Säkerhetskopiering

Örjan Lundberg – programmet för Data och Systemvetenskap, Luleå tekniska universitet
lundberg@home.se

ABSTRAKT

Att ta säkerhets kopior av viktiga data är en vanlig och ofta underskattad sysselsättning som en systemadministratör brukar ha ansvaret för. Tyvärr så underskattas ofta kostnaderna för dataförlust av ledningen och insikten att hanteringen av säkerhetskopieringen borde ha fått en högre prioritet (och därmed ett större ekonomiskt stöd) fås ofta först efter en katastrof har inträffat. I denna rapport försöker författaren ge systemadministratören en grund att stå på när denne skall ta fram en säkerhetskopieringsplan.

Inledning

Säkerhetskopierng[1] är en av de viktigaste uppgifter en systemadministratör ställs inför. Dock anses denna uppgift vara tråkigt och enformigt. Men oberoende av detta så är ett tillförlitligt rutin för säkerhetskopiering oerhört viktig. Om inte en sådan finns så kan företagets framtid, företagets kundrelationer eller systemadministratörens egen karriär vara i fara.

Större företag särskilt då dem med samhällskritiska[2] system har länge varit införstådda med hur viktigt det är att använda sig av kvalitetsäkrade och systematiska rutiner för att sköta säkerhetskopieringen. Deras rutiner bygger ofta på att data som genereras under dagen lagras på feltoleranta[3] enheter för att på arbetsdagens slut förflyttas till en säkerhetskopia på annan ort. Verktyg för att hantera säkerhetskopieringen på ett enkelt sätt finns idag till en överskådlig kostnad, vilket för att de flesta organisationer bör inse nyttan med att införskaffa och underhålla en pålitlig säkerhetskopieringsplan.

Säkerhetskopiering är i sig bara del av det säkerhetsarbete som ett modernt företag måste hålla sig med. Vid sidan av stöldlarm, brandlarm och vakter kan dock säkerhetskopiering vara en billig ”sista utväg” när en katastrof inträffat. Data som lagas i datoriserade system är både ömtåliga och lätta att säkerhetskopiera. Dra här själv parallellen till att säkerhetskopiera 100’000 A4 ark mot att kopiera innehållet på en diskett!

[1] Säkerhetskopia/reservkopia - kopia av fil eller andra data som sparas för att användas om originalet blir förstört Använd säkerhetskopia för det engelska substantivet backup eller backup copy. För det engelska verbet backup används säkerhetskopiera.[Svenska datatermgruppen]
[2] T.ex. banker, försäkringsbolag eller sjukhus
[3] T.ex. hårddiskar som speglats, dvs att data alltid lagras på två platser. På detta sätt kan inte en enskild komponent orsaka driftstörningar. Detta anses dock i sin tur öka komplexiteten i systemet, dvs svårt att överblicka, övervaka och felsöka. (se gärna "Driftstörningar i IT-system" , S. Axelsson & L. Johanssons, (1996), D-uppsats, LTU/DSV)

Bakgrund

I kursen IEA335 - Operativ datordrift 10p ingår ett större arbete inom ämnet system-administration. Det egna arbetet skall vara en fördjupning inom valfritt område av operativ datordrift

Syfte

Syftet med arbetet är att fördjupa mig inom den teori som beskriver säkerhetskopiering. Säkerhetskopiering är en arbetsuppgift som ofta utförs av personal anställda som ”systemadministratörer” och ingår därför i ämnet operativ datordrift.

Genomförande

Rapporten skapas utifrån kritisk granskning av material som insamlas m h a sökning på www samt den kursdokumentation som tillhandahållits.

Avgränsningar

Med säkerhetskopiering avser författaren redundant lagring av data som inte är direkt åtkomstbara, det vill säga att vissa arbetsmoment måste ske för att återställa data som förstörts. Detta innebär att redundanta lagringsmedier som RAID enheter ej direkt kommer att innefattas i rapporten.

Fokus i rapporten kommer att vara generella punkter som förts fram i den refererade litteraturen.

Mål med säkerhetskopiering

Oavsett vilken typ av arbetsplats man befinner sig på gäller samma huvudmål för säkerhetskopiering, nämligen:

- Att minimera dataförlusten
- Att minimera de resurser som krävs för att utföra säkerhetskopieringen
- Att minimera de resurser som krävs för att återställa data vid förlust
- Att maximera systemets tillförlitlighet
- Att maximera systemets förutsägbarhet
- Att maximera systemets flexibilitet

Dessa mål beskrivs mer detaljerat i rapporten ”Analysing Backup Systems” av Elizabeth D. Zwicky [Zwicky].

