HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Upravljanje sigurnošću informacijskih sustava

CCERT-PUBDOC-2003-11-49

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Sigurnost informacijskih sustava vrlo često je zanemarena na globalnoj razini. Najčešće se nude polovična rješenja koja se odnose na sigurnost nekog pojedinog istaknutog aspekta u sustavu, dok se drugi elementi zanemaruju. Izvjesno je, međutim, da je sigurnost cjelokupnog sustava uvijek proporcionalna sigurnosti najslabije točke.

Ovaj rad bavi se ključnim koracima pri implementaciji sigurnog informacijskog sustava.

Prva dva poglavlja opisuju neke osnovne koncepte sigurnog informacijskog sustava, te opisuju identifikaciju resursa unutar organizacije. Sljedeće poglavlje opisuje postupak upravljanja rizikom, odnosno analizu rizika i njeno značenje za organizaciju. U posljednjem poglavlju opisana je izrada dokumenta sigurnosne politike i njena implementacija kroz preporuke, standarde i detaljne procedure.

2. Koncepti

Upravljanje sigurnošću informacijskih sustava podrazumijeva identifikaciju (informacijskih) resursa, njihovo vrednovanje, procjenu rizika obzirom na moguće prijetnje, izradu odgovarajuće sigurnosne politike i njenu implementaciju u stvarnom okruženju.

Osnovni zahtjevi koje proces upravljanja sigurnošću informacijskih sustava mora ispuniti jesu:

- povjerljivost,
- integritet i
- raspoloživost.

Povjerljivost se odnosi na zaštitu određenih sadržaja, odnosno informacija od bilo kakvog namjernog ili nenamjernog otkrivanja neovlaštenim osobama.

Integritet mora osigurati konzistentnost informacija i onemogućiti bilo kakve neovlaštene promjene sadržaja.

Konačno, pojam raspoloživosti podrazumijeva da su sve relevantne informacije, u za to vremenski prihvatljivom terminu, raspoložive odgovarajućim subjektima.

Bilo koji od ovih zahtjeva može biti kompromitiran na razne načine; bilo namjernom ili nenamjernom ljudskom pogreškom, bilo zbog nedostataka i kvarova opreme i aplikacija ili zbog drugih izvanrednih događaja.

Osim osnovnih zahtjeva koje proces upravljanja sigurnošću sustava mora osigurati valja spomenuti i pojmove koji su usko vezani uz implementaciju sigurnosnih kontrola a to su:

- identifikacija,
- autentikacija,
- autorizacija,
- zaštita i
- mogućnost praćenja.

Identifikacija podrazumijeva predstavljanje korisnika unutar sustava, dok kroz proces autentikacije korisnik mora dokazati svoj identitet. Autorizacijom se korisniku odobrava ili zabranjuje pristup odnosno korištenje pojedinog resursa u sustavu. Sam pojam zaštite govori sam za sebe, dok mogućnost praćenja mora kroz sustav osigurati praćenje i nadzor nad akcijama subjekta.

2.1. Definicija uloga u sustavu

Bez odgovarajuće definicije uloga u sustavu nije moguće uspostaviti odgovarajući sustav odgovornosti, a samim time ni zaštite. To se odnosi na identifikaciju resursa, kao i na implementaciju sigurnosne politike. Općenito u sustavu korisnicima je moguće dodijeliti jednu od tri sljedeće uloge:

- vlasnik,
- odgovorna osoba i
- korisnik.

Vlasnik je obično osoba koja upravlja organizacijom ili nekim njenim dijelom. Ta osoba unutar organizacije snosi potpunu i konačnu odgovornost za pojedine resurse i njihovu zaštitu.

Za konkretnu uspostavu mehanizama zaštite i njihovo održavanje nije zadužen vlasnik već odgovorna osoba, zadužena za to od strane vlasnika resursa. U informacijskom sustavu ta osoba je obično administrator sustava.

