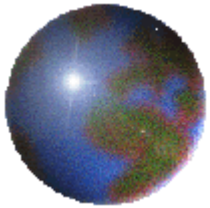
Fakultet organizacionih nauka
Uvod u informacione sisteme
Prof. dr Ognjen Pantelić



Bezbednost i zaštita informacionih sistema

Opasnosti po IS prema uzroku nastanka

- Prirodne opasnosti (elementarne nepogode, prirodna zračenja).
- Čovek sa aspekta nenamernosti (loša organizacija, nedisciplina, nemar, nehat, zamor i dr.).
- Čovek sa atributom namernosti (diverzija, sabotaža, zlonamernost, kriminal, špijunaža).

Ranjivost sistema

Drastično je povećana rasprostranjivanjem umrežavanja i pojavom wireless tehnologija.

- Klasifikacija **namernih** pretnji:
  - Krađa podataka
  - Neovlašćeno korišćenje podataka
  - Krađa računarskog vremena
  - Krađa opreme i / ili programa
  - Svesne manipulacije pri rukovanju
  - Unos, obrada i transfer podataka
  - Opstrukcije i štrajk
  - Sabotaže
  - Namerno oštećenje opreme
  - Destrukcija virusima
  - Teroristički napadi

Komponente integralne zaštite IS

- Fizička zaštita – računarske opreme i resursa.
- Zaštita pristupa – zabrana pristupa računarskim resursima neautorizovanim korisnicima.
- Zaštita komunikacija – kontrola kretanja podataka kroz mrežu.
- Zaštita aplikacija.

Mere bezbednosti pri nabavci, instalaciji, korišćenju i održavanju hardvera

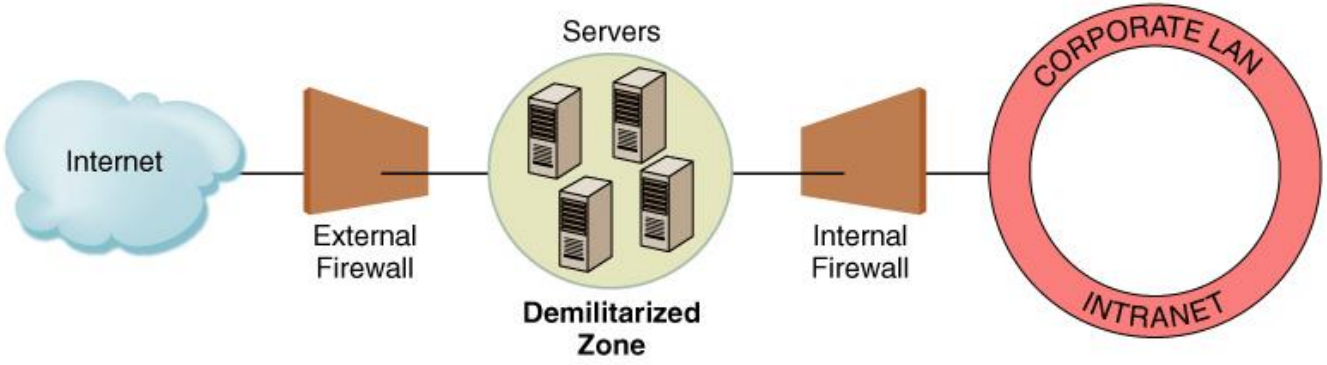
- Nabavka kvalitetnog hardvera od kvalitetnih dobavljača.
- Evidencija računarske opreme.
- Instalacija hardvera od strane kompetentnih lica.
- Korišćenje uređaja za neprekidno napajanje – UPS.
- Korišćenje hardvera uz:
  - mere tehničke zaštite,
  - zaključavanje prostorija,
  - plombiranje računara i ostale opreme.
- Izbegavati premeštanje, pozajmljivanje i iznošenje računarske opreme.
- Održavanje hardvera poveriti stručnoj organizaciji.

