HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Osnove sigurnosnih kopija

CCERT-PUBDOC-2006-04-156

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

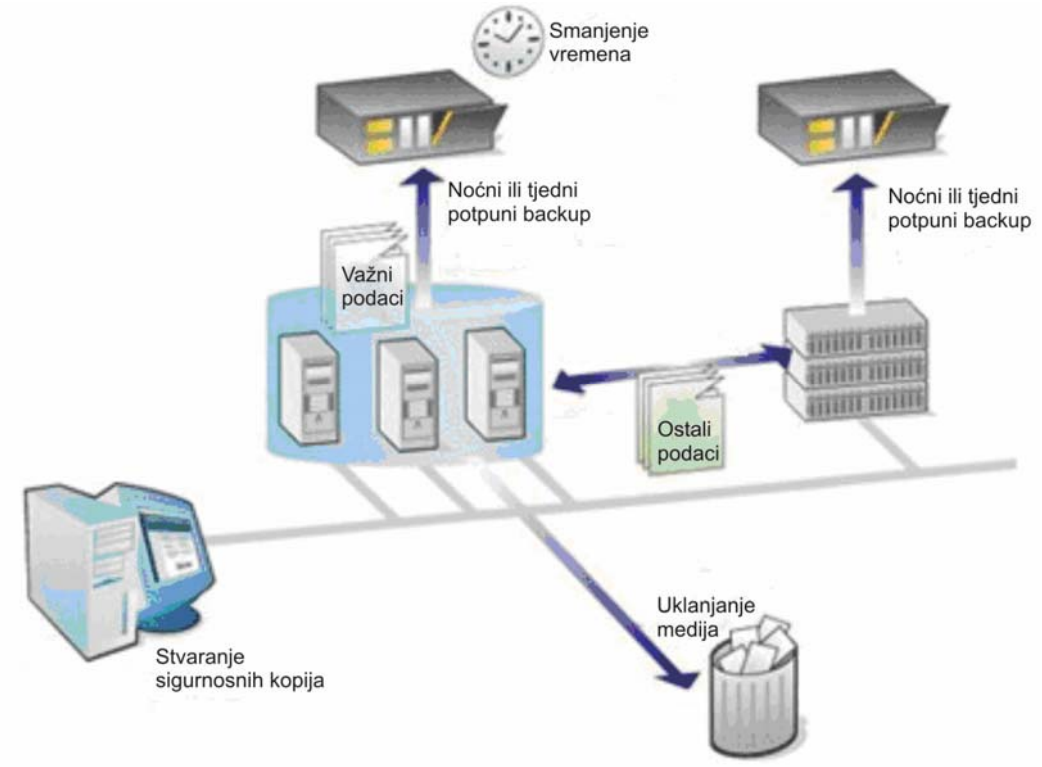
1. Uvod

Danas računala i aplikacije služe za povećavanje produktivnosti, smanjivanje troškova i uštedu vremena potrebnog za obavljanje posla. Ukoliko se nedovoljna pažnja posveti rizicima koji ugrožavaju računalne sustave, u organizacijama su moguće situacije koje mogu uzrokovati zastoje u poslovanju. I da se ne bi dogodio neplanirani zastoj, organizacije i korisnici moraju redovito obavljati procedure za izradu i održavanje sigurnosnih kopija. U protivnom može doći do katastrofalnih posljedica kako za korisnike tako i za organizaciju. Uzrok tome je što je poslovanje ovisno u informacijskim tehnologijama. Pred informatičke podatke se postavljaju visoki kriteriji zaštite koji su jednaki ili čak veći od kriterija zaštite zapisa u poslovnim knjigama. Informacijski sustav je dio infrastrukture organizacije te je stoga nedostupnost istog ili uništenje podataka veliki rizik za koji treba planirati mjere kontrole i obavljati postupke kojima se povećava potpuno, sigurno i jeftino vraćanje podataka.

Izrada sigurnosnih kopija (eng. *backup*) je osnovna pretpostavka koja se postavlja pred sustav koji mora zadovoljavati sigurnosne zahtjeve. Postupak izrade sigurnosnih kopija zajedno s postupkom povratka podataka, predstavlja osnovnu proceduru kojom se sustav zaštićuje od gubitka podataka i osigurava brza obnova podataka u slučaju nepravilnosti u radu sustava kao što su npr. prekidi u radu računalnog sustava, infekcije virusima ili pak prirodne katastrofe poput poplava i požara.

Potrebno je ispitati ispravnost sigurnosne kopije i procijeniti koliko je pouzdan medij na kojem je ona smještena. Sigurnosna kopija gubi svoju namjenu ukoliko se za vrijeme povrata podataka otkrije da je ona na krivom mediju, pogrešno označena ili uništena.

Dokument opisuje primjenjive postupke koji se mogu provesti i kod kućnih ili uredskih korisnika pa sve do velikih organizacija.



