# Uloga ključnih administratora u postizanju ciljeva integralne korporativne sigurnosti

PREZENTACIJA

RIJEKA, 2008.

# Uloga ključnih administratora u postizanju ciljeva integralne korporativne sigurnosti

PREZENTACIJA

Konferencija : Zagreb IPC PAES 2008

Predavač : mag. oec. Saša Aksentijević, univ.spec.za intel.el.posl.

RIJEKA, rujan, 2008

SADRŽAJ

# 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, financijske institucije, bolnice i privatna poduzeća prikupljaju velike količine povjerljivih informacija o svojim zaposlenicima, komitentima, proizvodima, istraživanjima i financijskoj 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.

Predmet izlaganja je elementarno funkcioniranje podsustava za zaštitu informacijskih sustava koji bi trebao biti implementiran u okviru informacijskog sustava tvrtke. Jači naglasak biti će 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. POVIJEST SIGURNOSTI INFORMACIJSKIH SUSTAVA

Od najranijih dana pisane povijesti, vladari i vojni vođe shvaćali su važnost mehanizma kojim bi se štitila povjerljivost pisane korespodencije i postojanje mehanizma kojim bi se detektiralo da je povjerljivost narušena. U početku su se u tu svrhu koristili pečati od voska i slične tehnike koje su davale dokumentima značajku autentičnosti i osiguravali povjerljivost korespondencije. Prva osoba koju pisana povijest spominje kao nekoga tko je formalizirao ovakav postupak je bio Julije Cezar koji je 50 godina prije Nove ere osmislio sustav „cezarovog šifriranja“ [1] kako bi spriječio da njegove tajne poruke dođu do neželjenih ruku.

Drugi svjetski rat doveo je do značajnog napretka po pitanju informacijske sigurnosti i tada dolazi do profesionalizacije te aktivnosti. Najveći naglasak dan je na pitanje fizičke zaštite informacija kojima je sprečavan pristup informacijskim centrima. Također dolazi do formalizacije i klasifikacije podataka ovisno o njihovoj osjetljivosti. Uvode se osobne provjere prije davanja pristupa podacima.

Krajem dvadesetog i početkom dvadeset i prvog stoljeća dolazi do naglog napretka u telekomunikacijama, informatičkoj opremi, elektronskim mrežama za razmjenu podataka i metodama šifriranja podataka. Raspoloživost manjih, snažnijih i jeftinijih računala omogućila je obradu podataka i u manjim poduzećima te domovima zaposlenika. Nagli rast i široka

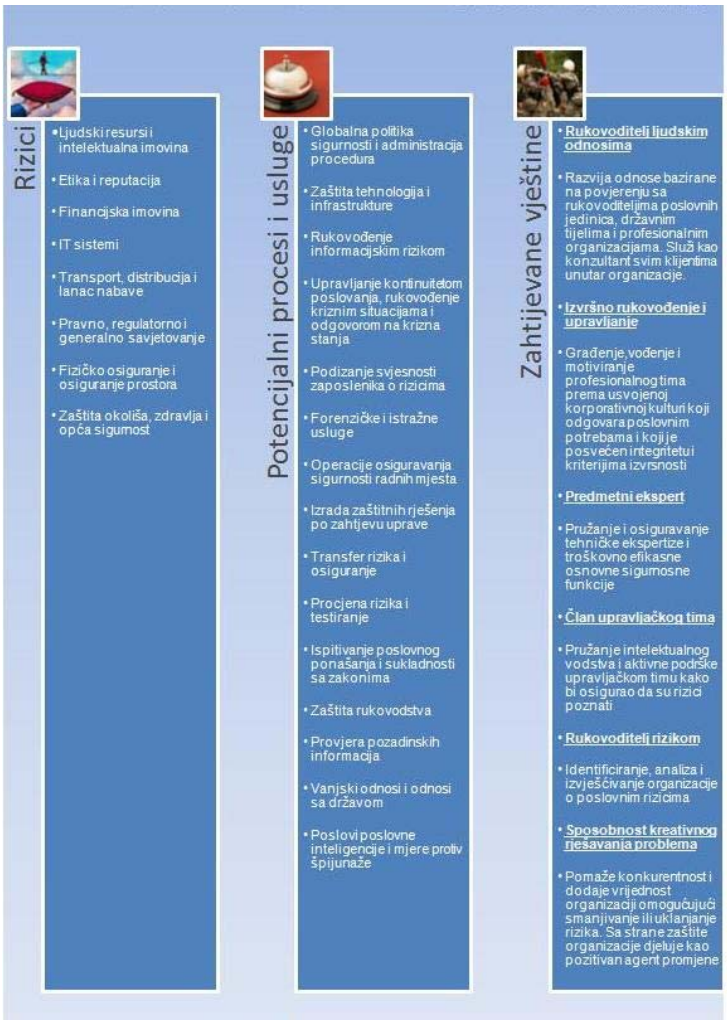
[1] http://www.secretcodebreaker.com/history2.html (03.06.2007.)