Mere bezbednosti pri nabavci, instalaciji, korišćenju i održavanju <u>softvera</u>

- Nabavka licencnog softvera.
- Stručna instalacija samo službeno potrebnog softvera.
- Korišćenje softvera
  - bez eskperimenata,
  - uz kopiju na rezervnom medijumu,
  - bez razmene softvera sa drugim korisnicima.
- Održavanje softvera od strane stručnog lica.

Mere bezbednosti u fazi eksploatacije IS

- Definisati procedure rada i vršiti kontrolu njihovog poštovanja.
- Vršiti kontorlu ovlašćenja izmena u aplikacijama.
- Definisati postupke u slučaju vanrednih situacija.
- Koristiti računar samo za izvršavanje službenih zadataka.
- Pristup sistemu pomoću lozinke.
- Računar sa najvažnijim podacima ne povezivati na Internet.
- Svi medijumi sa podacima treba da budu evidentirani.



Strategija zaštite

- Glavni zadaci strategije zaštite:
  1. Prevencija i zastrašivanje
  2. Detekcija
  3. Lokalizacja oštećenja
  4. Oporavak
  5. Korekcije
  6. Opreznost i disciplina

Strategija zaštite na Internetu

1. zaštita pristupa.
2. kontrola autentičnosti.
3. kontrola ovlašćenja.

