Predmet:
BEZBEDNOST INFORMACIONIH SISTEMA

VISOKA POSLOVNA ŠKOLA STRUKOVNIH STUDIJA
NOVI SAD

OSNOVI ZAŠTITE INFORMACIJA

9. UPRAVLJANJE BEZBEDNOSNIM RIZIKOM

Ciljevi

- **Razumeti i naučiti**:
  - koncept **bezbednosnog rizika**
  - **elemente procene bezbednosnog rizika**
  - vrste **modela za upravljanje rizikom**
  - **metodologiju procene rizika ISO/IEC 27005**
  - vrste i primeri **metoda za upravljanje/procenu rizika**
    - ❖*Kvalitativne*
    - ❖*Kvantitativne*

Primer: Model menadžmenta rizika

Politika zaštite

NIR, Arhitektura, Projektovanje i razvoj, Evaluacija, Testiranje, Sertifikacijai i akreditacija	Analiza osetljivosti IS, Detekcija malicioznih programa, Detekcija upada (IDS), Nadzor i kontrola	Upravljanje incidentom, Reinženjering, Re-sertifikacija i Re-akreditacija
Akvizicija	Operativni rad	Održavanje
Zaštite	Detekcija	Korekcija
Poverljivost	Integritet	Raspoloživost
Tehnologija	Procedure	Bezb. pouzdanost (*Assurance*)

Analiza i procena rizika

Analiza i procena pretnji

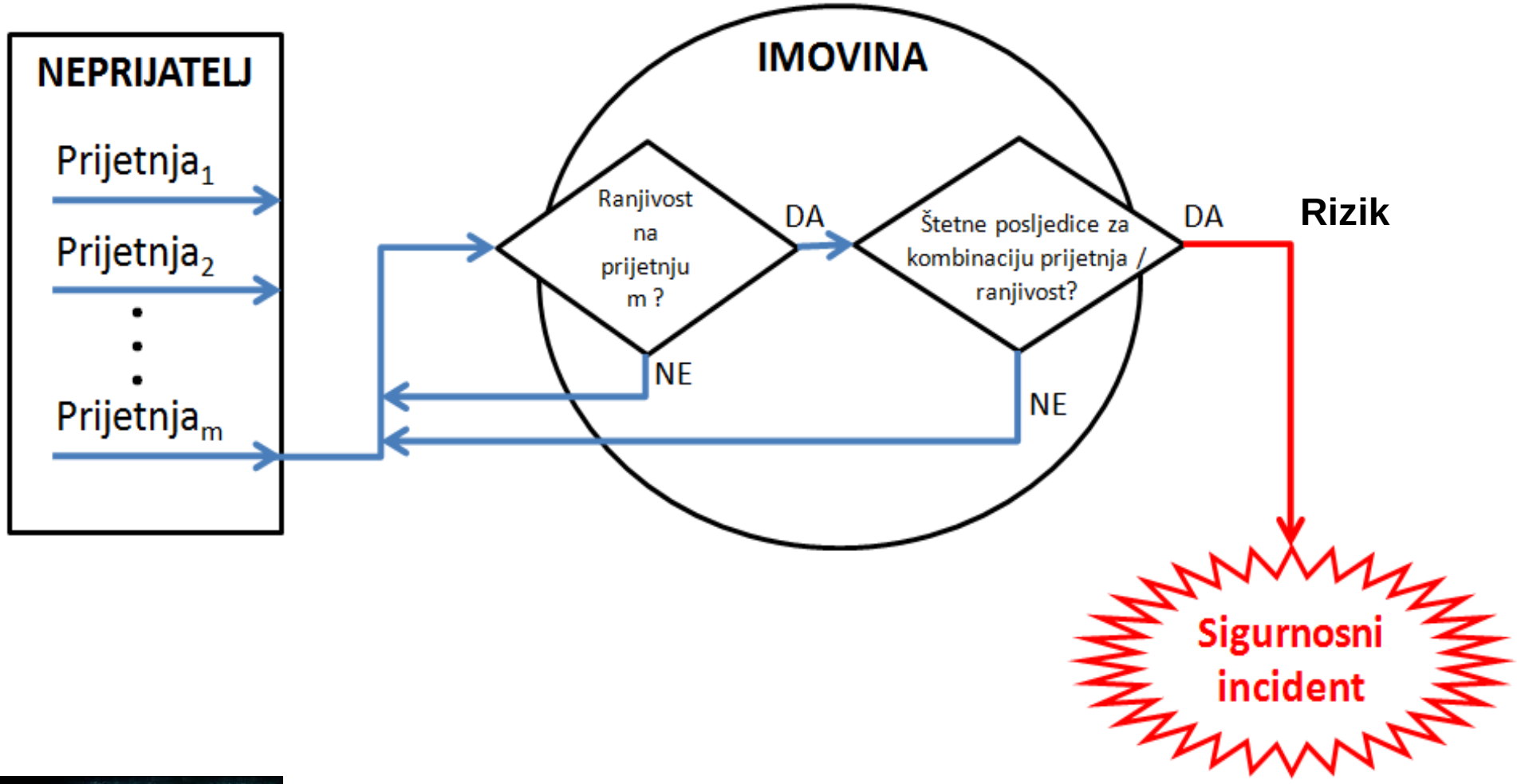
Svest o potrebi zaštite, obuka, obrazovanje

PRIMER: Šta je bezbednosni rizik?