Konačno, korisnikom se smatra svaka osoba koja se koristi resursima sustava. Korisnik je dužan koristiti resurse na način na koji je to propisano.

3. Identifikacija resursa

Prvi preduvjet za uspješno upravljanje sigurnošću informacijskog sustava podrazumijeva identifikaciju resursa koji su dio tog sustava. Bez precizne identifikacije resursa nije moguće implementirati njihovu kvalitetnu zaštitu.

Kroz proces identifikacije resursa potrebno je pobrojati sve resurse unutar informacijskog sustava, te procijeniti njihovu relativnu vrijednost za organizaciju. Na temelju toga je moguće kasnije, u procesu upravljanja rizikom, odnosno prilikom analize rizika, efikasno ocijeniti potrebnu razinu zaštite za svaki pojedini resurs unutar sustava.

Kvalitetnom identifikacijom resursa nužno je postići sljedeće zahtjeve:

- identificirati pojedine resurse unutar sustava,
- procijeniti vrijednost resursa,
- ustanoviti vlasnika, odnosno osobu koja je odgovorna za taj resurs,
- ustanoviti njegovo fizičko ili logičko mjesto u sustavu, te
- napraviti odgovarajuću dokumentaciju.

3.1. Podjela resursa

Podjelu resursa unutar nekog sustava moguće je napraviti prema raznim kriterijima. U informacijskim sustavima resurse je ugrubo moguće podijeliti u sljedeće kategorije:

- informacije (baze podataka, dokumentacija, autorska djela, interne procedure, sigurnosne politike itd.),
- programska podrška (aplikacije, operacijski sustavi, razvojni alati itd.),
- oprema (računalna oprema, mrežno-komunikacijska oprema, mediji za pohranu podataka i ostala oprema nužna za rad informacijskog sustava) i
- servisi (računalni i komunikacijski, te općeniti servisi kao što su grijanje, osvjetljenje itd.).

Za svaki od identificiranih resursa potrebno je napraviti procjenu njegove relativne vrijednosti unutar sustava, bez obzira u koju kategoriju pripada. Često se naglasak prilikom upravljanja sigurnošću informacijskog sustava daje na same informacije, dok su npr. servisi zanemareni, no gubitak nekog od tih resursa također može rezultirati narušavanjem rada sustava, pa čak i potpunim zastojem poslovnog procesa.

3.2. Klasifikacija informacija

Resurse koji pripadaju različitim kategorijama moguće je klasificirati na razne načine. Obzirom da je u informacijskom sustavu ipak najvažnija sama informacija, potrebno je uspostaviti adekvatni sustav klasifikacije.

Unutar sustava općenito su pohranjene informacije različite vrijednosti za organizaciju; od potpuno nevažnih do onih ključnih, pa i kritičnih.

Cilj klasifikacije informacija jest da se osigura njihova adekvatna zaštita. Klasifikacija se obično provodi obzirom na postavljene kriterije (vrijednost same informacije, utjecaj vremena na njenu vrijednost, povezanost s pojedinim osobama itd.). U većini organizacija općenito je prikladan sljedeći sustav klasifikacije:

- javne,
- osjetljive,
- povjerljive i
- tajne.

Javne informacije mogu se ponekad poistovjetiti i s informacijama koje ne spadaju u sustav klasifikacije, a odnose se na one informacije čije otkrivanje ne predstavlja nikakav potencijalni rizik za organizaciju. Za njih obično nije nužno implementirati sigurnosne kontrole.

Osjetljive informacije zahtijevaju veću razinu kontrole, pošto njihovo otkrivanje ili gubitak integriteta mogu rezultirati određenim gubicima (koji ne moraju biti direktno materijalne prirode).

