

Katastrofeberedskap: Hvorfor og hvordan?

For noen måneder siden utlyste Oracles norgeskontor en premie til den bedriften som kunne demonstrere en fungerende og pålitelig rutine for sikkerhetskopiering. Fokus var naturlig nok rettet mot databaser, og anledningen var en berettiget mistanke om at få virksomheter har tatt oppgaven tilstrekkelig alvorlig.

Problemstillingen er en tankevekker i seg selv: Vi er smertelig avhengige av våre data – deres kvalitet og tilgjengelighet. Det investeres store beløp i systemer, verktøy og infrastruktur, mens 'forsikringen' i tilfelle problemer ofte glemmes eller blir stemoderlig behandlet. Der mekanismer og verktøy for sikkerhetskopiering er på plass, blir de sjelden eller aldri kontrollert eller praktisk testet.

Fokus på beredskap og forebygging

Oracle fant sin premievinner, som på en eksemplarisk måte hadde tatt vare på hele problemstillingen – verktøy, rutiner, testing og kontroll. Selskapet oppnådde samtidig å sette fokus på en øm tå for både norske og internasjonale virksomheter: Beredskap – hva gjør vi dersom ulykken er ute? Hvor lenge kan vi tåle å være ute av drift? Hvilke forpliktelser har vi overfor kunder og partnere, og hva blir konsekvensene av å ikke være i stand til å innfri?

Store mørketall?

Spørsmålene dukker opp som perler på en snor, og svarene viser seg i mange tilfeller å være mangelfulle. Praksis har vist at det gjerne skal mindre enn en skikkelig vannlekkasje til for å sette selv mellomstore organisasjoner ut av spill for flere dager. Videre viser det seg at eksistensen av beredskap ikke er det samme som at den virker. Situasjonen er analog med hva vi observerer i forbindelse med sikkerhet generelt og brannmurer spesielt: Deres eksistens fungerer som sovemedisin, men har liten annen betydning.⁴

Det er ikke dermed sagt at fraværende eller dårlig beredskap er regelen, og det motsatte er unntaket. Statistisk er situasjonen noe bedre enn tilfellet er for sikkerhet. Imidlertid er det også et faktum at beredskapen sjelden er tilstrekkelig, og i mange tilfeller kan bli vesentlig bedre uten store investeringer. Klare behovssignaler fra markedet har foranlediget denne gjennomgangen av forhold, metoder og tiltak knyttet til beredskap generelt og katastrofeberedskap spesielt. Vi legger særlig vekt på planleggingen – den første og alltid like kritiske fasen som skal munne ut i bevissthet, løpende aktiviteter, oppfølging og ansvarsfordeling – i tillegg til konkrete planer.

⁴ Se "Brannmurer: God forsikring eller falsk trygghet?" i Mellvik-Rapporten nr. 37 og "Brannmurer: Mye penger, lite sikkerhet" i nr. 57. Begge utgavene er tilgjengelige i pdf-format via vår Web-tjeneste.

Hvilken katastrofe?

Vi befinner oss i en del av verden som er privilegert på en rekke måter, ikke minst med hensyn til naturlig risiko. Riktignok har evalueringen av risiko knyttet til internasjonal terror forandret seg vesentlig det siste halve året, men totalbildet er fortsatt fordelaktig for våre breddegrader.

Ikke desto mindre er truslene både reelle og aktuelle – og variable i forhold til hvor vi befinner oss, hvilken type virksomhet vi driver og beskaffenheten av våre fysiske aktiva. En del viktige forhold å ta hensyn til i den forbindelse er:

- ✓ Naturkatastrofer – på våre kanter som regel knyttet til ekstreme værforhold, for eksempel: Orkan, nedbør, flom, skred osv. – med følgeskader som brudd på veier, telekommunikasjoner og strømforsyning.
- ✓ Ulykker, terrorhandlinger, sabotasje – brann, eksplosjoner, flom/vannskader, flystyrt, trafikkulykker,⁵ osv. Vi kan være godt sikret mot alle tenkelige naturkatastrofer, men har vi noe å stille opp med dersom et vogntog med farlige kjemikalier eller sprengstoff velter rett utenfor bygningen?
- ✓ Spionasje – et forhold som sjelden tillegges særlig vekt på våre kanter, men som for en rekke virksomheter kan være truende for virksomhetens eksistens.
- ✓ Innbrudd og hærverk – fysisk eller via datasystemer og nettverk
- ✓ ... og så videre

Med erfaring og god fantasi samler vi flest mulig potensielle trusler, for deretter å stryke de som av ulike årsaker havner utenfor spekteret vi ønsker å dekke. Det viktigste i denne fasen er å få et forhold til dem, og til valgene som gjøres.

Videre må vi avklare hvor grensen går mellom hva som er plagsomt og hva som er en katastrofe – i tid (timer): 2 timer kan være plagsomt, men er 8 timer en katastrofe?

Vi kommer inn på metoder for å gjennomføre slike analyser nedenfor, og begynner med en definisjon:

En katastrofe er en brå, uventet og skjebnesvanger hendelse som setter organisasjonen ut av stand til å utføre kritiske virksomhetsfunksjoner for en gitt periode, og som resulterer i stor skade og/eller tap.

En klar definisjon er et nødvendig utgangspunkt for den videre prosessen. Sammen med etableringen av de kritiske tidsrammene vi nevnte, og som i definisjonen kalles 'gitt periode', danner den grunnlaget for våre evalueringer og planer.

⁵ Tåler virksomheten at hele styret, ledelsen eller en hel avdeling plutselig blir borte? Hvis ikke, er det nødvendig å planlegge slik at sjansen er minimal: Reise med forskjellige fly, aldri i samme bil, etc.

Katastrofeplanlegging

Katastrofeplanlegging er ingen nyhet, verken generelt eller i IT-sammenheng. Området har sågar sitt eget (engelskspråklige) fagblad, *Disaster Recovery Journal*, som har vært i virksomhet siden 1987 og har over 50.000 abonnenter. Bladet er tilgjengelig både i papirform og på nettet, og representerer en veritabel gullgrube med praktiske råd, erfaringer, maler og produktreferanser. Vi kommer avslutningsvis (neste utgave) tilbake til en rekke spesielt nyttige pekere fra DRJ.⁶

En fullstendig katastrofeplan består av 4 deler – eller 4 trinn i prosessen å komme tilbake til normal drift etter å ha vært utsatt for en uventet og dramatisk hendelse. Alle 4 er like viktige for den totale beredskapen:

- ✓ Katastrofehåndtering (øyeblikkelig hjelp)
- ✓ Kontinuitetsplan
- ✓ Midlertidig driftsplan (plan for oppstart av midlertidig drift)
- ✓ Restaureringsplan

I avsnittene nedenfor utdyper vi hva de forskjellige fasene inneholder og når de kommer til anvendelse.

Katastrofehåndtering

Dette er planen som trår i kraft umiddelbart etter at en katastrofe har inntruffet, og dekker de første 24 til 48 timer. Målsettingen er å begrense fysiske og andre skader maksimalt, og bringe ansvarsforhold, informasjonsflyt (media, myndigheter, partnere, medarbeidere, kunder, ...) og så videre under kontroll. Ulike katastrofetyper fordrer forskjellige tiltak i så henseende – en storbrann har ganske andre praktiske følger enn at taket blir blåst av eller 2 etasjer står under vann.

Forberedelsene består i å fordele oppgaver og ansvar til personer, stoppe eller styre skadeutviklingen, sørge for at personell er utenfor fare, og få de fysiske skadene under kontroll. I den forbindelse er det kritisk å få oversikt over skadene: Har vi med en katastrofe å gjøre, eller vil det være mulig å komme tilbake til normal drift i løpet av den 'magiske' tidsperioden? Med mindre hendelsen er rettet mot eller konsentrert om IT-systemer eller infrastruktur, er det få elementer i denne fasen rettet mot IT-siden – utover å sørge for at verken utstyr eller rekvisita kommer på avveie.

