Drejebog til udarbejdelse af beredskabsplaner

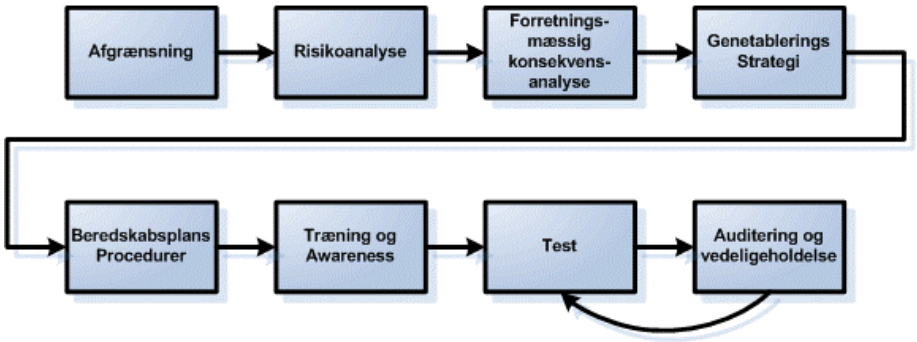
Udarbejdet for Københavns Universitet

Indholdsfortegnelse

1 Indledning

Dette dokument er udarbejdet for Københavns Universitet, og indeholder en ”drejebog” over de elementer, som en it-beredskabsplan bør indeholde.

For at få gennemløbet drejebogen i den mest relevante rækkefølge anvendes nedenstående model, der overordnet beskriver den proces, som PricewaterhouseCoopers (PwC) anbefaler følges i forbindelse med udarbejdelse af en beredskabsplan.



Figur 1: Overordnet model for udvikling af beredskabsplan

I afsnittene herefter vil de enkelte områder i ovenstående model blive gennemgået, og der vil blive beskrevet de ting, som bør adresseres inden for hvert af de enkelte områder.

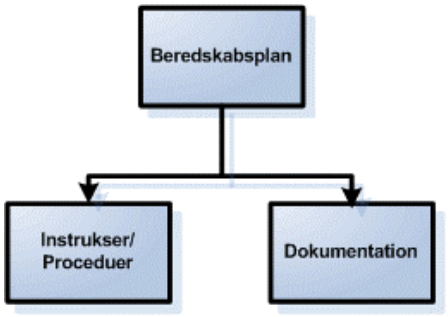
1.1 Beredskabsplanens definition

En beredskabsplan er overordnet set et dokument, som beskriver en række forskellige områder med hovedsigte på hurtigt og effektivt at få reetableret organisationens aktiviteter i tilfælde af utilsigtede hændelser.

For at opnå dette fastslår beredskabsprocessen typisk:

1. ”Hvem-gør-hvad”, hvornår og hvordan?
2. Har organisationen det faktuelle beredskab, såsom:
    a. tilstrækkelig dokumentation, som er direkte anvendelig
    b. den nødvendige backup på alle nødvendige systemer
    c. alternative kommunikationsmidler
    d. en beredskabsplan der dækker de resterende ikke it-relaterede områder, herunder:
        i. førstehjælp
        ii. evakueringsplaner
        iii. etc.

Opbygningen af beredskabsplans-”komplekset” er typisk forskellig fra organisation til organisation, men i dette dokument tages udgangspunkt i nedenstående opbygning:



Figur 2: Delelementer i en beredskabsplan

Det vil sige, at hele komplekset består af:

1. den overordnede beredskabsplan med alle formalia
2. en række specifikke instrukser (eller procedurer jf. DS[1])
3. henvisninger til den relevante dokumentation[2].

Dette dokument vil primært gennemgå del 1 og 2 inden for en it-relateret beredskabsplan.

[1] Dansk Standard kalder de underliggende dokumenter procedurer, jf. DS-484 afsnit 14
[2] Det er væsentligt at bemærke, at en beredskabsplan ikke er en øvelse i at genskrive al virksomhedens dokumentation. I stedet refereres til denne dokumentation i planen.

2 Afgrænsning

Det første punkt i processen med at udarbejde en beredskabsplan er, jf. Figur 1, punktet *Afgrænsning.* Denne aktivitet går ud på at få defineret omfanget for udvikling af hele beredskabsplanen og det dertilhørende kompleks. Da omfanget af beredskabsplanen også definerer, hvor risikovillig organisationen er, er det vigtigt at få afklaret områderne under dette punkt med **ledelsen.**

2.1 Omfang

At estimere omfanget af en beredskabsplan er ikke altid ligetil. Organisationen kan med fordel starte med at beskrive de scenarier, som den ønsker skal dækkes af beredskabsplanen. Det kan f.eks. afklares, om beredskabsplanen skal kunne håndtere:

- en isoleret brand i et serverrum
- et omfattende virusudbrud
- en storbrand i serverrumet og evt. hele den omkringliggende bygning
- en eksplosion i en UPS, som kvæster den centrale it-ansvarlige
- alle eller kun kritiske udvalgte dele af organisationens infrastruktur
- etc.

