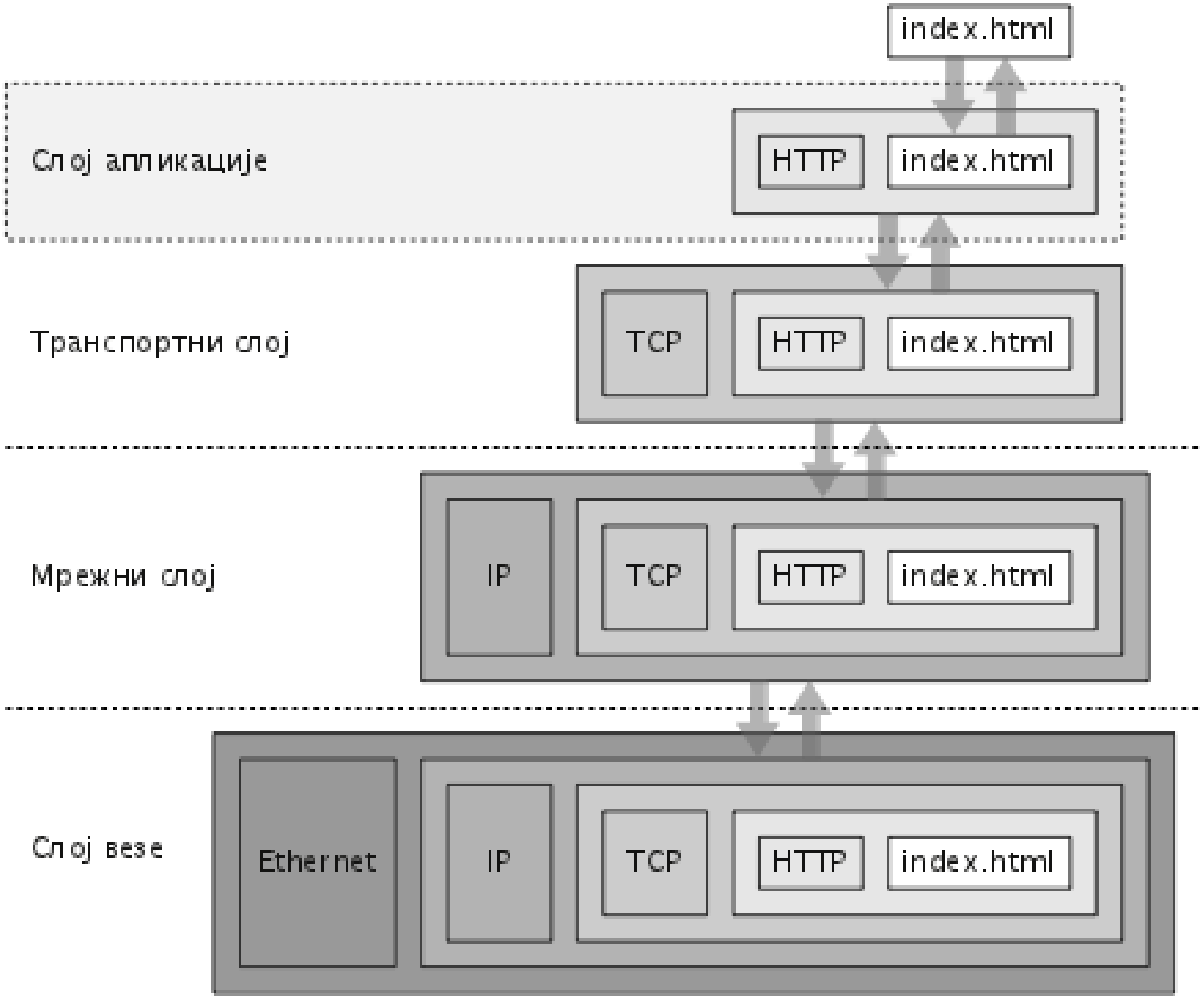
XII – Aplikacioni sloj

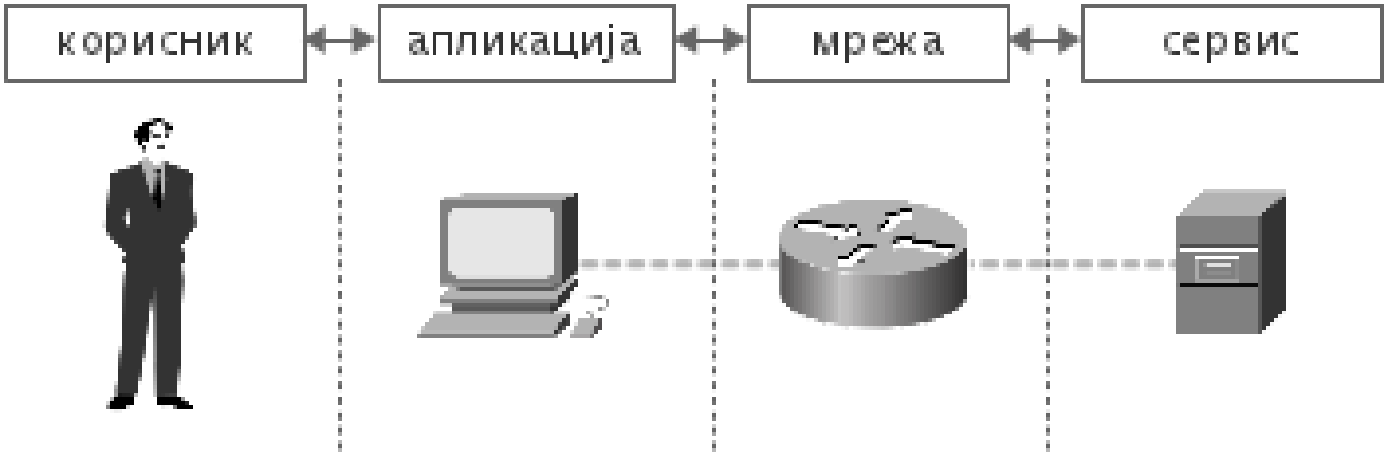
- Povećanjem broja korisnika Interneta povećavali su se i zahtevi za različitim aplikacijama koje su pratile sve složenije zahteve korisnika.
- Jedan od načina na koji se aplikacije, koje se danas koriste, mogu kategorizovati je na **tradicionalne** aplikacije i na **savremene** aplikacije
- TCP/IP je projektovan pre OSI modela i zato njegovi slojevi nisu u potpunosti usklađeni sa slojevima koje predviđa OSI.
- TCP/IP ima pet nivoa: niža četiri se uklapaju u niža četiri sloja OSI
- Peti, aplikacioni sloj TCP/IP-a ekvivalentan je kombinaciji prezentacionog, sloja sesije i aplikacionog sloja OSI modela.
- Slojevi ispod aplikacionog obezbeđuju pouzdani prenos podataka.
- Osim mogućnosti komuniciranja, oni ne pružaju neki drugi servis koji je od direktne koristi krajnjem korisniku.
- Tek na najvišem aplikacionom sloju nalazimo realne mrežne aplikacije.
- Na ovom nivou takođe postoji potreba za protokolima koji će omogućiti aplikacijama da ispravno funkcionišu.