Slika 1: Stvaranje sigurnosnih kopija i vraćanje podataka

2. Razlozi za izradu sigurnosnih kopija

Jedan od glavnih razloga za izradu sigurnosnih kopija je raspoloživost sustava. Svaki poremećaj u radu sustava se odražava u prestanku rada istog. Posljedice nemogućnosti odvijanja poslovnih procesa se zavisno o važnosti tih procesa, mjere u različitim iznosima (od tisuća do milijuna). S tim razlogom je potrebno osigurati izradu sigurnosnih kopija kako bi se u izvanrednim okolnostima moglo nastaviti s poslovanjem.

Osiguranje neprekinute raspoloživosti i mogućnost nastavka rada informacijskog sustava uslijed nepredviđenih okolnosti, čine uspješnim poslovanje organizacije, dok se u slučajevima neispunjena tih uvjeta uzrokuju uz financijske i neke nepopravljive štete kao što su gubitak ugleda, nepovjerenje klijenata i prestanak suradnje s dobavljačima. Ukoliko organizacija raspolaže sigurnosnim kopijama, u slučajevima elementarnih nepogoda (požar, potres, poplava, sabotaže, teroristički napadi, itd…) ili drugih uzroka prekidanja rada, organizacija posjeduje mogućnost uspostavljanja poslovanja na drugim lokacijima.

Neki od uzroka koji mogu prouzročiti prekid poslovanja su kvarovi pri opskrbi električnom energijom, kvarovi računala ili diskovnih medija čime se trenutno gube informacije. Osim tih uzroka prekidanja poslovanja postoje i oni uzrokovane ljudskim faktorom, a to su ljudska pogreške, zlonamjerne aktivnosti lokalnih korisnika ili udaljenih napadača. Također, virusi i drugi maliciozni programi mogu uništiti vrijedne podatke.

Još jedan razlog za izradu sigurnosnih kopija je zakonska obveza čuvanja financijskih i drugih sličnih podataka. Zavisno o propisanim rokovima za čuvanje određenih podataka definira se i politika izrade sigurnosnih kopija. Sigurnosne kopije su također valjan dokaz u sudskim procesima i stoga je ponekad važno posjedovati periodične sigurnosne kopije kojima se može dokazati postojanje određenih informacija.

Organizacije često trebaju čuvati stare podatke kada rade na poslovima koji uključuju istraživanje i razvoj. Naime, tijekom razvoja nekog programa ili sl., koji može trajati i više mjeseci ili godina, moguće su situacije u kojima je potrebno odustati od odabranog smjera rada i vratiti se u neku staru fazu koja može biti unatrag i nekoliko mjeseci.

3. Postupci u izradi sigurnosnih kopija

Svaki korisnik sam za sebe treba donijeti 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 generiranih aplikacijama dok se za same aplikacije u pravilu ne izrađuju sigurnosne kopije.

Prilikom procesa izrade sigurnosnih kopija pažnju je potrebno posvetiti i smještaju podataka. Naime, podaci se mogu spremati na lokalnom računalu, na udaljenom računalu koji služi kao datotečni poslužitelj ili na nekim prenosivim medijima. Sam proces izrade sigurnosnih kopija odvija se u nekoliko faza:

1) Identifikacija podataka

Administratori sustava zajedno s korisnicima trebaju odlučiti koji podaci su važni za organizaciju ili korisnike. U praksi se kao najbolja praksa pokazala simulacija kojom se definiraju podaci koje je potrebno vratiti u slučaju kvara računala. Obično su to podaci koje generiraju tekstualni i tabelarni programi, baze podataka i elektronička pošta. Mnogi od njih posjeduju mogućnost stvaranja jedinstvene *backup* datoteke iz koje je naknadno moguće vratiti podatke. Svakako je dobro posavjetovati se sa stručnjacima prilikom odlučivanja o tome što sve je potrebno staviti u sigurnosnu kopiju.

2) Određivanje prikladnog medija

S obzirom na prirodu sadržaja čija sigurnosna kopija se kreira, potrebno je odrediti i prikladan medij. To mogu biti trake, diskete – uključujući i ZIP diskete, CD, *flash* memorija, itd... Najčešće se odabire onaj medij koji je na jednostavan način podržan od računala, što znači da spremanje tekstualnih datoteka u obliku ispisanih stranica nije najprikladniji oblik.

3) Označavanje sigurnosnih kopija

Svi mediji koji sadrže sigurnosne kopije moraju biti jednoznačno i precizno označeni. Informacije koje su istaknute označavaju datum stvaranja kopije, broj kopije u nizu kopija i datum stvaranja. Preporuča

se održavanje zapisa o sigurnosnih kopijama u pisanom obliku gdje su navedene detaljnije informacije i reference.

4) Čuvanje sigurnosnih kopija

Zapise o sigurnosnih kopijama potrebno je određeno vrijeme čuvati. U praksi se koriste zapisi stari jedan dan, tjedan, mjesečni, polumjesečni, polugodišnji i godišnji – ovisno o tome koja je količina podataka koju želimo sačuvati. Ovim postupkom se organizacije i korisnici osiguravaju od gubitka podataka i postupak je za korisnike potpuno transparentan. Sam postupak se u praksi najčešće naziva "generacijska sigurnosna kopija" koja može sadržavati i po nekoliko generacija zapisa sigurnosnih kopija (npr. 3 generacije - *djed, otac i sin*).

