HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Upravljanje sigurnosnim rizicima

CCERT-PUBDOC-2003-10-44

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

Potreba za kvalitetno riješenim i pouzdanim sustavom upravljanja sigurnošću unutar organizacije postala je jedan od temeljnih zahtjeva za uspješno obavljane poslovnih zadataka. U vrijeme kada računalno-komunikacijska infrastruktura predstavlja okosnicu poslovanja gotovo svih modernih tvrtki i organizacija, upravljanje sigurnosnim rizicima igra iznimno važnu ulogu u procesu zaštite informacijskih resursa i poslovnih procesa.

Za proces upravljanja sigurnosnim rizikom slobodno se može reći da predstavlja temelj izgradnje sigurne i pouzdane računalne infrastrukture. Identifikacija kritičnih informacijskih resursa i određivanje pripadajućih sigurnosnih rizika, proces je koji omogućuje kvalitetnije i ekonomičnije donošenje odluka vezanih uz unaprjeđenje sigurnosti. Bez odgovarajućih analiza i kvalitetno razrađenih planova, razvoj i implementacija sigurnog računalnog okruženja vrlo je često kaotičan proces, koji rezultira brojnim propustima i nedostatcima.

U ovom dokumentu opisani su osnovni ciljevi i ideje procesa upravljanja sigurnosnim rizicima, načini njegovog provođenja, kao i tipični problemi koji se javljaju u ovom području. Veći dio dokumenta posvećen je procjeni rizika, postupku na kojem se bazira gotovo cijeli program upravljanja sigurnosnim rizikom.

2. Upravljanje sigurnosnim rizikom

Sigurnosni rizik definira se kao mogućnost realizacije nekog neželjenog događaja, koji može negativno utjecati na povjerljivost (engl. *confidentiality*), integritet (engl. *integrity)* i raspoloživost (engl. *availability*) informacijskih resursa. Pod informacijskim resursima podrazumijevaju se sva ona sredstva koja organizacija koristi u svrhu ostvarivanja svojih poslovnih ciljeva (hardver, softver, ljudski resursi, podaci i sl.). Precizna identifikacija, odnosno klasifikacija informacijskih resursa prvi je, i vrlo važan, korak procesa upravljanja sigurnosnim rizikom, budući da se na temelju njega određuje koji resursi zahtijevaju kakav tretman sa stanovišta sigurnosti. Neprikladno obavljena identifikacija resursa može cijeli proces odvesti u krivome smjeru, čime se u potpunosti gubi njegov značaj i smisao.

Upravljanje sigurnosnim rizikom (engl. *Risk Management)*, relativno je nova disciplina u području sigurnosti IT sustava, koja je proizašla iz potrebe za standardizacijom i formalizacijom postupaka vezanih uz upravljanje sigurnošću. Definira se kao proces identifikacije onih čimbenika koji mogu negativno utjecati na povjerljivost, integritet, i raspoloživost računalnih resursa, kao i njihova analiza u smislu vrijednosti pojedinih resursa i troškova njihove zaštite. Završni korak obuhvaća poduzimanje zaštitnih mjera koje će identificirani sigurnosni rizik svesti na prihvatljivu razinu, u skladu s poslovnim ciljevima organizacije.

U kojoj mjeri i na kojim mjestima će se pristupiti umanjivanju sigurnosnog rizika, odluka je prvenstveno menadžmenta, kao one funkcije koja ima mogućnost donošenja odluka i pravo raspolaganja nad budžetom organizacije. Sigurnosni rizik moguće je tretirati na nekoliko načina. Moguće ga je prihvatiti onakvim kakvim je, moguće je pristupiti njegovom umanjivanju, implementacijom odgovarajućih sigurnosnih kontrola, a moguće je i njegovo ignoriranje, odnosno prebacivanje drugim organizacijama. Spomenute tehnike biti će detaljnije opisane kasnije u dokumentu (Poglavlje 4). Donošenje odluka vezanih uz upravljanje rizikom vrlo je odgovoran i zahtjevan posao koji, osim određene razine stručnosti, zahtjeva i iznimno dobro poznavanje IT sustava i njegove funkcije.

Proces upravljanja sigurnosnim rizicima sastoji se od tri faze:

- procjena rizika (engl. *Risk Assessment*);
- umanjivanje rizika (engl. *Risk Mitigation*);
- ispitivanje i analiza (engl. *Evaluation and Assessment*).

Svaka od navedenih faza ima svoju ulogu i cilj u kompletnom programu upravljanja sigurnosnim rizikom. U nastavku dokumenta biti će detaljnije opisana svaka od faza, zajedno sa svojim osnovnim karakteristikama i specifičnostima.

3. Procjena rizika

Procjena rizika (engl. *Risk Assessment*), prva je faza procesa upravljanja sigurnosnim rizicima i predstavlja njegovu okosnicu. Cjelokupan proces upravljanja sigurnosnim rizikom uključuje identifikaciju, analizu i uklanjanje rizika, kao i njegovo periodičko ispitivanje i evaluaciju, dok je faza procjene rizika vezana isključivo uz konkretno određivanje sigurnosnog rizika, vezanog uz pojedini resurs. Detaljna analiza svih prijetnji i ranjivosti, vjerojatnosti realizacije rizika i mogućih posljedica, kao i *cost/benefit* analiza sigurnosnih kontrola za uklanjanje rizika, postupci su uključeni u ovaj proces.

Rezultati provedenog postupka procjene rizika redovito se daju na uvid menadžmentu organizacije, kao i izvještaj u kojem su izneseni detaljni podaci neophodni za donošenje odluka vezanih uz ulaganje u sigurnosna rješenja i proizvode. Na temelju dobivenih rezultata menadžment organizacije odlučuje kojim će se mjestima i u kojoj mjeri rizik reducirati, a na kojim će se mjestima primijeniti druge tehnike upravljanja rizikom (ignoriranje, prebacivanje drugim organizacijama i sl.).