Povjerljive informacije smatraju se namijenjenim samo internoj uporabi unutar organizacije. Njihovo otkrivanje može imati negativni utjecaj na organizaciju ili njene zaposlenike, tako da je nužna implementacija odgovarajućih sigurnosnih mehanizama.
Tajne informacije odnose se na najosjetljivije podatke i bilo kakve neovlaštene aktivnosti vezane uz njih mogu rezultirati vrlo ozbiljnim posljedicama za organizaciju. Adekvatna implementacija sigurnosti za ovakve informacije je od kritične važnosti.

4. Upravljanje rizikom

Ulaganje u informacijsku sigurnost potrebno je promatrati kao investiciju. Od svake investicije, pa tako i od ulaganja u informacijsku sigurnost, očekuje se pozitivni povrat sredstava. U tom kontekstu upravljanje sigurnosti se može promatrati u smislu smanjenja operacijskih troškova, prevencije potencijalnih troškova ili drugih negativnih utjecaja na poslovni proces.
U kontekstu upravljanja rizikom potrebno je identificirati osnovne elemente:
- osjetljivost (ranjivost) sustava,
- potencijalne prijetnje,
- posljedice i
- protumjere.

Svaki sustav u nekoj mjeri je osjetljiv na potencijalne prijetnje ili nedostatke. Ranjivost sustava proizlazi iz ranjivosti dijelova sustava, odnosno resursa. Potencijalne prijetnje mogu koristiti neku od ranjivosti sustava ili egzistirati neovisno o sigurnosti samog sustava. Izvori prijetnji mogu biti razni:
- pogreške ili kvarovi na resursima (programske pogreške, kvarovi na sklopovlju itd.),
- napadi (izvana i iznutra),
- havarije (požari, elementarne nepogode itd.),
- ljudske pogreške i drugi.

Isto tako, posljedice ostvarivanja neke prijetnje mogu varirati te općenito mogu biti materijalne (štete na uređajima i sl.) i nematerijalne (otkrivanje informacija, trajni ili privremeni gubitak informacija itd.).
Postojanje neke prijetnje ne implicira nužno da će ta prijetnja biti i ostvarena, odnosno da će doći do materijalne ili nematerijalne štete.
Važan dio upravljanja sigurnosti predstavlja upravljanje rizikom, odnosno uspostava relacija između ranjivosti, potencijalnih prijetnji i posljedica, odnosno utjecaja na informacijski sustav.
Proces upravljanja rizikom sastoji se od sljedećih koraka:
- identifikacije resursa,
- analize rizika,
- interpretacije rezultata i poduzimanja odgovarajućih protumjera.

Pri tom valja istaknuti da upravljanje rizikom ne podrazumijeva uspostavu apsolutne sigurnosti, već uočavanje potencijalnih rizika odnosno prijetnji, procjenu njihovog potencijalnog učinka i procjenu troškova potrebnih za implementaciju odgovarajućih protumjera.

4.1. Analiza rizika

Analiza rizika je postupak kojem je cilj ustanoviti ranjivosti sustava, uočiti potencijalne prijetnje (rizike), te na odgovarajući način kvantificirati moguće posljedice, da bi se mogao odabrati najefikasniji način zaštite, odnosno procijeniti opravdanost uvođenja dodatnih protumjera.
Postoje dva osnovna pristupa analizi rizika:
- kvantitativna analiza i
- kvalitativna analiza.

4.1.1. Kvantitativna analiza

Kvantitativna analiza podrazumijeva iskazivanje rizika u očekivanim novčanim troškovima na godišnjoj razini. Većina organizacija preferira ovakav načina analize pošto im je na taj način omogućeno planiranje novčanih sredstava, a upravi se omogućava da bez tehničkih pojedinosti može donijeti odgovarajuće odluke.

Pri tom valja imati na umu da vrijednost nekih resursa nije uvijek moguće iskazati novčano, a također se kao rezultat mogu pojaviti i brojke koje ne predstavljaju realno stanje.

