Predmet:
BEZBEDNOST INFORMACIONIH SISTEMA

VISOKA POSLOVNA ŠKOLA STRUKOVNIH STUDIJA
NOVI SAD

OSNOVI ZAŠTITE INFORMACIJA

4. KONTROLE i SERVISI ZAŠTITE

CILJ

- **Razumeti i naučiti:**
  - koncept i strukturu **kontrola** zaštite
  - koncept **bezbednosne kategorizacije** zaštite
  - značenje termina ***servis zaštite***
  - prirodu različitih **podela servisa zaštite**
  - koncept opšteg, **tehničkog modela servisa zaštite**
  - servise zaštite u **distribuiranom IKT sistemu**
  - proces **implementacije** servisa zaštite
  - servise poverljivog provajdera zaštite (**TTPS**)

Koncept *kontrola zaštite* (k/z) - namena

- **Struktuira katalog k/z**:
  - dinamički, skalabilan skup k/z
  - osnovni elementi uputstava za korišćenje k/z
- **Obezbedi:**
  - lakši izbor adekvatnih k/z u sistemu zaštite
  - konzistentan i ponovljiv pristup za izbor k/z
  - preporuke za **osnovni s/z** sa **minimumom k/z**
  - zaštitu informacione imovine prema standardima za **bezbednosnu kategorizaciju i klasifikaciju**
  - NIST KATALOG osnovnih kontrola zastite

Kontrole (mere) zaštite (NIST)

- **Generička SE definicija funkcije *kontrole***:
  - dovodi izlazni podatak/signal na ulaz („-“ povratna sprega)
  - zahteva primenu korektivnih mera (t/n-t)
  - krajnja klasifikacija mehanizama/protokola s/z
  - interfejs mehanizma/protokola zaštite i korisnika
  - neka funkcija arhitekture sistema zaštite:
    - **tehničke** (*logička AC*: log događaja, AVP, VPN...)
    - **operativne** (*procedura*: restrikcija ulaza)
    - **upravljačke** (*dokument*: standard i *Politika zaštite*)
  - osnov za procese *implementacije*, *provere*, *C&A* s/z

Kontrola zaštite (k/z)

- **Kontrole zaštite su kodirana zamena atributa**:
  - *Etičkog i kulturološkog okruženja:*
    - svest o potrebi, odnos prema z.- **obezbeđuju etički okvir**
  - *Normativno-pravnog okruženja:*
    - zakoni i standardi zaštite – **obezbeđuju i obavezuju**
  - *Dokumenata zaštite:*
    - program, plan, politika, procedure - **obavezuju i nameću**
  - *Organizacione strukture:*
    - praksa zaštite – **kontroliše odgovornost i usaglašenost**
  - *Tehničkih sistema zaštite:*
    - tehnički servisi zaštite – **izvršavaju funkcije zaštite**

Karakteristike kontrola zaštite (NIST)

1. **Osnovne karakteristike k/z zasnovane su na:**
   – *hw/sw mehanizmima i procedurama zaštite….*
2. **Kvalitet kontrole:**

- **robusnost**: *osnovna (**o**), srednja **(s),** visoka* (**v**)
  - *jačinu funkcije zaštite i garantovan nivo zaštite*
- **fleksibilnost**:
  – *primenu različitih politika zaštite i potreba* org.

3. **Kompenzujuće k/z:**
   – *koriste se za sve IS, grupu IS, tipične IS*

Struktura i organizacija kontrola zaštite (NIST)

- **Katalog kontrola** zaštite sadrži tri sekcije:

1. **Bezbednosni ciljevi:**
   - *osnovna (**O**)*, *poboljšana (**P**)*, *jaka* (**J**) zaštita
2. **Opis.**
   - specifični zahtevi za svaku k/z za ***O,P,J*** z.

Mapiranja k/z:

- da se izbegne nepotrebno dupliranje k/z

NIST katalog kontrola zaštite

Dimenzije kontrole zaštite (NIST)

1. **Životni ciklus**
   - *dizajn*
   - *implementacija*
   - *upotreba/održavanje*
   - *odlaganje*
2. **Forma:**
   - *politike/procedure*
   - *procesi*
   - *tehnološka rešenja*

3. **Namena za:**
   - *prevenciju*
   - *odvraćanje,*
   - *detekciju*
   - *redukciju,*
   - *oporavak,*
   - *korekciju,*
   - *monitoring,*
   - *razvoj svesti*

Dimenzije kontrole zaštite – 1 (NIST)

4. Kategorija događaja:

- kontrola *gubitaka*
- kontrola *pretnji*
- kontrola *ranjivosti*

5. Karakteistike:

- *robusnost*
- *fleksibilnost*

6. Relevantni parametri implementacije kontrola:

- *cena*
- *benefiti*
- *prioriteti*

Organizacija k/z (NIST)

1. **Klase k/z:**
   - upravljačke kontrole (**U**)
   - organizaciono/operativne kontrole (**O**)
   - tehničke kontrole zaštite (**T**)
2. **Familije k/z**
   - gradivni blokovi klasa k/z
3. **Kontrole zaštite - k/z**
   - gradivni blokovi familija zaštite

Klasa upravljačkih kontrola zaštite -NIST

Sadrži 5 familija procesa zaštite:

1. *Upravljanje programom/sistemom zaštite*
2. *Bezbednosna procena i autorizacija*
3. *Planiranje sistema zaštite*
4. *Procena rizika*
5. *Akvizicija sistema i servisa zaštite*