primjena elektronske obrade podataka te pojava tzv. e-business-a[2] paralelno s pojavom međunarodnog terorizma iznjedrila je potrebu za boljim načinima zaštite računala i informacija koje ona pohranjuju, obrađuju i razmjenjuju. Stoga u današnje doba sigurnost računalnih sustava postaje akademska disciplina unutra raznih profesionalnih organizacija, radeći na zajedničkom cilju osiguranja zaštite i sigurnosti informacijskih sustava.

[2] http://en.wikipedia.org/wiki/E-business (02.06.2007.)

## 2. INTEGRALNA KORPORATIVNA SIGURNOST

Integralna korporativna sigurnosna funkcija mora biti povjerena visokoj razini koja odgovara direktno Upravi društva. Ovisno o funkcionalnom modelu, može se raditi o izdvojenom odjelu koji zatim provodi akcije ka postizanju ciljeva integralne sigurnosti ili o jednoj osobi koja zatim koordinira i usmjerava ostale postojeće odjele.




izvor: izradio autor

# 3. 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.

Koraci koje treba poduzeti kod pripreme Plana informacijske sigurnosti su sljedeći:

1. Identificira se kritična dokumentacija kao podloga za pripremu Plana te standardi koji će biti primijenjeni
2. Procjenjuje se postojeće stanje informacijske sigurnosti unutar poduzeća ili organizacije
3. Definiraju se prioriteti informacijske sigurnosti
4. Identificiraju se odjeli te funkcije koje u operativnoj fazi rade s povjerljivim informacijama ili podacima
5. Identificiraju se mogući rizici po sigurnost sustava
6. Predlažu se metode za umanjenje ili potpuno uklanjanje rizika

## 3.1 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 poredstavlja sve moguće implementirane zaštite u klasičnim i kompjutorskim informacijskim sustavima. Sigurnost 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 konkurenciji 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.

3.2 Pravila dobrog ponašanja

Poslovni podaci i komunikacije mogu postati i javni pod već navedenim uvjetima, stoga u kolokvijalnoj, ali i pisanoj komunikaciji treba izbjegavati sljedeće:

1. pretjerivanje
2. ponižavajuće primjedbe
3. pretpostavljanje
4. neprimjerene karakterizacije ljudi i događaja koje bi se mogle krivo shvatiti

Ovo se jednako odnosi na elektroničku poštu, interneu dokumentaciju, memorandume, kao i na formalne izvještaje i dokumente.

3.3 „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. Princip 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.[3] 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 dokumentacijskih 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 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

[3] http://www.bcbsil.com/code/code_confident.htm (03.06.2007)

pristup njihovom radu. Stoga primjena ovog principa mora promovirati duh pozitivne suradnje a ne samo čuvati privatnost podataka.

## 3.4 Nivoi diskrecije

Ukoliko je potrebno, ključni korisnici unutar organizacije mogu interno uvesti Bell-LaPadula[4] 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. Najčešće se koriste sljedeći nivoi diskrecije:

1. Vrhovna tajna
2. Tajno
3. Povjerljivo
4. Neklasificirano

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.

[4] http://en.wikipedia.org/wiki/Bell-La_Padula_security_model (03.06.2007)

# 4. 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 direktan 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 primijenjen pošto se mora stalno dopunjavati.

## 4.1 Identificiranje rizika

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 opisani u nastavku.

