Predmet:
BEZBEDNOST INFORMACIONIH SISTEMA

VISOKA POSLOVNA ŠKOLA STRUKOVNIH STUDIJA
NOVI SAD

TEORIJSKA NASTAVA

Predavanja

- Information Systems Security
- The Internet of Things is Changing How We Live
- Malicious Attacks, Threats, and Vulnerabilities
- The Drivers of the Information Security Business
- Access controls
- Security Operations and Administration
- Auditing, Testing, and Monitoring
- Risk, Response, and Recovery

TEORIJSKA NASTAVA

Predavanja

- Cryptography
- Networks and Telecommunications
- Malicious Code and Activity
- Information Security Standards
- Information Systems Security Education and Training
- Information Security Professional Certifications
- Compliance Laws

PRAKTIČNA NASTAVA

Vežbe

- POLITIKA BEZBEDNOSTI
- ORGANIZACIJA BEZBEDNOSTI
- BEZBEDNOST LJUDSKIH RESURSA
- UPRAVLJANJE IMOVINOM ORGANIZACIJE
- KONTROLA PRISTUPA
- KRIPTOGRAFIJA
- FIZIČKA BEZBEDNOST I BEZBEDNOST OKOLINE
- OPERATIVNA BEZBEDNOST

PRAKTIČNA NASTAVA

Vežbe

- KOMUNIKACIONA BEZBEDNOST
- AKVIZICIJA, RAZVOJ I ODRŽAVANJE SISTEMA
- ODNOS SA DOBAVLJAČIMA
- UPRAVLJANJE INCIDENTIMA INFORMACIONE BEZBEDNOSTI
- ASPEKTI INFORMACIONE BEZBEDNOSTI U UPRAVLJANJU KONTINUITETOM POSLOVANJA
- USAGLAŠENOST

KONTAKT - LITERATURA

Kontakt:

- dr Predrag Ranitović dipl.ing
  predrag.ranitovic@gmail.com
  konsultacije: petak 17h-19h/kabinet 29

Literatura:

- Kim D., Solomon M. (2013), *Fundamentals Of Information Systems Security, Jones & Bartlett Learning*

  www.amazon.com

  – kako naručiti knjigu -

OCENA

Formiranje ocene:

- evidencija -

<u>Predispitne obaveze</u>

- Prisustvo na predavanjima i vežbama (70%) 5 poena
- predavanje MAX 4 izostanka
- vežbe MAX 3 izostanka
- 1 kolokvijum (vežbe) 15 poena
- 2 kolokvijum (vežbe) 15 poena
- Aktivnost (studije slučaja i radionice) 10 poena

(uslov za izlazak na ispit stečena 23 poena)

<u>Ispitne obaveze</u>

- Pismeni ispit 55 poena

(uslova za polaganje ispita stečena 26 poena)

100 poena

ISPIT

Ispit

- pismeni ispit – test - link -
- pitanja (zaokruživanje, da-ne, nabrajanje i definisanje)
- (prezentacije sa predavanja /pdf/ - knjiga) - lista pitanja

Plan održavanja ispita

- prema rasporedu održavanja ispita
- (npr. junski rok)

Nedeljni broj časova - predavanja

- 3 časa predavanja - u učionici

VEŽBE

Vežbe

- kolokvijum – vežbe - link -
- pitanja (logična pismena objašnjenja)
- (prezentacije sa vežbi /pdf/ - zadaci) - radionice/studije slučaja - praktični primeri

Plan održavanja kolokvijuma

- 1. kolokvijum – na sredni semestra (termin u vreme vežbi)
- 2. kolokvijum – na kraju semestra (termin u vreme vežbi)

Nedeljni broj časova - vežbe

- 2 časa vežbi – u računarskoj laboratoriji

OSNOVI ZAŠTITE INFORMACIJA

1. BEZBEDNOST I ZAŠTITA INFORMACIONIH SISTEMA

Ciljevi

Razumeti i naučiti:

- Semantičko značenje “*bezbednosti*”, “*sigurnosti*” i “*zaštite*”
- Funkcionalnu zavisnost *bezbednosti* i *zaštite*
- Ključne faktore bezbednosnog stanja IKT sistema
- Definicija sistema zaštite
- PIS (IKTS, IS, IT) kao objekat zaštite
- Opšti funkcionalni model sistema zaštite
- Optimalni sistem zaštite
- Novu pardigmu zaštite

Koncepti *termina* “*Bezbednost*”, „*Sigurnost*“, „*Zaštita*“

- „***Bezbednost***“ objektivno stanje zaštićenosti informacije
  - *Bezbednost* se postiže “***zaštitom***” informacija
- ***“Sigurnost*** “**-** subjektivan osećaj *bezbednosti*
- **B*ezbednost/sigurnost*** izaziva različite mentalne slike kod ljudi:
  - *fizičko obezbeđenje, lozinke, politička, ekonomska, državna...*
- **Cilj** *bezbednosti informacija**:*
  - *održavanje pouzdanog rada PIS i poslovnih procesa*
  - *donošenje poslovnih odluka na bazi procene rizika*
- **Stanje**:
  - Organizacije *bezbednost informacija* vide kao smetnju/teret?

*bezbednost informacija** = bezbednost informacione imovine (ISO/IEC 27001/2)

Informaciona imovina (ISO/IEC 27k)

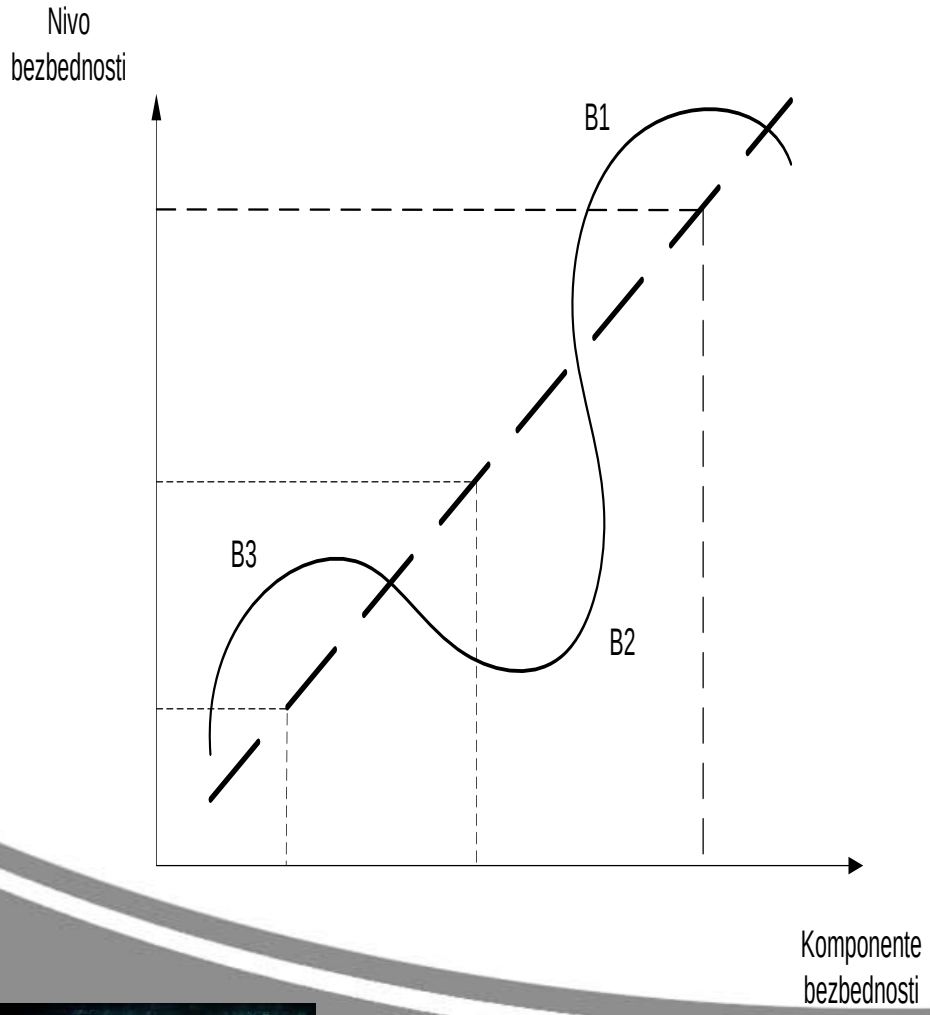
-*čista, fizička, humana*-

- **Čista:**
  - digitalni podaci i informacije
  - **opipljiva** informaciona imovina
  - **neopipljiva** inf. imovina (govor, znanja, tel razgovori...)
  - aplikativni programi
  - sistemski programi
- **Fizička:**
  - infrastruktura za podršku IKTS
  - kontrole okruženja IKTS
  - hardver IKTS
  - imovina IKTS
- **Humana:**
  - zaposleni,
  - nezaposleni
  - partneri ...