5) Smještaj sigurnosnih kopija

Sigurnosne kopije se trebaju smjestiti zajedno s pripadajućim zapisima na sigurnu lokaciju (npr., zaključana ladica, ormar ili vatrootporan sef). U idealnoj situaciji se kopije drže na drugoj lokaciji dovoljno udaljenoj od originalne kako bi se izbjegle 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 s medija. Ovim postupkom se provjerava da li su svi podaci iz sigurnosne kopije ispravno vraćeni. Time se osigurava proces eventualnog vraćanja podataka u slučaju neke opasnosti.

Organizacije uvijek moraju posjedovati plan za najgori mogući scenarij kao što je npr. potpuni gubitak podataka na sustavu. Zbog toga treba postojati definiran postupak vraćanja podataka na zamijenjeni hardver i uspostava prethodnog operativnog stanja. Nakon obavljene procedure vraćanja podataka često je potrebno obnoviti licence za pripadajuće aplikacije jer su postupci kojima se generira zaporka često vezani uz konfiguraciju hardvera na računalu kao što je čvrsti disk, MAC adresa mrežne kartice ili pak ime poslužitelja.

Postupak testiranja vraćanja podataka moguće je izvršiti u dvije faze:

- testiranje na postojećem računalu ili
- testiranje na računalu slične konfiguracije.

U postupcima izrade sigurnosnih kopija potrebno je obratiti pažnju na dodatne zahtjeve. Važno je gdje su podaci smješteni s obzirom na prirodu podataka i njihovu važnost za pojedinca ili organizaciju. S obzirom na postojeće zakone o čuvanju podataka, ukoliko se radi o financijskim podacima ili slično, potrebno je čuvati kopije određeni broj godina. Ukoliko se pri korištenju aplikacija radi o ugovorima o korištenju u određenom periodu, potrebno je osigurati uništenje podataka nakon isteka istog ugovora.

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

- da li su izrađene sigurnosne kopije svih podataka, operativnog sustava i pomoćnih programa adekvatno i sistematski,
- postoje li zapisi o sadržaju sigurnosnih kopija i njihovom smještaju,
- postoje li zapisi o licenciranim aplikacijama,
- postoje li kopije medija ili zapisa spremljene na udaljenoj lokaciji,
- da li je povremeno proveden postupak vraćanja podataka s medija,
- može li novi hardver čitati podatke s postojećih medija,
- hoće li se zbog postojećih licenci aplikacija pokretati na novom hardveru i
- da li je proveden postupak potpunog vraćanja podataka u određenom vremenskom periodu.

U praksi se ne preporuča korištenje samo jednog medija za potrebe arhiviranja. Rizik koji je povezan s gubitkom podataka je manji ukoliko postoji više kopija istih podataka. Ukoliko se radi o optičkim medijima preporuča se korištenje većeg broja jer je njihova cijena zanemariva s obzirom na štetu koja se može prouzročiti gubitkom podataka. Također, ukoliko se svakodnevno provodi izrada sigurnosnih kopija ili barem u nekim definiranim periodima, smanjuje se rizik gubitka podataka.

Ukoliko se periodično provodi stvaranje sigurnosnih kopija uvijek postoji mogućnost vraćanja podataka. A u slučajevima kada se radi o većem kvaru kao što je npr. mehanički kvar na tvrdom disku, onda su najčešće uništeni svi podaci na njemu. Jedini način vraćanja podataka je iz sigurnosne kopije. Preporuča se koristiti drugi medij od onog izvornog na kojem su podaci iz kojih su izrađene sigurnosne kopije.

Postoji više metoda za stvaranje sigurnosnih kopija. Jedna od najčešćih je stvaranje vlastitih arhiva od strane korisnika. Pri tome se najčešće izrađuju sigurnosne kopije za one podatke koje korisnicima predstavljaju važan informacijski resurs (npr. elektronička pošta). Osim takvih stvaranja arhiva određenih specifičnih informacija, često se koristi i stvaranje sigurnosnih kopija datotečnog sustava. Administratori u praksi provode stvaranje sigurnosnih kopija niza korisničkih direktorija. Pri tome administratori mogu raditi sigurnosne kopije svih podataka ili samo izmijenjenih tj. novih podataka. Pošto se kod izrade sigurnosnih kopija najčešće koriste velike količine datoteka, u pravilu se one komprimiraju odgovarajućim sistemskim alatima.

3.1. Najčešći uređaji za izradu sigurnosne kopije

Izbor medija ili uređaja na koji će se pohraniti sigurnosna kopija varira o 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, itd…

U nastavku je dan pregled najčešćih uređaja koji se koriste za pohranu sigurnosnih kopija:

1) *Floppy* disketa

Diskete su mediji kapaciteta 1-2 MB kojima je brzina čitanja i zapisivanja veoma spora, ali zato cijena medija nije visoka. Iako su u prošlosti diskete mogle sadržavati i cijele operacijske sustave, danas one ne mogu čuvati dovoljno velike količine podataka. Stoga se ova vrsta medija koristi za manje količine podataka kao što su manje datoteke. Prednost im je što su jednostavni za dodavanje novih podataka te uklanjanje starih. Njihova svrha kod izrade sigurnosnih kopija nije na razini organizacije, već korisnika koji njihovim korištenjem mogu sačuvati samo neke osnovne podatke.