Ukupno 42 kontrole zaštite

Klasa operativnih kontrola zaštite - NIST

Sadrži 9 familija*:*

1. *Svest o potrebi zaštite i obuka o zaštiti*
2. *Upravljanje konfiguracijom (promenama)*
3. *Planiranje kontinuiteta poslovanja*
4. *Upravljanje kompjuterskim incidentom*
5. *Zaštita integriteta sistema i informacija*
6. *Održavanje sistema zaštite*
7. *Zaštita medija*
8. *Fizička i zaštita okruženja*
9. *Personalna zaštita*

Ukupno 78 kontrola zaštite

Klasa tehničkih kontrola zaštite (NIST)

Sadrže 4 familije kontrola:

1. *Nadzor, revizija i odgovornosti*
2. *Kontrola pristupa (AC)*
3. *Identifikacija i autentifikacija*
4. *Zaštita sistema i komunikacija*

Ukupno 78 kontrola zaštite

Katalog kontrola zaštite (NIST)

- **Jedinstvena identifikacija k/z (ID)**
- **Klase i familija**:
  - skraćenica, npr. **VD** za *Vanredni događaj*
  - alfa-numerički **ID** nivoa robusnosti k/z:
    - **o** – *osnovna,* **p** – *poboljšana,* **j** - *jaka*
- **Broj k/z**: redosled značaja u okviru familije - prioritet implementacije

Primer: **VD-4.o** - 4. k/z u familiji *Planiranje VD* sa osnovnim nivoom robusnosti (**o**)

Sistem osnovnih k/z (OKZ) (NIST)

1. **Definisanje OK/Z** (*Baseline Security*): set **k/z za osnovnu z.**
   PRIMER: OKZ u OS Win 2k i >:
   - minimum kontrola zaštite, sistemski principi zaštite
   - obezbeđuju minimum zaštite za **B/K** (bezb. kategoriju)
2. **Potrebne i rentabilne k/z birati na bazi**:
   - *procene rizika i*
   - B/K/K* *informacione imovine*
3. **Svaka modifikacija mora se dokumentovati**
4. **U katalogu NIST k/z identifikovana su tri seta OKZ za**:
   - **N, S, V nivo zaštite** definisan u procesu **B/K/K**
   - lista **OKZ** daje se respektivno za svaki od **tri seta**

B/K/K* - bezbednosna kategorizacija i klasifikacija

Nivoi robusnosti (NIST)

- K/z u svakom od **3 seta OKZ:**
  - **NIST SP 800-53A, SP 800-53B, SP 800-53C**
  - kombinacija k/z od **3 nivoa** robusnosti

Primer:

- za **N rizik set OKZ** sadrži k/z sa **o** nivoom robusnosti
- za **S rizik set OKZ** - kombinuje k/z sa **o** i **p** nivoima robusnosti
- za **V rizik set OKZ** - kombinuje k/z sa **o, p** i **j** nivoima robusnosti

Relacija - *nivo robusnosti* : *OKZ* ***(NIST)***

- Ne postoji direktna relacija
- Odgovarajuće k/z biraju se za odgovarajuće nivoe OKZ

  Primer: neka k/z samo je na raspolaganju kao opcija za dopunu seta k/z

  Primer: NIST SP 800-53, v. 2009.

  – skup **OKZ** za **N** uticaj faktora pretnji ukupno (**198 k/z)**

  – sa **o** nivoom robusnosti: **42** U, **78** O**, 78** T k/z

Mapiranje k/z sa zahtevima zaštite (ZZ)

- Pomoću odgovarajuće **M**atrice za **P**raćenje **Z**ahteva – **MPZ*:**
  - –početi sa specifičnim i usaglašenim **ZZ**
  - –svaki **ZZ** mapira se prema odgovarajućoj k/z unutar seta izabranih OKZ

MPZ*- RTM (*Requirements Traceability Matrix*)

Mapiranje ZZ sa kontrolama zaštite (k/z)

- **1:1** (jedan prema jedan):
  - **1** ZZ rešava se sa **1** k/z
- **1:N** (jedan prema više):
  - **1** ZZ rešava se sa (više) **N** k/z
- **N:1** (više prema jedan):
  - više ZZ rešava se sa **1** k/z
- **N:M** (više prema više):
  - više (**N**) ZZ rešava se sa (više) **M** k/z

Primer: deo MPZ

Zahtevi zaštite	Mapiranje	Kontrole zaštite (k/z)
Zahtev br. 1	1:1	PS-1b
Zahtev br. 2	1:N	PE-2b, PE-3b, PE- 6e, PE-7b
Zahtev br. 3 Zahtev br. 4	N:1	CM-2e
Zahtev br. 5 Zahtev br. 6	N:N	IA-1e, IA-2e, IA-4b

Kontrole zaštite (ISO/IEC 27002:2005)

- **Standard ISO/IEC 27002:2005 ima 11 poglavlja**:

Procena i tretman rizika

1. *Politika zaštite*
2. *Organizacija zaštite informacija*
3. *Upravljanje informacionom imovinom organizacije*
4. *Zaštita ljudskih resursa*
5. *Fizička i zaštita okruženja*
6. *Upravljanje komunikacijama i operativnim radom sistema*
7. *Kontrola pristupa*
8. *Akvizicija, razvoj i održavanje IKT sistema*
9. *Upravljanje bezbednosnim incidentom za informacije*
10. *Upravljanje kontinuitetom poslovanja*
11. *Usaglašenost*

