XI- Bezbednost mrežnih operat.sistema

S A D R Ž A J

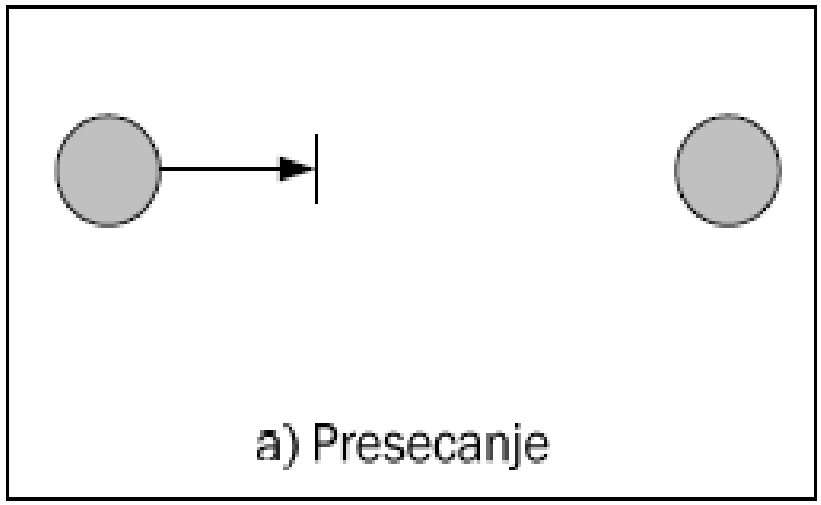
11.1 Pojam bezbednosti MOS

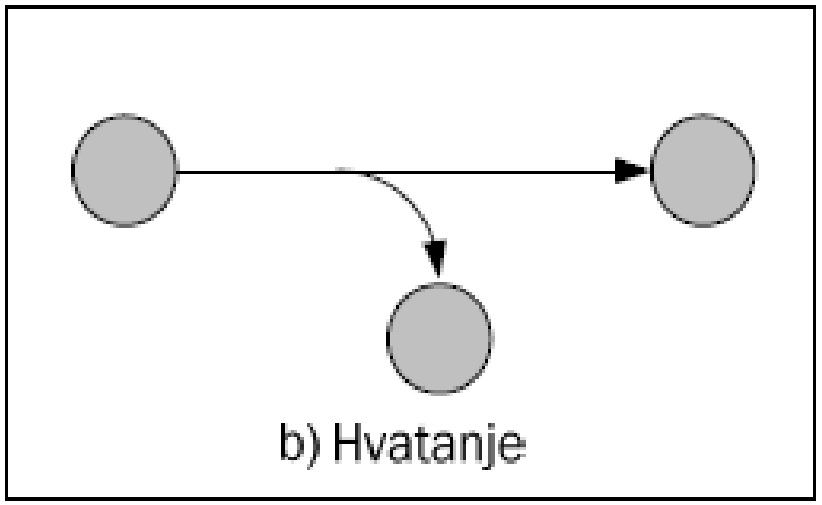
- Računarska mreža predstavlja centralno mesto za skladištenje različitih objekata: fajlovi,baze podataka,deljeni štampači,razni mrežni servisi ...
- Osnovni cilj je da omogući različite oblike komunikacije, poput E-maila, video konferencije i drugih naprednih tehnologija budućnosti
- Prvi i osnovni zadatak svake računarske mreže jeste da obezbedi pouzdano i bezbedno izvršavanje određenog servisa.
- U početku većina računarskih mreža bila je slabo obezbeđena, čak potpuno neobezbeđena, ali danas bezbednost mreže je na prvom mestu
- Na isti način kao što vlasnici radnji zaključavaju uazna vrata, ormare sa dokumentima ili registar kase da bi sačuvali svoja fizička dobra, tako i moderne kompanije nastoje da sačuvaju svoje informacije.
- Sistem bezbednosti jedne računarske mreže sastoji se iz više aspekata i u mnogome zavisi od mrežnog softvera koji se primenjuje.
- Bez obzira na to, ko je proizvođač mrežnog softvera koji koristimo, bezbednost računar.mreža se tipično svodi na dva osnovna elementa:
    1. **provera autentičnosti** (*authentication*)
    2. **autorizacija** (*authorization*)