Slika 2: Disketa

2) Optički mediji (CD-R/RW, DVD-R/RW)

Optički mediji danas su jedni od najčešće korištenih oblika za pohranu sigurnosnih kopija. Podijeljeni su na CD i DVD medije koji koriste različitu metodologiju za čitanje i pohranu podataka. CD mediji imaju kapacitete od par stotina MB, dok DVD mediji imaju kapacitet oko par GB. Ukoliko se radi o R (eng. *Read*) medijima onda je na te medije moguće jednokratno zapisivanje, dok je kod RW (eng. *Read Write*) medija postupak zapisivanja moguć i više puta jer ti mediji omogućavanju brisanje snimljenih podataka. Optički mediji su odlični mediji po pitanju performansi i cijene jer imaju velik kapacitet, umjerenu brzinu pristupa mediju, a nisku cijenu. Kreiranje medija se mora obaviti putem posebnog programa.

Slika 3: Optički disk

3) Alternativni tvrdi disk

Danas tvrdi diskovi imaju velike kapacitete (do nekoliko stotina GB podataka) i relativno su jeftini. Tvrdi disk je uređaj za čitanje i pisanje pa se radi o fiksnom i nezamjenjivom mediju. Tvrdi disk može biti lociran na istom računalu za koje se radi izrada sigurnosnih kopija, ali se može nalaziti i na posebnom poslužitelju namijenjenog samo u tu svrhu.

Prednost korištenja tvrdog diska na istom računalu za koje se rade sigurnosne kopije je u jednostavnosti izrade same sigurnosne kopije. Naime, postojeći disk se može u punom kapacitetu presnimavati na drugi disk. Nedostatak takvog korištenja je u činjenici što je sigurnosna kopija na alternativnom mediju izložena istim rizicima i u isto vrijeme kao i originalna kopija koja se nalazi na primarnom mediju.

U sustavu može postojati više računala koja su umrežena pa je stoga moguće organizirati pohranu sigurnosnih kopija na tvrdom disku drugog računala. Time je uglavnom uklonjen nedostatak opisan za slučaj korištenja tvrdog diska za sigurnosne kopije na istom računalu. Ipak, ukoliko je udaljeno računalo u istoj mreži kao i prvo računalo, tada se pojavljuje potencijalni problem virusa koji se širi mrežom. Također, dodatni rizik je što su sva računala spojena na istu električnu mrežu i podjednako izložena oscilacijama u naponu ili širenju elektriciteta putem računalne mreže u slučaju strujnog udara.

Slika 4: Tvrdi disk

4) ZIP disketa

ZIP je izmjenjiv medij kapaciteta većeg od disketa, a manjeg od optičkog medija. ZIP disketa je zbog svog povećanog kapaciteta bila najpopularnija zamjena za diskete. Ipak, u novije vrijeme se sve manje koriste jer ih zamjenjuju *flash* memorije.

Slika 5: ZIP pogon i diskete

5) *Flash* memorije i memorijske kartice

S razvojem računalnih čipova pala je i cijena memorije. Danas u upotrebi postoje čipovi memorijskog kapaciteta do nekoliko GB, a mogu fizički biti smješteni najčešće u obliku USB memorijskog priključka (eng. *stick*) ili pak u obliku memorijskih kartica koje češće koriste uređaji potrošačke elektronike dok su manje zastupljene kod računala. Prednost im je velika brzina i relativno malena cijena, dok im je glavni nedostatak to što se zbog male veličine mogu lako fizički oštetiti.

Slika 6: Varijante memorijskih kartica

6) Podatkovne trake

To su mediji za čitanje i pisanje prenosivog oblika kapaciteta od par GB do preko stotinu GB i posjeduju veliku brzinu zapisivanja. Ovo je odličan medij visokog kapaciteta koji se često koristi u velikim organizacijama. Nedostaci traka nalaze se u njihovoj osjetljivosti na vlagu, promjenu temperature i onečišćenja zraka pa je uz visoke inicijalne troškove samog uređaja potrebno osigurati i pogodne uvjete u radnom i skladišnom prostoru.

Slika 7: Magnetna podatkovna traka

7) Pisač

Običan pisač može također biti sredstvo za pohranu podataka. Pošto podaci ispisani na njemu više nisu dostupni u digitalnom obliku onda je veoma teško prenijeti podatke nazad u sustav.