Hotbild

Datorsystem speciellt lagringsenheter (t.ex. hårddiskar) går undantagslöst sönder någon gång och detta leder ofta till att viktiga dokument försvinner.

Datan hotas dock från flera andra saker som t.ex.:

- Användarfel
- Brand
- Översvämning
- Åsknedslag
- Datorvirus
- Störningar i kraftsystemen
- Krig (infologiskt och traditionellt)
- EMP
- Mjukvarufel (buggar)
- Hårdvarufel
- Stöld
- Terrorism
- Glömska
- Vandalism

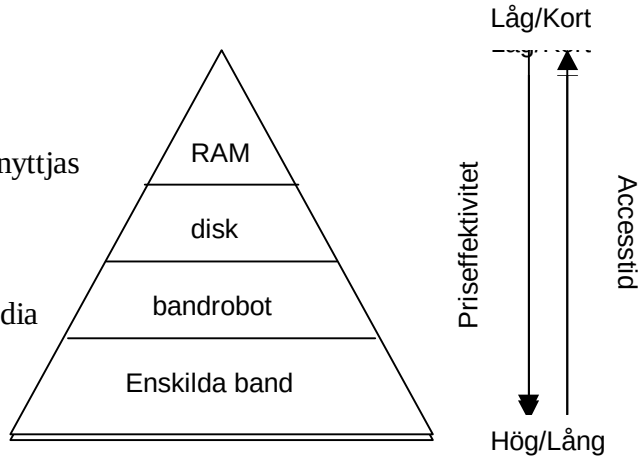
Viktigt att tänka på är att inte bara datan som hotas utan också lagringsmediat som säkerhetskopiorna ligger på. På samma sätt som datorer kan lagringsmediat förstöras av brand eller stjälas. Om man inte skyddar säkerhetskopiorna har man inte stor nytta av dem när en katastrof sker.

Hur kan säkerhetskopiering skydda mot dessa hot?

Med hjälp av säkerhetskopior kan man (bland annat):

- Verifiera systemets intrigitet
  – dvs undersöka om filer har förändrats (otillbörligt)
- Lagra flera versioner av dokument
  - så att korrupta data kan återtas från en äldre version
- Återta hela eller delar av filsystemen vid dataförlust
- Skydda bevis vid databrott[4]

Dessutom kan man genom loggning av säkerhetskopieringen upptäcka om resurser utnyttjas dåligt och då kanske flytta oanvända data till arkiveringskopior[5] så att dyrare medier kan användas till material som används dagligen. Kostnadsförhållandet mellan olika typer av media kan visualiseras med följande figur:



figur 1, förhållande mellan accesstid och priseffektivitet (källa: comp.arch.storage FAQ)

Detta är inte de enda variablerna man bör tänka på när man skall välja teknik för säkerhetskopiering. Några andra variabler kan ses i tabell 1, värdena är endast exempel:

	Media				
	Floppy Disk	Hård Disk	Band	CD-R	Dubblerat system
Initial kostnad	Låg	Hög	Medel	Medel	Hög
Långsiktig kostnad	Låg	Låg	Medel	Medel	Hög
Kopierings hastighet	Låg	M.Snabb	Medel	Snabb	Snabb
Återtagningshastighet	Låg	M.Snabb	Låg	Snabb	Direkt
Bekvämlighet	Låg	Hög	Medel	Medel	Hög
Enkelhet	Medel	Lätt	Lätt	Lätt	Medel
Tillgänglighet	Medel	Hög	Medel	Medel	Hög
Portabilitet	Hög	Låg	Hög	Hög	Ingen
Robusthet	Låg	Låg	Medel	Hög	Medel

tabell 1, jämförelse av olika lagringsmedier (källa: comp.arch.storage FAQ)

[4] Kräver krypografisk signering för att kunna användas som bevis vid brottsmål
[5] Arkivering och säkerhetskopiering bör särskiljas eftersom deras mål ej är desamma.

Typer av säkerhetskopiering

Säkerhetskopiering kan delas in i två huvudtyper nämligen lokala och nätverksbaserade (centraliserade). Den lokala typen är när varje dator har en egen enhet för säkerhetskopiering. Denna typ fungerar bäst i mindre organisationer. I nätverksbaserade säkerhetskopieringsystem delar flera datorer på en enhet. Den dator som tillhandahåller enheten kallas då server. Denna typ passar större organisationer bäst.