XII – Aplikacioni sloj



XII – Aplikacioni sloj

- Osnovni tipovi softvera na ovom sloju su korisničke aplikacije i servisi
- Aplikacije predstavljaju oblik realizacije softvera namenjen za neposredno korišćenje od strane korisnika
- Aplikacije poseduju odgovarajući (grafički, alfanumerički ili neki drugi) korisnički interfejs



- Servisi predstavljaju softverske procese koji se izvršavaju „u pozadini“ računarskog sistema i ne poseduju neki korisnički interfejs
- Uloga servisa je da daju podršku ostalim softverskim procesima na lokalnom ili udaljenim računarima kako bi došli do nekih podataka.
- Na primer, Web servis podrazumeva postojanje korisničke aplikacije (Web pregledača) i serverskog softvera (Web server)

XII – Aplikacioni sloj

Tradicionalne aplikacije

- **DNS** (*Domain Name System)* - usluga koja omogućava povezivanje imena stanice na Internetu i njegove numeričke IP adrese.
- **Telnet** - pruža servis logovanja na daljinu, koji omogućava korisniku na terminalu ili personalnom računaru da se loguje i koristi udaljeni računar na isti način kao da je direktno povezan sa tim računarom,
- **FTP** (*File Transfer Protocol)* - koristi se za slanje datoteka (fajlova) sa jednog na drugi računar. Datoteke mogu biti binarnog ili tekstualnog tipa.
- **SMTP** (*Simple Mail Transfer Protocol)* - obezbeđuje razmenu elektronskih pisama, tj. omogućava mehanizam za razmenu poruka između različitih korisnika.

XII – Aplikacioni sloj

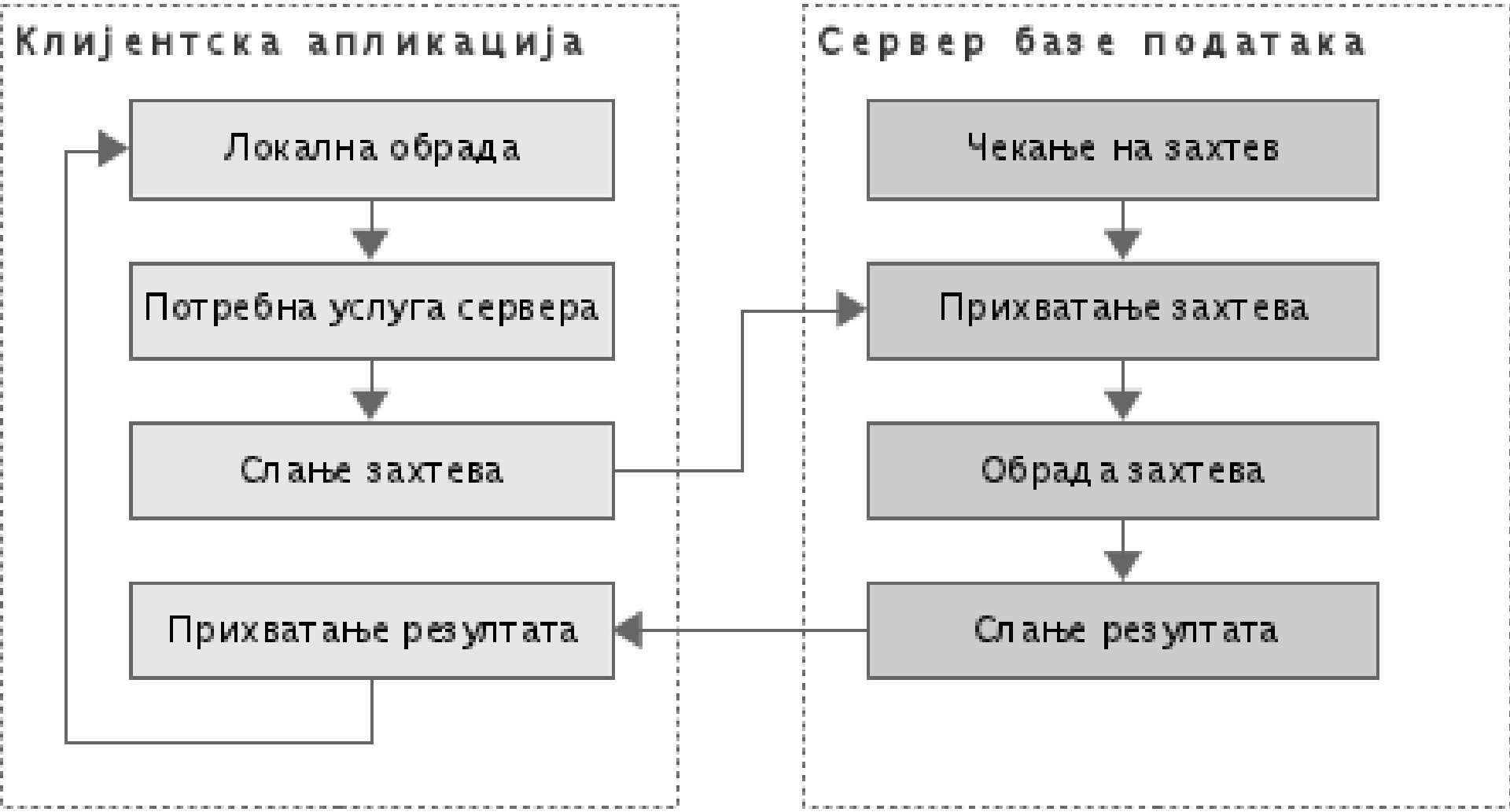
Savremene aplikacije

- **HTTP** (*Hypertext Transfer Protocol)* - protokol koji podržava razmenu zahteva i odgovora između WEB pretraživača i WEB servera.
- Protokoli za prenos aplikacija u realnom vremenu: **SIP** (*Session Initiation Protocol)* i **H323** - vode računa o uspostavljanju, modifikovanju i raskidanju veza aplikacija koje rade u realnom vremenu kao što je telefonija ili video, a koriste IP protokol.
  1. **H323** je serija standarda organizacije ITU-T koja se odnosi na povezivanje javnih telefonskih mreža preko Interneta (**VoIP**).
  2. **SIP** predstavlja jednostavniji protokol od H323 za prenos govora preko Interneta. Usvojila ga je organizacija IETF a opisan je u dokumentu RFC3261
- Protokol za upravljanje računarskim mrežama **SNMP** (*Simple Network Management Protocol)* - SNMP sistem za upravljanje mrežom predstavlja kolekciju alata za nadgledanje i upravljanje mrežom.

