Fælleskommunal IT beredskabsstrategi

Februar 2020

1. Versionsstyring

Versionsstyringen af dette dokument skal sikre, at alle rettelser, tilføjelser/fjernelser eller ændrede principper dokumenteres behørigt.

Det er i gruppen af deltagende kommuner vedtaget, at nedenstående person er ansvarlig for IT beredskabsstrategiens tekst og indhold, og har herefter udelukkende redigeringsretten:

Navn på ansvarlige: **Rikke Graff, Faaborg-Midtfyn Kommune**

Version	Udarbejdet af	Dato	Godkendt af
0.1	Claus Stoltenberg	29-11-2019	
0.2	Claus Stoltenberg	04-12-2019	
0.2.1	Steen Brodersen	23-12-2019	
0.2.2	Henrik Dyrhøj	08-01-2020	
0.2.3	Claus Stoltenberg	13-01-2020	
0.2.3.4	Rikke Graff	29-01-2020	
0.2.3.5	Rikke Graff & Claus Stoltenberg	19-02-2020	
1.0	Claus Stoltenberg	21-02-2020	

Indholdsfortegnelse

1. Versionsstyring 2
2. Indledning 4
3. Formålet med samarbejdet om IT beredskabsstrategien 5
4. Målsætninger for IT beredskabet 5
5. Udgangspunkt for IT beredskabet 6
6. Omfang og anvendelsesområde 7
7. Afgrænsning og præmisser for IT beredskabet 8
8. Funktioner, roller og opgaver 8
9. Reetableringsstrategier 10
10. Hændelsesforløb 10
11. Eksterne leverandører 11
12. Beredskabsscenarier 11
13. Kommunikation af IT beredskabet 12
14. Test af IT beredskabet 13

2. Indledning

Kommunerne leverer og gør hver eneste dag brug af digitale serviceydelser og -løsninger i forhold til borgere i alle aldre, ansatte i kommunerne og kommunernes samarbejdspartnere og leverandører. Som del af en stærkt digitaliseret offentlig sektor, er kommunerne i stigende grad afhængige af en stabil IT drift og en sikkerhedsmæssig robust IT infrastruktur. Når digitaliseringen øges, stiger risikoen samtidig for, at der opstår hændelser, der kan forhindre kommunerne i at levere og gøre brug af vigtige IT services – dette i en hverdag præget af en omverden med et vedvarende højt trusselsniveau, som f.eks. cyberkriminalitet, terror, ekstremt vejr, udstyrssvigt mv.

Derfor er det vigtigt at have et effektivt beredskab, der hurtigt kan sikre reetablering af kritiske IT servises, når uheldet rammer. Konsekvenserne ved ikke at have et beredskab kan være, at opgaverne ikke kan løses med deraf følgende både livstruende, økonomiske, juridiske og imagemæssige konsekvenser.

På baggrund af dette, er der er opstået et ønske blandt de fynske kommuner om at etablere et fælleskommunalt samarbejde om en fælles IT beredskabsstrategi, der skal støtte op om arbejdet med IT beredskabet. Samarbejdet skal styrke indsatser målrettet IT beredskabet i kommunerne, medvirke til øget bevidsthed om beredskabsarbejdet og understøtte bredere forankring på tværs af fagområder i kommunerne.

Følgende kommuner er en del af det fælleskommunale IT beredskab på Fyn:

- Assens Kommune
- Faaborg-Midtfyn Kommune
- Kerteminde Kommune
- Langeland Kommune
- Nordfyns Kommune
- Nyborg Kommune
- Ærø Kommune

Med afsæt i ovenstående udarbejdes denne IT beredskabsstrategi, som skal danne ramme om samarbejdet med IT beredskabet.

Der etableres et tværkommunalt IT beredskabsforum, som får til opgave at sikre godkendelsen af IT beredskabsstrategien, samt udarbejdelse, vedligeholdelse og test af de underliggende IT beredskabsplaner.

IT beredskabet er ledelsens ansvar og IT beredskabsstrategien godkendes efter kommunernes individuelle principper.

3. Formålet med samarbejdet om IT beredskabsstrategien

Formålet med IT beredskabsstrategien er at fastlægge fælles og ensartede overordnede rammer for de deltagende kommuners arbejde med IT beredskabet. Strategien indeholder en beskrivelse af de ønskede målsætninger for IT beredskabet og er et udtryk for kommunernes forventninger og krav.

