Osnove upravljanja rizikom informacijskog sustava

CENTAR INFORMACIJSKE SIGURNOSTI

Autor:

dr. sc. Suzana Stojaković – Čelustka

Hrvatska banka za obnovu i razvitak

E-mail: sstojakovic@hbor.hr

Sadržaj

- **1. dio – Osnovni pojmovi**
  - Upravljanje rizikom
  - Osnovni pojmovi
  - Integracija upravljanja rizikom u razvojni životni ciklus informacijskog sustava (SDLC)

Sadržaj

- **2. dio – Procjena rizika**
  - Procjena rizika – koraci
  - Karakterizacija sustava
  - Identifikacija prijetnji
  - Identifikacija ranjivosti
  - Analiza postojećih kontrola
  - Određivanje vjerojatnosti
  - Analiza utjecaja
  - Određivanje rizika

Sadržaj

- **3. dio – Mjere za smanjenje rizika**
  - Preporuka kontrola
  - Dokumentiranje rezultata
  - Ublažavanje rizika
  - Kategorije kontrola
  - Analiza troškova i dobitaka
  - Preostali rizik
  - Konačna procjena

Sadržaj

- **4. dio – Regulativa**
  - Okviri i norme
  - Zakonska regulativa u RH

Upravljanje rizikom

- U implementaciji sustava upravljanja informacijskom sigurnošću posebnu pozornost potrebno je obratiti upravljanju rizikom koji proizlazi iz korištenja informacijskog sustava.
- Upravljanje rizikom je proces koji omogućava upravi organizacije da se uravnoteže operativni i ekonomski troškovi zaštitnih mjera za očuvanje sigurnosti informacijskog sustava organizacije.
- Upravljanje rizikom je proces identifikacije rizika, procjene rizika i poduzimanja koraka da se rizik smanji na prihvatljivi nivo.

Osnovni pojmovi - Resursi

- opipljiva imovina (građevine, hardver, komunikacijska oprema)
- informacije/podaci
- softver
- sposobnost proizvodnje nekog proizvoda ili pružanja neke usluge (“know how”)
- osobe koje održavaju i koriste informacijski sustav
- neopipljiva imovina (zaštitni znak, reputacija)

Osnovni pojmovi - Prijetnja

- Prijetnja je bilo koji događaj ili okolnost, bilo vanjski ili unutarnji, koji ima potencijal da uzrokuje štetu sustavu ili njegovim pridruženim aplikacijama ili informacijama
- Prijetnja može prouzročiti neželjenu situaciju čija posljedica može biti nanošenje štete resursima organizacije
- Šteta nastaje kao posljedica ostvarenja prijetnje
- Prijetnja mora iskoristiti postojeću ranjivost resursa da bi se realizirala i rezultirala štetom

Obilježja prijetnji

- izvor (unutarnja ili vanjska prijetnja)
- motiv (npr. ostvarenje financijske dobiti)
- učestalost pojavljivanja
- razorna moć
- oblik
  - prirodna
  - uzrokovana ljudskim djelovanjem (slučajna ili namjerna)

Osnovni pojmovi - Ranjivost

- Ranjivost je skup stanja koji može omogućiti nekoj prijetnji da utječe na resurse
- Ranjivost je slabost koju je moguće slučajno aktivirati ili namjerno iskoristiti
- Posljedica iskorištenja ranjivosti je nanošenje štete informacijskom sustavu i poslovnim ciljevima

Osnovni pojmovi - Učinak

- Učinak je posljedica nekog neželjenog događaja izazvanog namjerno ili slučajno, koji utječe na resurse
- Mjerenje učinka
  - kvantitativno
  - kvalitativno

Osnovni pojmovi - Rizik

- Rizik je funkcija vjerojatnosti da će identificirani izvor prijetnje iskoristiti određenu ranjivost i učinka koji taj neželjeni događaj može imati na organizaciju

Upravljanje rizikom

- Proces identificiranja rizika, procjene rizika i poduzimanja koraka da se rizik smanji na prihvatljivi nivo, te održavanja tog nivoa rizika.
- Upravljanje rizikom zahtijeva analizu rizika u odnosu na potencijalne koristi, uzimanje u obzir alternativa i primjenu onoga što se utvrdi kao najbolji tijek akcije.

SDLC

- Razvojni životni ciklus sustava (System development life cycle – SDLC) ima pet faza: uvođenje, razvoj ili nabavka, primjena, rad ili održavanje, te na kraju odbacivanje.

SDLC i upravljanje rizikom (1)

SDLC faze	Karakteristike faza	Podrška putem upravljanja rizikom
Faza 1 - Uvođenje	Izražava se potreba za informacijskim sustavom i dokumentiraju se njegova svrha i cilj	Identificirani rizici se koriste da podrže razvoj zahtjeva na sustav, uključujući i sigurnosne zahtjeve, te sigurnosni koncept rada (strategiju)
Faza 2 – Razvoj ili Nabavka	Informacijski sustav je dizajniran, naručen, programiran, razvijen, ili drugačije konstruiran	Rizici identificirani za vrijeme ove faze mogu se koristiti da podrže sigurnosne analize informacijskog sustava koji mogu dovesti do kompromisa u arhitekturi ili dizajnu za vrijeme razvoja sustava

SDLC i upravljanje rizikom (2)

SDLC faze	Karakteristike faza	Podrška putem upravljanja rizikom
Faza 3 - Primjena	Sigurnosne karakteristike sustava bi trebale biti konfigurirane, omogućene, testirane i potvrđene	Proces upravljanja rizikom podržava procjenu primjene sustava u odnosu na zahtjeve i unutar njegovog modeliranog radnog okruženja. Odluke donesene u pogledu identificiranog rizika moraju se primijeniti prije rada sustava.

