

# **Snabblektion i katastrofberedskap för datordrift**



**Jan G. Sternudd**  
**Sternudd Consulting AB**

# Snabblektion i katastrofberedskap för datordrift

Utgåva 2.1 (Oktober 2008)

Författaren, **Jan G. Sternudd**, är civilingenjör och organisationskonsult med katastrofberedskap för företag och IT-enheter som specialitet. Han är sedan 1983 verksam i det egna företaget, **Sternudd Consulting AB**. Innan dess arbetade han tjugo år inom alla grenar av IT – systemutveckling, teknikstöd och datordrift – större delen av tiden i chefsbefattningar inom IBM.



Jan Sternudd är också författare till handboken och planeringsverktyget **Katastrofberedskap för datordrift**. Huvuddelen av denna handbok består av ett antal detaljerade *mallar till katastrofplaner*. Planerna är skrivna i “orderform” för en fingerad datoranläggning. De är därför konkreta, åtgärdsinriktade och rakt på sak. Anpassningar till en enskild datorinstallation och dess speciella förhållanden gör man genom ändringar, tillägg och strykningar.

Dessa mallar ingår:

- ➔ Policy för katastrofberedskap
- ➔ Åtgärder vid katastrof
- ➔ Plan för säkerhetsarkivering
- ➔ Plan för underhåll av katastrofberedskapen
- ➔ Plan för katastroftester
- ➔ Larminstruktion för datordriftspersonal

För att ytterligare underlätta arbetet med att bygga upp en fungerande katastrofberedskap finns i handboken också en *projekthandledning*. Denna ger förslag till projektorganisation, arbetsmetoder, projektaktiviteter och milstolpar. Det finns också en projektöversikt i form av Gantt-diagram. Handledningen beskriver steg för steg vad som behöver göras.

**Katastrofberedskap för datordrift** levereras i form av ett kompendium (ca 230 sidor) och en PC-diskett med *projekthandledning* och *mallar till katastrofplaner* som dokument för **Microsoft® Word for Windows® version 2003** och senare.

I priset för handboken ingår också rättigheten att använda och modifiera det elektroniska materialet för att utarbeta katastrofplaner för en enstaka datorinstallation, datacentral eller annan anläggning.

**Katastrofberedskap för företag** är en nedbantad version av ovan nämnda handbok. Den är tänkt för *en hel arbetsplats* i ett företag eller organisation. IT-verksamheten antas i första hand vara baserad på persondatorer, med ett LAN och en eller ett fåtal nätverkservrar. Platsledningen nöjer sig inte med en godtagbar katastrofberedskap enbart för själva datordriften, utan vill ha en dokumenterad krisplan för hela eller den prioriterade delen av verksamheten.

Båda handböckerna finns också i engelska versioner.

Läs mer på [www.sternudd.se](http://www.sternudd.se).

# Snabblektion i katastrofberedskap för datordrift

---

## Begreppet *katastrof* inom IT

Med *katastrof* inom IT-verksamheten i en organisation avses en så allvarlig störning eller skada inom datordrift eller tillhörande stödverksamhet att produktionen av IT-enhetens tjänster väsentligt inskränks. Riskerna för allvarliga störningar hos enskilda, interna enheter, hos kunder eller i samhället som helhet bedöms som överhängande.

Godtagbar service kan ej heller återupptas inom rimlig tid på ordinarie anläggning, utan verksamheten måste föras över till en reservanläggning. Vad som är rimlig tid beror på vilken del av tjänsteutbudet som drabbats, men torde för många IT-enheter röra sig om högst något eller några dygn, i värsta fall bara några minuter eller timmar.

Avbrottet kan vara förorsakat av t.ex. brand, explosion, omfattande vattenläckage, långvarigt strömavbrott eller utsläpp av farliga kemikalier. Berörda anläggningar kan vara mer eller mindre skadade, eller oskadade men avspärrade. Skadorna kan ha uppkommit genom olyckshändelse (oavsiktlig åverkan) eller genom sabotage eller terrorism (avsiktlig åverkan).