Samarbejdet omfatter udarbejdelse og vedligeholdelse af IT beredskabsstrategien, og den efterfølgende udarbejdelse, vedligeholdelse og test af kommunernes individuelle IT beredskabsplaner ud fra ensartede principper, skabeloner og metoder.

IT beredskabsstrategien skal støtte op om de overordnede beredskabsplaner, som er udarbejdet og udgivet af Beredskab Fyn. På den måde følger kommunerne samme principper som er defineret i de overordnede planer, og der er dermed en logisk sammenhæng mellem overordnede beredskabsplaner og underordnede nødplaner for kommunernes respektive fagområder, herunder IT beredskabet.

IT beredskabsstrategien og de underliggende nødplaner for de respektive fagområder, skal sikre, at der er etableret alternative forretningsgange ved nedbrud eller svigt af IT-services.

Den operationelle udmøntning af IT beredskabsstrategien beskrives særskilt i IT beredskabsplaner, som vil være individuel for hver kommune, men som følger samme overordnede principper.

Opdelingen af IT beredskabet i en strategi og separate og individuelle kommunale planer skyldes hensynet til det løbende vedligeholdelsesarbejde af IT beredskabsplanerne i hver kommune. Strategien er som udgangspunkt er mere langsigtet og dermed mindre vedligeholdelseskrævende end de operationelle planer

IT beredskabsstrategien, samt kommunernes individuelle IT beredskabsplaner, anvender Digitaliseringsstyrelsens og KL's vejledninger og skabeloner om "best practice" for IT beredskab.

4. Målsætninger for IT beredskabet

Den overordnede målsætning for kommunernes informationssikkerhed er at beskytte informationers fortrolighed, integritet og tilgængelighed. Med dette menes, at kun rette personer har adgang til informationer, at informationerne er korrekte, komplette og sikret mod uautoriserede ændringer, og at informationerne er tilgængelige og brugbare, når der er behov for det.

Med udgangspunkt i de forretningsmæssige behov, er en række elementer afgørende for, at IT beredskabet lever op til de prioriterede målsætninger. Elementerne er desuden grundlag for valg af reetableringsstrategier.

Følgende målsætninger skal således kunne opfyldes i IT beredskabet:

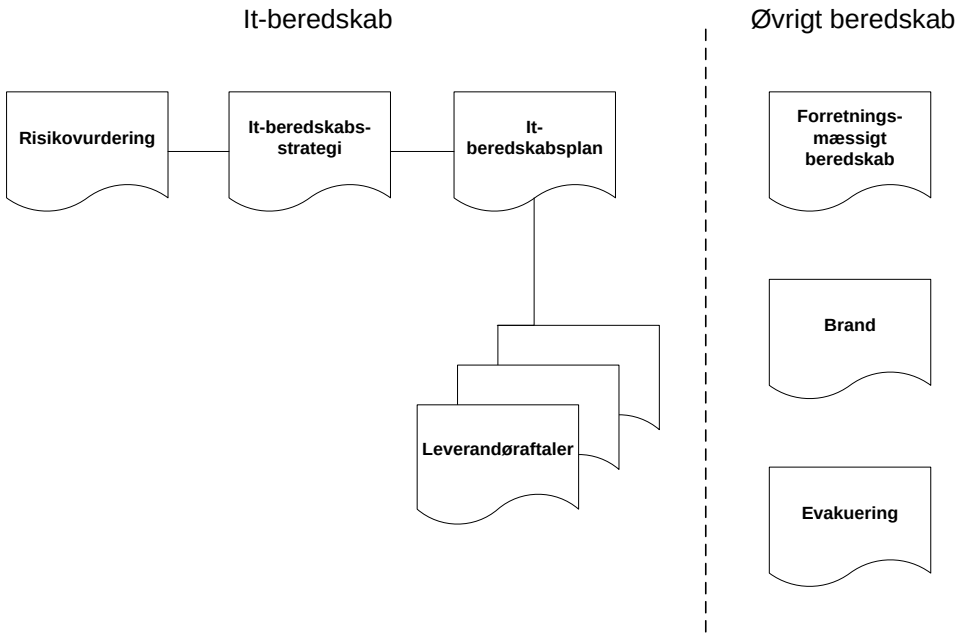
- Beredskabet skal begrænse skadevirkningerne ved ikke planlagt utilgængelighed på IT understøttede forretningsprocesser
- Beredskabet skal understøtte smidig reetablering af data og systemer efter et nedbrud
- Beredskabet skal understøtte, at medarbejdere uddannes i håndtering af sikkerhedshændelser, der vedrører tab af fortrolighed, integritet og tilgængelighed samt brud på den registreredes rettigheder
- Beredskabet skal understøtte kommunikationen i en beredskabssituation inkl. valg af informationskanal
- Beredskabet skal understøtte, at der kan etableres et smidigt samarbejde med leverandører i tilfælde af et nedbrud, der berører kommunernes IT anvendelse