Filozofija zaštite informacija u 4 koraka

1. Identifikacija bezbednosnog stanja informacija (*revizija*)
   Izlaz = **ocena nivoa bezbednosti (n/b)**
2. Procena rizika (*analiza imovine, pretnji, ranjivosti, rizika*)
   Izlaz = **odobren prihvatljivi nivo rizika (SoA)**
3. Projektovanje, implem. i integracija sistema zaštite
   - ***upravljačkih, org. i tehničkih*** **kontrola (mera) zaštite**
   Izlaz = funkcionalno operativan sistem zaštite
4. Nadzor, revizija (kontrola) i održavanje sistema zaštite
   Izlaz = **održavanje n/b na prihvatljivom nivou rizika u svim fazama životnog ciklusa sistema**

Bezbednost informacija
-funkcija komponenti bezbednosti-



$$Bu = \sum_{j=1}^{n} kj \cdot Bj,$$

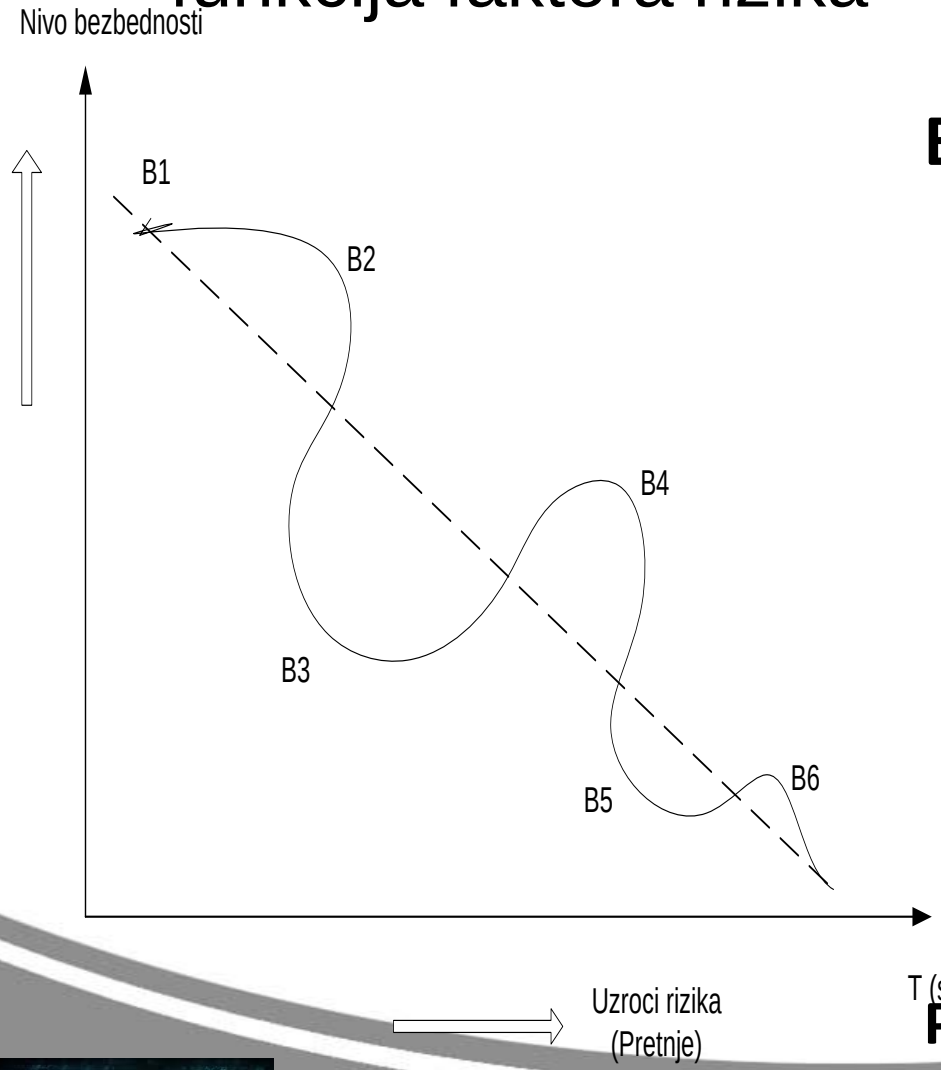
j= 1....n – komponente bezbednosti

kj = k1 .... kn - težinski faktori komponenti bezbednosti

Posledica: zahtev za sveobuhvatni pristup zaštiti!

Bezbednost IS

-funkcija faktora rizika-



$$Bu = \sum_{j=1}^{n} kj\,(Bj/Ri),$$

j= 1....n – komponente bezbednosti

kj = k1 .... kn - težinski faktori **uticaja** *faktora rizika*, komponenti bezbednosti

Ri = procenjeni, stohastički faktori rizika komponenti bezbednosti; **i= 1... n.**

Posledica: **redovna procena rizika**

Faktori bezbednosti savremenih IKTS

- **Faktori koji utiču na bezbednost IKTS:**
  1. ***Funkcionalni zahtevi IKTS***
  2. ***Organizaciona struktura IKTS i organizacije***
  3. ***Razvoj tehnologije***
  4. ***Ograničeni značaj politike zaštite***
  5. ***Obuka i razvoj svesti o potrebi zaštite***
  6. ***Praksa zaštite IKT sistema***

1. Uticaj funkcionalnih zahteva IKTS (PIS)

- **Kvalitet PIS presudan** za **upravljanje/odlučivanje:**
  - **Kvalitet PIS čine** *hardver*, *softver* i *bezbednost*
  - **Automatizacija PIS (BI*)** - skraćuje proces odlučivanje
  - **Kvalitet informacija (CIA**)** – kritičan, funkcija vremena**??**
  - **Bezbednost informacija = Kvalitet informacija**

6. **Bezbednost/zaštita informacija:**
   - zahteva menadžment rizika, planiranje i održavanje zaštite, kompatibilne sa dinamikom razvoja e-poslovanja, IKT...
7. **Rešenje:**
   - Sistem zaštite mora da prati razvoj PIS (tehnološki, organ.)

BI* - *Poslovna inteligencija*

****CIA** (*Confidentiality, Integrity and Aviability*) – **poverljivost, integritet, raspoloživost**

2. Uticaj organizacione strukture

1. **Problem**:
   – česte promene organizacione strukture utiču na:
     - obezbeđivanje kompetentnog specijaliste zaštite
     - obezbeđivanje izvršnih menadžera za podršku
2. **Rešenje**:
   – *kombinovana primena upravljačkih i operativno-organizacionih kontrola zaštite*

3. Uticaj razvoja tehnologije

1. Trend razvoja IKT:

- *integracija upravljanja sistema i procesa*
- *automatizacija* poslovanja (PIS, e-Uprave...)
- *razvoj nivih oblika računarstva* (BI, *Cloud Computing*...)