1. zaštita pristupa

- skeniranje na viruse
- Fierwalls
- privatne meže

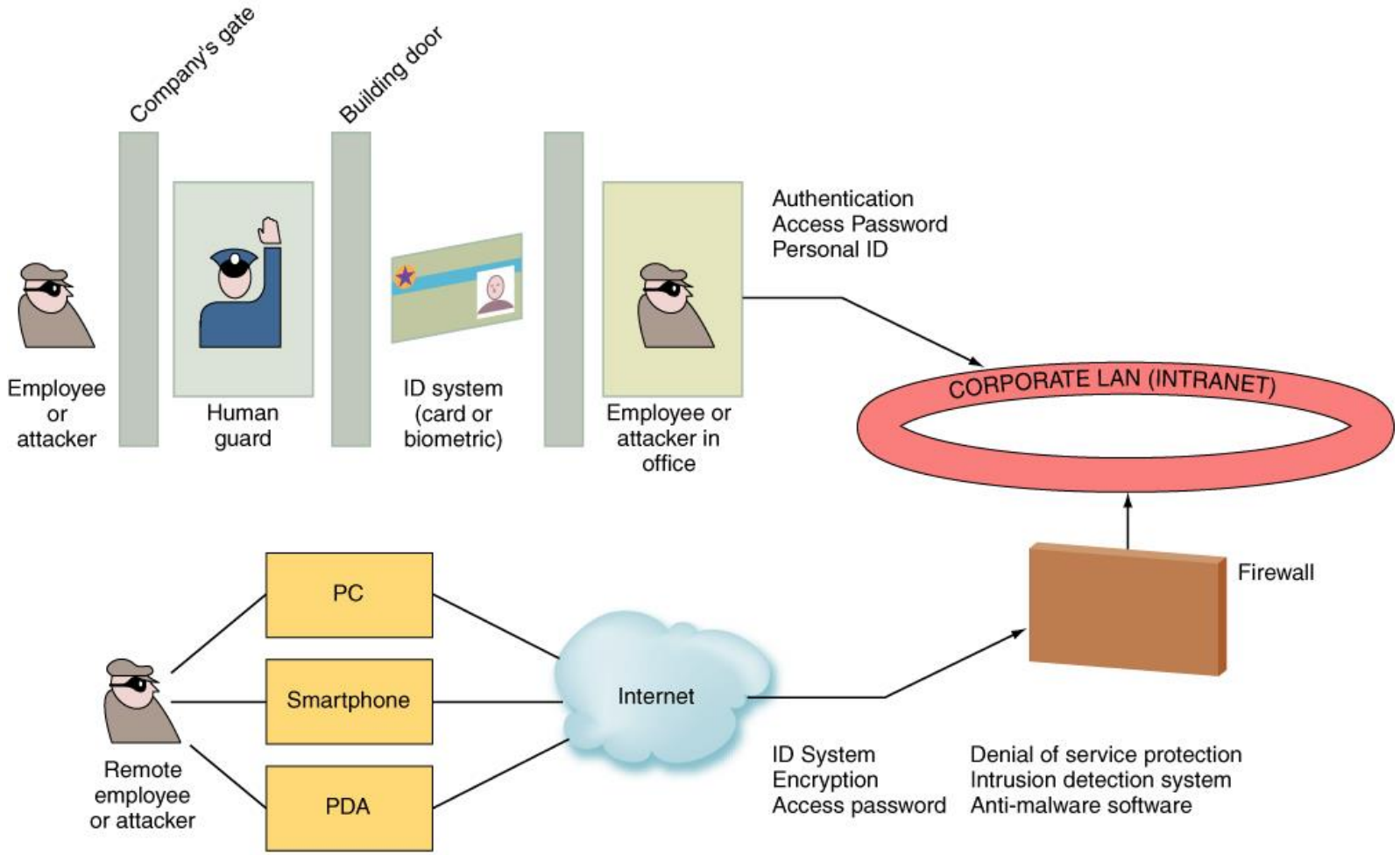
2. kontrola autentičnosti

- Korisnićko ime/lozinka
- Javni ključ
- Biomertija

3. kontrola ovlašćenja

- Ovlašćenja grupe
- Dodela uloga

Lokacije zaštitnih mehanizama

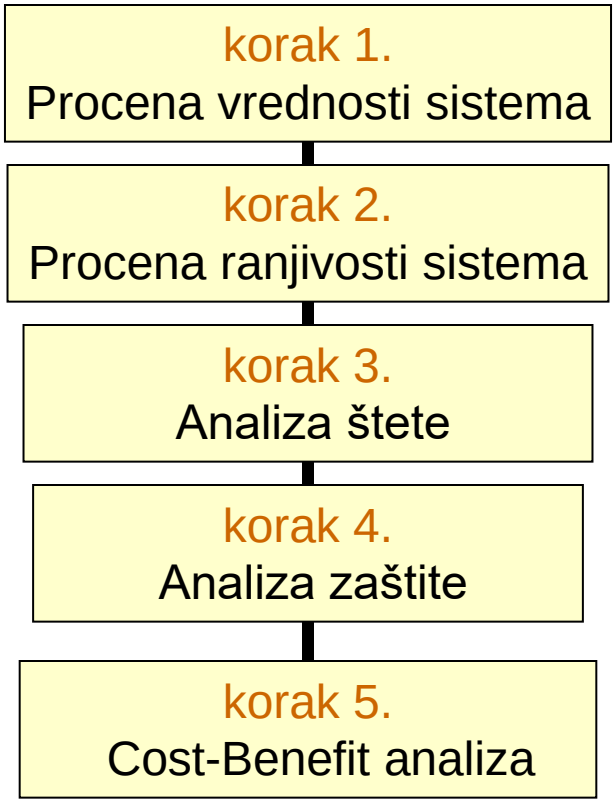