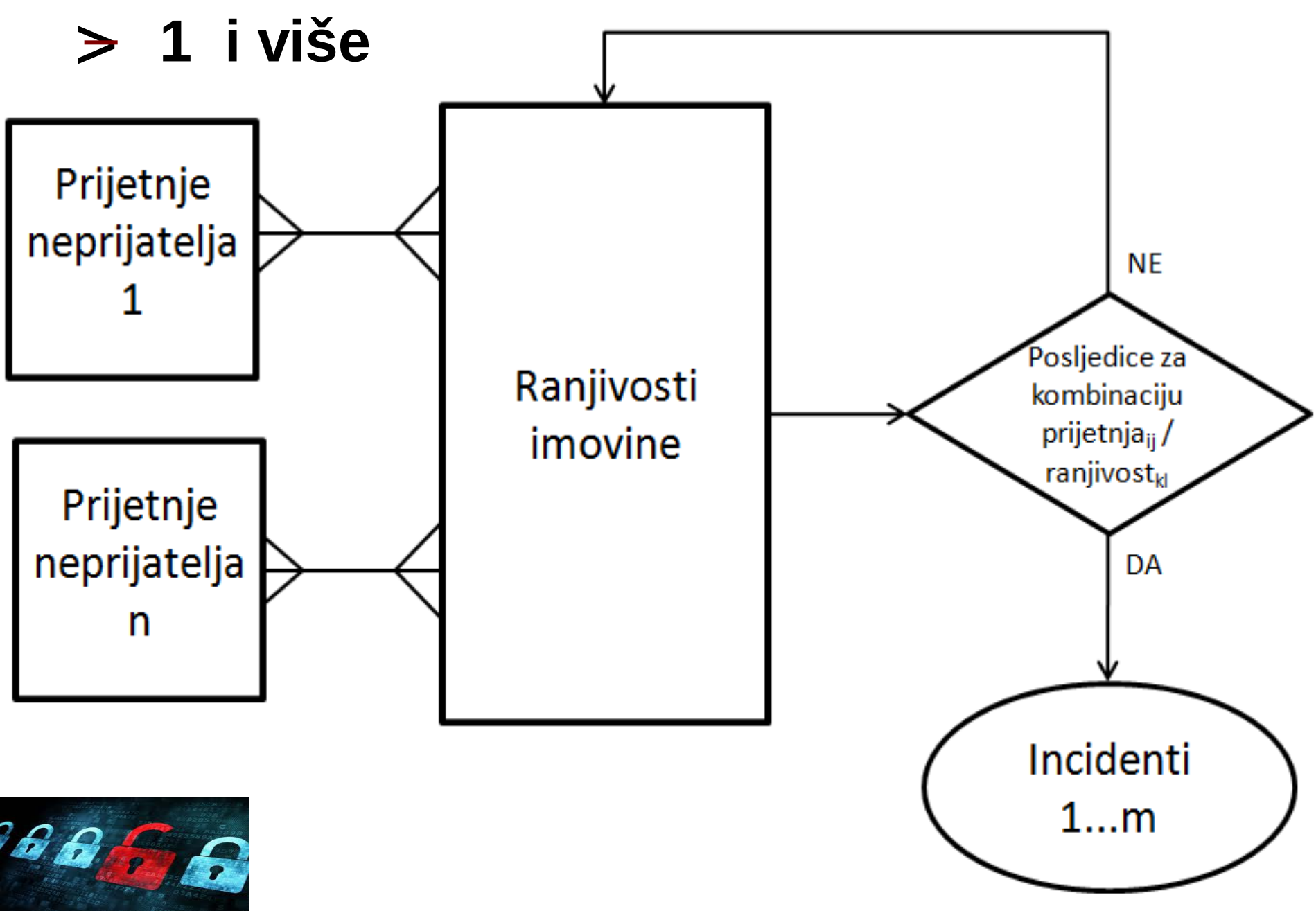
A *- imovina organizacije*
V *- ranjivosti imovine organizacije*
P *– pretnje za imovinu organizacije*
Rr *– relativni rizik*

Primer scenarija	Procena *A*	Procena *V*	Procena *T*	Procena *Rr*
Korpa sa mesom sa vukovima u šumi	Visoka	Visoka	Visoka	Visoka
Prazna korpa sa vukovima u šumi	Niska	Visoka	Visoka	Niska
Meso u hermetički zatvorenom kontejneru sa vukovima u šumi	Visoka	Niska	Visoka	Niska
Korpa sa mesom na kuhinjskom stolu	Visoka	Visoka	Niska	Niska