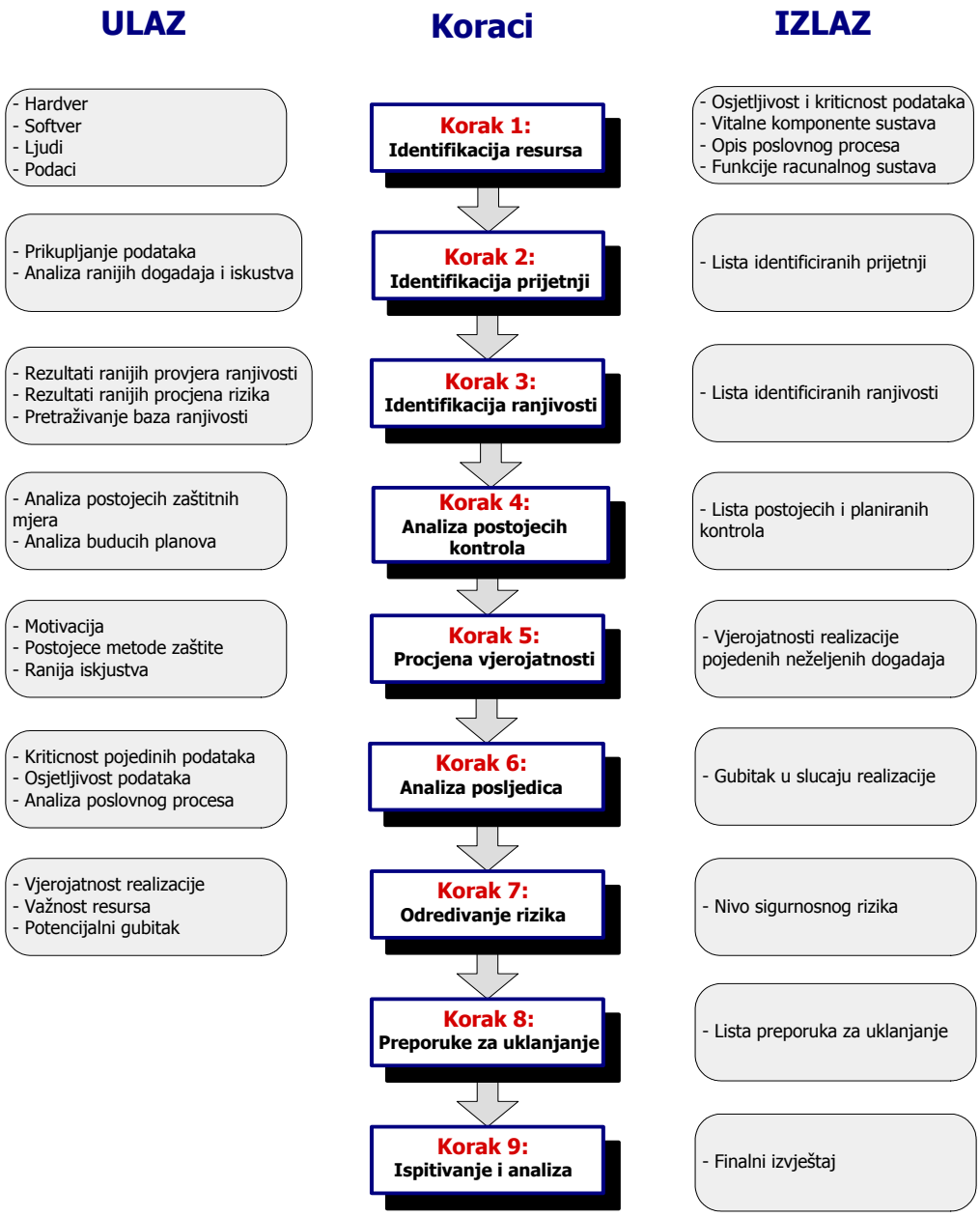
Procjena rizika vrlo je složen i zahtjevan postupak te stoga mora biti proveden profesionalno i temeljito kako bi se dobili mjerodavni podaci. Sam proces analize i procjene najbolje je delegirati sigurnosnim stručnjacima s iskustvom na području sigurnosti informacijskih sustava (po mogućnosti nezavisnim konzultantima), a rezultate procjene dati menadžmentu na temelju kojih će se donositi odgovarajuće odluke.

Proces procjene rizika sastoji se od devet koraka:

- **Korak 1:** Identifikacija i klasifikacija resursa (engl. *Asset Identification*);
- **Korak 2:** Identifikacija prijetnji (engl. *Threat identification*);
- **Korak 3:** Identifikacija ranjivosti (engl. *Vulnerability Identification*);
- **Korak 4:** Analiza postojećih kontrola (engl. *Control Analysis*);
- **Korak 5:** Vjerojatnost pojave neželjenih događaja (engl. *Likelihood Determination*);
- **Korak 6:** Analiza posljedica (engl. *Impact Analysis*);
- **Korak 7:** Određivanje rizika (engl. *Risk Determination*);
- **Korak 8:** Preporuke za umanjivanje (engl. *Control Recommendation*);
- **Korak 9:** Dokumentacija (engl. *Result Documentation*).

Na sljedećoj slici (

Slika *1*) priložen je dijagram na kojem je prikazan slijed navedenih faza sa ulaznim i izlaznim parametrima. Treba napomenuti da se koraci 2,3 i 4 mogu provoditi u paraleli nakon što je dovršen korak 1.



Slika 1: Procjena rizika - dijagram

Iako određivanje sigurnosnog rizika zahtjeva provođenje svih ovih koraka, sam rizik matematički se može promatrati kao funkcija tri parametra: prijetnji, ranjivosti i vrijednosti resursa (*Slika 2*).

$$Rizik = f(\Pr ijetnje, Ranjivosti, Vrijednostresursa)$$

Što je sustav više izložen prijetnjama, što je veći broj ranjivosti i što je resurs značajniji za organizaciju, to je i sigurnosni rizik veći. Naravno, jasno je da se sigurnosni rizik nikada neće uklanjati umanjivanjem vrijednosti resursa, već implementacijom odgovarajućih sigurnosnih kontrola koje će utjecati na parametre ranjivosti i prijetnji.

Vrijednost resursa koji je ovdje naveden kao jedan od parametara o kojemu ovisi razina sigurnosnog rizika, može se promatrati i na drukčiji način. Naime, vrlo često se umjesto vrijednosti resursa kao treći parametar u obzir uzima potencijalni gubitak za organizaciju u slučaju gubitka ili neraspoloživosti resursa o kojem se govori. Bez obzira o kojem je od dva navedena parametra riječ, ishod je identičan, budući da su vrijednost resursa i posljedice u slučaju gubitka dvije izravno vezane veličine.

Slika 2: Sigurnosni rizik

U nastavku dokumenta biti će ukratko opisan svaki od navedenih koraka sa svojim specifičnostima.

3.1. Identifikacija i klasifikacija resursa

Prvi korak u postupku procjene rizika je identifikacija, odnosno klasifikacija informacijskih resursa. U ovom koraku potrebno je identificirati sve one resurse koji predstavljaju značaj za organizaciju te im pridijeliti odgovarajuću vrijednost. Ukoliko postoji mogućnost, svakom resursu potrebno je pridijeliti konkretnu novčanu vrijednost, budući da to uvelike može pridonijeti kvaliteti rezultata cijelog postupka.