SDLC i upravljanje rizikom (3)

SDLC faze	Karakteristike faza	Podrška putem upravljanja rizikom
Faza 4 – Rad ili održavanje	Sustav izvršava svoje funkcije. Tipično, sustav je modificiran u procesu kroz dodavanje hardvera i softvera i kroz promjene organizacionih procesa, politika i procedura	Aktivnosti upravljanja rizikom se izvode za periodičke aktivnosti ponovne autorizacije (reakreditacije) sustava ili kad god su veće promjene učinjene u informacijskom sustavu u njegovom radnom, produktivnom okolišu (npr. nova sistemska sučelja).

SDLC i upravljanje rizikom (4)

SDLC faze	Karakteristike faza	Podrška putem upravljanja rizikom
Faza 5 – Odbacivanje	Ova faza može sadržavati odbacivanje informacija, hardvera ili softvera. Aktivnosti mogu uključivati premještanje, arhiviranje, odbacivanje ili uništavanje informacija, te sigurno odlaganje hardvera i softvera	Aktivnosti upravljanja rizikom se izvode za komponente sustava koje će biti odbačene ili zamijenjene da bi se osiguralo da su hardver i softver pravilno odloženi, da su preostali podaci pravilno održavani, te da je premještaj sustava proveden na siguran i sustavan način.

Procjena rizika (1)

- Procjena rizika je prvi proces u metodologiji upravljanja rizikom. Organizacije koriste procjenu rizika da bi odredile opseg potencijalnih prijetnji i rizika koji prate jedan informacijski sustav kroz SDLC. Ova aktivnost pomaže da se identificiraju odgovarajuće kontrole za smanjenje ili eliminaciju rizika za vrijeme procesa ublažavanja rizika.
- Da bi se odredila vjerojatnost budućih štetnih događaja, prijetnje informacijskom sustavu moraju se analizirati zajedno sa potencijalnim ranjivostima i postojećim kontrolama. Utjecaj se odnosi na veličinu štete koja može biti uzrokovana iskorištavanjem ranjivosti od strane prijetnje.

Procjena rizika (2)

- Metodologija procjene rizika sastoji se od devet koraka:
  - Karakterizacija sustava
  - Identificiranje prijetnji
  - Identificiranje ranjivosti
  - Analiza kontrola
  - Određivanje vjerojatnosti
  - Analiza utjecaja
  - Određivanje rizika
  - Preporuka kontrola
  - Dokumentiranje rezultata

Karakterizacija sustava (1)

- U procjeni rizika za neki informacijski sustav prvi korak je da se definira cilj poduhvata. U ovom koraku identificiraju se granice informacijskog sustava, zajedno sa uređajima i informacijama koji čine sustav.
- Karakterizacijom informacijskog sustava se ustanovljavaju cilj procjene rizika, te se daju osnovne informacije (npr. hardver, softver, komunikacijske veze, odgovorno osoblje) za definiranje rizika.

Karakterizacija sustava (2)

- Najprije je potrebno prikupiti informacije o samom sustavu kako slijedi:
  - Hardver
  - Softver
  - Sučelja sustava (npr. interna i vanjska povezanost)
  - Podaci i informacije
  - Osoblje koje održava i koristi informacijski sustav
  - Namjena sustava (npr. procesi koje izvršava informacijski sustav)
  - Kritičnost sustava i podataka (npr. vrijednost i važnost sustava za organizaciju)
  - Osjetljivost sustava i podataka

Karakterizacija sustava (3)

- Mogu se koristiti slijedeće tehnike prikupljanja informacija:
  - Upitnik
  - Intervjui odgovornog osoblja
  - Pregled dokumentacije
  - Uporaba automatskih skenirajućih alata
- Očekivani izlaz iz ovog koraka je karakterizacija procjenjivanog informacijskog sustava, dobra slika okoliša informacijskog sustava, i nacrt granica sustava

Identifikacija prijetnji (1)

- Sama prijetnja ne predstavlja rizik kada nema ranjivosti koja se može iskoristiti. U određivanju vjerojatnosti prijetnje potrebno je razmotriti prijetnje, potencijalne ranjivosti i postojeće kontrole.
- U procjeni prijetnji važno je razmotriti sve potencijalne izvore prijetnji koje mogu prouzročiti štetu u informacijskom sustavu i njegovoj radnoj okolini.

Identifikacija prijetnji (2)

- Prirodni izvori prijetnji su prirodne nepogode.
- Tehnički izvori prijetnji su tehnički kvarovi opreme.
- Ljudski izvori prijetnji su:
  - **unutarnji** - nestručni projektanti informatičkog sustava, neodgovorni vlasnici cjelokupnog i dijelova informacijskog sustava, ovlašteni korisnici koji zlouporabe svoje ovlasti, operatori sustava i usluga koji zlouporabe svoje ovlasti, službenici koji imaju fizički pristup informatičkoj opremi, a koji zlouporabe svoje ovlasti, itd.;
  - **vanjski** - zlonamjerni pojedinci izvana, kriminalne organizacije, strane obavještajne službe, komercijalne organizacije, terorističke organizacije, itd.

Identifikacija prijetnji (3)

- Prikaz prijetnji, ili lista potencijalnih izvora prijetnji, mora biti prilagođena pojedinoj organizaciji i njenom radnom okruženju (npr. običaji korisnika na računalu). Općenito, informacija o prirodnim prijetnjama (npr. poplavama, potresima, olujama), također bi trebala biti lako dostupna.