## Kvardröjande brister

Många företag eller andra organisationer har i dag arbetat systematiskt med planering av katastrofskyddet för IT-verksamheten under flera decennier eller mer. Först ut var oftast banker, andra finansinstitut och försäkringsbolag, med andra ord institutioner med ett extremt beroende av att kassaflödet inte stoppas upp.

Andra har mer motvilligt följt efter. Trots det omfattande och seriösa arbete som lagts ner, har katastrofberedskapen inom många IT-enheter fortfarande brister som inte bara är obetydliga.

Många har inte ens gjort en första risk- och konsekvensanalys för att klara ut vilket behov av katastrofberedskap som egentligen föreligger. Oftast gäller detta de mindre IT-enheterna.

## Omfattande arbete som kräver specialkunskaper

En av orsakerna till denna motvilja kan vara att det är ett förhållandevis omfattande arbete att ta fram och underhålla en katastrofplan för datordriften och att vidta de övriga mått och steg som krävs för en godtagbar katastrofberedskap. Dessutom krävs en specialistkompetens som ofta saknas inom den egna organisationen. Samtidigt är ju oftast personresurserna hårt ansträngda. De dagliga problemen tar överhanden; planering av katastrofskyddet känns inte så viktigt. Inte förrän den dag olyckan är framme . . .

I de efterföljande avsnitten kommer jag att ta upp en del frågor som jag anser att man måste ge sig i kast med, när man bestämmer sig för att skaffa sig och sin IT-enhet en acceptabel katastrofberedskap. De ämnesområden som jag kommer att beröra:

- Målformulering
- Säkerhetsarkivering och rekonstruktion efter katastrof
- Åtgärder vid katastrof
- Att vidmakthålla katastrofberedskapen
- Planering av katastrofskyddet – egentligen en del av systemutvecklingsarbetet!

Vårt ökande beroende av informationsteknik i det moderna samhället medför att konsekvenserna vid störningar i datorproduktionen undan för undan växer i praktiskt taget alla organisationer. För att öka säkerheten utformas därför, inom ramen för den normala driften, vissa grundläggande skyddsåtgärder. Trots detta grundskydd kan dock allvarliga driftavbrott inträffa. Det är här katastrofskyddet kommer in i bilden. Detta inriktas på *extraordinära* situationer som inte kan bemästras inom normal organisation och med normala resurser. Trots vidtagna preventiva skyddsåtgärder inom ramen för grundskyddet är en stor skada ett faktum och dess effekter måste lindras.

## Riskavvägning

Men att upprätthålla en viss katastrofberedskap kostar pengar. Planer skall tas fram, reservutrustning skall anskaffas eller kontrakteras, tester och övningar skall genomföras. Och ju högre skyddsnivå som krävs, t. ex. i form av vilka produktions- och servicenivåer man vill ligga på efter en katastrof, och ju kortare stilleståndstid man kan eller vill acceptera, desto mer förberedelser krävs och desto mer kostar det. Precis som i alla andra verksamheter gäller det då att göra en *riskavvägning*, dvs. att väga nytta mot kostnader och välja en nivå som är acceptabel ur alla aspekter.

## Övergripande målsättning

En IT-enhets övergripande målsättning med katastrofberedskapen skulle kunna se ut som exemplet nedan. Målen är på den här nivån endast kvalitativa och bör naturligtvis brytas ner i konkreta, kvantifierade delmål:

1. Möjliggöra att vi även i en krissituation reagerar systematiskt och organiserat, så att vi kan återuppta produktionen av datatjänster inom rimlig tid, utan förlust av för företaget väsentlig information.
2. Begränsa skador och följskador genom att vi snabbt sätter in åtgärder för röjning samt bärgning och sanering av drabbad utrustning, dokument och lagringsmedier.
3. Säkerställa att företagets eller organisationens kärnverksamhet kan fortsätta. Detta sker genom att vi prioriterar de datatjänster som (a) stödjer våra möjligheter att effektivt betjäna våra kunder och (b) säkerställer vår likviditet och därmed vår betalningsförmåga.

