

# Katastrofeberedskap: Hvorfor og hvordan?

*I forrige utgave introduserte vi katastrofeberedskap som fagfelt, og gjennomgikk hvordan problemstillingen organiseres og planleggingsprosessen angripes.*

I den forbindelse konstaterte vi at en katastrofeplan består av fire deler eller faser:

- ✓ Katastrofehåndtering (øyeblikkelig hjelp)
- ✓ Kontinuitetsplan
- ✓ Midlertidig driftsplan
- ✓ Restaureringsplan

Vi påbegynte prosessen – forarbeidet – som leder frem til planen, og gjennomgikk blant annet temaet risikoanalyse i den forbindelse.

## Konsekvensanalyse

Neste trinn er konsekvensanalyse: Hvordan påvirkes ulike prosesser i virksomheten av katastrofer av forskjellige slag? Den overordnede målsettingen er fortsatt den samme – å skaffe til veie tilstrekkelig kunnskap til å opprettholde kritiske funksjoner i en krisesituasjon. Konsekvensanalysen er spesielt interessant fordi den setter søkelyset på et område som altfor sjelden kommer i fokus: Hvilke prosesser finnes i virksomheten, hvem av dem er kritiske, hvordan henger de sammen (avhengigheter), hvordan påvirker de hverandre og hva skal til av ressurser og andre innsatsmidler for å holde dem i gang?

### Prosesser og prioriteringer

En slik gjennomgang bør gjøres regelmessig av helt andre årsaker enn i forbindelse med en katastrofeplan: Forbausende ofte dukker det opp prosesser som har gått ut på dato – som ikke lenger har noen mening i virksomheten, men som like fullt eksisterer i beste velgående og koster ressurser. Slike forhold bør avdekkes og behandles i andre sammenhenger enn i forbindelse med katastrofeplanlegging! Skulle de dukke opp, er det imidlertid all grunn til å flagge dem – om ikke på annen måte, så i alle fall ved å plassere dem nederst på prioriteringslisten.

En enkel handlingsplan som etablerer sammenhenger og konsekvenser, kan se ut som følger:

- ✓ Identifiser prosessene i virksomheten, kvalifiser deres betydning i kritiske sammenhenger – overfor kunder, medarbeidere, myndigheter osv. (vi kommer inn på mer detaljerte, praktiske råd nedenfor).
- ✓ Prioritér prosessene i forhold til hverandre og i henhold til behovene som må dekkes for å holde virksomheten i gang.

- ✓ Definér målsettinger og tidsrammer for hver enkelt av de mest kritiske prosessene: Hvilke funksjoner må være i gang igjen innen X minutter eller Y timer?
- ✓ Dokumentér det hele i en form og et format som passer virksomheten og personene som er involvert.

For hver kritisk prosess dokumenterer vi blant annet følgende:

- ✓ Dens funksjon, rolle og grensesnitt mot omverden
- ✓ Nøkkelpersoner
- ✓ Hva som er kritisk
- ✓ Hvilke ressurser som kreves

Vi ser at mens risikoanalysen fokuserte på forebygging og skadereduksjon, handler konsekvensanalysen primært om restituering av drift – hvordan vi skal komme i gang igjen etter at katastrofen er et faktum. Mens vi fokuserer på å finne godt gjemte eller mindre åpenbare prosesser, er det lett å glemme selvfølgelighetene – for eksempel grensesnitt mot forsikringsselskaper, offentlig brannvern, lokale og sentrale myndigheter – for ikke å snakke om presse og media, børsinformasjon og så videre. Om aldri så selvfølgelige, de er viktige brikker i et stort puslespill, og må være med i vår analyse.

### Metoder

Intervjuer, spørreundersøkelser, arbeidsgrupper, diskusjoner – metodene er tallrike, og alle må som regel tas i bruk for å få frem et pålitelig og kvalitativt tilfredsstillende resultat. Igjen er det slik at vi i en oversiktsartikkel kun kan 'skrape' litt i overflaten – skape et bilde av utfordringene og hvordan de kan angripes.

Som tilfellet var for risikoanalyse, finnes det også for konsekvensanalyser faglig referansemateriale som er til stor hjelp – teoretisk såvel som praktisk. Et godt eksempel er artikkelen *How to Conduct a Business Impact Analysis* (av Patricia A. P. Fisher),<sup>2</sup> som ble presentert i *Disaster Recovery Journal* sommeren 1996. Artikkelen er kort og konsis, og foreslår metodikk i forbindelse med datainnsamlingen, heriblant en rekke spørsmål som kan brukes i intervju-prosessen:

- ✓ "Hvilke oppgaver sorterer under din avdeling?"
- ✓ "Hvilke verktøy brukes i avdelingen? Hva skjer dersom verktøyene ikke er tilgjengelige? Har dere alternativer?"
- ✓ "Nevn eksempler på hva som ville utgjøre en katastrofe for din avdeling."
- ✓ "Hva ville du gjøre dersom telefon/IT/elektrisitet/?? ikke var tilgjengelig i X timer eller dager?"
- ✓ "Hva ville effekten av en katastrofe være for din avdeling?"
- ✓ "Hvilke funksjoner i din avdeling bidrar direkte til organisasjonens omsetning/inntjening?"