Identifikacija ranjivosti (1)

- Analiza prijetnji nekom informacijskom sustavu mora uključiti i analizu ranjivosti u okolini sustava. Cilj ovog koraka je da razvije listu ranjivosti sustava (pogreški ili slabosti) koje bi se mogle iskoristiti od strane određene prijetnje.
- Izrada tablice parova ranjivost/prijetnja

Identifikacija ranjivosti (2)

- Tablica ranjivosti i prijetnji

Ranjivost	Prijetnja	Akcija prijetnje
Iz sustava nisu uklonjeni korisnički računi otpuštenih zaposlenika	Otpušteni zaposlenici	Spajanje na mrežu organizacije i pristup povjerljivim podacima organizacije
Računalni centar koristi raspršivače vode za gašenje vatre; ali nema vodootpornih prekrivača za hardver i ostalu opremu	Vatra, nesavjesno osoblje	Uključivanje raspršivača vode u računalnom centru

Identifikacija ranjivosti (3)

- Preporučene metode za identificiranje ranjivosti sustava su upotreba izvora informacija o ranjivostima, sigurnosno testiranje sustava i razvoj liste sigurnosnih provjera.
- Potrebno je naglasiti da će tipovi ranjivosti koji će se pojaviti, kao i metodologija potrebna da se utvrdi da li ranjivosti postoje, obično ovisiti o prirodi informacijskog sustava i o fazi životnog ciklusa (SDLC) u kojoj se sustav nalazi.

Identifikacija ranjivosti (4)

- Ako informacijski sustav još nije dizajniran, potraga za ranjivostima bi se trebala usmjeriti na sigurnosne politike organizacije, planirane sigurnosne procedure, definicije zahtjeva na sustav, te sigurnosne analize produkata od strane dobavljača ili graditelja sustava.
- Ako je informacijski sustav u fazi primjene, identifikacija ranjivosti treba se proširiti da uključi više specifične informacije, kao što su planirana sigurnosna svojstva sustava, opisana u dokumentaciji sigurnosnog dizajna, te rezultate certifikacije i procjene sustava.
- Ako je informacijski sustav u radnoj fazi, proces identificiranja ranjivosti bi trebao uključiti analizu sigurnosnih svojstava sustava i sigurnosne kontrole, tehničke i proceduralne, koje se koriste za zaštitu sustava.

Identifikacija ranjivosti (5)

- Izvori informacija o ranjivostima:
  - Dokumentacija od prethodnih analiza rizika procjenjivanog informacijskog sustava
  - Izvještaji kontrolnih pregleda (audita) sustava, izvještaji o anomalijama sustava, izvještaji sigurnosnih pregleda, te izvještaji testiranja i procjene sustava
  - Liste ranjivosti
  - Sigurnosna upozorenja
  - Upozorenja dobavljača
  - Specijalizirane mailing liste
  - Sigurnosne analize softvera sustava

Identifikacija ranjivosti (6)

- Proaktivne metode koje koriste testiranje sustava mogu se upotrijebiti da se efikasno identificiraju ranjivosti sustava, ovisno o kritičnosti sustava i raspoloživih resursa. Metode testiranja mogu biti:
  - Automatizirani alati za skeniranje ranjivosti
  - Sigurnosni test i procjena (ST&E)
  - Penetracijsko testiranje

Analiza kontrola (1)

- Cilj ovog koraka je da se analiziraju kontrole koje su primijenjene ili su planirane za primjenu u organizaciji da bi smanjile ili uklonile vjerojatnost da prijetnja iskoristi ranjivost sustava.
- Sigurnosne kontrole obuhvaćaju upotrebu tehničkih i netehničkih metoda.
- Tehničke kontrole su zaštitni alati koji su ugrađeni u računalni hardver, softver ili firmver (npr. mehanizmi za kontrolu pristupa, mehanizmi za identifikaciju i autentikaciju, enkripcijske metode, softver za otkrivanje upada).
- Netehničke kontrole su kontrole upravljanja i radne kontrole, kao što su sigurnosne politike, radne procedure, te sigurnost osoblja, fizička sigurnost i sigurnost okoliša.

Analiza kontrola (2)

- I tehničke i netehničke kontrole mogu se dalje klasificirati na preventivne i aktivne:
  - **Preventivne kontrole** sprečavaju pokušaje prekršaja sigurnosne politike i uključuju takve kontrole kao što su kontrola pristupa, enkripcija i autentikacija.
  - **Aktivne kontrole** upozoravaju na prekršaje sigurnosne politike i sadrže takve kontrole kao što su nadzorna praćenja (audit trails), metode otkrivanja upada i kontrolne sume (checksums).