Fördelar med lokal säkerhetskopiering

- Mjuk och hårdvara är oftast billig
- En enhet kan flyttas mellan flera olika datorer
- Enkel miljö, inga krångliga säkerhetsrutiner
- Redundans, flera likadana säkerhetskopieringstationer kan användas vilket gör att alla kan läsa varandras band

Nackdelar med lokal säkerhetskopiering

- Användare har ansvaret, kan glömma att utföra säkerhetskopieringen
- Administration av media blir svår
- Scheman blir svåra att upprätthålla och kontrollera ju större organisationen är

Fördelar med serverbaserad säkerhetskopiering

- Servern måste ej stå i samma byggnad (stad, land) som klienterna
- Säkerhetskopieringen kan lättare automatiseras
- Central revision och övervakning förenklas
- Varningsystem kan varna användare och administratörer vid problem

Nackdelar med serverbaserad säkerhetskopiering

- Nätverksresurser belastas kraftigt under säkerhetskopieringarna
- Programvaror är generellt dyrare
- Mängderna data blir stora, utrustningen har ofta ett högt inköpspris
- Man blir beroende av serverdatorn och nätverket för att kunna återskapa data
- Det kan vara svårare att återställa en dator som har totalförstörts

Lagring av media

Hur man lagrar mediet är en viktig frågeställning som måste tänkas genom noggrant. Band bör t.ex. lagras i en utrymme där temperaturen hålls mellan 20°C och 22°C samt där fuktighets graden är mellan 40% till 60%[Coutu]. Om inte dessa krav uppfylls finns det risk för att data förvanskas. Vidare bör man lagra säkerhetskopiorna på en plats som är skild från det man tar säkerhetskopior på. Dvs att man ej lagrar säkerhetskopian i samma byggnad eftersom en brand då skulle kunna skada både kopian och originalet. Sådan extern lagring är ofta dyr och innebär extra åtgärder. Robert Coutu ger i sin artikelserie ”*The security of backup copies*” ett exempel på kategorisering av data som kan användas för att bestämma vilken data som skall förvaras på annan ort.

Coutu delar in mediet i tre kategorier. Nivåerna är baserade på hur viktiga data man lagrar.

Typ 1

Media som innehåller data som är kritiska för organisationens fortlevnad. Media som innehåller konfidentiella data hör också hit. Dessa måste förvaras under rigorösa säkerhets villkor. T.ex. i ett bankvalv som är garanteras säkert för de flesta naturkatastrofer och har en hög internationell säkerhetsklassning.

Typ 2

Media som måste förvaras på en annan plats för att förhindra att skada uppstår samtidigt som originalen. Dock krävs ingen speciellt säkerhetskydd.

Typ 3

Media som inte kräver förvaring på annan ort, eftersom de ej innehåller viktiga data.

Klassificering

Det är svårt att klassificera data efter en sådan mall men det är ändå systemadministratörens uppgift att se till att sådan sker. Viktigt är också att låta användarna av datan vara med och säga vad det anser är viktigt för dem.

Val av lagerplats

Detaljer man skall fundera på när man väljer en förvaringsplats för säkerhetskopior är:

- Konstruktion och förhållanden i förvaringsplatsen
  Säkerhetsvalv bör vara placerade ovan jord (för att undvika översvämmningar), och bestå av minst 32cm tjocka väggar av betong.

- Säkerhetsnivån/Konfidentiellitet
  Se till att leverantören av lagringsplatsen har minst lika höga krav som din egen arbetsplats.

- Lager och inventariehantering
  Har leverantören ett bra administrativt system för att märka inventarierna?

- Avstånd (från platsen du befinner dig på)
  Ligger lagret nog långt borta för att klara en större katastrof? (oversvämmning/explosion)
  Hur lång tid tar det att forsla mediet från lagringsplatsen vid behov?

- Tilläggstjänster
  Erbjuder leverantören transporttjänster, destruktion av band, inventering eller kloning av mediet?

- Kostnader

Att införa en säkerhetskopieringsplan

Att införa en säkerhetskopierings plan i en organisation kräver som alla andra omorganisationer och förändringar en tydlig och väl motiverad plan för att lyckas. Jody Schivley Leber tar i sin rapport ”Choosing a Backup Environment” upp följande stadier för att lyckas med en säkerhetskopieringsplan, stadierna är på varandra följande och utnyttjar de tidigare stadierna för att sammanställa en helhetslösning [Leber].

1. Kravspecifikation
   Man måste innan man gör något annat ställa upp vilka krav som gäller för organisationens säkerhetskopiering. Det vill säga:
   - vilka data som är viktiga
   – hur mycket data som skall säkerhetskopieras
   – hur stor ökning av datamängden som kan väntas de närmaste åren
   – vilka krav som ställs på prestanda och säkerhet
   – vilka datormiljöer som måste kunna stödjas
   – vilken är hotbilden
     - har katastrofer, sabotage skett tidigare?
     - har organisationen råd med ”negativ” PR?

