BEZBJEDNOST INFORMACIONIH SISTEMA

OSNOVI ZAŠTITE INFORMACIJA

1. BEZBJEDNOST I ZAŠTITA INFORMACIONIH SISTEMA

- Semantičko značenje “*bezbjednosti*”, “*sigurnosti*” i “*zaštite*”
- Funkcionalnu zavisnost *bezbjednosti* i *zaštite*
- Ključne faktore bezbjednosnog stanja IKT sistema
- Definicija sistema zaštite
- PIS (IKTS, IS, IT) kao objekat zaštite
- Opšti funkcionalni model sistema zaštite
- Optimalni sistem zaštite
- Nova paradigma zaštite

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

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

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

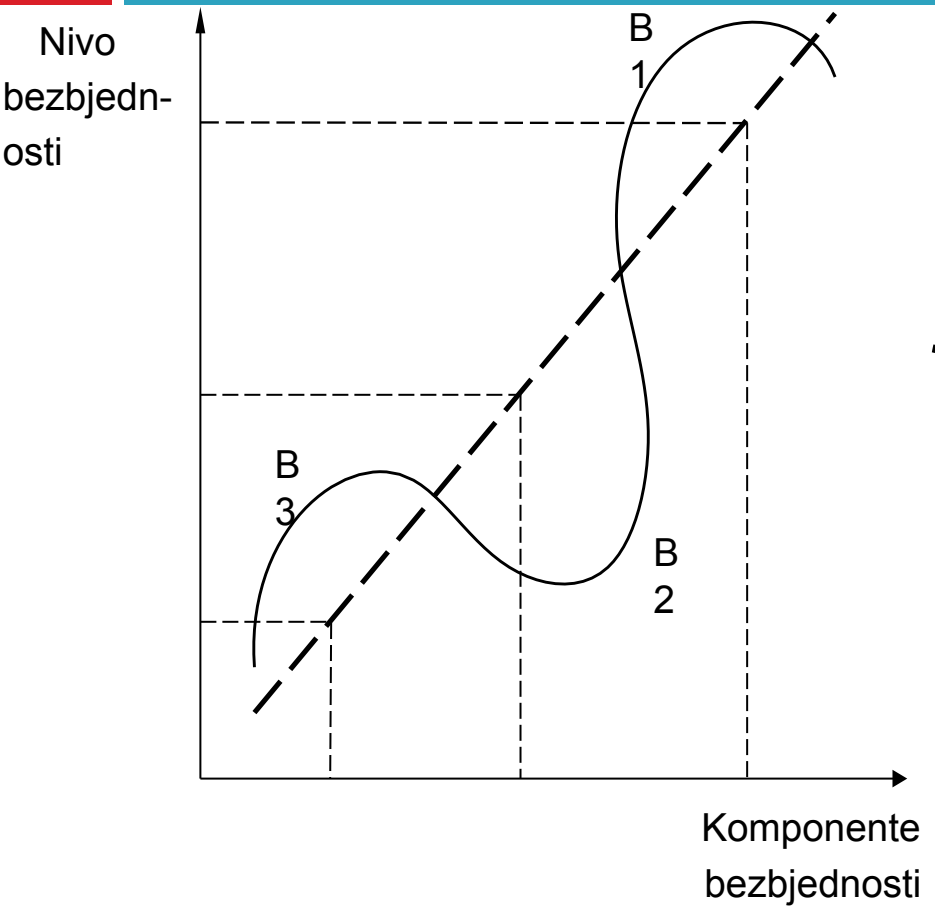
Informaciona imovina (ISO/IEC 27k)
-*čista, fizička, humana*-

- **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 bezbjednosnog stanja informacija (*revizija*)
   Izlaz = **ocjena nivoa bezbjednosti (n/b)**
2. Procjena rizika (*analiza imovine, prijetnji, ranjivosti, rizika*)
   Izlaz = **odobren prihvatljivi nivo rizika (SoA)**
3. Projektovanje, implem. i integracija sistema zaštite
   - ***upravljačkih, org. i tehničkih*** **kontrola (mjera) 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**

