DIGITALISERINGSSTYRELSEN

Vejledning i it-beredskab

Januar 2022

2022

Indholdsfortegnelse

Formålet med denne vejledning er at styrke organisationers evne til at styre, planlægge, anvende og forbedre organisationens it-beredskab. Denne vejledning kan bruges til at forbedre kvaliteten af eksisterende it-beredskabsplanlægning eller til at komme i gang med nye planlægningsaktiviteter.

Vejledningen har også til formål at hjælpe statslige myndigheder med at efterleve dele af den internationale sikkerhedsstandard ISO 27001, som alle statslige myndigheder er pålagt at implementere. Af sikkerhedsstandardens Anneks A fremgår det, at organisationer skal fastlægge, dokumentere, implementere og vedligeholde processer, procedurer og kontroller for at sikre den nødvendige informationssikkerhedskontinuitet i en kritisk situation. Et it-beredskab er en plan for retablering af it-infrastruktur og –systemer, og it-beredskab bidrager til at efterleve standardens krav til forretningskontinuitet.

Vejledningen bør benyttes i sammenhæng med andre materialer på Sikkerdigital.dk, der vejleder om andre dele af informationssikkerhedsarbejdet, herunder it-risikostyring, it-leverandørstyring mm.

Denne vejledning erstatter publikationen ”Vejledning til it-beredskab” fra 2013 samt ”Guide til it-beredskabsstyring fra 2015”.

Vejledningen er til ledere og medarbejdere, der er involveret i implementering og vedligeholdelse af et ledelsessystem for informationssikkerhed (ISMS) baseret på ISO 27001, og som delaktivitet herunder er ansvarlig for at styre og vedligeholde et it-beredskab. Du kan eksempelvis være leder med ansvar for informationssikkerhed, medarbejder på sikkerhedsområdet eller beredskabsansvarlig.

I tillæg til vejledningen findes skabeloner for blandt andet it-beredskabsplaner, it-beredskabspolitik og miniberedskabsplan i lommeformat. Skabelonerne henvender sig både til organisationer med og organisationer uden egen it-drift.

Her kan du læse mere: Beredskabsstyring (sikkerdigital.dk) og
Vejledninger og skabeloner (sikkerdigital.dk)

1. Indledning

Hovedparten af offentlige myndigheder er afhængige af it-systemer for at kunne løse sine opgaver. Når myndigheder rammes af ekstraordinære hændelser, eksempelvis hackerangreb og netværksnedbrud, kan det medføre it-nedbrud eller tab af data. Et it-beredskab har til formål at ruste organisationer til denne type ekstraordinære hændelser. Som organisation har man behov for flere typer beredskaber, der kan håndtere de mange forskelligartede risici, som en organisation står overfor.

It-beredskab har til formål at styrke evnen til at håndtere hændelser, i et it-system når det er nødvendigt. Hændelser skal håndteres så hurtigt og effektivt som muligt, og det kan være nødvendigt at iværksætte alternative forretningsprocesser, mens it-systemet er ude af drift. Til dette formål udarbejdes it-beredskabsplaner, som beskriver, hvordan organisationen skal handle, når krisen sætter ind.

Større it-nedbrud eller tab af data hos myndigheder kan betyde, at myndigheden ikke er i stand til at varetage sine samfunds- og forretningskritiske funktioner. Det kan også betyde, at data ikke kan gendannes, eller at omkostningen ved gendannelse er meget høj. Det kan også betyde, at data er fejlbehæftede, hvilket også kan have stor betydning for en myndigheds evne til at løse sin opgave.

It-systemer der indgår i de kritiske forretningsprocesser er ofte afhængige af hinanden. Fx overføres data mellem it-systemerne, og nogle systemer skal være funktionsdygtige, før andre kan fungere. Et samlet velfungerende it-beredskab er derfor afhængigt af, at organisationen koordinerer it-beredskabet for de enkelte it-systemer i forretningsprocesserne.

Denne vejledning lægger vægt på vigtigheden af, at it-beredskabsplanlægningen tager udgangspunkt i en kortlægning af kritiske it-systemer og deres interne afhængigheder samt organisationens risiko- og konsekvensvurderinger.

1.1 Struktur på it-beredskabsarbejdet

Mange organisationer har allerede it-beredskabsplaner for kritiske systemer, men hvis disse planer ikke testes og revurderes løbende, vil deres effektivitet med stor sandsynlighed mindskes over tid. Dette kan eksempelvis skyldes, at truslerne mod organisationer ændres, hvorfor risikovurderinger, der ligger til grund for it-beredskabsplanlægningen, bør ændres.

Organisationens it-beredskab bør derfor tilrettelæges, så det sker struktureret, ensartet og som en løbende proces, hvor it-beredskabet kontinuerligt testes, evalueres og forbedres. Det anbefales at tage udgangspunkt i modellen "plan-do-

check-act", som er en model, der skal sikre kontinuerlig forbedring af it-beredskabet gennem gentagende processer af hhv. planlægning, implementering, test og evaluering af indsatsen.

Figur 1
Plan-do-check-act modellen

Plan: Vi analyserer og laver en plan for at forbedre vores it-beredskab
Do: Vi implementerer vores plan
Check: Vi tester vores plan, og om de forudsætninger, som den bygger på holder
Act: Vi samler læring op fra testen, og justerer vores it-beredskab.

1.2 Vejledningens struktur

Denne vejledning er struktureret med udgangspunkt i logikken og strukturen fra denne model. Vejledningen er derfor bygget op som følger:

- **Ledelsesansvar**: Ledelsen træffer beslutning om organisationens prioriteter, herunder hvilke risici man kan og ikke kan acceptere.