- Beredskabet skal understøtte, at efterfølgende vurdering og evt. kontrol af forløbet kan redegøres gennem fyldestgørende udfyldelse af hændelsesjournal/-log

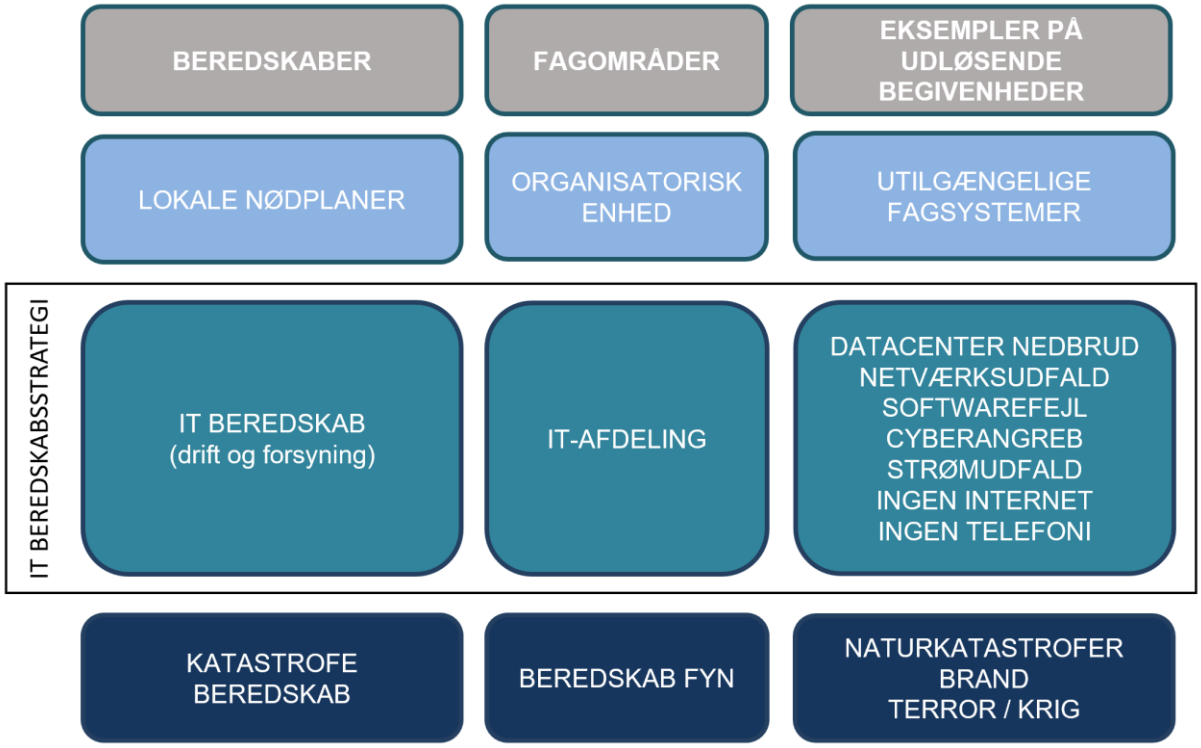
5. Udgangspunkt for IT beredskabet

IT beredskabet fastsættes med udgangspunkt i en risikovurdering, der er baseret på forretningsmæssige og organisatoriske behov, samt nationale strategier og lovkrav, der regulerer sikkerhed på kritisk infrastruktur og behandlingssikkerhed af persondata.

IT beredskabet skal være koordineret med den samlede beredskabsplan for hver enkelt kommune, herunder benævnt "øvrigt beredskab" illustreret i figuren nedenfor.