Kontrole zaštite (ISO/IEC 27002:2005)

- **11 poglavlja** pokriva **39 sekcija** i **133 k/z**
- Svaka *kontrola* ima **cilj** i **definiciju** kontrole
- Struktura *kontrola zaštite*:

Kontrola	Definicija kontrole zaštite sa izjavom koja se odnosi na potrebne kvalitete za ispunjavanje zahteva kontrole
Smernice za implementaciju	Uključuje informacije za implementaciju kontrole i smernice za ispunjavanje zahteva kontrole
Druge informacije	U nekim kontrolama se nalazi klauzula „druge informacije“, gde su reference na informacije koje se odnose na specifičnu kontrolu

Kontrole zaštite (ISO/IEC 27002:2005)

- **ISO/IEC 27002** - **uputstvo** za primenu **k/z** tipa **ŠTA:**
- **Uputstvo** koristiti za pisanje *politike i procedura z.*
- **Iz ciljeva k/z** - *derivirati* ***namenu politike*** zaštite
- **Detalji k/z** - za generisanje ***detalja politike/procedura***
- **ISO/IEC 27001 i ISO/IEC 27002** osnova:
  - **Okvira za upravljanje zaštitom** - **SMF** (*Security Management Framework*)

ISO/IEC 27002:2005

ISO/IEC 27002:2005 ANEX A

Revizija kontrola zaštite

- Kontrole zaštite **nisu statičke kategorije**
- Mogu se **revidirati i dopunjavati** na osnovu:
  - *prakse zaštite i iskustva* iz k/kriminala
  - *promena u zahtevima zaštite* u organizaciji
  - *pojave novih tehnologija* zaštite
  - *neke se k/z eliminišu, a druge dodaju*
  - dodavanje/brisanje/modifikacija k/z zahteva *rigoroznu* **raspravu, reviziju i konsenzus**

Kontrole zaštite (ISO/IEC 27002:2013)

- Ima **14 sekcija** i **114 kontrola zaštite**
- Neke kontrole iz prethodne verzje su ukinute
- Neke k/z su spojene, a neke redefinisane
- Iste promene su napravljene u **Anexu A** nove verzije ISO/IEC 27001: 2013
- Nova verzija olakšava implementaciju ISMS krajnjim korisnicima

Proces selekcije kontrola zaštite (NIST)

1. Početak procesa *formiranja s/z izborom k/z*

Poverenje u s/z informacija stiče se*:*

– pažljivom selekcijom **seta OKZ**

– implementacijom **definisanog seta k/z**

Proces selekcije k/z informacija:

– izbor inicijalnog **seta OKZ**

– kreiranje OKZ prema **ZZ** (mapiranje)

– **(idealno)** završeno u toku rane faze ŽC razvoja IS

– **procena rizika** organizacije (*plan tretmana, SoA*)

– dokumentovanje konačnog seta k/z u ***Planu zaštite***

Proces selekcije kontrola zaštite 1

1. korak:

B/K/K *OBJEKATA INFORMACIONE IMOVINE*

2. korak:

IZBOR MINIMUMA ODGOVARAJUĆIH ***OKZ***

3. korak:

PRILAGOĐENJE SETA ***OKZ*** *REZULTATIMA ANALIZE I PROCENE RIZIKA*

Proces selekcije kontrola zaštite 2

1. korak: B/K/K INF. IMOVINE

- **Iz *Plana zaštite* odrediti**:
  - granice i dekompoziciju sistema
  - kritičnost/osetljivost objekata sistema (A)
  - izloženost sistema napadima spolja (Te)
  - izloženost sistema napadima iznutra (Ti)
  - u izboru OKZ prvi korak je uspostavljanje **B/K/K**
  - **BK=(Up), (Ui), (Ur)=(U**ticaj na **p**overljivot**),(U**ticaj na **i**ntegritet),(**U**ticaj na **r**aspoloživost)
    =(N ili S ili V)(N ili **S** ili V)(N ili S ili **V**)=**V**

Proces selekcije kontrola zaštite 3

2. korak: Izbor minimuma odgovarajućih OKZ

- izabrati (za **N**) minimum k/z iz obaveznog seta OKZ
- izabrati dodatne minimalne k/z za **S** ili **V** uticaj **R**
- iz kataloga OKZ izabrati inicijalni set k/z na bazi *najveće vrednosti* BK**:**
  - najveći uticaj **N**-izaberu se OKZ za **N** uticaj rizika (**R**)
  - najveći uticaj **S**-izaberu se OKZ za **N** i **S** uticaj **R**
  - najveći uticaj **V**-izaberu se OKZ za **N,S** i **V** uticaj **R**
- inicijalni set OKZ - **baza k/z, uvećava se po potrebi**

Proces selekcije kontrola zaštite 4

3. korak: **Prlagođenje OKZ rezultatima procene ri*zika***

- Na bazi procene rizika *prilagoditi izabrani set OKZ*
- Navesti *povučene, zamenjene, modifikovane* k/z
- **Dokumentovati***:*
  - **sve** planirane/instalirane k/z u *planu zaštite*
  - *konačne k/z* selektovane/identifikovane
  - *obrazloženja* i **glavne razloge** za konačan izbor k/z
  - *objašnjenje* zašto k/z ispunjavaju **ZZ**
- **Osnova** za sertifikaciju/akreditaciju (C&A) sistema zaštite