Ovenstående afklarer, om omfanget skal være altfavnende eller begrænset, f.eks. på baggrund af de tilgængelige ressourcer, hvilket i øvrigt er det mest almindelige. Nu vil det være muligt at forsøge at definere et ressourcemæssigt budget for udarbejdelsen[3]. Dette kan f.eks. være:

- tidsforbrug i mandetimer
- økonomiske investeringer i udstyr til beredskab
- tidsmæssige begrænsninger, i form af en deadlines.

I ovenstående budget skal det også overvejes, i hvilket omfang test og uddannelse ønskes inddraget[4], hvilket vil påvirke budgettet.

[3] DS 14.1.1. f
[4] Selve udarbejdelsen af en eventuel test og typer af mulige tests er beskrevet

2.2 Struktur for beredskabsplanen

En anden del af afgrænsningen er opdelingen af beredskabsplanen. Beredskabsplaner kan typisk opdeles i de delkomponenter, der er illustreret i Figur 2 herunder:

Figur 3: Beredskabsplanens delkomponenter

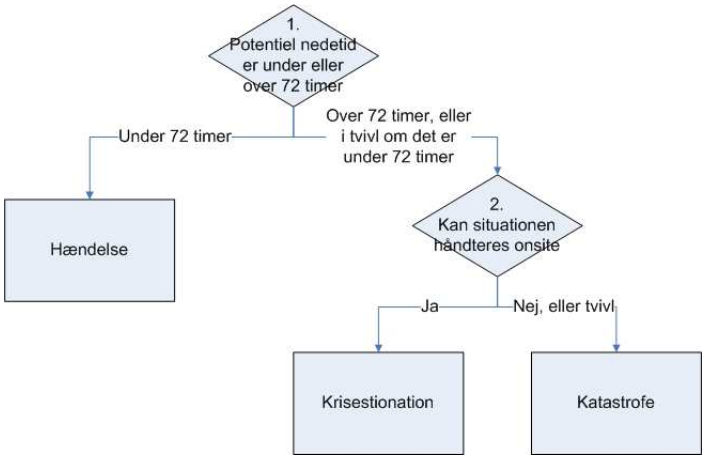
Denne opdeling afspejler i meget høj grad de valg, som blev truffet i forbindelse med de scenarier, som planen skal kunne håndtere.

Hændelseshåndtering beskriver, hvorledes organisationen håndterer hændelser, som påvirker organisationens drift i begrænset grad. Dette kunne f.eks. være et total servernedbrud i en central server, et virus udbrud etc.

Krisehåndtering håndterer større hændelser, som for alvor påvirker organisationens drift, men hvor den fysiske lokation er intakt. Dette kunne f.eks. være en mindre brand i kabelbakker, en UPS der eksploderer i serverrummet osv.

Katastrofehåndtering skal sikre, at selvom essentielle dele af driftsfaciliteterne er forsvundet, så kan forretningen stadig fungere. Dette kan f.eks. være ved en brand i serverrummet eller en bombetrussel mod lokationen, som opretholdes i længere tid. I så fald må man kan genetablere driften på en anden lokation. Så denne plans fokus er i høj grad et lokationsskift.

En anden måde at illustrere dette på er vist i Figur 4 herunder. Her er der ud over lokationsproblematikken også fokuseret på genetableringstiden.



Figur 4: Beslutningstræ for etablering af nøddrift

Alt efter størrelsen på organisationen, så kan disse tre delplaner enten være i en stor plan eller delt op i de tre dele. En række organisationer vælger også at afgrænse sig fra at kunne håndtere større katastrofer, som f.eks. ødelæggelse af et serverrum.

Ovenstående kan opsummeres i følgende valg som organisationen skal træffe:

Område	Truffet valg
Er der et minimumsniveau af hændelser, som beredskabsplanen skal håndtere?	
Er der nogen specifikke systemer, der som minimum skal være inkluderet?	
Er der nogen systemer, der tilnærmelsesvist altid vil køre?	
Hvilke rammer er der afsat til udarbejdelse af beredskabsplanen? • Økonomiske? • Mandetimer?	
Tidsplaner • Er der krav om, at planen skal være færdig på et givent tidspunkt?	
Ønsker vi kun at få udarbejdet en beredskabsplan, eller skal den også integreres i organisationen? Hvis den skal integreres, hvilket niveau ønskes så af • test • uddannelse • træning?	
Ønsker vi på baggrund af ovenstående en plan, som kan håndtere alt fra mindre hændelser til forretningskontinuitet i katastrofesituationer?	