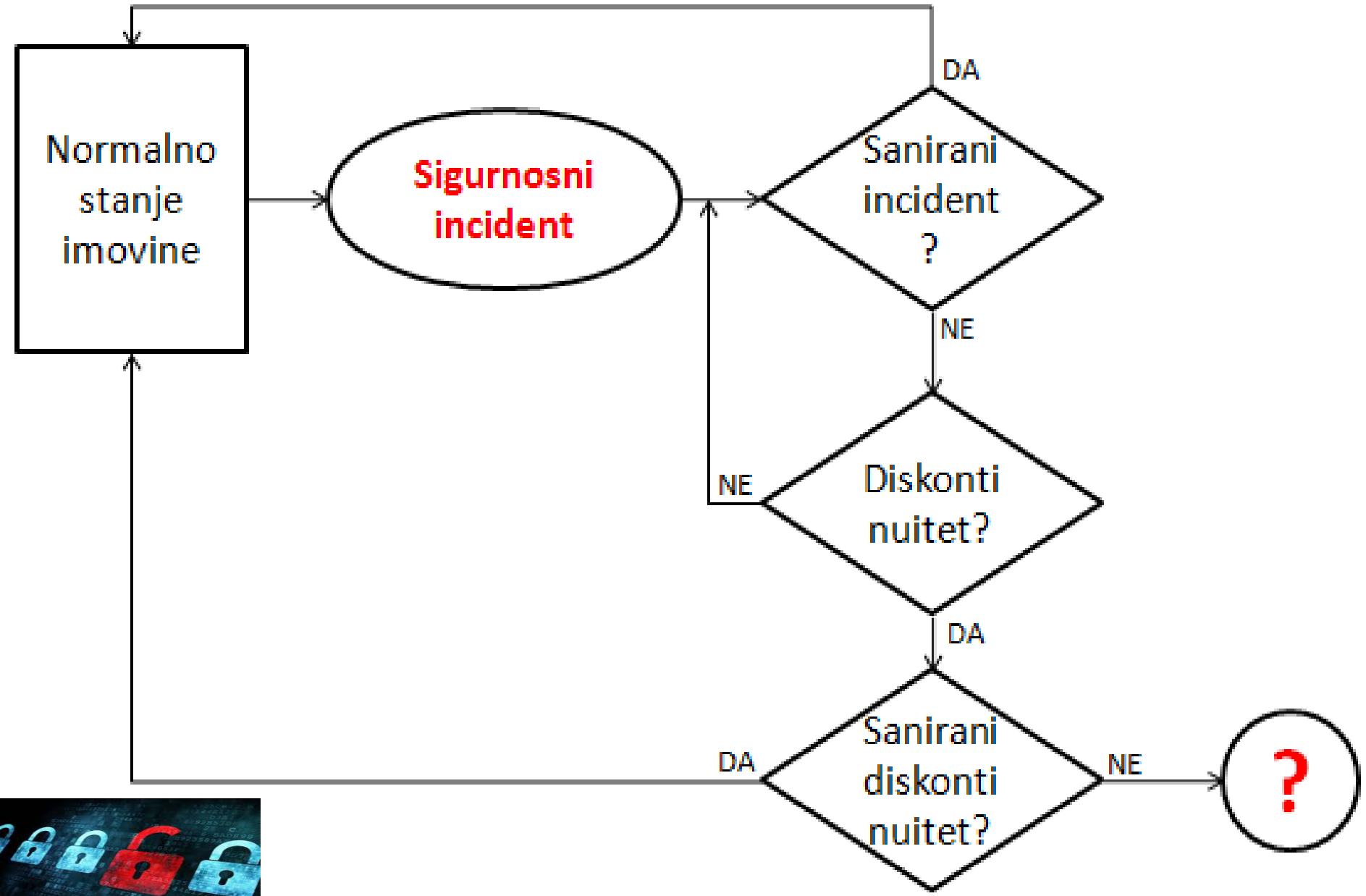
Primer: Fizički model rizika



Primer: Relacijski pristup fizičkom modelu rizika



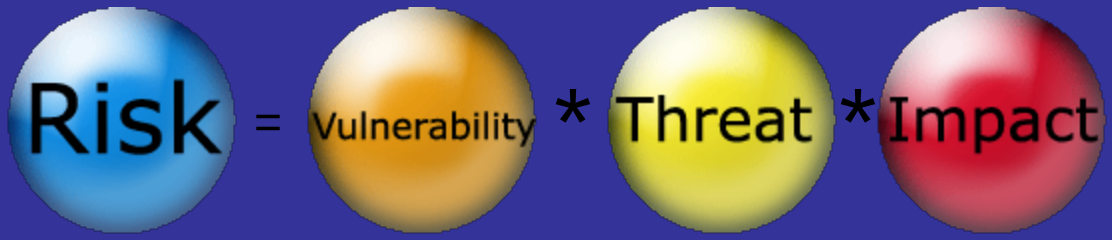
Primer: Oporavak bezbednosnog incidenta



Primer: Model pristupa proceni rizika

Povećati bezbednost = smanjiti faktore rizika

Rizik = Ranjivost * Pretnja* Uticaj



Primer: Model pristupa proceni rizika

Zašto je procena rizika važna?

Uticaj

Motivacioni faktor

Razlog zašto neko treba da uradi nešto – proceni rizik

Ranjivost

Problem

Indicira na šta se neko treba usmeriti

Pretnja

Katalizator

Koristi ranjivost ili ne **Nepredvidljiv događaj** koji nas primorava da nešto uradimo

Uzrokuje uticaj

Pretnja iskorišćava ranjivost

Primer: Model pristupa proceni rizika

Zašto je ovo važno?

Uticaj

- finansijski gubitak
- gubitak ugleda
- gubitak vremena
- gubitak *know -how*
- …

Ranjivost

- **Ljudske greške**
  - nedostatak k*now-how*
  - nedostatak interesa
  - zamor
  - …
- **Tehničke ranjivosti**
  - *nepečovan* OS
  - *nepečovane* aplikacije
  - otvorene mreže
  - WiFi *Bluetooth*
  - pogrešna konfiguracija sistema…

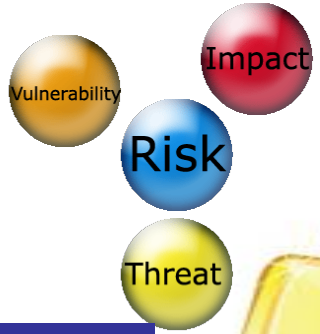
Pretnja

- **Namerne pretnje**
  - iznutra
  - izvana
  - fizičke
  - logičke
- **Nenamerne pretnje**
  - greške
  - kvarovi
  - konfiguracija …