IT beredskabet er ét blandt flere beredskaber til håndtering af katastrofesituationer i organisationen. IT beredskabet skal først og fremmest sikre genoprettelse af den IT drift, som kommunens IT afdeling har et driftsansvar for. Ved nedbrud, der betyder, at et eller flere fagsystemer eller IT services er utilgængelige, er det fagområdernes ansvar at etablere lokale nødplaner til håndtering af manglende adgang til IT services. Dette gælder både, hvis løsningen drives af IT afdelingen eller af en leverandør. Nedenfor ses en illustration af sammenhængen mellem IT beredskabet og øvrige aktører i beredskabet.



6. Omfang og anvendelsesområde

IT beredskabet skal skabe sikkerhed for, at kommunen kan genskabe en normal driftssituation hurtigt, sikkert og i prioriteret rækkefølge. IT beredskabet skal desuden også sikre, at et eventuelt brud på informationssikkerheden bliver håndteret, når sikkerhedshændelsen involverer komponenter, som kommunernes IT organisationer har ansvaret for at drive og vedligeholde.

Nedenstående er eksempler på hændelser, der kan aktivere IT beredskabet:

- Vandskader som følge af skybrud/oversvømmelser/brud på føringsrør mv.
- Brand- og eksplosionsulykker
- Nedbrænding af serverrum eller andre væsentlige lokationer
- Afbrydelse af forsyningslinjer (strøm og internetlinjer)
- Tyveri af vitalt IT udstyr
- Hardwarefejl
- Softwarefejl
- Sikkerhedsbrud, som f.eks. virus og hackerangreb
- Kompromittering af sourcede- og cloud løsninger
- Brud på persondatasikkerhed, når hændelsen skyldes eller involverer IT komponenter.
- Terrorhandlinger der direkte eller indirekte skader IT anvendelsen

7. Afgrænsning og præmisser for IT beredskabet

Nedenfor fremgår de afgrænsninger, kommunerne har lagt til grund for omfang og indhold af beredskabet og de udarbejdede underliggende beredskabsplaner:

- At IT beredskabet gælder for reetablering af IT infrastruktur og IT services, som stilles til rådighed for kommunernes IT brugere, herunder borgervendte IT løsninger
- At IT beredskabet gælder for den del af driften, f.eks. IT udstyr, kommunikationsudstyr, systemer, applikationer mv., som kommunerne selv driver. Beredskabet omfatter således ikke reetablering af udstyr, systemer og services, som leveres af leverandører. Der stilles dog krav til leverandørers etablering og vedligeholdelse af beredskabsplaner, ligesom leverandører indgår i kommunernes IT beredskabsplaner for så vidt angår kontaktinformationslister, notifikations- og eskalationsprocedurer, prioriterede systemlister, reetableringsteams mv.
- At IT beredskabet gælder for de driftsleverandører, der er specificeret i kommunernes egne IT beredskabsplaner

Beredskabet forventes at fungere effektivt under forudsætning af følgende antagelser:

- Det antages, at en katastrofe ikke samtidigt ødelægger fysiske lokationer hos både organisationen og driftsleverandører
- Det antages, at en katastrofe ikke er sammenfaldende med flere af beredskabets nøgleaktørers fratræden fra deres stillinger

8. Funktioner, roller og opgaver

Kommunernes ledelser har det overordnede ansvar for, at IT beredskabet etableres, vedligeholdes og testes løbende.

IT beredskabsstyringen omfatter en række opgaver af meget forskellig karakter, og der er flere forskellige aktører, som bidrager til såvel planlægning, udarbejdelse, vedligeholdelse og test af beredskabet.

Dette afsnit beskriver funktioner, roller og opgaver i relation til udarbejdelsen og vedligeholdelsen af de enkelte operationelle delelementer i IT beredskabsplanlægningen og de væsentligste planlægningsområder. For at lette vedligeholdelsen af den skrevne operationelle IT beredskabsplan, er opgaver og aktiviteter primært placeret i funktionelle enheder eller hos rolleindehavere frem for hos navngivne personer.

Nedenstående liste præciserer, hvilke funktioner, roller og opgaver der indgår i IT beredskabet.