Kontrola

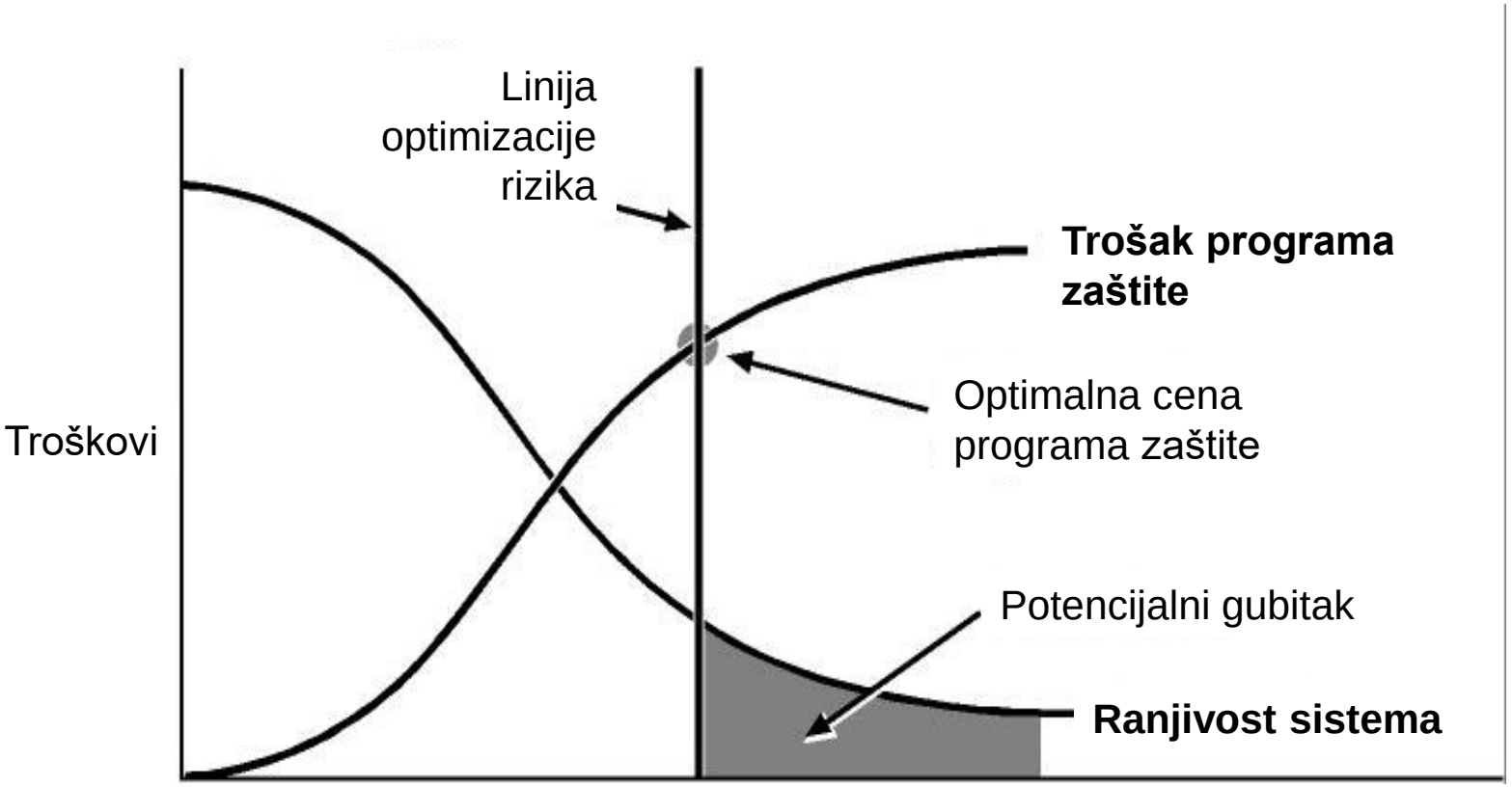
- Vrste kontrole:
  - Operaciona kontrola – da li sistem radi korektno?
  - Kontrola podobnosti – da li su sistemi zaštite odgovarajući i adekvatno ugrađeni?
- Tipovi kontrolora:
  - Interni – iz preduzeća, ali ne iz strukture ICT.
  - Eksterni – iz nezavisne firme.