2. Trend razvoja tehnologija zaštite - sledi ž/c IKT:

- *brz razvoj IKT* - utiče i na razvoj tehnologija zaštite
- zaštita se implementira pri kraju ž/c IS (*Firewalls, AVP*,...)
- sve poslove zaštite *nemoguće automatizovati*
  - ***uloga čoveka u zaštiti*** *- nezamenljiv i kritičan faktor*
- *sofisticirani napadi su ispred tehnologija zaštite*

3. Rešenje:

- *Brzi razvoj IKT zahteva brzi razvoj tehnologija zaštite*

4. Uticaj politike zaštite

1. **Procesi zaštite** - nisu dovoljno razvijeni:
   - odluke na bazi predefinisanih *politika zaštite*, ne procene **R**
   - upravljanje zaštitom na bazi **statičke** *politike zaštite*
   - pristup dobar za strategijske odluke, ne i taktička rešenja
2. **Dinamički promenljive pretnje**, zahtevaju:
   - rešenja zaštite na bazi *procene rizika u realnom vremenu*
   - *proaktivni i prediktivni* (inteligentni) *pristup* i brzo reagovanje
   - *upravljački okvir zaštite* (**SMF**) na bazi *mikroanalize **R***
   - fokus procesa zaštite na poslovne zahteve i *oper*. *rizik*
3. **Rešenje:**
   - *Politiku zaštite ažurirati u skladu sa redovnom procenom rizika*

5. Uticaj obuke i razvoja svesti o potrebi zaštite

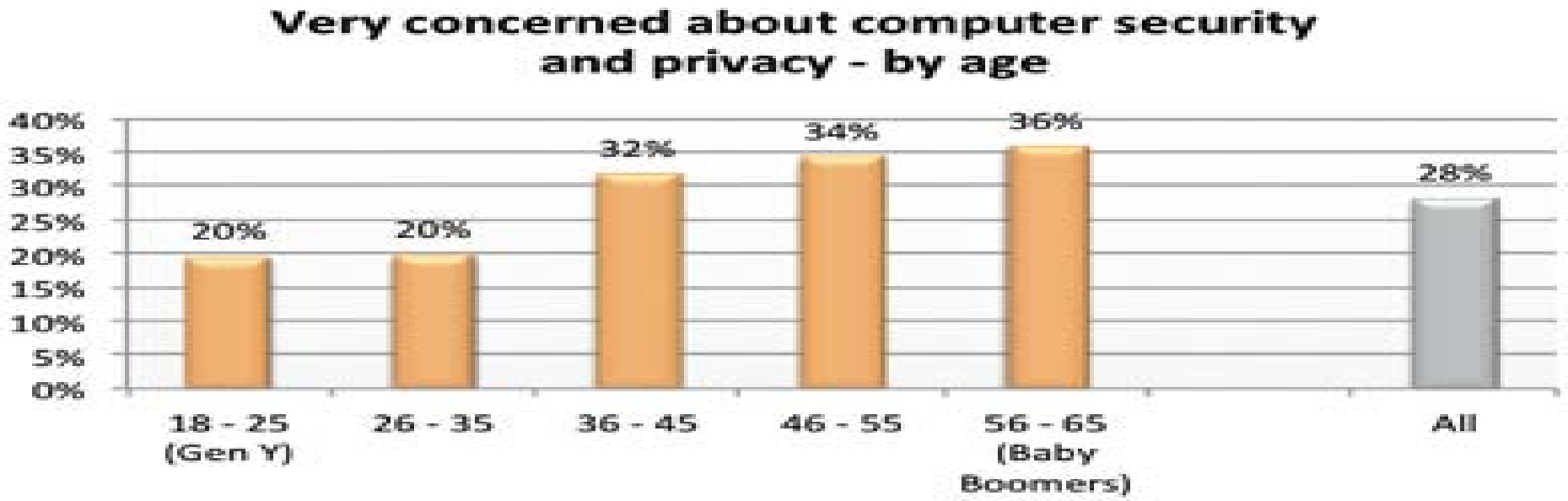
1. Problemi:

- složenost IKTS i tehnologija zaštite zahteva aktuelna znanja
- nedovoljna svest o potrebi zaštite, znanja i veštine:
  - *menadžera* o potrebi upravljanja rizikom i sistemom zaštite
  - *korisnika* o potrebi kontrole zaštite i ublažavanja uticaja rizika

2. Rešenje:

- *uvođenje regularnih programa obuke i razvoja svesti*
- *uvođenje procesa za upravljanje operativnim rizikom*
- *obezbediti praćenje i razumevanje realnog rizika*
- *manje forsiranje primene tehničkih rešenja zaštite*
- *obezbediti sveobuhvatni pristup zaštiti*

Odnos korisnika prema zaštiti informacija (2012)



- Prioritet zaštite informacija/računara sa godinama starosti
- Korisnici starosti 18 – 25 su preterano samouvereni u svoje znanje o zaštiti
- Korisnici starosti 18 – 25 imaju manje sofisticiranu zaštitu zbog finansijskih i tehničkih prepreka
- Iako su osetljivi podaci uskladišteni na računaru većina ne sprovodi najbolju praksu zaštite

6. Uticaj prakse zaštite

1. **Kompleksnost** IKTS:
   - *prepreka za koherentan sistem zaštite*
   - *ranjivosti softvera* (*agilna* proizvodnja, zatvoreni kod...)
2. **Kompleksnosti**, **distribuiranosti i umrežavanje** zahtevaju**:**
   - *skalabilnost* (nadogradivost) tehnologija zaštite
   - *primenu* u savremenim Internet tehnologijama (**BI, CC**)
   - *jaku autentifikaciju* u e- poslovanju
   - *standard poverenja* na Internetu **(PKI?!)**
   - *borbu protiv kompjuterskog kriminala...*
3. **Rešenje:**
   - *Taktiku primene tehnologija zaštite usklađivati sa zahtevima*

Savremeni PIS – objekat zaštite

1. Osnovne tehološke karakteristike PIS:

- RM OSI/Internet modela, visoko-distribuiran, klijent - server
- višeslojne (3-, 4 - slojne) arhitekture sw komponenti
- visoko umrežen/Internet tipa (*intranet*, *ekstranet*)
- virtuelizacija (SOA, *Cloud computing*...)

2. Osnovni zahtev sistema zaštite (S*I*Z) u svim fazama ž/c:

- *računarski sistem (RS)* - osnovna tehnička komponenta **S*I*Z**
- *smanjenje kompleksnosti PIS/SZ* primenom:
  1. *Sistemske analize* (**SA**) i *sistemskog inženjerstva* (**SE**)
  2. *Modelovanja (struktuirano i objektno-orijentisano - **OOM**)*
  3. ***Procesnog pristupa (*PDCA, SSE CMM ...)***

Savremeni PIS – objekat zaštite

1. ***Sistemska analiza* (SA) i *sistemsko inženjerstvo* (SE)**:
   – Intelektualni alati i iskustva iz drugih industrijskih disciplina

2. ***Struktuirano modelovanje:***

- *aktivni subjekti, pasivni objekti, pravila*
- *razmatra se*:
  – **namena** - funkcionalne ka-ke i kvalitet informacija
  – **zaštita objekata PIS** - *procesa, procedura, programa...,*
  – **zaštitu informacija** - *CIA*

Primer*:* Modelovanje logičke kontrole pristupa (LAC) računarskom sistemu

Savremeni PIS – objekat zaštite

2. Objektno orijentisano modelovanje (OOM):

- *svi su objekti ravnopravni – dekompozicija*
- *enkapsulacija ponašanja – vidljivi samo interfejsi*
- *polimorfizam i nasleđivanje*

- ***Grana objekata informacione imovine*** (*struktuira cilj zaštite*):
  - **CIA** informacione imovine ***(ISO/IEC 27001:2013)***
- ***Grana objekata za zaštitu*** (*struktuira sredstva zaštite*):
  - *upravljačke kontrole zaštite* (normativi, standardi, regulative)
  - *organizaciono-operativne kontrole (*proceduralne *mere*)
  - *tehničke kontrole* (hardversko-softverski alati)

3. Procesni pristup (PDCA=PPPP, ISO/IEC 27001:2013)

Osnovni zahtevi za sistem zaštite

1. Sprečavanje, detekcija, oporavak *informacione imovine* od:

- ugrožavanja bezbednosti lica, organizacija i države
- krađe, pronevere, gubitaka, izmene
- neovlašćenih aktivnosti u RS i RM, razne zloupotrebe
- povreda intelektualne imovine, privatnosti i poverljivosti

2. Obezbeđivanje informacione imovine (PS* u celini) kroz:

- efektivnu i efikasnu zaštitu
- kvalitetno upravljanje zaštitom

PS* - Poslovnii Sistem

Definicija sistema zaštite

– *Organizovan i koherentan skup **ljudi** i **mera** (**U, O i T** kontrola) i njihovih veza i ograničenja, primenjenih na informacionu imovinu, da bi se zaštitila **CIA,** a time održao/povećao:*
  - *željeni nivo bezbednosti informacione imovine (PS),*
  - *obezbedilo namenjeno funkcionisanje i izvršavanje poslovnih ciljeva i misije organizacije*

Sistem zaštite

- **Gradivni blokovi sistema zaštite:**
  1. ***servisi***
  2. ***mehanizmi***
  3. ***kontrole zaštite***

1. Servisi zaštite:

- logičke aplikacione jedinice izvršene kroz **različite akcije**:
  - *metode za implementaciju kontrola zaštite,*
  - *funkcionisanje ili transformisanje bezbednosnih funkcija (**Bf**),*
  - *implementacija politika, rukovanje mehanizmima zaštite ...*

2. Mehanizmi i protokoli zaštite:

- *u logičkom smislu – sredstva za realizaciju servisa zaštite*
- *algoritmi, metodi ili hw-sw moduli za izvršavanje **Bf***
- *neki su mehanizmi za jedan, a neki za više različitih servisa*

Primer: *kriptografski* mehanizmi za digitalni potpis.