Funktion	Roller	Opgaver
IT beredskabsleder	I en katastrofesituation udpeges en IT beredskabsleder, som har det overordnede ansvar for, at reetableringen af IT services under katastrofen forløber effektivt, smidigt og styret. Beredskabslederen har ansvaret for at uddele action cards til relevante personer i beredskabet og sikre en rettidig og tilstrækkelig kommunikation til relevante parter under katastrofens forløb, herunder leverandører og myndigheder. Efter katastrofens ophør har IT beredskabslederen endvidere ansvaret for, at alle trin i	• Effektiv styring af katastrofeforløbet • Uddeling af action cards • Kommunikation med relevante parter under katastrofen • Evaluering og forbedring af IT beredskabet

Funktion	Roller	Opgaver
	beredskabsforløbet evalueres og eventuelt korrigeres, hvis der identificeres forbedringspotentialer.	
IT beredskabsteam (Emergency Response Team)	Beredskabsteamet er dem der alarmeres når det er vurderet, at der er tale om en nød-/katastrofesituation eller situationen er i fare for at indtræffe. Teamet træffer beslutning om, i hvilket omfang beredskabet skal iværksættes. De medarbejdere, som skal eskalere en hændelse til et IT beredskabsteamet, skal være forsynet med en oversigt over IT beredskabsteamets kontaktoplysninger. IT beredskabsteamet har til opgave at IT beredskabsplanen for hændelser identificeret i denne plan, såvel som i tilfælde af andre udefineret hændelser eller begivenheder, der vil kunne påvirke kommunens evne til at operere normalt. IT beredskabsteamet træffer desuden beslutning om, hvorvidt et forretningsberedskabsteam skal underrettes	• Reagere omgående på en potentiel katastrofe • Vurdere omfanget af katastrofen, og dens indvirkning på virksomheden • Beslutte hvilke elementer af Business Continuity Planen der skal aktiveres • Underrette Business Recovery Team • Mobilisere og administrere et Disaster Recovery Team, som sørger for at genskabe og/eller opretholde vitale forretningsprocesser, for herefter at vende tilbage til normal drift • Sørge for, at relevante medarbejdere underrettes og fordeler ansvarsområder og ak-tiviteter efter behov
IT genoprettelsesteam (Disaster Response Team)	Teamets leder vil blive kontaktet af IT beredskabsteamet, som har erklæret katastrofesituationen, og sørger for at indkalde og samle resten af genoprettelsesteamet. Det er It genoprettelsesteamets opgave at sikre, at nødvendige forretningsunderstøttede IT systemer og processer genskabes hurtigst muligt.	• Etablere faciliteter til nøddrift indenfor et aftalt tidsrum • Gendanne vigtige forvaltningssystemer og processerprocesser indenfor et aftalt tidsrum • Genskabe ”Business as usual” indenfor et aftalt tidsrum • Koordinere aktiviteterne med teamlederen samt de øvrige medlemmer af IT genoprettelsesteamet
Forretningsgenoprettelsesteam (Business Recovery Team)	Forretningsgenoprettelsesteamet består af ledende repræsentanter fra de vigtigste forvaltningsområder, samt ledende personer hos driftsleverandører. Teamet aktiveres af IT genoprettelsesteamet, og består af en leder samt medlemmer. Lederen af teamet vil være et ledende medlem af kommunens ledelse, og vil have det overordnede ansvar for, at hele beredskabsprocessen forløber struktureret og kontrolleret. Forretningsgenoprettelsesteamet aktiveres, når beredskabet iværksættes på tværs af flere nødplaner. Lederen af teamet skal desuden sikre, at kommunen vender tilbage til normal driftssituation så tidligt som muligt.	• Ledelsesteam, som skal sikre genoprettelsen af forvaltningsprocesser • Er i tæt dialog med IT genoprettelsesteamet i forhold til fremdrift på reetableringen af forvaltningsprocesser • Sikrer, at nødplaner på tværs af forvaltninger koordineres, kommunikeres og styres • Sikrer og koordinerer kommunikationen af beredskabet med Beredskab Fyn

9. Reetableringsstrategier

Formålet med reetableringsstrategien er at planlægge, hvordan enheder og systemer overordnet set reetableres i en IT beredskabssituation under hensyntagen til de forretningsmæssige behov der er i form af krav til reetablering (Recovery Time Objective / RTO) og evt. tolerance for datatab (Recovery Point Objective / RPO).