## Längsta acceptabla avbrottstid

Då man bedömer effekterna av ett driftavbrott, bör man som ett minimum också klargöra tidpunkten då effekterna faktiskt antar *katastrofkaraktär*. Denna tidpunkt varierar naturligtvis beroende på tillämpning. Kraven i en processindustri är annorlunda än för ett företags traditionella administrativa rutiner.

Denna *längsta acceptabla avbrottstid* styr i hög grad vilka förberedelser som krävs och därmed sammanhängande kostnader. Jämför t. ex. omfattningen av förberedelser om längsta acceptabla avbrottstid är något dygn eller flera veckor:

- Dygn** Reservutrustning måste finnas installerad och färdig att tas i bruk på egen eller kontrakterad reservanläggning.
- Förberedda reservtelefonförbindelser eller godtagbara offline-baserade alternativ måste finnas.
- Lämpliga tester och övningar måste genomföras minst en gång om året.
- Veckor** Oftast räcker det om datorer, teletjänster eller annan utrustning som behövs för katastrofdrift beställs och installeras vid katastroftillfället.
- Avancerade teletjänster och udda utrustning kan ha lång leveranstid och kan därför behöva förbeställas.
- Om särskild miljöförsörjning krävs, såsom upphöjt golv, el, kyla och brandskydd, måste detta förberedas.
- Inga regelbundna tester krävs, utom att verifiera att nödvändiga säkerhetskopior finns och är läsbara samt att kopiorna är synkroniserade med varandra.

## Skyddsklassning av datatjänster

Alla datatjänster bör skyddsklassas (dvs. prioriteras inbördes), *senast* i samband med produktionsöverlämningen, så att detta inte behöver göras då rekonstruktionsarbetet startas efter en eventuell katastrof.

Till grund för skyddsklassindelningen läggs med fördel *längsta acceptabla avbrottstid*.

## Lägsta acceptabla servicenivå

Av samma skäl som man under katastrofdrift avstår från alla, inte absolut nödvändiga datatjänster, kan man kanske också nöja sig med lägre servicenivåer än under normaldrift.

Exempel på sådana åtgärder är:

- Längre svarstider för realtidssystem
- Färre anslutna terminaler, dvs. användare får samsas om terminaler
- Kortare tider för öppethållande
- Minskad bearbetningsfrekvens för batchapplikationer

## Val av reservrutin och dess omfattning

I de allra flesta fall kostar reservrutiner extra pengar att utveckla och underhålla. Detta gäller vare sig man väljer en manuell eller halvmanuell reservrutin som substitut för datorbearbetningarna under normaldrift eller väljer att fortsätta med en datoriserad katastrofdrift.

Där så är möjligt och försvarbart, bör man därför utforma reservrutinerna med lägre ambitionsnivå än under normaldrift och avstå från alla, inte absolut nödvändiga datatjänster. Merkostnaden för detta anpassningsarbete (om sådant krävs) bör naturligtvis alltid vägas mot merkostnaden för att hålla utrustning i reserv för att kunna köra det kompletta systemet.

# **Säkerhetsarkivering och rekonstruktion efter katastrof**

För att katastrofplanen skall kunna fullföljas måste tillräckligt material för rekonstruktion och återstart finns intakt. Den enda garantin för att så verkligen är fallet, om olycka är framme, är att allt kritiskt material blivit säkerhetsarkiverat eller att det kan återskapas från originalverifikationer inom rimlig tid.

Med **säkerhetsarkivering** avses sålunda arkivering av material, vars primära syfte är att användas vid rekonstruktion efter en katastrof, dvs. då motsvarande ordinarie material skadats eller helt gått förlorat.