Određivanje vjerojatnosti (1)

- Da bi se izvela klasifikacija vjerojatnosti koja označava mogućnost da se iskoristi ranjivost od strane prijetnje, moraju se razmotriti slijedeći faktori:
  - Motivacija i mogućnosti prijetnje
  - Priroda ranjivosti
  - Postojanje i učinkovitost tekućih kontrola

Određivanje vjerojatnosti (2)

Nivo vjerojatnosti	Definicija vjerojatnosti
Visoki	Prijetnja je visoko motivirana i ima dovoljno mogućnosti za realizaciju, a kontrole koje bi trebale spriječiti iskorištavanje ranjivosti su neefektivne.
Srednji	Prijetnja je motivirana i ima mogućnosti za realizaciju, ali postoje kontrole koje mogu spriječiti uspješno izvođenje prijetnje.
Nizak	Prijetnja nije motivirana ili nema dovoljno mogućnosti za realizaciju, ili postoje kontrole koje mogu spriječiti iskorištavanje ranjivosti

Analiza utjecaja (1)

- Slijedeći važan korak u mjerenju nivoa rizika je da se odredi štetni utjecaj koji je rezultat uspješnog iskorištavanja ranjivosti od strane prijetnje.
- Prije početka analize utjecaja, potrebno je dobiti slijedeće informacije:
  - Svrha sustava (npr. proces koji treba izvršiti sustav)
  - Kritičnost sustava i podataka (npr. vrijednost sustava ili njegova važnost za organizaciju)
  - Osjetljivost sustava i podataka

Analiza utjecaja (2)

- Ove informacije mogu se dobiti iz postojeće dokumentacije organizacije, kao što su izvještaj o analizi utjecaja na poslovanje ili izvještaj o procjeni kritične opreme.
- Analiza utjecaja na poslovanje klasificira nivoe utjecaja koji bi mogli ugroziti informatička sredstva organizacije zasnovano na kvalitativnoj ili kvantitativnoj procjeni osjetljivosti i kritičnosti tih sredstava.
- Procjena kritične opreme identificira i klasificira osjetljivu i kritičnu informacijsku opremu organizacije (npr. hardver, softver, sustave, servise i pripadna tehnološka sredstva) koja podržava kritične poslovne procese organizacije.

Analiza utjecaja (3)

- Neki utjecaji se mogu mjeriti kvantitativno, kao npr. gubitak u prihodu, troškovi popravka sustava, ili nivo napora koji se zahtijeva da se poprave problemi uzrokovani uspješnom akcijom prijetnje.
- Drugi utjecaji (npr. gubitak povjerenja javnosti, gubitak vjerodostojnosti, šteta interesu organizacije) se ne mogu mjeriti određenim jedinicama, ali se mogu opisati pojmovima visokog, srednjeg ili niskog nivoa utjecaja.

Analiza utjecaja (4)

Veličina utjecaja	Definicija utjecaja
Visoka	Iskorištenje ranjivosti može (1) rezultirati u visokim troškovima zbog gubitka glavnih fizičkih sredstava ili resursa; (2) značajno ugroziti, oštetiti ili spriječiti poslovanje organizacije, njenu reputaciju ili interes; (3) rezultirati ljudskom smrću ili teškim ozljeđivanjem.
Srednja	Iskorištenje ranjivosti može (1) rezultirati u znatnim troškovima zbog gubitka glavnih fizičkih sredstava ili resursa; (2) ugroziti, oštetiti ili spriječiti poslovanje organizacije, njenu reputaciju ili interes; (3) rezultirati ljudskim ozljeđivanjem.
Niska	Iskorištenje ranjivosti može (1) rezultirati u troškovima zbog gubitka glavnih fizičkih sredstava ili resursa; (2) značajno utjecati na poslovanje organizacije, njenu reputaciju ili interes

Analiza utjecaja (5)

- Glavna prednost kvalitativne analize utjecaja je da ona klasificira rizik i identificira područja za neposredno poboljšanje uvidom u ranjivosti. Mana kvalitativne analize je da ne daje specifične kvantitativne mjere veličine utjecaja, tako da se ne može provesti analiza troškova.
- Glavna prednost kvantitativne analize utjecaja je da ona omogućuje mjerenje veličine utjecaja koje se može iskoristiti u procjeni troškova za preporučene kontrole. Mana kvantitativne analize je da, ovisno o numeričkim područjima koja se koriste za prikaz mjerenja, značenje ovakve analize može biti nejasno, zahtijevajući da se rezultati ipak interpretiraju kvalitativno.

Određivanje rizika (1)

- Svrha ovog koraka je procjena nivoa rizika za informacijski sustav. Određivanje rizika za određeni par prijetnja/ranjivost može se prikazati kao funkcija od:
  - vjerojatnosti određene prijetnje da iskoristi određenu ranjivost
  - veličine utjecaja ako je prijetnja uspješno iskoristila ranjivost
  - prikladnosti planiranih ili postojećih sigurnosnih kontrola za smanjenje ili eliminiranje rizika

Određivanje rizika (2)

Vjerojatnost prijetnje	Utjecaj		
	Niski (10)	***Srednji (50)***	***Visoki (100)***
Visoka (1.0)	Niski 10 X 1.0 = 10	Srednji 50 X 1.0 = 50	Visoki 100 X 1.0 =100
Srednja (0.5)	Niski 10 X 0.5 = 5	Srednji 50 X 0.5 = 25	Srednji 100 X 0.5 = 50
Niska (0.1)	Niski 10 X 0.1 = 1	Niski 50 X 0.1 = 5	Niski 100 X 0.1 = 10

Određivanje rizika (3)

Nivo rizika	Opis rizika i potrebne akcije
Visoki	Ako je neka pojava procijenjena kao visoki rizik, postoji jaka potreba za korektivnim mjerama. Postojeći sustav može nastaviti s radom, ali plan korektivnih akcija mora se ostvariti što prije moguće.
Srednji	Ako je neka pojava procijenjena kao srednji rizik, potrebne su korektivne akcije i mora se razviti plan da se te akcije ostvare u razumnom vremenu.
Nizak	Ako je neka pojava procijenjena kao nizak rizik, mora se odlučiti da li su potrebne korektivne akcije ili se rizik može prihvatiti.