### 4.1.1 Pristup povjerljivim informacijama od strane neovlaštene osobe

Povijesno, kao što su uvijek postojali unutrašnji korisnici informacijskog sustava koji su pokušavali neovlašteno pristupiti informacijama, postojat će i osobe ili organizacije izvan organizacijskog sustava koji će htjeti dobiti neautorizirani pristup informacijama. Razlozi za takav pristup su višestruki, od puke zabave do krađe informacija zbog materijalne koristi ili jednostavno iz malicioznih razloga, kako bi se kompromitirala cjelovitost informacijskog sustava.

### 4.1.2 Kompromitiranje sistemske sigurnosti kao rezultat pristupa od strane „hakera“

Po definiciji, hakiranje je neovlašteno korištenje ili pokušaj neovlaštenog korištenja da bi se zaobišli sigurnosni mehanizmi zaštite informacijskog sustava ili računalne mreže. U

početku termin „haker“[5] je izazivao poštovanje informatičke zajednice koji se koristio između programera, dizajnera sustava i inženjera. „Hakeri“ su kreirali originalne programe koji su rješavali određene probleme. Nažalost, danas se termin koristi za opis ljudi koji ulaze u informacijske sustave, uništavaju ili kradu podatke ili zaštićene programe te vrše ostale destruktivne ili ilegalne zahvate na računalima i mrežama.

### 4.1.3 Presretanje podataka tijekom transakcije

Internet je izgrađen kao mješavina distribuiranog i hijerarhijskog sustava: krajnji korisnici poput individualnih osoba ili poduzeća su spojeni na mrežu pružatelja usluga preko modemskih ulaza ili kabelskih veza dok su pružatelji usluga spojeni na veće pružatelje usluga koji se protežu preko više država a oni su pak spojeni između sebe. Posebna računala ili mrežna oprema - routeri i gatewayi - imaju zadaću pronaći ispravan put kojim će paketi podataka proći i biti proslijeđeni sve dok ne stignu do svog odredišta. Stoga se put podataka od izvora do odredišta naziva rutom podataka. Rute podataka odabiru se ovisno o raspoloživosti mrežnih resursa i opterećenju mreže. Rute se mogu dinamički mijenjati, ponekad više puta tijekom dana. Iz tog razloga paketi podataka potuju do odredišnog poslužitelja kroz mnoge različite mreže i preko više različitih rutera i gatewaya.

Nakon što paket podataka napusti mrežu pružatelja usluge gotovo je nemoguće predvidjeti njegovu rutu, pošto ona primarno ovisi o odredištu. Ukoliko je odredište isto, ruta se svejedno može promijeniti. Da bi se mogla pratiti nečija aktivnost na Internetu potrebno je pratiti promet koji ide preko mreže pružatelja usluga. Na taj način fukcioniraju sustavi poput Carnivorea[6] ili Echelona[7] unutar Europske unije. Neke manje države te dosta arapskih zemalja imaju svega nekoliko ili čak jedan jedini glavni podatkovni izlaz iz države, što omogućuje nadzor čitave države ili geografskog područja te je tehnički vrlo jednostavno analizirati promet ili ga čak blokirati.

Minimalni zahtjev zaštite od presretanja podataka tijekom transakcije je da su oni šifrirani na hardverskom ili bar softverskom nivou nakon što napuste mrežu štićene organizacije, poduzeća ili pojedinca. Ista se tehnologija mora primijeniti i kada se koristi tehnologija virtualnih privatnih mreža ili daljinskog spajanja korisnika na domicilni informacijski sustav.

### 4.1.4 Gubitak podataka ili povjerljivosti informacija zbog greške korisnika

U praksi najčešći razlog zbog kojega dolazi do otkrivanja povjerljivih podataka i informacija je greška korisnika. Priroda i veličina štete ovise o osjetljivosti podataka. Načini na koje može doći do greške korisnika, nenamjerne ili namjerne, su doista mnogobrojni:

- korisnik može ostaviti u štampaču papire s povjerljivim informacijama
- optički ili drugi memorijski mediji mogu biti poslani na krivu adresu bez da su prije toga obrisani osjetljivi podaci s njih
- zbog neadekvatne administracije korisničkih prava korisnik može promijeniti ili obrisati podatke bez da je svjestan kakav je utjecaj takve akcije
- nova aplikacija koja vrši dohvat nad postojećim podacima uvodi se u poduzeće, posljedica je da neautorizirane osobe mogu doći u posjed povjerljivih informacija

[5] http://www.cs.berkeley.edu/~bh/hacker.html (30.05.2007.)
[6] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci508347,00.html (31.05.2007.)
[7] http://fas.org/irp/program/process/echelon.htm (25.05.2007.)