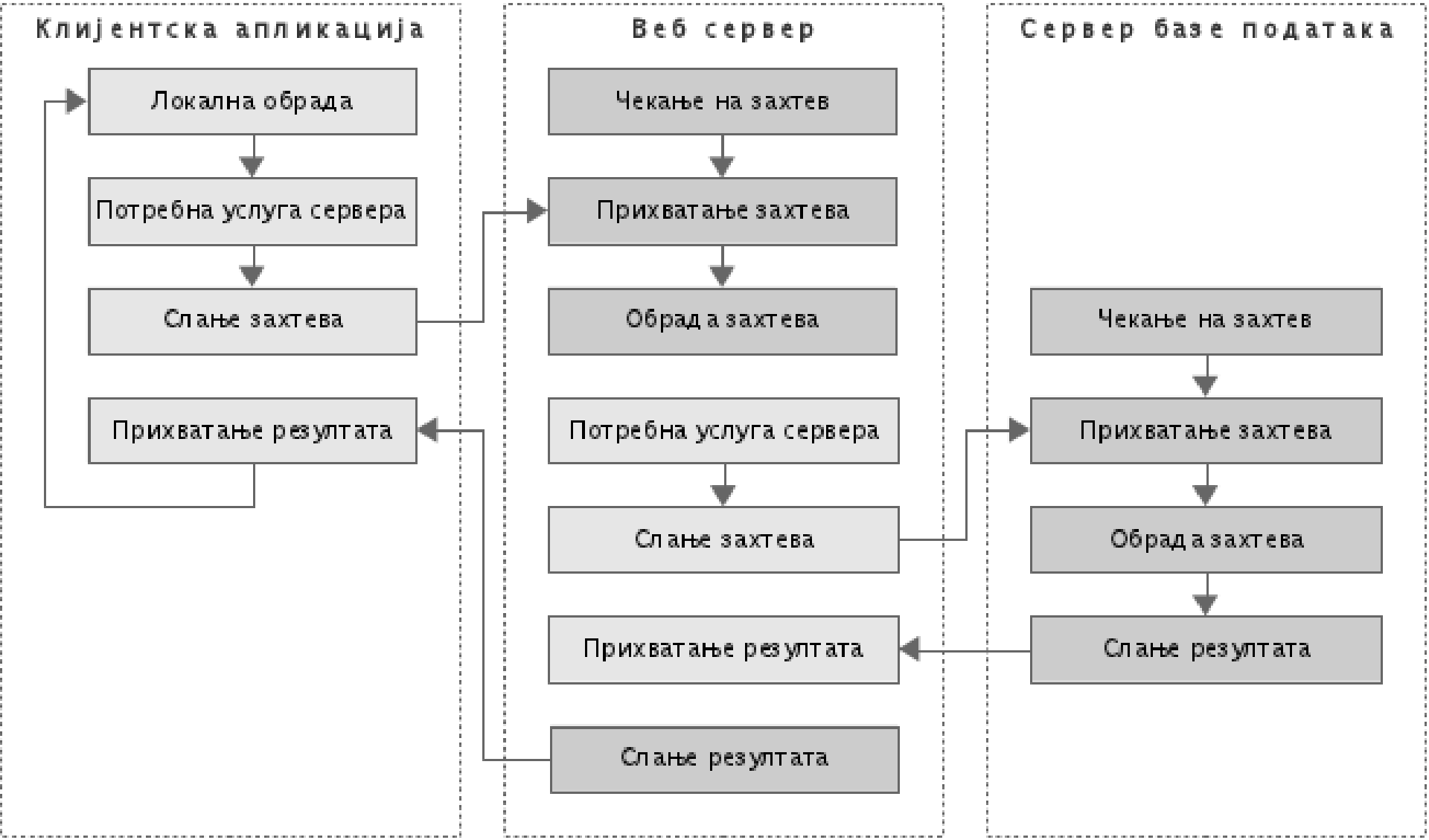
XII – Klijent server model

- Za korišćenje Internet servisa neophodni su aplikacioni programi koji se izvršavaju na dva krajnja računara i međusobno komuniciraju.
- Aplikacioni programi koji koriste Internet zasnovani su na obliku distribuiranog procesiranja koji se zove ***klijent-server model***.
- Jedan aplikacioni program **klijent-**koji se izvršava na lokalnoj mašini, traži uslugu od drugog programa **server-**izvršava se na udaljenoj mašini
- Server nudi usluge mnogim klijentima, a ne samo jednom klijentu.
- Klijent server model odgovara relaciji tipa: ″**više-prema-jedan**″: više klijenata može koristiti servise jednog servera.
- Klijentski program se izvršava samo kada je usluga servera potrebna.
- Sa druge strane, serverski program, koji pruža uslugu, radi sve vreme, zato što unapred ne zna kada će neki klijent zatražiti uslugu.
- Klijentski program je **konačan** jer se pokreće od strane korisnika ili nekog aplikacionog programa, kada je usluga potrebna a završava se kada je tražena usluga dobijena.
- Serverski program je **beskonačan** (nikada se ne završava), i nikada ne pokreće servis a da on nije zatražen,već kada zahtev stigne,on odgovara

XII - Klijent server model



XII - Klijent server model



XII - TELNET

- Glavni zadatak Interneta i TCP/IP-ja je da obezbede mrežne servise
- Bilo bi dobro da korisnici mogu da izvršavaju različite aplikacione programe na udaljenim računarima,a da rezulte prenesu na svoj računar
- Jedan od načina kako se može ostvariti ovaj zahtev jeste da se kreira posebna klijent-server aplikacija za svaki od potrebnih servisa
- Programi koji podržavaju FTP, E-mail,..., su primeri ovakvog pristupa
- Nemoguće je napisati aplikacioni program za svaku iskazanu potrebu.
- Rešenje: klijent-server program opšte namene, koji će omogućiti da se pristupi bilo kom aplikacionom programu na udaljenom računaru.
- Omogućava korisniku da se prijavi za rad (*login*), na udaljeni računar
- Nakon prijavljivanja, korisnik može da koristi servise dostupne na udaljenom računaru i prenese rezultate nazad na svoj računar.
- **TELNET** je upravo takav klijent-server program.
- TELENT omogućava uspostavljanje konekcije sa udaljenim sistemom na način da se lokalni terminal ponaša kao da je terminal tog udaljenog sistema, tj. da korisnik radi kao da se nalazi na udaljenom računaru.

XII – Koncept rada TELNET-a

1.<u>Sistemi sa raspodelom vremena</u> **-** razvijen je kada su većina OS (UNIX), podržavali koncept raspodele vremena koji je omogućavao da više korisnika koristi jedan veliki računar. Interakcija između korisnika i računara ostvaruje se putem terminala (kombinacija tasture, monitora i eventualno miša). Celokupna obrada se obavlja na centralnom računaru, a terminali se koriste za unos i prikaz podataka. OS sa raspodelom vremena kreiraju iluziju da svaki korisnik radi na izdvojenom, namenskom računaru. Korisnik može da pokrene program, pristupa sistemskim resursima, prelazi iz jednog u drugi program i slično.

2.<u>Lokalni Login</u> **-** svaki autorizovani korisnik poseduje prava pristupa sistemskim resursima i svoju identifikaciju (u vidu korisničkog imena) i lozinku. Da bi pristupio sistemu, korisnik daje svoje korisničko ime i lozinku. Kada se prijavi za rad na lokalnom sistemu sa raspodelom vremena (putem korisničkog imena i lozinke) kaže se da je korisnik izvršio **lokalni login.** Kako korisnik kuca na tastaturi terminala, svaki pritisak na dirku se prenosi *drajveru terminala*. Drajver terminala prenosi zadate karaktere OS, koji poziva odgovarajući program**.**

XII – Koncept rada TELNET-a

3. Udaljeni login - kada korisnik pristupa programu lociranom na udaljenom računaru, on obavlja **udaljeni login** (*remote login*). TELNET je posrednik u ovoj interakciji. Klijentska strana TELNET aplikacije izvršava se na strani korisnika, a serverska na strani udaljenog računara. Pritisak na dirku sa tastature lokalnog terminala prenosi se ka terminal drajveru, od koga OS preuzima karaktere, ali ih ne interpretira, već ih šalje TELNET klijentu. TELNET klijent prevodi karaktere (ASCII, EBCDIC ili neki drugi kod) u univerzalni karakter kod (**NVT** - *Network Virtual Terminal chracters*) i isporučuje ih lokalnom TCP/IP steku. Komande ili tekst, u NVT obliku, prenose se kroz Internet i stižu do TCP/IP steka udaljenog računara, koji ih daje OS, a on TELNET serveru, gde se karakteri konvertuju iz NVT formata u oblik razumljiv udaljenom računaru. Kako OS nije projektovan da karaktere dobija direktno od TELNET servera već od lokalnog terminala (putem terminal drajvera) projektovan je specifičan program, ***pseudoterminal drajver***, koji se prema OS ponaša kao terminal drajver, ali sa suprotne strane, karaktere ne očekuje od lokalnog terminala već od TELNET servera.