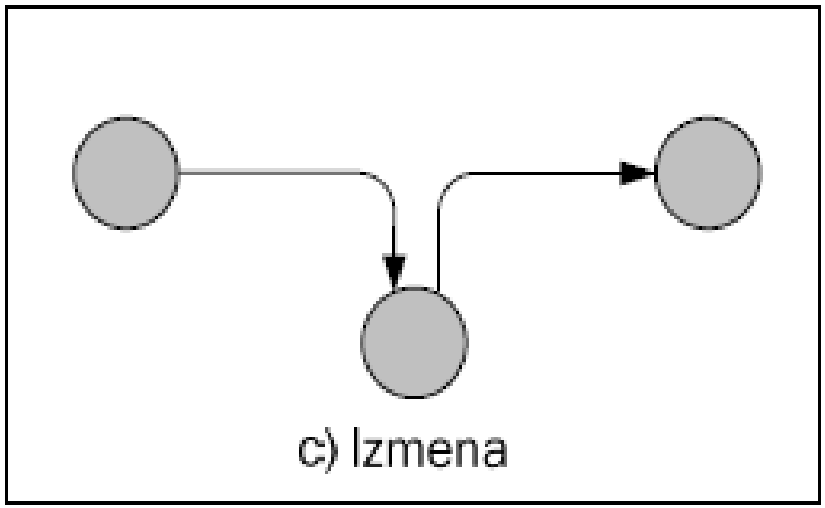
11.1 Pojam bezbednosti MOS

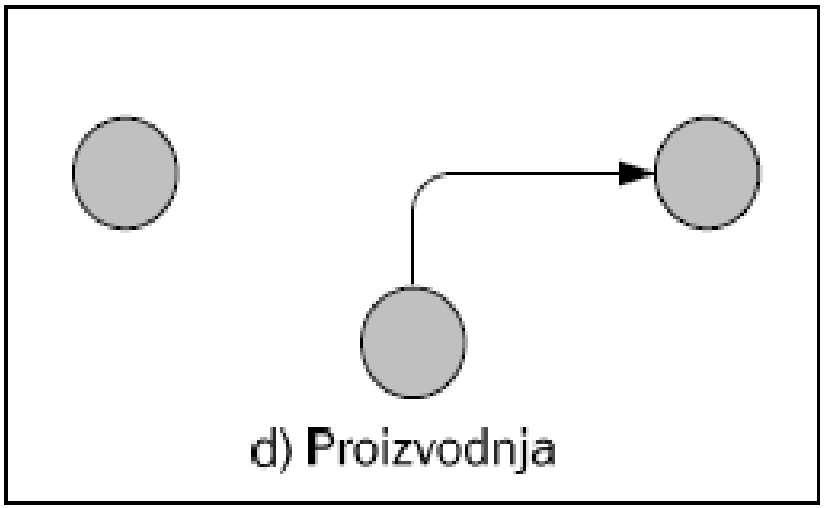
- Podaci jednog preduzeća ključni su za njegov opstanak i moraju da budu veoma dobro zaštićeni od moguće zloupotrebe.
- Administratori mreža moraju da obezbede da podaci sačuvaju svoj integritet, da uvek budu pouzdani i nepristupačni za neovlašćene.
- Postoje mnogobrojni mehanizmi koji se mogu upotrebiti kao pomoć za očuvanje integriteta i tajnosti podataka.
- Tu spadaju definisanje strogih pravila pristupa podacima, šifrovanje, kopiranje (*backup*) i omogućavanje stalne raspoloživosti podataka
- Podaci su podložni napadu i krađi neprekidno i to od trenutka kada korisnik upiše svoje ime i lozinku pa do pamćenja raznih podataka.
- Postoje i neke druge metode prijavljivanja na sistem u koje spadaju u znatno sigurniji načini prijavljivanja za mrežni rad: pametne kartice (*smart card*) i identifikacija putem bioloških karaktristika klijenta
- Sledeći problem koji se javlja je kako da se obezbedi pouzdan prenos tih podataka do kontrolera domena gde oni treba da se provere.
- Četiri osnovne radnje mogu se primeniti na podatke duž cele te putanje kojom oni prolaze: ***Presecanje, Hvatanje, Izmena, Proizvodnja***.