<sup>2</sup> <http://www.drj.com/articles/sum96/fish.html>

- ✓ “Vet du om dine eller avdelingens data blir sikkerhetskopierte, og eventuelt hvor ofte?”

Både metodikk, omfang og dybde må tilpasses organisasjonens størrelse, type virksomhet og omgivelser.

Når de kritiske prosessene er kartlagt og dokumentert, må virkningen av ulike grader/former for katastrofer klarlegges – for hver enkelt prosess. En del av kunnskapen som trengs, er allerede skaffet til veie via arbeidet vi beskrev ovenfor. Den må organiseres, tilgjengeliggjøres og i en del tilfeller utfylles. Igjen kommer Disaster Recovery Journal oss til hjelp med stoff som supplerer artikkelen vi refererte til ovenfor: *Some Techniques for Business Impact Analysis* (av Geoffrey H. Wold)<sup>3</sup> går konkret og generelt til verks med systematisering, områder og problemstillinger som må adresseres.

Armert med metodikken fra disse to kildene, står vi godt rustet for å få på plass en konsekvensanalyse som ikke bare kan stå på egne ben, men som representerer et vesentlig bidrag til den totale katastrofeplanen.

## Veien videre

Analysene er på plass, men hvordan bruker vi dem og hvordan kommer vi videre? Vi skal i første omgang ende opp med et dokument – en plan – som skal være oversiktlig, tilgjengelig og forståelig. I og med at det alltid vil ta flere runder før planen er ferdig, er det ikke noe mål i seg selv å strebe etter perfektjon i første runde. Testingen vil uvegerlig avsløre svake punkter og mangler som må korrigeres.

Avhengig av organisasjonens størrelse og planens omfang kan enten standardverktøy (for eksempel MS Office) benyttes, eller spesielle verktøy kan anskaffes. Sistnevnte kategori inneholder gjerne maler, retningslinjer og ‘hjelpere’ som bidrar til å redusere tidsforbruket. At de primært forefinnes på engelsk, typisk for det amerikanske markedet, gjør dem uoptimale, men langt fra uegnet for våre forhold.

### IT-beredskap

Analysene vi har vært igjennom gir grunnlag for å sette opp en prioritert liste av IT-verktøy og deres avhengigheter:

- ✓ Hvor lenge hvert enkelt av dem kan være ute av drift
- ✓ Hvem (hvilke brukergrupper og deres størrelse) som har den største avhengigheten
- ✓ Hvilke ressursbehov de har (også med hensyn til data og kommunikasjon)
- ✓ Minimum tilgjengelighet (*worst case scenario* – for eksempel totalskade ved brann, hva som må til for å holde et minimum av drift)

Oversikten gir oss grunnlaget for å definere ulike nivåer av beredskap og få en pekepinn om kostnader og nødvendige investeringer. Der spe-

<sup>3</sup> <http://www.drj.com/articles/fal96/wold.html>

### Beredskap som business

Katastrofeberedskap er ikke bare et eget fagfelt, men også et eget forretningsområde. Slik har det vært siden 60-tallet, og igjen var banker og finansinstitusjoner først ute med å sikre seg mot langvarige driftsavbrudd. På 80- og tidlig på 90-tallet dukket nye aktører opp i dette segmentet, og mens de klarte seg bra i USA og enkelte andre land, ble markedet og interessen for liten her hjemme. I dag er denne situasjonen i rask forandring, blant annet som en følge av ASP-bølgens opp- og nedtur: En hel næring med utgangspunkt i IT-tjenester er i ferd med å modnes. Blant disse tjenestene finner vi i voksende grad tilbudet om beredskapssystemer – dedikerte systemer som alltid står parat til å overta, eller tilgjengelig kapasitet som kan settes i drift på kort varsel.

sielle verktøy for dokumentasjonsoppgaven blir for kostbart, er et moderne regneark et ypperlig substitutt.