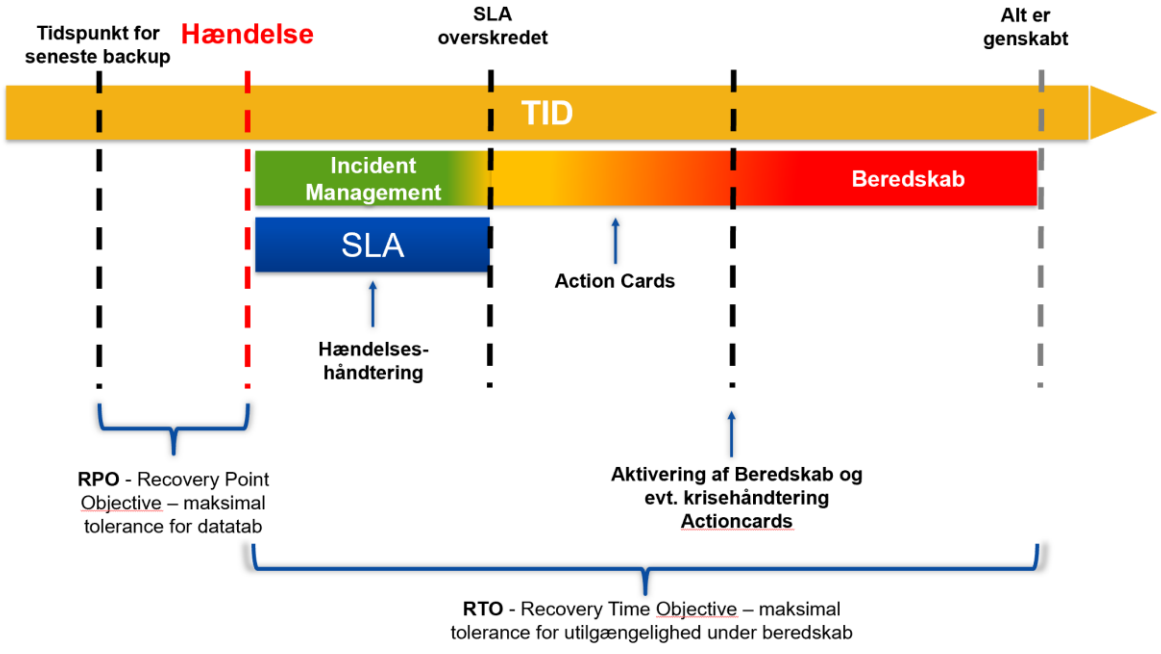
For de IT systemer der i risikovurderingen er identificeret som kritiske, er der defineret uddybende reetableringsstrategier i beredskabsplanerne jævnfør nedenstående tabel.

Reetableringsstrategierne for kommunernes enheder og systemer med lavere prioritering fremgår desuden separat i de operationelle beredskabsplaner.

SLA	RTO	RPO	Reetableringsstrategi
SLA'en (Service Level Agreement) er den aftale der er indgået mellem forretningen og IT eller leverandører af IT servicen, og beskriver den tid der må gå fra en hændelse opstår til systemet skal være tilgængeligt igen. Der er tale om almindelige hændelser og altså ikke katastrofesituationer under beredskabet.	RTO'en beskriver den tid der maksimalt må gå fra en hændelse er opstået og kritiske systemer er utilgængelige, til systemet skal være retableret under beredskabet. Den opståede hændelse skal være af katastrofemæssig karakter.	RPO'en er et udtryk for, hvor mange data i et system man maksimalt kan tåle at tabe. RPO'en kan både anvendes i forbindelse med almindelige hændelser og hændelser af katastrofemæssig karakter.	Strategien kan både være at etablere redundans, retablere fra backup på test/udviklingsmiljøer eller på udstyr der leveres hurtigt fra en leverandør. Backup og frekvensen af backup er en del af strategien, herunder opbevaring af backup, restore-tests, test af failover mv.

10. Hændelsesforløb

Figuren nedenfor viser den tidsmæssige sammenhæng mellem de forskellige elementer i et hændelsesforløb, som starter med en hændelse og ender med, at IT understøttelsen er genskabt. Denne IT beredskabsstrategi vedrører tidsmæssigt udelukkende forløbet fra IT beredskabet aktiveres til alle IT services er genskabt.