4.1.2. Kvalitativna analiza

Kvalitativna analiza rizika predstavlja subjektivniji pristup pri kojem se resursi, rizici i protumjere promatraju relativno obzirom na sam sustav. Za provođenje kvalitativne analize nije nužno detaljno poznavanje poslovnih procesa i njihove vrijednosti, već je dovoljan općeniti uvid u sam sustav.
Rezultat kvalitativne analize iskazuje samo relativni odnos vrijednosti šteta nastalih djelovanjem neke prijetnje i implementacije protumjera. Pri tome valja imati na umu da je ta procjena subjektivne naravi te da je kao takva podložna pogreškama.
Tablica 1 daje usporedbu kvalitativne i kvantitativne analize rizika.

Svojstvo	Kvalitativna analiza	Kvantitativna analiza
financijski prikaz	NE	DA
omjer uloženog i dobivenog	NE	DA
složenost	NE	DA
subjektivnost	DA	NE
mogućnost automatizacije	NE	DA
potrebno vrijeme	KRATKO	DUGO
potrebna količina informacija	MALA	VELIKA

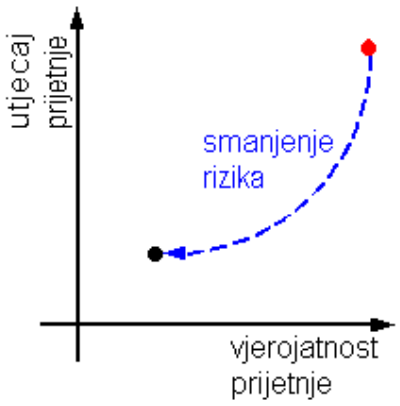
Tablica 1: Usporedba kvalitativne i kvantitativne analize rizika

4.2. Interpretacija rezultata

Analizom rizika moraju se utvrditi sljedeće činjenice:
- kritični resursi i njihova vrijednost (relativna ili novčana),
- popis mogućih prijetnji i vjerojatnost njihove pojave,
- potencijalni gubici koje uzrokuje ostvarenje prijetnje,
- preporučene protumjere i zaštita.

Na temelju dobivenih rezultata potrebno je odlučiti kakve protumjere treba poduzeti. Postoje tri mogućnosti djelovanja, koje nisu nužno međusobno isključive:
- smanjenje rizika,
- prijenos rizika i
- prihvaćanje rizika.

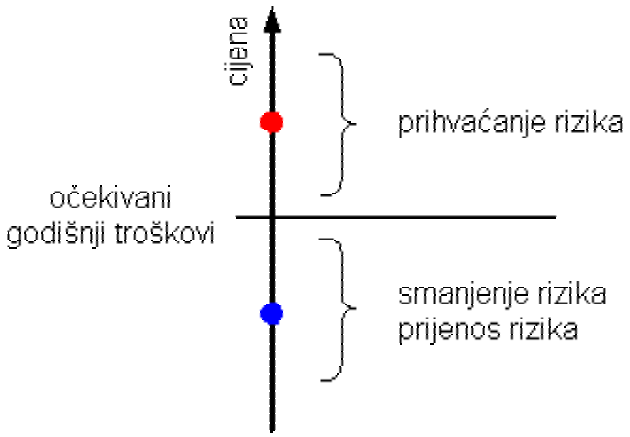
Jedini važni parametar pri odabiru načina djelovanja jest isplativost za organizaciju.



Slika 1: Postupak smanjenja rizika

Smanjenje rizika predstavlja proces u kojem se na temelju provedene analize rizika nastoje provesti odgovarajuće protumjere i implementirati sigurnosne kontrole da bi se zaštitili resursi organizacije. U

tom postupku nastoji se smanjiti vjerojatnost prijetnje i/ili njen utjecaj na organizaciju. ***Slika 1*** prikazuje proces smanjenja rizika.
Ukoliko se pokaže isplativijim, rizik je moguće prenijeti na treću stranu (npr. osiguravajuće društvo). Isto tako, moguće je da implementacija protumjera ili prijenos rizika nisu isplativi. U tom slučaju organizacija može odlučiti prihvatiti rizik, odnosno troškove koji proizlaze iz toga.
Slika 2 ilustrira način odabira odgovarajućih protumjera za zaštitu pojedinog resursa po izvršenoj analizi rizika.



