Akademija tehničko vaspitačkih nauka
Katedra za informaciono komunikacione tehnologije - Niš

Zaštita podataka u komunikac. mrežama

Profesor: dr Mirko R. Kosanović
mirko.kosanovic@vtsnis.edu.rs

Asistent: Nikola Vasić
nikola.vasic@vtsnis.edu.rs

ESPB bodovi: 6
Semestar: VI
Fond časova: 2+2+1

Zaštita podataka u komun.mrežama

Literatura:

Sigurnost računarskih sistema i mreža, *D.Pleskonjić, N.Maček, B.Đorđević,M.Carić, Mikro knjiga 2007*

Osnove bezbednosti mreža: Aplikacije i standardi, *William Stallings, CET 2014*

The Cryp Tool Book: Learning and Experiencing Cryptography with Crypool and SageMath, *Bernhard Esslinger, 2018*

Power Point prezentacije *– Zaštita podataka u komunikacionim mrežama – Mirko Kosanović,*

Zaštita podataka u komun.mrežama

Polaganje ispita:

- Predispitne obaveze:
  - ✓ Laboratorijske vežbe - **obavezne** **0 - 15**
  - ✓ Predavanja **0 - 5**
  - ✓ I kolokvijum **(-5) - 25**
  - ✓ II kolokvijum **(-5) - 25**

Ukupno 0-70 poena, **minimum 30** za izlazak na ispit

- Ispit - pismeni **0 - 30**

Zaštita podataka u komun.mrežama

Ocene:

51 - 60	**:**	**6 (šest)**
61 - 70	**:**	**7 (sedam)**
71 - 80	**:**	**8 (osam)**
81 - 90	**:**	**9 (devet)**
91 - 100	**:**	**10 (deset)**

Programski sadržaj predmeta

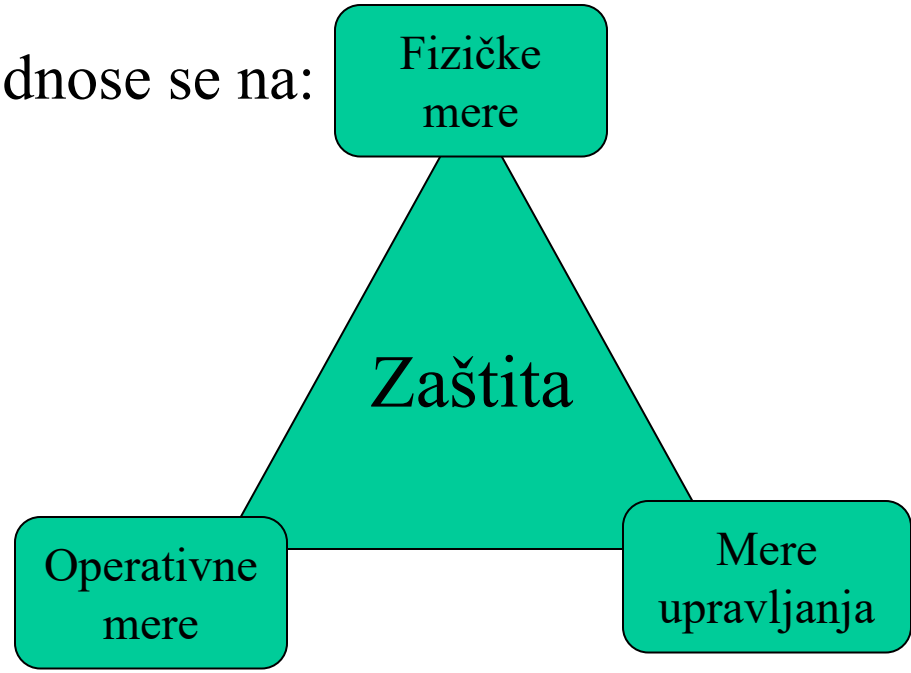
1. Opšti pojmovi o sigurnosti, pretnje, napadi i metode zaštite
2. Procene rizika od napada i neovlašćenog pristupa
3. Osnovni kriptografski pojmovi i njihova primena
4. Kriptografija sa javnim ključevima, heš funkcije, digitalni potpisi i sertifikati.
5. Sigurnosne arhitekture i protokoli, IPSec, SSL
6. Sigurnosni protokoli - SSH, Kerberos, Radius
7. **Prvi kolokvijum**

Programski sadržaj predmeta

8. Nadzor računarskih mreža i mrežne barijere
9. Sigurnost i nadzor bežičnih računarskih mreža i mobilnih mreža
10. Kontrola pristupa i zaštita operativnog sistema
11. Sigurnost baza podataka i sigurnosni aspekti programiranja
12. Bezbednost elektronskog poslovanja i Interneta
13. Organizacione, fizičke i pravne metode zaštite i sistemi za otkrivanje i sprečavanje napada
14. **Drugi kolokvijum**