2. Policy och politik
   Viktigt är att skapa dokument som beskriver:
   - säkerhetspolicy
   – policyförklaring för säkerhetskopiering
   - ansvarsskyldighet
   - planering av utbildning
   – debiteringsplan

   Detta alltså utifrån kravspecifikationen. Detta är viktigt eftersom det kan uppstå organisatoriska problem om inte sådana dokument finns och tydligt markerar ledningens ställning i frågan.

3. Val av mjukvara
   Selektering av mjukvara som stöder kravspecifikation och policyförklaringar. T.ex. kanske mjukvaran måste stödja kryptering.

4. Val av hårdvara
   Selektering av hårdvara som uppfyller de tidigare ställda kraven på funktion och kapacitet.

5. Testning
   Utvärdering av valen som gjordes i stadierna (4) och (5) gentemot kravspecifikationen. Genom att testa hård och mjukvaran kan man få en bättre bild över vilka olika kombinationer som kan ge önskat resultat. Nya problem dyker upp och man kan skaffa sig en bättre bild över om kravspecifikationen är riktigt skriven. Eftersom systemutveckling är en iterativ process kan det nu vara lägligt att återgå till stadie 1 om man upptäcker att fel val har gjorts. Genom testning kan man också lära sig väldigt mycket om vilka rutiner och procedurer som måste utvecklas för att systemed skall fungera i just din organisations driftsmiljö. Det är viktigt att testning och integration inte sker i samma stadie eftersom målet för testning är att utvärdera men målet för integration är att väva in säkerhetskopieringsystemet i din produktionsmiljö.

6. Integration
   Efter testning har genomförts är det dags att integrera hård och mjukvaran i den organisation du arbetar i. Detta kan kräva att produkten måste modifieras för att passa dina krav.

7. Drift och administration (förvaltning)
   Administration och förändring av säkerhetskopieringsystemet kommer att behövas under hela dess livstid. Denna förvaltning tar olika mycket tid i anspråk beroende på hur stort och komplicerat ditt system är. Detta stadie innehåller alltså allt som krävs för att hålla ditt säkerhetskopieringsystem dugligt. Det är viktigt att förstå att ett säkerhetskopieringsystem inte bara kan tas i drift utan kräver administration och övervakning för att vara tillförlitliga.

Skapa ett säkerhetskopierings schema/rutin

Det bästa sättet att se till att säkerhetskopiering sker konsekvent och i rätt tid (under stadie 7) är att fastställa ett schema. Ett bra säkerhetskopierings bör förenkla hanterandet av säkerhetskopieringen för administratören. Därför är det viktigt att hålla det enkelt. Frågeställningar man bör ställa sig själv är:

- Vilka data måste säkerhetskopieras?
  – Idealt skulle allting på alla system säkerhetskopieras, men mängden data som lagras i dagens arbetsstationer har de senaste åren ökat avsevärt. Det är inte ovanligt att en ordinär PC idag har en lagringskapacitet på 1-2Gb. I och med att användningen av nätverk (t.ex. Internet) har användningen av lagringsutrymmet också ökat. Detta därför att det nu är mycket enklare att överföra data mellan varandra.
  – Det är därför viktigt att klassificera datan och kanske sätta en prislapp på den. Detta kan göras genom att fråga sig hur mycket det skulle vara värt/kosta dig att få tillbaka datan om den skulle försvinna.

- Vem skall genomföra / vara ansvarig för att säkerhetskopieringen sköts?
  – Detta innefattar att bedöma hur stort ansvar för säkerhetskopiorna som systemadministratören har samt hur stort ansvar användarna har att se till att säkerhetskopiera sina egna data.

- Var, när och hur skall säkerhetskopieringen ske?
  Vilka system skall användas? Vilken tid på dagen är bäst?

- Hur ofta förändras filerna som skall säkerhetskopieras?

- Hur snabbt måste datan kunna återställas?

- Vilka data är konfidentiella och måste t.ex. krypteras för att kunna lagras på band?

- Var skall datan återställas? Av vem? Hur mycket skall det kosta att återställa filer?

Dokumentation av rutiner

"*Arnold's Laws of Documentation:*

1.) If it should exist, it doesn't.

2.) If it does exist, it's out of date.

3.) Only documentation for useless programs transcends the first two laws."