Kontinuitetsplan

Dette er planen som skal sørge for at virksomheten ikke utraderes av en katastrofe. Graden av detaljplanlegging og investeringer avhenger naturligvis av virksomhetens type og bransje: En datasentral har helt andre behov enn en trelastforretning eller en rørlegger. Likeledes betyr virksomhetens størrelse og geografiske spredning mye for både hva som er mulig og til hvilken pris. I denne forbindelse står IT-funksjoner og tjenester sentralt.

⁶ ON LINE utgaven av DRJ er gratis, vi trenger kun å registrere oss for å få adgang til sidene.

Viktige forhold, spørsmål og observasjoner i den forbindelse er:

- ✓ Skape trygghet – for kundene, dernest for eiere og toppledelse, som skal vite (og har det overordnede ansvaret for) at situasjonen er under kontroll.
- ✓ Sørge for stabilitet: Avbruddet må være minst mulig og må virke kontrollert utad. Kaos er et dårlig signal og kan vanskelig unngå å få konsekvenser, for eksempel for virksomhetens bilde utad og dermed for markedsandeler.
- ✓ Fokus på kritiske funksjoner i virksomheten og hva som skal til for å holde dem i gang.
- ✓ IT-funksjoner (nettverk, systemer) og kommunikasjonssystemer må gjøres tilgjengelige slik at de kritiske funksjonene kan utøves.

Elementer som muliggjør slik kontinuitet i tilfelle katastrofe, er midlertidige lokaler med grunnleggende infrastruktur og tilgjengelige data – sistnevnte er allerede ivaretatt via fjernlagring av sikkerhetskopier.⁷ I den forbindelse er det nødvendig å verifisere at tiden det tar å gjøre en tilgjengelig infrastruktur operativ, for eksempel gjennom å bringe til veie og 'rulle inn' en sikkerhetskopi på alternative systemer, ikke overstiger kravet for hele operasjonen. Likeledes må det trenes til for å sikre at planene ikke blir en ren papirøvelse, men lar seg realisere i praksis.

I de fleste tilfeller er det hensiktsmessig å etablere en kontinuitetsplan gjennom samarbeid med en tjenesteleverandør som spesialiserer seg på nettopp slike tjenester, eller via forretningspartnere som kan være 'backup-sites' for hverandre.

Mens dette kan virke svært så omstendelig, og i mange tilfeller vil være temmelig omfattende, er det verdt å minne om at kun virksomhetens aller mest kritiske funksjoner skal ivaretas i kontinuitetsplanen.

Plan for midlertidig drift

Tredje nivå i vår katastrofeplan er å få virksomheten raskt i gang igjen – via utstrakt bruk av midlertidige virkemidler, men på en måte som kan fungere tilfredsstillende over en periode på flere måneder. Her skal alle medarbeidere være i stand til å utføre sine oppgaver – med rimelig effektivitet. Virksomhetens ansikt utad – generelt og overfor leverandører og kunder – er avhengig av at det ikke trekkes i langdrag før en slik situasjon kan etableres.

Det er uunngåelig at driften blir mer kostbar og mindre effektiv i en periode, et forhold som kan være dekket av en forsikringspolise.

Restaureringsplan

Dette er planen som skal bringe virksomheten tilbake til normal drift. Den må ta høyde for at opprinnelige lokaliteter kan være fullstendig

⁷ Vi inkluderer ikke slik fjernlagring i beredskapsplanen fordi dette er et forhold som skal og må være ivaretatt uansett. Om så ikke er tilfelle, er det et riktig sted å starte.

ødelagt. Med andre ord må alternative løsninger avhengig av katastrofens art og grad være tatt høyde for.