1 – Opšti pojmovi sistema zaštite

- Zaštita podataka informacionog sistema obuhvata tri osnovne oblasti, koje se odnose na različite delove zaštite računarskih sistema.
- Efikasni plan zaštite sadrži procenu rizika i odgovarajuću strategiju i metode za svaku pojedinačnu oblast.
- Te oblasti zaštite računarske mreže odnose se na:
  1. **fizičke** mere zaštite
  2. **operativne** mere zaštite
  3. **upravljanju** i **politika** zaštite



- Svaka od navedenih oblasti ima izuzetnu važnost u uspostavljanju efikasnog sistema zaštite u nekoj organizaciji
- Posao administratora sistema zaštite jeste i da daje predloge organima upravljanja o potrebama i nedostacima, da preduzima mere za smanjenje rizika i izloženosti podataka i sistema, i da uspostavlja, unapređuje i održava sigurnost sistema sa kojim radi.

1.1 – Zaštita fizičkog okruženja

- Fizička zaštita podrazumeva sprečavanje da neovlašćene osobe pristupe opremi i podacima.
- Fizičke mere štite elemente koji se mogu videti, dodirnuti ili ukrasti.
- "Nosioci" ovakvih pretnji mogu biti serviseri, domari, klijenti, dobavljači, pa čak i svi radni ljudi u preduzeću.
- Sve fizičke mere zaštite mogu se podeliti u nekoliko koraka i to:

1. Smanjivanje privlačnosti fizičke lokacije kao cilja eventualnog napada: zaključavanje vrata, instaliranje opreme za nadzor, alarmni sistemi i td.
2. Detekcija napada ili kradljivca - korisnik mora znati gde je došlo do provale, šta nedostaje i kako je došlo do gubitka.
3. Oporavak organizacije nakon krađe ili gubitka ključnih podataka i sistema, kako bi organizacija mogla i dalje da normalno nastavi obavljanje redovnog posla. Oporavak zahteva detaljno planiranje, razmišljanje i testiranje kritičnih momenata.

1.2 – Operativne mere zaštite

- Odnose se na način obavljanja poslovnih funkcija u organizaciji.
- One obuhvataju računare, mreže i komunikacijske sisteme, ali i rad sa dokumentima.
- Operativne mere pokrivaju široku oblast, tako da predstavljaju osnovno polje angažovanja profesionalnog osoblja na poslovima zaštite.
- Operativne mere zaštite uključuju kontrolu pristupa, identifikaciju i topologiju zaštite nakon instaliranja računarske mreže, čime su obuhvaćeni dnevno funkcionisanje mreže, njeno povezivanje sa ostalim mrežama, način kreiranja rezervnih kopija (*backup*) i planovi oporavka nakon teških oštećenja.
- Ukoliko primenite sveobuhvatne mere za ograničenje roka trajanja lozinki, korisnici će morati da menjaju lozinke svakih 30 do 60 dana.

1.3 – Upravljanje i politika

- Upravljanje i politika (*management and policies*) osiguravaju osnovne upute, pravila i procedure za implementaciju zaštićenog okruženja.
- Definisana politika mora imati punu podršku organa upravljanja da bi bila efikasna.
- Profesionalci u oblasti zaštite predlažu mere koje će biti ugrađene u politiku, ali im je za punu implementaciju tih mera potrebna pomoć organa upravljanja.
- Zaštita mreže zahteva definisanje brojnih pravila koja se navode u sledećoj listi:
  - ✓ administrativna politika
  - ✓ zahtevi u pogledu dizajna softvera
  - ✓ planovi oporavka sistema nakon težih padova
  - ✓ u oblasti podataka
  - ✓ politika zaštite
  - ✓ pravila upotrebe
  - ✓ pravila koja definišu korisnička ponašanja

2 – Ciljevi sistema za zaštitu

- Ciljevi sistema za zaštitu podataka su jasni i precizni i predstavljaju okvir za planiranje kompletnog sistema zaštite i za njegovo održavanje.

Prevencija podrazumeva sprečavanje nastanka prekršaja u vezi sa računarima ili podacima. Pojave narušavanja sistema zaštite nazivaju se incidentima i oni se mogu javiti zbog narušavanja unapred propisanih procedura zaštite.

Detekcija podrazumeva identifikaciju događaja nakon njihovog nastanka. Ona je često otežana jer napad na neki sistem može biti izvršen znatno ranije tj. pre nego što se pokaže uspešnim. Detekcija incidenta podrazumeva utvrđivanje dela opreme koja je izložena napadu. Proces detekcije zahteva primenu složenih alata, ali je nekada dovoljno da se pregledaju sistemske datoteke-dnevnika (***log*** datoteke).