3.2. Smjernice za izradu sigurnosnih kopija

U nastavku slijede preporuke iz prakse za izradu sigurnosnih kopija:

- Provjera vraćanja podataka nakon nepravilnosti u radu sustava - u praksi se obavljaju provjere 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 smjernice koje analiziraju koliko je potrebno da se poslovanje vrati u fazu kad su izgubljeni podaci, koji su preduvjeti potrebni za to, tko je odgovoran i sl. Sve ove smjernice moraju biti sadržane prilikom izrade politike sigurnosnih kopija.
- Periodična provjera sigurnosnih kopija - iz razloga što mediji i pripadajući hardver mogu biti veoma nepouzdani potrebno je periodički provoditi testiranja koja se odnose na njihovu ispravnost. Velika količina podataka pohranjenih na trakama ili disketama je beskorisna ukoliko se ne mogu pročitati s istih. U tu svrhu potrebno je periodično provjeravati ispravnost sigurnosnih kopija.
- Čuvanje starih verzija sigurnosnih kopija - nekad je potrebno izvjesno vrijeme kako bi se utvrdilo da je neka datoteka uništena ili pobrisana. Zbog takvih slučajeva uvijek je potrebno čuvati stare verzije sigurnosnih kopija izvjesno vrijeme ili onoliko koliko nalaže zakon. Moguće je čuvati tjedne, mjesečne, polugodišnje ili godišnje verzije sigurnosnih kopija. Preporuča se stare kopije čuvati na različitoj lokaciji od one na kojoj su podaci.
- Provjera datotečnog sustava prije izrade sigurnosnih kopija - ukoliko se radi o povratku podataka sustava koji je prethodno uništen onda je sigurnosna kopija beskorisna. Preporuča se prije izrade sigurnosne kopije provjeravanje integriteta datotečnog sustava.

- Provjera da se datoteka ne koristi tijekom stvaranja sigurnosnog zapisa - ukoliko se datoteka koristi prilikom izrade sigurnosne kopije ona je beskorisna jer ne sadrži ispravnu i važeću verziju.
- Stvaranje sigurnosne kopije prije velikih preinaka u datotečnom sustavu - korisno je imati rezervnu kopiju prije testiranja novog hardvera, popravaka na sustavu ili instalacije novih aplikacija.

3.3. Uobičajeni podaci za koje je potrebno izrađivati sigurnosne kopije

Donošenje odluke o tome za koje podatke je potrebno izrađivati sigurnosne kopije ovisi kako od osobe do osobe tako i od organizacije do organizacije. U osnovi, za sve podatke koje nije jednostavno, lako ili ih uopće nije moguće zamijeniti u slučaju gubitka, treba raditi sigurnosne kopije. U nastavku slijedi popis podataka za koje se preporuča izrada sigurnosnih kopija:

- elektronička pošta,
- bankovni podaci i drugi financijski podaci kao što su npr. ugovori,
- digitalne fotografije
- programi koji su skinuti s Interneta ili kupljeni,
- osobni i organizacijski projekti,
- adresar iz aplikacije za elektroničku poštu,
- kalendar rada, itd…

4. Strategije sigurnosnih kopija

Administratori obično nemaju problema postaviti sigurnosne kopije na čvrsti disk ili traku. Pravi izazov je čuvati vrijedne poslovne informacije o tekućem poslovanju. Bez obzira radilo se o kvaru na disku, nestanku struje ili prirodnoj nepogodi, gubitak podataka je činjenica s kojom se organizacije susreću u svakodnevnom poslovanju. Teža posljedica istog je što se prekida poslovanje, a zakon ili klijent te organizacije u tom slučaju može zahtijevati naknadu za izgubljene podatke. Zbog toga administratori trebaju poduzeti određene akcije u svrhu zaštite informatičkih resursa. U nastavku ovog poglavlja slijedi prikaz nekih od preporučenih strategija.

4.1. Smještanje kopija na trake

Ovo je najstariji postupak smještaja zapisa sigurnosnih kopija. Prednost ovog tipa tehnologije je što su veoma pouzdane i poznate pa time i jeftine, ali su istovremeno spore u radu pa stoga služe kao osnovna platforma za čuvanje podataka. Zbog sporosti se sve češće zamjenjuju diskovnim zapisima.
Tehnologija smještanja podataka na trake omogućava čitanje podataka na svim sličnim sustavima. Postoji više tehnologija u praksi, ali nije moguće čitati zapise stvorene na jednoj tehnologiji na nekoj drugoj. Kao medij traka je izvedena kao savitljiva plastika prekrivena magnetskim medijem i namotana u namotaje. Namotaji se nalaze zaštićeni u plastičnom ovoju čime se sprječava fizičko uništenje trake. Vijek trajanja traka je veoma malen jer postoji fizički kontakt između glave i trake. Preporuča se zamjena traka nakon ciklusa od 2000 čitanja/pisanja. Uređaj koji čita trake je spojen na računalo s kojeg se rade sigurnosne kopije. Način na koji uređaj čita podatke naziva se *helican scan* ili *linear*. U *helican scan* načinu rada rotirajuća magnetna glava je postavljena s obzirom na traku pod kutom i dijagonalno čita podatke s trake. U *linear* načinu rada magnetna glava je fiksno postavljena pred traku koja prolazi preko nje. Postoji više tehnologija koje prate oba pristupa kao što su AIT (eng. *Advanced Intelligent Tape*), DDS (eng. *Digital Data Storage*), DLT (eng. *Digital Linear Tape*), LTO (eng. *Linear Open Tape*) i Travan tehnologija. Izbor trake ovisi o obujmu potrebnog kapaciteta, brzini, troškovima i vijeku trajanja tehnologije.