Fra tanke til plan

Slike planer har mange fellestrekk med alminnelig forsikring: Vi håper at det aldri blir bruk for dem, men erkjenner viktigheten av å ha dem i orden. På den andre siden er katastrofeplanlegging langt mer komplisert enn forsikring, fordi detaljeringsnivået er høyt og vi er henvist til å gjøre store deler av jobben selv, eventuelt i samarbeid med spesialister.⁸

Idet vi starter, har vi kun vage anelser om hvor vi vil ende opp – kostnadmessig og praktisk. Hvor store ressurser det er rimelig å avse til formålet, er også et åpent spørsmål idet vi starter: Før vi har fått et realistisk bilde av risikomomentene og konsekvensene, er det umulig å fastsette en rimelig 'forsikringspremie'. Prosessen fra tanke til plan består noe forenklet av følgende hovedfaser:

- ✓ Mandat, støtte fra ledelsen
- ✓ Innsamling av data og informasjon
- ✓ Risikoanalyse og konsekvensanalyse
- ✓ Utarbeide plan (design)
- ✓ Implementasjon og test
- ✓ Motivasjon, opplæring
- ✓ Forbedringer (kontinuerlige oppdateringer)

Mange vil allerede her observere en rekke fellestrekk med tilsvarende prosess når vi arbeider med IT-sikkerhet. Dette er ikke tilfeldig, og i et overordnet bilde inngår IT-sikkerhet som et element i den totale katastrofeplanleggingen.

Datainnsamling

Datainnsamlingen utføres av en person eller en gruppe – avhengig av organisasjonens størrelse. Relevante informasjonskilder kan være målsettinger, regelverk, policies, prosedyrer, strategier, handlingsplaner, planer og tegninger knyttet til bygninger og kontorer (forandringer, nybygg etc.), prosjekter, bemanning og så videre.

Hensikten med innsamlingen er å skaffe oversikt over kritiske ressurser i organisasjonen: Hvor dynamisk er informasjonen, hvor avhengige er vi av dens tilgjengelighet i den daglige driften og hvordan blir den lagret? Disse parametrene vil til slutt fortelle oss hvordan informasjonen skal behandles (lagres), og dens prioritet i en krisesituasjon. Fjernlagring av kritiske data er forhåpentlig på plass allerede, og jobben blir å kontrollere at rutinene virker, at den lagrede informasjonen er oppdatert og at den kan gjøres tilgjengelig innenfor de tidsrammene vi til slutt definerer.

⁸ Det er verken tilfeldig eller overraskende at slike spesialister ofte er å finne i nettopp forsikringsbransjen.

Typiske kategorier data som skal være å finne i et fjernlager – utover sikkerhetskopier fra IT-systemene, er regnskapsdata, produksjonsinformasjon, tegninger og spesifikasjoner for produkter og prosesser, forretningshemmeligheter, systemdokumentasjon, lisensinformasjon (også for programvare), spesiell programvare og internt utviklede applikasjoner.

I mellomstore og store organisasjoner kan informasjonsmengden være bortimot uendelig. Desto viktigere er det å være kritisk og selektiv i denne prosessen. Grunnlaget for riktige valg er igjen å tenke funksjoner, prosesser og mennesker: "Virksomheten kan ikke leve/overleve uten _____".

Risikoanalyse

Oppgaven er like kritisk som den er vanskelig – og heldigvis finnes det hjelpemidler som bidrar et viktig stykke på vei. At disse (som regel) er amerikanske, er sjelden negativt – snarere tvert imot: Det betyr at erfaringsgrunnlaget de bygger på er desto bedre.

Risikoanalyse er en vitenskap og et fagfelt i seg selv, som for det første er like gammelt som forsikringsbransjen, og for det andre får betydelig oppmerksomhet fra akademiske- og forskningsmiljøer. Statistiske verktøy, analyseverktøy og metodestudier bidrar til å raffinere tilgjengelige hjelpemidler – med hensyn til såvel anvendelighet som nøyaktighet.