Struktura znanja

Primer: Model pristupa proceni rizika

- **Ciljevi:**
  - *procena rizika potrebna za:*
    - *lica, organizacije i državnu administraciju*
  - ***nisu jednaki, ali su slični !!!!***



- **Topologija parametara rizika:**
  - *različita za različitr ciljeve*

Primer: Model pristupa proceni rizika

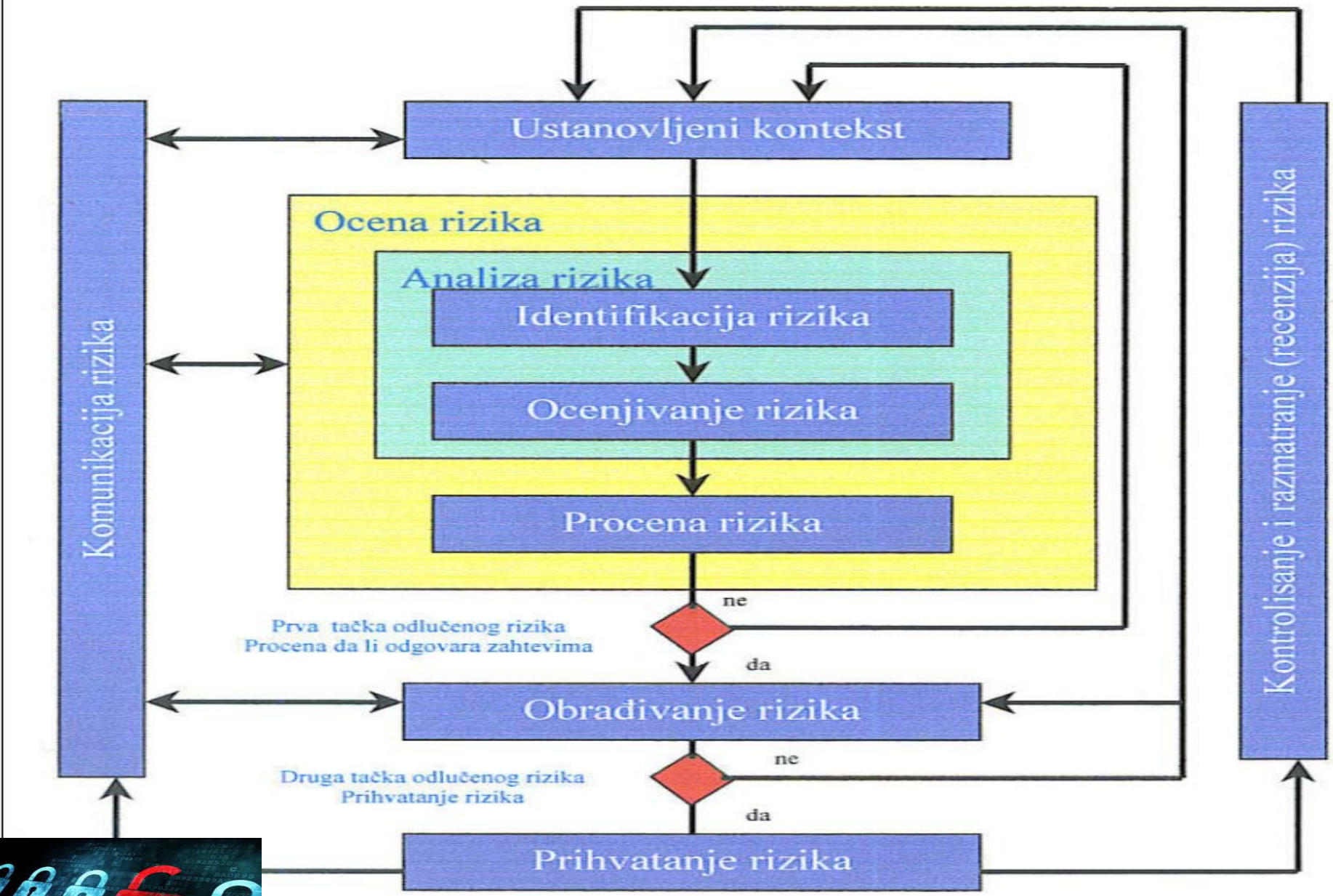
Dimenzije rizika

- Rizik se kreće u granicama između **0 i Rmax**:
  - Ako se izvrši normiranje rizika:
    - **Rmax = 1,** ne razmatra se jer predstavlja **siguran događaj** (nema nesigurnosti)
    - **R=0**, ne razmatra se jer predstavlja **nemoguć događaj** (nema nesigurnosti)
  - **Rmax** zavisi od unapred usvojenih granica vrednosti rizika, od strane menadžmenta, kroz politiku i procedure zaštite (npr: 100%)

Menadžment rizika (ISO/IEC 27005:2005)

1. Osnovni parametri menadžmenta rizika (A,V,T)
2. Definisanje obima i granica analize rizika
3. Uspostavljanje i organizacija tima za menadžment rizika
4. Uspostavljanje strukture i procesa procene rizika

Primer: Model menadžmenta bezbednosnog rizika ISO/IEC 27005



1. Osnovni parametri menadžmenta rizika

- **Kontekst za procenu rizika:**
  a. **Izbor** odgovarajućeg **pristupa z**a procenu rizika
  b. **Uspostavljanje kriterijuma za evaluaciju** rizika
  c. **Uspostavljanje kriterijuma za procenu verovatnoće** uticaja,
  d. **Uspostavljanje kriterijuma za prihvatanje i tretman** rizika
  e. **Određivanje potencijalno raspoloživih resursa za tretman rizika**