- **Planlægningsgrundlag**: Kortlægning af kritiske it-systemer, deres interne afhængigheder samt risiko- og konsekvensanalyser danner grundlag for it-beredskabet.
- **Forebyggelse:** Præventive tiltag, der kan forhindre hændelser eller reducere deres sandsynlighed og konsekvenser
- **It-beredskabsplaner**: Planer der beskriver, hvordan man har forberedt sig på at håndtere ekstraordinære hændelser på en struktureret og ensartet måde.
- **Uddannelse**: Alle der har en rolle i organisationens it-beredskab, bør opkvalificeres til at varetage opgaven.
- **Øvelser/test**: Organisationen bør kontinuerligt øve alle faser i it-beredskabet.
- **Evalueringer og forbedringstiltag**: Øvelser evalueres og der udarbejdes forbedringstiltag på baggrund heraf.

Denne struktur læner sig op ad Beredskabsstyrelsens struktur i vejledningen "Helhedsorienteret beredskabsplanlægning" med det formål at lette koordineringen af it-beredskabet med det øvrige beredskab i organisationen.

I denne vejledning opereres med tre typer handleplaner, som bidrager til det samlede it-beredskab:

Forretningsnødplan	En plan for hvordan organisationen håndterer og viderefører de opgaver og forretningsprocesser, som påvirkes ved en it-beredskabssituation. Den beskriver, hvilke nødprocedurer organisationen eventuelt kan tage i brug i tilfælde af et nedbrud på de it-systemer, som normalt varetager opgaverne.
Intern krisestyringsplan	En plan for den interne krisestyring i organisationen under en it-beredskabssituation. Dvs. at planen fastlægger en governance for, hvordan den midlertidige organisation skal se ud under en beredskabssituation
Reetableringsplan	En teknisk plan for, hvordan it-systemer skal reetableres under en it-beredskabssituation. Opgaven skal ofte løftes af eksterne leverandører af it.-systemer.

2. Ledelsesansvar

Ledelsen har ansvaret for, at organisationen råder over et passende it-beredskab. Princippet for aktiv involvering af ledelsen i it-beredskabsplanlægningen adskiller sig ikke fra organisationens øvrige ansvarsområder. Dvs. at det er ledelsen, der skal fastsætte målsætninger, foretage overordnede prioriteringer, uddelegere opgaver, tildele ressourcer og følge op på fremdriften i planlægningen.

2.1 It-beredskabspolitik

Ledelsen bør derfor sikre, at der udarbejdes en it-beredskabspolitik, som fastlægger de grundlæggende rammer for, hvordan it-beredskabsplaner skal udarbejdes. Politikken fastlægger klare mål, vision og ansvarsfordeling, som er en forudsætning for udarbejdelsen af et effektivt it-beredskab. Offentlige myndigheder kan eventuelt udarbejde en koncernfælles it-beredskabspolitik, som gælder på tværs af et ministeriums departement og styrelser.

It-beredskabspolitikken bør tage stilling til følgende:

- Hvad er målet med it-beredskabet?
- Hvilke formelle krav (love og regler) skal organisationen opfylde?
- Hvilke kritiske it-funktioner har organisationen et beredskabsmæssigt ansvar for at opretholde?
- Hvordan er roller og ansvar for it-beredskabet fordelt?

For mere information om tilrettelæggelse af informationssikkerhedspolitikker henvises til "Vejledning i politikker for informationssikkerhed".

2.2 Årshjul for it-beredskab

Med udgangspunkt i organisationens it-beredskabspolitik, udarbejdes et årshjul for it-beredskab (et it-beredskabsprogram), som omdanner ledelsens overordnede prioriteter til konkrete aktiviteter, som skal understøtte test og justering af beredskabet i løbet af et år.

Årshjulet for et it-beredskab bør indeholde:

- En prioritering af aktiviteter i den kommende periode
- Hvordan arbejdet organiseres, og hvem der har ansvar for hvilke opgaver
- Hvordan ledelsen løbende involveres i:
    - Prioritering af fokusområder i it-beredskabet
    - Aktiv deltagelse i it-beredskabet
    - Evaluering af it-beredskabet

Disse fokuspunkter bidrager til at sikre, at it-beredskabsarbejdet afspejler ledelsens prioriteringer og vil dermed forbedre muligheden for en sammenhængende og effektiv it-beredskabsplanlægning.

** Tip: It-beredskabsprogrammets aktiviteter bør indarbejdes i årshjul for de samlede informationssikkerhedsindsatser.*

For mere information om planlægning af it-sikkerhedsarbejde henvises til "Vejledning i planlægning af sikkerhedsarbejdet". "Skabelon til it-beredskabspolitik" kan desuden benyttes i forbindelse med dette arbejde

Tjekliste:

- Er der etableret en (koncernfælles) it-beredskabspolitik, som fastsætter den overordnede ramme for organisationens it-beredskabsarbejde?
- Er der, på baggrund af it-beredskabspolitikken, udarbejdet et årshjul/it-beredskabsprogram, som omdanner it-beredskabspolitikkens mål til konkrete aktiviteter?

3. Planlægningsgrundlag

Organisationens it-beredskab har til formål at håndtere hændelser mod de kritiske forretningsprocesser og deres understøttende it-systemer. Derfor er det afgørende for det videre arbejde med it-beredskabet at få skabt et grundigt overblik over organisationens kritiske forretningsprocesser, og de systemer, som understøtter dem. Organisationen bør derfor få overblik over,

- hvilke forretningsprocesser i organisationen, som er samfunds- eller forretningskritiske
- hvilke it-systemer der understøtter de samfunds- eller forretningskritiske processer
- hvilke interne afhængigheder, der er mellem it-systemer, der understøtter samfunds- eller forretningskritiske processer
- hvilke trusler der er imod organisationen
- hvilke risici organisationen bør håndtere

3.1 Kortlægning af kritiske forretningsprocesser og understøttende it-systemer

Der skal dannes et overblik over, hvilke forretningsprocesser og tilhørende it-systemer, som er nødvendige for, at organisationen kan varetage sine opgaver. Dette overblik danner grundlag for at kunne prioritere, hvilke forretningsprocesser og it-systemer, der skal kunne opretholdes, selvom organisationen påvirkes af ekstraordinære hændelser, og/eller hvis genopretning skal prioriteres først i en beredskabssituation.