11.1 Pojam bezbednosti MOS







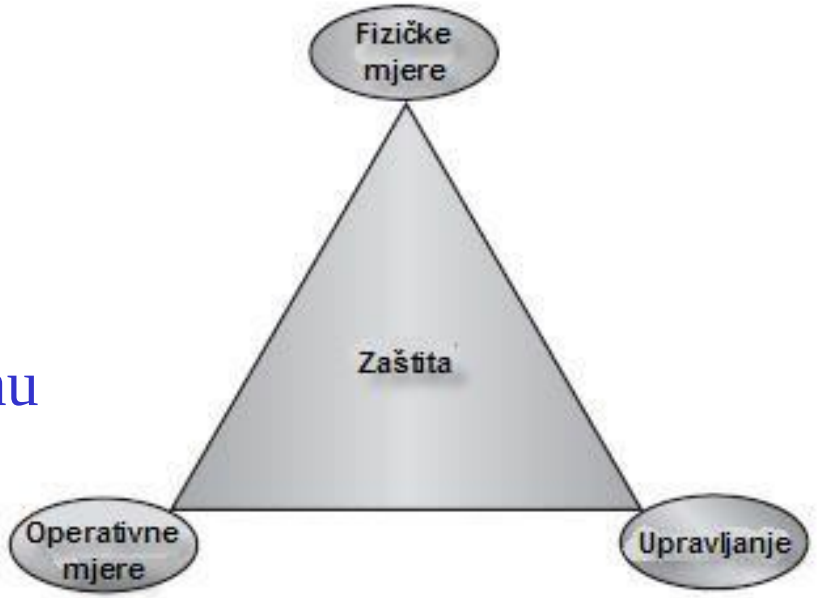


11.1 Pojam bezbednosti MOS

- Ako nisu šifrovani ili ako su vrlo slabo šifrovani, postoji mogućnost da neko ko prisluškuje saobraćaj na mreži presretne razmenu podataka između vašeg ulaznog uređaja i kontrolera domena.
- Da bi to sprečio Windows OS koristi složene tehnologije šifrovanja prilikom prenosa podataka i mrežnih komunikacija (***Ipsec, SSL***), kao i pri upisu datoteka na diskove i za njihovu zaštitu (***EFS***, ***BitLocker***).
- Sledeći korak u stvaranju bezbednog mrežnog računarskog sistema je da se svi podaci koji se čuvaju na mrežnim diskovima, kako sistemski tako i korisnički, obezbede od potencijalnih hardverskih kvarova ili prirodnih nepogoda.
- Jedno od mogućih rešenja ovog problema predstavlja svakodnevno redovno pravljenje rezervnih kopija i njihovo čuvanje na sigurnim mestima (*backup serivce*).
- Windows Server OS nudi nam veliki spektar rešenja ovog problema koji su u mnogome unapredili ovaj servis i olakšali rad administratorima u jednom veoma važnom segmentu obezbeđivanja bezbednog i pouzdanog mrežnog računarskog sistema.

11.1 Pojam bezbednosti MOS

- 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:
  - **fizičke mere zaštite**
  - **operativne mere zaštite**
  - **upravljanje i politika zaštite**



- Svaka od navedenih oblasti ima izuzetnu važnost u uspostavljanju efikasnog sistema zaštite u organizaciji.
- Zaštita računarskih sistema, organizacija i njeno poslovanje se moraju posmatrati kao celina, uz evidentiranje svih mogućih problema.
- 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.

11.1 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.
- Oni mogu otuđiti dokumenta, oštetiti ih ili izneti iz kancelarije, iz koša za otpatke ili iz kase.
- "Nosioci" ovakvih pretnji mogu biti serviseri, domari, klijenti, dobavljači, pa čak i svi radni ljudi u preduzeću.
- **Prva mera** fizičke zaštite podrazumeva smanjenje privlačnosti fizičke lokacije kao cilja eventualnog napada kao što su zaključavanje vrata i instaliranje opreme za nadzor ili alarmnih sistema.
- **Druga mera** podrazumeva detekciju napada ili kradljivca. Korisnik mora da zna gde se dogodila provala, šta nedostaje i kako je došlo do gubitka. Neophodno je da se snimaju osetljiva mesta radi detektovanja neovlašćenog pristupa i moguće krađe kao i njihovih počinilaca.
- **Treća mera** obuhvata oporavak nakon krađe ili gubitka ključnih podataka i sistema, kako bi organizacija mogla dalje normalno nastaviti obavljanje redovnog posla.

11.1 Operativne mere zaštite

- Odnose se na način obavljanja poslovnih funkcija u organizaciji.
- One se odnose na računare, mreže, komunikacijske sisteme, ali i na rad sa dokumentima.
- Operativne mere pokrivaju široku oblast, i one 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.