1. Osnovni parametri menadžmenta rizika

a. Izbor odgovarajućeg pristupa za procenu rizika

- **Formalna metodologija** za analizu rizika:
  - ISO/IEC TR 13335-3, **ISO/IEC 27005**
- Interaktivne programske **aplikacije:**
  - **HESTIA**, CRAMM, COBRA, vsRISK, RA2…,
- **OCTAVE** (***O****perationally****C****ritical,****T****hreat,****A****sset,&****V****ulnerability* ***E****valuation*):
  - analiza operativno kritičnih faktora rizika
- **BAR-brza** analiza kritičnih faktora rizika:
  - procenu A, T i V vrši tim organizacije (*brainstorming*)
  - procenu rizika vrši specijalista za upravljanje rizikom

1. Osnovni parametri menadžmenta rizika

b. Kriterijumi za evaluaciju bezbednosnog rizika informacija

1. Neki tipični kriterijumi

- **legalni i normativni zahtevi** i ugovorne obaveze
- posledice gubitka ***poverljivosti*** informacija i servisa
- posledice gubitka ***integriteta*** informacija i servisa
- posledice gubitka ***raspoloživosti*** informacija i servisa
- ***negativan uticaj na reputaciju***, konkurentnost i poslovanje…

1. Osnovni parametri menadžmenta rizika

c. Uspostavljanje kriterijuma za procenu verovatnoće uticaja zasniva se na:

- operativnim, tehničkim, finansijskim, legalnim, normativnim, socijalnim ili drugim kriterijumima,
- zavisi od interne politike organizacije, poslovnih ciljeva i interesa relevantnih učesnika,
- mogući su višestruki kriterijumi (npr, normativne, zakonske, ugovorne obaveze bez obzira na procenjeni nivo rizika)

1. Osnovni parametri menadžmenta rizika

d. Određivanje potencijalno raspoloživih resursa:

- izbor tima za ublažavanje (tretman) i upravljanje rizikom u organizaciji
- izbor kontrola zaštite
- implementacija kontrola zaštite
- sertifikacija i akreditacija sistema zaštite

1. Osnovni parametri menadžmenta rizika

f. Prihvatanje i tretman rizika zavisi od:

- odluke da li je faktor rizika, ispod ili iznad predefinisanog praga prihvatljivosti,
- mogući su i različiti nivoi praga prihvatanja rizika u rezličitim odeljenjima iste organizacije…

2. Definisanje obima i granica menadžmenta rizika

a. *Obim procesa menadžmenta rizika* određuju:

- **strateški i kratkoročni poslovni ciljevi** organizacije, procesi i strategije
- **politika zaš**tite organizacije
- **legalni i normativni zahtevi**
- **oblast primene**, npr., definisan sistem ili granica lokacije
- **opravdanje za isključivanje** nekog objekta iz obima procesa upravljanja rizikom

2. Definisanje obima i granica menadžmenta rizika

***b. Granice procesa upravljanja rizikom* uključuju:**

- **ciljeve i politiku** poslovanja
- **informacionu imovinu** organizacije - čistu, hardversku i humanu (zaposlene, partnere, podugovoraче, spoljne saradnike, klijente…)
- **fizičko okruženje** (zgrade i druge objekte)
- **društveno-kulturološko** okruženje
- **poslovne procese** i aktivnosti…

3. Uspostavljanje i organizacija tima za menadžment rizika

- **identifikacija i analiza** relevantnih učesnika
- **izbor lidera** tima
- **izbor članova** tima iz organizacije:
  - *izvršni menadžeri*
  - *praktičari koji rade u poslovnom procesu*
  - *pravnik organizacije*
  - *informatičari – administratori sistema i mreže*
  - *specijalisti zaštite,*
  - ***digitalni forenzičar***
- definisanje uloga i odgovornosti relevantnih učesnika
- Uspostavljanje odnosa i **potpune komunikacije** između članova tima i tima i organizacije

4. Uspostavljanje procesa analize i procene rizika

1.4.1. Komunikacija u procesu procene rizika

- **Predmet komunikacije**-članova *Tima za procenu rizika* sa relevantnim internim i eksternim učesnicima u svakoj fazi
- **Cilj komunikacije**-razumevanje procesa procene rizika za sve članove tima:
  - *sakupljanje informacija* za identifikaciju faktora rizika
  - *analizu toka informacija* za izbegavanje ili redukciju bezbednosnih incidenata
  - *konsultacije* za bolje međusobno razumevanja procesa upravljanja rizikom kod relevantnih učesnika,
  - *plan komunikacije* odnosnih pitanja treba razviti u ranoj fazi procesa procene rizika.