11. Eksterne leverandører

Kommunernes krav til sikkerhed og tilgængelighed skal opfyldes, også selvom kommunerne er afhængige af eksterne leverandørers leverancer af IT services. Derfor skal det som en del af IT beredskabet sikres, at leverandørerne kan leve op til passende og tilstrækkelige sikkerhedskrav til beskyttelse af IT services samt det serviceniveau i forhold til fortrolighed, integritet og tilgængelighed, som kommunerne kontraktuelt har forpligtet leverandørerne til.

Det er op til hver enkelt kommune at definere krav til leverandørernes efterlevelse af ovennævnte sikkerhedsniveauer, som har indflydelse på beredskabsleverancernes efterlevelse.

I en IT beredskabssituation kan det være nødvendigt at ændre eller omgå de normale sikringsforanstaltninger, og leverandøren skal derfor være særlig opmærksom på, hvilke krav der er til beskyttelse af fortroligheden.

Kommunernes konkrete krav til maksimal accepteret nedetid (Recovery Time Objective / RTO) og tolerance for datatab (Recovery Point Objective / RPO) fremgår af driftsaftalerne og er beskrevet i IT beredskabsplanerne for hvert system og dermed hver leverandør. Løbende kontrol af, om leverandøren kan efterleve disse krav, udføres jævnfør de konkrete aftaler og består af en eller flere af følgende kontroller:

- SLA-aftaler samt aftaleforhold, der forpligter leverandører til et højt kvalitets- og sikkerhedsniveau (f.eks. efterlevelse af ISO27001)
- Periodevise revisionserklæringer
- Via periodiske test og målinger
- Løbende rapportering af resultater som er defineret i leverandøraftalerne.

12. Beredskabsscenarier

I dette afsnit er der en oversigt over de valgte beredskabsscenarier, som kommunerne anser som mulige konsekvenser ud fra trusselsbilledet, og som de operationelle beredskabsplaner skal kunne håndtere. Scenarierne indikerer hvilke operationelle delplaner, der skal defineres i beredskabsplanerne og aktiveres i en beredskabssituation.

I beredskabsmæssig forstand fokuseres oftest på scenarier, der vedrører tilgængeligheden af IT understøttelsen. Dog omfatter denne strategi også scenarier, der vedrører tab af integritet og/eller fortrolighed af data og informationer, da hændelser i disse kategorier kan sagtens have en alvorlighed, der kræver aktivering af IT beredskabet.

De scenarier der kan aktivere beredskabet, tager sit udgangspunkt i en række primære trusler. Truslerne er udvalgt fra trusselskataloget i ISO27005 (se bilag 1 til inspiration). Aktiver som kan udsættes for nedenstående scenarier er specificeret yderligere i kommunernes individuelle IT beredskabsplaner.

Trusler	Katastrofescenarie
Fejlende hardware Menneskelige fejl	Svigt af en **enkelt komponent** i IT infrastrukturen, som udgør "single point of failure" (SPOF), hvorved der udløses et hændelsesforløb af beredskabsmæssig karakter
Fejlende hardware Hackerangreb	Svigt af **netværksinfrastruktur**, hvorved en hel lokation afskæres fra IT understøttelse
Malware Hackerangreb Sabotage Menneskelige fejl Bevidst handling	Svigt af **centrale servere**, hvorved kritiske systemer bliver utilgængelige, og væsentlige opgaver ikke kan løses
Naturkatastrofer/ekstremt vejr Terrorisme Sabotage Menneskelige fejl	Fysisk ødelæggelse af **serverrum**, hvorved kritiske systemer bliver utilgængelige, og væsentlige opgaver ikke kan løses
Naturfænomener Terrorisme Sabotage Menneskelige fejl	**Forsyningssvigt**, hvorved kritiske systemer bliver utilgængelige, og væsentlige opgaver ikke kan løses
Naturfænomener Terrorisme Sabotage Menneskelige fejl	Ødelæggelse af **fysiske lokation**er, hvorved kritiske systemer bliver utilgængelige, og væsentlige opgaver ikke kan løses
Terrorisme Sabotage Hackerangreb Konfigurationsfejl Menneskelige fejl Bevidst handling	Svigt af eller fejl i **software/programmel** som følge af fejl, ændringer eller opdateringer, foretaget af autoriserede eller uautoriserede, hvorved informationers tilgængelighed, korrekthed eller fortrolighed påvirkes, og væsentlige opgaver ikke længere kan udføres.