I forbindelse med kortlægningen er det centralt at identificere, hvilke systemer som understøtter hhv. samfunds- og forretningskritiske funktioner.

- **Samfundskritiske it-systemer** er it-systemer, hvor større driftsforstyrrelser resulterer i væsentlige udfordringer for samfundet som helhed fx i form af økonomiske tab hos stat, virksomheder eller borgere, længerevarende nedbrud af kritisk infrastruktur eller reelle trusler for den nationale sikkerhed. Samfundskritiske it-systemer er således it-systemer, hvor utilgængelighed og driftsustabilitet i it-systemerne kan få markante følger for samfundet og for opretholdelsen af samfundskritiske processer.

- **Forretningskritiske it-systemer** er it-systemer, hvor driftsforstyrrelser kan medføre, at størstedelen af myndighedens medarbejdere ikke kan arbejde, eller at myndigheden vanskeligt kan overholde sine forvaltningsmæssige forpligtigelser.

Denne kortlægning følger også af krav til statslige myndigheder i model for porteføljestyring af statslige it-systemer. For mere information om kortlægning af kritiske forretningsprocesser og understøttende it-systemer kan "Model for porteføljestyring af statslige it-systemer" benyttes.

3.2 Kortlægning af interne afhængigheder mellem systemer

Foruden at skabe et overblik over kritiske forretningsprocesser og underliggende it-systemer, er det også vigtigt systematisk at kortlægge eventuelle afhængigheder mellem pågældende it-systemer. Dvs. hvilke systemer som skal være i drift før de øvrige it-systemer i forretningsprocessen er funktionsdygtige.

Et overblik over afhængigheder har dels betydning for evnen til at begrænse følgevirkningerne af en ekstraordinær hændelse. Dels har det betydning for organisationens evne til at prioritere it-beredskabsarbejdet – herunder rækkefølgen på reetableringen af it-systemer (mere herom i kapitel 5 om it-beredskabsplaner).

Kortlægningen kan udføres ved at udarbejde lister over kritiske funktioner og kritiske it-systemer. Det anbefales, at der udelukkende fokuseres på samfunds- og forretningskritiske funktioner og it-systemer, så listerne ikke bliver unødigt lange.

Tjekliste til den offentlige myndighed:

- Er samfunds- eller forretningskritiske processer kortlagt?
- Er understøttende it-systemer kortlagt?
- Er interne afhængigheder mellem understøttende it-systemer kortlagt?

3.3 Risiko- og konsekvensvurderinger

Som organisation står man med en lang række risici af forskellig karakter. Det er for ressourcekrævende at forsøge at håndtere dem alle, hvorfor man bør prioritere. It-beredskabet bør tilrettelægges, så det målrettes de største konsekvenser for forretningen.

Systemspecifikke risikovurderinger

Det er vigtigt at sikre, at risikovurderinger er rettet mod de relevante it-systemer. Det vil sige, at det ikke er tilstrækkeligt udelukkende at lave risikovurderinger af forhold på meget overordnet niveau i organisationen. Der skal også udarbejdes vurderinger af de direkte konsekvenser, hvis et it-system ikke leverer nødvendig datakvalitet til en given forretningsproces.

Risikovurderinger af tværgående afhængigheder

Risikovurderinger skal ikke blot være vurderinger af det enkelte it-system, men også af eventuelle afhængigheder til andre it-systemer og støttesystemer. Fx skal det belyses, hvilke andre systemer, som et kritisk system er afhængigt af. Det kan være meget komplekst at identificere disse afhængigheder, men det er vigtigt at gøre forsøget.

For mere viden og vejledning i håndteringen af risici, henvises til "Vejledning til risikostyring inden for informationssikkerhed" på Sikkerdigital.dk

3.4 Vurdering af it-systemers nedetid (RTO) og datatab (RPO)

På baggrund af organisationens risiko- og konsekvensvurderinger skal det besluttes, hvad forretningsprocessernes maksimale nedetid er (MTD). På baggrund heraf vurderes det, hvor længe de understøttende it-systemer kan accepteres at være nede (RTO eller recovery time objective) under en hændelse, og hvor stort et datatab (RPO eller recovery point objective) der kan accepteres. Målet med it-beredskabsplaner er, at organisationen er i stand til at håndtere ekstraordinær hændelser uden at overskride fastsatte grænser for maksimal nedetid af it-systemer og maksimalt datatab.

Når organisationen stiller krav til de enkelte it-systemers grænser for nedetid og datatab, er det vigtigt at koordinere kravene for de it-systemer, som er afhængige af hinanden. Man bør altså sikre sig, at de it-systemer, der løbende udveksler data i forretningsprocesserne, har nogle krav der stemmer overens med hinanden. Disse krav til RTO og RPO er centrale, når it-beredskabsplaner skal udarbejdes (mere om dette i kapitel 5 om it-beredskabsplaner).

Figur 2
Etablering af et fokuseret it-beredskab

Tjekliste:

- Er der udarbejdet risikovurderinger af de relevante it-systemer og afhængigheder til andre systemer?
- Har ledelsen på baggrund af risiko- og konsekvensvurderinger truffet beslutning om, hvilke risici den vil acceptere, og hvilke risici den ikke vil acceptere? Stemmer it-beredskabet overens hermed?
- Er der gjort overvejelser angående tolerancer for it-systemers nedetid (RTO) og maksimale datatab (RPO)?