Bezbjednost informacija
-funkcija komponenti bezbjednosti-



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

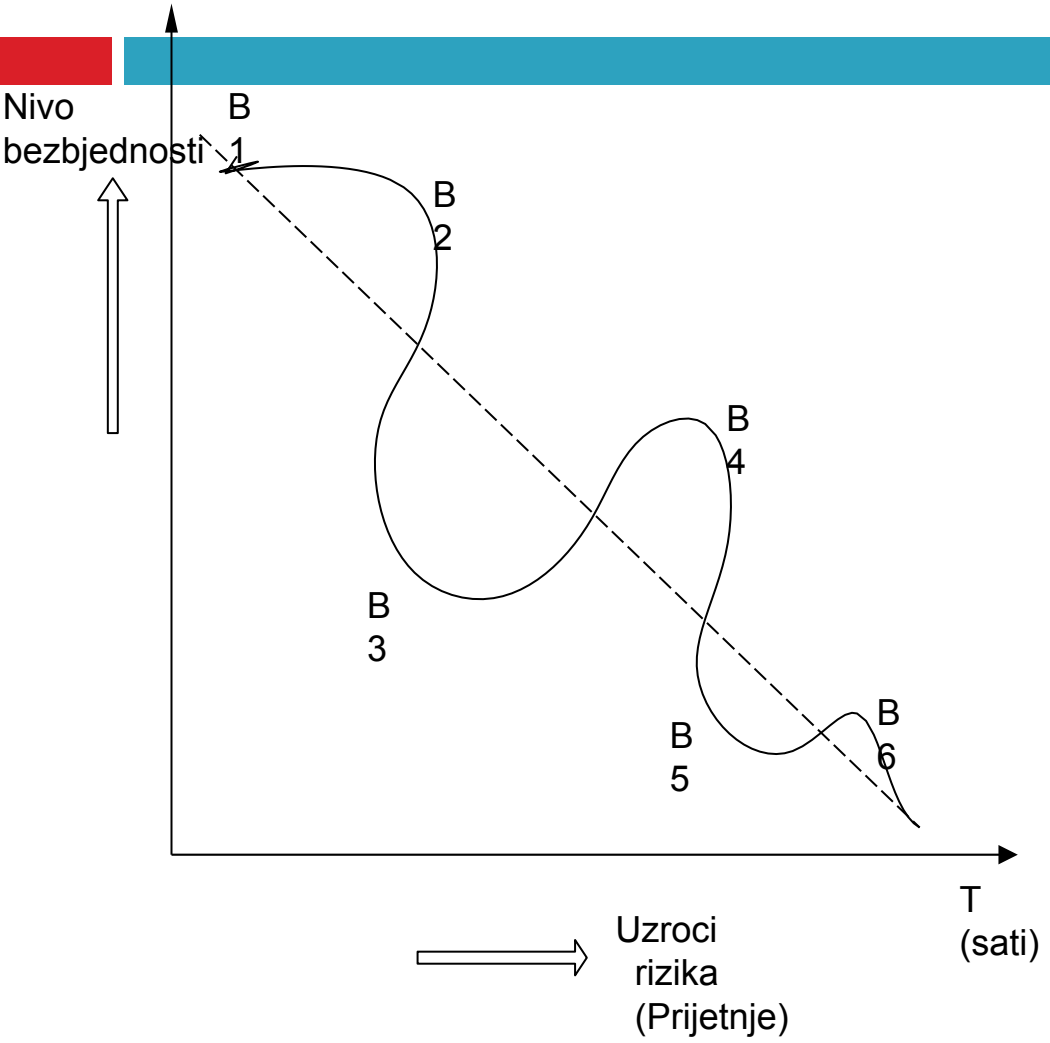
j= 1....n – komponente bezbjednosti

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

Posljedica: zahtjev za sveobuhvatni pristup zaštiti!

Bezbjednost IS

-funkcija faktora rizika-



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

j= 1....n – komponente bezbjednosti

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

Ri = procijenjeni, stohastički faktori rizika komponenti bezbjednosti; **i= 1... n.**

Posljedica: redovna procjena rizika

Faktori bezbjednosti savremenih IKTS

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

1. Uticaj funkcionalnih zahtjeva IKTS (PIS)

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

6. **Bezbjednost/zaštita informacija:**
   - zahtijeva menadžment rizika, planiranje i održavanje zaštite, kompatibilne sa dinamikom razvoja e-poslovanja, IKT...

7. **Rješenje:**
   - Sistem zaštite mora da prati razvoj PIS (tehnološki, organ.)

BI* - *Poslovna inteligencija*

****CIA** (*Confidentiality, Integrity and Availability*) – **povjerljivost, integritet, raspoloživost**

2. Uticaj organizacione strukture

1. **Problem**:
   – česte promjene organizacione strukture utiču na:
     • obezbjeđivanje kompetentnog specijaliste zaštite
     • obezbjeđivanje izvršnih menadžera za podršku
2. **Rješenje**:
   – *kombinovana primjena upravljačkih i operativno-organizacionih kontrola zaštite*

3. Uticaj razvoja tehnologije

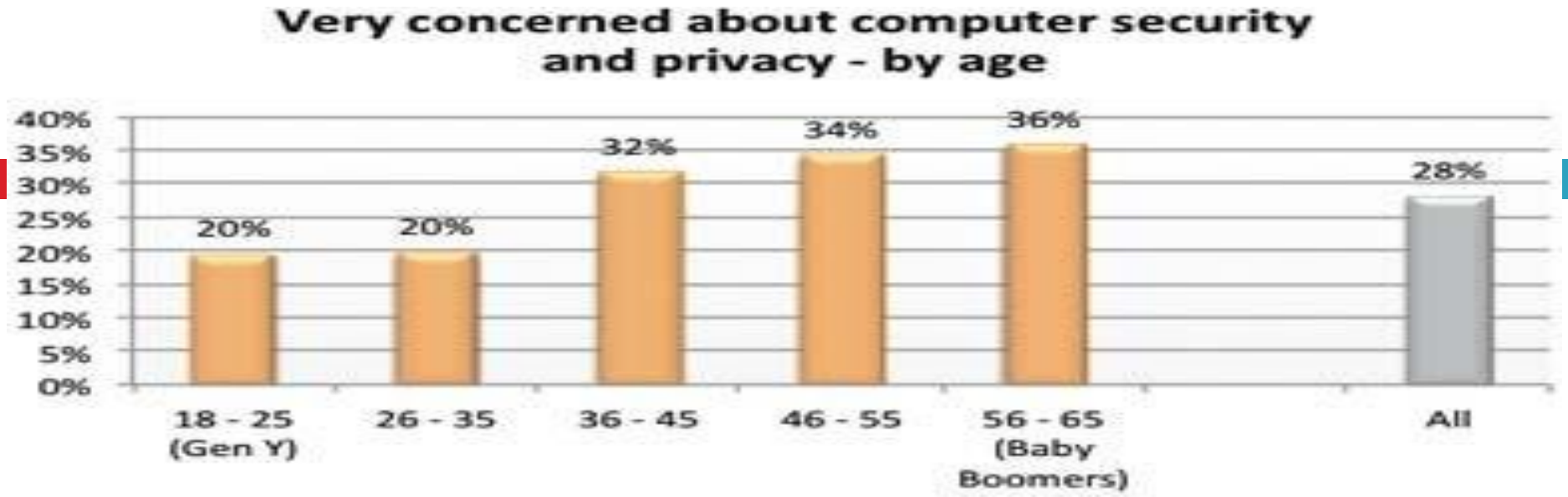
1. **Trend razvoja IKT**:
   - *integracija upravljanja sistema i procesa*
   - *automatizacija* poslovanja (PIS, e-Uprave...)
   - *razvoj novih oblika računarstva* (BI, *Cloud Computing*...)
2. **Trend razvoja tehnologija zaštite** - sledi ž/c IKT:
   - *brz razvoj IKT* - utiče i na razvoj tehnologija zaštite
   - zaštita se implementira pri kraju ž/c IS (*Firewalls, AVP*,...)
   - sve poslove zaštite *nemoguće automatizovati*
     - ***uloga čovjeka u zaštiti*** *- nezamjenljiv i kritičan faktor*
   - *sofisticirani napadi su ispred tehnologija zaštite*
3. **Rješenje:**
   - *Brzi razvoj IKT zahtjeva brzi razvoj tehnologija zaštite*

4. Uticaj politike zaštite

1. **Procesi zaštite** - nisu dovoljno razvijeni:
   - odluke na bazi predefinisanih *politika zaštite*, ne procjene **R**
   - upravljanje zaštitom na bazi **statičke** *politike zaštite*
   - pristup dobar za strategijske odluke, ne i taktička rješenja
2. **Dinamički promjenljive prijetnje**, zahtijevaju:
   - rješenja zaštite na bazi *procjene 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 zahtjeve i *oper*. *rizik*
3. **Rješenje:**
   - *Politiku zaštite ažurirati u skladu sa redovnom procjenom rizika*