11.1 Upravljanje i politika

- Upravljanje i politika (*management and policies*) osiguravaju osnovne upute, pravila i procedure za implementaciju zaštićenog okruženja.
- Profesionalci u oblasti zaštite predlažu mere koje će biti ugrađene u politiku, ali im je za punu implementaciju tih mera potrebna pomoć organa upravljanja kako bi one bile efikasne.
- Zaštita mreže zahteva definisanje brojnih pravila po sledećim pitanjima:
  - ✓ o administrativnoj politici
  - ✓ o zahtevima u pogledu dizajna softvera
  - ✓ o planovima oporavka sistema nakon težih padova
  - ✓ o načinu korišćenja podataka
  - ✓ o politici zaštite
  - ✓ o pravilima upotrebe opreme i softverskih paketa
  - ✓ o pravilima koja definišu upravljanje korisnicima

11.2 Osnovni ciljevi zaštite podataka

- Ciljevi sistema za zaštitu podataka su jasni i precizni.
- Oni 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 zbog narušavanja propisanih procedura zaštite nazivaju se **incidenti.**
- **Detekcija** - podrazumeva identifikaciju događaja nakon njihovog nastanka. Ona je često otežana jer napad na neki sistem može biti započet znatno pre nego što se detektuje. Detekcija incidenta podrazumeva utvrđivanje dela opreme koja je izložena napadu. Proces detekcije zahteva primjenu složenih alata dok je ponekad dovoljno pregled sistemskih datoteka-dnevnika (***log*** datoteka).
- **Odgovor** - podrazumeva razvoj strategija i tehnika radi neutraliziranja napada i gubitaka. Podrazumeva implemetaciju kontrole pristupa, primenu antivirusnog programa, firewall-a, proxy servera, primenu sigurnosnih protokola, server sertifikata, korišćenje tehnika kriptovanja, formiranje demilitarizovane zone i td.

11.3 Faktori koji ugrožavaju bezbednost

- Postoji mnogo razloga zbog kojih bi neko ugrozio bezbednost našeg računarskog sistema i to je moguće uraditi i spolja i iznutra.

❑ **Spoljno okruženje**

✓ Do nedavno, jedini način da ugrozite bezbednost neke organizacije bio je da ugrozite neku njenu fizičku imovinu.

✓ Danas je neuporedivo jeftinije i bezbednije da se napad izvede putem računarske mreže sa nekog udaljenog mesta.

✓ Serveri su prepuni dragocenih podataka jer se gotovo svi podaci čuvaju negde u mreži u datotekama i bazama podataka.

❑ **Unutrašnje okruženje**

✓ Pretnje po bezbednost iz untrašnjeg okruženja potiču od zaposlenih u firmi, koji mogu da budu zlonamerni, neznalice ili da nenamerno greše.

✓ Njihove posledice mogu da budu izbrisane datoteke, oštećenje baze podataka, izbrisani direktorijumi za elektronsku poštu i tome slično.

✓ Često uzrok nema nikakve veze sa korisnicima, već je rezultat lošeg rada lenjog administratora servera ili mreže.

11.3 Osnovne pretnje

❑ Špijuniranje

- ✓ Neki ljudi bi rado provalili u vašu „zabranjenu zonu“ da bi saznali poslovne tajne, nacrte proizvoda preduzeća, finansijske podatke itd.
- ✓ Ovo je najopasnija pretnja po bezbednost jer su napadači izuzetno motivisani da uspešno ostvare napad.
- ✓ Ukoliko napadači ostanu neotkriveni, šteta je često nepopravljiva.
- ✓ Odbrana od ovakve vrste napada je najteža, jer ne znate gde je napad.

❑ Obaranje sistema

- ✓ Svrha ove vrste napada je da se potpuno uništi napadnuti računar.
- ✓ Cilj napadača mogu da budu računari na vašoj fizičkoj lokaciji ili cela vaša mreža ako korisnicima dozvoljavate daljinski pristup.
- ✓ Ovo ubrzano postaje najpopularniji način uništavanja vašeg truda: prvo, zbog zavisnosti vaše organizacije od mreže i drugo, zato što napadač ne mora da je fizički prisutan u vašoj mreži da bi izveo napad.
- ✓ Napad kojim se sistem toliko zaguši da ne može da obavlja svoje funkcije (***Denial of Service***, DoS) može da bude u obliku zatrpavanja mrežnog prolaza ogromnim brojem poruka,ili u obliku *syn* napada.

11.3 Osnovne pretnje

Neprijateljske aplikacije

- ✓ Na Internetu postoje „neprijateljski nastrojene“ aplikacije koje posetioci Web lokacija preuzimaju ništa ne sluteći.
- ✓ Kada tu vrstu aplikacije pokrenete unutar svoje mreže, ona počinje da obavlja svoj prljavi posao, što ne mora da bude nešto po čemu biste je odmah otkrili, sa ciljem da pronađe ili sakupi određene podatke.
- ✓ Ova vrsta aplikacije poznata je i pod nazivo **trojanski konj**.