4.2. Sustavi arhiva sigurnosnih kopija – podatkovni centri

Čak i najnovije tehnologije smještaja zapisa na traku ne osiguravaju dovoljno automatizacije za smještaj podataka. Zbog toga se u radu većih organizacija koriste podatkovni centri u kojima postoji aplikacija koja upravlja trakama, organizira ih u grupe i periodično ih presnimava čime se organizacija osigurava od gubitka podataka. Cijeli proces je često podržan robotskom rukom koja upravlja trakama i cjelokupnom njihovom arhivom. Aplikacije za upravljanje sigurnosnim kopijama su kritične poslovne aplikacije jer pristupaju hardveru za izradu sigurnosnih kopija i pripadajućim medijima sa

zapisima. Često se koriste u velikim podatkovnim centrima gdje bez ljudske intervencije u neradno vrijeme stvaraju sigurnosne kopije.

4.3. Smještaj sigurnosnih kopija na tvrdi disk

Pošto je skoro svako računalo opremljeno tvrdim diskom, logičan izbor za proces stvaranja sigurnosnih kopija je smještaj podataka na isti. Obično se koristi za osobne potrebe ili u manjim sustavima zbog manje cijene i veće brzine od traka. Manje i srednje organizacije koriste smještaj podataka na tvrdi disk jer nemaju vremena da se u neradno vrijeme podaci prebacuju na spore trake, a u radu imaju veliku količinu podataka. U zadnje vrijeme cijene tvrdih diskova se sve više smanjuju na prihvatljive razinu što je još jedan od razloga za korištenje tvrdih diskova u postupku izrade sigurnosnih kopija. Ukoliko dođe do zastoja u radu podaci se vraćaju trenutno ili u roku nekoliko sati dok se pri korištenju traka isti postupak može provesti i do više dana što je za organizacije takve veličine često nedopustivo.

4.4. Stvaranje sigurnosnih kopija u radu

Najjednostavniji postupak stvaranja sigurnosnih kopija je s jednog tvrdog diska na drugi. Ukoliko ima problema u radu jednog diska onda se podaci čuvaju na njegovoj kopiji. Ova tehnologija se naziva zrcaljenje podataka (eng. *mirror*) i primijenjena je u tehnologiji komercijalno nazvanoj RAID (eng. *Redundant Array of Independent Disks*). Ukoliko se kombiniraju tehnologije diskova i traka onda se tehnologija naziva D2D2T (eng. *disc to disc to tape*). Originalni zapis se čuva na traci i presnimljen je na disk koji ima kopiju na drugom disku. Prednost ovog sistema je što je sustav stalno operativan i nema zastoja u radu kad se podaci presnimavaju na traku. Podaci smješteni na traku se mogu poslati na drugu lokaciju s koje mogu biti vraćeni ukoliko postoji zastoj u radu.
U radu se često koristi polje od više diskova koji simuliraju rad traka – tzv. VLT (eng. *Virtual Tape Library*). Tu se radi o načinu rada diskova koji oponašaju datotečni sustav korišten na trakama pa stoga nije potrebo prevođenje podataka prilikom prebacivanja s diska na trake. Time je omogućeno brže stvaranje sigurnosnih kopija i vraćanje podataka pa je na neki način tako riješena mana sporih traka.

4.5. Udaljeno stvaranje sigurnosnih kopija

Jedan od najvećih problema u današnjim organizacijama su udaljeni uredi. Ponekad su poslužitelji na kojima se smještaju podaci smješteni na drugoj lokaciji od operativne lokacije. Često administratori nisu u mogućnosti biti na obje lokacije pa se fizički smještaj medija za pohranu zapisa prepušta drugim osobama. U praksi se najčešće radi o organizacijama u WAN obliku infrastrukture (eng. *wide area network*) – širokopojasna mreža iz koje se podaci distribuiraju u centre za prihvat podataka. U praksi se pojavljuje problem propusnosti mreže. Brza mreža je skupa pa se u praksi koriste tehnike koje premošćuju te zapreke. Jedna od najčešćih je brisanje duplih podataka kojom se uspješno premošćuju probleme propusnosti mreže. Kako bi se osigurao velik broj transfera podataka po mreži koriste se tehnologije ubrzanja aplikacija kao što je WAFS (eng. *Wide Area File Services*). Njegova prednosti je što omogućava tretiranje udaljenih zapisa poput lokalnih jer se u radu koristi tehnikama međuspremnika podataka.
Umjesto da se podaci smještaju na medije, oni se također mogu prenositi i preko interneta. Ukoliko se podaci šalju s jednog računala na drugo radi se o udaljenom stvaranju sigurnosnih kopija. U takvim slučajevima kada se izgubi neki zapis, isti se veoma lako povrati preko interneta. Udaljeno stvaranje sigurnosnih kopija ima i tu prednost što podaci mogu biti dohvaćeni s bilo koje lokacije u svijetu što je korisno za ljude koji putuju ili rade na više lokacija ili pak imaju namjeru da informacije na kojima rade dijele s većim brojem osoba koje se ne nalaze na istoj lokaciji. Postoje dvije varijante udaljenog stvaranja sigurnosnih kopija:

- Pomoću lokalnog programa se stvara sigurnosna kopija i program ju postavlja na udaljeni poslužitelj. Prednost u tome je što se sigurnosna kopija kreira lokalno i prilikom spajanja na internet moguće ju je postaviti na poslužitelj. A ukoliko je veza na internet nedostupna uvijek je moguće vratiti podatke iz zadnje stvorene lokalne kopije.
- Korištenjem udaljenog programa izrađuje se sigurnosna kopija nekih lokalnih podataka. Uobičajeno se koristi sučelje iz kojeg se biraju podaci za koje je potrebno stvoriti sigurnosnu kopiju. Kako se sve odvija na udaljenom poslužitelju, dok se računalo ne spoji na njega nije moguće stvoriti sigurnosnu kopiju niti vratiti podatke iz zadnje sesije. Za razliku od prethodne opcije ova je više korisnički orijentirana jer se uglavnom unos podataka obavlja

putem web aplikacije i time olakšava dijeljenje informacija. Razlika u odnosu na prvu mogućnost je što se sva priprema oko stvaranja sigurnosnih kopija odvija na udaljenom poslužitelju pa u slučaju zastoja u radu nije moguće dohvatiti zadnje sigurnosne kopije.

Prednosti udaljenog stvaranja sigurnosnih kopija preko interneta su:

- jednostavnije je za postaviti i pokrenuti od drugih opcija jer se koriste gotova rješenja,
- nije potrebno kupovati novi hardver, održavati ili popravljati hardver i medije,
- postupak je potpuno automatski što ostavlja višak vremena,
- jednostavno za održavanje,
- nije potrebno brinuti o pohrani i očuvanju medija,
- izostanak vođenja brige o roku trajanja medija i njihovoj obnovi,
- neke aplikacije uz sigurnosne kopije nude i mogućnost sinkronizacije podataka ili udaljeni pristup,
- sve stvorene sigurnosne kopije su dostupne bilo kada u cijelom svijetu i
- svi podaci su kriptirani prije slanja na internet što osigurava visok nivo sigurnosti.

4.6. Druge tehnike stvaranja sigurnosnih kopija

Sigurnosne kopije se uglavnom mogu svrstati u dvije glavne kategorije:

- Potpuna tehnika - sadrži sve zapise koje želimo sačuvati. Obično se radi o više stotina GB podataka i obično je potrebno više vremena za izradu potpunih sigurnosnih kopija, ali je zato jednostavnije i brže iz njih vratiti podatke. U praksi se primjenjuje nakon instalacije operativnog sustava i pomoćnih programa i aplikacija čime je omogućen povratak sustava u prvotno stanje.
- Postupna kopija - sadržava izmjene podataka u nekom periodu od zadnje potpune kopije. U praksi se izvodi svakodnevno. U zapisu se nalaze samo izmjene podataka, no ne i originalni podaci i operativni sustav te služi za povremene kontrole. Obično se koristi u kombinaciji s potpunom tehnikom čime se osigurava kontrola ulaznih podataka i tok njihove izmjene. Potrebno je manje vremena da se učini postupna kopija, ali je teže iz nje vratiti podatke jer je potrebno korištenje potpune kopije.

Slika sustava je postupak da se u određenim vremenskim periodima provodi *backup* cijelog sustava i ukoliko se radi o problemu u radu vraća se zadnje snimljeno stanje. Ovaj postupak je koristan ukoliko se provode promjene u sustavu nakon čega nije moguće normalno obavljanje procesa pa se vraća zadnje snimljeno stanje (npr. kod testiranja nekog virusa). Obično se koristi u manjim sustavima ili kod kućnih korisnika jer ukoliko se radi o većim sustavima bilo bi potrebno mnogo vremena da se obavi potpuno stvaranje sigurnosne kopije.

Sigurnost je također važna kod stvaranja sigurnosnih kopija. Organizacije u svojim podacima sadrže mnoge informacije koje mogu biti klasificirane kao poslovna tajna pa se prema medijima treba prikladno odnositi. Potrebno je obratiti posebnu pažnju prema podacima. Jedan od najsigurnijih načina zaštite podataka je enkripcija. Kriptirani podaci se ne mogu čitati bez pripadajućeg ključa, jer bez njega nije moguće prikazati podatke u originalnom obliku te su kriptirani neovlaštenim osobama potpuno neupotrebljivi.

Zanimljiv postupak izrade sigurnosnih kopija je i CVS (eng. *Concurrent Version System*). CVS sustavi se najčešće koriste kad više korisnika rade na istim datotekama. CVS registrira svaku verziju koju svaki korisnik promjeni. Stoga za jednu datoteku postoji pregled svih prethodnih inačica te iste datoteke. CVS podržava rad na udaljenom poslužitelju i na lokalnom računalu. Sam postupak je potpuno automatiziran i njime je omogućena sinkronizacija i izbjegavanje konflikata što je korisno ukoliko se radi o repozitoriju više projekata. Sam pristup je omogućen kao anoniman, korisnički, ili putem web aplikacije.