XII – Network Virtual Terminal

- Različiti računari i OS koriste različita kodiranja karaktera i prepoznaju različite specijalne kombinacije karaktera - heterogeni sistemi
- DOS-a za kraj fajla koristi kombinacija **CTRL+Z**, a UNIX **CTRL+D**.
- TELNET rešava problem heterogenosti uvođenjem univerzalnog skupa karaktera, **NVT** (***Network Virtual Terminal*** - mrežni virtuelni terminal)
- TELNET klijent prevodi lokalni skup karakter u NVT oblik, a server iz NVT u skup odgovarajućih karaktera udaljenog računara.
- Omogućena je interakcija raznorodnih računara i operativnih sistema.
- Kod OSI modela, konverzija podataka je zadatak prezentacionog sloja.
- Kod TCP/IP, funkcije prezentacionog sloja su pridružene aplikacionom
- NVT sadrži dva skupa 8-bitnih karaktera, jedan za podatke, a drugi za kontrolne (upravljačke) informacije.
- Najviši bit karaktera za podatke ima vrednost 0, dok kod kontrolnih karaktera ima vrednost 1.
- Nižih 7 bitova karaktera za podatke je isti kao kod ASCII kôda.

XII – Network Virtual Terminal

Ugrađivanje **-** TELNET koristi samo jednu TCP konekciju. Server koristi dobro-poznati **port 23**, dok se za klijente koriste dinamički portovi. Ista konekcija se koristi kako za slanje podataka tako i za slanje kontrolnih karaktera. To se postiže ugradnjom kontrolnih karaktera u tok podataka. Da bi se napravila razlika između podataka i kontrolnih karaktera, svaka sekvenca kontrolnih karaktera počinje specijalnim kontrolnim karakterom koji se označava skraćenicom **IAC** (*Interpret As Control* - interpretiraj kao kontrolu).

Primer: zamislimo da korisnik traži od servera da prikaže sadržaj fajla *file1*. Korisnik unosi komandu: *cat file1*. Međutim, umesto da unese *file1*, korisnik je pogrešio u kucanju i uneo *filea1*. Da bi ispravio grešku, korisnik koristi taster *backspace*, tako da je niz unetih karaktera: ***cat filea <backspace>1***. Međutim, kod prvobitnih implementacija TELNET-a, lokalno editovanje nije moguće, već se radi na udaljenom serveru. Karakter *backspace* se prevodi u dva karaktera (**IAC EC**) i ugrađuje u tok podataka koji se šalje serveru.

XII – File Transfer Protocol

- Protokol za prenos fajlova je aplikacioni protokol za kopiranje fajlova.
- Prenos fajlova između hostova je jedan od najčešćih zadataka koji se očekuje od bilo kog mrežnog okruženja.
- Postoje problemi koji se moraju rešiti kako bi prenos bio omogućen.

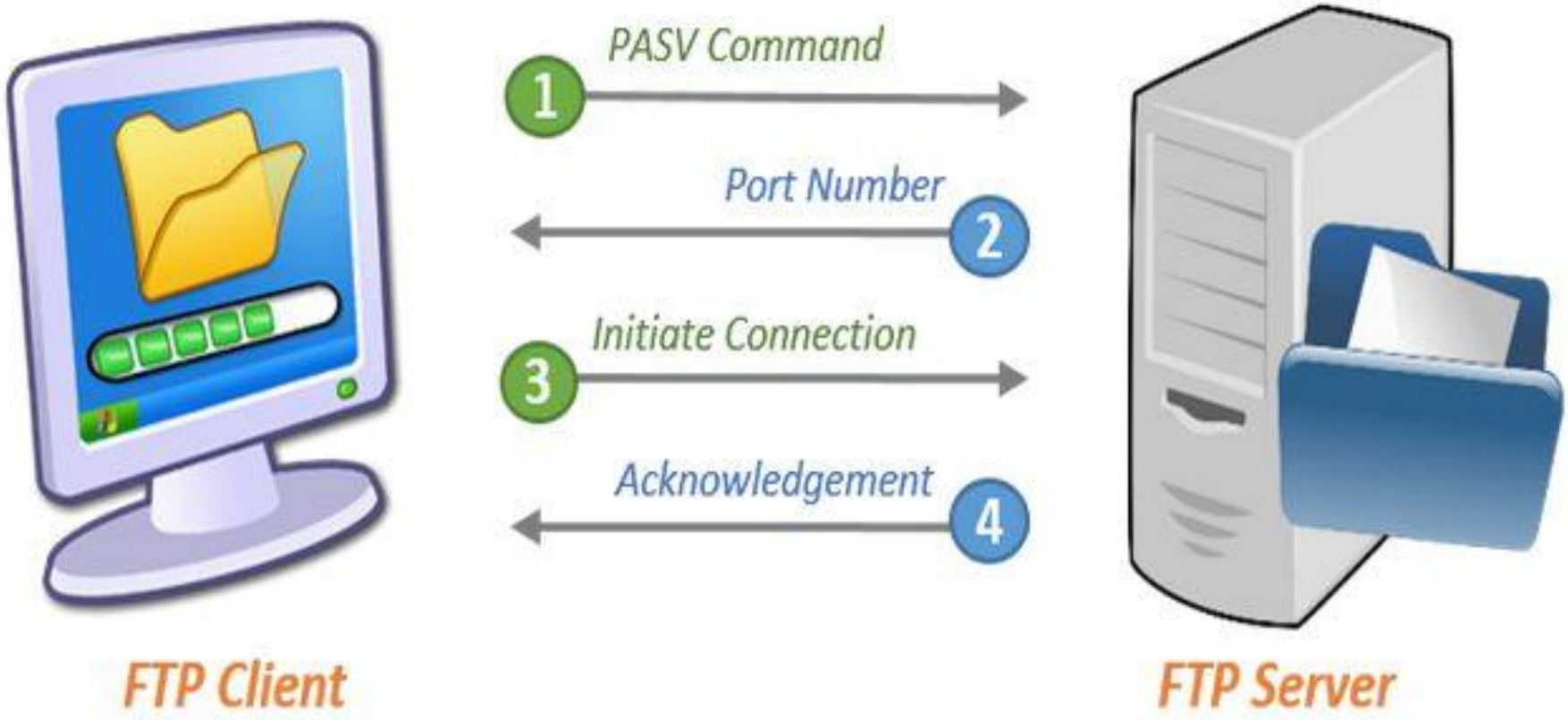
Primer: dva sistema mogu koristiti različite konvencije za imenovanje fajlova, načine za predstavljanje teksta i drugih tipova podataka, ili podržavati različite strukture direktorijuma.

- FTP se razlikuje od drugih klijent-server aplikacija po tome što ne uspostavlja samo jednu već **2** TCP konekcije između klijenta i servera
- Jedna konekcija se koristi za prenos podataka, a druga za prenos upravljačkih informacija (komande i odzivi).
- FTP klijent sadrži tri komponente: **korisnički interfejs**, **proces za upravljanje klijentom** i **proces za prenos podataka**.
- Server ima dve komponente: **proces za upravljanje serverom** i **proces za prenos podataka**.
- Upravljačka konekcija se uspostavlja između upravljačkih, a konekcija za prenos podataka između procesa zaduženih za prenos podataka

XII – File Transfer Protocol

- Upravljačka konekcija ostaje aktivna za sve vreme trajanja jedne FTP sesije tj. dok se ona ne zatvori
- Konekcija za prenos podataka se otvara, a onda i zatvara za prenos svakog pojedinačnog fajla.
- Upravljačka konekcija se uspostavlja kada korisnik otvori FTP sesiju.
- Dok je upravljačka konekcija otvorena, konekcija za prenos podataka može biti otvarana i zatvarana više puta, ako se prenosi više fajlova.
- Upravljačka konekcija koristi jednostavna pravila komunikacije: klijent šalje komandu, a server vraća odziv.
- Konekcija za prenos podataka zahteva složenija pravila komunikacije, obzirom na brojne tipove fajlova i specifične načine prenosa podataka.
- FTP koristi TCP protokol za slanje podataka tj. fajlova.
- Upravljačka konekcija se ostvaruje preko porta **21**, a konekcija za prenos podataka preko porta **20**.

