otuđenja povjerljivih informacija potrebno je da pružatelji konzultantskih ili tehničkih usluga predoče certifikate iz kojih je razvidno da su osposobljeni za manipulaciju povjerljivim dokumentima na odgovarajući način. Ovisno o raspoloživosti certifikata, poduzeća često traže provjeru korištenih procedura. Svi ugovori s pružateljima usluga moraju sadržavati klauzulu o privatnosti koja zahtijeva od njih da primijene adekvatne mjere kako bi se očuvala povjerljivost informacija i kako bi se suzdržali od slučajnog ili namjernog otkrivanja klasificiranih informacija. Vrlo često od njih se traži da budu dodatno osigurani u slučaju da otkriju povjerljive informacije te da dođe do pravno utemeljenih zahtjeva od strane osoba ili poduzeća čija je privatnost povrijeđena.

4.7 Kontrola pristupa informacijama sadržanim unutar informacijskog sustava poduzeća

Kontrola pristupa informacijama koje su sadržane unutar informacijskog sustava poduzeća vrlo je kompleksna aktivnost koja može biti zaseban predmet vrlo opširnog razmatranja. Ona obuhvaća sve radnje koje se poduzimaju unutar programskog i hardverskog podsustava kako bi se ograničio pristup povjerljivim informacijama unutar sustava i kako bi se pristup odgovarajućim kategorijama podataka dozvolio samo određenim osobama. U ovu grupu kontrola između ostalog pripadaju sljedeće instance:

1. kreiranje kriterija pristupa računalnoj mreži (uključuje kontrolu pristupa osobnih računala, mobilnih telefona i prijenosnika korisnika izvan sustava)
2. kreiranje korisničkih grupa
3. kontrola pristupa elektroničkoj pošti
4. kontrola pristupa Internet servisima
5. kontrola pristupa telefonskom sustavu
6. kontrola daljinskog pristupa
7. kontrola pristupa preko virtualnih privatnih mreža

5. SURADNJA ORGANIZACIJSKIH CJELINA U PROVOĐENJU PLANA INFORMACIJSKE SIGURNOSTI

Važno je naglasiti da identificirane straške, taktičke i operativne jedinice unutar poduzeća nemaju izoliranu odgovornost po pitanju provođenja plana informacijske sigurnosti pošto su njihove odgovornosti obično međusobno isprepletene, ali je isto i s rizicima. Npr. jedan odjel može biti vlasnik podataka koji se odnose na zdravlje zaposlenika, stoga njihova kvaliteta prelazi operativnu razinu i prelazi na stratešku. Odjel kontrole projekata koji posjeduje povijesni pogled na izvedene projekte u biti radi s podacima koji imaju ne samo stratešku nego i operativnu kvalitetu. Iz tog razloga, kada se procjenjuje kritičnost primjene zaštite informacija, a zbog kompleksnosti poslovnih organizacija, potrebno je ne oslanjati se isključivo na klasifikacije koje se izvode na početku izrade plana već je potrebno svako razmatranje staviti u odgovarajuću perspektivu koja izvire iz stvarnih operativnih potreba.

U okviru ovih aktivnosti unutar poduzeća potrebno je jasno identificirati organizacijske cjeline, odjele i ključni korisnike koji ravnopravno dijele odgovornost za sigurnost informacijskog sustava u cjelini. Sve razine u provođenju plana informacijske sigurnosti moraju u suradnji sa stručnjakom za informacijsku sigurnost periodički testirati i prilagođavati plan informacijske sigurnosti novonastalim zahtjevima. Iz tog razloga potrebno je izrađivati minimalno godišnje izvještaje o stanju informacijske sigurnosti koji propituju adekvatnost postojećih kontrola informacijske sigurnosti u skladu s procedurama i

preporukama za implementaciju istih. Godišnji izvještaj o stanju informacijske sigurnosti mora biti odobren od strane odgovarajuće instance unutar poduzeća a treba sadržavati sljedeće elemente:

- dodatke planu informacijske sigurnosti koji proističu iz tehnološkog i operativnog razvoja informacijske tehnologije i poslovnih zahtjeva
- procjenu stanja primjene postojećeg plana informacijske sigurnosti
- status primjene postojećeg plana informacijske sigurnosti
- prijedlog mjera za poboljšanje informacijske sigurnosti poduzeća
- vrijeme potrebno za primjenu mjera poboljšanja
- vezane troškove i proračun potreban za primjenu predloženih mera

6. ZAKLJUČAK

Neprekinuta poslovna aktivnost i ispravno funkcioniranje informacijskih sustava je danas osnovni zahtjev koji se postavlja pred stručnjake koji su u poduzećima zaduženi za sigurnost informacijskih sustava. Prijetnje informacijskim sustavima i procesima tako postaju prijetnje kvaliteti poslovne aktivnosti i efikasnosti. Cilj sigurnosti informacijskih sustava je postaviti u funkciju mjere koje mogu eliminirati ili barem značajno smanjiti prijetnju tim sustavima na prihvatljivi nivo. Sigurnost i menadžment rizika su stoga nužno vezani uz menadžment sustava upravljanja kvalitetom.

Sigurnost informacijskih sustava je zaštita informacija, informacijskih sustava i usluga od katastrofalnih događaja, grešaka i manipulacija tako da se smanji mogućnost i utjecaj sigurnosnih incidenata na čim manju mjeru. Sigurnost informacijskih sustava sastoji se od osiguranja povjerljivosti informacija, integriteta informacija, raspoloživosti informacija i informacijskih sustava te poštovanja zakonskih propisa. U današnje doba gotovo sva poduzeća koriste informacijske sustave kao podršku svojoj svakodnevnoj poslovnoj aktivnosti. Ukoliko te informacije postanu raspoložive konkurentima, postanu tehnički oštećene tijekom prijenosa, netočne ili obrisane, postavlja se pitanje integriteta poslovne aktivnosti i na kraju, da li se poslovna aktivnost uopće može nastaviti u opsegu i na način na koji se obavljala do takvog neželjenog događaja. U današnje doba kada su informacijski sustavi umreženi, rizik pojave neželjenih događanja se višestruko multiplicira.

Zbog svega navedenog, u poduzeću mora postojati procjena rizika te mjera koje će provesti kako bi se definirale procedure postupanja s osjetljivim podacima i tehnološke mjere kojima će se oni osigurati. Informacije se daju na korištenje svim zaposlenicima u vidu plana informacijske sigurnosti koji priprema stručnjak za informacijsku sigurnost a koji je između ostalog preduvjet za primjenu sustava upravljanja kvalitetom. Plan upravljanja informacijskom sigurnošću sadrži i ključne korisnike unutar poduzeća koji dijele odgovornost za upravljanje sigurnošću informacijskih sustava ali i godišnje izvještaje o stanju informacijske sigurnosti koji služe kao podloga za stalno poboljšavanje plana i stanja sigurnosti informacijskih sustava unutar poduzeća.

7. LITERATURA

1. „Operative Information Protection Plan“, Saša Aksentijević, Saipem Mediteran Usluge d.o.o interna dokumentacija, Rijeka, 15.08.2006.
2. <http://en.wikipedia.org/wiki/E-business> (02.06.2007.)
3. http://www.bcbsil.com/code/code_confident.htm (03.06.2007)
4. http://en.wikipedia.org/wiki/Bell-La_Padula_security_model (03.06.2007)
5. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci508347,00.html (31.05.2007.)
6. <http://fas.org/irp/program/process/echelon.htm> (25.05.2007.)

7. <http://www.microsoft.com/protect/yourself/phishing/identify.mspx> (03.06.2007.)
8. <http://www.cs.berkeley.edu/~bh/hacker.html> (30.05.2007.)
9. <http://www.secretcodebreaker.com/history2.html> (03.06.2007.)
10. Saipem Spa, Milano, Italija, interna dokumentacija