5. Uticaj obuke i razvoja svijesti o potrebi zaštite

1. **Problemi**:
   - složenost IKTS i tehnologija zaštite zahtijeva aktuelna znanja
   - nedovoljna svijest o potrebi zaštite, znanja i vještine:
     - *menadžera* o potrebi upravljanja rizikom i sistemom zaštite
     - *korisnika* o potrebi kontrole zaštite i ublažavanja uticaja rizika
2. **Rješenje**:
   - *uvođenje regularnih programa obuke i razvoja svijesti*
   - *uvođenje procesa za upravljanje operativnim rizikom*
   - *obezbijediti praćenje i razumijevanje realnog rizika*
   - *manje forsiranje primjene tehničkih rješenja zaštite*



- Prioritet zaštite informacija/računara sa godinama starosti
- Korisnici starosti 18 – 25 su preterano samouvjereni u svoje znanje o zaštiti
- Korisnici starosti 18 – 25 imaju manje sofisticiranu zaštitu zbog finansijskih i tehničkih prepreka
- Iako su osjetljivi 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**

   zahtijevaju**:**
   - *skalabilnost* (nadogradivost) tehnologija zaštite
   - *primjenu* u savremenim Internet tehnologijama (**BI, CC**)
   - *jaku autentifikaciju* u e-poslovanju
   - *standard povjerenja* na Internetu **(PKI?!)**
   - *borbu protiv kompjuterskog kriminala...*
3. **Rješenje:**
   - *Taktiku primjene tehnologija zaštite usklađivati sa zahtjevima prakse*

Savremeni PIS – objekat zaštite

1. **Osnovne tehnološke 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 zahtjev sistema zaštite (S/Z) u svim fazama ž/c:**

- *računarski sistem (RS)* - osnovna tehnička komponenta **S/Z**
- *smanjenje kompleksnosti PIS/SZ* primjenom:
  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*:
     - **namjena** - funkcionalne ka-ke i kvalitet informacija
     - **zaštita objekata PIS** - *procesa, procedura, programa,...*
     - **zaštitu informacija** - *CIA*

Primjer*:* 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 nasljeđivanje*

- ***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 *mjere*)
  - *tehničke kontrole* (hardversko-softverski alati)

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

Osnovni zahtjevi za sistem zaštite

1. **Sprječavanje, detekcija, oporavak *informacione imovine* od:**
   - ugrožavanja bezbjednosti lica, organizacija i države
   - krađe, pronevjere, gubitaka, izmjene
   - neovlašćenih aktivnosti u RS i RM, razne zloupotrebe
   - povreda intelektualne imovine, privatnosti i povjerljivosti

2. **Obezbjeđivanje informacione imovine (PS* u cjelini) kroz:**
   - efektivnu i efikasnu zaštitu
   - kvalitetno upravljanje zaštitom

PS* - Poslovni Sistem

Definicija sistema zaštite

– *Organizovan i koherentan skup **ljudi** i **mjera** (**U, O i T** kontrola) i njihovih veza i ograničenja, primijenjenih na informacionu imovinu, da bi se zaštitila **CIA,** a time održao/povećao:*

- *željeni nivo bezbjednosti informacione imovine (PS),*
- *obezbijedilo namijenjeno 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 bezbjednosnih 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*

   Primjer: *kriptografski* mehanizmi za digitalni potpis.

Sistem zaštite

3. ***Kontrole zaštite***:
   - koriste se za upravljanje mehanizama zaštite
   - konačna klasifikacija mehanizama zaštite
   - bezbjednosna funkcija arhitekture sistema zaštite
   - interfejs između mehanizma zaštite i čovjeka
   - implicira suštinsku potrebu neprekidne *kontrole* sistema zaštite

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

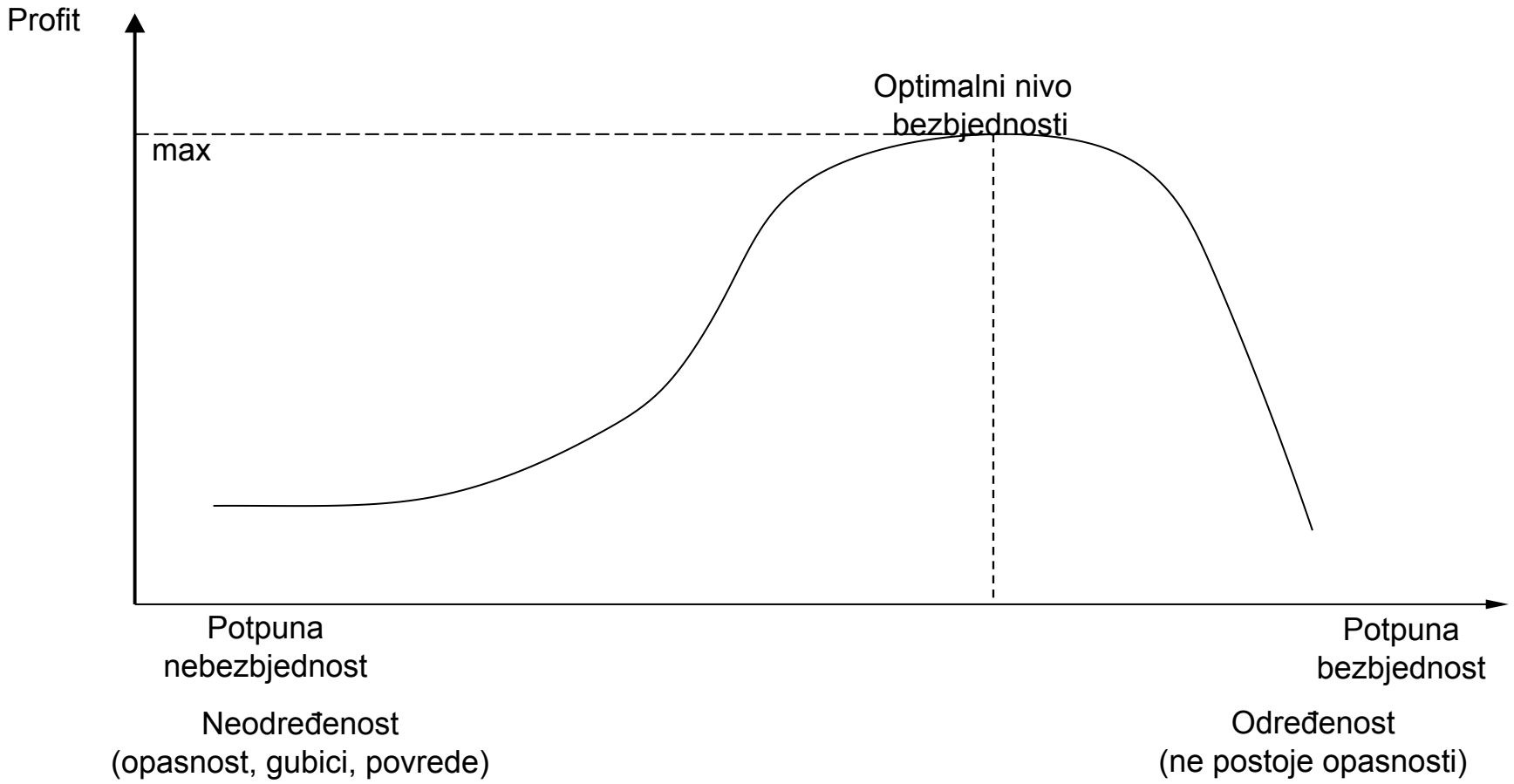
- ***U** (upravljačko–administrativne)* - npr. primijenjen standard
- ***O** (organizaciono-operativne)* - npr. barijere za fizički pristup
- ***T** (tehničke)* - npr. alarm IDS, antivirusni program - AVP