Område	Truffet valg
Ønsker vi at kunne håndtere katastrofer, der omhandler flytning til en anden lokation? • Eller vil vi "bare" antage, at der altid vil være noget tilbage af den fysiske infrastruktur?	
Skal vi have det hele samlet i en plan? • Eller vil vi have den opdelt på en specifik måde?	
Er der en specifik grænse for længden af et acceptabelt driftsstop, som gælder for alle aktiver, før vi taler om en krise eller katastrofe? • Eller ønskes det defineret pr. aktiv[5]?	
Ønsker vi at involvere eksterne konsulenter, eller vil vi udarbejde beredskabsplan og beredskab selv?	

[5] Den maksimale tolerable nedetid (MTD) pr. aktiv vil blive defineret i en senere fase.

3 Risikoanalyse og forretningsmæssig konsekvensanalyse[6]

Der er allerede i dag et arbejde i gang på de forskellige fakulteter og institutter omkring udarbejdelse af risikoanalyser. For en forklaring af dette henvises til risikoanalyseprocesbeskrivelsen. I forbindelse med beredskabsplanlægningen antages det, at der er udført en risikoanalyse.

Den forretningsmæssige konsekvensanalyse tager udgangspunkt i den foretagne risikoanalyse, og udbygger denne ved at omfatte yderligere aktiver, som anses for værende kritiske, men som måske havde en mindre værdi end det cut, der bliver udarbejdet under risikoanalysen. For at finde disse yderligere kritiske aktiver, kan følgende fremgangsmåde anvendes:

1. De kritiske processer i organisationen identificeres[7]
2. De it-aktiver, der understøtter ovenstående processer, identificeres
3. Aktivlisten fra risikoanalysen sammenholdes med ovenstående liste, og eventuelle mangler tilføjes.

Når den samlede liste af aktiver er identificeret, skal følgende defineres for hvert aktiv:

1. Had er den maksimale nedetid (MTD), som forretningen kan acceptere?
   - Med dette menes den maksimale periode, som dette aktiv må være nede, før organisationen vil være væsentligt mærket af dette.
2. Hvilke andre aktiver er dette aktiv afhængig af for at kunne fungere?
   - Det skal sikres, at de aktiver, som udpeges her, også kommer på listen over kritiske aktiver.

Når denne fase er overstået, bør organisationen have følgende:

Område	Findes JA/NEJ
En liste over alle kritiske processer	
En liste over alle forretningskritiske aktiver[8], rangeret efter MTD, som illustrerer, i hvilken rækkefølge aktiver skal genetableres.	
En liste (eller graf), der illustrerer sammenhængene mellem de aktiver, der er nødvendige for, at de forretningskritiske aktiver fungerer efter hensigten. Et eksempel på en sådan graf er at finde i figuren herunder.	

Figur 5: Eksempel på et afhængighedsgraf

[6] Overordnet beskrevet i DS afsnit 4 og 14.1.2
[7] DS 14.1.1 a og b
[8] DS 14.1.1 b og c

4 Genetableringsstrategi

Under genetableringsstrategien udvælges og beskrives, hvorledes de krav, som ledelsen har stillet omkring forretningskontinuitet, rent faktisk skal implementeres. Alt efter det niveau, som ledelsen har lagt i afsnit 2.1, og den liste af aktiver, der er udarbejdet herover i afsnit 3, så skal følgende spørgsmål besvares om sikringen af centrale komponenter[9]:

Område	Svar
Har vi nogen kritiske servere/enheder, hvor MTD er meget lille, eller som ledelsen har defineret som værende meget kritiske jf. afsnit 2.2?	
Hvis ja[10]: - Skal disse enheder yderligere dubleres? - Har vi enheder, hvor vi skal have redundant drift i et sekundært driftscenter? - Er der data, vi skal have spejlet? Eller har vi allerede gjort tilstrækkeligt på komponentniveau?	
Har vi nogle it-aktiver, som skal fungere i tilfælde af strømafbrud?	
Hvis ja: - Hvor lang en tidshorisont ønskes sikret? o Er korttidssikring tilstrækkeligt (UPS)? o Skal vi have langtidssikring (Generator)?	

Når de komponentorienterede spørgsmål er besvaret, skal der, alt efter ledelsens ønske omkring håndtering af den kontinuerte drift, tages stilling til mere "fysiske" aspekter.