Odgovor podrazumeva razvoj strategija i tehnika radi neutralisanja napada i gubitaka. Ukoliko incident predstavlja samo sondažu terena, napadač verovatno želi da prikupi podatke o mreži i računarskim sistemima kako bi omogućio kasniji napad na sistem.

3 – Implementacija kontrole pristupa

1. **Mandatory Access Control** (MAC), **obavezna** kontrola pristupa predstavlja statički model koji koristi unapred definisani skup prava pristupa ka resursima u nekom računarskom sistemu. Parametre definiše sistem administrator koji ih dodeljuje nalozima, datotekama ili resursima i koristi labele za definisanje nivoa osjetljivosti,
2. **Discretionary Access Control** (DAC), **proizvoljna** kontrola pristupa predstavlja model prava pristupa koji definiše vlasnik podataka-resursa. U ovom modelu labele nisu obavezne. DAC model omogućava deljenje datoteka između korisnika, odnosno rad sa datotekama koje je neka druga osoba proglasila djeljivim. Model uspostavlja listu kontrole pristupa (**ACL-*Access Control List***), u kojoj su navedeni svi korisnici kojima je dozvoljen pristup do podataka.
3. **Role-Based Access Control** (**RBAC**), kontrola pristupa na osnovu **uloga**, predstavlja model koji definiše ulogu koju korisnik ima u organizaciji. Korisnicima se dodjeljuju određene uloge na nivou čitavog sistema, na osnovu kojih oni obavljaju određene funkcije ili dužnosti. **RBAC** model uobičajen je za razne uloge administratora na mreži.

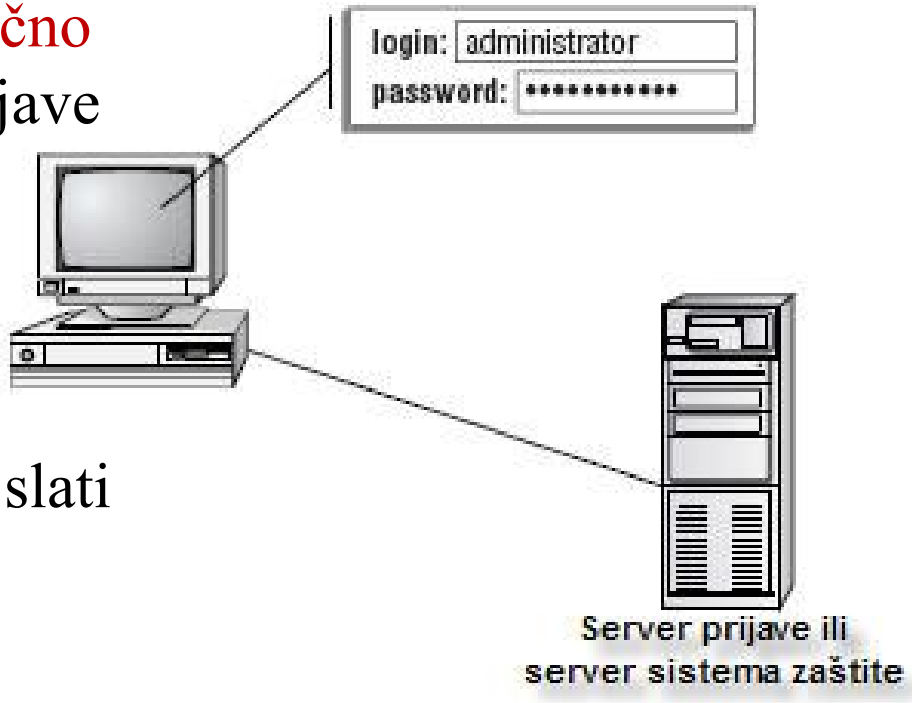
3 – Kako funkcioniše identifikacija ?

- Procesom identifikacije utvrđuje se da li je neka osoba, zaista ona osoba za koju se predstavlja.
- U suštini, to su uvek dva vezana procesa koji se nazivaju ***Identification and Authentication*** (**I&A**).
- Sistemi ili metodi identifikacije zasnovani su na sledećim faktorima:
  1. na nečemu **što korisnik zna**, kao što su lozinka ili PIN
  2. na nečemu **što korisnik poseduje**, poput smart kartice ili nekog identifikacijskog uređaja
  3. na nečemu **što fizički određuje korisnika**, kao što su otisak prsta ili izgled lica, oka, boja glasa, DNK skeneri i td.

- Višestruka identifikacija je proces identifikacije koji se vrši pomoću dva ili više različitih metoda.
- Ukoliko sistem koristi smart kartice i lozinke za pristup resursima, govorimo o dvostrukoj identifikaciji.