XII - File Transfer Protocol



XII – File Transport Protocol

Upravljačka konekcija -Upravljačka konekcija se uspostavlja na isti način kao i kod drugih standardnih mrežnih aplikacionih programa, kao što je npr. TELNET. Konekcija se uspostavlja u dva koraka:

1. Server izvršava pasivno otvaranje dobro-poznatog porta **21** i čeka da se klijent javi tj. čeka da primi zahtev klijenta.
2. Klijent otvara dinamički izabran port i inicira aktivno otvaranje konekcije sa serverom.

➢Konekcija ostaje otvorena za sve vreme trajanja FTP sesije.

Konekcija za prenos podataka - konekcija za prenos podataka na strani servera koristi dobro-poznati port **20**. Međutim, kreiranje konekcije se razlikuje u odnosu na standardnu proceduru jer su potrebna tri koraka:

1. Klijent, a ne server, izvršava pasivno otvaranje dinamičkog porta.
2. Klijent šalje broj dinamičkog porta serveru, korišćenjem komande PORT (prenosi se preko upravljačke konekcije).
3. Server prima broj porta i izvršava aktivno otvaranje konekcije sa klijentom koristeći dobro-poznati port **20** za sebe i primljeni dinamički broj porta za klijenta.

XII – File Transport Protocol

1. Komunikacija preko upravljačke konekcije

- Za komunikaciju preko upravljačke konekcije kod FTP-a se koristi, kao i kod TELENT-a ili SMTP-a, **NVT** ASCII skup karaktera.
- Komunikacija se stvaruje putem komandi i odziva.
- Ovakav način komunikacije (polu dupleks) je pogodan za upravljačku konekciju zato što se preko konekcije, u bilo kom trenutku, prenosi najviše jedna komanda (ili odziv).
- Komande i odzivi su kratke linije teksta,tako da nema potrebe brinuti o različitim tipovima fajlova ili strukturama fajlova na klijentu i serveru.

2. Komunikacija preko konekcije za podatke

- Konekcija za podatke ima različitu namenu i ostvaruje se na drugačiji način u odnosu na komunikaciju preko upravljačke konekcije.
- Preko konekcije za podatke se prenose fajlovi.
- Za svaki fajl koji želi da prenese, klijent mora definisati tri atributa:
    1. tip fajla,
    2. strukturu podataka
    3. način prenosa.

XII – File Transport Protocol

Tip fajla: mogu se prenositi sledeći tipovi fajlova:

- ✓ ***ASCII***. Ovo je podrazumevani format prenosa tekstualnih fajlova.
- ✓ ***EBCDIC***. tekstualni fajl se može prenositi korišćenjem EBCDIC koda.
- ✓ ***Image***. Ovo je podrazumevani format za prenos binarnih fajlova. Fajl se prenosi kao kontinualni tok bitova bez bilo kakve interpretacije ili kodiranja. Uglavnom se koristi za prenos izvršnih programa.

Struktura podataka: koristi jednu od tri interpretacije strukture podatka

1. ***File*** (podrazumevana opcija). Fajl sadrži kontinualni tok bajtova.
2. ***Record*** - fajl je podeljen na zapise. Moguće samo kod tekstualnih fajlova, tabela ili baza podataka.
3. ***Page*** - fajl je podeljen na stranice. Svaka stranica ima broj i zaglavlje. Stranicama se može pristupati bilo sekvencijalno bilo proizvoljno.

XII – File Transport Protocol

Način prenosa: tri načina prenosa fajlova preko konekcije za podatke:

1. ***Stream**:* podrazumevani način prenosa. FTP isporučuje TCP-ju podatke u vidu kontinualnog toka podataka. TCP je odgovoran za podelu podataka na segmente odgovarajuće veličine. Ako su podaci koji se prenose prosti tok bajtova (struktura tipa *File structure*), marker za kraj fajla (**EOF**-*End-Of-File*) nije potreban. U ovom slučaju, kraj fajla podudara se sa zatvaranjem konekcije od strane predajnika. Ako su podaci podeljeni na zapise (struktura tipa *Record structure*), svakom zapisu se pridodaje jedno-bajtni specijalni karakter *end-of-record* (**EOR**), dok se kraj celokupnog fajla označava karakterom **EOF**.
2. ***Block**:* FTP može isporučivati TCP-ju podatke i u blokovima. U ovom slučaju, svakom bloku prethodi 3-bajtno zaglavlje. Prvi bajt je bajt za opis bloka (*block descriptor*), dok sledeća dva bajta definišu veličinu bloka u bajtovima.
3. ***Compressed**:* ako je fajl isuviše veliki, podaci su mogu komprimovati, kako bi se smanjila količina podataka koju treba preneti preko mreže.

Simple Network Management Protocol

- **Jednostavni protokol za upravljanje mrežom** (SNMP) je projektovan da bi obezbedio jednostavan metod za centralizovanje upravljanja TCP/IP mrežama. Osnovni ciljevi SNMP protokola su:
  - ✓ Održavanje niskih troškova razvoja da bi se smanjilo opterećenje zaposlenih koji se bave mrežom
  - ✓ Obezbeđivanje daljinskog upravljanja uređajima
  - ✓ Nezavisnost protokola od osnovne arhitekture mreže
  - ✓ Jednostavnost
- Dva glavna učesnika u SNMP-u su menađer i agent.
- Menađer je obično softverski program koji radi na radnoj stanici ili nekom većem računaru i komunicira sa agentskim procesima koji se izvršavaju na svakom kontrolisanom računaru.
- Aplikacije koje su projektovane kao menađerska strana SNMP softvera razlikuju se po ceni i funkcionalnosti.
- One mogu da : kontrolišu mrežni saobraćaj, izrađuju mapu topologije mreže, uočavaju izabrane događaje i alarmiranje korisnika, daju izveštaje o kontrolisanim promenljivima.

XII – Sistem imena domena (DNS)

- Bez obzira što se stanice na mreži prepoznaju po svojim IP adresama korisnicima je lakše da koriste ime računara (hosta) umesto IP adrese
- U TCP/IP okruženju DNS predstavlja distribuiranu bazu podataka koja obezbeđuje vezu (mapiranje) između IP adrese i imena računara.
- Svaka od aplikacija može da pristupi standardnoj bazi podataka.
- Zadatak distribuirane baze je da izvrši povezivanje imena računara i njihovih IP adresa i da obezbedi podatke potrebne pojedinim servisima
- Svaki domen održava sopstvenu bazu podataka na svom serveru kome drugi sistemi (klijenti) preko Interneta mogu da pristupe.
- Sistem imena domena (DNS) obezbeđuje protokole koji omogućavaju klijentima i serverima da međusobno komuniciraju.
- Na početku za razrešavanje imena računara u IP adresu koristio se *hosts* fajl - tekstualni fajl u kome su se nalazila povezivanja (mapiranja) između imena računara i njegove IP adrese (/etc/hosts, na Linux,UNIX, i \%SystemRoot%\System32\Drivers\Etc na Win OS
- Svi računari na Internetu morali su sa centralnog mesta da prenesu i koriste *hosts* fajl. *Hosts* fajl je centralizovana „ravna” baza.