Slika 2: Odabir adekvatnih protumjera

5. Sigurnosna politika

Sigurnosna politika predstavlja temelj za implementaciju informacijske sigurnosti unutar neke organizacije. Sama vrijednost sigurnosne politike, međutim, u većini organizacija potpuno je zanemarena. Najčešća pogreška koja se vrlo često pojavljuje jest implementacija tehničkih sigurnosnih rješenja, bez ikakvog strateškog planiranja, identifikacije resursa, procjene rizika ili postojanja strukturiranih dokumenata sigurnosne politike te procedura i preporuka za njenu implementaciju. Posljedica takvog načina implementacije sigurnosti jesu neefikasne i krivo usmjerene sigurnosne kontrole.
Uspješno upravljanje sigurnošću informacijskih sustava podrazumijeva izradu modularnog i hijerarhijski strukturiranog dokumenta sigurnosne politike. Dokument sigurnosne politike ne smije biti monolitni statički dokument iz više razloga. Kao prvo, različiti dijelovi dokumenta namijenjeni su različitim subjektima koji se nalaze na različitim mjestima unutar organizacijske hijerarhije. Nadalje, dokument sigurnosne politike mijenja se kontinuirano pošto se informacijski i drugi resursi koje koristi organizacija tijekom vremena mijenjaju, uvode se novi elementi ili povlače stari. Također, relativna vrijednost nekog resursa za organizaciju vremenom se može promijeniti. Konačno, svaki dio dokumenta sigurnosne politike mora biti čitljiv i bez suvišnih elemenata koji nisu bitni za onaj dio korisnika kojem je namijenjen.

5.1. Struktura

Kako je u uvodu rečeno, sigurnosna politika jest hijerarhijski strukturirani dokument koji se sastoji od više međusobno povezanih elemenata. Osnovni elementi globalnog dokumenta sigurnosne politike su sljedeći:

- politike,
- standardi,
- preporuke i
- procedure.

5.1.1. Politike

Same politike su dokumenti koji opisuju sigurnost na općenitoj razini i ne daju detaljne tehničke specifikacije za njenu konkretnu implementaciju. Osnovni element svake politike jest odluka. Politika definira smjer u kojem je potrebno razvijati implementaciju sigurnosti na pojedinoj razini. Hijerarhijski se sigurnosne politike mogu podijeliti na sljedeće:

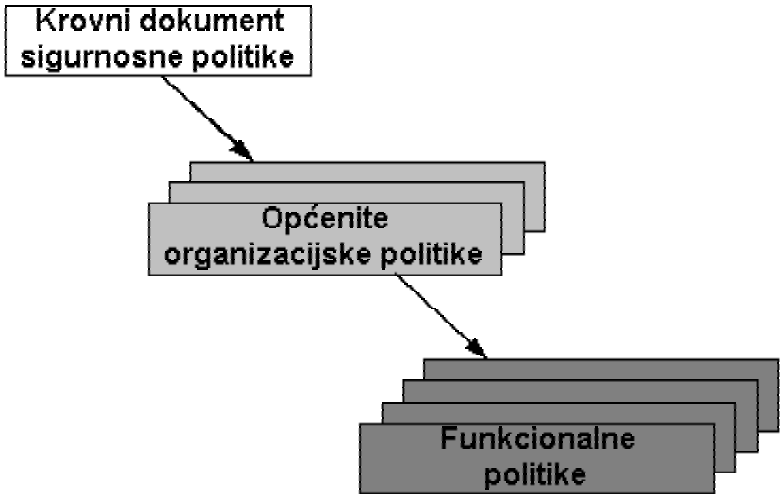
- krovni dokument sigurnosne politike,
- općenite organizacijske politike i
- funkcionalne politike.