13. Kommunikation af IT beredskabet

Kommunikation og implementering af IT beredskabet i kommunerne sker efter "top-down" princippet, hvor ledelsen og IT- eller informationssikkerhedskoordinatoren har ansvaret for at kommunikere både IT beredskabsstrategien og IT beredskabsplanerne videre til de medarbejdere, som indgår i IT beredskabsorganisationen samt de, som forventes at spille en aktiv rolle i en beredskabssituation.

Kommunikationen spiller en vigtig rolle og skal sikre, at både den strategiske, taktiske og operationelle plan og fremtidige opdateringer hertil formidles effektivt og direkte.

Målet med kommunikationen er at:

- gøre medarbejdere opmærksomme på, at der eksisterer en IT beredskabsstrategi og -planer, hvad den/de indeholder, og hvordan den/de vil kunne påvirke medarbejderen i en beredskabssituation
- informere beredskabsorganisationen og IT afdelingen om opdateringer til IT beredskabsplanen, når det er relevant
- skabe en distributionskanal for den opdaterede IT beredskabsplan og sikre og forbedre beredskabssituationen

En god implementering af IT beredskabsplanen viser sig i en beredskabssituation, hvor kommunikationen og håndteringen af beredskabet:

- er præcis og rettidig
- sikrer tilstrækkelig information til medarbejdere, brugere, samarbejdspartnere og pressen
- sikrer konsistens i informationen om hvilke systemer, der er berørte, hvilken konsekvens situationen medfører, forventninger til reetableringstidsrammen m.v.

14. Test af IT beredskabet

Beredskabsplanen bør afprøves mindst en gang om året for at sikre, at den er effektiv, og at beredskabsorganisationen har kendskab til den. Planen skal desuden altid afprøves, hvis der foretages væsentlige ændringer i planen eller i kommunernes IT anvendelse.

Efter hver test skal der ske en evaluering, hvor der tages stilling til, hvorvidt beredskabsplanen skal revideres.

Test af IT beredskabet bør aftales med leverandører. Leverandører bør altid foretage periodiske test af IT beredskabet. Her vil fokus særligt være på den tekniske reetablering, og evnen til at efterleve organisationens behov i form af definerede RTO (maksimal accepteret nedetid) og RPO (tolerance for datatab). Men IT beredskabet bør også afprøves samlet for at sikre, at kommunikationen mellem kommuerne og leverandørerne fungerer effektivt i en krisesituation.

Valget af testtype og omfanget af testen skal planlægges i forhold til det konkrete behov. Følgende eksempel beskriver, hvordan afprøvningen og frekvens for afprøvning kan planlægges.

Frekvens	Testtype	Omfang
x gange årligt	Skrivebordstest	Der foretages en skrivebordstest med udgangspunkt i et foruddefineret scenarie. Skrivebordstesten skal bl.a. afprøve eskaleringsprocessen og sikre, at kontaktoplysninger m.v. er korrekte. Der foretages ikke afbrydelser i IT driften. Denne testform har mere karakter af at være en gennemgang af procedurer og sikring af at alle kender deres opgaver og ansvar. Mangler der noget, eller er der forhold, som har ændret sig så planerne kræver en justering.
Hvert år	Simuleringstest	Planen simuleres, og de forskellige aktiviteter udføres i praksis for at teste reaktionstider og udfald af de forskellige handlinger. F.eks. reetablering eller overgang til alternativ lokation. Testen af planen baseres på forskellige scenarier af typen ”Hvad nu hvis… ”. Scenarierne kan indeholde alt fra brand i maskinstuen, strømsvigt, persondata-læk til nedbrud på en server. Her testes også samspillet og samarbejdet mellem de mange aktører. Dette er en vigtig test, da mange problemer opstår i samspillet og kommunikationen mellem krisestyringens interne og eksterne parter, og fordi de anvendte værktøjer ofte viser sig at være utilstrækkelige.

Frekvens	Testtype	Omfang
Hvert x år	Fuld test	Der foretages en fuld test af en eller flere handlingsplaner, hvor et eller flere systemer retableres med udgangspunkt i leverandørens reetableringsplaner. Ved en fuld test gøres testen så realistisk som muligt. Her afbrydes de systemer, der fejler i henhold til scenariet, og driften forsøges genoptaget på en alternativ lokation. En fuld test er den mest effektive og omfattende test, men den vil også være forbundet med en vis risiko og skal derfor planlægges omhyggeligt.