4. Forebyggelse

Et centralt element i it-beredskabsplanlægningen er at implementere forebyggende tiltag og integrere disse i organisationens eksisterende processer. Formålet med forebyggende tiltag er enten helt at forhindre hændelser, reducere sandsynligheden for hændelser eller at nedbringe konsekvenserne til et acceptabelt niveau, hvor hændelserne kan håndteres af den almindelige driftsorganisation frem for ved iværksættelse af et afhjælpende it-beredskab/kriseberedskab.

4.1 Hvilke hændelser skal forebygges?

På baggrund af risiko- og konsekvensvurderinger udarbejdet i foregående fase, skal det identificeres, hvilke risici der er uacceptable for organisationen. Hvilke risici der vurderes uacceptable, afhænger af organisationens risikovillighed og præferencer. Derefter vurderes det, hvilke af disse risici, som organisationen kan påvirke ved hjælp af forebyggende initiativer. Sådanne forebyggende tiltag kaldes "kontroller/foranstaltninger" i sikkerhedsstandarden ISO 27001.

Ved udvælgelse af uacceptable risici, skal fokus primært rettes mod de relativt sjældne, men mest alvorlige hændelser. Man bør dog også forholde sig til mere almindeligt forekomne hændelser, hvis de samlet set resulterer i uacceptable konsekvenser over en given periode.

Forebyggende tiltag kan have karakter af eksempelvis tekniske og fysiske foranstaltninger eller adfærdsmæssige indsatser, der skal sikre, at mennesker er i stand til at forhindre eller standse uønskede hændelser.

For mere information om adfærdsindsatser, læs vejledningen "Metode til at arbejde med adfærdsindsatser indenfor cyber- og informationssikkerhed" på Sikkerdigital.dk.

Forebyggelsen er en central del af it-beredskabet, fordi forebyggelsen kan reducere omkostningerne til det afhjælpende it-beredskab. Dog er det ikke muligt at forebygge alle risici, hvorfor det afhjælpende it-beredskab er en nødvendighed at have. Men mange tiltag har både forebyggende og afhjælpende effekt, hvorfor det ikke er muligt at lave en skarp adskillelse af de to initiativer. Mere om det afhjælpende it-beredskab i næste kapitel.

Tjekliste:

- Er der, med udgangspunkt i risiko- og konsekvensvurderinger, truffet beslutning om, hvilke forebyggende tiltag (kontroller), der skal implementeres i forretningsprocesserne, så sandsynligheden for iværksættelse af it-beredskabet mindskes?

- Er der implementeret både tekniske og adfærdsmæssige forebyggende tiltag?

5. It-beredskabsplaner

Når en ekstraordinær hændelse rammer, og de forebyggende tiltag, som organisationen har implementeret, ikke er tilstrækkelige til at forhindre eksempelvis et it-nedbrud, er der behov for at iværksætte et afhjælpende it-beredskab. Det kan være hensigtsmæssigt at nedbryde it-beredskabet i operationelle handlingsplaner for forskellige områder. Fx kan man udarbejde nødplaner for de kritiske forretningsprocesser samt interne krisestyrings- og reetableringsplaner for de understøttende it-systemer. Mere om disse i slutningen af dette kapitel.

Offentlige myndigheder er forpligtet til at underrette Center for Cybersikkerhed om større sikkerhedshændelser.

Læs mere om dette via dette link.

Udformningen af planer varierer fra organisation til organisation, men der er en række tommelfingerregler, som man bør følge. En god it-beredskabsplan bør være:

- **Handlingsorienteret:** Planen skal indeholde klare retningslinjer for, hvordan organisationen skal håndtere hændelser. Hvem gør hvad, hvornår og hvordan?
- **Overskuelig:** Planen skal være logisk og hurtig at slå op i, da informationerne skal være nemme og hurtige at tilgå i en beredskabssituation.
- **Ajourført:** Planen skal revideres, når lovgivningen stiller krav om det, når trusselsbilledet ændrer sig væsentligt, når erfaringer fra hændelser eller øvelser tilsiger det og når organisationens struktur ændres.
- **Tilgængelig:** Relevante personer skal kunne tilgå planen.
- **Realistisk:** Der skal være overensstemmelse mellem ressourcer, der forventes anvendt ifølge planen, og de ressourcer, der er til rådighed under en faktisk hændelse.
- **Læst og forstået:** Brugere af planen skal have læst og forstået planen inden anvendelse af planen.
- **Afprøvet:** Planen skal jævnligt afprøves af organisationen.

Brug gerne "Skabelon til it-beredskabsplan" og "Miniberedskabsplan i lommeformat" (Sikkerdigital.dk) som udgangspunkt for udarbejdelse af it-beredskabsplaner.

5.1 It-beredskabsplaner skal leve op til krav for maksimal nedetid (RTO) og maksimalt datatab (RPO)

På baggrund af organisationens risiko- og konsekvensvurderinger, er der truffet beslutning om tolerancer for it-systemers maksimale nedetid (RTO) og maksimale datatab (RPO). Målet med it-beredskabsplanerne er, at organisationen gøres i stand til at håndtere ekstraordinære hændelser uden at overskride disse fastsatte grænser for RTO og RPO. Det er ikke altid muligt at forhindre en overskridelse af grænser for maksimalt datatab og nedetid, men det bør være dét, der tilstræbes.

For at sikre sammenhæng i it-systemernes reetableringstid, skal de systemer i forretningsprocessen, som skal reetableres først, som minimum have et lavere eller samme krav til reetableringstiden i forhold til de øvrige systemer i forretningsprocessen.