Amerikanske FEMA, *Federal Emergency Management Agency*, har lagt ned store ressurser de siste 20 årene på en rekke områder innen katastrofeplanlegging, inklusive risikoanalyse. Organisasjonens Web-tjener inneholder en lang rekke viktige dokumenter, rapporter og opplæringsprogrammer, inklusive en grundig gjennomgang av hvordan utfordringen risikoanalyse kan angripes.⁹ Videre har den amerikanske Riksrevisjonen (GAO, *General Accounting Office*) utarbeidet et omfattende dokument som diskuterer hvordan risiko evalueres i store organisasjoner. Gjennomgangen er gull verdt for å skape forståelse for utfordringene og som grunnlag for etablering av metodikk.¹⁰

Viktige momenter i prosessen er:

- ✓ Skaff til veie all relevant informasjon som forteller om risiko (historiske hendelser og erfaringer, tekniske og menneske-relaterte risikoer, antatte og/eller faktiske systemsvakheter [IT-systemer, ventilasjonssystemer, bygninger etc.]).
- ✓ Hele virksomheten må dekkes, ikke én bygning eller én avdeling.
- ✓ Sørg for å få flere synspunkter på samme problemstilling – en sak har alltid flere sider, og tilfeldighetene virker ikke slik at

Hvor er det hjelp å få?

Vi befinner oss i et på alle måter rolig hjørne av verden, hvilket er forklaringen på at vi mangler offentlige instanser som beskjeftiger seg med katastrofeberedskap og -forebygging. Denne privilegerte situasjonen skal vi glede oss over, men den kan lett bli en sovepute. En kraftig påminnelse om hvordan dette fungerer fikk vi fra våre politikeres kommentarer etter terrorhandlingene i USA i september 2001. Slik sløvheter er beredskapens største fiende.

I mangel av lokale ressurser er det naturlig å benytte seg av de som finnes internasjonalt. Amerikanerne har spesielt velutviklede institusjoner i så henseende. FEMA (www.fema.gov) er den viktigste ressursen i den forbindelse, godt supplert av *Disaster Recovery Journal* (www.drj.com) og *Environmental Systems Research Institute, Inc.* (www.esri.com). Flere relevante pekere finnes på Web-siden med tilleggsstoff til denne utgaven av Mellvik-Rapporten, se side 35 for detaljer.

Skadebegrensning

Tiltak for skadebegrensning og forebygging er viktige elementer i en katastrofeplan. Enkle eksempler med tilknytning til IT-systemer er overspenningsvern, nødstrømsaggregater, UPSer, doble strømforsyninger, HA-systemer og så videre.

FEMA leverer et grundig kurs i skade-forebygging via Internettet, med materialet tilgjengelig for alle. Tittelen er "Introduction to Mitigation", og adressen:

www.fema.gov/emi/is3931st.htm.

9 Dokumentet er et kapittel i en omfattende samling kursmateriale, og har tittelen "ANALYZING THE RISKS" (6 sider). Det er tilgjengelig i PDF-format fra adressen <http://www.fema.gov/emi/pdf/is2-2-a.pdf>.

10 "INFORMATION SECURITY RISK ASSESSMENT – PRACTICES OF LEADING ORGANIZATIONS" er tilgjengelig på adressen <http://www.gao.gov/special.pubs/ai00033.pdf>.

vi alltid kommer med den optimale vinklingen i første forsøk. Ingen har den fulle oversikten, og det som er uviktig for noen kan like fullt være kritisk for virksomheten.

- ✓ Ha alltid fokus på tid: Havner en risiko – eller konsekvensene av den – på den riktige eller gale siden av hva vi regner som en katastrofe?
- ✓ Kost/nytte er alltid viktig: Er skadene eller konsekvensene for små til å kreve oppmerksomhet eller er beskyttelse og beredskap for kostbart til å være mulig?
- ✓ Sørg for å få et klart bilde av virksomhetens toleransegrenser, som er avhengig av størrelse, geografisk spredning og plassering, virksomhetens art og produkter/tjenester, stabens kvalifikasjoner og engasjement, og ikke minst økonomi.