Preporuka kontrola (1)

- Za vrijeme ovog koraka u procesu upravljanja rizikom, preporučuju se kontrole koje mogu ublažiti ili eliminirati rizik, na način koji odgovara radnim operacijama organizacije.
- Cilj preporuke kontrola je smanjiti nivo rizika za sustav i njegove podatke na prihvatljivi nivo.

Preporuka kontrola (2)

- Slijedeći faktori trebaju se razmotriti u preporuci kontrola:
  - Efektivnost preporučenih kontrola (npr. kompatibilnost sa sustavom)
  - Zakoni i uredbe
  - Organizaciona politika
  - Utjecaj na rad
  - Sigurnost i pouzdanost
- Preporuka kontrola je rezultat procesa procjene rizika i daje smjernice za proces ublažavanja rizika, za vrijeme kojeg se preporučene proceduralne i tehničke sigurnosne kontrole procjenjuju, klasificiraju i primjenjuju.

Dokumentiranje rezultata

- Rezultati procjene rizika (identificirane prijetnje i ranjivosti, procijenjeni rizik i preporučene kontrole) trebaju se dokumentirati u obliku izvještaja.

- Izvještaj o procjeni rizika opisuje prijetnje i ranjivosti, mjeri rizik i preporučuje kontrole koje se trebaju primijeniti.

Ublažavanje rizika

- Ublažavanje rizika, drugi proces upravljanja rizikom, sadrži klasifikaciju, procjenu i primjenu odgovarajućih kontrola za smanjenje rizika koje su preporučene u procesu procjene rizika.
- Budući da je eliminacija ukupnog rizika obično nepraktična ili nemoguća, na upravi leži odgovornost za upotrebu najisplativijeg pristupa i primjenu najviše odgovarajućih kontrola za smanjenje rizika misije na prihvatljivi nivo, sa minimalnim štetnim utjecajem na resurse i misiju organizacije.

Opcije za smanjenje rizika (1)

- **Preuzimanje rizika** – znači prihvaćanje potencijalnog rizika i nastavak rada.
- **Izbjegavanje rizika** – znači izbjeći rizik eliminacijom uzroka rizika i/ili posljedica (npr. odricanje od određenih funkcija sustava ili isključivanje sustava kada se identificiraju rizici).
- **Ograničenje rizika** – znači smanjenje rizika primjenom kontrola koje minimiziraju štetni utjecaj iskorištenja ranjivosti od strane prijetnje (npr. uporaba preventivnih i aktivnih kontrola).

Opcije za smanjenje rizika (2)

- **Planiranje rizika** – znači upravljanje rizikom razvojem plana ublažavanja rizika koji klasificira, primjenjuje i održava kontrole.
- **Istraživanje i priznanje** – znači smanjiti rizik gubitka priznavanjem slabosti ili greške i istražiti kontrole da bi se popravila ranjivost.
- **Prijenos rizika** – znači prenošenje rizika korištenjem drugih opcija za kompenzaciju gubitka, kao što je osiguranje kod nabave.

Opcije za smanjenje rizika (3)

- Potrebno je uzeti u obzir ciljeve i misiju organizacije kod odabira bilo koje od opcija za ublažavanje rizika. Moglo bi biti nepraktično baviti se svim identificiranim rizikom, pa je potrebno dati prioritete parovima prijetnji i ranjivosti koji imaju potencijal da uzrokuju znatnu štetu poslovanju.
- Također, u zaštiti poslovanja organizacije i njenih informacijskih sustava, zbog jedinstvenih ciljeva i okoliša svake pojedine organizacije, opcije koje se koriste za smanjenje rizika kao i metode primjene kontrola mogu varirati.
- Najbolji pristup je upotreba odgovarajućih tehnologija sigurnosnih proizvoda od raznih dobavljača, zajedno sa odgovarajućom opcijom za ublažavanje rizika i netehničkim, administrativnim mjerama.

Strategija ublažavanja rizika

- Za strategiju ublažavanja rizika vrijede slijedeća pravila:
  - Kada postoji ranjivost (ili greška, slabost) – primijeniti tehnike osiguranja da bi se smanjila vjerojatnost iskorištavanja ranjivosti.
  - Kada se ranjivost može iskoristiti – primijeniti slojevitu zaštitu, arhitekturalne dizajne i administrativne kontrole da bi se smanjio rizik ili spriječio taj događaj.
  - Kada su napadačevi troškovi manji nego potencijalni dobitak – primijeniti zaštitu da bi se smanjila napadačeva motivacija povišenjem troškova napadača (npr. korištenje kontrola sustava kao što je ograničavanje pristupa i rada korisnika u sustavu može znatno smanjiti dobitak napadača).
  - Kada je gubitak prevelik – primijeniti principe dizajna, arhitekturalne dizajne i tehničke i netehničke zaštite da bi se smanjio opseg napada, na taj način smanjivši mogućnost gubitka.

Primjena kontrola (1)

- Pri primjeni kontrola vrijedi slijedeće pravilo:

Treba pretpostaviti najveći rizik i težiti odgovarajućem ublaženju rizika uz najmanju cijenu, te uz minimalan utjecaj na poslovanje.