Område	Svar
Har vi nogle it-aktiver, som skal fungere i tilfælde af strømafbrud?	
Hvis ja: - Hvor lang en tidshorisont ønskes sikret? o Er korttidssikring tilstrækkeligt (UPS)? o Skal vi have langtidssikring (Generator)?	
Har vi et generelt behov for at sikre vores drift, også i tilfælde af f.eks. totalt nedbrud af vores serverrum eller anden central infrastruktur[11]?	

[9] Ledelsen skal sandsynligvis inddrages i besvarelsen af nedenstående spørgsmål.
[10] DS 14.1.1 e
[11] DS afsnit 14.1.3

Område	Svar
Hvis Ja • Hvor hurtigt skal vi kunne reetablere driften?	
Hvad skal en ekstern lokation kunne tilbyde, for at organisationen kan reetablere driften inden for den givne tidsramme? a) Lokal, fysisk kabling og strøm (Cold Site) (minimalistisk) b) a + enkelte kritiske aktiver (Warm Site) (nødvendig for kritiske servere) c) b + komplet dublering af alle systemer (Hot Site) d) c + kontinuert kopiering af produktionsdata mellem lokationer (Mirrored Site) a) er selvfølgelig den billigste løsning, mens d) er den dyreste.	
Er der nogen oplagte steder, hvor vi vil kunne genetablere driften, som overholder vores krav herover[12]? • Er der et nabofakultet eller -institut? • Er der en god samarbejdspartner?	

Når ovenstående detaljer er blevet afklaret, skal alle kontrakter med eksterne leverandører, som skal være med til at understøtte vores genetableringsstrategi, gennemgås. Dette kan f.eks. være kontrakter om:

1. Levering af nye komponenter, som f.eks. servere og infrastrukturkomponenter
2. Levering af diesel eller andet brændstof til generatorer
3. Fremmøde af konsulenter, håndværkere, vikarer ol. i krisesituationer
4. Råderet over lokaler, maskinstuer, serverrum, serverkraft, lagringskapacitet ol.
5. Adgang til og transport af backupbånd fra eksterne lokationer - også uden for normal åbningstid.

Nr. 5 vil oftest være en af de mest vigtige, da det er essentielt, at backuppen er tilgængelig på rette sted og tid.

[12] Man skal være opmærksom på, at de midlertidige lokaler skal have samme sikkerhedsniveau som den daglige lokation, jf. DS 14.1.3 nederst.

5 Beredskabsplansprocedurer

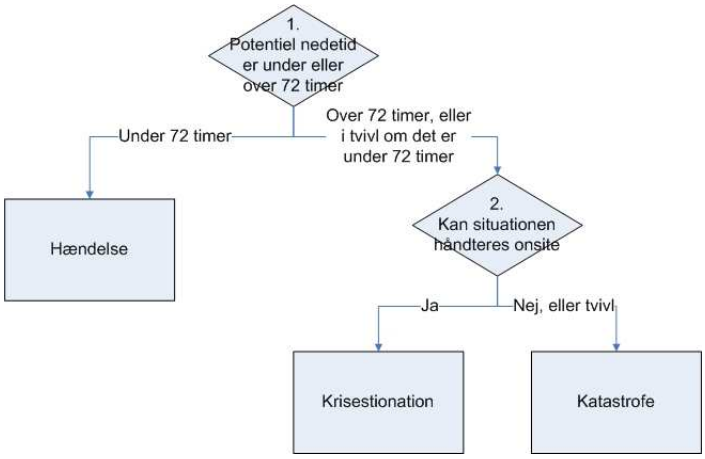
Efter at have afklaret grundlaget for selve beredskabsplanen skal denne udarbejdes[13]. Uanset størrelsen på organisationen er der en række forskellige områder, der skal berøres - disse er nævnt herunder.

5.1 Varsling af katastrofe

Område	Svar
Er der en klar definition af betingelser for aktivering af beredskabsplanen og de procedurer, som skal følges i forbindelse med aktivering[14]?	
Hvem kan beslutte om en hændelse er en katastrofe og dermed iværksætte beredskabet?	
Hvad hvis de beslutningsmyndige personer ikke er til stede, hvordan håndteres varslingen så?	
Eskaleringsplan: Hvis der er forskellige måder at håndtere de 3 niveauer i beredskabsplanen på, hvornår er noget så en: - hændelse? - krise? - katastrofe? Hvornår i forløbet kan man evt. ”opgradere” en hændelse? Er der særlige tidspunkter, hvor hændelsen skal revurderes? • Hver time? • Hver anden time? Hvem kan ”opgradere” eller ”nedgradere” hændelsen?	