3 – Metode identifikacije

- Korisničko ime i lozinka jednoznačno identifikuju korisnika prilikom prijave na sistem (logon).
- Većina operativnih sistema koristi korisnički ID i lozinku za proces identifikacije.
- ID i lozinka se preko mreže mogu slati u otvorenom ili šifriranom obliku.

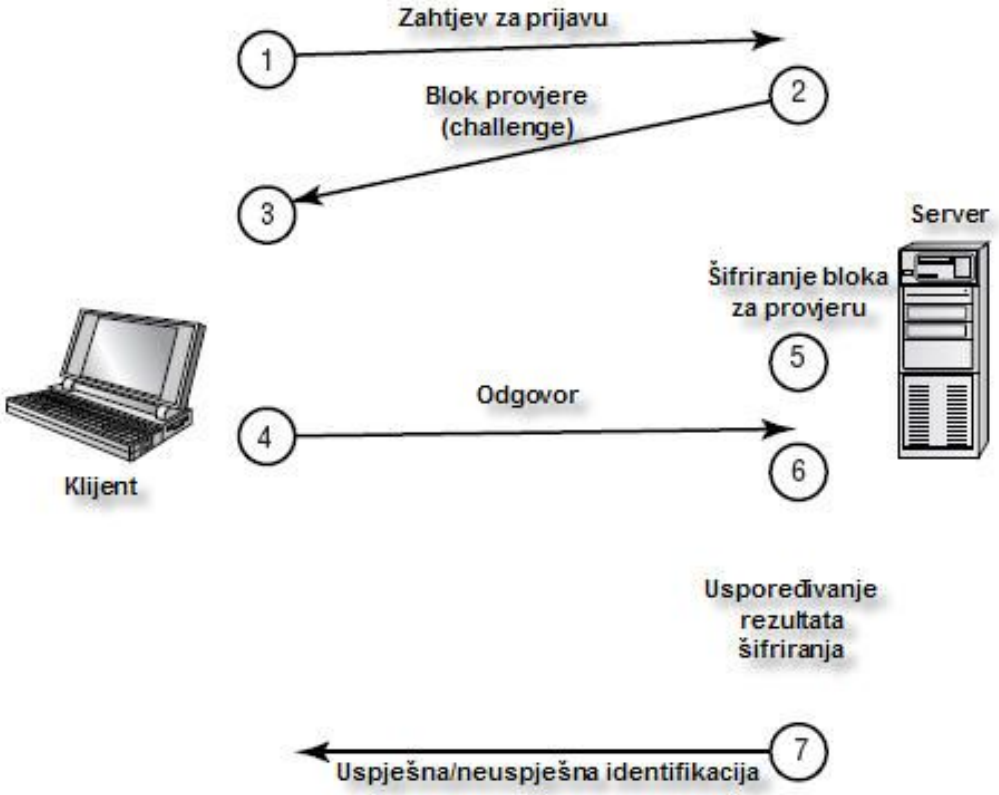


1. **Password Authentcation Protokol** (PAP) ne nudi punu sigurnost ali je jedan od najjednostavnijih metoda identifikacije.
- Korisničko ime i lozinka se u obliku otvorenog teksta šalju na server gde se vrši njihova provera.
- U slučaju da ime i lozinka odgovaraju podacima na serveru korisniku se odobrava pristup, u suprotnom, pristup je zabranjen.

3 – Metode identifikacije

2. Challenge Handshake Authentication Protocol (CHAP) koristi proveru sistema da bi ustanovio identitet korisnika.

- On ne koristi mehanizam korisnički ID/lozinka.
- Korisnik šalje zahtev za prijavu (**1**) sa klijentskog računara prema serveru
- Server šalje blok za proveru (***challenge***) ka klijentu (**2-3**).
- Klijentski računar šifrira dobijeni blok i vraća ga do servera (**4-5**).
- Server proverava dobijenu vrednost (**6**) i u slučaju da je primljena vrednost ispravna potvrđuje identifikaciju (**7**)