5. Politike sigurnosnih kopija

Politike sigurnosnih kopija imaju namjeru da jednoznačno u cijeloj organizaciji definiraju načine postupanja prema podacima, načine izrade sigurnosnih kopija te vraćanja podataka u slučaju određenih gubitaka. Rizik koji se odnosi prema informacijama određuje svaki korisnik zasebno, a učestalost izvođenja izrade sigurnosnih kopija se određuje u skladu s važnošću informacija i pripadajućim rizikom. Postupak izrade sigurnosnih kopija i vraćanje podataka treba biti dokumentiran u obliku procedure i primjenjiv u svim dijelovima organizacije.

Što se tiče fizičkog smještaja medija potrebno je da se na isti primjenjuju što je moguće viši nivoi zaštite. Politika sigurnosnih kopija nalaže da se u određenim vremenskim periodima provjeri i testira vraćanje podataka s medija. Mediji trebaju biti na odgovarajući način označeni što podrazumijeva da sadrže sistemsko ime, datum stvaranja, klasifikaciju važnosti podataka i kontaktne informacije. Ukoliko se ne pridržava navedenih procedura politika propisuje i odgovarajuće disciplinske akcije. Ogledni primjerci politika sigurnosnih kopija sadržavaju stavke:

- svi podaci se tretiraju kao povjerljivi i tajni od strane korisnika i činjenica da su snimljeni u elektroničkom obliku ne sprječava da se prema njima ne odnosi kao prema povjerljivim i tajnim,
- podaci su vlasništvo organizacije i ukoliko korisnik napušta istu potrebno je organizaciji prepustiti sva prava na podatke,
- dio organizacije koji ima vlasništvo na proces izrade sigurnosnih kopija mora poduzeti odgovarajuće korake kako bi se osigurao integritet podataka i sigurnost svih aplikacija i podataka generiranih njima,
- nadležna služba mora omogućiti adekvatnu kontrolu pristupa podacima na sigurnosnim kopijama i nadgledati sustav u smislu ispravnog korištenja. Pristup mora biti prikladno dokumentiran, autoriziran i kontroliran,
- svi odjeli unutar organizacije moraju imaju planove kontinuiranog odvijanja poslovanja u skladu s pripadajućim rizicima i poslovnih zahtjevima (ovo podrazumijeva redovito testiranje vraćanja podataka),
- svi ugovori, licence i slično trebaju imati odgovarajuće sigurnosne kopije s ciljem povećanja opće sigurnosti sustava organizacije,
- svi sustavi koji se nalaze izvan organizacije moraju biti nadgledati od strane organizacije i na njih se primjenjuju politike sigurnosnih kopija kao i u samoj organizaciji, itd…

6. Zaključak

Procesom stvaranja sigurnosnih kopija i povratom podataka smanjuju se rizici kojima je izložen informacijski sustav. Redovit i pouzdan postupak izrade sigurnosnih kopija je postupak koji se ne smije izbjeći. Bez obzira kako se tretira sustav ne mogu se izbjeći rizici od neželjenih posljedica. Rizici su obično veći nego su ljudi to sposobni shvatiti, a prema podacima se treba odnositi ozbiljno prije nego se osjete posljedice gubljenja istih. Po statistici 90% organizacija propada ako izgube vitalne zapise što pokazuje koliko su moderne organizacije ovisne o informacijskoj podršci.

Jedan od nedostataka izrade sigurnosnih kopija je cijena. Naime, proces uključuje odgovarajuće medije, opremu na kojoj se pohranjuju informacije, zaposlenike koji su zaduženi za održavanje sigurnosnih kopija i primjenu politike izrade sigurnosnih kopija, a to organizacijama uzrokuje troškove bez jasno vidljivih rezultata. Ipak, dugoročno gledano ta cijena je zanemariva u odnosu na cijenu koju može platiti tvrtka ili pojedinac ukoliko nije u stanju obavljati posao.

Dodatan problem koji je moguć kod organizacija koje provode politiku izrade sigurnosnih kopija je otpor zaposlenika. Zaposlenici često sam postupak izrade sigurnosnih kopija smatraju bespotrebnim jer nisu svjesni važnosti sigurnosnih kopija za cijelu organizaciju.

Ipak svi su ovi potencijalni nedostaci izrade sigurnosnih kopija zanemarivi u odnosu na mogućnost prekida poslovanja i propadanja organizacije u slučaju izostanka podataka. Stoga je podatke potrebno adekvatno zaštiti, a jedan od neophodnih načina je i izradom sigurnosnih kopija.

7. Reference

[1] Backup Tutorial, http://www.datamills.com/Tutorials/backup_tutorial_Index.htm
[2[Tape Storage, http://www.pctechguide.com/35Tape.htm
[3] Backup And Recovery – Overview, http://www.tcd.ie/ITSecurity/backup/index.php
[4] Brief Overview of Online Backup, http://free-backup.info/brief-overview-of-online-backup.html
[5] S. J. Bigelow: Backup overview,
http://searchstorage.techtarget.com/originalContent/0,289142,sid5_gci1165511,00.html
[6] Backup Security, http://infosecurity.utpa.edu/Policies/backup_security_policy.html