4. Uspostavljanje procesa analize i procene rizika

1.4.2. Procedura za upravljanje rizikom

- **Ciljevi:**
  - da **eksplicitno prenese stav organizacije** prema zaštiti
  - da **proaktivno** smanji potencijalni uticaj proboja SZ
- **Namena**:
  - da **obezbedi ponovljivost i sigurnost procesa** upravljanja bezbednosnim rizikom organizacije.
  - da **obezbedi sakupljanje i agregaciju informacija o riziku** za svaku procenu rizika
  - da **smanji verovatnoću proboja sistema zaštite**, zbog nerazumevanja relevantnih učesnika i donosioca odluka

4. Uspostavljanje procesa analize i procene rizika

1.4.3. Monitoring i revizija procesa menadžmenta rizika

- ***Monitoring***:
  - identifikuje promene okruženja i faktore rizika u ranoj fazi
  - inicira regularnu proveru menadžmenta rizika kod glavnih promena
- ***Cilj revizije***:
  - *odrediti **relevantnost** procene rizika , ako nije, redefinisati*:
    - kontekst za procenu *i* kriterijume za evaluaciju *rizika*
    - pristup i metodologiju za procenu *rizika i* opcije tretmana
    - metod komunikacije u procesu procene *rizika*
    - pristup i analizu rezultata monitoringa *(rizika*

4. Uspostavljanje procesa analize i procene rizika

1.4.3. Monitoring i revizija procesa menadžmenta rizika

- **Predmet revizije (provere)**:
  - legalni okvir i kontekst upravljanja rizikom
  - kontekst konkurencije/
  - potencijalnih napadača
  - kriterijumi za evaluaciju rizika
  - kategorizacija i vrednovanje imovine (**A**)
  - prag za odlučivanje o tretmanu rizika (R) (prihvatljiv/neprihvatljiv)
  - vrednovanje troškova kontrola zaštite za ublažavanje rizika

4. Uspostavljanje procesa analize i procene rizika

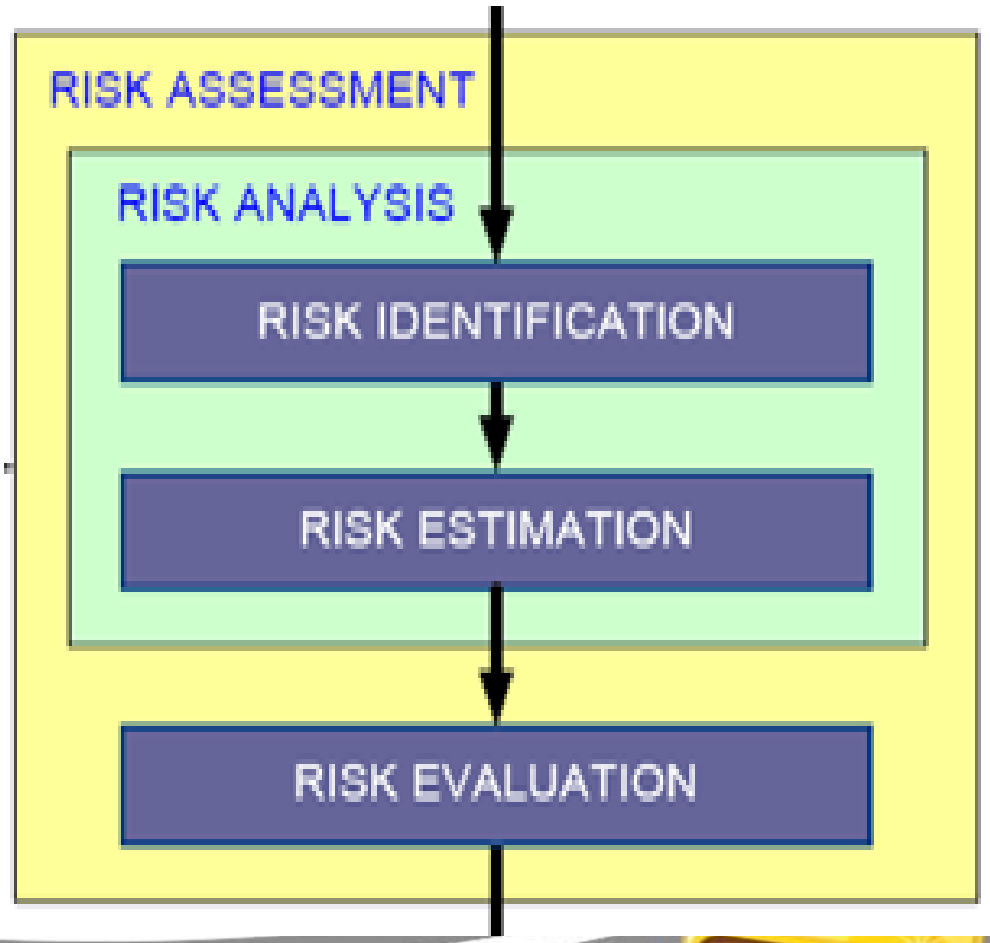
1.4.4. Proces procene rizika (Risk assessment)

- ***Uključuje:***

a. Analizu rizika:

  - *identifikaciju i*
  - *estimaciju rizika*

b. Evaluaciju rizika



4. Uspostavljanje procesa analize i procene rizika

a. Analiza rizika

Identifikacija -sveobuhvatna, struktuirana

- faktora rizika koje treba tretirati, pod i izvan kontrole organizacije
- ***imovine (A), pretnji (T), ranjivosti (V)***, (verovatnoće pojave- P_T, frekvencije -***f***, intenziteta - ***i***) i ***uticaja*** (poslovnih posledica, štete) ili ***verovatnoće*** da će pretnja/e iskoristiti ranjivost/i
- ***neprihvatljivih*** posledica rizika
- ***metodi*** za identifikaciju faktora rizika:
  - *ček liste, Intervjui, sistemska analiza i*
  - *sistem inženjerske tehnike*

Izlaz 1: *Inventar (vrednosti) informacione imovine*

Izlaz 2: *Taksonomija relevantnih pretnji*

Izlaz 3: *Taksonomija relevantnih ranjivosti*

4. Uspostavljanje procesa analize i procene rizika

a. Analiza rizika

- **<u>Estimacija (kvalitativna) parametara rizika</u>***:*
  - *Vrednosti imovine* **- *A****: N, S, V***
  - *Pretnji -**T**: N. S, V*
  - *Ranjivosti - **V**: N, S, V*