3 - Sertifikati

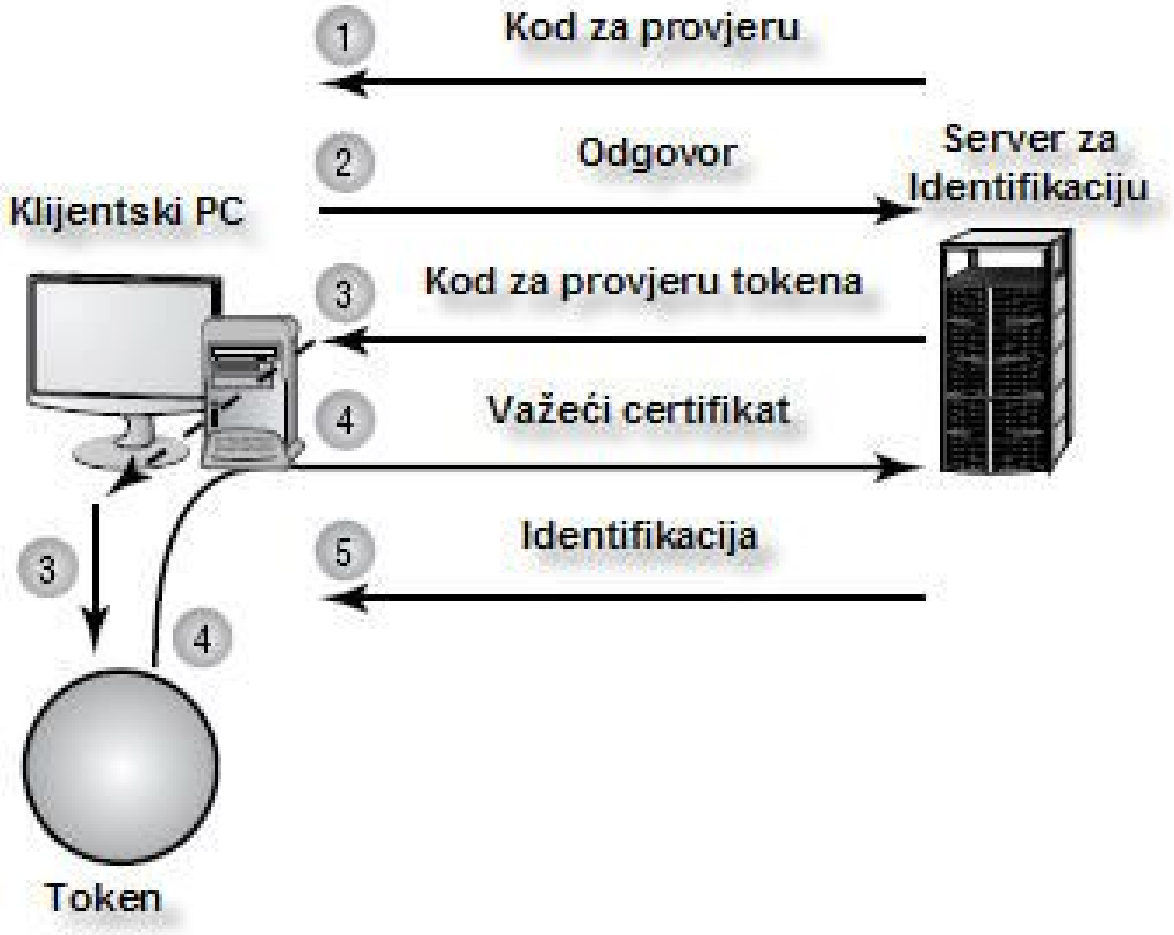
3. Sertifikati se izdaju u obliku fizičkih uređaja, poput smart kartica, ili u elektronskom obliku, u kome se upotrebljavaju kao deo procesa identifikacije.

- Izdavanje i upravljanje sertifikatima je definisano dokumentom čiji je naziv ***Certificate Practice Statement*** (CPS).