- papirnata dokumentacija se baca u smeće bez da je prije toga izrezana u posebnim rezačima papira
- pokvarena računala šalju se na servisiranje s podacima koji se još nalaze na njima
- povjerljivi podaci greškom se šalju na krivi štampač
- informacije se šalju na krivu adresu zbog pogrešnog odabira email adrese
- papirnati dokumenti (npr. ugovori) se šalju na krive adrese
- „izreži i zalijepi“ funkcija je korištena kada to nije trebalo

4.1.5 Fizički gubitak podataka uslijed katastrofe

Fizički gubitak podataka uslijed katastrofe (požar, poplava, potres, terorističke akcije) može djelomično ili u potpunosti paralizirati poduzeće. Čak i ograničeni događaj, npr. požar u serverskoj sobi ili podatkovnom centru može imati katastrofalne posljedice po informacijsku strukturu poduzeća. Međutim, čak i nenadani događaj izvan poduzeća može rezultirati posljedicama po samo poduzeće, ukoliko poduzeće koristi u potpunosti ili djelomično udaljene poslužitelje za spremanje svojih podataka i servisa, u slučaju katastrofe moguće je da bude pogođena infrastruktura poduzeća iako nije njegova vlastita. Isto se može dogoditi u slučaju posljedica po strujnu mrežu, sustav telefonije, međunarodne i satelitske veze i GSM mrežu. Iz tog razloga poduzeća bi trebala poduzeti sve moguće razumne mjere da svedu ove rizike na minimum. Mjere koje se poduzimaju obično se definiraju posebnim dokumentom koji se naziva Plan sanacije nakon katastrofalnog događaja.

4.1.6 Nekompletnost i nedokumentiranost transakcije

Svaka transakcija koja se odvija unutar informacijskog sustava, osobito ukoliko su uključeni povjerljivi podaci i informacije trebača bi biti dokumentirana, no trebala bi imati i vlasnika koji mora osigurati njenu potpunost te da je nakon toga adekvatno dokumentirana. Ako transakcija nije dokumentirana, odgovornost je ključnog korisnika da osigura njezinu potpunost i prati do kraja izvršenja.

Dokumentacija koja prati transakciju trebala bi biti dovoljno detaljna i morala bi biti procesirana kroz odgovarajuće informacijske i hijerarhijske kanale unutar poduzeća. Sve možebitno zainteresirane strane morale bi biti upoznate s njenim postojanjem, no posebna pažnja mora se pridati tome da količina informacija bude održana na razumnom nivou kako bi se izbjeglo da se ljudi preopterećuju irelevantnim informacijama ili informacijama koje nisu im nisu potrebne. Iz tog razloga svi izvještaji i dokumentacija trebali bi biti prezentirani na koncizan i precizan način.

4.1.7 Neautorizirani pristup povjerljivim informacijama od strane zaposlenika

Pristup podacima i informacijama iz informacijskog sustava ali i papirnatim dokumentima treba biti ograničen na one zaposlenike koji ih moraju znati iz poslovnih razloga. Unutar svakog informacijskog sustava potrebna je segmentacija elemenata prema vlasniku i svrsi, gdje god je moguće podsustavi moraju biti zaštićeni lozinkama a promjena lozinke mora se vršiti ciklički.

Baze podataka koje sadrže osjetljive ili povjerljive informacije moraju biti raspoložive samo rukovodiocima ili ključnim korisnicima na odgovarajućim pozicijama koje moraju biti dokumentirane u Matrici autorizacija i odgovarajućim punomoćima koje mogu biti ili formalne, nakon imenovanja na poziciju ili neformalne.

Odjeli zaduženi za informacijske sustave moraju poduzeti razumne i adekvatne akcije da bi se držali u korak s trenutačnim tehnološkim stupnjem razvijenosti i kako bi osigurali da informacije u tranzitu budu sigurne, te da pohranjene informacije budu dostupne samo onima koji su autorizirani za pristup. To se odnosi na održavanje operativnog sustava, aplikacija, ali i primjenu adekvatnih sigurnosnih zakrpa na vrijeme.

Fizički pristup serverskoj sobi te kritičnim dijelovima mrežnog sustava mora biti dozvoljen samo autoriziranim zaposlenicima. O pristupu se mora voditi pisana evidencija.