Krovni dokument sigurnosne politike predstavlja odluku uprave i definira općeniti smjer u kojem je potrebno razvijati sigurnost. U tom dokumentu ističe se važnost informacijskog sustava za poslovanje, a on sam služi kao potpora za daljnju implementaciju informacijske sigurnosti kroz organizaciju na nižim razinama.

Na temelju krovnog dokumenta sigurnosne politike izrađuju se općenite organizacijske politike koje definiraju smjernice unutar pojedinih segmenata informacijskog sustava organizacije ili nje same.

Najnižu razinu u toj hijerarhiji zauzimaju funkcionalne politike koje identificiraju pojedine elemente sustava te daju općenite smjernice na temelju kojih se zatim kroz preporuke i procedure implementira sigurnost.

Slika 3 daje hijerarhijski pregled strukture sigurnosnih politika.



Slika 3: Hijerarhijska struktura sigurnosnih politika

5.1.2. Preporuke, procedure i standardi

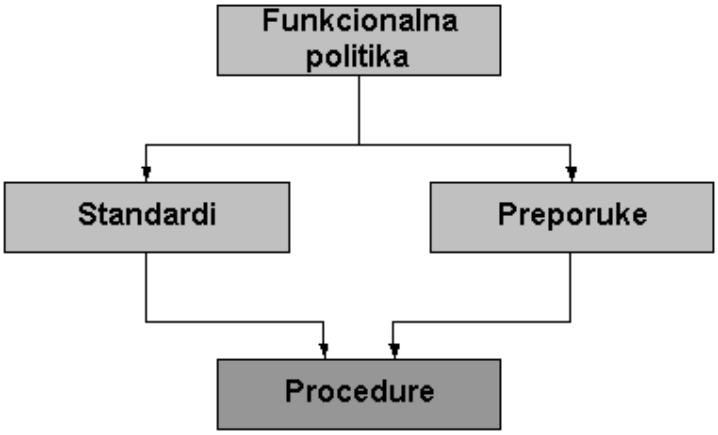
Politike definiraju smjer u kojem je potrebno razvijati informacijsku sigurnost. Konkretna implementacija sigurnosnih politika temelji se na skupu preporuka i procedura koje detaljno definiraju način na koji će se ostvariti sigurnost pojedinog elementa informacijskog sustava, uvažavajući pri tom postojeće standarde.

Ponekad je kroz same sigurnosne politike teško osigurati interoperabilnost pojedinih elemenata informacijskog sustava. Zbog toga se određuju standardi koji služe kao temelj za izradu detaljnih procedura za implementaciju sigurnosti informacijskog sustava.

Preporuke definiraju preporučene načine zaštite sustava. Implementacija mjera definiranih preporukama poželjna je, no ne i nužna, što preporuke čini fleksibilnim elementom u implementaciji sigurnosne politike. Preporuke se najčešće koriste na onim mjestima gdje sigurnost nije moguće, nije potrebno ili nije poželjno strogo definirati.

Procedure predstavljaju posljednji korak u implementaciji organizacijske sigurnosti. One egzaktno opisuju na koji način je potrebno implementirati postojeće standarde i preporuke za svaki bitni element informacijskog sustava.

Slika 4 prikazuje međusobnu povezanost sigurnosnih politika, te standarda, preporuka i procedura na kojima se temelji njihova implementacija.



Slika 4: Povezanost politika, standarda, preporuka i procedura

5.2. Izrada i implementacija sigurnosne politike

Prvi i osnovni korak pri izradi i implementaciji sigurnosne politike jest odluka uprave kojim se određuje važnost sigurnosti za poslovne procese, odnosno izrada krovnog dokumenta sigurnosne politike. Nakon toga se izrađuju općenite organizacijske politike, koje, kako je ranije rečeno, mogu slijediti organizacijsku strukturu ili organizaciju informacijskog sustava.