Primjena kontrola (2)

- **Metodologija ublažavanja rizika**
  - **Određivanje redoslijeda akcija**
    - Određuje se redoslijed akcija na osnovu nivoa rizika predstavljenih u izvještaju procjene rizika. Prioritet se treba dati akcijama vezanim uz najveći rizik (Vrlo visok ili Visok)
    - Izlaz iz ovog koraka – Prioritet akcija od Visok do Nizak
  - **Procjena preporučenih kontrola**
    - Cilj je izabrati najbolje odgovarajuće kontrole za minimiziranje rizika.
    - Izlaz iz ovog koraka – Popis ostvarivih kontrola
  - **Izvođenje analize troškova i dobitaka**
    - Analiza troškova i dobitaka se izvodi da bi se pomoglo u donošenju odluke o najisplativijim kontrolama.
    - Izlaz iz ovog koraka – Analiza troškova i dobitaka koja opisuje troškove i dobitke uslijed primjene i neprimjene kontrola.

Primjena kontrola (3)

- **Metodologija ublažavanja rizika**
  - **Izbor kontrola**
    - Na osnovu rezultata analize troškova i dobitaka određuju se najisplativije kontrole za smanjenje rizika misije organizacije.
    - Izlaz iz ovog koraka – Izabrane kontrole
  - **Raspodjela odgovornosti**
    - Izabiru se odgovarajuće osobe za primjenu izabranih kontrola.
    - Izlaz iz ovog koraka – Popis odgovornih osoba

Primjena kontrola (4)

- **Metodologija ublažavanja rizika**
  - **Razvoj plana primjene zaštita**
    - Plan bi kao minimum trebao sadržavati slijedeće informacije:

1. Rizike (parovi ranjivost/prijetnja) i odgovarajući nivoi rizika (dobiveni iz izvještaja o procjeni rizika
2. Preporučene kontrole (iz izvještaja o procjeni rizika)
3. Redoslijed akcija (sa prioritetima koji su povezani s jedinicama sa Vrlo visokim i Visokim nivoima rizika)
4. Izabrane planirane kontrole (određene na osnovu ostvarivosti, efektivnosti, doprinosa za organizaciju, te cijene)
5. Potrebni resursi za primjenu izabranih planiranih kontrola
6. Popis odgovornih timova i osoblja
7. Početni datum primjene
8. Datum ispunjenja cilja u primjeni
9. Zahtjevi održavanja

Primjena kontrola (5)

- **Metodologija ublažavanja rizika**
  - **Primjena izabranih kontrola**
    - Ovisno o pojedinoj situaciji, primijenjene kontrole mogu smanjiti nivo rizika, ali ne i otkloniti sav rizik.
    - Izlaz iz ovog koraka – Preostali rizik

Kategorije kontrola

- U primjeni preporučenih kontrola za ublažavanje rizika, organizacija bi trebala uzeti u obzir **tehničke**, **upravljačke** i **radne** sigurnosne kontrole ili kombinaciju takvih kontrola da bi se maksimizirala učinkovitost kontrola za njen sustav.

Tehničke kontrole (1)

- Tehničke sigurnosne kontrole za ublažavanje rizika mogu se konfigurirati da štite od određenih tipova prijetnji. Ove kontrole mogu sadržavati jednostavne do kompleksnih mjera i obično uključuju arhitekturu sustava, inženjerske discipline, te sigurnosne pakete sa smjesom hardvera, softvera i firmvera. Sve ove mjere bi trebale raditi zajedno da osiguraju kritične i osjetljive podatke, informacije i funkcije sustava.

Tehničke kontrole (2)

- Tehničke kontrole se mogu grupirati u slijedeće kategorije:
  - **Podrška** – ove kontrole moraju biti postavljene da bi se mogle primijeniti druge kontrole.
  - **Prevencija** – preventivne kontrole koje sprečavaju prijetnje da se ostvare.
  - **Otkrivanje i oporavak** – ove kontrole služe za otkrivanje sigurnosnog incidenta, te za oporavak od njega.

Tehničke kontrole za podršku

- **Identifikacija** – ova kontrola omogućuje jedinstveno identificiranje korisnika, procesa i informatičkih resursa.
- **Upravljanje kriptografskim ključevima** – kriptografski ključevi se moraju brižljivo čuvati kada se kriptografske metode koriste u drugim kontrolama. Upravljanje kriptografskim ključevima uključuje generiranje ključeva, distribuciju, pohranjivanje i održavanje ključeva.
- **Administracija sigurnosti** – sigurnosna svojstva nekog sustava moraju se konfigurirati (npr. omogućiti ili onemogućiti) tako da odgovaraju potrebama specifične instalacije i da prate promjene u radnom okolišu. Sigurnost sustava može se ugraditi u operativni sustav ili aplikacije.
- **Zaštita sustava** – primjeri zaštite sustava su preostala zaštita informacije, najmanja prava, odvajanje procesa, modularnost, niveliranje, minimizacija povjerenja.

Tehničke preventivne kontrole

- **Autentikacija** – omogućuje verifikaciju identiteta subjekata da bi se osiguralo da je navedeni identitet valjan. Autentikacijski mehanizmi uključuju lozinke, osobne identifikacijske brojeve (PIN) i strogu autentikaciju (tokene, «smart card», digitalne certifikate, Kerberos).
- **Autorizacija** – omogućuje specifikaciju i upravljanje dozvoljenih akcija u sustavu.
- **Kontrola pristupa** – omogućava održanje cjelovitosti i povjerljivosti podataka.
- **Neporecivost** – odgovornost sustava ovisi o mogućnosti da pošiljatelji ne mogu negirati slanje informacije, a primatelji primanje.
- **Zaštićene komunikacije** – osiguravaju cjelovitost, raspoloživost i povjerljivost kritičnih informacija u prijenosu. Zaštićene komunikacije koriste metode za enkripciju podataka (npr. VPN, IPSEC protokol) i kriptografske tehnologije (npr. DES, Triple DES, RAS; MD4, MD5) da bi se minimizirale prijetnje sa mreže.
- **Privatnost transakcija** – ove kontrole štite od gubitka privatnosti (npr. SSL, SSH).