Sistem zaštite

3. *Kontrole zaštite*:

- koriste se za upravljanje mehanizama zaštite
- konačna klasifikacija mehanizama zaštite
- bezbednosna funkcija arhitekture sistema zaštite
- interfejs između mehanizma zaštite i čoveka
- implicira suštinsku potrebu neprekidne *kontrole* sistema zaštite

Primeri*: proceduralne (*U, O) i tehničke (T) kontrole zaštite.

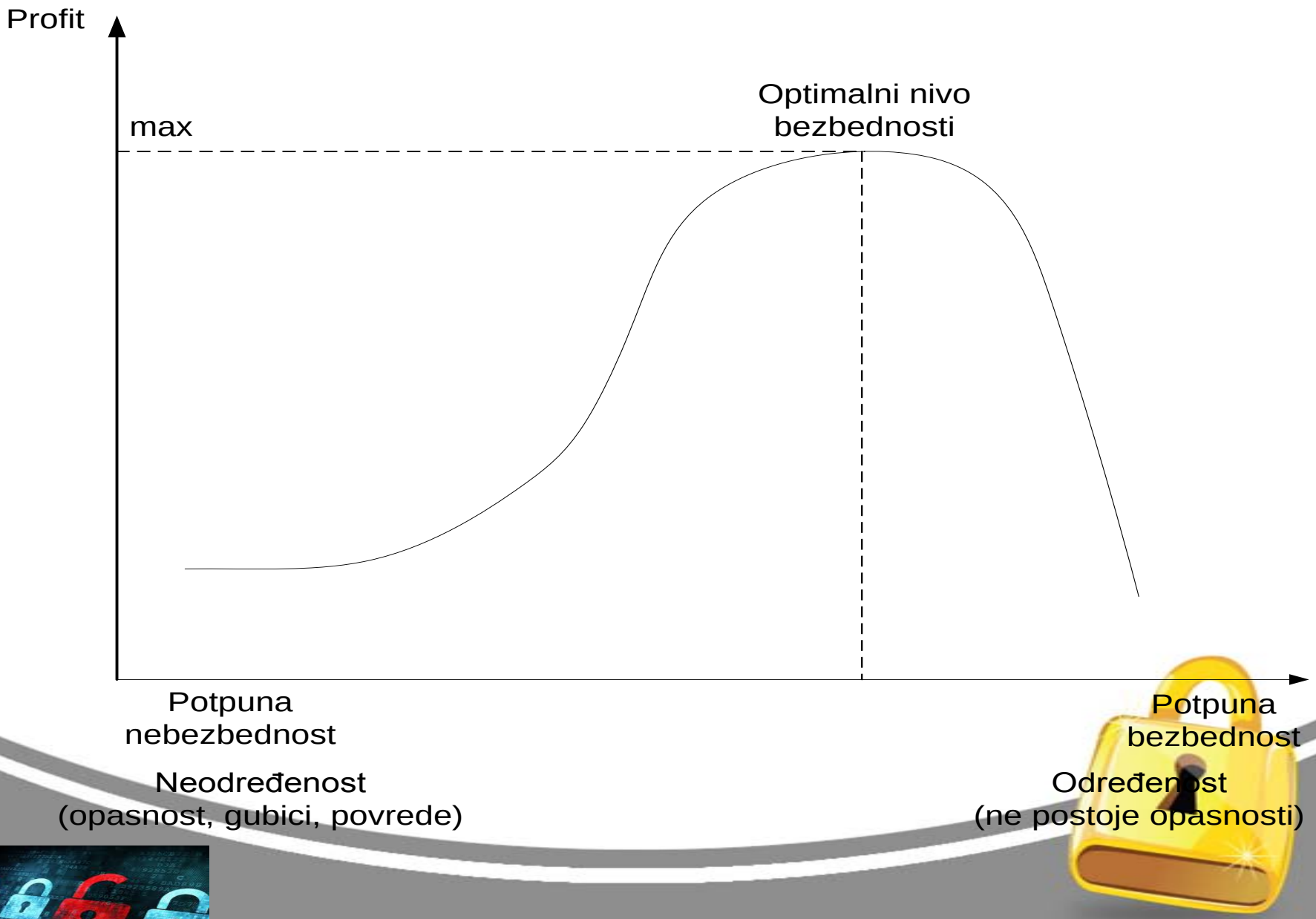
- ***U** (upravljačko–administrativne)* - npr. primenjen standard
- ***O** (organizaciono-operativne)* - npr. barijere za fizički pristup
- ***T** (tehničke)* - npr. alarm IDS, antivirusni program - AVP

Optimalni sistem zaštite

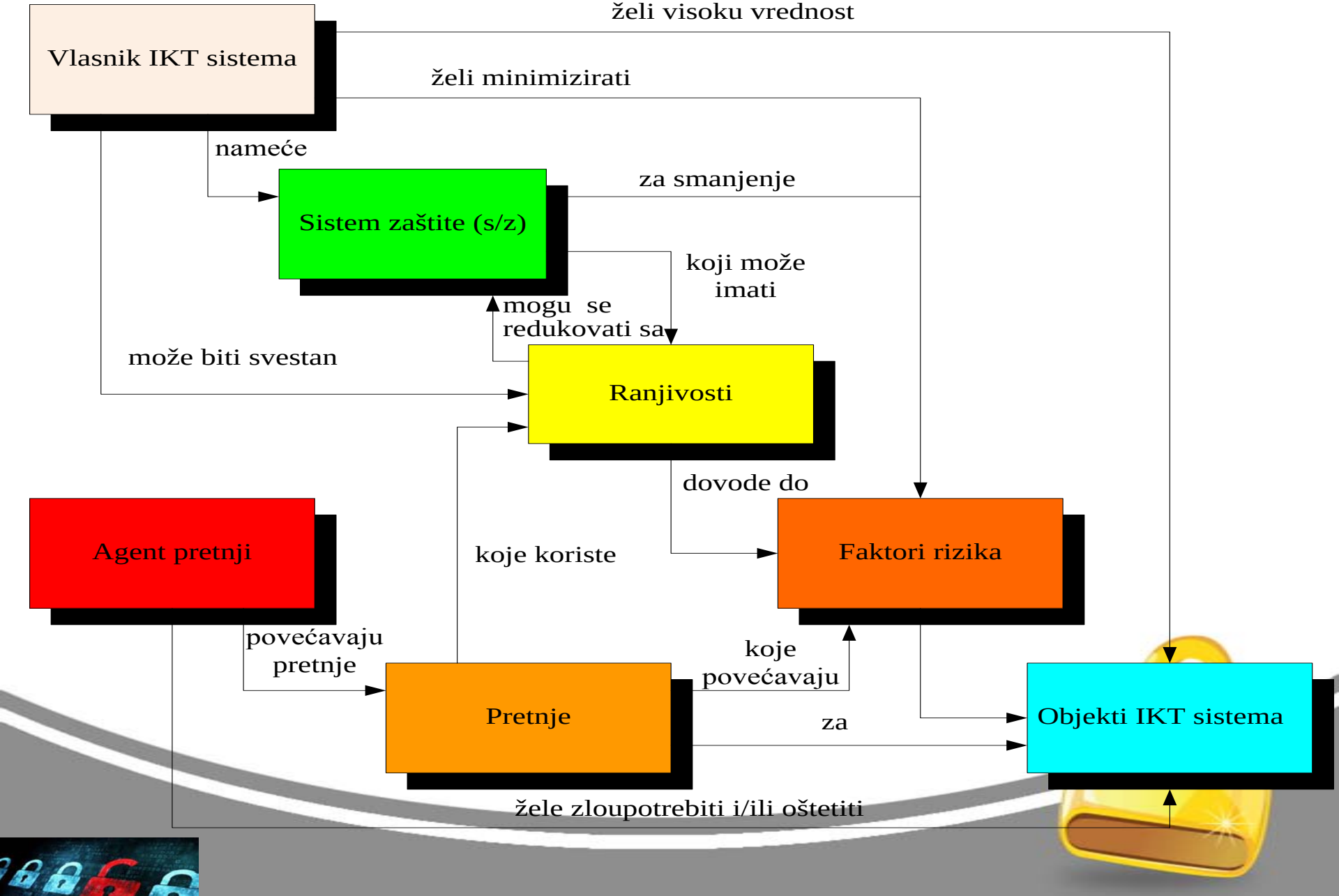
- **Resursi sistema zaštite značajno poskupljuju PIS**
- **Cilj procesa upravljanja zaštitom (ISMS*):**
  - uspostaviti i dostići bezbednosne ciljeve
  - projektovati, implementirati i održavati *optimalan SZ*
- **Optimalno rešenje zaštite (**generički koncept**)**:
  - *rentabilan i funkcionalno efektivan skup kontrola zaštite:*
    - *dobijen najracionalnijom raspodelom resursa,*
    - *koji u datim uslovima na najbolji način zadovoljava sve zahteve zaštite*