Kada postoje općenite sigurnosne politike može se pristupiti izradi funkcionalnih politika. Za ovaj korak vrlo je važna prethodno provedena odgovarajuća identifikacija resursa i procjena rizika. Bez toga nije moguće uopće definirati koje funkcionalne politike treba izraditi. Potpuno je besmisleno i pogrešno pristupiti izradi funkcionalnih politika za one dijelove sustava koji su potpuno nebitni ili za dijelove koji uopće ne postoje. Isto tako, nije nužno niti poželjno integrirati sve sigurnosne politike u jedan jedini dokument. Na taj način olakšava se distribucija dokumenta, eliminira se potreba za pronalaženjem pojedinih dokumenata koje se tiču pojedinih subjekata, a istovremeno se olakšava promjena i osvježavanje pojedinih politika. Također, prilikom promjena u strukturi informacijskog sustava, koje su normalne i očekivane u svakom sustavu, postojeći skup politika jednostavno se može proširiti.

Konačno, potrebno je izraditi odgovarajuće preporuke, koje treba slijediti prilikom izrade procedura za implementaciju sigurnosne politike uz uvažavanje prethodno određenih standarda koji osiguravaju interoperabilnost i kompatibilnost na razni organizacije.

5.2.1. Sustav odgovornosti

Vrlo važan aspekt prilikom implementacije sigurnosnih politika jest definicija uloga i uspostava sustava odgovornosti. Osim ranije definiranih uloga vlasnika, odgovornih osoba i korisnika, obično se koriste još termini koji se odnose na osobe zadužene za nadgledanje sustava (engl. *auditor*), te upravitelje sustava sigurnosti.

Suština definiranja uloga leži u tome što je za implementaciju sigurnosne politike nužna uspostava sustava odgovornosti, te definicija prava i obveza subjekata u sustavu. Bez toga sigurnosna politika ne može biti primijenjena u stvarnim uvjetima.

5.3. Primjena sigurnosne politike

Sigurnosne politike moguće je primijeniti na gotovo sve elemente informacijskog sustava. Pri tome uvijek valja imati u vidu stvarne i buduće potrebe organizacije. Prema ISO/IEC 17799 standardu, s aspekta sigurnosti potrebno je pokriti sljedeća područja:

- osobnu sigurnost,
- fizičku sigurnost,
- upravljanje operacijama i komunikacijama,
- kontrolu pristupa,
- razvoj i održavanje sustava,

- planiranje kontinuiranosti poslovnih procesa i
- usklađenost s zakonskim propisima.

Osobna sigurnost podrazumijeva definiranje prava i obveza korisnika sustava, njegovo obrazovanje i pravila ponašanja prilikom pojave incidenata.
Fizička sigurnost odnosi se na sigurnu implementaciju i održavanje sigurnosti vezano uz fizičke (uredi, zgrade itd.) i infrastrukturne (oprema, kabliranje, električne instalacije itd.) elemente sustava.
Upravljanje operacijama i komunikacijama treba pokriti područja razmjene informacija (razmjena putem raznih medija, elektroničke pošte, programske podrške i sl.), zaštitu od zlonamjernih programa (npr. antivirusna zaštita), rukovanje medijima za pohranu podataka, upravljanje mrežnim resursima, održavanje (*backup*) i planiranje sustava.
Kontrola pristupa treba pokriti područja pristupa korisnika i njihovih ovlasti, pristupa mrežnim uslugama, operacijskim sustavima i aplikacijama. Također trebaju biti pokriveni aspekti nadgledanja sustava, te pristupa s udaljenih lokacija.
Razvoj i održavanje sustava pokriva elemente planiranja razvoja sigurnih aplikacija, osiguranja sistemskih datoteka, te implementacije kriptografskih metoda. Također treba biti pokriveno i područje sigurnosti u razvojnim i pomoćnim procesima.
Planiranje kontinuiranosti poslovnih procesa odnosi se na upravljanje poslovnim procesom i osiguravanje njegove neprekinutosti. Ovim aspektom treba pokriti potencijalne mogućnosti ugrožavanja kontinuiteta poslovnog procesa, te razraditi planove za njegovo održavanje i ponovnu uspostavu u slučaju prekida.
Posljednji aspekt koji standard pokriva odnosi se na usklađenost sa zakonskim propisima (intelektualno vlasništvo, ugovorne obveze, zakonske obveze itd.).