Identifikaciju i pridjeljivanje vrijednosti pojedinim resursima potrebno je obaviti kako bi se u konačnici implementirale samo one sigurnosne kontrole koje su financijski isplative. Jasno je da nema smisla uložiti 50.000kn u zaštitu resursa koji vrijedi 30.000kn. Takvo ulaganje bilo bi potpuno neopravdano i predstavljalo bi dodatni gubitak.

Postupku pridjeljivanja vrijednosti resursima potrebno je posvetiti posebnu pažnju, budući da loše procjene u ovom slučaju mogu cijeli proces odvesti u krivom smjeru. Prilikom određivanja vrijednosti potrebno je u razmatranje uzeti brojne druge faktore, osim inicijalnih troškova njegove nabave. Neki od faktora koje je potrebno uzeti u obzir su:

- troškovi razvoja;
- troškovi održavanja i administracije;
- troškovi edukacije;
- vrijednost koju isti resurs predstavlja konkurentskim organizacijama;
- troškovi zamjene, nadogradnje i sl.

Neki od tipičnih resursa koji predstavljaju važnost za organizaciju su:

- hardver;
- softver;
- podaci;
- ljudski resursi i sl.

3.2. Identifikacija prijetnji

Pod sigurnosnim prijetnjama (engl. Threat) smatraju se svi oni neželjeni faktori koji se mogu negativno odraziti na integritet, povjerljivost i dostupnost resursa. Izvori prijetnji (engl. *threat agents*) mogu se podijeliti u dvije osnovne skupine:

- *Namjerne* – oni izvori koji ciljano iskorištavaju nedostatke u sustavima u svrhu ostvarivanja neovlaštenog pristupa. U ovu skupinu najčešće spadaju neovlašteni korisnici, razni maliciozni programi (crvi, virusi…) i sl.
- *Nenamjerne* - oni izvori koji rezultiraju slučajnim iskorištavanjem ranjivosti u sustavu, npr. elementarne nepogode kao što su požari, poplave, potresi, udari groma i sl.

U okviru procjene rizika vrlo je važno generirati iscrpnu listu svih onih prijetnji, namjernih i nenamjernih, koje predstavljaju potencijalnu opasnost za informacijski sustav.
Prilikom identifikacije prijetnji poželjno je u obzir uzeti sve ranije incidente i ostale neželjene događaje, motive koji mogu biti podloga za provođenje napada, lokaciju na kojoj se nalaze resursi te ostale faktore koji na bilo koji način predstavljaju prijetnju za IT sustav. Vrlo često od koristi mogu biti i razgovori sa administratorima sustava ili drugim osobljem, koje je u svakodnevnom kontaktu sa komponentama sustava.
Neke od prijetnji koje su tipične za informacijske sustave uključuju:

- neovlaštene korisnike,
- maliciozne programe (virusi, crvi, trojanski konji,…),
- elementarne nepogode (poplave, potresi, požari,…),
- korisničke pogreške (namjerne i slučajne),
- krađu,
- greške u programiranju (namjerne i slučajne),
- neispravno rukovanje resursima,
- industrijsku špijunažu,
- interne napade, i sl.

Za svaku od identificiranih prijetnji potrebno je odrediti povezanost sa resursima organizacije, motive koji stoje iza svake od njih te načine na koje prijetnje mogu utjecati na poslovne procese. Što je detaljnije razrađena lista prijetnji to je jednostavnije odrediti sigurnosni rizik povezan sa odgovarajućim resursom.

3.3. Identifikacija ranjivosti

Pod pojmom ranjivosti (engl. *Vulnerability*), smatraju se svi propusti i slabosti u sustavu sigurnosti koji omogućuju provođenje neovlaštenih aktivnosti. Ranjivosti mogu biti posljedica pogrešaka u procesu dizajna ili implementacije sustava, kao i propusta u sustavu provođenja sigurnosnih pravila i procedura. Iako se ranjivosti najčešće povezuju uz greške u programskom kodu, mogući su i brojni drugi primjeri, kao što su površno implementirana fizička sigurnost, nepoznavanje i neprikladan odabir tehnologija i alata, propusti u održavanju sustava i sl.
Prema izrazu za sigurnosni rizik, danom na samom početku ovog poglavlja (Poglavlje 3), za uspješno određivanje sigurnosnog rizika potrebno je također identificirati i sve ranjivosti, odnosno sigurnosne propuste u sustavu. Bez adekvatne analize ranjivosti, gotovo je nemoguće pouzdano određivanje sigurnosnog rizika. Ovisno o broju i karakteru ranjivosti u sustavu, sigurnosni rizik može biti veći ili manji. Implementacijom sigurnosnih kontrola kojima će se umanjiti broj ranjivosti u sustavu, izravno je moguće utjecati na umanjivanje sigurnosnog rizika.
Kada se govori o procjeni rizika, iznimno je važno da se ranjivosti analiziraju u kombinaciji sa identificiranim prijetnjama, budući da su ova dva parametra međusobno povezana. Ukoliko ne postoji prijetnja koja bi iskoristila određenu ranjivost, tada ne postoji niti sigurnosni rizik. Tamo gdje nema rizika ne isplati se ulagati u zaštitu, što je osnovni cilj postupka upravljanja sigurnosnim rizikom: implementacija samo onih zaštitnih mjera koje će biti opravdane i smislene u pogledu zaštite poslovnih ciljeva organizacije.
U sljedećoj tablici (*Tablica 1*), dan je primjer nekih od ranjivosti koje su tipične za IT sustave, zajedno s prijetnjama koje su vezane uz svaku od njih.

Ranjivost	**Prijetnja**
Sigurnosni propusti u programskom kodu	Neovlašteni korisnici Maliciozni programi Nezadovoljni zaposlenici Teroristi
Neprikladna konfiguracija vatrozida	Neovlašteni korisnici Maliciozni programi Industrijska špijunaža
Nedostatak protupožarne zaštite	Požar
Nedostatak antivirusne zaštite	Maliciozni programi (virusi, crvi, trojanski konji).

Ranjivost	Prijetnja
Nekontrolirano korištenje modema	Neovlašteni korisnici Maliciozni programi Bivši i nezadovoljni zaposlenici

Tablica 1: Prijetnje i ranjivosti

Ono što se nameće kao osnovno pitanje kada se raspravlja o identifikaciji i analizi ranjivosti je način na koji je najbolje provesti njihovu detaljnu i temeljitu analizu. Neki od mogućih pristupa su:

- analiza rezultata ranije provedenih procjena rizika (ukoliko takvi postoje),
- analiza internih izvještaja i dokumentacija vezanih uz ispitivanje, analizu i unaprjeđenje sigurnosti,
- provođenje specijaliziranih sigurnosnih ispitivanja (*Vulnerability Scanning, Pentration Testing, Application Testing i* sl.*),*
- pretraživanje javnih baza ranjivosti (BUGTRAQ, CERT, ...),
- intervjui sa zaposlenicama i sistem administratorima itd...