[13] DS afsnit 14.1.3 generelt
[14] DS 14.1.4 a

Husk, at en måde definere forskellen mellem hændelse, krise og katastrofe kan være som en kombination af den forventede tid inden genetablering kombineret med omfanget af hændelsen, hvilket er illustreret herunder:

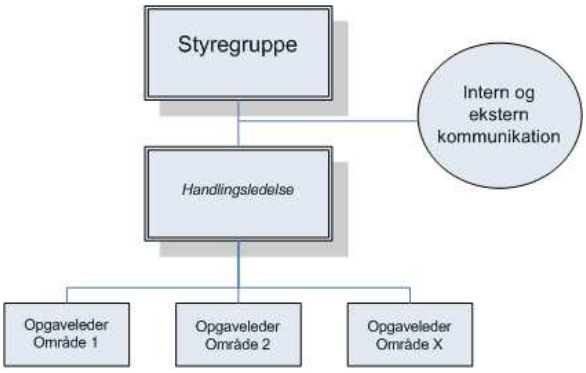


Figur 6: Beslutningstræ for etablering af nøddrift

5.2 Beredskabsorganisation

Et af de essentielle punkter i beredskabsplanen er at få defineret selve beredskabsorganisationen. Her er det vigtigt, at alle essentielle ansvarsområder er defineret, og at de involverede i planen har fået besked herom.

En beredskabsorganisation kan se ud som illustreret i eksemplet herunder:



Figur 7: Organigram over katastrofeorganisationen

Selve ansvarsområderne, som de enkelte personer i katastrofeorganisationen har, skal selvfølgelig beskrives nærmere.

Nogle af de spørgsmål, der skal besvares i forbindelse med etablering af beredskabsorganisationen, er at finde herunder:

Område	Svar
Hvordan ser vores katastrofeorganisation ud?	
Hvem er handlingsledelse for organisationen?	
Hvem har ansvaret for[15]: - den tekniske del? o servere o klienter o infrastruktur (switche, firewalls) - den fysiske del? o bygninger o intern vedligeholdelse o samarbejdet med eksterne leverandører ▪ VVS-folk ▪ elektrikere ▪ murere - ekstern kommunikation? - intern kommunikation? Har vi udpeget stedfortrædere for ALLE ansvarsområder?	
Ligger der en beskrivelse af hvilke opgaver, der ligger inden for hvert af ovenstående ansvarsområder?	

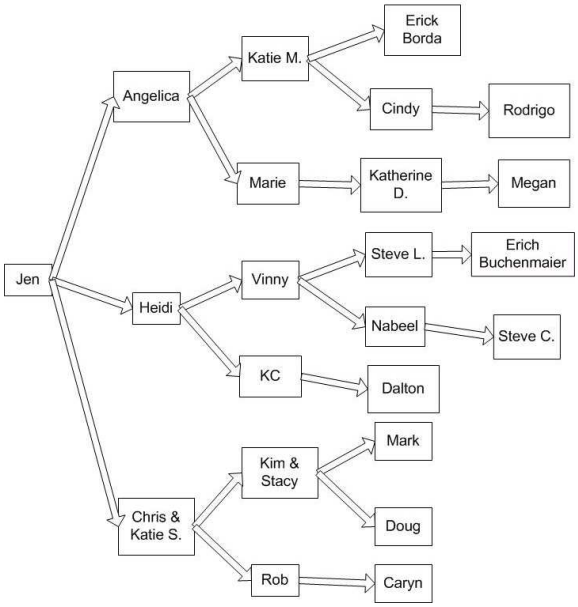
En vigtig del af det at have en beredskabsorganisation er, at det er muligt at få fat i de personer, der er en del af beredskabsorganisationen. Til dette formål er en opdateret telefonliste essentiel. Denne kan f.eks. indeholde følgende dele:

Navn	Telefon-1	Telefon-2	Rolle/Ansvarsområde	Billede
			Direktør, medlem af både styregruppe og handlingsledelse Kommunikationsansvarlig	{Indsæt billede}
			Produktionschef Teknisk ansvar, ekskl. applikation og telefon-central	{Indsæt billede}
			Overordnet applikationsansvar	..
			Ansvar for al decentral teknik	..

[15] DS 14.1.4 h.

Det er en fordel ud over de mest almindelige kontaktoplysninger også at have et billede tilknyttet hver person, således at eksterne parter i en krisesituation også kan finde en given person.