-- fortune(1)

Dokumentation av rutiner vid säkerhetskopiering bör vara en självklarhet. Vid en katastrof måste allt arbete med säkerhetskopiering fungera smärtfritt. Viktigt är också att det finns flera personer i organisationen som kan ta sig an arbetet så att organisationen ej är beroende av en nyckelperson. Nedan följer en enkel mall för hur en rutin kan se ut:

- Allmänt
  – Vad, När, Hur, Varför skall säkerhetskopior tas, testas, verifieras.

- Dokumentation
  - hur sker förändringar i rutiner
  – vem skall godkänna, verifiera
  – vem skall meddelas vid förändring
  – var finns dokumentet
  – vem får ta del av dokumentet

- Beräknad skada/Klassificering av data

- Dokumentation av
  - programvara
  – hårdvara
  – media
  – referenser till manualer

- Scheman

- Hur sker säkerhetskopiering

- Hur sker återtagande

Analysera din säkerhetskopieringslösning

När ditt säkerhetskopieringsystem är färdigställt bör du ställa dig följande frågor [Zwicky:OH]:

- Är alla filer som är av intresse för användarna säkerhetskopierade?
- Är alla systemkonfigurations filer lagrade i flera versioner så att det är enkelt att gå tillbaka till en tidigare konfiguration?
- Vet användarna vilka filer som säkerhetskopieras och vilka som inte säkerhetskopieras?
- Finns det fler än en person som förstår säkerhetskopieringssystemet?
- Sker säkerhetskopiering automatiskt och konsekvent?
- Är återföringsproceduren förstådd och använd (testad)?
- Är säkerhetskopiorna lagrade på en säker plats?
- Går rätt säkerhetskopia att hitta snabbt?
- Finns det en plan för att återställa verksamhetskritiska dator funktioner vid en katastrof?
- Revideras säkerhetskopieringssystemet externt och inte av de som har skapat det?
- Hur överensstämmer din säkerhetskopieringslösning med målen:
  - Att minimera dataförlusten: Sker säkerhetskopieringen tillräckligt ofta?
  - Att minimera de resurser som krävs för att utföra säkerhetskopieringen
    Är all hantering av säkerhetskopiorna rutiner/automatiserade?
  - Att minimera de resurser som krävs för att återställa data vid förlust
    Är denna hantering dokumenterad/automatiserad?
  - Att maximera systemets tillförlitlighet
    Verifieras säkerhetskopiorna när de är klara?
    Finns det redundanta kopior (flera av varje)?
    Finns det automatiska kontroller som undersöker om säkerhetskopieringen har fungerat?
    Sköts säkerhetskopieringen automatiskt?
  - Att maximera systemets förutsägbarhet
    Känner du till under vilka förhållanden systemet kommer att fungera eller inte fungera?
  - Att maximera systemets flexibilitet
    Finns det spelrum i resursutnyttjandet?
    Finns det reservplaner om säkerhetskopieringssystemet skulle haverera?

Slutsats

Säkerhetskopiering är ett allvarligt och komplext arbete som tar stora mängder mantimmar om resultatet skall hålla en hög kvalitetsnivå. Ett system för att utföra detta är inte något du kan

köpa på hyllan eller sätta ihop för att sedan låta det ”rulla på”. Att implementera en plan för säkerhetskopiering är ett fortgående arbete. Planens mål och utförande måste förändras tillsammans med organisationen som den ”lever” i för att kunna fungera effektivt. Genom att ställa upp en plan och dokumentera arbetet kan man lättare få ledningens stöd, då man kan visa på kostnader både för det pågående arbetet samt troliga förluster vid en katastrof.

Referenser

[Svenska datatermgruppen]

Svenska datatermgruppen, http://www.nada.kth.se/dataterm/, 18 oktober 1997

[comp.arch.storage FAQ]

comp.arch.storage FAQ, http://alumni.caltech.edu/~rdv/comp-arch-storage/FAQ-1.html, 20 oktober 1997

[Coutu]

Robert Coutu, (1996), ”The security of backup copies”, http://www.ocaq.qc.ca/bilan/bilan_96 , 20 oktober 1997

[Zwicky]

Elizabeth D. Zwicky, (1993), ”Analysing Backup Systems”, SRI International

[Zwicky:OH]

Elizabeth D. Zwicky, (1993), ”Are we there yet? Evaluating your site’s system administration”, The Ninth Systems Administration Conference (LISA '95)

[Leber]

Jody Schivley Leber, (1997), ”Choosing a Backup Environment”, Lehman Brothers. Inc, http://www.usenix.org/publications/library/proceedings/nt-sysadmin97/schivley.html , 21 oktober 1997