Rezultat ove faze treba biti detaljna lista ranjivosti prisutnih u sustavu, kao i njihova povezanost sa prijetnjama identificiranim u prethodnom koraku.

3.4. Analiza postojećih kontrola

U ovom koraku cilj je analizirati one sigurnosne kontrole koje su već implementirane ili koje se namjeravaju implementirati u svrhu zaštite informacijskih resursa. Ukoliko se želi izračunati vjerojatnost iskorištavanja pojedine ranjivosti od strane identificiranih prijetnji, što je sljedeći korak procesa procjene rizika, potrebno je u obzir uzeti sve postojeće kontrole prisutne u sustavu.

Vrlo je mala vjerojatnost da će određena slabost ili nedostatak biti iskorišteni, ukoliko su implementirane kvalitetne sigurnosne kontrole ili ukoliko postoji mali interes za njenim iskorištavanjem. Sustavi koji barataju povjerljivim podacima kao što su npr. brojevi kreditnih kartica, obračuni plača i sl., predstavljaju puno veći izazov za neovlaštene korisnike u odnosu na ostale sustave koji rukuju manje povjerljivim podacima.

Sigurnosne kontrole mogu biti tehničke i ne-tehničke prirode. Pod tehničkim sigurnosnim kontrolama smatraju se sve one kontrole koje su implementirane u oblik hardvera, softvera ili nekog drugog sličnog rješenja (npr. vatrozidi, IDS sustavi, antivirusna zaštita, sustavi kontrole pristupa i sl.).

Pod ne-tehničkim kontrolama smatraju su kontrole poput sigurnosnih politika, preporuka i procedura i koje su najčešće rezultat usmene ili pismene predaje.

Još jedna od podjela, koja je više prisutna u krugovima koji se bave računalnom sigurnošću, je ona koja sigurnosna rješenja i mehanizme dijeli na:

- **Preventivne** (engl. *Prevention*) – ona rješenja koja djeluju preventivo u smislu sprječavanja neovlaštenih aktivnosti (npr. antivirusni programi, vatrozidi, kontrola pristupa, i sl.)
- **Detekcijske** (engl. *Detection*) – sustavi koji omogućuju detekciju neovlaštenih aktivnosti (npr. IDS sustavi, alati za provjeru integriteta, i sl.);
- **Reakcijske** (engl. *Reaction*) – oni mehanizmi koji pomažu pri reakciji na detektirane neovlaštene aktivnosti (npr. forenzička analiza);

Rezultat ovog koraka je lista postojećih ili predviđenih sigurnosnih kontrola kojima je cilj zaštiti informacijske resurse organizacije.

3.5. Vjerojatnosti realizacije

Sljedeći korak u procesu procjene rizika je određivanje vjerojatnosti iskorištavanja pojedine ranjivosti od strane pripadajućih sigurnosnih prijetnji. Neki od čimbenika koje je ovdje potrebno uzeti u obzir su:

- motivacija i interes izvora prijetnji,
- karakter ranjivosti,
- prisutnost i kvaliteta postojećih sigurnosnih kontrola.

Vjerojatnost iskorištavanja ranjivosti od strane određenog izvora prijetnji najbolje je izraziti stupnjevito: npr. visoki, srednji i niski stupanj, pri čemu svaki od definiranih stupnjeva ima određeni značaj i smisao.

U sljedećoj tablici (*Tablica 2*) dan je primjer jedne takve podjele, s time da je moguće ići i na precizniju podjelu, ovisno o potrebama.

Vjerojatnost	Definicija
Visoka	Izvor prijetnje je posebno motiviran za iskorištavanje ranjivosti s obzirom na mogućnost dolaska do povjerljivih podataka. Postojeće sigurnosne kontrole su nedovoljne ili sadrže slabosti koje omogućuju zaobilaženje definiranih sigurnosnih mjera.
Srednja	Izvor prijetnje je djelomično motiviran. Iako postoje mogućnosti za iskorištavanje ranjivosti postojeće kontrole to otežavaju.
Niska	Izostanak motivacije za iskorištavanje ranjivosti. Sigurnosne kontrole kvalitetno su implementirane i iskorištavanje ranjivosti prilično je otežano.

Tablica 2: Vjerojatnost iskorištavanja ranjivosti

Rezultat ovog koraka sadrži vjerojatnosti iskorištavanja pojedinih ranjivosti identificiranih u prethodnom koraku, s obzirom na navedene prijetnje.

3.6. Analiza posljedica

Sljedeći vrlo važan korak u procesu procjene rizika je analiza posljedica, odnosno mogućih gubitaka u slučaju iskorištavanja pojedine ranjivosti. Ovaj korak iznimno je važan, budući da izravno utječe na razinu sigurnosnog rizika (Poglavlje 3). Prilikom provođenja ovog koraka potrebno je voditi računa o sljedećim elementima:

- namjena i uloga resursa u poslovnom procesu (funkcija koju resurs ima u poslovnom procesu organizacije),
- kritičnost resursa (značaj za organizaciju),
- osjetljivost podataka i resursa (povjerljivost).

Podatke o navedenim parametrima moguće je najjednostavnije dobiti analizom postojećih dokumentacija, kao što je npr. izvještaj o neželjenim utjecajima na poslovni proces (engl. ***B**ussines **I**mpact **A**nalysis* - BIA).

***B**ussines **I**mpact* analiza proces je kojim se identificiraju i analiziraju neželjene posljedice za organizaciju u slučaju nepredviđenih događaja kao što su npr. elementarne nepogode, računalni incidenti i sl., kao i definiranje metoda koje omogućuju njihovo mjerenje i prikazivanje.

Ukoliko takva dokumentacija nije dostupna, osjetljivost i kritičnost podataka moguće je odrediti na temelju zaštitnih mjera koje je potrebno implementirati kako bi se osigurao njihov integritet, povjerljivost i raspoloživost, tri osnovna principa računalne sigurnosti. Budući da je vlasnik resursa ili podataka najodgovorniji u pogledu određivanja njihove osjetljivosti ili kritičnosti, intervju s korisnicima i administratorima sustava također može pomoći.