Napadi virusa

- ✓ Svakako najčešća vrsta napada na mrežu obavlja se putem virusa.
- ✓ Suprotno tvrdnjama da postoji preko 10 000 potpuno različiti virusa, samo mali broj ljudi može da tvrdi da su sami napisali određeni virus
- ✓ Na Internetu postoji velika količina virusnog koda koji možete slobodno preuzeti, prepraviti ili unaprediti svojim kodom.
- ✓ Zbog toga se svakog meseca pojavljuju nove varijacije starih virusa.
- ✓ Neke možete da otkrijete i očistite omoću antivirusnog softvera.
- ✓ Drugi su mnogo opasniji, jer ih antivirusni softver otkriva nakon što oni izvrše svoj kod a tada je kasno jer je određena šteta već naneta.

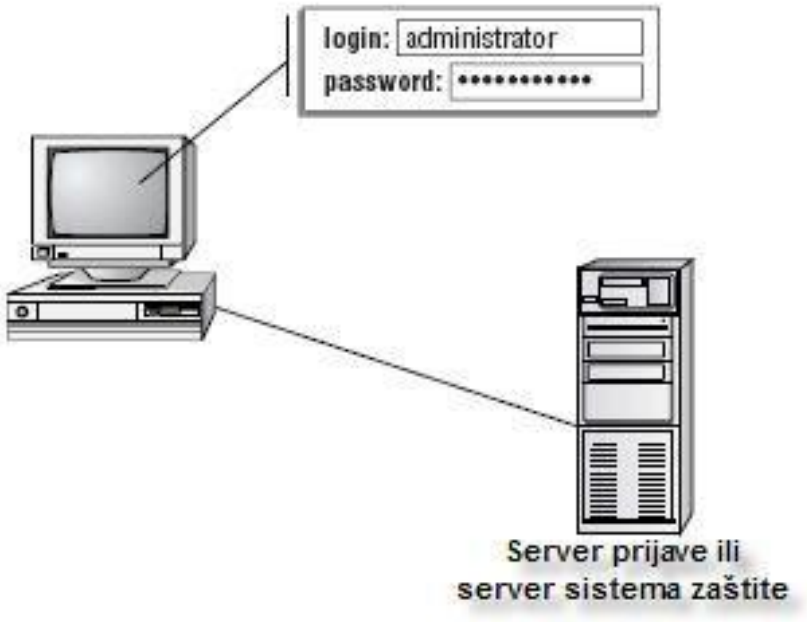
11.4 Implementacija kontrole pristupa

- Jedan od najvećih zadataka danas predstavlja bezbedno okruženje.
- Kompanije su mnogo otvorenije u dozvoljavanju partnerima da pristupe podacima na njihovim mrežama, ali su i mnogo strože kada se radi o bezbednosti tih podataka i komunikacija.
- Izazov za administratora je pronaći ravnotežu između upotrebljivosti i bezbednosti.
- Ranije verzije Windows OS su imale brojne nedostatke u bezbednosti.
- Od Windows Servera 2003 Microsoft je napravio ogroman napredak u unapređivanju bezbednosti sopstvenih OS i aplikacija.
- Svi softveri moraju da prođu rigorozne testove da bi se proverile sve poznate pukotine, osetljivost bafera i ostala potencijalna pitanja u vezi sa bezbednošću pre nego što se proizvod pojavi na tržištu.
- Uspostavljanje kontrole pristupa predstavlja ključni deo čitavog sistema zaštite računarskih resursa jer ona definiše međusobnu komunikaciju korisnika i računarskih sistema.
- Ona ograničava i kontroliše pristup sistemskim resursima, uključujući i podatke, čime se sprečava neovlašćen pristup podacima.

11.4 Kako funkcioniše kontrola pristupa

- Procesom identifikacije utvrđuje se da li je neka osoba, zaista ona osoba za koju se predstavlja.
- Ona je ključni deo sistema zaštite i predstavlja deo procesa koji se naziva ***Identification and Authentication*** (I&A).
- Sistemi ili metodi identifikacije zasnovani su na sledećim faktorima:
  - ✓ na nečemu što korisnik zna, kao što su lozinka ili PIN
  - ✓ na nečemu što korisnik poseduje, poput smart kartice
  - ✓ na nečemu što fizički određuje korisnika, otisak prsta, dužica oka

- Korisničko ime i lozinka jednoznačno identifikuju korisnika tokom prijave na sistem (*logon*).



- Većina OS koristi korisnički ID i lozinku za proces identifikacije koji se preko mreže mogu slati u otvorenom ili šifrovanom obliku.