Derudover kan det være en fordel at definere en telefonkæde[16], enten hvor en eller flere har ansvaret for at ringe til alle, eller en rigtig kæde, hvor det er defineret, hvem den næste i kæden er, så alle ved, hvem de skal ringe til. Sidstnævnte er illustreret herunder:



Figur 8: Eksempel på telefonkæde

[16] Telefonkæde bør dække over private, mobilnummer- og SMS-kæder eller andre løsninger, som sikrer, at kommunikationen kan etableres

5.3 Instrukser

Instrukser er udstukne regler, som skal følges. Instrukser kan f.eks. være ”instruks om skadesvurdering” eller ”instruks for reetablering af data”.

5.3.1 Hvor skal vi mødes?

Hvis der opereres med en plan, der håndterer katastrofer, er det vigtigt at beskrive, hvor alle skal samles i tilfælde af f.eks. en storbrand. Beskrivelsen kan kombineres med f.eks. et oversigtsbillede:

”I tilfælde af brand mødes vi ved pølsevognen på bagsiden af Vor Frue Kirke”

5.3.2 Genetablering af systemer

Ud over de organisatoriske aspekter skal der også etableres instrukser for genetablering af forskellige typer af enheder[17].

Herunder er et eksempel på en instruks for genetablering af en Windows-server.

Nr.	Action	Noter
1.	Udføres af:	
2.	Klargør hardware, der matcher de nødvendige krav som specificeret i dokumentationen for systemet. ▪ Hvis ikke der er hardware tilgængeligt, bestil dette hos leverandør XX. LINK til instruks for bestilling	

[17] DS 14.1.3 d

3.	Udfør præinstallation af basis-software (Windows og backupklient) LINK til procedurer for udførelse af præinstallation.	
4.	Genskab systemtilstande (eks. systemstate) fra backupbånd. LINK til procedure for bestilling/fremfinding af backupbånd.	
5.	Genskab backup fra bånd LINK til procedure for backup-restore.	
6.	Kontroller etableret backup i henhold til dokumentationen udarbejdet for hvert enkelt system, kaldet ”Klargøring af xxxx”, hvor xxxx er navnet på servicen.	
7.	Oplys handlingsledelsen om status på genetablering.	
8.	Kontakttidspunkt til handlingsledelsen.	
9.	Evt. opfølgning efter denne kontakt.	
10.	Kommentarer og yderligere information.	

Som det fremgår af instruksen, er den forholdsvis simpel, da dens primære opgave er at dirigere folk hen til de korrekte procedurer og den korrekte dokumentation, således at serveren kan genetableres bedst muligt.

Det vil være en meget stor fordel, hvis beredskabsinstrukserne også anvendes i den daglige drift, således at det kontinuert bliver ”testet”, om instrukserne fungerer.

5.4 Dokumentation

Grundlaget for enhver effektiv beredskabsplan er den underliggende dokumentation[18], der rent faktisk er anvendelig. Beredskabsplanen skal ikke opfinde ny dokumentation, medmindre den eksisterende tilnærmelsesvist er ikke-eksisterende eller ikke er tilstrækkelig. Beredskabsplansprojektet skal i langt højere grad **stille krav** til den eksisterende dokumentation.

Dokumentation bør indeholde en beskrivelse, der gør personalet i stand til at reetablere systemet. Dokumentationen bør kunne forstås af en udenforstående, og den bør kunne gøre vedkommende i stand til at genetablere systemet fra "bare-metal"[19].

Dokumentation bør gøre brug af henvisninger til øvrig dokumentation, ellers bliver det alt for omfattende at anvende i praksis. Dokumentationen kan sammenlignes med et bibliotek, som indeholder et samlet arkiv for de kritiske systemer. Det kan f.eks. være: brugermanualer, backup- og restore-procedurer, applikationsspecifikke beskrivelser, leverandørdokumentation og softwaremedier etc.

Dokumentationen af systemer bør som minimum dække følgende 3 niveauer:

1. **Detaljeret beskrivelse** af alle grundkomponenter, f.eks.:
    - ID
    - Type (Server, Infrastruktur, Klient)
    - Model
    - CPU
    - RAM
    - Harddisk
        - Partitioner
    - Placering i rack
    - Skærmswitch
    - Ejer
    - MTD
    - Værdi i risikoanalyse
    - Nødvendige password (behørigt sikret - evt. i særskilt krypteret liste).
2. **Konfigurationsbeskrivelse** af alle grundkomponenter
    - Således installeres denne server og alle services igen fra "bare-metal".
3. **Afhængighedsbeskrivelse** af, hvorledes de væsentligste systemer[20] er afhængige af andre systemer og services, således at der ultimativt er dokumenteret en hel række af afhængigheder, så det er dokumenteret, i hvilken rækkefølge ALLE enheder skal genetableres og startes. Dette giver også en bedre mulighed for at identificere de systemer, der vil blive påvirket af en enkelt defekt komponent.