Analiza gubitaka vrlo je kompleksan i zahtjevan posao. Osim opipljivih posljedica koje se manifestiraju kao financijski gubitak, u obzir je potrebno uzeti i druge čimbenike, kao što su gubitak reputacije i kredibiliteta i sl.

Potencijalne gubitke također je moguće kategorizirati u stupnjeve od kojih svaki ima određeni značaj (*Tablica 3*).

Gubitak	Definicija
Visok	Iskorištavanje ranjivosti može rezultirati: – trajnim gubitkom ili uništenjem resursa, – ozbiljnim ugrožavanjem poslovnih ciljeva i misije organizacije, – ozbiljnim ugrožavanjem ljudskih resursa.
Srednji	Iskorištavanje ranjivosti može rezultirati: – djelomičnim gubitkom ili uništenjem resursa, – djelomičnim narušavanjem poslovnih ciljeva i misije organizacije, – djelomično ugrožavanje ljudskih resursa.
Nizak	Iskorištavanje ranjivosti može rezultirati: – lakšim oštećenjem resursa, – primjetnim narušavanjem poslovnih ciljeva i misije organizacije.

Tablica 3: Potencijalni gubici

Prilikom analize i određivanja potencijalnih gubitaka, u obzir treba razmotriti prednosti i nedostatke kvantitativne, odnosno kvalitativne analize. Radi se o dva različita pristupa koja imaju identičan cilj, ali se razlikuju u načinu prikaza rezultata.

Osnovna prednost kvalitativne analize je ta što daje jasne i pregledne rezultate o kritičnim komponentama sustava koje zahtijevaju hitnu reakciju u smislu uklanjanja identificiranih ranjivosti. Nedostatak iste je taj što rezultati ne sadrže konkretne brojeve, niti bilo kakve druge mjerljive veličine koje bi olakšale analizu dobiti i gubitka (engl. *cost/benefit* analiza).

Za razliku od kvalitativne, kvantitativna analiza rezultira konkretnim brojkama i veličinama, koje olakšavaju planiranje troškova i donošenje odluka vezanih uz ulaganje u sigurnosna rješenja. Najčešći problem kvantitativne analize je taj što iste vrlo često rezultiraju brojnim izračunima i kalkulacijama, koje mogu biti teške za interpretaciju. Iskustva pokazuju da se najbolji rezultati dobivaju korištenjem kombinacije oba pristupa, pri čemu se nastoje što više iskoristi prednosti svakog od njih.

Prilikom procjene gubitaka vrlo je često potrebno u obzir uzeti i dodatne faktore kao što su:

- analiza učestalosti iskorištavanja pojedinih ranjivosti od strane identificiranih prijetnji u određenom periodu (npr. na godišnjoj bazi),
- aproksimativni troškovi u slučaju realizacije pojedinog neželjenog događaja itd…

3.7. Određivanje sigurnosnog rizika

Ključni korak cijelog procesa je određivanje samog sigurnosnog rizika. Rizik je potrebno odrediti za sve parove prijetnja/ranjivost, pri čemu u obzir treba uzeti sljedeće elemente:

- vjerojatnost iskorištavanja pojedine ranjivosti od strane pripadajuće prijetnje,
- posljedice u slučaju uspješne realizacije,
- kvaliteta i pouzdanost postojećih i planiranih sigurnosnih kontrola.

Za određivanje i analizu sigurnosnog rizika poželjno je kreirati matricu sigurnosnog rizika, koja će biti opisana u nastavku poglavlja.

Razine sigurnosnog rizika moguće je najjednostavnije odrediti na temelju podataka i tablica koje su proizašle iz dva prethodna koraka: analize vjerojatnosti realizacije (Tablica 2) i analize potencijalnih gubitaka (Tablica 3). Na temelju ovih podataka moguće je kreirati matricu rizika koja će opisivati različite razine sigurnosnog rizika prisutne u sustavu. Primjer jedne takve matrice dan je u nastavku (*Tablica 4*).

Vjerojatnost realizacije	Posljedice (Gubici)		
	Visoki (10)	Srednji (50)	Niski (100)
Visoka (1.0)	Nizak 10 x 1.0=10	Srednji 50 x 1.0=50	Visok 100 x 1.0=100
Srednja (0.5)	Nizak 10 x 0.5=5	Srednji 50 x 0.5 =25	Srednji 100 x 0.5=50
Niska (0.1)	Nizak 10 x 0.1=1	Nizak 50 x 0.1=5	Nizak 100 x 0.1=10

Skala sigurnosnog rizika	
Visok rizik	50 –100
Srednji rizik	10 – 50
Nizak rizik	1 - 10

Tablica 4: Matrica i skala sigurnosnog rizika

Matrica prikazana na prethodnoj tablici veličine je 3x3, što je posljedica odabranog načina stupnjevanja u koracima 5 i 6. Ukoliko postoji potreba moguće je odabrati i precizniju podjelu, što će rezultirati i većim brojem razina sigurnosnog rizika (npr. vrlo niski, niski, srednji, visok, iznimno visok). Iznimno visok rizik može predstavljati one situacije koje zahtijevaju hitnu reakciju pa čak i isključivanje sustava.

Način numeriranja pojedinih razina također je proizvoljan i moguće ga je prilagoditi potrebama. U ovome primjeru, za označavanje vjerojatnosti odabrane su tri razine (1.0 – vrlo vjerojatno, 0.5 – 50% vjerojatno i 0.1 – vrlo malo vjerojatno), isto kao i za označavanje potencijalnih gubitaka (100 – iznimno velik gubitak, 50 – srednji gubitak, 10 – maleni gubici).

3.8. Preporuke za umanjivanje rizika

Nakon što je identificiran sigurnosni rizik za pojedine resurse, kao zadnji korak ovog postupka je analiza i davanje preporuka za umanjivanje identificiranog sigurnosnog rizika.
Cilj ovog koraka je analiza mogućih načina zaštite u svrhu umanjivanja rizika, odnosno njegovog svođenja na prihvatljivu razinu. Prilikom davanja preporuka za implementaciju sigurnosnih kontrola potrebno je voditi računa o sljedećim faktorima:

- pouzdanost i kvaliteta kontrola;
- troškovi implementacije i održavanja;
- sigurnosna politika organizacije;
- pravna ograničenja;
- globalni utjecaj na poslovanje;
- navike i moguće reakcije korisnika i sl.;

Preporuke za implementaciju sigurnosnih kontrola mogu se promatrati kao krajnji rezultat procesa procjene rizika i kao ulazni parametri za sljedeću fazu koja uključuje analizu i evaluaciju danih preporuka te njihovu implementaciju prema prioritetima i mogućnostima organizacije (Poglavlje 4).
Implementirane će biti samo one preporuke koje će se nakon *cost/benefit* analize, provedene u sklopu sljedeće faze, pokazati opravdanima i isplativima. Pritom je također potrebno analizirati i ostale faktore koji utječu na funkcionalnost, ostvarljivost i isplativost sigurnosnih kontrola.