Säkerhetsarkivering i erforderlig omfattning är med andra ord grunden i allt katastrofskydd. Det är tämligen meningslöst att lägga ner tid, arbete och pengar på andra åtgärder, om man ändå inte har något material att återstarta ifrån.

## **Krav på lokaler för säkerhetsarkiv**

Det särskilda säkerhetsarkivet byggs som brandsäkert rum, enligt minst samma normer som det ordinarie arbetsarkivet och med tillfredsställande tillträdesskydd.

Säkerhetskopior måste dessutom arkiveras på betryggande avstånd från datorhallar och arbetsarkiv, i annan byggnad och i särskild arkivlokal.

Avståndet skall vara så stort att inte ens en omfattande brand kan sprida sig till säkerhetsarkivet. Ej heller skall en eventuell avspärrning av området kring den ordinarie datacentralens lokaler, efter t. ex. en brand, omöjliggöra användning av materialet i säkerhetsarkivet. I Norden torde 500 meter vara ett minimiavstånd mellan datacentral och säkerhetsarkiv. I andra länder, med risk för exempelvis jordbävningar eller tropiska stormar, handlar det ofta om betydligt större avstånd, ibland även om riktning.

## **Rekonstruktion av förlorad information**

Återskapandet av skadad eller förlorad information efter ett allvarligt driftavbrott (katastrof) måste normalt ske i ett antal rekonstruktionssteg. Dessa steg beskrivs nedan, låt vara att alla steg inte nödvändigtvis kan eller måste genomföras i varje enskilt fall.

Av framställningen nedan torde framgå att ett medvetet beslut bör fattas om hur långt det skall vara möjligt att rekonstruera maskinellt (elektroniskt) och från vilken punkt man därefter tvingas att rekonstruera manuellt genom omregistrering, i värsta fall föregånget av förnyad datainsamling. Detta beslut styr i sin tur ett beslut om säkerhetskopiornas typ, omfattning och frekvens. Några frågor som man bör ställa sig är:

- Finns allegat, i original eller kopia, lätt tillgängliga?
- Hur stora är transaktionsvolymerna?
- Hur lång tid står till förfogande för omregistreringen?
- Finns de maskiner och den personal som krävs, med hänsyn till den tid som står till förfogande?

### **Steg 1: Återställning av grundinformation**

Från säkerhetsarkivet hämtas den yngsta, fullständiga kopian av den aktuella informationsmängden (databasen, huvudregistret eller vilken benämning man nu använder). Denna kopia är av förklarliga skäl oftast inte helt aktuell; åtminstone gäller detta real-

tidssystem. Det finns ett informationsglapp motsvarande alla de transaktioner som datamängden uppdaterats med, från den tidpunkt då kopian togs fram till den tidpunkt då avbrottet inträffade.

Aktualisering av datamängden fram till tidpunkten för avbrottet måste därför oftast göras. Detta kan ske på följande sätt:

### **Steg 2: Uppdatering från central transaktionslogg**

I realtidssystem loggas normalt alla uppdaterande transaktioner i den centrala datorn. I batchapplikationer loggas ofta ingående transaktioner på en särskild transaktionslogg. Alternativt sparas ingående transaktionsmedium (band, diskett eller dylikt).

Fullständig rekonstruktion från centrala transaktionsloggar kan dessvärre inte påräknas i realtidssystem, annat än då loggning fortlöpande sker till enhet på annan ort (s.k. electronic vaulting), exempelvis via kanalförlängarteknik och optisk fiberkabel.

I alla, andra fall kommer ett informationsglapp att kvarstå även om loggarna går till säkerhetsarkiv, vilket ofta inte är fallet.

För batchapplikationer kan fullständig rekonstruktion påräknas om loggen eller det ingående transaktionsregistret hunnit iväg till säkerhetsarkivet innan avbrottet.

### **Steg 3: Uppdatering från distribuerad transaktionslogg**

I ett modernt terminalsystem med distribuerad intelligens, såsom i ett bankterminalsystem, är varje kassaterminal ansluten till en mindre, lokal dator, belägen i anslutning till bankkontoret.