Det bør vurderes, hvordan datatab i ét af it-systemerne eventuelt påvirker resten af forretningsprocessen. Derfor bør man sikre sig, at de it-systemer, der løbende udveksler data i forretningsprocesserne, har krav til maksimalt datatab, der stemmer overens med hinanden.

Der skal desuden tages stilling til, i hvilken rækkefølge it-systemer skal reetableres, hvis flere systemer går ned samtidig.

5.2 Roller og ansvar

It-beredskabsplanen skal tydeligt fortælle, hvem der har ansvar for hvad i en it-beredskabssituation. Bemærk at roller som medarbejdere indtager i it-beredskabet kan afvige fra de roller, de indtager i det daglige arbejde. For hver rolle bør udpeges en medarbejder til at udfylde rollen samt mindst én stedfortræder. Man bør overveje, hvem man placerer i it-beredskabet. Det kan eksempelvis være en fordel, hvis én eller flere har erfaring med risikostyring og krisekommunikation.

Som minimum bør følgende rolle indgå i it-beredskabsplaner:

- **It-beredskabsledelsen**: Øverste beslutningsorgan for it-beredskabet. Foretager væsentlige beslutninger vedrørende håndtering af it-beredskabsmæssige situationer.
- **It-beredskabskoordinator/it-beredskabsansvarlig**: Bistår ledelsen i koordinering af it-beredskabsaktiviteter.
- **Kommunikationsansvarlig**: Ansvarlig for kommunikationen med eksterne og interne interessenter.
- **Reetableringsansvarlig**: Ansvarlig for reetablering af den almindelige drift (kan være outsourcet).
- **It-beredskabssekretær**: Ansvarlig for at føre en log over alle beslutninger og aktiviteter.

Rollelister bør indgå tydeligt i it-beredskabsplaner, så man hurtigt kan finde navne og kontaktoplysninger på relevante medarbejdere.

En ekstraordinær hændelse, som eksempelvis et it-nedbrud, kan stå på i lang tid og være en omfattende logistisk opgave. For at undgå at overbelaste medarbejdere kan det være relevant at have planlagt flere bemandingshold til at løfte ovennævnte roller.

5.3 Kommunikation

Kommunikationsindsatsen er en af de vigtigste (og ofte mest udfordrende) opgaver, der skal løses under en it-beredskabssituation. Mangelfuld kommunikation under en krise kan hurtigt blive en kilde til fejl i it-beredskabsindsatsen. Kommunikationsindsatsen bør derfor også indgå i de respektive it-beredskabsplaner. Dvs. at der skal udarbejdes en plan for, hvordan der skal kommunikeres, når it-beredskabet er aktiveret. Denne plan skal sikre en passende kommunikation til relevante interessenter i rette tid og med rette indhold.

Kommunikationsplanen bør både forholde sig til, hvordan man kommunikerer internt mellem it-beredskabsmedlemmerne, men også hvordan man kommunikerer eksternt til eksempelvis andre myndigheder, driftsleverandører (som ikke er involveret i selve it-beredskabet), pressen, borgere mv.

Man kan med fordel benytte "Vejledning til kommunikation i en beredskabssituation" (Sikkerdigital.dk) til at udarbejde kommunikationsplaner.

5.4 It-beredskabsplanlægning hos leverandør

Ofte er driften af centrale dele af organisationens it-systemer udliciteret til eksterne leverandører. Det er vigtigt, at man tydeligt definerer leverandørens ansvar i en it-beredskabssituation. Hvis det eksempelvis er et it-system, som en leverandøren drifter, der bryder ned, er det leverandøren, der har ansvar for reetablering af it-systemet.

Som offentlig myndighed har man ansvar for at stille klare krav til leverandøren og at føre tilsyn med, at leverandørens it-beredskabsplaner lever op til myndigheden krav. Udgangspunktet for at definere kravene til leverandørens beredskab bør – ligesom med det resterende it-beredskabsarbejde – være en risiko- og konsekvensanalyse samt myndighedens overordnede målsætning for it-beredskabet. Krav til it-beredskabet skal være dokumenteret i leverandøraftaler.

Når it-beredskab skal koordineres med leverandører, bør følgende overvejelser indgå:

- Hvilket ansvar har leverandøren, hvis der sker en ekstraordinær hændelse som påvirker myndighedens it-systemer?

- Hvilket it-beredskab skal leverandøren have?
- Hvilke snitflader er der mellem myndighedens og leverandøres it-beredskab, og er det aftalt, hvordan der samarbejdes?
- Hvordan skal kommunikationen foregå mellem leverandør og organisation under en hændelse?

Læs mere om generel leverandørstyring i vejledningen "Informationssikkerhed i leverandørforhold" (Sikkerdigital.dk)

For kunder hos Statens It gælder, at de eksplicitte krav, herunder systemets kritikalitet, skal være dokumenteret via "kundeaftaler" og databehandleraftaler. Kunder hos Statens It har selv ansvar for at teste reetablering af egne fagsystemer. Krav til Statens Its beredskabsplan er beskrevet i Kundeaftalen, bilag 2, Varedeklaration for Informationssikkerhed. Finansministeriets Koncernrevision og Tilsyn og fører tilsyn på vegne af alle kunder, ift. at kravene overholdes.

5.5 It-beredskabsplaners faser

It-beredskabsplaner bør bygges op om fem faser.

Figur 3
De fem faser for it-beredskabsplaner

Kilde: Cyberforsvar der virker (cfcs.dk)

Aktivering
Organisationen skal fastlægge, hvilke kriterier der medfører, at it-beredskabet aktiveres, og hvem i organisationen der har mandat til at aktivere dette.

Mobilisering
Når it-beredskabet er aktiveret, skal it-beredskabsledelsen mobiliseres. Det bør beskrives i detaljer, hvordan it-beredskabsledelsen kontaktes og af hvem, hvor og hvornår de skal mødes.