3 - Sigurnosni tokeni

4. Sigurnosni tokeni - po funkciji slični sertifikatima.

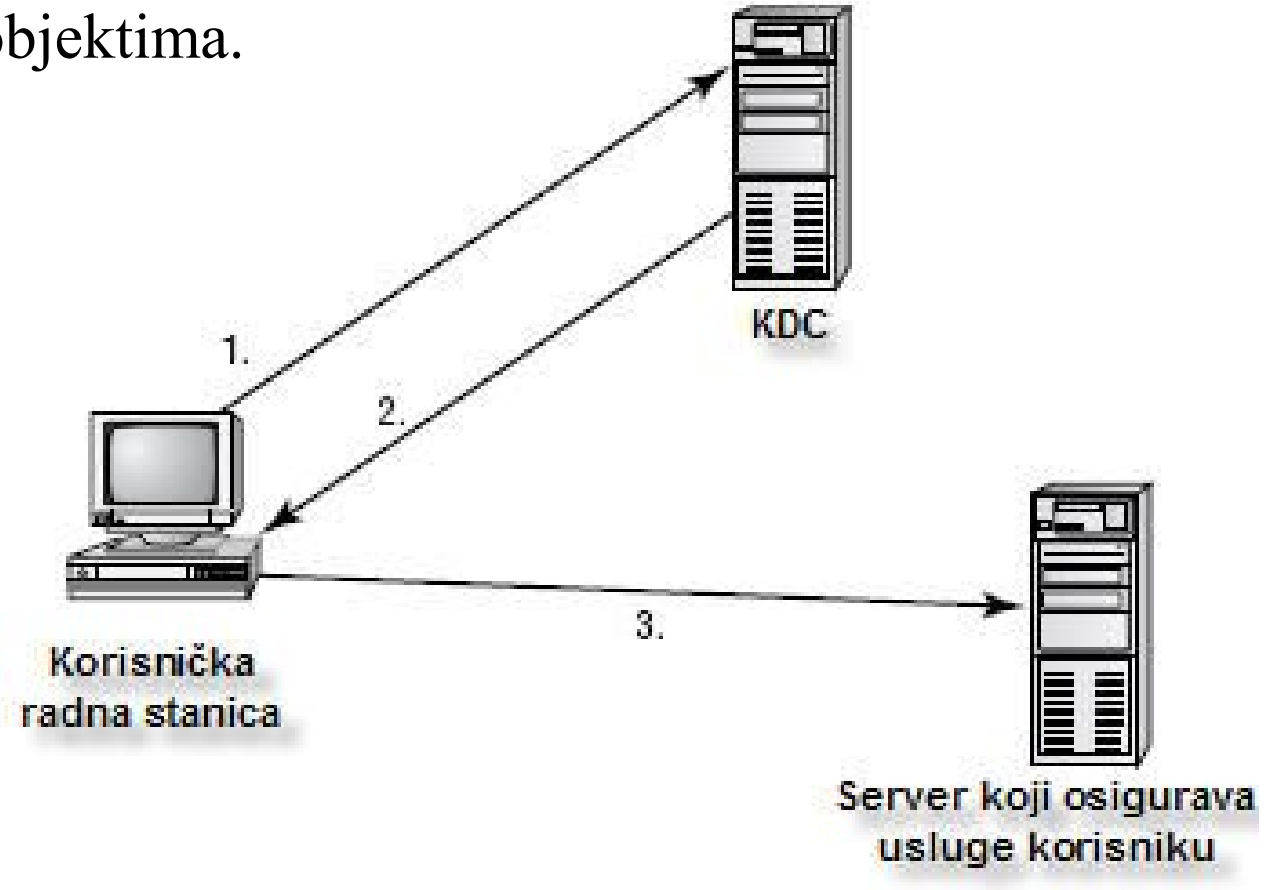
- Sistem za identifikaciju kreira **token** prilikom svakog prijavljivanja korisnika ili na početku sesije.
- Nakon završetka sesije token se uništava.



3 - Kerberus

5. Kerberos je protokol namenjen identifikaciji korisnika.

- Kerberos identifikacija koristi usluge KDC-a (***Key Distribution Center***) koji reguliše celi proces.
- KDC vrši identifikaciju inicijatora procesa i dodjeljuje mu kartu.
- Izdana karta se može iskoristiti za identifikaciju prilikom pristupa drugim objektima.



4 – Topologija zaštite

- Topologija zaštite na mreži definiše dizajn mreže i implementaciju sa stanovišta sistema zaštite.
- Za razliku od mrežne topologije, topologija zaštite se bavi tehnikama pristupa, zaštitom i upotrebljenom tehnologijom.
- Topologija zaštite obuhvata četiri osnovna pitanja:

1. **dizajnerske zahteve**
2. **zaštitne zone**
3. **tehnologiju**
4. **zahtevi poslovnog procesa**

4.1 – Dizajnerski zahtevi

- Određuju probleme poverljivosti, integriteta, dostupnosti i nadležnosti.
- Obično se kaže da su poverljivost, integritet i dostupnost **CIA** sistema mrežne sigurnosti, mada je i nadležnost isto tako važna.

Poverljivost sprečava ili umanjuje mogućnost neovlašćenog pristupa i otkrivanja zaštićenih podataka i informacija. Postoji veliki broj podataka čija se tajnost mora štititi u skladu sa zakonskim odredbama i propisima.

Integritet podataka treba da osigura korektnost podataka sa kojima se radi. On je ključan sa stanovišta topologije zaštite. Organizacije rade sa podacima koji su im dostupni i u skladu sa njima donose važne odluke. Ukoliko podaci sa kojima se trenutno radi nisu ispravni ili ih je izmenila neovlaćena osoba, posledice mogu biti katastrofalne.

Dostupnost osigurava zaštitu podataka i sprečava njihov gubitak. Ukoliko se podacima ne može prići, njihova vrednost je minimalna.

Nadležnost - najveći deo resursa neke organizacije ima deljiv karakter, tako da ih koristi više organizacionih celina i pojedinaca. Dobra je praksa da se uvek definiše vlasnik tih podataka ili resursa koji je odgovoran za njihovu validnost i korišćenje.