3.9. Završna dokumentacija

Nakon što su uspješno provedeni svi koraci procesa procjene rizika, potrebno je izraditi završnu dokumentaciju u kojoj će biti izneseni dobiveni rezultati. Prilikom izrade dokumentacije treba imati na umu da se ona isporučuje menadžmentu organizacije, koji na temelju iznesenih rezultata donosi odluke o tome koji će se rizik umanjivati i na koji način, a koji će se prihvatiti onakvim kakav je.
Izvještaj mora biti jasan i pažljivo strukturiran, kako bi rezultati bili što pregledniji i jednostavniji za interpretaciju.

4. Umanjivanje rizika

Umanjivanje rizika druga je faza procesa upravljanja sigurnosnim rizikom, u kojoj se analiziraju, evaluiraju, a kasnije i implementiraju odgovarajuće sigurnosne kontrole.
Sigurnosni rizik nikada se ne uklanja u potpunosti, budući da to nema smisla, a vrlo često je i nemoguće. Potpuno uklanjanje rizika vrlo je skupo i vrlo često neopravdano. Rizik se umanjuje u onoj mjeri koja će zadovoljiti potrebe i ciljeve organizacije. Na koji će se način i u kojoj mjeri umanjivati rizik, odluka je menadžmenta organizacije i donosi se na temelju detaljne evaluacije ponuđenih rješenja.
Ideja je da se implementiraju ona rješenja koja su financijski najprihvatljivija, ona koja će rezultirati što kvalitetnijim i što pouzdanijim sigurnosnim kontrolama, s minimalnim utjecajem na misiju i poslovne procese organizacije.

4.1. Opcije za umanjivanje rizika

Postoji nekoliko različitih načina na koje je moguće reagirati na identificirane sigurnosne rizike. To su:

- ***Umanjivanje rizika*** – pristup koji podrazumijeva implementaciju odgovarajućih sigurnosnih kontrola s ciljem umanjivanja identificiranog sigurnosnog rizika.
- ***Transfer rizika*** – u ovom slučaju se rizik i troškovi u slučaju njegove realizacije prebacuje nekoj drugoj organizaciji (engl. *outsourcing*);
- ***Prihvaćanje rizika*** – postupak kojim se identificirani rizik prihvaća kao takav bez implementacije ikakvih sigurnosnih kontrola. Ukoliko *cost/benefit* analize pokažu da je veći trošak ulagati u zaštitu resursa, nego što predstavlja njegov gubitak, tada se primjenjuje ovaj pristup. Odluka o prihvaćanju rizika povlači veliku odgovornost, i redovito zahtjeva pismeno izvješće o tome tko je odgovoran i zašto kontrole nisu implementirane;

– ***Odbacivanje rizika*** – pristup koji podrazumijeva potpuno zanemarivanje sigurnosnog rizika. Opovrgavanje ili svjesno ignoriranje rizika u nadi da on nikada neće biti realiziran potpuno je neprihvatljiv pristup i ne smije se provoditi niti u jednom slučaju.

Koji će se od opisanih pristupa primijeniti ovisi o odlukama menadžmenta organizacije.

Umanjivanje rizika pristup je koji se primjenjuje u većini situacija. Implementacijom odgovarajućih sigurnosnih kontrola i mehanizama, prihvatljivih sa financijskog i tehničkog stanovišta, sigurnosni rizik se svodi na prihvatljivu razinu.

Rizik koji ostaje nakon implementacije sigurnosnih kontrola naziva se **rezidualnim rizikom** i on podrazumijeva sve one prijetnje i ranjivosti za koje se smatra da ne zahtijevaju dodatni tretman u pogledu umanjivanja postojećeg rizika.

Prisutnost rezidualnog rizika posljedica je provedenih *cost/benefit* analiza kojima je ustanovljeno da su troškovi zaštite veći od troškova u slučaju njegove realizacije.

4.2. Metodologija rukovanja rizicima

Kao što je već ranije spomenuto, prilikom implementacije sigurnosnih kontrola potrebno je držati se sljedećeg pravila: rizik se uklanja prvenstveno prema prioritetu, pri čemu se implementiraju ona rješenja koja su financijski najprihvatljivija; ona koja će rezultirati što kvalitetnijim i što pouzdanijim sigurnosnim kontrolama sa minimalnim utjecajem na misiju i poslovne procese organizacije.

Donošenje odluka prema spomenutom pravilu nije nimalo jednostavan zadatak, pogotovo ukoliko se radi o kompleksnim sustavima s velikim brojem korisnika. Umanjivanju rizika potrebno je pristupiti metodološki, s dobro razrađenim i evoluiranim rješenjima.

U nastavku poglavlja opisano je sedam faza čije provođenje rezultira kvalitetnijom i efikasnijom implementacijom sigurnosnih kontrola.

4.3. Korak 1: Određivanje prioritetnih akcija

Na temelju rezultata prikupljenih u fazi procjene rizika, potrebno je donijeti odluke o implementaciji onih sigurnosnih kontrola koje će biti u skladu s prioritetima organizacije. Na mjestima na kojima je identificiran sigurnosni rizik visoke razine, neprihvatljiv u pogledu izvršavanja poslovnih ciljeva organizacije, potrebno je prvo krenuti sa implementacijom sigurnosnih kontrola za reduciranje rizika.

Određivanje liste prioriteta posebno je važan korak kako bi se sigurnosni rizik najprije uklonio na onim mjestima gdje je to prijeko potrebno. Treba shvatiti da neprikladan odabir aktivnosti, prilikom implementacije sigurnosnih kontrola, može kritične komponente sustava nepotrebno dugo ostaviti izloženim različitim sigurnosnim prijetnjama.

Upravo je stoga vrlo važno da se kao prvi korak postupka umanjivanja sigurnosnog rizika napravi lista prioritetnih zadataka, kojom će se definirati redoslijed uklanjanja sigurnosnog rizika prema kritičnosti.

4.4. Korak 2: Evaluacija preporučenih sigurnosnih kontrola

U ovom koraku potrebno je detaljno analizirati preporuke koje su dobivene kao rezultat osmog koraka procesa procjene rizika (Preporuke za umanjivanje rizika, Poglavlje 3.8). Neke od preporuka mogu iz određenih razloga biti neprikladne ili neizvedive za pojedinu organizaciju ili informacijski sustav. Ograničenja mogu biti raznolika; od onih tehničkih, pa do onih pravnih kao što su zakonske regulative u državi u kojoj organizacija ili tvrtka djeluje.