Organisering
It-beredskabsledelsens medlemmer skal kunne bruge ekstraordinære ressourcer og træffe beslut-

ninger, som påvirker organisationen væsentligt. Derfor skal repræsentanterne i it-beredskabsledelsen have beslutningsmandat, herunder mulighed for at disponere over økonomiske og personalemæssige ressourcer.

Håndtering
Når it-beredskabsledelsen er samlet, skal der aftales en fast kadence og dagsorden for it-beredskabsledelsens møder. Formålet med møder er at danne et situationsoverblik, og at der træffes passende beslutninger for at håndtere hændelsen hurtigst muligt. I næste afsnit findes beskrivelser af forskellige typer it-beredskabsplaner (nødplaner, indsatsplaner og reetableringsplaner), som kan benyttes i denne fase.

Afslutning
Når reetableringen af it-systemerne er opnået, skal it-beredskabet afsluttes og normal drift genindføres. Det bør i den forbindelse bekræftes, at reetableringen af it-systemer er gennemført (eller at der er en tidsplan for, hvornår den er gennemført). At relevant dokumentation fra beredskabsforløbet er dokumenteret og at krisekommunikationen til interne og eksterne interessenter er afsluttet. Endeligt bør aftales et opfølgningsmøde, hvor læringspunkter fra it-beredskabsforløbet drøftes.

5.6 Forskellige typer it-beredskabsplaner (handlingsplaner)

Når der opstår en it-beredskabssituation, er der behov for handling på forskellige områder, og dermed også behov for forskellige typer it-beredskabsplaner. Organisationen vælger selv, hvilke typer planer den udarbejder, og hvad disse planer kaldes. Et forslag er at udarbejde hhv. nødplaner for kritiske forretningsprocesser samt reetableringsplaner og indsatsplaner for understøttende it-systemer.

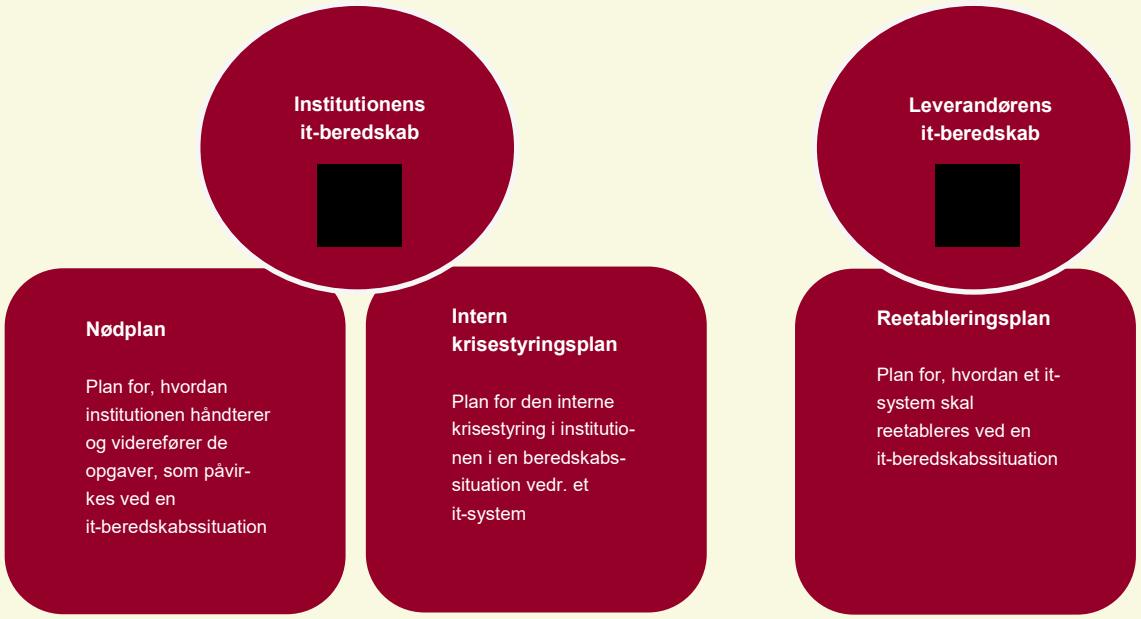
- **Nødplaner** er planer for, hvordan organisationen håndterer og viderefører de opgaver og forretningsprocesser, som påvirkes ved en it-beredskabssituation. De beskriver, hvilke nødprocedurer organisationen eventuelt kan tage i brug i tilfælde af et nedbrud på de it-systemer, som normalt varetager opgaverne. Det kan fx være, at organisationen må bruge manuelle procedurer eller alternative it-systemer for at løbe opgaverne. Nødplaner kan med fordel udarbejdes for de enkelte forretningsprocesser.
- Benyt evt. skabelon til nødplan, som ligger tilgængelig på sikkerdigital.dk.

- **Interne krisestyringsplaner** er planer for den interne krisestyring i organisationen under en it-beredskabssituation. Dvs. at planen fastlægger en governance for, hvordan den midlertidige organisation skal se ud under en beredskabssituation:
    - Hvem er i krisestaben?
    - Hvem skal informeres om fx et it-nedbrud?
    - Hvilke dokumenter skal være tilgængelige for it-beredskabsgruppen?

  Bemærk at interne krisestyringsplaner skal hjælpe med at lave en struktur under en it-beredskabssituation i form af en række overskuelige, letforståelige og let anvendelige informationer, så it-beredskabsgruppen kan træffe (hurtige) beslutninger på det bedst mulige grundlag. Vær opmærksom på at denne information løbende opdateres, når der sker ændringer i organisationen.

- **Reetableringsplaner** er tekniske planer for, hvordan it-systemer skal reetableres under en it-beredskabssituation. I ministerier er det ofte eksterne leverandører, der drifter it-systemer, hvorfor det også typisk er eksterne leverandører, der håndterer reetableringen.