Optimalni sistem zaštite

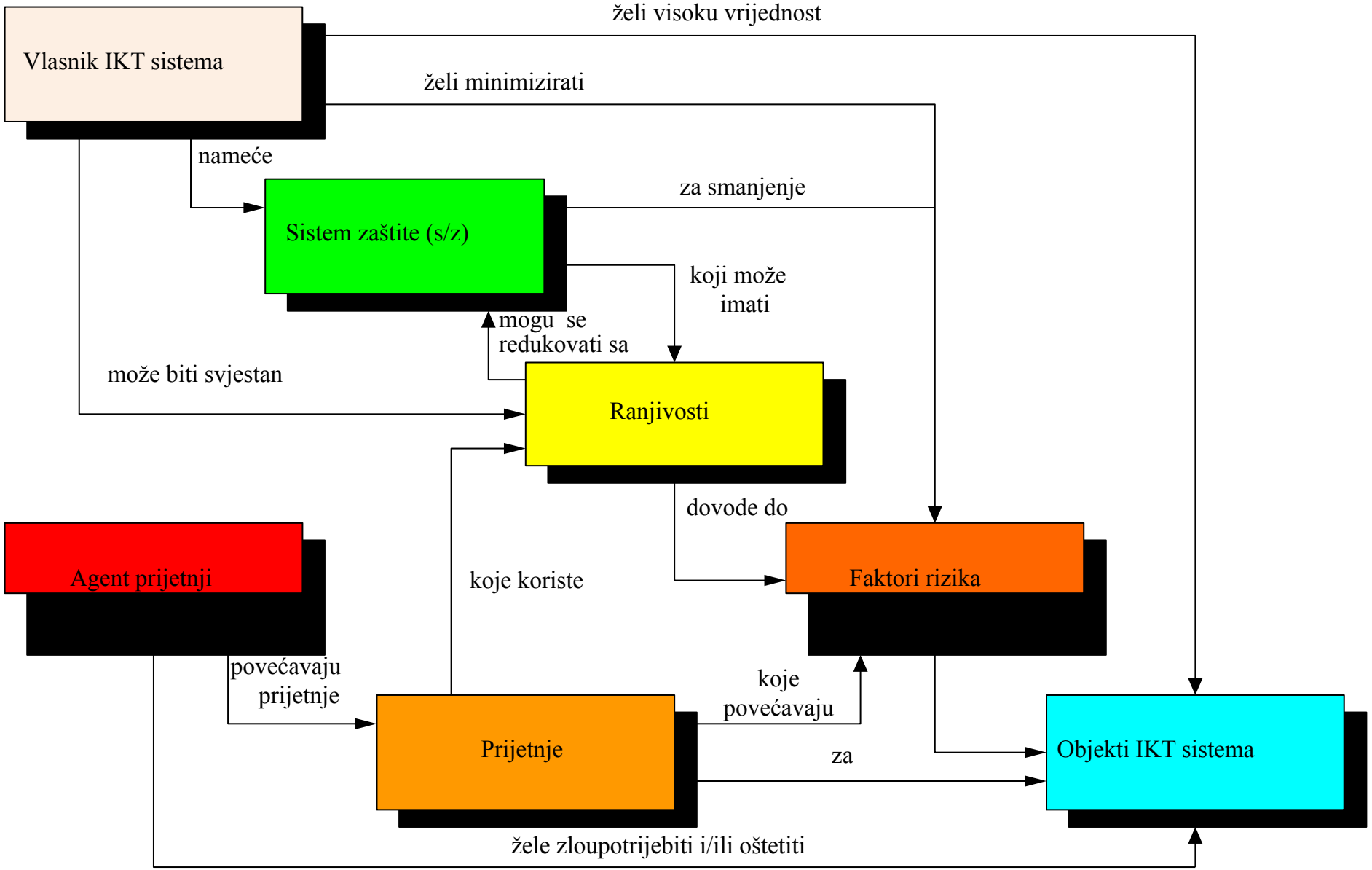
- **Resursi sistema zaštite značajno poskupljuju PIS**
- **Cilj procesa upravljanja zaštitom (ISMS*):**
  - uspostaviti i dostići bezbjednosne ciljeve
  - projektovati, implementirati i održavati *optimalan SZ*
- **Optimalno rješenje zaštite (**generički koncept**):**
  - *rentabilan i funkcionalno efektivan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