Strategija izbora k/z za smanjenje rizika

1. **Napad postoji:**
   - **mera zaštite**: *implementirati adekvatne TK/Z*
2. **Napad iskoristiv** (postoji ranjivost):
   - **mera zaštite***: primeniti slojevitu zaštitu i projektovati adekvatnu arhitekturu IS i sistema kontrola zaštite*
3. **Troškovi napada < od dobiti napadača**:
   - **mera zaštite**: *povećati T/KZ da se povećaju troškovi napada*
4. **Gubitak suviše velik:**
   - **mera zaštite***: primena GAISP principa, višeslojna arhitektura zaštite, izbor optimalnih U,O i T k/z, ograničen obim osetljivih objekata...*

SERVISI ZAŠTITE

Misija i ciljevi sistema zaštite (S/Z)

- **Misija S/Z je da obezbedi:**
  - *bezbednost rada PIS i poveća efektivnost poslovnih procesa, održavanjem inf. Imovine na prihvatljivom nivou rizika*
- **Definicija s/z-** *logičke aplikacione jedinice koje se izvršavaju akcijama, uključujući***:**
  - *metode za implementaciju procesa zaštite*
  - *funkcionisanje ili transformisanje funkcija zaštite*
  - *implementaciju poslovnih pravila*
  - *rukovanje mehanizmima zaštite*
  - *implementaciju zahteva zaštite*
  - *dodavanje, pregledanje, modifikaciju mehanizama zaštite* itd.

Ciljevi servisa zaštite

- **Primarni i sekundarni**
- **Primarni ciljevi** s/z su:
  - zaštita **CIA informacione imovine** organizacije
  - uključujući **sekundarne ciljeve**:
- **Sekundarni ciljevi** s/z su:
  - **odgovornost** do individualnog nivoa
  - **neporecivost** izvršenih akcija
  - **autentifikaciju** pristupa
  - **garantovanu bezbednost** (*security assurance*)

Primarni ciljevi zaštite

1. **Zaštita poverljivosti informacione imovine:**
   - Npr. uskladištenih, procesiranih i prenošenih p/i
2. **Zaštita integriteta informacione imovine:**
   - Npr. sadržaja p/i,konfiguracije, sesije, konekcije
3. **Zaštita raspoloživosti informacione imovine:**
   - *tehničke i funkcionalne raspoloživosti*
   - od namernog/slučajnog, neovlašćenog korišćenja inf. imovine, odbijanja servisa (DoS/DDoS)...