Tehničke kontrole za otkrivanje i oporavak

- **Nadzor (audit)** – nadzor događaja važnih za sigurnost, kao i praćenje abnormalnosti u sustavu su veoma važni za “detekciju poslije događaja” i oporavak nakon prekršaja sigurnosti.
- **Otkrivanje upada i onemogućavanje napadača** – važno je da se prekršaji sigurnosti (npr. mrežni upadi, sumnjive aktivnosti) otkriju na vrijeme da bi se na njih moglo i odgovoriti na vrijeme. Otkrivanje upada je od malo koristi ako ne postoji efektivni odgovor na incidente. Otkrivanje upada i onemogućavanje napadača daju te mogućnosti.
- **Dokaz cjelovitosti** – kontrola za dokaz cjelovitosti analizira cjelovitost sustava i nepravilnosti u sustavu, te time identificira “otkrivenost” i potencijalne prijetnje. Ova kontrola ne sprječava prekršaje sigurnosne politike nego otkriva prekršaje i pomaže da se odrede potrebne korektivne akcije.
- **Obnavljanje sigurnog stanja** – ova usluga omogućuje sustavu da se vrati u poznato sigurno stanje, nakon što se desio prekršaj sigurnosti.
- **Otkrivanje i otklanjanje virusa** – softver za otkrivanje i otklanjanje virusa, instaliran na serverima i radnim stanicama, otkriva, identificira i otklanja računalne viruse da bi se osigurala cjelovitost podataka i sustava.

Upravljačke kontrole

- Upravljačke sigurnosne kontrole, zajedno sa tehničkim i radnim kontrolama, koriste se da bi se upravljalo rizikom i da bi se smanjio rizik od gubitka, te da bi se zaštitila misija organizacije.
- Upravljačke kontrole imaju za cilj izgradnju politika, vodiča i standarda za zaštitu informacija, koji se primjenjuju kroz radne procedure da bi se ispunili ciljevi i misija organizacije.

Preventivne upravljačke kontrole

- **Pridjeljivanje odgovornosti za sigurnost** da bi se osigurala adekvatna sigurnost za IT sustave koji su kritični za misiju
- **Razvoj i održavanje planova sigurnosti sustava** da bi se dokumentirale postojeće kontrole i pripremile planirane kontrole za IT sustave koje podržavaju misiju organizacije
- **Primjena sigurnosnih kontrola osoblja**, koje uključuju odvajanje dužnosti, najmanja prava, registraciju pristupa računalu i završetka rada
- **Tehnička obuka i tečajevi svjesnosti** da bi se osiguralo da su krajnji i sustavski korisnici svjesni pravila ponašanja i svojih odgovornosti u zaštiti misije organizacije.

Upravljačke kontrole za otkrivanje

- **Primjena sigurnosnih kontrola osoblja** što uključuje ispitivanje osoblja, provjeru prošlosti i rotaciju dužnosti
- **Periodički pregled sigurnosnih kontrola** da bi se osiguralo da one efektivno funkcioniraju
- **Izvođenje periodičkih pregleda sustava**
- **Provođenje upravljanja rizikom** da bi se procijenio i ublažio rizik
- **Autorizacija sustava** da se ima uvid u i prihvati preostali rizik.

Upravljačke kontrole za oporavak

- **Kontinuiranost podrške i razvoj, testiranje i održavanje kontinuiranosti radnih planova** da bi se omogućio nastavak poslovnog procesa i osigurala kontinuiranost radnih operacija za vrijeme hitnih stanja i nesreća ili nepogoda.
- **Uspostavljanje grupe za odgovore na incidente** da bi se pripremili za prepoznavanje, izvješćivanje i odgovor na incidente, kao i povratak informacijskog sustava u radno stanje.

Radne kontrole

- Sigurnosni standardi neke organizacije trebali bi uspostaviti skup kontrola i vodiča da se osigura da sigurnosne procedure upravljaju upotrebom informatičkih sredstava i resursa organizacije, te da se oni koriste u skladu sa poslovnim ciljevima organizacije.

Preventivne radne kontrole (1)

- Kontrola pristupa podatkovnim medijima i odbacivanja tih medija (npr. kontrola fizičkog pristupa, demagnetizacijske metode)
- Ograničenje vanjske distribucije podataka (npr. upotreba oznaka)
- Kontrola računalnih virusa
- Sigurnosna kontrola računalnog prostora (npr. zaštitni čuvari, ulazne procedure za posjetioce, elektronički bedževi, biometrijska kontrola pristupa, upravljanje i distribucija lokota i ključeva, zapreka i ograda)
- Sigurni ormari za ožičenje, hubove i kablove
- Mogućnosti backupa (npr. procedure za redovni backup podataka i sustava, pričuvni logovi koji čuvaju sve promjene u databazama i koji se mogu iskoristiti za oporavak)

Preventivne radne kontrole (2)

- Procedure i sigurnost za pohranjivanje izvan radnog prostora
- Zaštita laptopa, osobnih računala (PC), radnih stanica
- Zaštita informatičke opreme od vatre (npr. zahtjevi i procedure za upotrebu aparata za gašenje vatre, vodootpornih pokrivača, suhi raspršivački sustavi, halonsko gašenje vatre)
- Izvor električnog napajanja za hitne slučajeve (npr. zahtjevi za neprekidno napajanje, interni generatori)
- Kontrola vlažnosti i temperature računalnih prostorija (npr. uređaji za klimatizaciju, sustavi za grijanje).