XII – Prostor imena

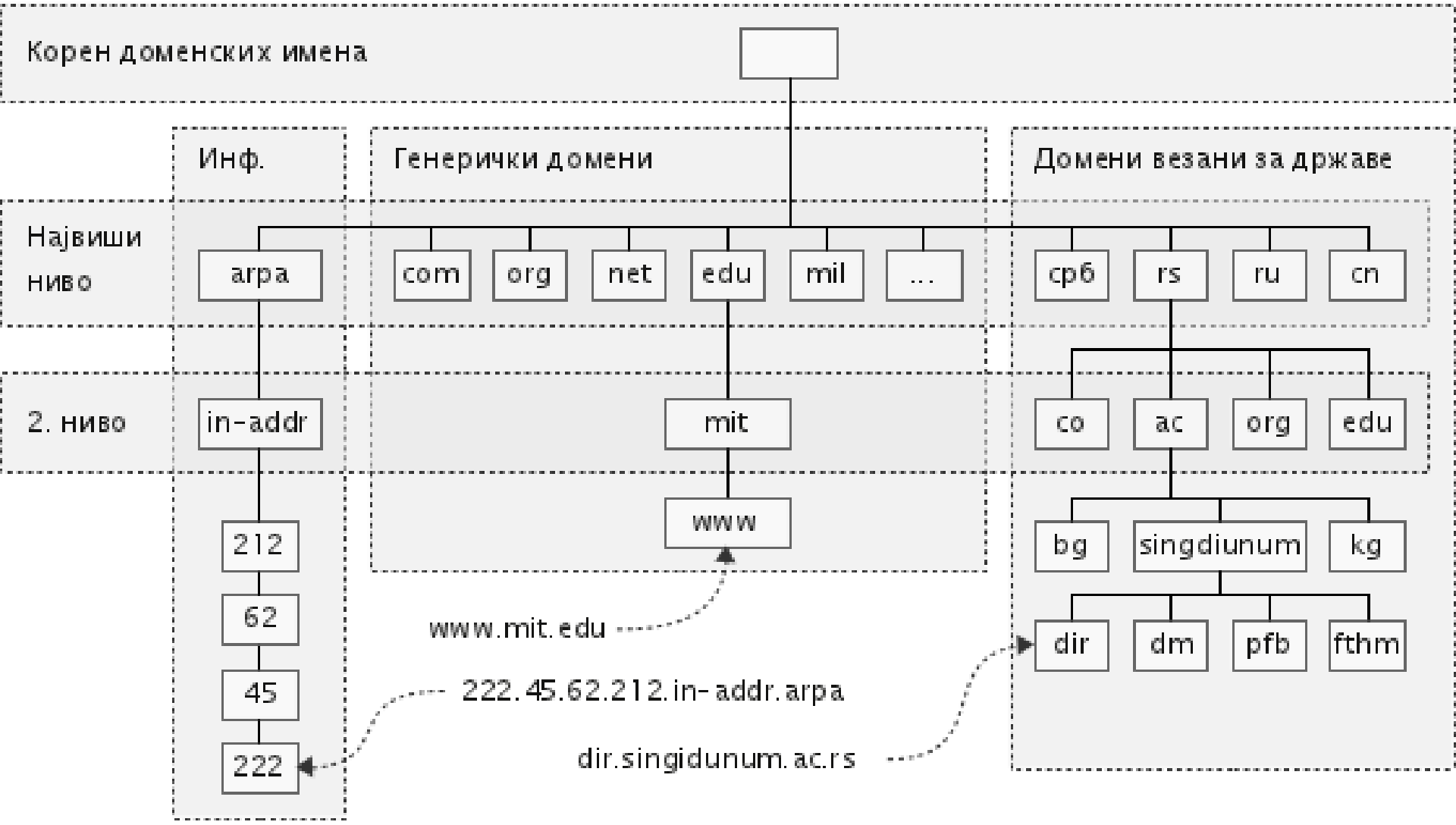
- Prostor imena domena je hijerarhijska struktura.
- Svaki čvor ima oznaku (labelu).
- U stablu čvor može biti jedinstveno identifikovan na osnovu svog potpuno kvalifikovanog imena **FQDN**-*Fully Qualified Domain Name*
- Oznaka može da ima najviše 63 karaktera.
- Koren stabla je specijalan čvor bez oznake.
- Ime domena svakog čvora stabla je skup oznaka koje počinju od tog čvora idući ka korenu, sa tačkom koja razdvaja oznake.

- Domeni na nivou vrha (*Top level domains)* podeljeni su u 3 kategorije:

1. *arpa* je specijalan domen koji se koristi za povezivanje adrese i imena
2. sedam domena označenih sa tri karaktera nazivaju se generički ili organizacijski domeni,
3. domeni označeni sa dva karaktera nazivaju se domeni država ili geografski domeni.

Domen	**Opis**
com	Komercijalna organizacija
edu	Obrazovna institucija
gov	Vladine organizacije
int	Međunarodne organizacije
mil	Vojne organizacije
net	Mreže
org	Druge organizacije

XII - Karakteristike prostora imena



XII – Karakteristike prostora imena

- Nijedna od celina nije zadužena za sve oznake u stablu.
- Umesto toga jedna celina vodi računa o delu stabla (domenima na nivou vrha) i delegira odgovornost drugima za određenu zonu.
- Zona je deo DNS drveta koji se administrira nezavisno.
- Jednom kada se dodeli (*Delegated*) nadležnost (*Authority)* stvar je administratora zone da obezbedi server imena za tu zonu.
- Kada se novi sistem instalira u određenoj zoni DNS, administrator te zone dodeljuje mu ime i IP adresu i ubacuje te podatke u bazu podataka
- Za server imena kaže se da je nadležan za jednu ili više zona.
- Osoba koja je zadužena za zonu mora da obezbedi primarni server imena za tu zonu i jedan ili više sekundarnih servera imena.
- Primarni i sekundarni serveri moraju da budu međusobno nezavisni i redundantni,tako da servis nije ugrožen ako je jedan od sistema u kvaru
- Razlika primarnog i sekundarnog servera imena je u tome što primarni skuplja i skladišti informacije a sekundarni ih dobija od primarnog.
- Prebacivanje informacija od primarnog servera ka sekundarnom serveru naziva se prenos zone (*Zone transfer)*.

XII – Karakteristike prostora imena

Šta radi server kada nema informacije koje se od njega traže?

- On mora da potraži informacije od drugog servera imena.
- Ovo je primer distribuiranosti DNS-a.
- Svaki server imena ne mora da zna kako da stupi u vezu sa svim ostalim serverima imena.
- Umesto toga svaki server imena mora da zna kako da stupi u vezu sa serverom imena korena stabla (*Root name servers*).
- Od 1993. godine postoji osam servera imena korena stabla i primarni serveri imena moraju da znaju IP adrese svakog od njih.

Primer: Klijent šalje upit o ***www.ministarstvo.gov*** lokalnom serveru U iterativnom upitu server imena kome je upit upućen vraća najbolji mogući odgovor. To može da bude razrešeno ime ili referenca na drugi server imena, koji može da odgovori na originalan klijentov zahtev.