#### 4.1.8 Neautorizirani zahtjev telefonom ili emailom za povjerljivim informacijama („phishing“)

„Phishing“ [8]je oblik kriminalne aktivnosti kojim je moguće doći do povjerljivih informacija koristeći tehnike socijalnog inženjeringa. Obično se radi o pokušajima dolaska do osjetljivih informacija prevarom, predstavljanjem da se radi o povjerenja vrijednim osobama ili poduzećima. Često se lažno traže korisničko ime i lozinka pod izlikom provjere. Isto tako je moguće da se korisnicima daju lažne Web poveznice preko kojih je moguće doći do korisničkih podataka.

#### 4.1.9 Neautorizirani pristup preko papirnih dokumenata i izvještaja

Papirnati dokumenti moraju se držati u ormarina ili sefovima koji se zaključavaju. Samo ovlašteni zaposlenici trebaju znati kombinacije šifri i lokaciju ključeva. Pri bacanju, papirnate dokumente treba rezati. Papirnati dokumenti ne smiju se bacati u obične kante za smeće, osobito ako nisu izrezani.

Tijekom radnog vremena radni dokumenti trebaju biti stavljeni licem prema dolje i trebaju biti pohranjeni u registratorima koji su neprozirni kako bi se izbjeglo slučajno otkrivanje informacija. Posebnu pažnju treba posvetiti slanju papirnatih dokumenata izvan poduzeća.

#### 4.1.10 Neautorizirani transfer povjerljivih informacija preko treće strane

Da bi se osiguralo od neautoriziranog transfera informacija preko treće strane primarno je potrebno organizirati barijere fizičkom pristupu. Pritom se primarno misli na naprave protiv provale, kamere, registraciju posjetitelja koji ulaze u poduzeće, praćenje do njihovog odredišta i generalno, fizičku zaštitu zgrade. Serverske sobe su u ovom smislu osobito predmet posebne zaštite.

[8] http://www.microsoft.com/protect/yourself/phishing/identify.mspx (25.05.2007.)

# 5 KONTROLA I UPRAVLJANJE RIZIKOM

## 5.1 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 relevantnih funkcija unutar poduzeća.

U svakom slučaju, minimalan zahtjev po ovom pitanju je da kriterij prikupljanja informacija poštuje operativne potrebe i legislativu okoline u kojoj poduzeće posluje.

## 5.2 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 ključnog korisnika 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 pisanom i elektroničkom 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.

## 5.3 Obrazovanje

Novi zaposlenici obično ne posjeduju specifična znanja potrebna za održanje 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.

## 5.4 Fizička sigurnost 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.

### 5.4.1 Čuvanje dokumenata

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.

### 5.4.2 Uništavanje 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 na taj način da se spriječi neautorizirani pristup povjerljivim informacijama, dakle rezanjem. 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.

## 5.5 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 takvog plana, minimalni zahtjev je da je takav dokument potpisan od strane ključnog korisnika, da sadrži datum donošenja, te da definira sljedeće zahtjeve:

- naziv ureda, odjela, projekta ili organizacijske jedinice koja manipulira povjerljivim podacima
- imena osoba koje imaju pristup takvim 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

## 5.6 Zahtjevi prema trećim stranama

Zbog specijaliziranih znanja koja su potrebna da bi se dizajnirale, primijenile te servisirale nove tehnologije, te zbog kratkog roka na raspolaganju 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.

Iz tog razloga potrebno je da pružatelji takvih usluga predoče certifikate iz kojih je razvidno da su osposobljeni za manipulaciju povjerljivim dokumentima na odgovarajući način. Ovisno o tim certifikatima, poduzeća često traže provjeru 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 takvih 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.

## 5.7 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
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

# 6 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 stratrešku 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 mjera

# 7 ULOGA KLJUČNIH ADMINISTRATORA

Uloga ključnih administratora razvijala se paralelno s razvojem poslovnog okruženja i u današnje doba obuhvaća veliku paletu odgovornosti. Ovisno o poziciji u organizaciji, ključni administrator se bavi dolaznim pozivima, provjeravanjem poruka elektroničke pošte, slanjem poruka, istraživanjem, rezervacijama itd. Međutim, uspješan ključni administrator mora imati i vještine rukovodstva, organizacijske vještine, diplomatske sposobnosti, taktičnost, pokazati dobre komunikacijske sposobnosti, sposobnost pravovremene i brze procjene te održavanja povjerljivosti.