Denna dator står i sin tur i förbindelse med bankens centrala datoranläggning.

En vanlig systemlösning är då att fortlöpande registrera alla uppdaterande transaktioner på en transaktionslogg (diskett eller annat lämpligt medium) i lokaldatorn innan informationen sänds i väg till centraldatorn. Spartiden för transaktionerna på loggen synkroniseras med periodiciteten för säkerhetskopiering av de databaser som transaktionerna påverkar i centraldatorn.

Förfarandet medger i bästa fall helt automatiserad rekonstruktion av berörda datamängder fram till tidpunkten för avbrottet, genom att återigen transmitta de tidigare loggade transaktionerna. Disketten med de loggade transaktionerna kan alternativt skickas till centraldatorn för central uppdatering.

### **Steg 4: Förnyad dataregistrering**

Om inga andra, mer automatiska metoder står till buds, måste en förnyad registrering göras från originalverifikationer eller andra underlag.

### **Steg 5: Förnyad datainsamling**

Finns inga allegat eller har dessa förstörts vid katastrofen har dessvärre motsvarande information gått förlorad, såvida inte denna kan skaffas fram utifrån, t. ex. från kund eller leverantör. Även om så skulle kunna ske, är förfarandet oftast både osäkert och tidsödande.

## Organisation och bemanning

Det egentliga rekonstruktionsarbetet efter en katastrof bedrivs inom IT-enheten med fördel i en eller flera *insatsgrupper*, underordnade en kris- eller *katastrofledning*. Strävan bör naturligtvis vara att göra så små förändringar som möjligt i förhållande till ansvar och arbetsuppgifter i ordinarie organisation.

Ovanför IT-enhetens katastrofledning finns oftast en *företagsledning*. Denna arbetar *utåtriktat* mot allmänhet, massmedier, myndigheter och samverkande organisationers ledningar. IT-enheten arbetar *inåtriktat* med att rekonstruera verksamheten. Man sköter också kontakterna på operativ nivå med interna och externa användare.

Det aktuella skadeläget styr hur stor del av katastroforganisation som behöver engageras. Katastrofledningen avgör slutgiltigt detta.

Katastrofledningen bemannas och organiseras så att rekonstruktionsarbetet kan ges kvalificerad ledning dygnet om, åtminstone tills driften stabiliserats på reservanläggningen. Typiska befattningshavare i katastrofledningen är *IT-chef*, *driftchef* och *systemchef*.

IT-enhetens storlek styr om en eller flera insatsgrupper skall organiseras. Oberoende av insatsgruppernas antal skall dock som ett minimum följande funktioner bemannas:

- Säkerhetsarkiv** – inventerar och administrerar säkerhetsarkivet.
- Kartläggning av skadeläget** – bedömer skadornas omfattning och kopplar in försäkringsbolaget.
- Bärgning och sanering** – Tar hand om skadat och oskadat gods samt ombesörjer vid behov sanering.
- Kundkontakt** – sköter löpande kontakter med användarna.
- Ersättningsutrustning** – anskaffar och installerar ersättningsutrustning.
- Driftsystem** – installerar och underhåller driftprogramvara på reservanläggningen.
- Datakommunikation** – upprättar och underhåller reservdatanätet.
- Applikationer** – iordningställer applikationer (styrinformation, program, data).
- Förråd** – anskaffar data- och förbrukningsmaterial.
- Transporter** – ordnar transporter under rekonstruktionsarbetet, mellan olika produktionsställen och till/från användarna.
- Produktion** – dukar för och genomför produktion på reservanläggningen.

I en liten IT-organisation måste sannolikt en och samma person ta hand om flera funktioner. IT-enhetens katastroforganisation kan dock förstärkas med personal från andra enheter i företaget, såsom Inköp och Fastighet.

## Reservanläggningar

Om tidskraven är knappa måste reservanläggningar och reservteleförbindelser finnas förberedda, i egen regi eller kontrakterade. Behov av förberedelser är snarare regel än undantag.