ISMS*- *Information Security Management System*

Optimalan sistem zaštite



GENERIČKI MODEL SISTEMA ZAŠTITE



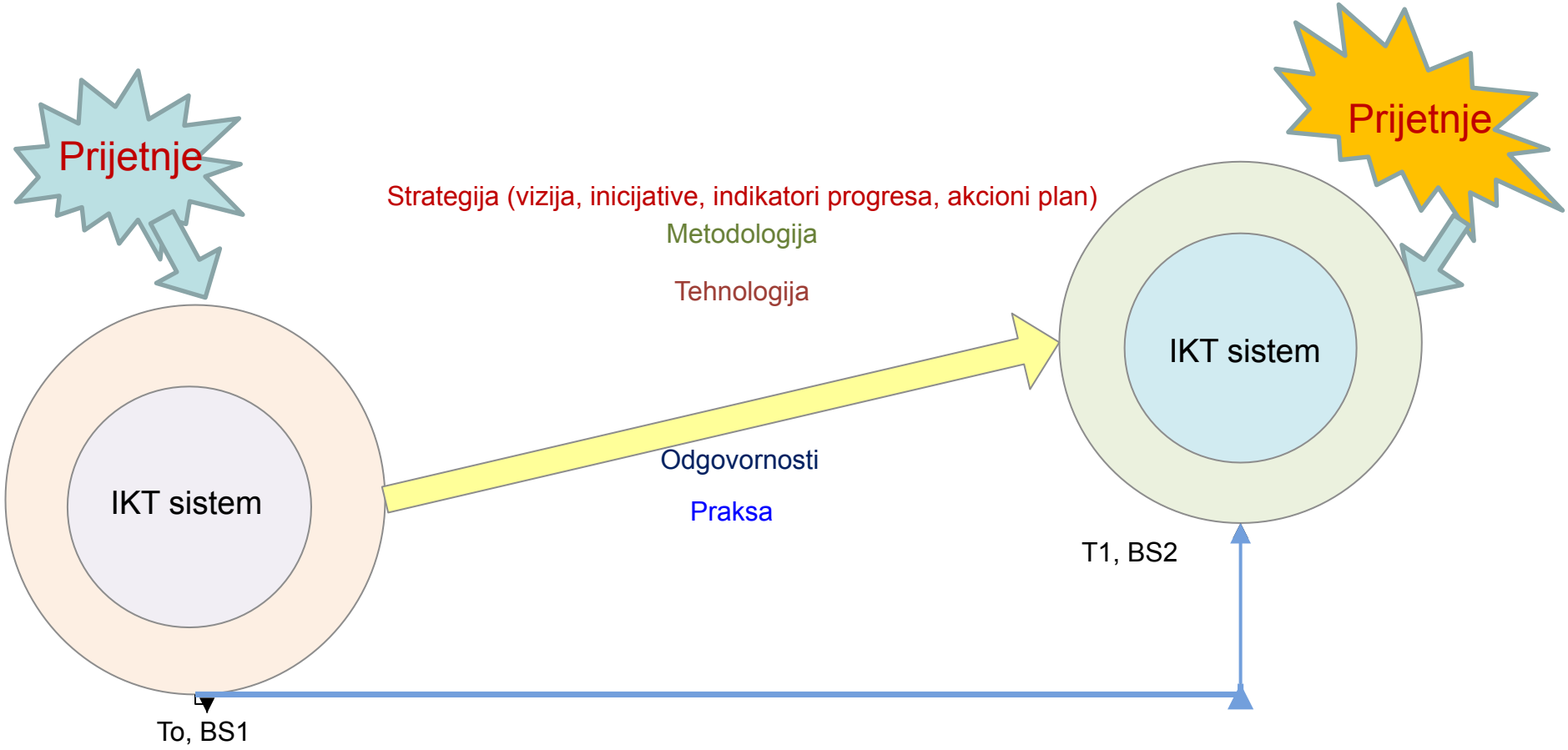
Generički model sistema zaštite (SZ)

1. **SZ štiti informacionu imovinu (ISO/IEC 27001)** od:
   - **Prijetnji***: potencijalni, slučajni i namjerni agenti-faktori rizika koji mogu izazvati štetu*
     Primjer*: maliciozni kodovi, greške hw-sw, ljudske aktivnosti*
   - **Napada:** *realizovana prijetnja = bezbjednosni incident*

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

Promjena stanja bezbjednosti

Proces promjene stanja bezbjednosti informacija



Primjer: *OCTAVE* metodi implementacije programa/SZ

Proces 4-fazne tranzicije bezbjednosnog 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

Primjer: *OCTAVE* metodi implementacije programa/SZ

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

Primjer: *OCTAVE* metodi implementacije programa/SZ

1. Obuka zaposlenih

- ***Svi zaposleni*** - izgraditi svijest 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 svijest o potrebi zaštite, da razumiju ulogu i odgovornost
- ***Operativno osoblje*** - dodatnu obuku (po planu zaštite)

Primjer: *OCTAVE* metodi implementacije programa/SZ

2. Kontrola usaglašenosti - integracija S/Z:

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

1. *Kontrola opšte* usaglašenosti:– vrši upravna struktura:
   - korišćenja IS i primjeni *normativa* i standarda zaštite
   - **alat: menadžerska, interna i nezavisna provjera**
2. *Kontrola specifične* usaglašenosti:
   - *prakse zaštite sa politikom*
   - *podrške poslovnim procesima*
   - *operativnog korišćenja tehnologija zaštite*
   - **alat: menadžerska i interna provjera**

Primjer: *OCTAVE* metodi implementacije programa/SZ

3. Nametanje obaveze izvršavanja i izvještavanja:

- slijedi obuku, nadzor i provjeru usaglašenosti prakse i politike zaštite

- **Izvještaj o nadzoru, kontroli, provjeri**:
  - 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 unaprijed osmisliti - od **upozorenja** do **otpuštanja sa posla**, ili **sudskog gonjenja**

Primjer: *OCTAVE* metodi implementacije programa/SZ

- ***ISACA*** (*Information System Audit and Control Association*) predlaže da izvještaj provjeravača:
  - **pokaže** koji sistem mjera je koristio *auditor*
  - **pomogne** u planiranju, radu i kontroli rada *auditor*-a
  - **olakša** nezavisnu provjeru rada *auditor*-a
  - **evaluira** sistem kvaliteta **programa provjere**
  - **obezbijedi** 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 najvrijednije 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*