### Handlingsplan

Arbeidet munner ut i en handlingsplan for etablering av beredskap, som kan inneholde innslag fra følgende liste. Flere av punktene er innlysende – på grensen til det banale, men blir ikke mindre viktige av den grunn:

- ✓ Utarbeid metoder eller arkitektur for full eller delvis gjenopp-  
retting av den enkelte tjeneste.
- ✓ Skaff fullstendig oversikt over hvilke programmer/program-  
pakker/produkter og tilhørende datasett som er nødvendige  
for den enkelte tjeneste/løsning.
- ✓ Sørg for at oversikten ovenfor også tar med innbyrdes avhen-  
ghetsforhold: To eller flere tjenester som er avhengige av  
samme data kan åpenbart ikke gjenopprettes hver for seg.
- ✓ Kontrollér at rutiner og dokumentasjon for sikkerhetskopie-  
ring og fjernlagring av slike kopier stemmer overens, og at de  
er adekvate i forhold til de behov som er avdekket. Ta i den  
forbindelse spesielt hensyn til prioriteringene som er etablert,  
slik at de viktigste datasettene er lettest tilgjengelig og kan  
'rulles inn' raskt og på kort varsel.
- ✓ I forbindelse med sikkerhetskopiering, sørg for at ikke bare  
data, men også applikasjoner og verktøy blir kopiert – på en  
måte som gjør det enkelt å få dem i drift på nytt utstyr i nye  
omgivelser. Forholdet må være dokumentert i policy og ruti-  
ner for sikkerhetskopiering.
- ✓ Kontrollér – og sørg for regelmessig oppdatering av – reserve-  
kapasitet, enten den er i egen regi eller leid hos en tjenestele-  
verandør (se margramme på foregående side). Kapasitet i  
overflod er til liten nytte dersom den ikke forefinnes på riktig  
plattform (X86/SPARC/PA RISC/AS400/PPC osv.). Likeledes  
har sikkerhetskopiene liten verdi dersom format eller media  
ikke er kompatible med programvare og utstyr på reservesys-  
temene.
- ✓ Sammen med ekstern lagring av sikkerhetskopier er det nød-  
vendig å ha et kriselager av spesialtrykksaker (formularer,  
brevark, etc.).
- ✓ Dersom det vil være behov for spesielle transportløsninger –  
for medarbeidere, produkter, kunder eller leverandører –  
mens en kriseløsning er i drift, må disse planlegges og kon-  
trolleres – eventuelt avtales med leverandører av slike tjenes-  
ter.
- ✓ Sørg for finansiering – i første omgang av forberedelser og  
vedlikehold av beredskapen, dernest at den er tilgjengelig den  
dagen katastrofen er et faktum. Det finnes eksempler på  
grundige planer og velorganisert beredskap som har vært til

liten praktisk nytte, fordi ingen personer med tilstrekkelig prokura var å få tak i da krisen var et fatkum.

- ✓ Ha sikkerheten under kontroll – den fysiske såvel som den IT-messige. Å komme raskt i gang etter en katastrofe eller ulykke har beskjeden verdi dersom vi samtidig åpenbarer virksomhetens konfidensielle informasjon for hele verden. Sabotasje er en katastrofe så god som noen, som riktignok forekommer sjelden på våre kanter, men som ikke desto mindre er en særdeles effektiv måte å skaffe seg tilgang til informasjon på.
- ✓ Lag en oversikt over alle viktige kontaktpunkter, og sørg for at den er tilgjengelig for alle som kan trenge den: Ansvarsforhold, telefonnummere (også til myndigheter, partnere etc.), adresser og så videre.

Nøkkelord hele veien er enkelhet, klare ansvarsforhold og en tilgjengelig toppledelse – som holder seg i bakgrunnen, ikke i frontlinjene. Still relevante kontrollspørsmål underveis: Hvor er kommandosentralen (må være et stykke unna bygningen/området beredskapen gjelder), vet alle hvor den er, har sentralen bemanningsplaner for 24 timers drift, er bemanningen liten nok (skal være minst mulig), etc.<sup>4</sup>

### Katastrofeplanen

Mens handlingsplanen bygger opp beredskapen og forbereder en katastrofal situasjon, kommer selve katastrofeplanen til anvendelse først når katastrofen er et faktum. Vi gjennomgikk dens fire faser i forrige utgave:

- ✓ **[Fase 1]** Katastrofehåndtering – øyeblikkelig hjelp, dekker (for eksempel) de første 6/12/24/48 timene etter at katastrofen har inntruffet. Hovedfokus går på mennesker – få dem ut av bygninger, bort fra områder som er truet, til behandling osv.
- ✓ **[Fase 2]** Kontinuitetsplan – få i gang minimal drift.
- ✓ **[Fase 3]** Midlertidig drift – etablere et virksomhetsnivå som kan holdes gående noen dager eller uker, og som tar vare på fundamentale prosesser.
- ✓ **[Fase 4]** Gjenoppbygging/restaurering – veien tilbake til normale forhold.