U ovom smislu potrebno je provesti studiju izvedivosti i efikasnosti kojom će se utvrditi koje su od preporuka prihvatljive i izvedive, a koje ne. Prilikom provođenja analize u obzir treba uzeti kompatibilnost sa ranijim rješenjima i proizvodima, edukaciju korisnika, poslovne ciljeve, u kolikoj se mjeri rizik umanjuje implementacijom preporučenih kontrola i sl.

4.5. Korak 3: Analiza dobivenog i uloženog

Ono što je sa stanovišta menadžmenta najvažnije prilikom donošenja odluka o implementaciji sigurnosnih kontrola i mehanizama je analiza uloženog i dobivenog (engl. *cost/benefit analysis*). Cilj ovog koraka je da se analiziraju i evaluiraju sva moguća rješenja, te da se u skladu sa budžetom i mogućnostima organizacije odaberu ona koja će dati najbolje rezultate.

Slično kao i kod procjene rizika, *cost/benefit* analiza može biti kvantitativna i kvalitativna. Bez obzira o kojem se od navedenih pristupa radi, cilj je isti: pokazati da se implementacija odgovarajućih sigurnosnih kontrola isplati u odnosu na potencijalne gubitke u slučaju realizacije pojedinog rizika.
Prilikom razmatranja mogućnosti novih sigurnosnih kontrola i mehanizama u okviru analize dobivenog i uloženog, potrebno je u razmotriti sljedeće:

- analiza utjecaja novih kontrola na organizaciju i njene poslovne ciljeve,
- analiza posljedica u slučaju ako se predviđene kontrole NE implementiraju,
- procjena troškova implementacije:
  - troškovi hardvera i softvera,
  - troškovi uvođenja novih politika, procedura i preporuka,
  - troškovi zapošljavanja dodatnog osoblja za rukovanje sustavom,
  - troškovi obuke,
  - troškovi održavanja i sl.

Rezultat ovog koraka je *cost/benefit* analiza koja opisuje dobitke i gubitke u slučaju implementacije pojedinih kontrola, odnosno bez njihove implementacije.

4.6. Korak 4: Odabir sigurnosnih kontrola

Na temelju rezultata *cost/benefit* analize provedene u prethodnom koraku, menadžment organizacije mora donijeti konačnu odluku o implementaciji najisplativijih i najefikasnijih kontrola.
Rezultat ovog koraka je lista sigurnosnih kontrola i mehanizama čijom će se implementacijom dobiti najučinkovitiji rezultati u pogledu zaštite informacijskih resursa i ciljeva organizacije.

4.7. Korak 5: Podjela odgovornosti

U sklopu ovog koraka potrebno je odabrati stručnjake (interne ili eksterne) sa potrebnim znanjima i iskustvima, koji će biti zaduženi za implementaciju potrebnih kontrola. Pritom je potrebno definirati sve zadatke te raspodijeliti odgovornosti kako bi proces implementacije tekao sa što manje problema i nepredviđenih događaja. Za uspješnu realizaciju ciljeva, podjela odgovornosti i zaduženja mora biti što jasnija.
Rezultat ovog koraka je lista zaduženja i odgovornosti vezanih uz implementaciju odabranih kontrola.

4.8. Korak 6: Izrada plana za implementaciju sigurnosnih kontrola

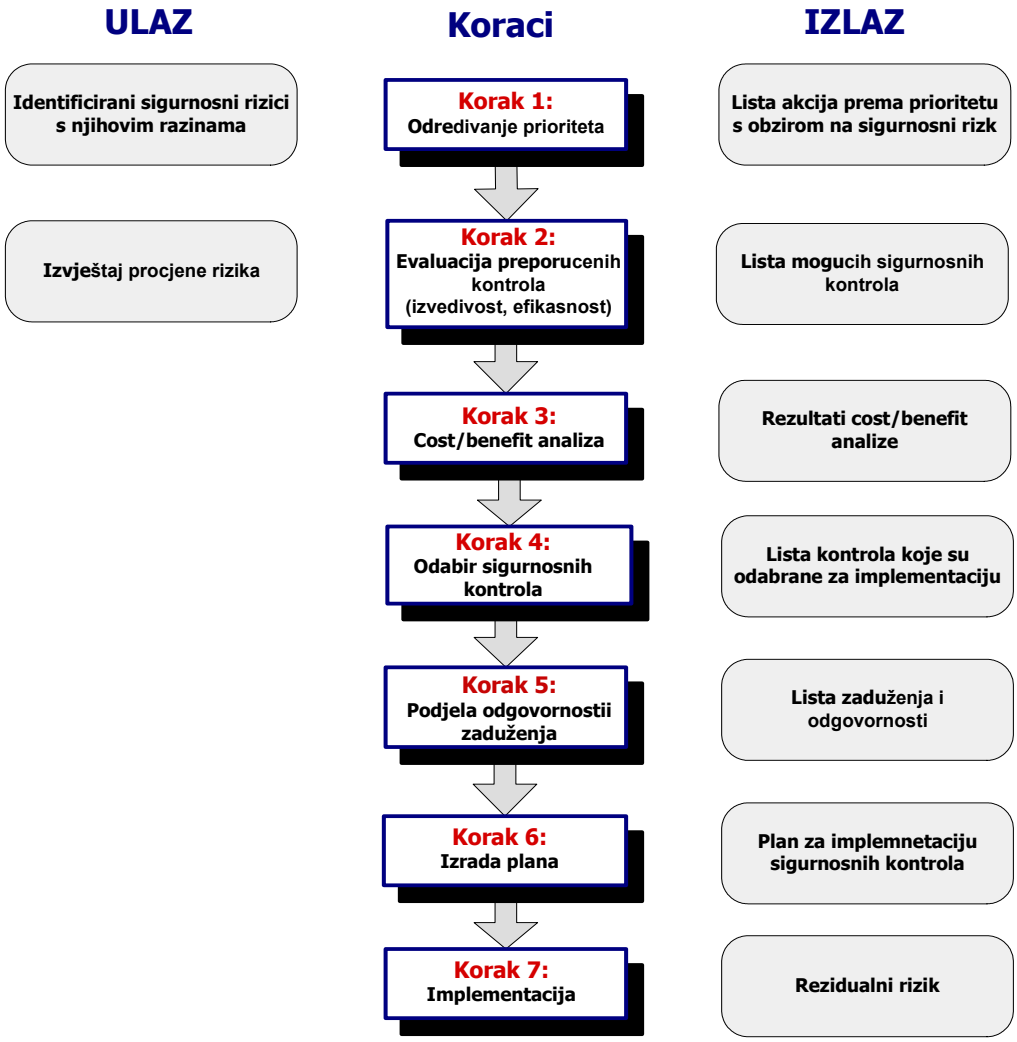
Nakon odabranih kontrola potrebno je izraditi temeljiti plan koji će omogućiti njihovu implementaciju. Takav plan trebao bi minimalno uključivati sljedeće informacije:

- identificirani sigurnosni rizik za svaku kombinaciju prijetnje i ranjivosti i njegovu razinu,
- lista preporučenih kontrola na temelju provedene procjene rizika,
- prioritet akcija tako da se svakoj od njih pridijeli odgovarajuća oznaka koja opisuje njen prioritet,
- lista odabranih kontrola,
- datum početka implementacije,
- datum završetka implementacije,
- odgovorno osoblje.