11.5 Postupak izrade sigurnosnih kopija

- Svaki korisnik sam za sebe treba doneti odluku o tome koji su mu podaci važni i za koje podatke je potrebno izrađivati sigurnosne kopije.
- U praksi se obično izrađuju sigurnosne kopije podataka generisanih aplikacijama dok se za same aplikacije u pravilu ne izrađuju kopije.
- Prilikom procesa izrade sigurnosnih kopija pažnju je potrebno posvetiti i smeštaju podataka.
- Podaci se mogu smestiti na lokalnom računaru, na udaljenom računaru koji služi kao fajl server ili na nekim prenosivim medijima.

- Sam proces izrade sigurnosnih kopija odvija se u nekoliko faza:

1) Identifikacija podataka

- ✓ Administratori sistema zajedno sa korisnicima trebaju da odluče koji podaci su važni za organizaciju ili korisnike.
- ✓ U praksi se kao najbolja praksa pokazala simulacija kojom se definišu podaci koje je potrebno vratiti u slučaju kvara računara.
- ✓ Obično su to podaci koje generišu tekstualni i tabelarni programi, baze podataka i elektronska pošta.

11.5 Postupak izrade sigurnosnih kopija

2) Određivanje prikladnog medija

- ✓ Sa obzirom na prirodu sadržaja čija se sigurnosna kopija kreira, potrebno je odrediti i prikladan medijum.
- ✓ To mogu biti trake, diskete,ZIP diskete,CD/DVD, *flash* memorija, itd...

3) Označavanje sigurnosnih kopija

- ✓ Svi mediji koji sadrže sigurnosne kopije moraju biti jednoznačno i precizno označeni.
- ✓ Informacije koje se ispisuju odnose se na datum stvaranja kopije i broj kopije u nizu kopija.
- ✓ Preporučuje se održavanje zapisa o sigurnosnim kopijama u pisanom obliku gde su navedene detaljnije informacije i reference.

4) Čuvanje sigurnosnih kopija

- ✓ Zapise o sigurnosnim kopijama potrebno je određeno vreme čuvati.
- ✓ U praksi se koriste zapisi stari jedan dan, nedeljni, mesečni, polumesečni, polugodišnji i godišnji – zavisno od toga kolika je količina podataka koju želimo sačuvati.
- ✓ Ovim postupkom organizacije se osiguravaju od gubitka podataka

11.5 Postupak izrade sigurnosnih kopija

5) Smeštaj sigurnosnih kopija

- ✓ Sigurnosne kopije se trebaju smestiti zajedno sa pripadajućim zapisima na sigurnu lokaciju (npr., zaključana fijoka, ormar ili vatrootporan sef).
- ✓ U idealnoj situaciji kopije se drže na drugoj lokaciji dovoljno udaljenoj od originalne kako bi se izbegle prirodne nepogode (vatra, poplava,…) i time omogućilo sigurno vraćanje podataka i odvijanje procesa poslovanja

6) Testiranje sigurnosnih kopija

- ✓ Nakon obavljanja procesa izrade sigurnosnih kopija potrebno je testirati vraćanje podataka sa medija.
- ✓ Tako se proverava da li su svi podaci iz kopije ispravno vraćeni
- ✓ Organizacije uvek moraju posedovati plan za najgori mogući scenario kao što je npr. potpuni gubitak podataka na sistemu.
- ✓ Zbog toga treba postojati definisan postupak vraćanja podataka na zamenjeni hardver i uspostavljanje prethodnog operativnog stanja.
- ✓ Postupak testiranja vraćanja podataka moguće je izvršiti u dve faze: testiranje na postojećem računaru ili na računaru slične konfiguracije.

11.5 Postupak izrade sigurnosnih kopija

Pri izradi sigurnosnih kopija dobro je imati ovakvu listu za proveru:

- ✓ da li su izrađene sigurnosne kopije svih podataka, OS i pomoćnih programa adekvatno i sistematski,
- ✓ postoje li zapisi o sadržaju sigurnosnih kopija i njihovom smeštaju,
- ✓ postoje li zapisi o licenciranim aplikacijama,
- ✓ postoje li kopije medija/zapisa koji su smešteni na udaljenoj lokaciji,
- ✓ da li je povremeno proveren postupak vraćanja podataka sa medija,
- ✓ može li novi hardver čitati podatke sa postojećih medija,
- ✓ da li se zbog postojećih licenci aplikacija pokreće na novom hardveru
- ✓ da li je sproveden postupak potpunog vraćanja podataka u određenom vremenskom periodu.