A = Pv + R+ I (ili +Po) ,

Pv-poverljivost, **R**-raspoloživost, **I-**integritet, **Po-**pouzdanost/ iskoristivost

V = DxKxTrxIsxZa

D-detektibilnost, **K** -korisnost, **Tr** -trajnost, **Is** -iskoristivost, **Za** –zaštićenost

- **T=T1+T2+...+T8= ∑ T**
- **Rr = AxVx ∑ T**
- **Rrp= (Rr/Mz) x Ut = ((AxVx ∑ T)/Mz) x Ut -** nivo preostalog rizika
- **Mz**–mere zaštite **(k/z -** osnovne, poboljšane**)**
- **Ut (**uticaj **= AxTixTfxTv ≡ OGG**

4. Uspostavljanje procesa analize i procene rizika

a. Analiza rizika

- **<u>Estimacija ukupnog rizika</u>:**
  - **Kvalitativna aproksimacija**, *uključuje faktor neodređenosti rizika – nizak (**N**), srednji (**S**), visok (**V**)*
  - *Relativni rizik* **- Rr= AxVxT (ili Rr=A+V+T – manje tačan)**
  - *Relativni preostali rizik* - **Rpr = (AxVxT)/Mz**,
    - **Mz -** efektivnosti postojećih/implementiranih kontrola zaštite
  - **Kvantitativna aproksimacija** *(statistička, numerička, uključuje faktor neodređenosti rizika) u novčanim vrednostima:*
    - **Metodi rentabiliteta** (*cost-benefit)* **smanjenja rizika***:*
      - **Atributi rizika***: **A**, verovatnoća realizacije pretnje – **Tp***
      - **OGG** (očekivani godišnji gubici)= ***Tp* x *A***

4. Uspostavljanje procesa analize i procene rizika

b. Evaluacija rizika

- priprema za izradu *plana tretmana rizika*
- razmatranje/izbor kriterijuma za evaluaciju rizika
- priprema procene rizika na bazi strogo utvrđenih kriterijuma:
  - bezbednosnih
  - značaja poslovnog procesa podržanog informacionom imovinom
  - potrebe tretmana rizika
  - potrebe preduzimanja hitnih aktivnosti za tretman rizika
  - komparacije nivoa estimacije faktora rizika sa pre-definisanim kriterijumima (rezultatima prethodne procene rizika),

Izlaz 1: *Lista prioriteta faktora neprihvatljivog rizika* i
Izlaz 2: *Lista prihvatljivih faktora rizika* (i sa **N** uticajem)

4. Uspostavljanje procesa analize i procene rizika

1.4.5. Proces procene (*assessment*) bezbednosnog rizika

- Identifikovanje potencijalnih ***uticaja*** na poslovanje
- Identifikovanje verovatnoće događanja *bezbednosno relevantnih incidenata* (realizovanih štetnih napada)
- *Incident* može uticati na ljude, poslovanje, procese, informacije itd.
- Na *verovatnoću uticaja* (**izloženost** - *verovatnoću da će pretnja iskoristiti datu ranjivost*) utiču:
  - *atraktivnost imovine za napadača*
  - *stepen težine iskorišćenja ranjivosti*
  - *motivacija napadača i*
  - *sposobnost napadača*

4. Uspostavljanje procesa analize i procene rizika

1.4.5. Proces procene (assessment) bezbednosnog rizika IS

- **Rezultate procene rizika** treba:
  - koristiti za identifikovanje opcija za *tretman rizika* i
  - dokumentovati u *politici zaštite* i *planu tretmana rizika.*
  - rangirati faktore rizika po prioritetu tretmana
  - grupisati faktore riziku u grupe sa **N, S, V** rizikom
  - faktore rizika procenjene kao **N**-*niske* smatrati prihvatljivim iako se tretman ovih faktora rizika ne zahteva
  - faktore rizika procenjene sa **S** i **V** treba tretirati (**V**-prioritetno)
  - dokumentovati u *izjavi o prihvatljivoti rizika* (**SoA**)

Izlaz: *Izjava o primenljivosti (**SoA**) ili Izveštaj o proceni rizika*

4. Uspostavljanje procesa analize i procene rizika

1.4.6. Plan tretmana rizika

- **Razmotriti opseg opcija za tretman rizika:**
  - *izbegavanje, transfer, prihvatanje, ublažavanje* faktora rizika
- **Priprema**:
  - *Plana tretmana rizika* i
  - *Implementacija plana tretman rizika*
- **Plan tretmana rizika:**
  - obezbediti odluku menadžmenta o prihvatanju rizika (SOA)
  - identifikovati faktore rizika koji se *izbegavaju, transferišu ili prihvataju*
  - identifikovati izabrane opcije za tretman neprihvatljivih faktora rizika
  - identifikovati kombinacije opcija za tretman rizika
  - izabrati *kontrole osnovne zaštite* za ublažavanja neprihvatljivih faktora rizika