XII – Karakteristike prostora imena

1. Pretraživač šalje rekurzivni DNS upit ka svom lokalnom DNS serveru tražeći IP adresu za ***www.ministarstvo.gov***. Lokalni server imena odgovoran je samo za razrešavanje imena u svom domenu.
2. Lokalni server imena proverava svoje zone i ne pronalazi zonu koja odgovara traženom imenu pa šalje iterativni upit ka korenom (**.**) serveru
3. Koreni server imena nadležan je za koreni domen i odgovoriće IP adresom servera imena za vrh ***.gov*** domena.
4. Lokalni server imena šalje iterativni upit za ***www.ministarstvo.gov*** ka serveru imena za ***.gov*** domen.
5. ***.gov*** server imena odgovara IP adresom servera imena koji opslužuje domen ***ministarstvo.gov***.
6. Lokalni server imena šalje iterativni upit za ***www.ministarstvo.gov*** ka serveru imena odgovornom za domen ***ministarstvo.gov***.
7. Server imena za domen ***ministarstvo.gov***. odgovara sa IP adresom koja odgovara računaru ***www.ministarstvo.gov***.
8. Lokalni server imena šalje IP adresu stanice (računara) ***www.ministarstvo.gov*** natrag ka originalnom pretraživaču.

XII – Karakteristike prostora imena

Inverzni upiti

- Pretraživač šalje inverzni upit, zahtev serveru imena sa zadatkom da nađe (razreši) ime hosta za poznatu IP adresu.
- U DNS prostoru imena ne postoji veza između imena i IP adresa
- Samo pretraživanje svih domena garantovalo bi korektan odgovor.
- Da bi se ovo izbeglo napravljen je specijalan domen '***in-addr-arpa***'.

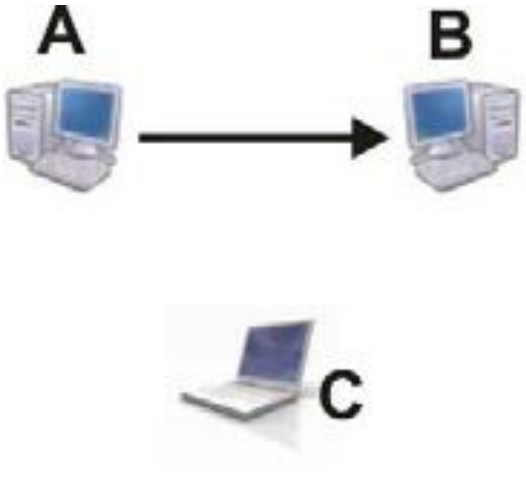
Pamćenje vremena trajanja

- Kada server imena obrađuje rekurzivni upit to može zahtevati slanje nekoliko upita dok se ne pronađe odgovor.
- Server imena pamti sve informacije (IP adrese) dobijene u tom procesu za jedno određeno vreme.
- Ovo vreme se naziva vreme trajanja i označava se TTL (***Time to Live***).
- Informacija o vremenu trajanja sadržana je u povratnim podacima.
- Kada DNS server zapamti podatke, zapamti i njihovo vreme trajanja (TTL) ali istovremeno mora da započne smanjivanje tog vremena da bi znao kada da te podatke izbriše iz svoje memorije.

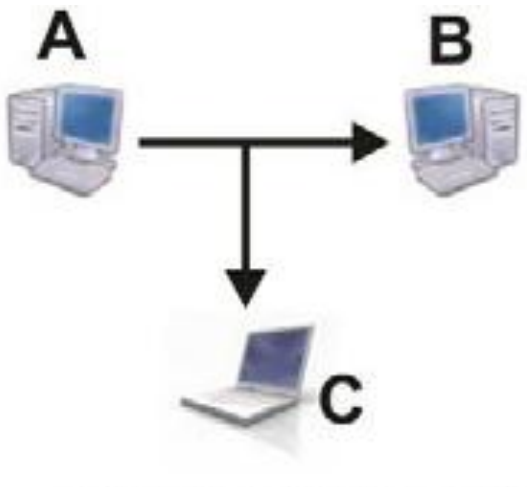
XII – Osnove mrežne bezbednosti

- Sve većom upotrebom računarskih i komunikacionih tehnologija za savremeno poslovanje, problem sigurnosti sve više dobija na značaju tako da se njemu mora posvetiti posebna pažnja.
- Samim tim javila se i potreba za novim i automatizovanim alatima za zaštitu datoteka i drugih informacija.
- Sigurnost neke informacije možemo da posmatramo kroz tri aspekta:
  1. ***napad na sigurnost*** *(security attack)* - bilo koja akcija koja ugrožava sigurnost informacija;
  2. ***sigurnosni mehanizam*** *(security mechanizam)* - mehanizam koji treba da detektuje i predupredi napad ili da sistem oporavi od napada;
  3. ***sigurnosna usluga*** *(security service)* - usluga koja povećava sigurnost sistema za obradu i prenos podataka, gde sigurnosna usluga podrazumeva primenu jednog ili više sigurnosnih mehanizama.
- Napadi predstavljaju akcije koje su usmerene na ugrožavanje sigurnosti informacija, računarskih sistema i mreža.
- Postoje različite vrste napada, mi ćemo ih kategorisati u 5 kategorija.

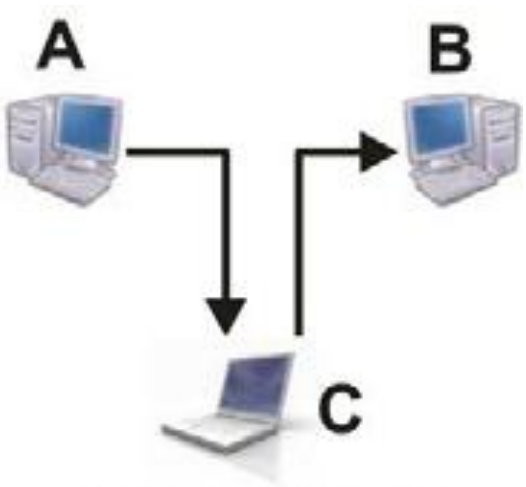
XII - Napadi i pretnje



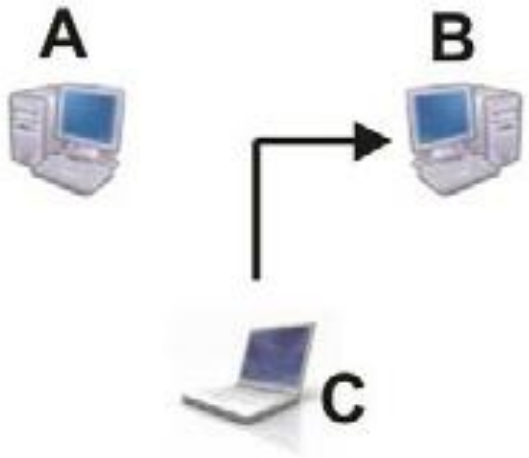
a) Normalan tok



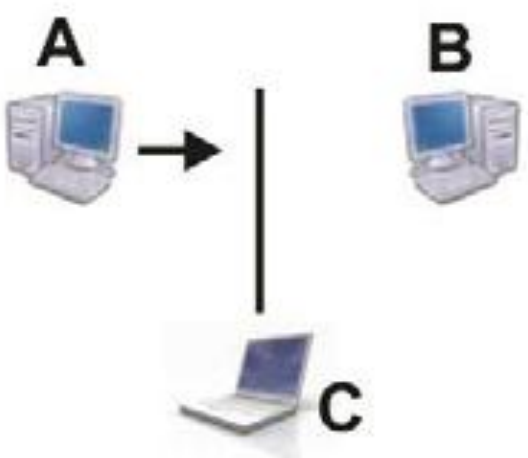
b) Prisluškivanje



c) Modifikacija



d) Uklanjanje informacija



e) Prekid toka

XII – Napadi i pretnje

b) Hvatanje ili Prisluškivanje (*interception*) - napad na poverljivost (*confidentialy*). Hvatanje u praksi predstavlja prisluškivanje sabraćaja, nadziranje njegovog intenziteta, uvid u osetljive informacije i slično.

c) Izmena (*modification*) - napad na integritet (*integrity*) jer je osnovni cilj neovlašćeno brisanje, umetanje ili izmena podataka. Iako menja podatke ili sistem, često ostaje neprimećen izvesno vreme, kako zbog nepažnje, tako i zbog složenih tehnika koje se pri ovom napadu koriste.