- ➢ U praksi se ne preporučuje korišćenje samo jednog medija
- ➢ Rizik koji je povezan sa gubikom podataka je manji ukoliko postoji više kopija istih podataka.
- ➢ Ukoliko se radi o optičkim medijima preporučuje se korišćenje većeg broja jer je njihova cena zanemariva sa obzirom na štetu koja se može prouzrokovati gubikom podataka.

11.5 Postupak izrade sigurnosnih kopija

- Postoji više metoda za stvaranje sigurnosnih kopija.
- Jedna od najčešćih je stvaranje vlastitih arhiva od strane korisnika.

Tip bekapovanja	*Opis*
Normal (Normalno)	Kopira sve selektovane fajlove, a zatim resetuje bit arhive.
Incremental (Inkrementalno)	Kopira sve selektovane fajlove sa postavljenim bitom arhive, a zatim resetuje bit arhive.
Differential (Diferencijalno)	Kopira sve selektovane fajlove sa postavljenim bitom arhive, ali ne resetuje bit.
Daily (Dnevno)	Kopira sve selektovane fajlove koji su bili editovani u danu kada je izvršeno bekapovanje.
Copy (Kopiranje)	Kopira sve selektovane fajlove, ali ne resetuje bit arhive.

11.6 Medijumi za izradu sigurnosnih kopija

- Izbor medija ili uređaja na koji će se upamtiti sigurnosna kopija zavisi od više faktora:

- kolika je važnost podataka za koje se izrađuje sigurnosna kopija,
- koliko se često izrađuju sigurnosne kopije,
- kolika je veličina sigurnosnih kopija,
- koliko se dugo sigurnosne kopije trebaju čuvati,
- kakve su mogućnosti organizacije u pogledu kreiranja i čuvanja sigurnosnih kopija

1) Floppy disketa

- Diskete su stari medijumi kapaciteta 1-2 MB kojima je brzina čitanja i zapisivanja veoma spora, ali zato cena medija nije visoka.
- Iako su u prošlosti diskete mogle sadržati i cele operativne sisteme, danas one ne mogu čuvati dovoljno velike količine podataka.
- Zato se ova vrsta medija koristi za manje količine podataka kao što su manje datoteke i to za sigurnosne kopije pojedinih korisnika
- Prednost im je što su jednostavne za dodavanje novih podataka i uklanjanje starih

11.6 Medijumi za izradu sigurnosnih kopija

2) Optički mediji (CD-R/RW, DVD-R/RW)

- Optički mediji danas su jedni od najčešće korišćenih oblika za skladištenje sigurnosnih kopija.
- Podeljeni su na CD, DVD i Bluray medije koji koriste različitu metodologiju za čitanje i skladištenje podataka.
- CD mediji imaju kapacitete od par stotina MB, DVD mediji imaju kapacitet oko par GB a Bluray diskovi od nekoliko desetina GB.
- Optički mediji su odlični mediji po pitanju performansi i cene jer imaju veliki kapacitet, umerenu brzinu pristupa mediju a malu cenu

3) Tvrdi disk (Hard Disk)

- Danas HD imaju velike kapacitete i relativno su jeftini
- HD je fiksni nezamenjivi magnetni uređaj za čitanje i pisanje
- HD može biti lociran na istom računaru za koje se radi izrada sigurnosnih kopija, ali se može nalaziti i na posebnom serveru
- U sistemu može postojati više računara koja su umrežena pa je zato moguće organizovati smeštanje sigurnosnih kopija na HD drugog računara.

11.6 Medijumi za izradu sigurnosnih kopija

4) ZIP disketa

- ZIP je izmenjiv medijum kapaciteta većeg od disketa,
- Zbog svog povećanog kapaciteta bila popularna zamena za diskete.
- Danas se sve manje koriste jer ih zamenjuju flash memorije

5) Flash memorije i memoriske kartice

- Sa razvojem proizvodnje mikročipva pala je i cena memorije.
- Danas se koriste čipovi kapaciteta do nekoliko desetina GB, a mogu fizički biti smešteni najčešće u obliku USB memorijskog priključka ili pak u obliku memorijskih kartica (SD diskovi)
- Prednost im je velika brzina i relativno niska cena, dok im je glavni nedostatak to što se zbog male veličine mogu lako fizički oštetiti.

6) Magnetne trake

- Medijum koji je dugo bio najčešće korišćen za skladištenje velikih količina podataka, rezervnih kopija, arhiviranje i razmenu.
- Traka je medijum sa sekvencijalnim pristupom, tako da, iako pristupno vreme može biti veliko, stepen kontinualnog upisa ili očitavanja podataka može zaista biti veoma brz.