Figur 4
Typer af it-beredskabsplaner



Ansvaret for og i de forskellige it-beredskabsplaner skal være tydeligt. Vær især opmærksom på, i hvilke sammenhænge eksterne leverandører har et ansvar.

Følgende tre bokse tjener som eksempler på, hvad man skal være opmærksom på i tilrettelæggelsen af sine it-beredskabsplaner, hvis man vælger at organisere dem som hhv. nødplaner, interne krisestyringsplaner og reetableringsplaner. Vælger man en anden organisering, bør man også tage disse spørgsmål i betragtning.

Disse vejledende spørgsmål kan bruges, når der udarbejdes **nødplaner** for kritiske forretningsprocesser:

- Er planen ajourført årligt?
- Beskriver planen, hvornår den aktiveres?
- Omfatter planen alle centrale it-systemer i forretningsprocessen?
- Fremgår der kontaktoplysninger på nøglepersoner internt i organisationen?
- Beskriver planen rolle- og ansvarsfordeling internt i organisationen?
- Giver nødplanen konkrete svar på, hvordan en forretningsproces skal køre, hvis et eller flere systemer ikke fungere som planlagt?

- Er det besluttet, hvor planen opbevares, så man ved, hvor den er i en it-beredskabssituation?

Benyt evt. skabelon til nødplan, som ligger tilgængelig på sikkerdigital.dk.

Disse vejledende spørgsmål kan bruges, når der udarbejdes **interne krisestyringsplaner** for it-systemer, der understøtter kritiske forretningsprocesser:

- Er planen ajourført årligt?
- Beskriver planen, hvornår den aktiveres?
- Beskriver planen, hvor krisestaben mødes?
- Fremgår der kontaktoplysninger på nøglepersoner internt i organisationen?
- Fremgår der kontaktpersoner på eksterne interessenter?
- Beskriver planen rolle- og ansvarsfordeling internt i organisationen?
- Beskriver planen, hvilke it-systemer der påvirkes af et systemnedbrud eller datatab?
- Indgår der beskrivelser af kommunikation til eksterne og interne aktører?
- Er det besluttet, hvor planen opbevares, så man ved, hvor den er i en it-beredskabssituation?

Disse vejledende spørgsmål kan bruges, når der udarbejdes **reetableringsplaner** for it-systemer, der understøtter kritiske forretningsprocesser:

- Beskriver planen, hvornår den aktiveres?
- Beskriver planen eller kontrakten kriterier for at vende tiltage til normal drift?
- Er det besluttet, hvor planen opbevares, så man ved, hvor den er i en it-beredskabssituation?
- Fremgår der kontaktoplysninger på nøglepersoner hos leverandøren og organisationen?
- Beskriver planen rolle- og ansvarsfordeling mellem leverandør og organisation?
- Fremgår der krav til RTO af planen eller kontrakten?
- Fremgår der krav til RPO af planen eller kontrakten?
- Beskriver planen nødvendige aktiviteter for at reetablere it-systemer?
- Beskriver planen, hvordan it-systemet kan køre i nøddrift?

Tjekliste:

- Er der udarbejdet it-beredskabsplaner, herunder evt. nødplaner for alle kritiske forretningsprocesser og reetableringsplaner for de understøttende it-systemer?
- Er der taget højde for grænser for nedetid (RTO) og maksimalt datatab (RPO)?

- Er rolle- og ansvarsfordeling tydelig? Også i forbindelse med leverandører?
- Er informationer i intern krisestyringsplan let forståelige og let anvendelige?

6. Uddannelse

Organisationen skal sikre, at personer der indgår i it-beredskabet har de nødvendige kompetencer til at løfte opgaven. I den forbindelse bør man danne et overblik over, hvilke kompetencer, der er behov for, hvilke personer der kompetenceudvikles, og hvordan kompetenceudviklingen skal foregå og vedligeholdes. Alle medarbejdere der indgår i it-beredskabet, bør kende organisationens it-beredskabspolitik, it-beredskabsprogram og it-beredskabsplaner. Organisationen kan med fordel igangsætte et egentligt uddannelsesprogram til relevante medarbejdere.

Tjekliste:

- Er det blevet kortlagt, hvilke kompetencer organisationen har behov for, for at kunne håndtere en it-beredskabssituation?
- Er det besluttet, hvilke personer som evt. skal uddannes?
- Er det besluttet, hvordan uddannelsen skal foregå og vedligeholdes?

7. Test/øvelser

Det er afgørende for it-beredskabets effektivitet, at organisationen regelmæssigt tester sit it-beredskab, dvs. øver håndteringen af ekstraordinære hændelser. It-beredskabsplaner er kun brugbare, hvis de medarbejdere, der skal aktivere it-beredskabet rent faktisk ved, hvor de finder it-beredskabsplaner, underliggende nødplaner mv., og at de ved, hvordan de tages i anvendelse.

Formålet med øvelserne er således, at afprøve og udvikle it-beredskabsplaner, medarbejdere, samarbejde og tekniske foranstaltninger.

Øvelser bygges som regel op om en bestemt hændelsestype beskrevet i et øvelsesscenarie. Hvad man som organisation vælger at øve, bør afhænge af organisationens behov for udvikling.

Som tidligere nævnt, er det typisk hensigtsmæssigt at nedbryde it-beredskabet i en række operationelle handlingsplaner, såsom nødplaner for kritiske forretningsprocesser samt interne krisestyringsplaner og reetableringsplaner for understøttende it-systemer. Det er vigtigt, at alle typer planer testes regelmæssigt, og at leverandører inddrages, hvis it-systemer driftes eksternt.