4.2 – Zaštitne zone

- Uspostavljanjem **sigurnosnih zona** u mrežama postiže se efekat koji omogućava izoliranje sistema i sprečavanje neovlaštenog pristupa.
- U praksi se najčešće sreću **četiri tipa** sigurnosnih zona:

1. **Internet**
2. **Intranet**
3. **Ekstranet**
4. **Demilitarizirana zona (DMZ)**

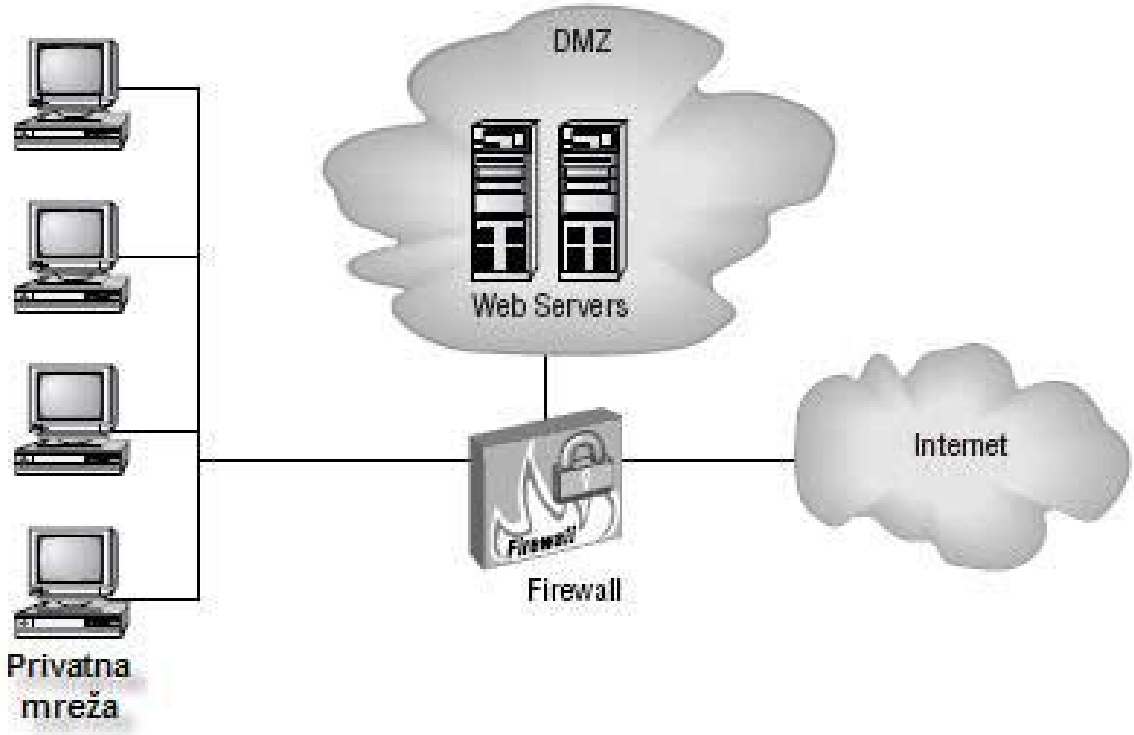
Internet predstavlja globalnu mrežu koja povezuje računare i mreže. Može ga koristiti svako ko ima pristup preko operatera (ISP – *Internet Service Provider*). Takvo okruženje nameće potrebu za niskim stepenom poverenja u ostale korisnike Interneta.

Intranet je vrsta privatne Internet mreže koja je uspostavljena u nekoj kompaniji ili organizaciji. Pristup intranet mreži dozvoljen je samo proverenim korisnicima unutar korporativne mreže.

Ekstranet proširuje granice intranet mreže, tako da u nju uključuje i veze ka spoljnjim korisnicima. Ekstranet podrazumeva povezivanje onih organizacija koje uživaju međusobno poverenje a nisu u istim mrežama.

4.2 – Demilitarizovana zona (DMZ)

- Predstavlja **oblast** u kojoj se smešta javni server radi pristupa onih osoba koje ne uživaju puno poverenje.
- Izoliranjem servera u okviru DMZ prikriva se ili se sprečava pristup do ostatka mreže.
- Serveru se i dalje može prići sa lokalne mreže, ali vanjski korisnici neće moći da koriste ostale mrežne resurse.
- Zona se kreira pomoću ***firewall***-a, koji potpuno izolira ostatak mreže.