Kvantifiseringen av risiko påvirkes i stor grad av hvilke tiltak som er satt i verk for å begrense skader når ulykken er ute. For eksempel blir risikoen for en katastrofal brann vesentlig redusert dersom bygningen befinner seg i nærheten av en brannstasjon som er bemannet døgnet rundt. Likeledes vil alarmsystemer og brannslukningsanlegg ha stor innflytelse på risikobildet. **Forebyggende tiltak er en viktig del av beredskapsplanen.** De vil bidra til å redusere skadeomfanget og kan i enkelte tilfeller forhindre selve katastrofen.

Tabell 1 Eksempel på hvordan Wold/Shriver-modellen benyttes til å skaffe oversikt over risiko og konsekvenser.

Trussel	Faktorer				Konsekvenser ^a				Vekttall
	Sannsynlighet ^b	Hastighet ^c	Varsel	Varighet ^d	Aut. funksjoner ^e	Administrasjon	Drift	Brukere	
Brann	M	R	Nei	K/M	3	3	3	3	
Oversvømmelse	L	R	Nei	M	3	3	3	3	
Lynnedslag	L	R	Nei	K	2	2	2	2	
Storm/kraftig vind	M	R	Nei	K	2	2	2	2	
Strømbrudd ^f	M	R	Nei	M	1	1	0	1	
Varme/ventilasjon	M	Begge	Kanskje	M					
Alvorlig systemsvikt	M	R	Kanskje	U					
Brudd, komm.linjer	M	R	Nei	U					
Sabotasje	L	Begge	Kanskje	M/L					
Terrorisme	L	Begge	Kanskje	K/M					
Ran	M	R	Kanskje	M					
Flyulykke	L	R	Nei	M					
Bilulykke	M	R	Nei	K/M					
Kjemiske utslipp	L	R	Nei	L					
Bombetrussel/eksplosjon	L	R	Nei	L					

a Konsekvensene graderes (for eksempel) fra 0 (små) til 3 (store).

b Liten, Middels, Høy

c Hvor brått kommer hendelsen: Raskt eller Sakte.

d Kort, Middels, Lang eller Ukjent (ikke kvantifiserbar, avhenger av omstendigheter og system).

e Styringssystemer for varme, lys, alarmer, IT-systemer – alt som ikke fordrer personer til stede for å fungere.

f Graderingen (konsekvenser) antar at nødstrøm finnes.

De ulike risikoene – det kan gjerne være flere hundre av dem – samles og systematiseres, prioriteres og evalueres. Sannsynlighet for fore-

komst og forventede konsekvenser er opplagte faktorer som påvirker prioriteringen. Der det er naturlig, introduseres effekten av forebyggende tiltak i bildet, og flytter prioriteringen nedover på listen sammen med risikofaktoren.

Uten verktøy og hjelpemidler er dette en uoverkommelig oppgave – med mindre vi begrenser oss til de aller største risikofaktorene. En slik innsnevring av fokus er imidlertid lite tilrådelig: Sjansene er store for at vi får med oss de mest innlysende i stedet for de mest sannsynlige risikoene.

En så omfattende oppgave krever innsikt og kunnskap, samt metodikk og verktøy. Vi har allerede nevnt noen viktige kilder i så måte. I 1997 publiserte DRJ artikkelen *Risk Analysis Techniques* av ekspertene Geoffrey H. Wold og Robert F. Shriver,¹¹ som har dannet skole for utviklingen av verktøy og metodikk. Prinsippene er illustrert i tabell 1, og gir – til tross for at selve tabellen kan bli omfangsrik, både bedre oversikt og godt grunnlag for kvantifisering av trusler og prioritering av tiltak. Artikkelen beskriver hvordan vektallene bør fordeles og vektlegges for å komme frem til et retningsgivende resultat.

Neste utgave

I neste utgave fortsetter vi med konsekvensanalyse, som munner ut i en oversikt over hva planen bør inneholde. Vi avslutter med en diskusjon om implementasjon, testing og opplæring – og nyttige referanser til maler og verktøy. ■

¹¹ Artikkelen finnes på adressen http://www.drj.com/new2dr/w3_030.htm.