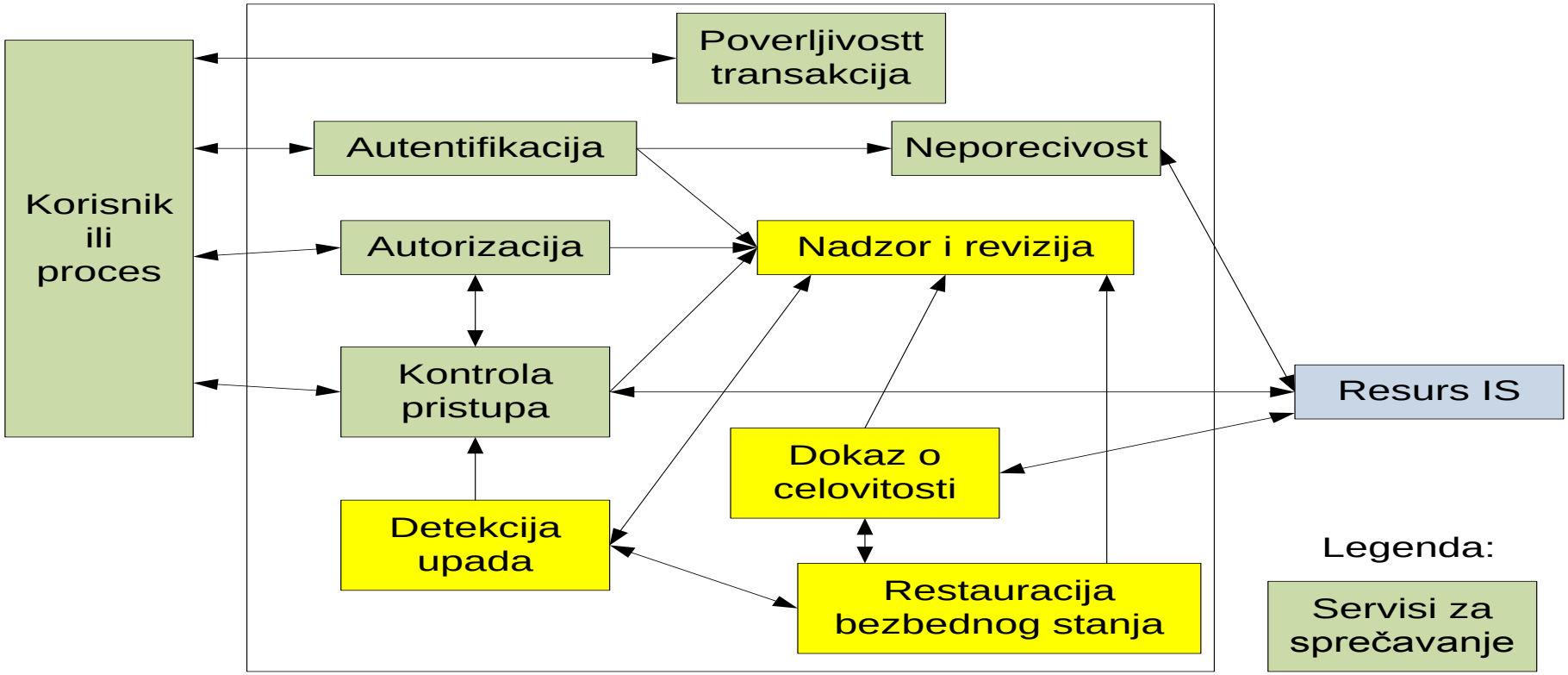
Sekundarni ciljevi zaštite

- **Utvrđivanje odgovornosti**:
  - **princip:** zahtev za odgovornost dokumentovati u *politici zaštite*
  - **uključuje:** *neporecivost, odvraćanje, izolaciju grešaka, detekciju, sprečavanje upada, oporavak, etički/normativni okvir*
- **Autentifikacija**: verifikacija identiteta (u zaštiti *integriteta*)
- **Garantovana bezbednost (*assurance*):**
  - osnova za sticanje poverenja da **U/O/T k/z** korektno rade
  - bitan **cilj zaštite**, neprekidan je proces (ciklično se obnavlja)
- **Realizacija ciljeva zaštite kroz:**
  - *korektnu implementacija k/z*
  - *dovoljan nivo zaštite od slučajnih grešaka* (korisnika ili hw/sw)
  - *dovoljnu otpornost s/z na namerni proboj* ili *zaobilaženje*

Model servisa zaštite

- **Generički model servisa zaštite:**
  - **Primarni:** *upravljački, org.-operativni, tehnički*
  - **Sekundarni** *za*: *podršku, oporavak*
  - **Kriterijum podele**: *primarna funkcionalna namena*
  - **Kontekst**: *međuzavisnosti primarnih i sekundarnih s*
- **Tehnički orijentisan model servisa zaštite,** za
  - *podršku (proaktivnu)*
  - *sprečavanje (proaktivno)*
  - *oporavak* (*reaktivan*)

Primer: Opšti tehnički model servisa zaštite



Zaštićene komunikacije
(od otkrivanja, zamene, modifikacije, ...)

Identifikacija (i imenovanja)

Upravljanje kriptološkim ključevima

Administracija sistema zaštite

Sistemska zaštita (najmanje privilegija, ponovno korišćenje, separacija procesa i.t.d.)

Legenda:

Servisi za sprečavanje

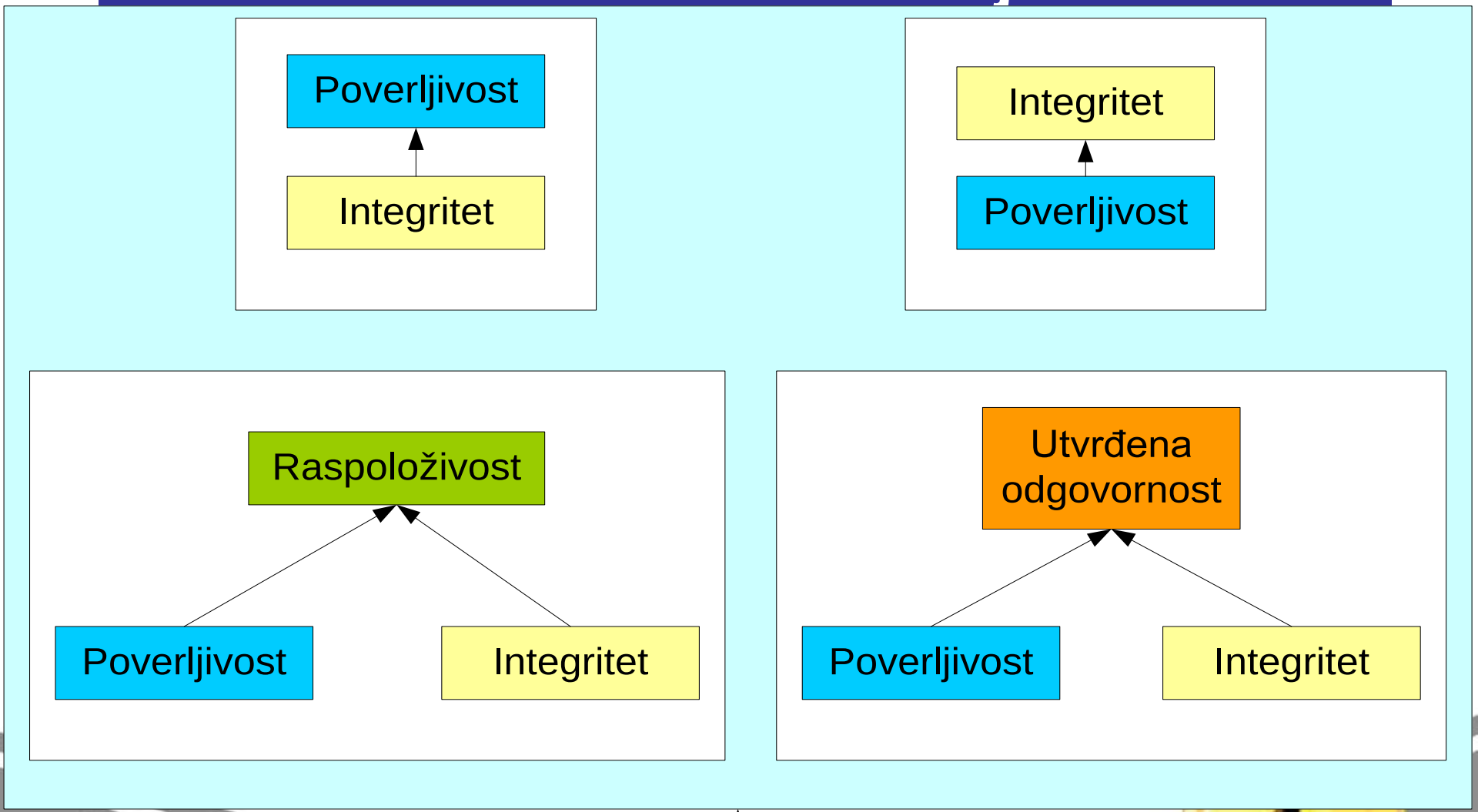
Servisi za oporavak

Servisi za podršku

Međuzavisnost servisa zaštite

- **Bezbednosni ciljevi servisa z.** su međusobno zavisni
- Cilj *zaštite poverljivosti* zavisi od cilja *zaštite integriteta:*
  - *Kako?*
- Cilj *zaštite integriteta* zavisi od cilja *zaštite poverljivosti:*
  - Kako?
- Ciljevi *zaštite raspoloživosti i kontrolisane odgovornosti* zavise od ciljeva zaštite *poverljivosti i integriteta:*
  - Kako?

Primer: Međuzavisnost ciljeva zaštite

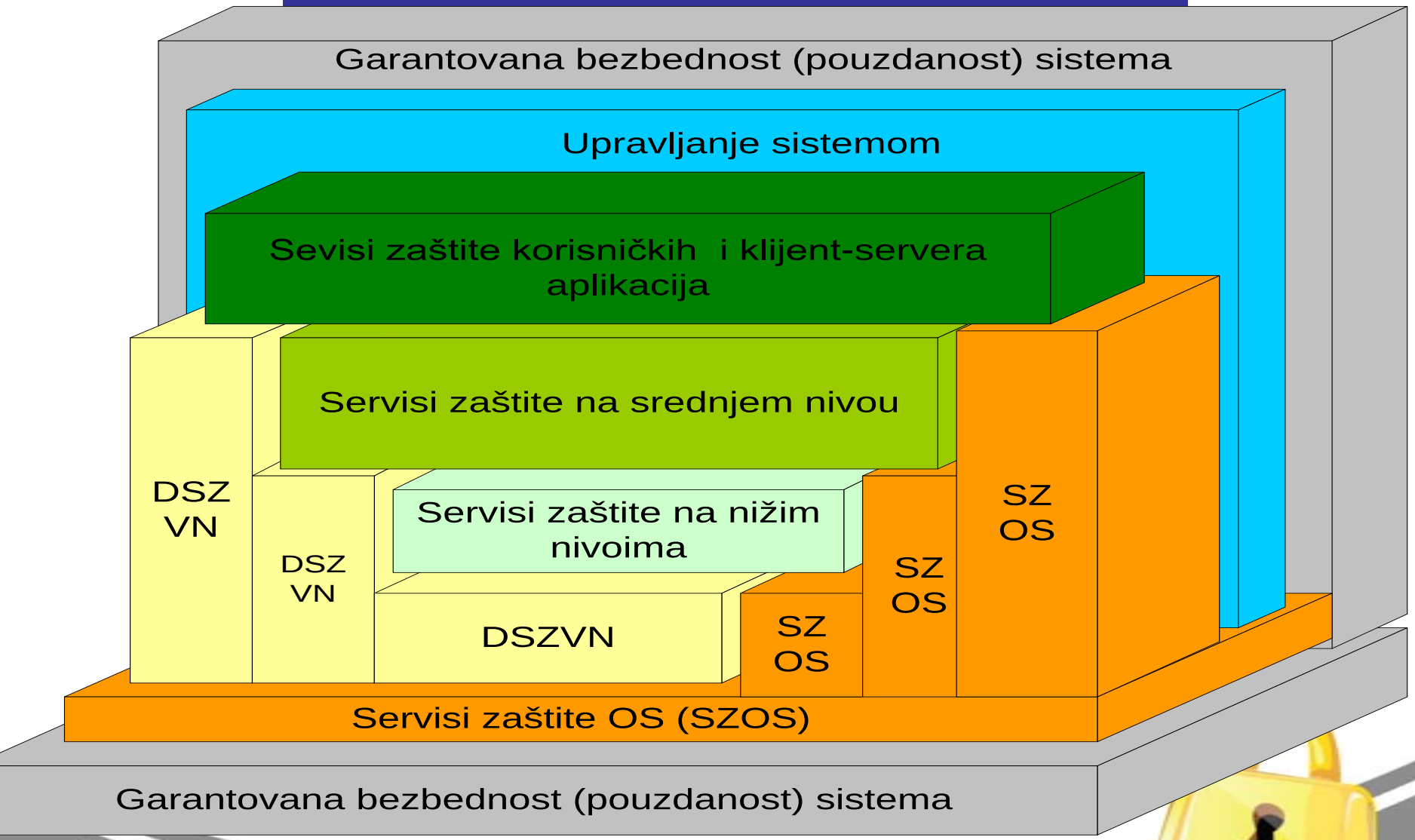


Garantovana bezbednost (assurance)

Servisi zaštite u distribuiranom IKTS

- Fizički i **logički** distribuirani IS (RM, **domen zaštite**)
- Svi **servisi** konačno zavise **od mehanizama OS**
- **Garantovana bezbednost** (pouzdanost) s/z je:
  - ključni aspekt sistema zaštite
  - obuhvata sve kapacitete sistema zaštite
  - u međuzavisnoj vezi sa svim ciljevima zaštite
- **Upravljanje sistemom zaštite (ISMS)** je:
  - drugi važan aspekat za efikasnost mera zaštite