ISMS*- *Information Security Management System*

Optimalan sistem zaštite



GENERIČKI MODEL SISTEMA ZAŠTITE



Generički model sistema zaštite (SZ)

1. **SZ štiti informacionu imovinu (ISO/IEC 27001)** od:
   - **Pretnji***: potencijalni, slučajni i namerni agenti-faktori rizika koji mogu izazvati štetu*

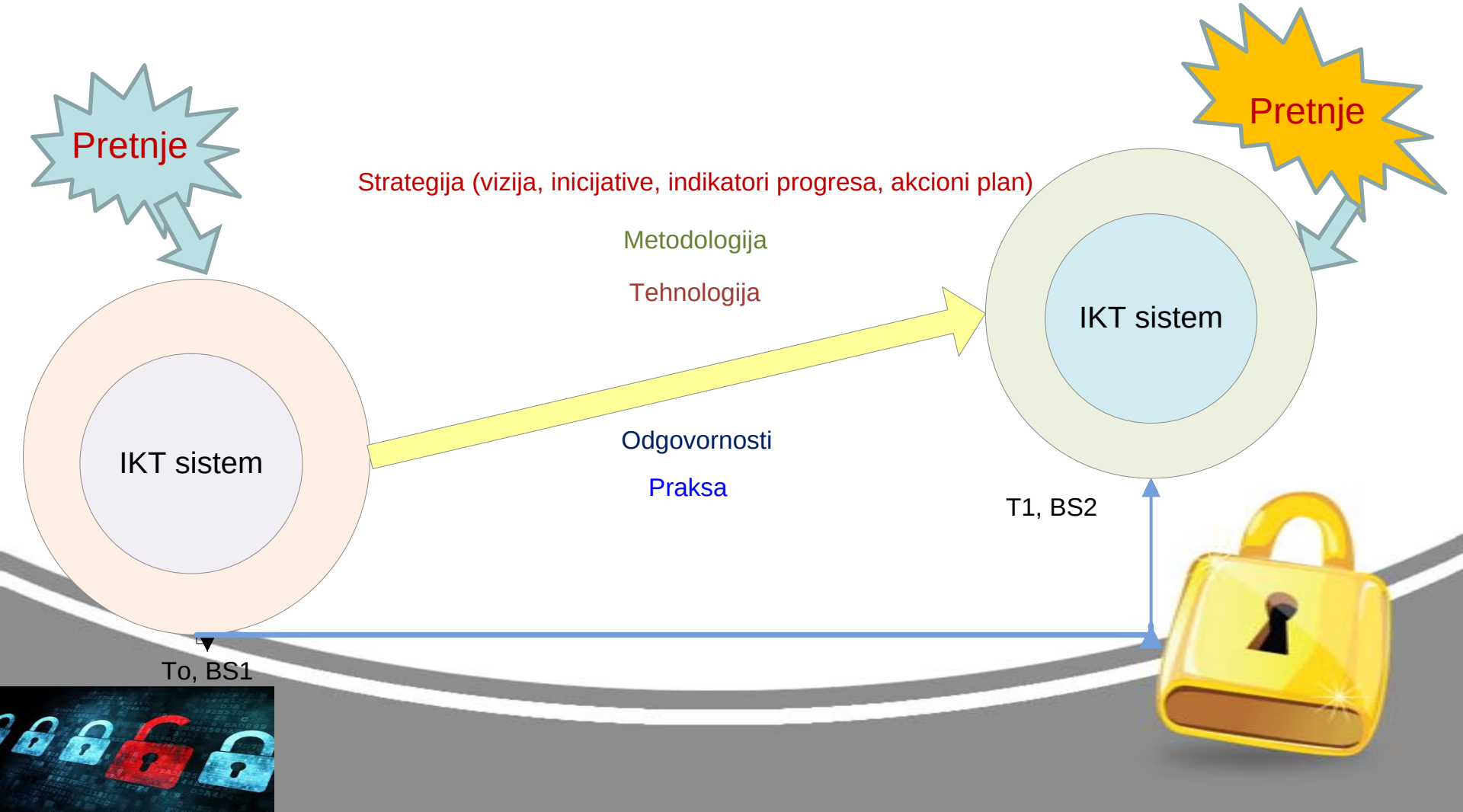
     Primer*: maliciozni kodovi, greške hw-sw, ljudske aktivnosti*

   - **Napada:** *realizovana pretnja = bezbednosni incident*

2. **Vlasnici instaliraju kontrole zaštite** (**U, O, T**) da:
   - implementiraju zahteve *politika zaštite*,
   - minimiziraju rizik svim sredstvima
   - redukuju uticaj pretnji na ranjivosti inormacione imovine
   - štite inf. imovinu na nivou preostalog prihvatljivog R (**Rpp**)
   - smanjuju Rpp u neprekidnom (cikličnom) procesu

Promena stanja bezbednosti

Proces promene stanja bezbednosti informacija



Primer: *OCTAVE* metodi implementacije programa/SZ

Proces 4-fazne tranzicije bezbednosnog stanja IS:
metod implementacije zaštite *najkritičnijih* objekata IS
Faze implementacije programa/sistema zaštite

Faza	Kritični objekti za misiju	Kritični objekti	Primarni objekti	Opšti objekti
1.	20 glavnih faktora rizika (FR.)	0	0	0
2.	50 glavnih faktora rizika	20 glavnih FR	0	0
3.	100 glavnih faktora rizika	50 glavnih FR	20 glavnih FR	0
4.	200 glavnih faktora rizika	100 glavnih FR	50 glavnih FR	20 glavnih FR

Primer: *OCTAVE* metodi implementacije programa/SZ

- **PROCES IMPLEMENTACIJE SZ:**
  1. ***Izbor tima*** za koordinaciju i monitorisanje
  2. ***Identifikovanje bezbednosnih faktora rizika***
  3. ***Obavezna provera (revizija) projekta zaštite***
  4. ***Integracija i prilagođavanje programa***
  5. ***Obavezne komponente sadržaja procesa***:
     1. *obuka zaposlenih*
     2. *provera usaglašenosti*
     3. *nametanje obaveze izvršavanja* politika i procedura zaštite (disciplinske mere/sankcije)