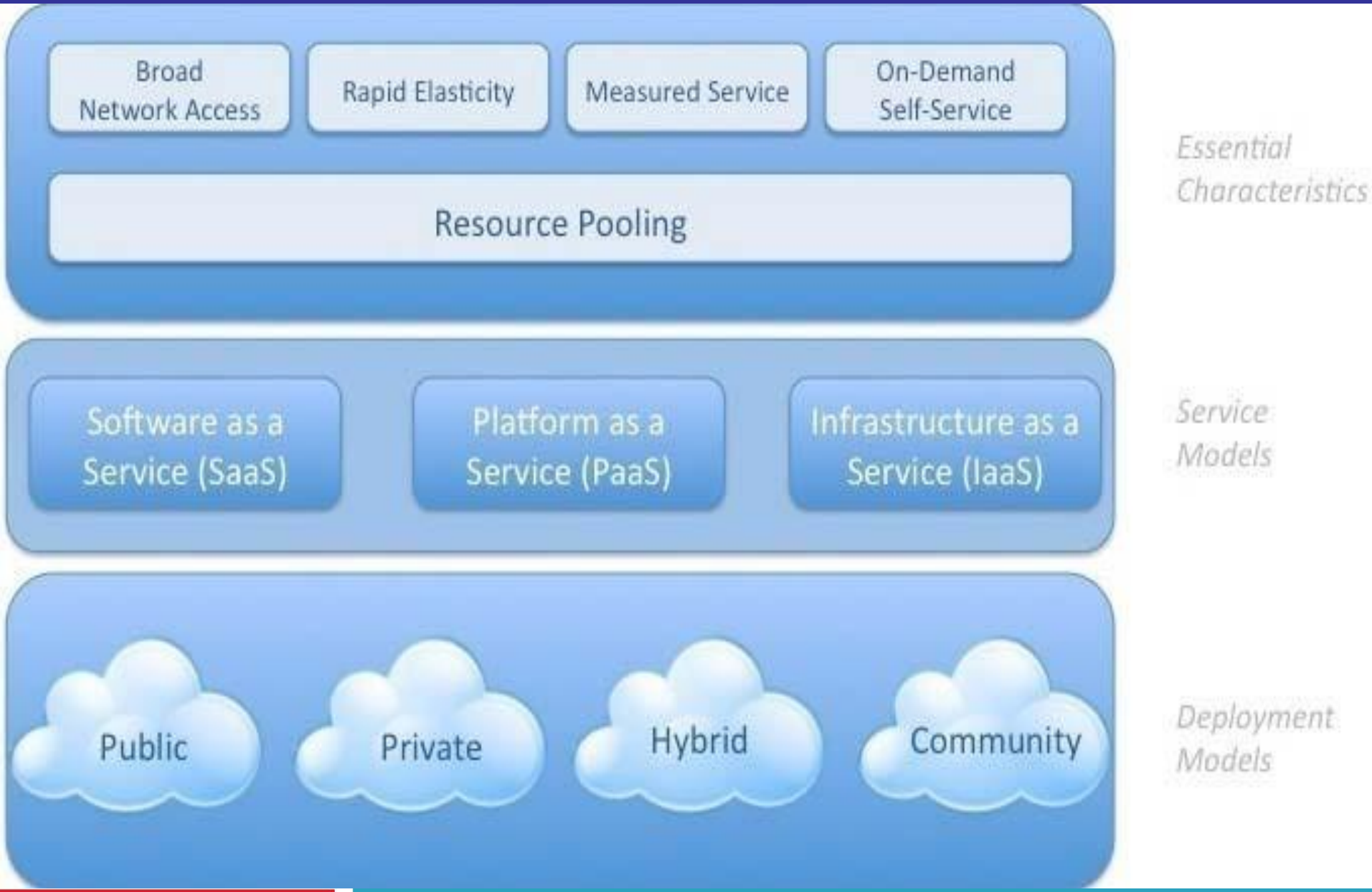
Nova paradigma zaštite informacija

- **Gube se fizičke granice organizacije** (e-poslovanje, CC...)
- **Ozbiljne interne prijetnje (**krize, nezadovoljni korisnici**...)**
- Organizacije sve više **diverzifikuju lanac vrijednosti**
- Učestvuju različite org., koje imaju jednako značajne uloge
- Neki slojevi zaštite biće efektivni - samo ako se **implementiraju** svima **u distribuiranom lancu vrijednosti**.
- **Virtuelizacija serverske i klijentske strane**:
  - mijenja zaštitu ***slojeva luka*** na ***prstenove slojeva luka*** ili
  - **distribuiranu slojevitu zaštitu po dubini**
- **CC sistemi zahtijevaju promjenu 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 dijeljenje i iznajmljivanje servisa* za nadoknadu
  - *pouzdanost* (redundantnost) i *skalabilnost resursa*,
  - *održivost i **bezbjednost?***
- **Problem:**
  - *novi tipovi ranjivosti*
  - *zaštita informacija 1000-e korisnika*
  - *DF istraga u slučaju napada*

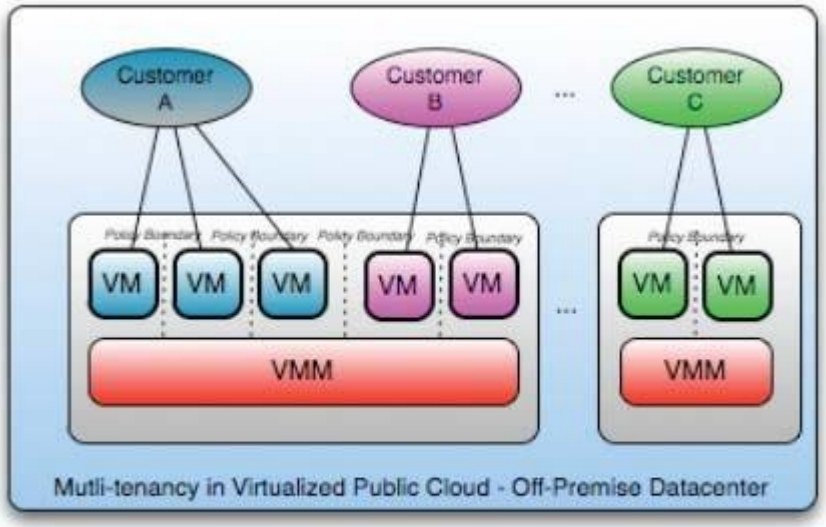
Primjer: Vizuelni model definicije *CC* (NIST)