Plan implementacije pojedinih kontrola definira ciljeve projekta, rokove za implementaciju, odgovornosti i zaduženja, odnosno sve ono što je potrebno za uspješnu realizaciju odabranih sigurnosnih rješenja.

4.9. Korak 7: Implementacija kontrola

Ovaj korak podrazumijeva sam postupak implementacije sigurnosnih kontrola prema podijeljenim zaduženjima. Njihovom implementacijom sigurnosni rizik se smanjuje na prihvatljivu razinu, pri čemu ostaje spomenuti rezidualni rizik, za kojeg su analize pokazale da ga se ne isplati uklanjati.
Koraci opisani u prethodnih nekoliko podglavlja prikazani su još jednom na sljedećoj slici (*Slika 3*).

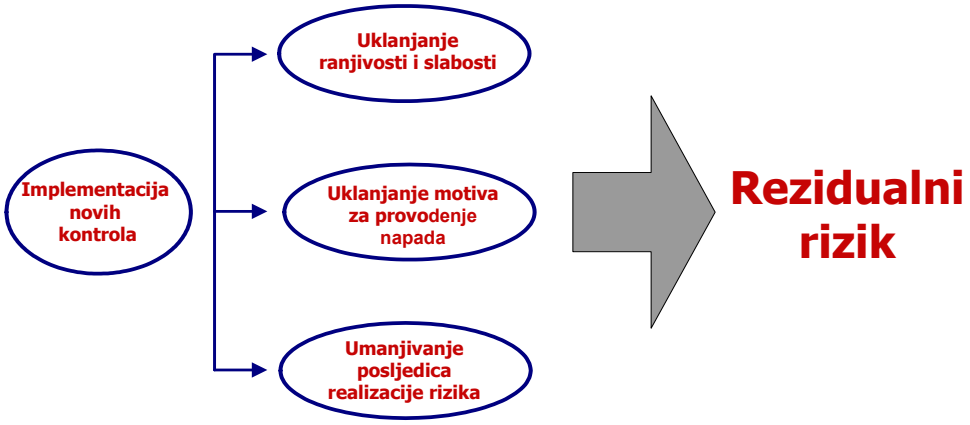


Slika 3: Proces umanjivanja rizika

U kojoj je mjeri sigurnosni rizik reduciran implementacijom novih ili unaprjeđenjem postojećih kontrola, moguće je utvrditi ponovnom analizom utjecaja prijetnji i ranjivosti, kao glavnih čimbenika koji utječu na razinu sigurnosnog rizika.

Implementacijom novih kontrola rizik može biti umanjen na jedan od sljedećih načina (*Slika 4*):

- eliminacija ranjivosti u sustavu,
- smanjivanje motivacije za provođenja napada, odnosno iskorištavanja ranjivosti,
- smanjivanje potencijalnih gubitaka u slučaju realizacije rizika.



Slika 4: Metode umanjivanja sigurnosnog rizika

5. Ispitivanje i analiza

Budući da su informacijski resursi podložni vrlo čestim promjenama, potreba za periodičkim analizama i evaluacijama neophodna je za održavanjem jednom postignute razine sigurnosti.

Promjene u mrežnoj i računalnoj opremi, nadogradnja ili instalacija novih programskih paketa, promjene u ljudskom kadru i sl., sve su elementi koji utječu na sigurnosni rizik u informacijskim sustavima. Ukoliko se o ovakvim promjenama ne vodi dovoljno računa, sustav se vrlo brzo može dovesti u stanje koje predstavlja neprihvatljiv sigurnosni rizik za organizaciju i njene poslovne ciljeve.

Koliko često će se provoditi proces procjene rizika, opisan u poglavlju 3, ovisiti će primarno o dinamici promjena u organizaciji. Ukoliko je sustav izložen čestim promjenama, procjenu rizika poželjno je raditi češće (na godišnjoj ili dvogodišnjoj bazi), dok je inače ovaj postupak preporučljivo provoditi svake tri godine.

Na samom kraju navedeni su neki od faktora koji su ključni za uspješno provođenje *risk management* programa:

- potpora i inicijativa od strane menadžmenta,
- podrška i sudjelovanje IT stručnjaka,
- kompetentnost osoblja uključenog u proces procjene rizika,
- savjest i suradnja korisnika, odnosno zaposlenika organizacije,
- periodičko ispitivanje i analiza.

Ukoliko su ispunjeni svi od navedenih uvjeta, proces upravljana sigurnosnim rizicima gotovo će sigurno biti uspješno proveden, a rezultati bi se u kratkom vremenu trebali odraziti na poslovanje i efikasnost organizacije u cjelini.

6. Zaključak

Proces upravljanja sigurnosnim rizicima jedan je od temeljnih elemenata upravljanja sigurnošću informacijskih sustava. Osnovni cilj ovog procesa je zaštiti informacijske resurse i poslovne procese organizacije od neželjenih događaja kao što su elementarne nepogode, neovlaštene aktivnosti s Interneta, interni napadi i sl. S obzirom sve veću na ulogu koju informacijski resursi imaju u poslovanju, upravljanje sigurnosnim rizicima postaje obavezan proces u programu upravljanja sigurnošću.

Okosnicu *risk management* programa čini procjena rizika, proces kojem je cilj identificirati informacijske resurse organizacije s pripadajućim prijetnjama i ranjivostima te na temelju toga odrediti sigurnosni rizik koji je prisutan u sustavu. Na temelju provedene procjene rizika, menadžment organizacije odlučuje na koji način tretirati identificirani rizik.

U ovom dokumentu opisana su osnovna načela i ciljevi procesa upravljanja sigurnosnim rizikom, način njegovog provođenja, kao i tipični problemi koji se javljaju u ovom području.