7.1 Forskellige typer it-beredskabsøvelser

Organisationen kan vælge mellem forskellige former for øvelser:

- Procedureøvelser
- Dilemmaøvelser
- Krisestyringsøvelser
- Fuldskalaøvelser

Procedureøvelser har til formål at afprøve, om én eller flere specifikke procedurer i organisationens it-beredskab virker efter hensigten eller om der er behov for udvikling. En procedureøvelse kan eksempelvis være en test af, om alarmeringssystemer i organisationen fungerer. Fx om man kan få kontakt relevante medlemmer af krisestaben og derved om alarmering virker som tiltænkt.

Dilemmaøvelser (også kaldet diskussionsøvelser eller table-top øvelser) samler relevante deltagere og gennemspiller en hændelse. Hver person påtager sig en rolle og et hændelsesforløb udspilles. Det anbefales at mere erfarne organisationer afholder dilemmaøvelser, hvor der lægges pres på deltagerne ved løbende at præsentere problemer (fx tidspres eller ufuldstændig information), som forekommer under virkelige hændelser.

Under **krisestyringsøvelser** kan deltagerne øve deres rolle under en krise i deres normale arbejdssituation. Denne type øvelse tester dermed også de praktiske forhold omkring krisestyringen, om end beslutninger kun træffes på papiret. Denne type øvelse kræver mere forberedelse i form af eksempelvis drejebog, observatører mv.

Fuldskalaøvelser afprøver den operative indsats i forbindelse med en stor hændelse. Øvelsen kan indeholde elementer fra en beredskabsindsats såsom alarmering, indsættelse af mandskab og koordinering mellem flere forskellige myndigheder eller organisationer. Dette er en ressourcetung øvelsesform i kraft af både logiske og mandskabsmæssige behov.

Testprocessen

Der skal skabes klare rammer for testprocessen. Man bør følge fire trin:

1. Undersøg og fastlæg hvilke områder, der skal afprøves og hvor ofte. Man bør både udføre større og mindre øvelser løbende.
2. Der skal fastsættes klare målkriterier for øvelsen, herunder skal der vælges et passende scenarie til dette formål. Målene bør især defineres i forhold til de mangler, der er fundet ved tidligere øvelser eller sikkerhedshændelser.
3. En it-beredskabskoordinator faciliterer øvelser, blandt andet ved brug af en oversigt over aftalte tidstolerancer (jf. grænser for nedetid og datatab). Efter øvelsen afholdes en kort evalueringssession for at identificere læringspunkter fra øvelsens deltagere
4. Der udarbejdes en øvelsesevaluering med henblik på at dokumentere erfaringer og muligheder for forbedringer. Planen godkendes af ledelsen før den sættes i værk.

Tjekliste:

- Udføres it-beredskabsøvelser regelmæssigt? Både internt og hos relevante leverandører?
- Er det tydeligt, hvad formålet med øvelserne er, og hvilke målekriterier der benyttes til vurdering?

8. Evaluering og forbedringstiltag

Når it-beredskabet har været aktiveret, bør indsatsen evalueres. Dette gælder både i forbindelse med faktiske hændelser og efter øvelser. Formålet er at evaluere, hvad der fungerede godt, og hvad der fungerede mindre godt og som dermed bør forbedres.

Evalueringerne skal gerne give svar på følgende:

- Er relevante forebyggende tiltag (kontroller) iværksat mhp. at undgå at den konkrete hændelser indtræffer igen, eller findes der bedre alternativer?
- Har medarbejderne de fornødne kompetencer via uddannelse, øvelser og hændelseshåndtering?
- Er der behov for justeringer af it-beredskabsplaner?
- Fungerer it-beredskabets tekniske hjælpemidler, så de understøtter en god kommunikation og beslutningskraft?
- Fungerer de nuværende arbejdsgange tilfredsstillende under en hændelse, eller bør de justeres?
- Fungerer samarbejdet med eksterne leverandører under en it-beredskabssituation?

Der kan med fordel udarbejdes et generelt evalueringskoncept med retningslinjer for, hvordan evalueringer kan gennemføres. Der bør tages stilling til:

- Hvem skal udføre evalueringerne
- Hvilke kriterier der skal evalueres ud fra
- Evalueringsprocessen

Der bør uddrages læringspotentiale og udarbejdes en handlingsplan for forbedringsinitiativer. Handlingsplanen skal godkendes af ledelsen.

Tjekliste til den offentlige myndighed:

- Er der udarbejdet evalueringer på baggrund af aktivering eller test af it-beredskabet?
- Er der udarbejdet en handlingsplan for forbedringstiltag, som er godkendt af ledelsen?

9. Skabelonoversigt

Tabellen herunder indeholder oversigt over skabeloner og andet materiale relateret til it-beredskabet.

Type	Dokument	Anvendelse
Skabelon	It-beredskabspolitik	Sikring af ledelsesforankring og grundlag for beredskabsarbejdet
Skabelon	It-beredskabsplan	Plan til organisationer for struktureret igangsætning og gennemførelse af aktiviteter til reetablering af it efter en hændelse
Guide	Kommunikation i en beredskabssituation	Guide om roller, ansvar og andre overvejelser i forbindelse med kommunikation i en beredskabssituation
Guide	Miniberedskabsplan i lommeformat	Guide med de vigtigste elementer at have styr på under en beredskabssituation.

Vejledning i it-beredskab
Udgivet januar 2022 (opdateret september 2022)
Udgivet af Digitaliseringsstyrelsen

Publikationen er kun udgivet elektronisk

Henvendelse om publikationen kan i øvrigt ske til:

Digitaliseringsstyrelsen
Landgreven 4
1017 København K
Tlf. 33 92 52 00

Publikationen kan hentes på
www.sikkerdigital.dk.

Foto Colourbox

ISBN: 978-87-93073-46-3