Analysene og det øvrige arbeidet vi har gjennomgått så langt, gir det faglige og informasjonsmessige grunnlaget for katastrofeplanens ulike deler. Prosessen videre ligner til forveksling på tilsvarende i forbindelse med generell IT-sikkerhet: Organisasjonen skal bevisstgjøres, læres opp og motiveres. Informasjon og motivasjon skal inn i informasjonspakken til nyansatte og bevisstheten for organisasjonen som helhet skal opprettholdes. Terroraksjonene mot USA 11. september 2001 har

<sup>4</sup> Ytterligere inspirasjon til både denne og andre deler av arbeidet er å finne i dokumentet GUIDELINES FOR CONTINGENCY PLANNING FOR INFORMATION RESOURCES SERVICES RESUMPTION, utarbeidet av DEPARTMENT OF INFORMATION RESOURCES i delstaten Texas, USA – <[www.dir.state.tx.us/TIC/dir\\_info/contngcy.htm](http://www.dir.state.tx.us/TIC/dir_info/contngcy.htm)>.

gitt et vesentlig bidrag til slik motivasjon. Utfordringen nå er å opprettholde dette nivået.

Likeledes er planen et levende dokument som må evalueres og tilpasses virkeligheten med jevne mellomrom, for eksempel 2 ganger i året. En slik regelmessig prosedyre gjenspeiler det faktum at både beredskapen i seg selv og den underliggende planen er deler av en prosess, ikke et prosjekt. At få organisasjoner prioriterer en slik hyppighet betyr ikke at den er verken unyttig eller uviktig – uansett om vi snakker om IT-sikkerhet eller katastrofeberedskap.

Enkelte hendelser eller forandringer i eller rundt organisasjonen er i seg selv viktige nok til å re vitisere planene. Eksempler er:

- ✓ Store organisasjonsendringer (fisjoner, fusjoner, nedbemanninger, flytting ...)
- ✓ Nye eller endrede krav fra myndighetene
- ✓ Store forandringer på IT-siden (omlegging av infrastruktur, nye løsninger av stort omfang, *outsourcing* ...)
- ✓ Viktige endringer på leverandørsiden, produktsiden eller eiersiden

Sist, men ikke minst er forsikringene et element som krever jevnlig ettersyn: Er katastrofeforsikringen i orden? Finnes det tiltak som kan redusere premien? Er slike tiltak allerede implementert?<sup>5</sup>

### Test, prøvekjøring

Planer, allokerte ressurser og grundige forberedelser er vel og bra – viktige og uunnværlige. Betydningen av praktiske prøver kan imidlertid ikke overdrives: Det er her feil og svakheter finnes, som i en virkelig krise kan være like alvorlige som katastrofen i seg selv. Vi har allerede nevnt eksempler på små tuer som kan velte store lass. De finnes i fleng, og avsløres kun unntaksvis uten praktiske øvelser.

Det er primært fasene 2 og 3 som kan og bør prøvekjøres. Hastigheten med hvilken det er mulig å få virksomheten på fote igjen, er helt avhengig av kvaliteten på dette arbeidet.

## Beredskap i hverdagen

Vi påpekte den opplagte sammenhengen i forrige artikkel: Beredskap er som forsikring – den er nødvendig, men kommer forhåpentlig aldri til reell anvendelse. Unyttig er den likevel ikke, selv i hverdagen. Ikke bare gir en fungerende og oppdatert beredskap ro i sjelen for de av oss som har ansvaret for den slags, selve prosessen gir en innsikt i organisasjonens virkemåte – gjøren og laden – som ofte har tallrike positive bieffekter.

Dessuten viser erfaring at god beredskap har positive effekter også på 'små' forhold: Driftsprosedyrer, policy, sikkerhet – for å nevne noen få – blir tilgodesett med ekstra ettersyn og oppdateringer. Videre får vi

<sup>5</sup> En særdeles relevant referanse i forbindelse med katastrofeforsikring er artikkelen *Prepare for the Worst* fra *Darwin Magazine* – <[www.darwinmag.com/read/120100/worst.html](http://www.darwinmag.com/read/120100/worst.html)>.

kontrollert og dokumentert organisasjonens overensstemmelse med offentlige reguleringer og pålegg.

Dessuten – som vi også var inne på ovenfor – får vi en kontroll av forsikringene i forhold til virkeligheten, hvilket i seg selv kan spare betydelige beløp, og derigjennom redusere de reelle kostnadene knyttet til katastrofeberedskap. ■

Kopiering forbudt