---

[18] DS generelt 14.1.4 og 14.1.3 d og e

[19] Med "bare-metal" menes helt fra bunden, såfremt en ny server blev stillet til rådighed, hvilket ofte vil være situationen i forbindelse med en katastrofesituation.

[20] De væsentligste systemer er fundet under dels risikoanalysen og dels under den forretningsmæssige konsekvensanalyse.

Sidstnævnte kan f.eks. vises i et afhængighedstræ som illustreret herunder:

Figur 9: Eksempel på et afhængighedstræ

Når dokumentationen er inkorporeret i beredskabsplanen, kan følgende kontrolspørgsmål være med til at sikre, at dokumentationen har et tilstrækkeligt niveau. Hvis der ikke er svar på spørgsmålene, bør dokumentationen revurderes, indtil der er svar på nedenstående.

Kontrolspørgsmål	Svar
Hvis en service stopper, kan vi så fastslå, hvilken påvirkning dette vil have på andre services? • Ved vi, hvem vi skal ringe til for at fortælle, at dette vil blive et problem?	
Hvordan opdager vi, at en service stopper?	
Hvis der skal leveres en ny server til vores centrale database, vil vi så kunne genetablere og få den til at køre fra grunden? • Hvad vil tidshorisonten være for ovenstående øvelse? • Vil vi kunne se, hvilken størrelse harddiske og ram vi skal bestille? • Vil vi kunne se, hvordan harddisken skal partitioneres?	
Forefindes der backup- og restoredokumentation til alle identificerede systemer? • Vil denne kunne forstås af en ekstern person, som ikke er en del af den daglige drift?	
Hvis vi anvender ekstern backuplagring, hvor hurtigt vil vi så kunne få denne ud til en ekstern lokation?	
Findes der manuelle arbejdsprocesser, der kan erstatte de it-baserede funktioner for en periode, såfremt de it-baserede funktioner ikke er tilgængelige?	

5.5 Krisekommunikation

Der bør udarbejdes en kommunikationsplan, som adresserer, hvorledes der kommunikeres, dels internt, og dels til eksterne interessenter, hvis krisen er af en sådan karakter.

Kommunikationen i forbindelse med krisen omhandler kommunikation før, under og efter aktivering af beredskabsplanen. Der bør være en klar sammenhæng med universitetets generelle presse- og kommunikationspolitik, herunder at det måske er KU's pressekorps, som udtaler sig om sager, der påvirker universitetet som helhed.

Kontrolspørgsmål	Svar
Hvem ejer kommunikationsplanen?	
Hvorledes kommunikeres internt i tilfælde af en beredskabssituation? • Fungerer denne type af kommunikation også, hvis f.eks. intranet, mail og alm. telefon er ude af drift[21]?	
Hvem varetager kommunikation med pressen? • Har vi nogen standardbeskrivelser for, hvad der må siges?	

Også på dette område vil det være fornuftigt at udarbejde en instruks til den presseansvarlige, der sikrer, at nedenstående spørgsmål bliver adresseret, og at den presseansvarlige ved, hvor de relevante oplysninger findes:

- Hvilken type af krise er indtruffet?
- Hvilken type af "krisemanual" skal anvendes?
- Hvem er målgruppen?
    - Hvordan kommunikerer vi med dem?
    - Hvordan sikrer vi, at de har modtaget kommunikationen?
- Er der et overblik over, hvilke informationer vi skal udsende?
- Skal der følges en særlig instruks for informering af
    - interne ansatte
    - pårørende
    - kunder
    - medierne generelt?

[21] I dette tilfælde vil f.eks. en SMS-kæde, som illustreret i Figur 8, side 15, kunne anvendes i stedet - eller evt. et opslag på et foruddefineret sted som f.eks. en kantine eller lign.

5.6 Opbevaring af planen

Opbevaring af planer er et centralt punkt, så alle er i stand til at finde og tilgå beredskabsplanerne og øvrig dokumentation i tilfælde af en krise.

Planerne skal opbevares på en sådan måde, at det er muligt at få adgang til dem uanset krisen og dennes omfang. Ud over planerne skal anden relevant information og dokumentation være tilgængelig[22].

Informations- og dokumentationsmængden i beredskabsplanen kan være så omfattende, at det kan være vanskeligt at have alle oplysninger i papirform. Derfor bør det overvejes, hvordan det er praktisk muligt at opbevare dokumentationen.