Primer: *OCTAVE* metodi implementacije programa/SZ

1. Obuka zaposlenih

- ***Svi zaposleni*** - izgraditi svest o potrebi zaštite
- ***Tehničko osoblje*** - korišćenje i održavanje opreme i tehnologija zaštite
- ***Sistem administratori i članovi CIRT*** - specijalizovanu obuku za administraciju s/z
- ***Menadžerska struktura*** - razvija svest o potrebi zaštite, razume ulogu i odgovornost
- ***Operativno osoblje*** - dodatnu obuku (po planu zaštite)

Primer: *OCTAVE* metodi implementacije programa/SZ

2. Kontrola usaglašenosti - integracija S/Z:

- Stepen integracije implementiranog programa/SZ meri se stepenom ***opšte i specifične*** usaglašenosti:

1*. Kontrola opšte* usaglašenosti:– vrši upravna struktura:

- korišćenja IS i primeni *normativa* i standarda zaštite
- **alat: menadžerska, interna i nezavisna provera**

2. *Kontrola specifične* usaglašenosti:

- *prakse zaštite sa politikom*
- *podrške poslovnim procesima*
- *operativnog korišćenja tehnologija zaštite*
- **alat: menadžerska i interna provera**

Primer: *OCTAVE* metodi implementacije programa/SZ

3. Nametanje obaveze izvršavanja i izveštavanja:

- sledi obuku, nadzor i proveru usaglašenosti prakse i politike zaštite

- **Izveštaj o nadzoru, kontroli, proveri**:
  - ulazna informacija za reinženjering politike i SZ
- **Kritičan faktor:**
  - implementacija politike/procedura zaštite bez represivnih mehanizama za obavezu izvršavanja
- **Sankcije za nesprovođenje** politike zaštite:
  - dobro ih planirati i unapred osmisliti - od **upozorenja** do **otpuštanja sa posla**, ili **sudskog gonjenja**

Primer: *OCTAVE* metodi implementacije programa/SZ

- ***ISACA*** (*Information System Audit and Control Association*) predlaže da izveštaj proveravača:
  - **pokaže** koji sistem mera je koristio *auditor*
  - **pomogne** u planiranju, radu i kontroli rada *auditor*-a
  - **olakša** nezavisnu proveru rada *auditor*-a
  - **evaluira** sistem kvaliteta **programa provere**
  - **obezbedi** podršku za naplatu polise osiguranja
  - **pomogne** profesionalni razvoj specijalista zaštite itd.

Nova paradigma zaštite informacija

- **Osnovni principi reaktivnog sistema zaštite informacija**:
  - *odbrana po dubini*, implementacija nezavisnih mehanizama z.
  - *primarna zaštita najvrednije informacione imovine* – CIA informacija
  - *prstenovi zaštite* tipa ***slojeva luka*** *ili* ***slojeva OSI*** *modela RM*
  - zaštita *sadržaja informacija u kontejneru*

- **Ograničenja reaktivne zaštite:**
  - virtuelizacija u savremenom *Cloud Computing* **sistemu**
  - *informacije su znatno dinamičnije i fluidnije*
  - *zaštita sadržaja u kontejneru nije dovoljna*
  - *nemogućnost zaštite od naprednog, ciljanog i zero day napada*

- **Porast zloupotreba i kompjuterskog (sajber) kriminala**:
  - prevare, krađa identiteta, iznuđivanje novca, terorizam, inf. rat...

Klasičan koncept slojevite zaštite

- *Osnovni SMF* (zakon, standardi, politika, ljudi, procesi)
- *Fizička zaštita* informacione imovine
- Zaštita perimetra RM (DMZ)
- Zaštita RM po dubini
- Zaštita host RS - **NOSSS***
- *Zaštita na aplikativnom sloju*

Zaštita podataka uskladištenih u RS-u

NOSSS* **-** *Native OS Security Subsystem*

Nova paradigma zaštite informacija

- **Gube se fizičke granice organizacije** (e-poslovanje, CC...)
- **Ozbiljne interne pretnje (**krize, nezadovoljni korisnici**...)**
- Organizacije sve više **diverzifikuju lanac vrednosti**
- Učestvuju različite org., koje imaju jednako značajne uloge
- Neki slojevi zaštite biće efektivni - samo ako se i**mplementiraju** svima **u distribuiranom lancu vrednosti**.
- **Virtuelizacija serverske i klijentske strane**:
  - menja zaštitu ***slojeva luka*** na ***prstenove slojeva luka*** ili
  - **distribuiranu slojevitu zaštitu po dubini**
- **CC sistemi zahtevaju promenu klasične paradigme zaštite**:

Cloud Computing servisi

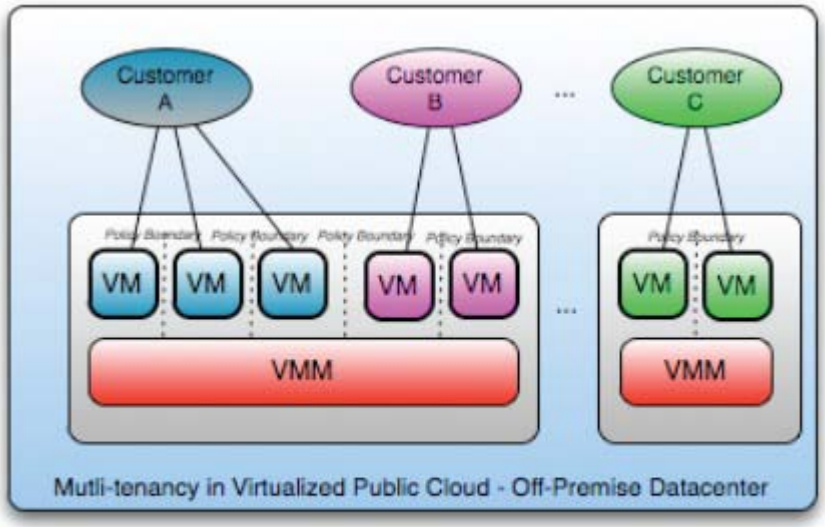
- **Modeli CC servisa:**
  - *Infrastruktura kao servis* (**IaaS**)
  - *Platforma kao servis* (**PaaS**)
  - *Softver kao servis* (**SaaS**)
- **Ključne karakteristike**:
  - *agilnost*, *manji troškovi, nezavisnost od tipa uređaja/lokacije*
  - *istovremeno deljenje i iznajmljivanje servisa* za nadoknadu
  - *pouzdanost* (redundantnost) i *skalabilnost resursa*,
  - *održivost i **bezbednost?***
- **Problem:**
  - *novi tipovi ranjivosti*
  - *zaštita informacija 1000-e korisnika*
  - *DF istraga u slučaju napada*

Primer: Vizuelni model definicije *CC* (NIST)

Primer: višestruko rentiranje servisa

-Multy-tenancy-

(**NIST**)