Primjer: višestruko rentiranje servisa

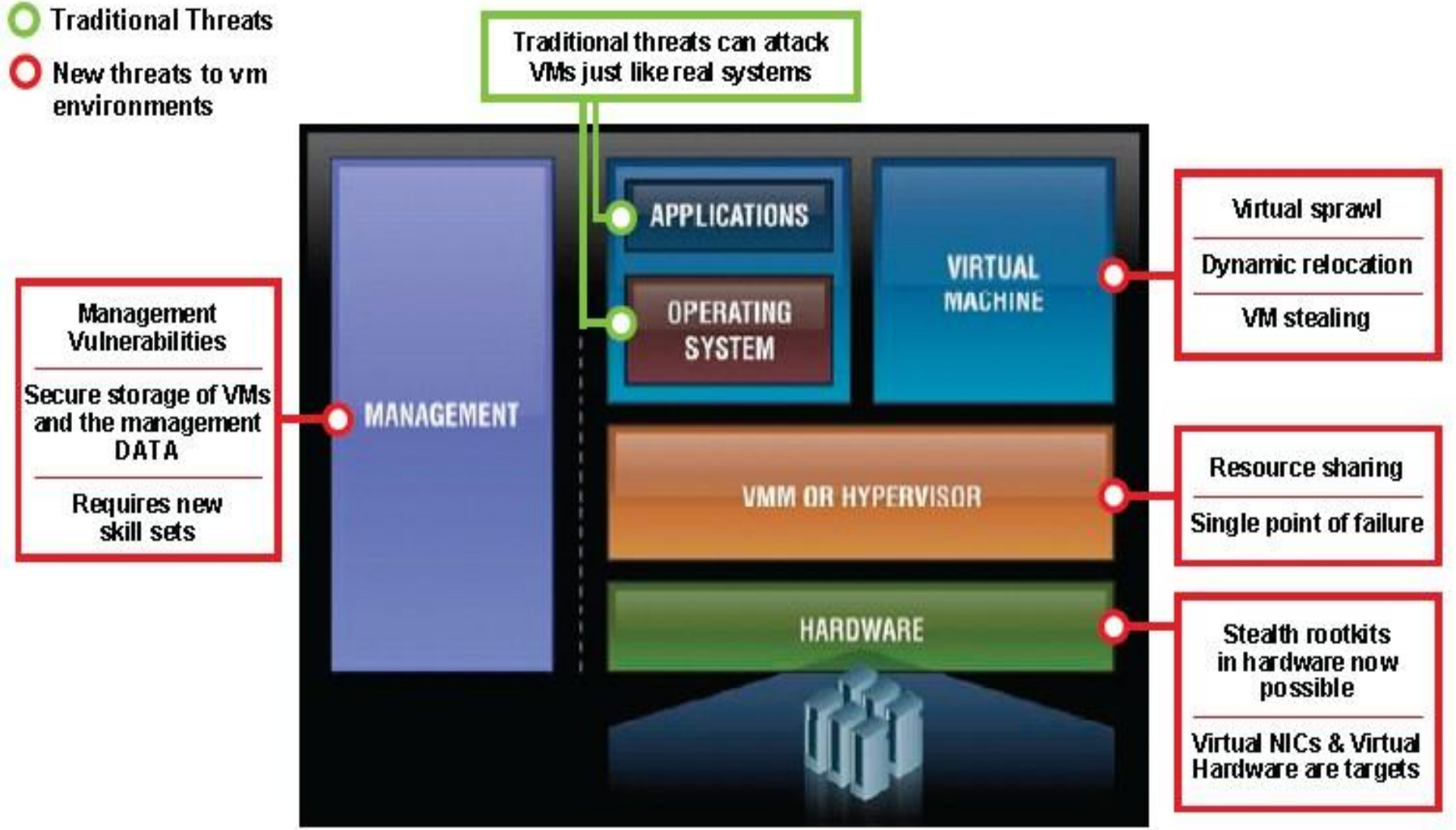
-Multy-tenancy-

(**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)



MORE COMPONENTS = MORE EXPOSURE

Koncept zaštite informacija u CC

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

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

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

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

CSP *(Cloud Service Provider) u CC sistemu*

Nova paradigma zaštite informacija

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

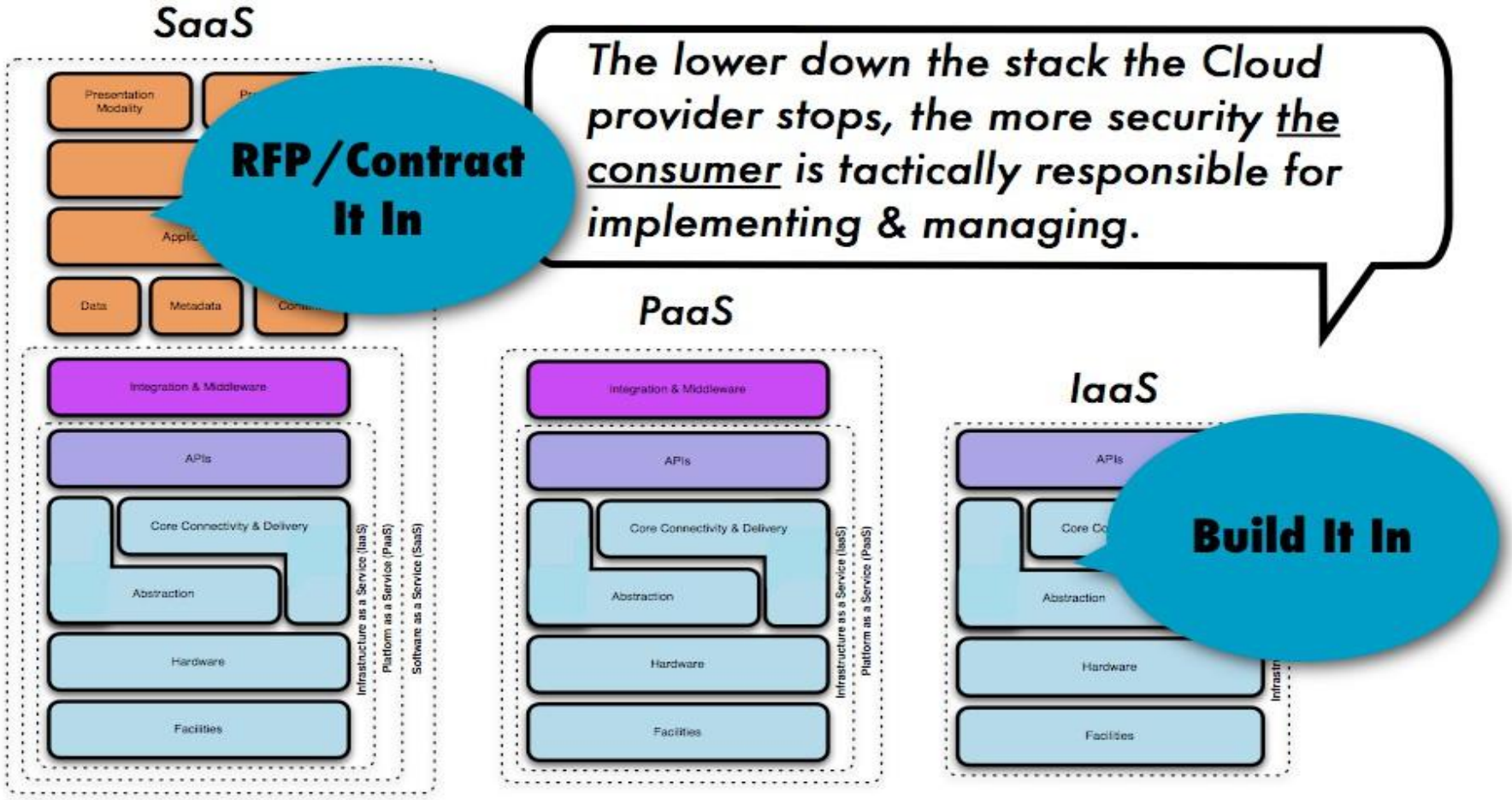
1. **Dopuniti generičku metodologiju za upravljanje rizikom sa:**
   - *mikoranalizom rizika,* umjesto scenarija rizika na *makro* planu
   - obaveznim uključivanjem upravljanja rizikom u poslovno odlučivanje
   - uključivanjem realnih prijetnji, ranjivosti i uticaja na poslovne procese
2. **Intenzivirati 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 prijetnji
   - *prediktivni sistem zaštite* (inteligentni agenti)
   - *proaktivna DF* i *integracija servisa DF istrage* u sistem CC zaštite...