Izlaz: *Plan tretmana rizika*

4. Uspostavljanje procesa analize i procene rizika

1.4.7. Implementacija plana tretmana bezbednosnog rizika IS

- **Rpr- preostali relativni rizik ostaje posle procesa tretmana**:
  - uvek ga ima - uticaj nizak, tretman skup
- Provera **Rpr posle tretmana**:
  - prema kriterijumima za prihvatanje rizika u procesu **C&A** SZ
- **Ako se pojavi neprihvatljivi faktor rizika posle revizije (provere)**:
  - treba ga ili prihvatiti ili ponovo procenjivati
- Rezultati procesa tretmana i prihvatanja rizika su osnova za **Plan (zaštite) implementacije tretmana rizika** koji obuhvata:
  - *akcije upravljanja, odgovornosti, prioritete, dinamiku, budžet, očekivani izlazi, merenja performansi i proces revizije*
  - *mehanizme za procenu nivoa implementacije na bazi kriterijuma za ocenu performansi, individualnih odgovornosti i drugih ciljeva i*
  - *monitorisanje kritičnih kontrolnih tačaka implementacije*

Izlaz: *Plan implementacije tretmana rizika ili Plan zaštite*

Metodi za procenu rizika

1. **Kvantitativne metode** *(statistička, numerička, uključuje faktor neodređenosti rizika) u novčanim vrednostima:*

- **Metodi rentabiliteta** (*cost-benefit)* **smanjenja rizika***:*
  - **Atributi rizika***: **A**, verovatnoća realizacije T –* ***Tv***, ***V***
  - **OGG** (očekivani godišnji gubici)= ***Tv*** **x** ***A***
  - **Vrste**: *NIST*, *IBM, vlade SAD/FIPS 65 , RISKCALC, BDSS, RISKWATCH...*

2. **Kvalitativne metode**:

  - **Rangiranje A,V,T i R sa: N, S, V; 1, 2, 3, 4, 5**
  - **Vrste**: **CRAMM***,* **OCTAVE,** *RISKPAC, MARION*, *Buddy System*....

CRAMM:

- **Faza 1** - Identifikacija i evaluacija imovine (**A**)
- **Faza 2** - Procena **T** i **V**
- **Faza 3** - Identifikacija, izbor *kontrola zaštite*, provera

Problem: održavanje ažurne baze podataka, cena komponenti

Primer: Metodi za procenu rizika

OCTAVE (Operationally Critical, Threat, Asset, and Vulnerability Evaluation)

- **nije moguće redukovati ili otkloniti sav rizik**
- **resursi za zaštitu uvek su ograničeni**
- **ne mogu se sprečiti svi napadi** na sistem
- **incidente treba prepoznati/neutralisati**, sistem oporaviti
- **optimalno iskoristiti resurse** za preživljavanje neophodnih funkcija IKTS i organizacije
- **koristi tri kataloga** informacija:
  1. **kritične imovine (A),**
  2. **pretnji (T) i ranjivosti (V)**
  3. **kontrole zaštite (praksa zaštite)**

Primer: Metodi za procenu rizika
OCTAVE i drugi metodi evaluacije rizika

OCTAVE	**Drugi tipovi evaluacije**
evaluacija organizacije (ne samo IKTS)	evaluacija IKT sistema
pažnja usmerena na praksu zaštite	pažnja usmerena na tehnologiju zaštite
strategijska pitanja	taktička pitanja
samo-vođena metodologija	vođena od strane eksperta (skupa)
adaptivna za većinu organizacija	specifična za svaku organizaciju
uravnotežuje: *operativni rizik, praksu zaštite i tehnologiju zaštite*	

Primer: Metodi za procenu rizika -Metod OCTAVE-

- **Analitički tim:**
  - **identifikuje** objekte organizacije
  - **usmerava analizu rizika na kritične objekte** (KO)
  - razmatra **pretnje i ranjivosti** (*proceduralne i tehnološke*) **KO**
  - **evaluira** faktore rizika u operativnom kontekstu
  - **planira** strategiju zaštite na bazi prakse zaštite
- **Trofazni metod evaluacije:**
  - **Faza 1:** Identifikacija i izrada profila pretnji **(T)**
  - **Faza 2:** Analiza ranjivosti **(V)**
  - **Faza 3:** Planiranje i razvoj strategije i plana zaštite

Primer: Metodi za procenu rizika
-Kriterijumi metoda OCTAVE-

- **Skup kriterijuma** uključuje zahteve metoda :
  - ***principa*** (npr. samo-vođenja***)***
  - ***atributa*** (različiti kvaliteti ili karakteristike procesa evaluacije)
  - ***izlaznih rezultata*** (očekivani rezultati svake faze i procesa evaluacije)
- **Metodi OCTAVE**:
  - **OCTAVE metod** (za srednje i velike organizacije) i
  - **OCTAVE –S metod** (za male organizacije)
- **Proces OCTAVE** je evaluacioni, definisan i zatvoren, a ne neprekidni:
  - *planiranje, implementacija, kontrola i korekcija sistema zaštite*
- **Poboljšanje prakse zaštite:**
  - **planira** implementaciju strategije zaštite kroz detaljne akcione planove (dnevne, nedeljne, mesečne,..),
  - **monitoriše** dinamiku sprovođenja i efektivnosti realizacije akcionih planova
  - **kontroliše** varijacije i preduzima odgovarajuće korektivne aktivnosti

Primer: Kritični koraci za automatizovano smanjenje rizika – (*QualysGuard*)

1. Otkriti glavnu imovinu IS (**A**)
2. Izvršiti bezbednosnu klasifikaciju imovine **A**
3. Izvršiti brzu i tačnu identifikaciju ranjivosti imovine (**V**)
4. Transformisati sirove podatake u informaciju – procena rizika u realnom vremenu
5. Obezbediti merenje trenda stanja bezbednosti IS za dinamičku kontrolu rizika
6. Integrisati procese za tretman rizika
7. Kontrolisati usaglašenosti (interne, eksterne) i redovno izveštavanje

Pitanja