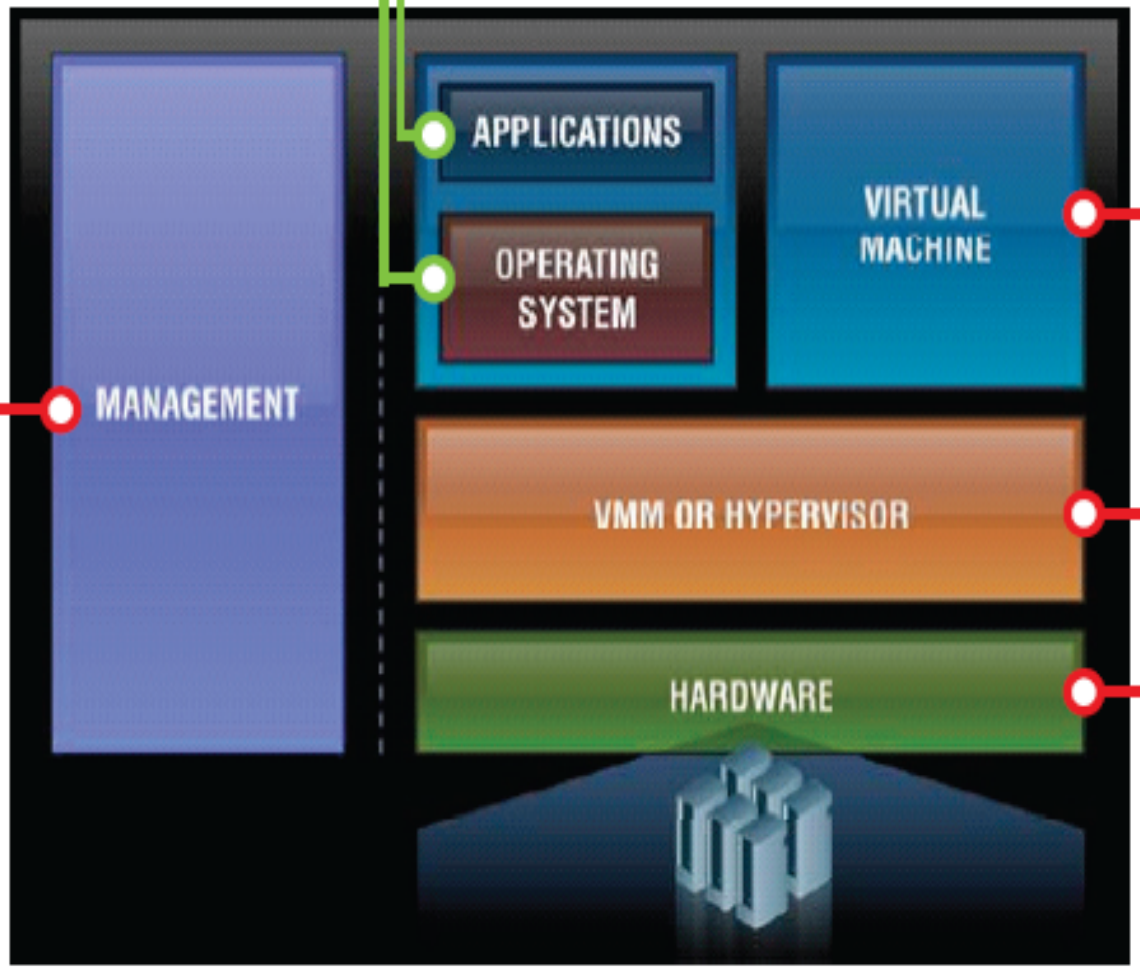
Public Cloud Provider with 3 business customers, each with different security, SLA, governance and billing policies on shared infrastructure

Nove ranjivosti u CC okruženju (IBM)

Traditional Threats

New threats to vm environments

Traditional threats can attack VMs just like real systems



Management Vulnerabilities

Secure storage of VMs and the management DATA

Requires new skill sets

Virtual sprawl

Dynamic relocation

VM stealing

Resource sharing

Single point of failure

Stealth rootkits in hardware now possible

Virtual NICs & Virtual Hardware are targets

MORE COMPONENTS = MORE EXPOSURE

Koncept zaštite informacija u CC

- **Životni cikllus S/Z počinje *zaštitom CC centra***
- ***CC centar* ne pokriva većinu slučajeva u kojima se nalaze informacije korisnika**
- **U CC okruženju relevantne su dve varijable zaštite**:

1. *Koncept klasične zaštite kontejnerskog tipa:*
2. **Uloga ljudskog faktora TTP* (CSP) - sa aspekta klijentaa**:
   - alati zaštite nisu *laki za korišćenje i pristupačni*

- **Zaštita *CC centra* vrši se**:
  - klasičnom tehnologijom zaštite
  - primenom koncepta *distribuirane slojevite zaštite*

TTP*-*Trusted Third Party (*poverljivi provajder*...)*

CSP *(Cloud Service Provider) u CC sistemu*

Nova paradigma zaštite informacija

- **U CC i e-okruženju, organizacije moraju:**

1. Dopuniti generičku metodologiju za upravljanje rizikom sa:

- *mikoranalizom rizika,* umesto scenarija rizika na *makro* planu
- obaveznim uključivanjem upravljanja rizikom u poslovno odlučivanje
- uključivanjem realnih pretnji, ranjivosti i uticaja na poslovne procese

2. Intenzivirati razvoj novih alata:

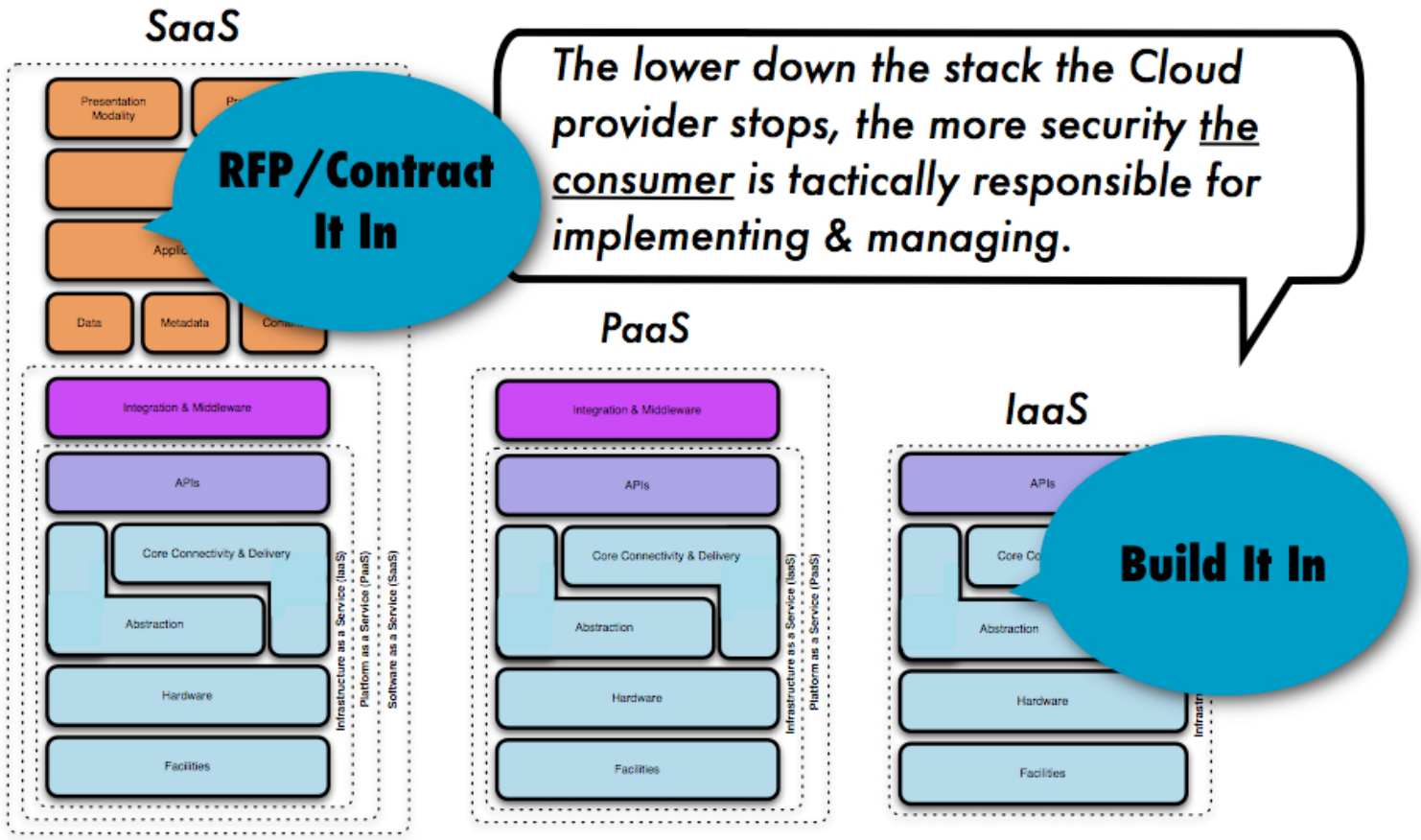
- servisi zaštite na heterogenim platformama u virtuelnom okruženju
- šire dostupne *kriptografske tehnike i tehnologije višeslojne zaštite RM*
- *distribuirane barijere*, *IDPS* skeneri, *web* filteri
- centralno upravljanje zaštitom preko zaštićenih veza
- *proaktivni sistemi zaštite* od poznatih i nepoznatih pretnji
- *prediktivni sistem zaštite* (inteligentni agenti)
- *proaktivna DF* i *integracija servisa DF istrage* u sistem CC zaštite...