Følgende bør undersøges og overvejes:

Kontrolspørgsmål	Svar
Er det muligt at gemme dokumentation/information på anden lokation? • I et spejlet miljø (elektronisk)? • Offsite lokation hos en 3 part? • I en "krisekuffert[23]" på et eller flere aftalte steder? • I papirudgaver hos f.eks. kriseledelsen? o Hvordan skal dette opdateres? På en eller flere bærbare PC'er?	

Vær opmærksom på, at beredskabsplanen indeholder væsentlige oplysninger om f.eks. infrastrukturen, oplysninger som kan kompromittere organisationens sikkerhed, hvis uvedkommende får adgang hertil. Det betyder, at ved opbevaring eksternt eller hos 3. part[24] skal der tages hensyn til dette. I praksis er det ikke unormalt, at selve beredskabsplanen er en papirudgave, og at den detaljerede systemdokumentation er i elektronisk form. Det sætter selvfølgelig krav til opbevaringen af systemdokumentationen, jf. ovenstående.

[22] DS 14.1.3 nederst
[23] En Krisekuffert indeholder planer, kommunikationsudstyr og anden relevant udstyr
[24] DS484 14.1.3 og 14.1.4

6 Træning, awareness og test

Efter at have udarbejdet selve planen skal denne også integreres i organisationen[25]. Som tidligere nævnt er det f.eks. vigtigt, at alle involverede i planen ved, at de har en rolle at spille, samt hvad deres ansvar præcist er. Dette gøres proaktivt gennem træning og informering af alle involverede, og kan efterfølgende kontrolleres ved at udføre en test af beredskabet. Der findes en række forskellige former for tests[26]:

- Tjeklistetest
  - De forskellige interessenter får en kopi af planen og kan komme med kommentarer.
- Structured walk through-test (skrivebordstest).
  - De forskellige interessenter samles og gennemgår planen sammen baseret på forskellige scenarier uden for alvor at simulere scenarierne.
- Simulationstest
  - Planen simuleres i forskellige scenarier, hvor der arbejdes med knappe ressourcer, tilkald af eksterne ressourcer. Alt dette op til, at systemer flyttes til et evt. ekstern site.
- Parallel test
  - Ressourcer flyttes til et eventuelt eksternt site, startes, og driften overflyttes/simuleres på disse "nye" systemer.

Ledelsen har allerede tidligere tilkendegivet et niveau på dette område. Herunder er en uddybning af de ting, der skal overvejes.

Kontrolspørgsmål	Svar
Hvor realistisk en test ønsker vi?	
Hvad må den koste?	
Ønsker vi en ekstern facilitator til at "opfinde" scenarier - og styre selve testen?	
Hvordan får vi dokumenteret fejl og mangler fundet under testen?	
Hvordan får vi implementeret fejl og mangler i beredskabsplanen, og hvem har ansvaret for dette?	

[25] DS14.1.3. f, og 14.1.5
[26] DS 14.1.5 a-f

Ud over at de enkelte involverede kender deres roller, så er det vigtigt, at selve organisationen ved, hvorledes en hændelse rapporteres og til hvem. Såfremt der i forvejen arbejdes med awareness (brugerbevisthedskampagner), vil dette med fordel kunne inkorporeres i den overordnede kampagne.

Kontrolspørgsmål	Svar
Ved brugerne, hvor de skal henvende sig til i tilfælde af en hændelse? - Central e-mail? - Hotline? - Den it-sikkerhedsansvarlige? - Direkte til den ansvarlige for beredskabsplanen?	
Ved brugerne, hvornår noget er en hændelse?	
Ved brugerne, om der er nogen ting, de skal sikre sig at få med ud af bygningerne, hvis der opstår en hændelse?	

7 Auditering og vedligeholdelse

Når planen er udarbejdet og efterfølgende testet, er der vigtigt, at planen kontinuert bliver opdateret[27]. For at sikre at planen løbende bliver opdateret, er det ydermere vigtigt, at der periodisk bliver udført en stikprøvekontrol for at se, om planen rent faktisk bliver opdateret.

Efter at opdateringsprocedurer er blevet beskrevet, kan følgende kontrolspørgsmål anvendes:

Kontrolspørgsmål	Svar
Hvem har det overordnede ansvar for, at planen bliver opdateret?	
Ønsker vi at uddelegere ansvaret vedrørende forskellige dele til nogle af de involverede?	
I hvilke aspekter af den daglige vedligeholdelse skal vi være opmærksomme på at få noteret rettelser, som kan have indflydelse på beredskabsplanen?	
Hvorledes "indberetter" vi rettelser til beredskabsplanen? - Centralt? - Decentralt?	
Hvordan og hvor ofte ønsker vi at kontrollere, om planen bliver opdateret?	
Hvem har ansvaret for at kontrollere dette?	

[27] DS 14.1.4 f