Nova paradigma zaštite informacija

3. **Obezbijediti određeni nivo digitalne forenzičke istrage**

- **Veći broj digitalnih uređaja na Internetu zahtijeva**:
  - praćenje bezbjednosno 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 prijetnji koje pogađaju kritične procese*
  - *aktivna, selektivna analiza bezbjednosnih događaja u log serveru*
  - *konvergencija i integracija* ***forenzičkih i alata zaštite***

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



Primjer: mehanizmi zaštite CC

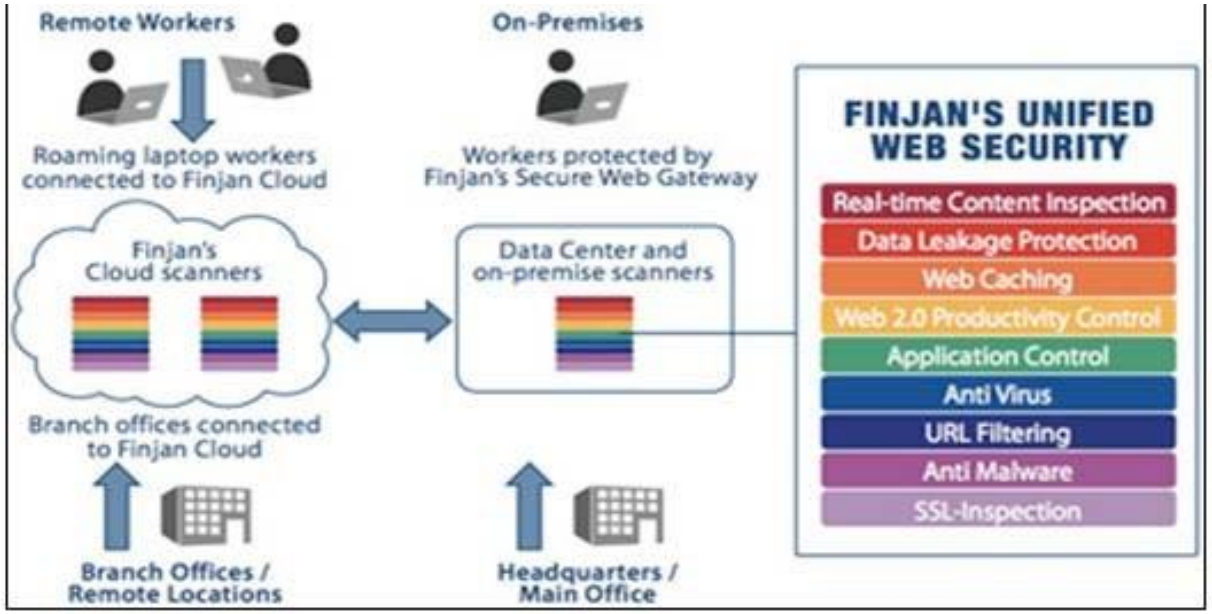
1. **Distribuirana veb aplikaciona barijera (DWAF):**
   - dinamički skenira CPU, računare, servere i mrežne uređaje
   - usmjerena je na detekciju/sprječavanje napada
   - treba da bude:
     - *virtuelna, softverska aplikacija*, *plug-in*, *SaaS,* ili *integrisana* u postojeći hardver
     - laka za 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

Primjer: 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 obezbijedi *proaktivnu virtuelnu zaštitu:***
   - da imaju **mehanizme za upravljanje zaštićenom sesijom, šifrovanje URL i autentifikaciju**
   - da **obezbijede virtuelizaciju forme i polja na nivou DWAF, a ne samo na nivou aplikacije**

Primjer: mehanizmi zaštite CC

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



Primjer: mehanizmi zaštite CC

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

- **Problem klasičnih AVP sistema zaštite**:
  - *reaktivni* SZ neprekidno štite RS/RM od *poznatih* prijetnji
  - 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
- **Rješenje:**
  - razvoj bržeg metoda skeniranja na bazi *paralelnog procesiranja*
  - računarske podatke dijeli u *batche* fajlove koji se procesiraju paral.
  - slično, proces skeniranja AVP dijeli se prema specifičnim prijetnjama

Primjer: 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 prijetnji – MP (viruse, crve, trojance...)
     - kada *DM* otkrije prijetnju, brzo privuče druge DM
     - na određenoj koncentraciji privlače pažnju administratora zaštite da pokrene istragu KI
     - zatim se brzo vrate redovnim zadacima

Primjer: 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
  - tragovi privlače druge DM do mjesta napada
  - kolonija digitalnih mrava označava potencijalnu infekciju računara i
  - zahtijeva intervenciju administratora zaštite

Primjer: 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 uspješno otkrili
  - Cilj - implementirati u RM 3.000 različitih tipova DM
  - Model najviše odgovara za velike RM koje dijele 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

Primjer: mehanizmi zaštite CC
-IBM rješenja-

- *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