Radne kontrole za otkrivanje

- **Osiguravanje fizičke sigurnosti** (npr. upotreba detektora kretanja, TV nadzora, senzora i alarma)
- **Osiguranje sigurnosti okoline** (npr. upotreba detektora dima i vatre, senzori i alarmi)

Analiza troškova i dobitaka (1)

- Da bi se predvidjeli resursi i primijenile najisplativije kontrole, organizacije, nakon identificiranja svih mogućih kontrola i procjene njihove izvedivosti i efektivnosti, trebaju provesti analizu troškova i dobitaka za svaku predloženu kontrolu da bi se odredilo koje su kontrole odgovarajuće za dane uvjete.

- Analiza troškova i dobitaka može biti kvalitativna ili kvantitativna. Njezin cilj je da pokaže da trošak primjene kontrola može biti opravdan smanjenjem nivoa rizika.

Analiza troškova i dobitaka (2)

- Analiza troškova i dobitaka obuhvaća:
  - Određivanje utjecaja primjene novih ili proširenih kontrola
  - Određivanje utjecaja ako se ne primjene nove ili proširene kontrole
  - Procjenu troškova implementacije koja obuhvaća:
    - nabavku softvera i hardvera
    - smanjena radna efektivnost ako je rad sustava ograničen radi povećane sigurnosti
    - troškovi primjene dodatnih politika i procedura
    - troškovi zapošljavanja dodatnog osoblja za primjenu predloženih politika, procedura ili usluga
    - troškovi obuke
    - troškovi održavanja
  - Procjenu troškova i dobitaka primjene s obzirom na kritičnost sustava i podataka da bi se odredila važnost primjene novih kontrola za organizaciju, uz dane njihove troškove i relativni utjecaj.

Analiza troškova i dobitaka (3)

- **Uprava organizacije treba odlučiti što je prihvatljivi nivo rizika.** Utjecaj kontrola se tada može procijeniti, te se kontrola može uključiti ili isključiti.
- Slijedeća pravila se mogu uzeti u obzir za određivanje upotrebe novih kontrola:
  - Ako će kontrola smanjiti rizik više nego što je potrebno, tada treba vidjeti da li postoji jeftinije rješenje
  - Ako će kontrola koštati više nego smanjenje rizika, treba pronaći nešto drugo
  - Ako kontrola ne smanjuje dovoljno rizik, treba potražiti više kontrola ili drugačiju kontrolu
  - Ako kontrola omogućava dovoljno smanjenje rizika i isplativa je, treba je upotrijebiti.
- **Često je trošak primjene kontrole prihvatljiviji od njezine neprimjene.**

Preostali rizik

- Primjena novih ili proširenih kontrola može smanjiti rizik:
  - Odstranjivanjem nekih od ranjivosti sustava (grešaka i slabosti), čime se smanjuje broj mogućih prijetnji.
  - Dodavanjem ciljanih kontrola da bi se smanjio kapacitet i motivacija prijetnje.
  - Smanjenjem veličine štetnog utjecaja.
- Rizik koji preostaje nakon primjene novih ili proširenih kontrola je **preostali rizik**. Nijedan sustav nije slobodan od rizika, a također ga ne mogu u potpunosti otkloniti ni sve primijenjene kontrole. Ako preostali rizik nije bio smanjen na prihvatljivi nivo, ciklus upravljanja rizikom se mora ponoviti da bi se identificirao način smanjenja preostalog rizika na prihvatljivi nivo.

Konačna procjena

- U većini organizacija će se mreža kontinuirano širiti i obnavljati, a njene komponente mijenjati i softverske aplikacije zamijeniti ili obnoviti novim verzijama. Također će se i osoblje mijenjati što znači da će se i sigurnosne politike morati mijenjati s vremenom. Ove promjene znače da će se pojaviti novi rizik, a rizik prethodno smanjen može opet doći u obzir. To znači da je proces upravljanja rizikom neprekinut i u stalnom razvijanju.

Dobra sigurnosna praksa

- Proces procjene rizika se mora ponavljati svake godine.
- Upravljanje rizikom trebalo bi ugraditi u SDLC za informacijski sustav, ne zato što to zahtijeva zakon ili uredba, nego i zato što je to dobra praksa i podržava poslovne ciljeve i misiju organizacije.
- Trebao bi postojati specifičan redoslijed za procjenu i ublažavanje rizika, ali taj periodički proces bi trebao također biti i dovoljno fleksibilan da omogući promjene u informacijskom sustavu i radnom okolišu zbog promjena u politikama i tehnologiji.

Okviri i norme

- **Okviri**
  - CobiT 4.1 + Risk IT + Val IT
  - COBIT 5
- **Norme**
  - ISO 27001/27002
  - ISO 27005
  - ISO 31000
  - ISO 31010
  - NIST SP 800-30

Zakonska regulativa u RH

- **Bankarski sektor u RH je dobro reguliran slijedom smjernica okvira Basel II**
- **Regulativa:**
  - Zakon o kreditnim institucijama (poglavlje o operativnom riziku i o ostalim rizicima)
  - Odluka o primjerenom upravljanju informacijskim sustavom (rizik informacijskog sustava)
  - Smjernice (HNB-a) za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika (rizik informacijskog sustava)

Pitanja?

CENTAR INFORMACIJSKE SIGURNOSTI

Hvala na pozornosti!

CENTAR INFORMACIJSKE SIGURNOSTI