Det är inte realistiskt att tro att man kan komma igång på en annan anläggning utan förberedelser på kortare tid än en vecka, annat än då det rör sig om enstaka persondatorer som skall ersättas. Som regel tar det mycket längre tid. Ju större anläggning och ju komplexare installation, desto längre tid. Att bygga upp ett nytt datanät är det som oftast tar längst tid.

## **Arbetsplatser för insatspersonalen**

Katastrofledningen och den övriga insatspersonalen behöver någonstans att ta vägen med sina förberedelser, redan innan man kan komma in på reservanläggningen. Inte minst gäller detta katastrofledningen som snabbt bör upprätta en *ledningscentral*.

Det kan räcka med ett enda stort rum, där lämpligt antal arbetsplatser ordnas. Konferensmöjligheter bör också finnas (konferensbord, skrivtavlor), liksom en anslagstavla för allmän information. Glöm inte tillgång till telefoner, vanligt kontorsmaterial, kopia- tor och fax.

## **Instruktioner för insatspersonalen**

Katastroforganisationens ansvar och arbetsuppgifter bör dokumenteras i en särskild *handlingsplan* med bland annat instruktioner för de olika insatsfunktionerna som beskrivits tidigare, vem eller vilka personer som skall besätta en funktion samt larmlistor.

## **Tidsschema**

Rekonstruktionsarbetet bör sättas igång så snart rimlig misstanke om allvarlig störning finns, även om informationen om skadeläget är ofullständig. Genom att vänta tills fullständig klarhet skapats beträffande skadeläget, kan värdefull tid gå förlorad.

Ett tidsschema för rekonstruktionsarbetet bör ingå i katastrofplanen. Tidsschemat omfattar hålltider för viktigare aktiviteter för att planerad tidpunkt för produktionsstart på reservanläggningarna skall kunna hållas.

I tidsschemat bör formella beslutspunkter finnas inlagda. Beroende på hur skadeläget bedöms vid den aktuella tidpunkten, fattas där beslut om att antingen avbryta katastrofåtgärderna eller fortsätta rekonstruktionsarbetet enligt katastrofplanen.

## **Arbetsmaterial**

För att rekonstruera verksamheten och komma i gång med katastrofdriften på reservanläggningen behövs en hel del arbetsmaterial – inte bara särskilda katastrofinstruktioner utan praktiskt taget all ordinarie driftdokumentation. Systemdokumentation kan också behövas.

Räkna aldrig med att det material som förvaras på det ordinarie driftstället är åtkomligt och användbart. Den dokumentation som man har till sitt förfogande är de säkerhetskopior som finns, eventuellt kompletterade med sådant ordinarie material som normalt förvaras utanför skadeplatsen. Det senare kan ju vara fallet om företaget bedriver verksamhet på flera olika platser.

# Att vidmakthålla katastrofberedskapen

---

## Periodisk översyn av dokument som berör katastrofberedskapen

Hur lätt händer det inte att en katastrofplan, när den väl är färdig, precis som alla andra planer, stoppas in i en pärm, ställs i en hylla och sedan får samla damm år efter år. Det dröjer inte länge innan en stor del av innehållet har blivit inaktuellt.

Det är därför nödvändigt att man inom IT-enheten utarbetar en rutin för periodisk översyn av sina katastrofplaner och andra dokument som berör katastrofberedskapen.

Med undantag för larmlistorna, som sannolikt måste revideras oftare, är årlig revision oftast (men inte alltid) tillräcklig. Det är då lämpligt att koppla revisionen av katastrofplanerna till det årliga arbetet med budget och verksamhetsplaner som i många företag pågår under hösten. Delar av katastrofskyddet, t. ex. kostnader för reservkapacitet av olika typer, är för övrigt uppgifter som direkt krävs i budgetarbetet.