4.3 – Nove tehnologije

Virtuelna privatna mreža (*virtual local area network* - VLAN) omogućava formiranje grupe korisnika i računarskih sistema i njihovo grupisanje u okviru segmenta na mreži. Podela mreže na segmente omogućava njihovo međusobno prikrivanje, čime se osigurava i kontrola pristupa. **VLAN** se može podesiti da kontroliše put podataka od jedne tačke do druge. On predstavlja dobar način za zadržavanje mrežnog prometa u okviru određenog dela mreže.

Network Address Translation (NAT) pruža zasebnu mogućnost za poboljšanje zaštite mreže. Povećanje broja upotrebljivih Internet adresa je osnovna namena NAT-a. Pomoću njega organizacija može povezati sve računare na Internet preko jedne jedine javne IP adrese.

Tuneliranje podrazumeva kreiranje namenske virtuelne veze između dva sistema ili mreže. Tunel između dve tačke kreira se (enkapsulacijom) podataka u zaseban protokol prenosa koji je ugovoren između dve strane. U većini implementacija podaci koji prolaze kroz tunel izgledaju kao da potiču sa drugog dela mreže. Protokoli tuneliranja obično osiguravaju i zaštitu podataka i njihovo šifriranje.

4.4 – Poslovni proces

Utvrđivanje resursa - Svaka organizacija i poslovni proces imaju vredne resurse i aktivu, na koje se mora računati, kako u fizičkom, tako i u funkcionalnom smislu. *Utvrđivanje resursa* (*asset identification*) predstavlja proces u kome organizacija procenjuje vrednost podataka i sistema kojima raspolaže.

Procena rizika - Postoji nekoliko načina za procenu rizika (*risk assessment* ili *risk analysis*), od naučnih metoda, zasnovanih na formuli, do običnog razgovora s korisnicima. U principu, u proceni rizika treba identifikovati troškove zamene ukradenih podataka ili sistema, troškove usled nefunkcionisanja sistema i sve ostale moguće probleme.

Definisanje pretnji - Podrazumeva procenu rizika od internih i eksternih pretnji (engl. *threat*) kojima podaci i mreža mogu biti izloženi.

Proračun "ranjivosti„ - Zaštitne mogućnosti softvera i sistema koji se koriste u poslovanju će verovatno biti osnovna preokupacija specijaliste u oblasti računarske zaštite. Veliki broj operativnih sistema je u bliskoj prošlosti pitanjima zaštite poklanjalo samo deklarativnu pažnju

5 - Upravljanje rizikom

- Nemoguće u potpunosti ukloniti rizik pa je razvijena je metodologija upravljanja rizikom koja se sastoji od tri koraka:

1. **Analiza rizika** je sistematična identifikacija izvora rizika i procena moguće štete i obuhvata identifikaciju i evidentiranje svih resursa organizacije. Za svaki od resursa potrebno je identifikovati slabosti kao i pretnje koje mogu iskoristiti otkrivene slabosti.
2. **Proračun rizika** je proces poređenja procenjenog rizika sa zadanim kriterijumom rizika. Kriterijum je skalar koji određuje važnost rizika u odnosu na postavljene prioritete koji mogu da budu finansijskog, pravnog ili društvenog karaktera. Postoji više načina proračuna rizika, ali se najčešće koristi očekivani godišnji gubitak (**ALE** - ***Annualized Loss Expectancy***) za svaki od potencijalnih slučajeva gubitka.

$$\mathbf{ALE = AV \times EF \times ARO}$$

- **AV** (***asset value***) - vrednost imovine koja je izložena riziku.
- **EF** (***Exposure Factor***) - faktor izloženosti
- **ARO** (***Annual Rate of Occurrence***) - godišnja učestalost događanja

5 - Upravljanje rizikom

3. Tretman rizika je izbor i provera mera za promenu rizika.

- Odluka o izboru neke od prikazanih mera se donosi na osnovu proračuna posledica rizika i proračuna odnosa troškova tretmana rizika i troškova realizacije rizika.

a) Izbjegavanje rizika je odluka da se ne uključi u neku radnju ili da se povuče iz neke situacije, ako se proceni da su povezane sa određenim, prevelikim rizikom.

b) Prihvatanje rizika je odluka da se ne poduzimaju nikakve mere smanjenja rizika.

c) Prenos rizika je prenos tereta rizika na druga lica putem osiguranja ili sličnog ugovora.

d) Optimizacija rizika je postupak minimiziranja negativnih i maksimizacije pozitivnih posledica. Optimizacija je jedini postupak koji se bavi smanjenjem posledica rizika primenom različitih mera

- Vrednost neke od mera zaštite može se izračunati na sledeći način:

Vrednost mere zaštite = ALE (bez mere) − Trošak (provođenja mere) − ALE (sa merom)

Hvala na pažnji !!!

Pitanja

? ? ?