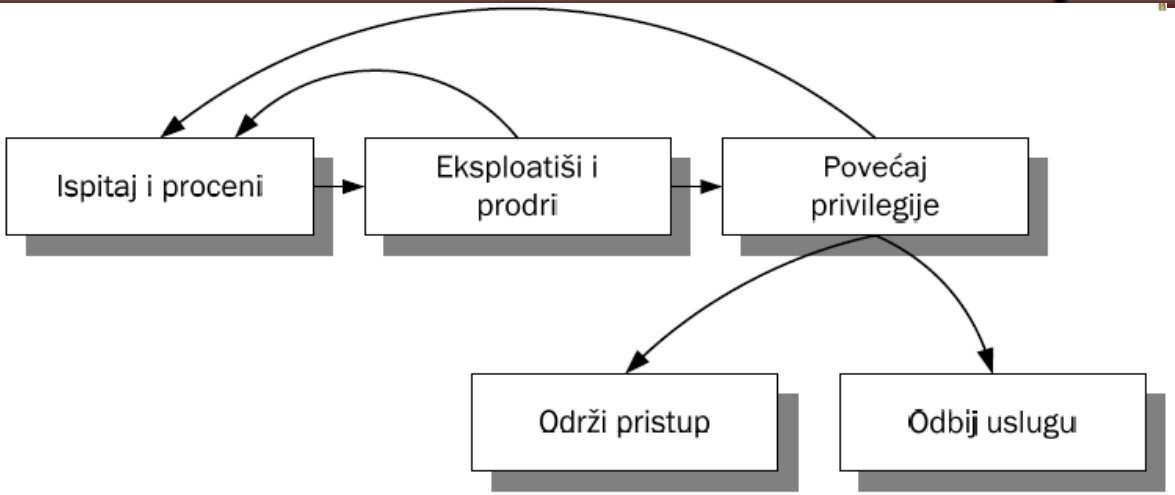
d) Uklanjanje ili proizvodnja (*fabrication*) - napad na autentičnost (*authenticity*). Napadač izvodi ovaj aktivni napad tako što generiše lažne podatke, lažni saobraćaj ili izdaje neovlašćenje komande.

e) Presecanje (*interruption*) - napad na raspoloživost (*availability*). Ovim načinom se prekida tok informacija, čime se onemogućava pružanje neke usluge.

f) Napadi radi „gušenja“ servisa i distribuirano „gušenje“ servisa

Napadi radi „gušenja“ usluga (*Denial of Service, DOS*) onemogućavaju ovlašćenim korisnicima pristup računar. resursima i njihovo korišćenje.

XII – Osnovni koraci napadača



Ispitaj i proceni (*survey and assess*) - istražne radnje radi ispitivanja potencijalne mete i indentifikovanje i procena njenih karakteristika.

Eksoploatiši i prodri (*exploit and penetrate*) - pokušava da eksploatiše ranjivost i da prodre u mrežu ili sistem.

Povećaj privilegije (*escalate privileges*) - nakon ubacivanja (*injecting*) koda u aplikaciju, pokušava da poveća svoja prava

Održi pristup (*maintain access*) - preduzima korake da olakša buduće napade i da prikrije tragove (*back-door* programi, brisanje *log* fajlova)

Odbij uslugu (*deny service*)-ako ne može da pristupi sistemu, preduzima napad koji prouzrukuje odbijanje usluge (*Denial of Service - DoS*)

XII – 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 propisanih procedura zaštite.

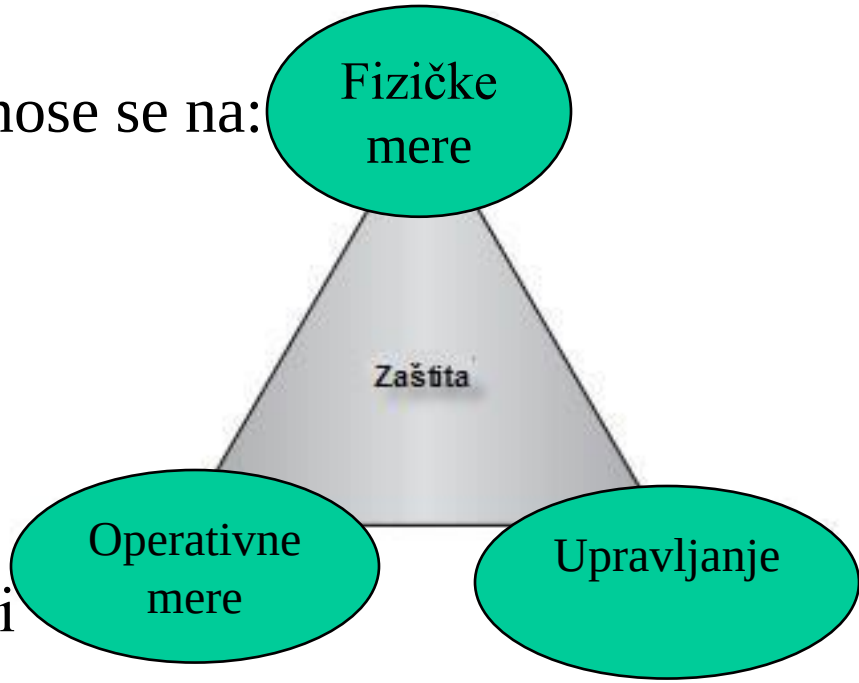
Detekcija podrazumeva identifikaciju događaja nakon njihovog nastanka. Ona je često otežana jer napad na neki sistem može biti izvršen znatno ranije tj. pre nego što se pokaže uspešnim. Detekcija incidenta podrazumeva utvrđivanje dela opreme koja je izložena napadu. To zahteva primenu složenih alata,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

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.

XII-Opšti pojmovi sistema zaštite

- Zaštita podataka neke računarske mreže 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 politici zaštite**



- Svaka od navedenih oblasti ima izuzetnu važnost u uspostavljanju efikasnog sistema zaštite u 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.

XII – 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.

1. Podrazumeva smanjivanje privlačnosti fizičke lokacije kao cilja eventualnog napada tj.: instaliranje opreme za nadzor, alarmni sistemi, posebna prostorija koja se zaključava, upotreba UPS – neprekidnog izvora napajanja, pravilno korišćenje hardverskih komponenti, odgovarajući uslovi u kojima uređaji rade i td.
2. Podrazumeva detekciju napada ili kradljivca. Korisnik mora znati gde je došlo do provale, šta nedostaje i kako je došlo do gubitka.
3. Obuhvata oporavak organizacije nakon krađe ili gubitka ključnih podataka i sistema, kako bi organizacija mogla dalje normalno nastaviti obavljanje redovnog posla. Oporavak zahteva detaljno planiranje, razmišljanje i testiranje kritičnih momenata.

XII – Operativne mere zaštite

- Odnose se na način obavljanja poslovnih funkcija u organizaciji.
- One obuhvataju dokumente koji propisuju kako se ophodimo prema računarima, mreži, komunikacijskim sistemima 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.

XII – 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 i dokumenata
  - ✓ politika zaštite
  - ✓ pravila upotrebe
  - ✓ pravila koja definišu upravljanje korisnicima

Hvala na pažnji !!!

Pitanja

? ? ?