## Dokumentkontroll

Det ligger i sakens natur att åtminstone delar av innehållet i katastrofplaner och liknande dokument är av känslig natur. Dels är det viktigt att informationen är korrekt, dels kan det vara olämpligt att viss information kommer till obehörigas kännedom.

En viss kontroll över de dokument som sprids i organisationen är alltså av nöden. Väsentliga dokument bör fastställas formellt på lämplig nivå i företaget och endast spridas till personer och funktioner enligt fastställd distributionslista. Alla dokument bör vara försedda med giltighetsdatum, utgåvenummer och liknande identifikation. Regler bör finnas hur dokument skall förvaras, t. ex. inlåsta. Man bör överväga att i kontrollerad form förstöra alla kopior av en utgående utgåva då reviderad utgåva distribuerats.

## Tester och övningar

Det som mer än något annat förvandlar den papperstiger, som katastrofplanerna ursprungligen utgör, till en reell förmåga att hantera en katastrof är att katastrofrutinerna regelbundet *testas och övas*. Grovt sett finns tre olika typer av tester eller övningar:

1. **Tekniska tester:** För att verifiera att t. ex. en viss kritisk datatjänst (system) kan köras på reservanläggningen. Detta innebär bland annat:
  - Att driftsystemen måste fungera på reservutrustningen.
  - Att ett reservdatanät kan upprättas mellan reservanläggningen och de planerade arbetsplatserna inom företaget.
  - Att aktuella register, databaser, bibliotek, blanketter, m.m. måste finnas lagrade "utanför huset" i säkerhetsarkivet och vara åtkomliga för bearbetning på reservutrustningen.
  - Att aktuella applikationsprogram, som skall fungera korrekt tillsammans med det data som nämnts ovan, finns lagrade i säkerhetsarkivet och åtkomliga för bearbetning på reservutrustningen.
2. **Larmövningar:** För att verifiera att larmlistorna stämmer och att framför allt nyckelpersoner kan nå inom de tidsramar som förutbestämts.

3. **Ledningsövningar:** För att verifiera att berörda chefer, arbetsledare och deras ersättare både kan klara av ålagda arbetsuppgifter och bemästra oförutsedda situationer (såsom ändringar i tidsscheman och prioriteter, oförutsedda problem och bortglömda aktiviteter).

Alla typer av övningar avser också att verifiera att uppsatta tidsramar för rekonstruktion och återstart kan hållas.

## Arbetsmetoder för tester och övningar

Det finns inga praktiska möjligheter att testa eller öva alla applikationer, rutiner eller aspekter på katastrofberedskap. Testverksamheten begränsas därför till de områden som bedöms som viktigast eller där effekten av insatta resurser bedöms bli störst.

Teknisk test av katastrofberedskapen bör göras minst årligen, gärna en gång i halvåret utom för de allra minsta installationerna, genom att ett sammanhängande applikationskomplex väljs ut för körning på reservanläggningen. Såväl online- som batch-applikationer testas. Reservdatanätet upprättas minst i den omfattning som krävs för att testa online-verksamheten.

Test sker så långt möjligt med material från säkerhetsarkivet. Om man av säkerhetsskäl väljer att genomföra testet med annat material än säkerhetskopior, bör man vara medveten om att värdet av testet avsevärt reduceras. Avsaknad av nödvändiga säkerhetskopior är nämligen en ofta återkommande brist, kanske den allra vanligaste.

Tester och övningar bör ske med allt mer stegrad svårighetsgrad, allteftersom erfarenhet vinnas. Till en början kan god tid för förberedelser ges och tidskraven när det gäller att få applikationerna i luften på reservanläggningen kan vara måttliga. Så småningom, sedan tillräcklig erfarenhet vunnits, bör tester och övningar att bli mer tillämpade till sin karaktär. Detta innebär att ingen tid för förberedelser ges, samtidigt som tidskraven blir de som gäller i ett verkligt läge.

Tillämpade tester och övningar ger god erfarenhetsåtervinning, men är ofta mycket tids- och resurskrävande att förbereda.