Primer: Distribuirani servisi zaštite



DSZVN- distribuirani servisi zaštite na više nivoa
SZOS -servisi zaštite operativnog sistema (NOSSS)

Garantovana bezbednost

- **Odražava poverenje** da su ispunjeni svi ciljevi zaštite
- Direktno zavisi od **arhitekture** IKTS i **kontrola zaštite**
- Razvijene su tehnologije za merenje bezbednosnih nivoa (**SSE CMM**)
- **Garantovana bezbednost** se može povećati sa:
  - *primenom TCB* i manje kompleksnih tehničkih rešenja,*
  - *korišćenjem tehnički pouzdanih komponenti IKTS/SZ*
  - *modularnim projektovanjem i implementacijom **IDPS***
  - *Implementaijom proaktivne i prediktivne zaštite*
  - *implementacijom komponenti za oporavak sistema…*

TCB*(*Trusted Computing Base*) – poverljivi računarski sistem

Servisi zaštite u domenu zaštite (D/Z)

- **Koncept domena zaštite (D/Z)**:
  - **skup aktivnih objekata informacione imovine**
  - **zaštite inf. imovine na bazi** *zajedničke politike zaštite*
  - **obezbeđuje restrikciju toka i/p i procesa** unutar/između D/Z
  - **D/Z** tipično **deli demilitarizovana zona** (**DMZ**)
- **Podela D/Z:** *logički i fizički*

Primer:

- D/Z-e u IKTS ≈ **fizičkoj zaštiti zgrade**
- Logička barijera (*firewalls)* ≈ ograda oko zgrade
- *Gateways* ≈ kapija za ulazak u zgradu
- T servisi (*AC, IAA*) ≈ fizičko obezbeđenje u video nadzor

Domeni zaštite (D/Z)

- **D/Z se definišu** pomoću jednog/više kriterijuma:
  - **fizički** (npr. zgrade, kamp, region, itd.)
  - **poslovni procesi** (tj. personal, finansije, itd.)
  - **logički mehanizmi zaštite** (tj. na nivou OS, RM itd.)
- **Ključni elementi**:
  - fleksibilnost, projektovana i implementirana zaštita
  - međusobne relacije domena
- **Bezbednosni efekat deljenja** u **D/Z** (*gataways)***:**
  - ograničava oštećenja na jedan D/Z u slučaju proboja

Primer:

- **Tipični D/Z u RM -** *intranet, periferijska mreža (DMZ), ekstranet*

Domen zaštite - *intranet*

- **Interna mreža** organizacije, koja koristi **Internet tehnologije**
- Fizički distribuiran i povezan uređajima (često bez kontrole org.)
- Može se podeliti u *relativno nezavisne module* sa odvojenim *D/Z*
  - *slično vodonepropusnim vratima na pregradama broda*
  - *lakše se implementira politika zaštite*
  - *ograniče se gubici u slučaju proboja sistema zaštite*
- Za segmentaciju mreže koriste se **mrežne kapije** (*gataways)*
- Postoji više rešenja **segmentacije domena intraneta**:
  - obezbeđuju *polubezbedni* D/Z– DMZ sa *ograničenim servisima* za spoljne mreže