Upravljanje rizikom

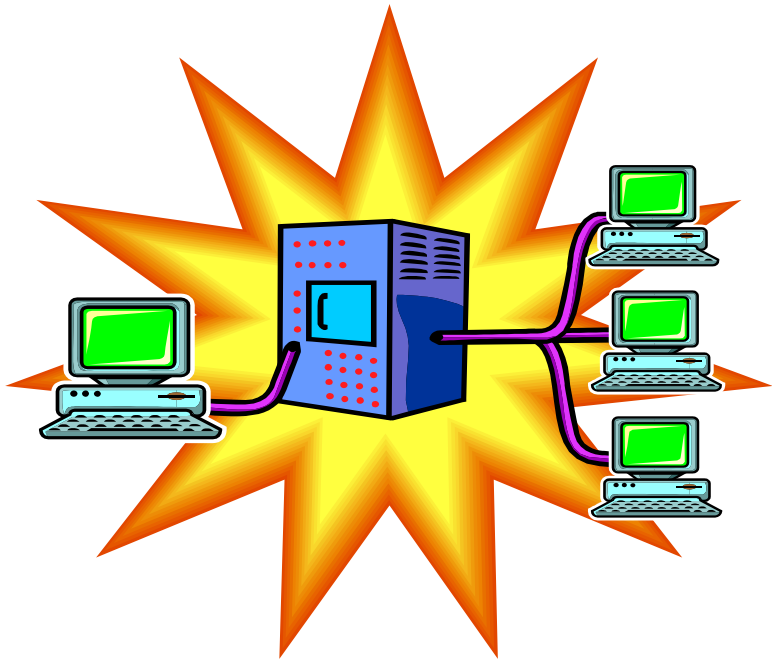
- Nije ekonomično uvođenje zaštite od svih mogućih pretnji.
- Program zaštite treba da obuhvati očekivane pretnje.



Optimizacija rizika



HAVARIJA

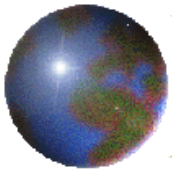


Plan oporavka - važan elemenat zaštite

- Cilj plana je održanje kontinuiteta poslovanja.
- Plan mora biti čuvan na sigurnom mestu, njegove kopije kod svih menadžera, raspoloživ i na Intranetu i periodično ažuriran.
- Plan mora biti napisan jasno i nedvosmisleno, da bi bio upotrebljiv u trenutku nezgode.
- Sve kritične aplikacije moraju imati jasne procedure za oporavak.
- Ispitivanje plana podrazumeva korišćrenje what-if analize.
- Plan mora sadržati opciju i za slučaj potpunog uništenja kapaciteta.

Elementi Plana oporavka

- **Analiza uticaja na poslovanje.**
- **Organizaciona odgovornost** pre i posle havarije.
- **Strategija oporavka** Data centara, file servera po sektorima, mrežnih srevera, desktop računara (“in office” i "at home"), laptopa i PDA.
- **Procedure za oporavak** u formi ček-lista.
- **Plan procesa administracije**.
- **Tehnički dodatak** koji uključuje neophodne brojeve telefona i tačke za kontakt.
- **Opis posla menadžera za oporavak** (na max 3 strane) – uključuje i opise poslova članova tima za oporavak.
- **Plan rada sa šablonima za modifikacije i implementacije**. Sadrži listu rezultata za svaki zadatak.



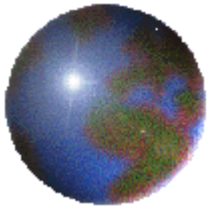
Elementi za test Plana oporavka

- **Odgovornosti menadžera** za oporavak
- **Distribucija** Plana oporavka
- Ažuriranje **Analize uticaja na poslovanje**
- **Trening** tima za oporavak
- **Evaluacija** testa Plana oporavka
- **Održavanje** Plana opopravka
- **Usklađenost sa standardom ISO 27000** (ranije ISO 17799)

Stanje u Srbiji: svest o informacionoj bezbednosti je nedovoljno razvijena

UZROCI:

- još uvek mali obim primene IKT i relativno mali obim ugrožavanja bezbednosti,
- odsustvo šire stručne analize i kritike stanja bezbednosti,
- malo javnih e-servisa (e-uprava, e-trgovina, e-plaćanje, e-zdravstvo)
- slaba informisanost građana o pravu na zaštitu podataka o ličnosti i pravu na privatnost,
- nepoznavanje i potcenjivanje potencijalnih opasnosti,
- neangažovanost države u razvoju normativnog okvira za informacionu bezbednost i primenu postojećih propisa,
- mali broj kompanija ima internu regulativu o informacionoj bezbednosti,
- skrivanje informacija o gubljenju, uništavanju i zloupotrebi podataka.