## Testplaner och testprotokoll

Till grund för testverksamheten läggs en *övergripande plan för katastroftester och övningar*. Detta är ett planeringsdokument som översiktligt beskriver de olika fristående test- och övningsmoment som bör genomföras för att säkerställa att IT-enhetens katastrofberedskap är tillfredsställande. Dokumentet utformas med fördel som en rullande tvåårsplan.

När testplanen skrivits färdig och fastställts, blir det respektive testledares ansvar att utarbeta de detaljerade projektplaner och testmanuskript som krävs för varje testetapp. Testledaren ansvarar även för att testerna genomförs planenligt.

Under en test eller övning skall problem, avvikelser från förväntade resultat eller andra anomalier fortlöpande dokumenteras i detalj i form av testprotokoll, så att nödvändiga korrigeringar i applikationer, rutiner, instruktioner, osv. kan ske efter genomförd test eller övning.

Testledaren för resp. test eller övning ansvarar för att protokoll upprättas och att rättelser blir gjorda.

# Planering av katastrofskyddet – egentligen en del av systemutvecklingsarbetet!

---

Som jag nämnde redan i det inledande avsnittet, har många företag i dag arbetat systematiskt med katastrofskydd för IT-verksamheten under flera decennier eller mer.

Jag konstaterade också att katastrofberedskapen, trots det omfattande och seriösa arbete som lagts ner, inom många IT-enheter ändå har brister som inte bara är obetydliga.

## Behov av katastrofberedskap beaktas för sent

En av orsakerna till detta är att frågor rörande lämplig katastrofberedskap ofta aktualiseras *alldeles* för sent i en datatjänsts (systems) livscykel, oftast först efter det att det aktuella systemet tagits i produktion. Man blir gång på gång tagen på sängen.

Spörsmål om lämplig skyddsnivå vid katastrof kommer nästan som en överraskning var gång de aktualiseras. Idéer om nya tjänster på marknaden kläcks, lönsamhetskalkyler görs, system utvecklas, utrustning anskaffas, produktion startas, osv. utan att frågor rörande behov och omfattning av katastrofberedskap över huvud taget beaktas.

Ibland övervägs inte ens behovet av ett katastrofskydd på miniminivå i form av säkerhetsarkivering utanför ordinarie produktionsställe av program, register och driftokumentation. Långt mindre diskuteras behovet av en mer utbyggd beredskap i form av tillgång till reservkapacitet inom vissa planerade tidsramar.

## Naturlig del av utvecklingsarbetet

För att långsiktigt och fortlöpande kunna hantera frågor rörande katastrofberedskap på ett strukturerat och effektivt sätt, är det nödvändigt att göra dessa frågor till en självklar del av *systemutvecklingsarbetet*.

Första gången frågan om katastrofberedskap berörs i denna process, borde vara redan i förstudien. I varje efterföljande etapp i utvecklingsarbetet fram till produktionssättningen ges sedan frågor rörande katastrofberedskap det utrymme som krävs för att en acceptabel skyddsnivå skall uppnås.

Så borde t. ex. fullt genomförda konsekvens- och sårbarhetsanalyser föreligga senast under den utvecklingsetapp som leder fram till kravspecifikationen för systemet. Kravspecifikationen omfattar även behov av säkerhetsarkivering, behov av katastrofproduktion, erforderlig återstarttid vid katastrof, osv. Under konstruktionsarbetet fastställs nödvändig reservutrustning samt utarbetas eventuella särskilda rutiner, program och annat som krävs för att uppfylla kravspecifikationen. Och så vidare . . .



**Dagen efter. Brandkårens mordbrandsexpert letar efter ledtrådar.**





## **Sternudd Consulting AB**

Mellingerum 1, 570 91 Kristdala

Tel: 0491-750 22, 070-548 44 88, E-post: [info@sternudd.se](mailto:info@sternudd.se)

*Specializing in Business Continuity Planning*

[www.sternudd.se](http://www.sternudd.se)