5.4. Najčešće pogreške

Implementacija sigurnosne politike, odnosno sigurnosnih kontrola općenito povlači određene posljedice. Vrlo često povećanje razine sigurnosti može rezultirati negativnim utjecajem na funkcionalnost i/ili jednostavnost korištenja. Prilikom implementacije sigurnosti to svakako valja imati na umu. Ovdje je vrlo važno istaknuti da je adekvatna identifikacija resursa te procjena rizika vrlo bitna u ovom procesu, jer se samo tako mogu izdvojiti elementi informacijskog sustava prema njihovoj vrijednosti za organizaciju, te na temelju toga izraditi odgovarajuće sigurnosne politike.
Vrlo česta pogreška u organizacijama koje već imaju izrađeni dokument sigurnosne politike jest da taj dokument opisuje stanje, a ne odluku ili smjer u kojem se upravljanje sigurnosti mora razvijati. Druga pogreška jest da se postojeća sigurnosna politika u praksi uopće ne koristi, nego predstavlja dokument koji je izrađen zbog zakonskih ili drugih potreba, a ustvari nema utjecaja na stvarne procese unutar informacijskog sustava. Isto tako dokument sigurnosne politike često bude pogrešno izrađen u integralnom obliku čime je, sa strane onih kojima je namijenjen, otežano snalaženje i pronalaženje njima bitnih dijelova, dok je sa strane onih koji su zaduženi za njegovo provođenje i stalne modifikacije koje dokument moraju držati aktualnim, taj posao praktički onemogućen.

6. Zaključak

Upravljane sigurnošću informacijskog sustava zahtjevan je i odgovoran zadatak kojem se mora pristupiti analitički i detaljno. *Ad hoc* implementacija parcijalnih rješenja nije pristup kojim se rješava sigurnost informacijskog sustava organizacije, čiji se poslovni procesi u većem ili manjem dijelu oslanjaju upravo na ispravno funkcioniranje te informacijske infrastrukture.
Za kvalitetno upravljanje sigurnošću sustava potrebno je izraditi procjenu rizika, te sastaviti i implementirati odgovarajuću sigurnosnu politiku.
Identifikacijom resursa i procjenom rizika moguće je uočiti kritične, ali i druge elemente sustava i na njima primijeniti odgovarajuće sigurnosne kontrole. Osnovni razlog za procjenu rizika jest financijska isplativost, odnosno smanjenje troškova koji se mogu pojaviti u sustavu. Bez adekvatne procjene rizika implementacija sigurnosnih kontrola može biti neefikasna i financijski neopravdana.
Kod sigurnosne politike najvažnije je shvatiti da je to "živi" dokument, odnosno skup dokumenata koji mora određivati smjer u kojem se razvija upravljanje sigurnošću organizacije. Pravilna izrada sigurnosne politike podrazumijeva globalno sagledavanje kompletnog sustava, uvažavajući pri tom i rezultate analize rizika, te razvijanje odgovarajućih partikularnih procedura na temelju odabranih

standarda i preporuka. Takav pristup je jedini pravilni ukoliko se želi osigurati kompletna sigurnost za čitavu organizaciju.

Literatura

"The CISSP Prep Guide—Mastering the Ten Domains of Computer Security", Ronald L. Krutz, Russell Dean Vines, John Wiley & Sons, Inc.

"Internet Security Policy: A Technical Guide", Barbara Guttman, Robert Bagwill, NIST

International Standard ISO/IEC 17799

CISSP Security Management and Practices, Roberta Brag, http://www.informit.com/articles/index.asp