Cyber kriminal i Cyber forenzika

Cyber kriminal

- Korišćenje ICT i računarskih mreža u cilju realizacije kriminalnih aktivnosti.

Cyber forenzika

- Prepoznavanje situacija u kojima se primena ICT i računarskih mreža transformiše u kriminalne aktivnosti.
- Obezbeđivanje dokaza neophodnih za krivično gonjenje počinilaca cyber kriminala.

Aktivnosti FORENZIČKE PRAKSE

- Sprovođenje forenzičke istrage u okviru slučajeva kompjuterskog kriminala, veštačenja i super veštačenja.
- Identifikacija, analiza, obezbeđenje i prezentacija digitalnih i cyber kompjuterskih dokaza:
  - Data mining-a u oblasti cyber forenzike.
  - E-mail forenzika, povraćaj obrisanih podataka, Disk imageing.
  - Implementacija oblika auditinga.
  - Izrada softverskih forenzičkih alata.
- Pružanja stručne pomoći u monitoringu i zaštiti informacionih sistema i kompjuterskih mreža.
- Uvođenje cyber forenzike u sistem unutrašnje kontrole poslovanja.

Metodologija upravljanja kompjuterskom forenzikom

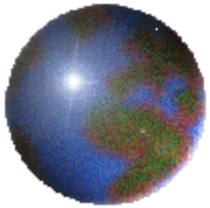
- **Identifikacija**: izvori digitalnih dokaza.
- **Prikupljanje**: snimanje uređaja na mestu zločina.
- **Čuvanje**: Lanac staranja i očuvanja integriteta podataka u cilju obezbeđenja da se nijedna informacija ne izgubi ili izmeni.
- **Izveštavanje**: izveštavanje o svim zaključcima i korišćenim procesima.

PROBLEMI :
- Nedostatak ažurnih smernica
- Nedostatak odgovarajućih trening programa
- Nedostatak finansijskih sredstava

Prinicipi Asocijacije policijskih inspektora (Association of Chief Police Officers – ACPO

- **Princip 1:** Nikakva aktivnost od strane istražnih organa i njihovih agenata ne sme da bude usmerena u pravcu izmene podataka koji se čuvaju na računaru ili nekom drugom skladištu, ako postoji mogućnost da će se ti podaci koristiti tokom sudskog procesa.
- **Princip 2:** U izuzetnim slučajevima, kada pojedinac smatra da je neophodan pristup originalnim podacima na računaru ili nekom drugom skladištu, taj pojedinac mora da bude stručan da to i uradi, kao i da pruži razloge i implikacije ovakvog čina.
- **Princip 3:** Mora de se napravi i sačuva zapis svih realizovanih aktivnosti nad elektronskim dokazima. Nezavisno treće lice treba da bude u mogućnosti da ispita te aktivnosti i ostvari isti rezultat.
- **Princip 4:** Pojedinac zadužen za istragu (istražitelj slučaja) snosi svu odgovornost za sprovođenje zakona i ovih principa.

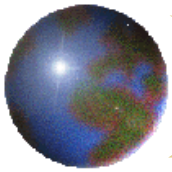
Smernice su javne i moguć je njihov *download* sa sajta http://www.7safe.com/electronic_evidence



Trendovi u razvoju sigurnosti Informacionih sistema

Trendovi u razvoju IT sigurnosti

- Povećanje pouzdanosti sistema
- Računari sa sposobnošću samoozdravljenja
- Inteligentni sistemi za rano otkrivanje upada
- Inteligentni sistemi za praćenje i rano otkrivanje prevara
- Veštačka inteligencija u biometrici
- Ekspertni sistemi za predviđanje i dijagnozu nezgoda
- Smart kartce



Sledeća tema:

- Etički, socijalni i globalni aspekti IS