S vremenom, poslovi ključnih administratora mogu se pretvoriti u angažman u nekim drugim dijelovima u organizaciji. Ovisno o korporativnoj kulturi, demonstriranom radnom učinku, osobinama i nivou obrazovanja, ključni administratori mogu zauzeti odgovarajuće važne pozicije drugdje unutar organizacije.

Činjenica je kako ključni administratori tijekom svog rada akumuliraju velike količine informacija od kojih su mnoge, zbog blizine destinataru koji njima upravlja, povjerljive. Vrlo često između ključnih administratora i korisnika njihovih usluga razvijaju se odnosi koji nisu striktno samo poslovni, već i privatni, prijateljski, pa čak i savjetodavni. Administratori često nisu formalni dio drugih odjela organizacije, nego odgovaraju direktno unutar ureda korisnika usluga, te često odgovaraju samo njemu. Iz tog razloga, smještaj ključnih administratora u hijerarhiji dodatno podcrtava značaj uloge u odnosu prema informacijskoj i integralnoj sigurnosti organizacije.

Zbog svega navedenog, administratori nikako nisu pasivni provoditelji informacijske i integralne sigurnosti već moraju biti njeni aktivni kreatori. Temeljni postulat sigurnosti je da ona uvijek kreće iz vrha organizacija, tj. za postizanje njenih ciljeva mora biti obvezano upravno tijelo. Pošto se administratori nalaze u blizini tog upravnog tijela, oni mogu direktno utjecati na provođenje politika sigurnosti i njihovu diseminaciju (širenje) na niže te operativne razine.

Osobni je, ali i poslovni interes, upoznati ključne administratore s temeljnim dokumentima i procedurama koje reguliraju proces provođenja informacijske i integralne sigurnosti unutar organizacije. Administratori bi trebali biti upoznati s politikama, radnim uputama, pisanim i usmenim procedurama, ključnim pozicijama, osobama i procesima koji reguliraju ovu tematiku. No, administratori bi također morali pokazati osobni interes i stremljenje ka postizanju ovog cilja.

S obzirom na blizinu vrhu rukovodstva, dobro obaviješteni i educirani administrator tako može postati usmjernik i kanalizator procesa postizanja izvrsnosti kod integralne i informacijske sigurnosti.

Preporuča se administratorima upoznati se s temeljnim zakonima, propisima i odredbama koje definiraju područje informacijske sigurnosti, postupaka i procedura u Republici Hrvatskoj, kako s općima, tako i s onima koji se odnose na banke i osiguravajuća društva:

1. Zakon o zaštiti osobnih podataka
2. Zakon o informacijskoj sigurnosti
3. Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka

4. Zakon o zaštiti na radu
5. Zakon o bankama
6. Smjernice za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika
7. Odluka o primjerenom upravljanju informacijskim sustavom
8. Zakon o osiguranju
9. Pravilnik o detaljnom obliku i najmanjem opsegu te sadržaju revizorskog prijedloga i revizorskog izvješća društava za osiguranje

# 7. ZAKLJUČAK

Neprekinuta poslovna aktivnost i ispravno funkcioniranje informacijskih sustava je danas osnovni zahtjev koji se predstavlja pred one 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 povjerljivosti informacija, integriteta informacija, raspoloživosti informacija i informacijskih sustava te poštovanja zakonskih propisa.

U današnje doba gotovo sva poduzeća koriste informacijske sustave kao podršku njihovoj svakodnevnoj poslovnoj aktivnosti. Ukoliko te informacije postanu raspoložive konkurentima, postanu korumpirane, 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. Te se informacije daju na korištenje svim zaposlenicima daju u vidu plana informacijske sigurnosti koji priprema stručnjak za informacijsku sigurnost a koji je između ostalog preduvjet za primjenu sustava upravljanja kvalitetom ISO. Plan upravljanja informacijskom sigurnosti 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.

Ključni administratori moraju biti uključeni u proces konstantnog rada na poboljšavanju informacijske sigurnosti i zbog svoje prirode posla te rada s povjerljivim informacijama moraju među prvima biti educirani o temeljima informacijske i integralne sigurnosti.

8. 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