Nova paradigma zaštite informacija

3. Obezbediti određeni nivo digitalne forenzičke istrage

- **Veći broj digitalnih uređaja na Internetu zahteva**:
  - praćenje bezbednosno relevantnih događaja u realnom vremenu
  - centralizovano skupljanje *log* podataka u ***log server***
  - automatizovanu analizu log datoteka
- **Ključ za proaktivnu detekciju incidenta (proaktivnu DF)**:
  - *alati zaštite ugrađeni (ne implementirani) u hw/sw proizvode*
  - *jak monitoring sistem*
  - *poznavanje realnih pretnji koje pogađaju kritične procese*
  - *aktivna, selektivna analiza bezbednosnih događaja u log serveru*
  - *konvergencija i integracija **forenzičkih i alata zaštite***

Primer: Kako integrisati sistem zaštite u CC modele (NIST)?



Glavni principi zaštite u CC

Princip	Opis
1.	Mehanizme zaštite ugraditi, a ne samo integrisati u infrastrukturu IS
2.	Razviti različita rešenja, proizvoda i servisa zaštite
3.	Kreirati beskontaktni i transparentni sistem zaštite
4.	Obezbediti centralizovano upravljanje i k/z proporcionalne sadržaju
5.	Zaštititi tok informacije u infrastrukturi DR od napada spolja i iznutra
6.	Dinamičku zaštitu zasnivati na proceni rizika za infrastrukturu i informacije
	Uspostaviti samoobučavajući sistem zaštite za praćenje dinamike DR i MP

Primer: mehanizmi zaštite CC

1. **Distribuirana veb aplikaciona barijera (DWAF):**
   - dinamički skenira CPU, računare, servere i mrežne uređaje
   - usmerena je na detekciju/sprečavanje napada
   - treba da bude:
     - *virtuelna, softverska aplikacija*, *plug-in*, *SaaS,* ili *integrisana* u postojeći hardver
     - laka za administraciju svoje aplikacije
     - konfigurisana zaštićenom aplikacijom, sa mnogo većom granulacijom i sa čarobnjakom
     - sa više administratorskih privilegija za efektivno upravljanje
     - set mehanizama za zaštitu kernela distribuiranih sistema VM

Primer: mehanizmi zaštite CC

2. DWAF treba da sadrži IDPS koji:

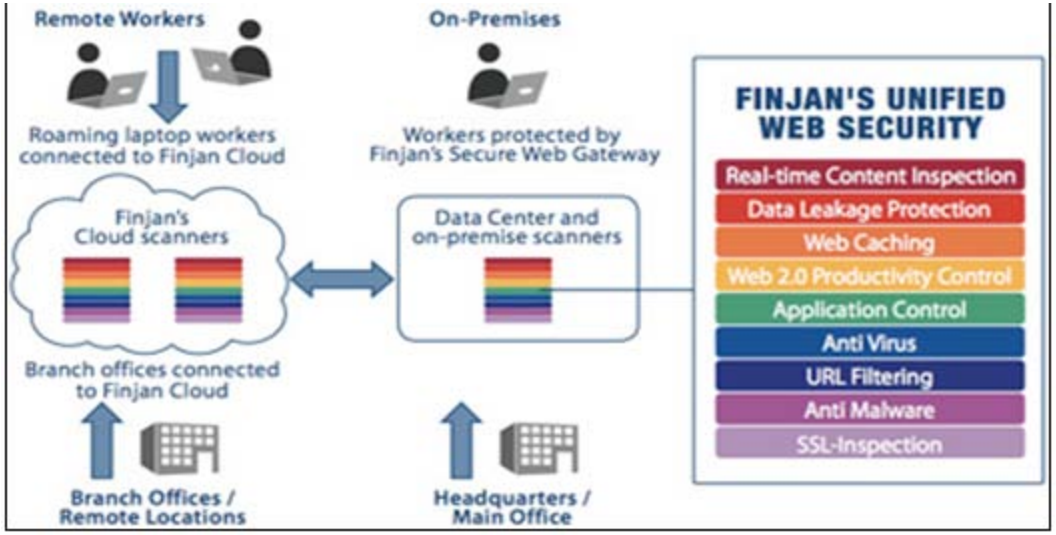
- *nemaju lažne pozitive* u realnom **DWAF** sistemu
- omogućavaju skriveni monitoring i detekciju
- omogućavaju transparentnost pravila za konfigurisanje
- koriste *skener veb ranjivosti*, inteligentne *algoritme* ili
- *statički analizator izvornog kôda* za sugerisanje seta pravila

3. DWAF treba da obezbedi *proaktivnu virtuelnu zaštitu:*

- da imaju **mehanizme za upravljanje zaštićenom sesijom, šifrovanje URL i autentifikaciju**
- da **obezbede virtuelizaciju forme i polja na nivou DWAF, a ne samo na nivou aplikacije**

Primer: mehanizmi zaštite CC

3. Finjan *Vital Cloud* i *Vital Cloud Hybrid*



Primer: mehanizmi zaštite CC

4. Model *Inteligentne kolonije digitalnih mrava (DM*)

- **Problem klasičnih AVP sistema zaštite**:
  - *reaktivni* SZ neprekidno štite RS/RM od *poznatih* pretnji
  - brojni MP modifikuju svoj kôd u prva 24 časa
  - AVP često ne mogu detektovati i ukloniti MP
  - troše resurse RS za dugotrajno skeniranje, računari rade sporije
- **Rešenje:**
  - razvoj bržeg metoda skeniranja na bazi *paralelnog procesiranja*
  - računarske podatke deli u *batche* fajlove koji se procesiraju paral.
  - slično, proces skeniranja AVP deli se prema specifičnim pretnjama

Primer: mehanizmi zaštite CC

4. Model *Inteligentne kolonije digitalnih mrava (DM*):

- Obećava potpunu transformaciju postojeće zaštite **kiber-prostora**
- Simulira inteligenciju kolonije mrava
- *Inteligentni agenti za zaštitu* („DM“):
  - lutaju kroz RM i traže agente pretnji – MP (viruse, crve, trojance...)
  - kada *DM* otkrije pretnju, brzo privuče druge DM
  - na određenoj koncentraciji privlače pažnju administratora zaštite da pokrene istragu KI
  - zatim se brzo vrate redovnim zadacima

Primer: mehanizmi zaštite CC

- **Principi rada modela *Inteligentne kolonije DM:***
  - svaki tip DM traga za različitim dokazom napada
  - dok se kreću kroz RM *digitalni mravi* ostavljaju *digitalne tragove*
  - za svaki dokaz napada DM ostavlja jači digitalni trag
  - tragaovi privlače druge DM do mesta napada
  - kolonija digitalnih mrava označava potencijalnu infekciju računara i
  - zahteva intervenciju administratora zaštite

Primer: mehanizmi zaštite CC

- **Prototip modela *Inteligentne kolonije DM:***
  - Ispitan u (SAD*) na RM od 64 računara
  - U RM ubačen crv i digitalni mravi su ga uspešno otkrili
  - Cilj - implementirati u RM 3.000 različitih tipova DM
  - Model najviše odgovara za velike RM koje dele resurse i imaju veliki broj identičnih mašina
  - Kolonija digitalnih mrava ne može greškom ostati u RS
  - Administrator sistema monitoriše i upravlja *kolonijom DM* preko aplikacije („*čuvara kolonije*“) instalirane na svakoj mašini

* ***Errin Fulp***, Profesor kompjuterskih nauka, ***Wake Forest* Univerziteta**; **Glenn Fink**, istraživač *Pacific Northwest National Laboratory* (PNNL), *Richland, Washinton*, SAD; *Wes Featherstun* i ***Brian Williams***, diplomirani studenti *Wake Forest* Univerziteta, 2009

Primer: mehanizmi zaštite CC
-IBM rešenja-

- *IBM Proventia® Server Intrusion Prevention System (IPS)*
- *IBM Proventia® Network Intrusion Prevention Systems (IPS)*
- *IBM Proventia® Network Mail Security System*
- *IBM Proventia® Network Multi-Function Security (MFS)*
- *Data Loss Prevention*
- *IBM Proventia® Virtualized Network Security Platform (VNSP)*
- *IBM Proventia® Network Mail Security System*

Pitanja