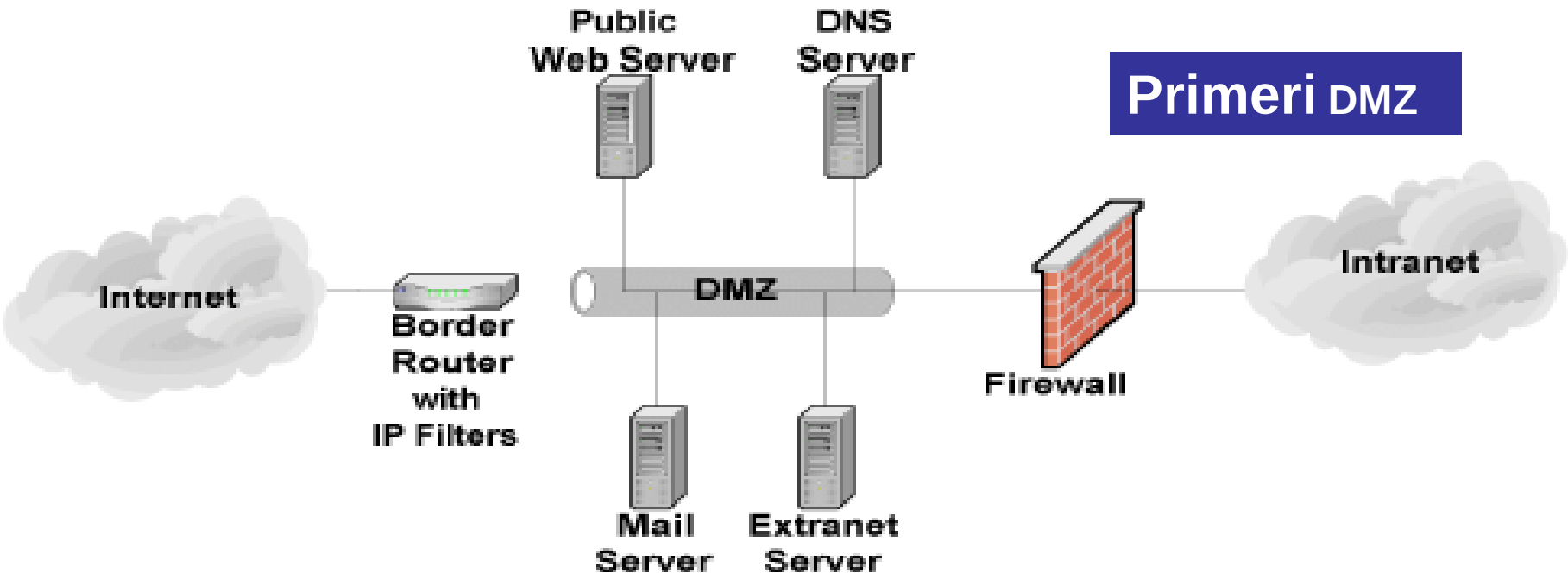
Domen zaštite - *periferijska mreža*

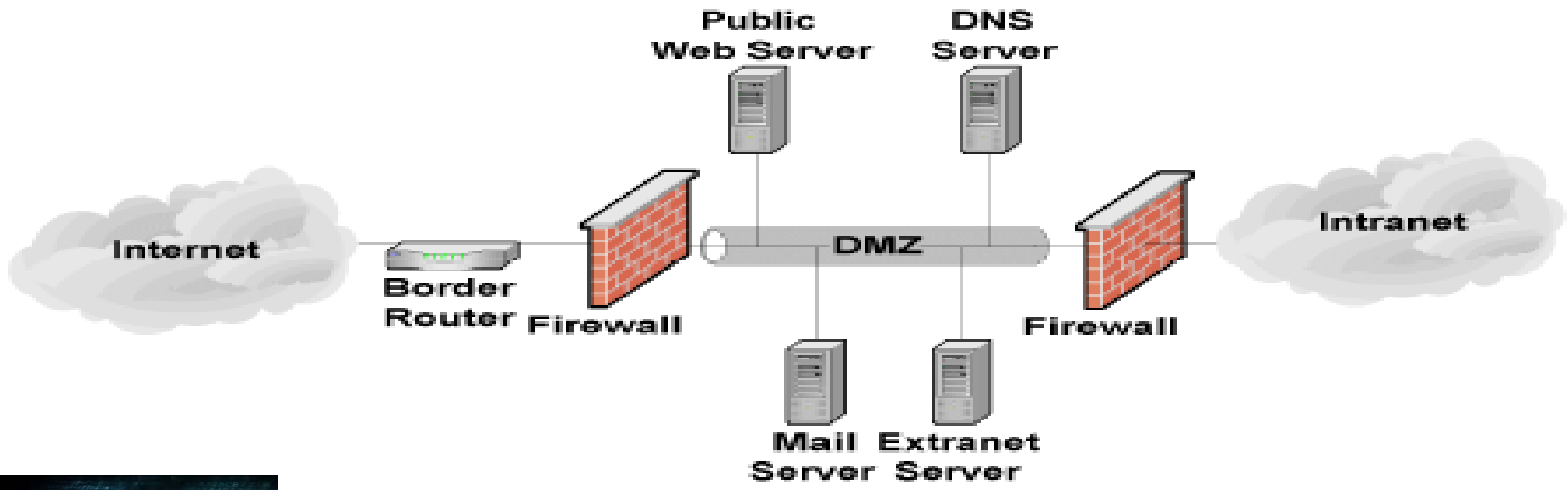
(zaklonjena podmreža, demilitarizovana zona – **DMZ)**

- **Segment RM između dve mrežne barijere** *(firewals)*
- Deli mrežnu infrastrukturu na odvojene *D/Z*
- Koristi se za *firewals* **zaštitu *web* servera**, dopušta:
  - **pristup** *HTTP protokolu* za *web* servise (port **80**), a ograničava sve druge protokole
  - **spoljni** *firewal* štiti *intranet* od pristupa sa **Interneta**
  - **unutrašnji** *firewal* sprečava odlazak zaposlenih na zabranjene *web* lokacije

Firewall – filtrira IP adrese

Primeri DMZ


Public
Web Server
DNS
Server
Internet
Border
Router
with
IP Filters
DMZ
Firewall
Intranet
Mail
Server
Extranet
Server


Public
Web Server
DNS
Server
Internet
Border
Router
Firewall
DMZ
Firewall
Intranet
Mail
Server
Extranet
Server

Domeni zaštite - *ekstranet*

- *Prošireni intranet* za pristup udaljenih korisnika resursima intraneta i deljenje informacija i servisa
- Pojam *eksternog okruženja* intraneta nije lako odrediti
- Realizuje se pomoću bezbedne *virtuelne privatne mreže* – **VPN** sa šifrovanom vezom (**IPSec**)
- **VPN** zahteva **dva VPN servera** ili **VPN server i klijent:**
  - za transakcije **izvan mreže** ili **interne** transakcije

Primer: *kriptozaštićen prenos od tačke-do-tačke*

Razvoj i implementacija servisa zaštite

- Vrše same organizacije ili *poverljivi provajder zaštite* (**TTPS**)
- U skladu sa **GAISP** i **najboljom praksom zaštite**
- **Projektovanje servisa zaštite** kroz **6 faza ŽCSZ***:
  - *Faza 1: Priprema*
  - *Faza 2: Procena rizika*
  - *Faza 3: Dizajniranje/projektovanje*
  - *Faza 4: Implementacija*
  - *Faza 5: Operativni rad*
  - *Faza 6: Odlaganje*

*Životni ciklus sistema zaštite

Pitanja