11.6 Medijumi za izradu sigurnosnih kopija

7) Udaljeni backup uređaji (*Storage Area Networks*)

- Kako širokopojasni pristup Internetu postaje uveliko zastupljen, tako i udaljeni servisi za rezervne kopije dobijaju na popularnosti.
- Pravljenje rezervnih kopija preko Interneta na udaljenoj lokaciji može zaštiti podatke od nekih najgorih scenarija kao što su požari, poplave ili zemljotresi, koji mogu uništiti svaku rezervnu kopiju
- Postoji, svakako i niz nedostataka pri kreiranju rezervne kopije na udaljenoj lokaciji.
- Prvo, Internet veze su generalno dosta sporije od brzine lokalnih uređaja za skladištenje, što može predstavljati problem za ljude koji rade sa velikim količinama podataka.
- Drugo, korisnici treba da imaju poverenja u treća lica koji upravljaju ovim servisima, kako po pitanju privatnosti tako i po pitanju bezbednosti podataka.
- Rizik u vezi prepuštanja ličnih ili osetljivih podataka trećim licima može se smanjiti šifrovanjem tih podataka tako da njihov sadržaj ne može da se vidi bez ključa.

11.7 Preporuke za izradu sigurnosnih kopija

Provera vraćanja podataka nakon nepravilnosti u radu sistema

- U praksi se obavljaju provere i testiranja da li je moguće nastaviti poslovanje npr. nakon kvara na čvrstom disku, ukoliko smo izgubili medije sa sigurnosnim kopijama ili su one ukradene.
- U testiranje su uključene različite smernice koje analiziraju koliko je potrebno da se poslovanje vrati u fazu pre nego što su izgubljeni podaci, koji su preduslovi potrebni za to, ko je odgovoran i sl.
- Sve ove smernice moraju biti sadržane prilikom izrade politike sigurnosnih kopija.

Periodična provera sigurnosnih kopija

- Kako mediji i pripadajući hardver mogu biti veoma nepouzdani potrebno je periodično sprovoditi testiranja koja se odnose na njihovu ispravnost.
- Velika količina podataka smeštenih na trakama ili disketama je beskorisna ukoliko se ne mogu pročitati sa istih.
- Zato je potrebno periodično proveravati ispravnost sigurnosnih kopija.

11.7 Preporuke za izradu sigurnosnih kopija

Čuvanje starih verzija sigurnosnih kopija

- Potrebno je vreme kako bi se utvrdilo da je neka datoteka uništena
- Zbog takvih slučajeva uvek je potrebno čuvati stare verzije sigurnosnih kopija izvesno vreme ili onoliko koliko nalaže zakon.
- Moguće je čuvati dnevne, mesečne, polugodišnje ili godišnje verzije
- Preporučuje se čuvanje stare kopije na različitoj lokaciji

Provera sistema datoteka pre izrade sigurnosnih kopija

- Ukoliko se radi o povratku podataka sistema koji je prethodno uništen onda je sigurnosna kopija beskorisna.
- Preporučuje se pre izrade sigurnosne kopije proveravanje integriteta sistema datoteka.

Provera da se datoteka ne koristi tokom stvaranja kopije

- Ukoliko se datoteka koristi prilikom izrade sigurnosne kopije ona je beskorisna jer ne sadrži ispravnu i važeću verziju.

Stvaranje sigurnosne kopije pre velikih promena u sistemu datoteka

- Korisno je imati rezervnu kopiju pre testiranja novog hardvera, popravaka na sistemu ili instalacije novih aplikacija.

11.8 Alati za Backup i Recovery

- Postoje tri alata za obavljanje bekapa i vraćanja podataka u Windows
  1. GUI pod nazivom Windows Server Backup,
  2. Alat za korišćenje iz komandnog prompta ***wpadmin.exe***
  3. PowerShell *cmdlets* set komandi za kontrolu bekapa i oporavka podataka.
- Na Server Core instalaciji, imamo na raspolaganju samo *wpadmin.exe* i PowerShell-ov *cmdlets* kao alate za rad sa bekapom.
- Pored ovih alata, još jedan vredan alat koji možemo iskoristiti da bismo zaštitili podatke koji su deljeni je ***Volume Shadow Copy Service***.
- Ova alatka stvara rezervne kopije u određenom trenutku vremena nad podacima koji se nalaze u deljenim folderima.
- nost da štite sebe od slučajnog brisanja ili prepisivanje fajlova ava da uporede verzije datoteka nad kojima se vrši Shadow Copy.

Hvala na pažnji !!!

Pitanja

? ? ?