INFORMATIONSSIKKERHED

DREJEBOG TIL HÅNDTERING AF

BEREDSKAB FOR INFORMATIONS-SIKKERHED

Drejebog til håndtering af beredskab for informationssikkerhed

© KL
2. udgave, 1. oplag 2022

Produktion: Kommuneforlaget A/S
Design: e-Types
Foto: Colourbox

KL
Weidekampsgade 10
2300 København S
Tlf. 3370 3370
kl@kl.dk
www.kl.dk
@kommunerne

Produktionsnr. 830851
ISBN 978-87-93950-71-9-pdf

INDHOLD

BEREDSKABSPLANEN – DIN BEDSTE VEN I EN KRISESITUATION

De færreste organisationer kan bryste sig af aldrig at have haft en krise eller nødsituation.

Hvorvidt en krise afvikles roligt og med små tab eller udvikler sig og medfører dårlig omtale, store økonomiske omkostninger eller fyringer afhænger i høj grad af den enkelte organisations evne til at håndtere nødsituationer.

Kriser kan altid opstå, uanset hvor godt man er forberedt. Netværk kan bryde ned. Der kan ske menneskelige fejl og informationer kan blive kompromitteret.

Det mest hensigtsmæssige er selvfølgelig, at der opstår færrest mulige kriser.

Men når en krise opstår, ved du så, hvordan du skal forholde dig?

- Hvordan sørger I for at få krisen standset, så den ikke breder sig?
- Hvem har ansvar for hvad, mens krisen står på?
- Hvilke typer kriser har I størst risiko for at blive udsat for?

I har et kommunalt redningsberedskab til at slukke en brand i et serverrum, men hvem sørger for at organisationens ansatte kan fortsætte med at arbejde, mens der ryddes op? Ligesom de færreste af jeres medarbejdere er brandmænd, er det også de færreste brandmænd, der kan få jeres it-systemer på benene igen, efter branden er slukket. Til dette skal I i stedet have et separat beredskab for informationssikkerhed.

Når oprydningen starter, har I så helt styr på hvilke af jeres systemer, der er mest kritiske? Tandlægen kan måske undvære sine patientjournaler indtil systemet er genoprettet, mens det potentielt kan koste liv, hvis plejehjem ikke kan tilgå beboernes medicinkort. Forskellige systemer indebærer forskellige risici, og det skal en beredskabsplan tage hensyn til.

Hvis en medarbejder trykker på et link, og hele netværket bliver låst, hvad gør man så, når den it-ansvarlige netop er rejst til Mallorca? På hvilket tidspunkt i processen skal leverandører, borgere eller Datatilsynet involveres?

Med en beredskabsplan forbereder I jer på sådanne situationer, så I ikke skal forholde jer til både simple og komplekse spørgsmål om procedurer og bemanding under krisen, hvor tiden er knap. Her kan I i stedet fokusere på at løse krisen effektivt og systematisk, fordi I er forberedt og har testet og opdateret jeres beredskabsplan løbende. At investere noget tid i forberedelse inden krisen, vil når krisen opstår potentielt kunne spare jer for store tab af både omdømme og økonomi.

Måske har jeres organisation allerede et beredskab, men er det opdateret? Lige så hurtigt som den brugbare teknologi udvikler sig og understøtter jeres arbejde, lige så hurtigt udvikler den skadelige teknologi sig, som bruges til at stjæle eller manipulere med jeres data. Truslerne er både flere og anderledes, end de var for bare et par år siden, så måske er det tid til at gennemgå beredskabsplanen igen.

Hvis et eller flere af ovenstående overvejelser lyder bekendte, så læs *Drejebog for beredskab for informationssikkerhed* og få hjælp til, hvordan I implementerer en beredskabsplan.

INDLEDNING

Truslen fra cyberkriminalitet er ifølge Center for Cybersikkerhed meget høj, og den teknologiske udvikling gør, at truslen er i konstant forandring. Samtidig følger der med databeskyttelsesforordningens ikrafttræden krav om, at kommunerne ved sikkerhedsbrud/kompromittering af borgernes data skal anmelde sikkerhedsbrud til Datatilsynet inden for 72 timer. Det stiller store krav til kommunernes sikkerhedsforanstaltninger og beredskab.

Beredskabet skal sikre kommunens kritiske forretningsprocesser og informationsaktiver, hvis der indtræffer alvorlige hændelser, som kan påvirke borgerne og kommunens muligheder for at operere. Desuden skal det sikre, at kommunen fortsat kan løse opgaver, der ikke er berørt af hændelserne. Beredskabet skal ligeledes håndtere scenarier, der vedrører tab af fortrolighed, da sådanne hændelser kan have en alvorlighed, der kræver aktivering af den "undtagelsestilstand", som beredskabet er et udtryk for.

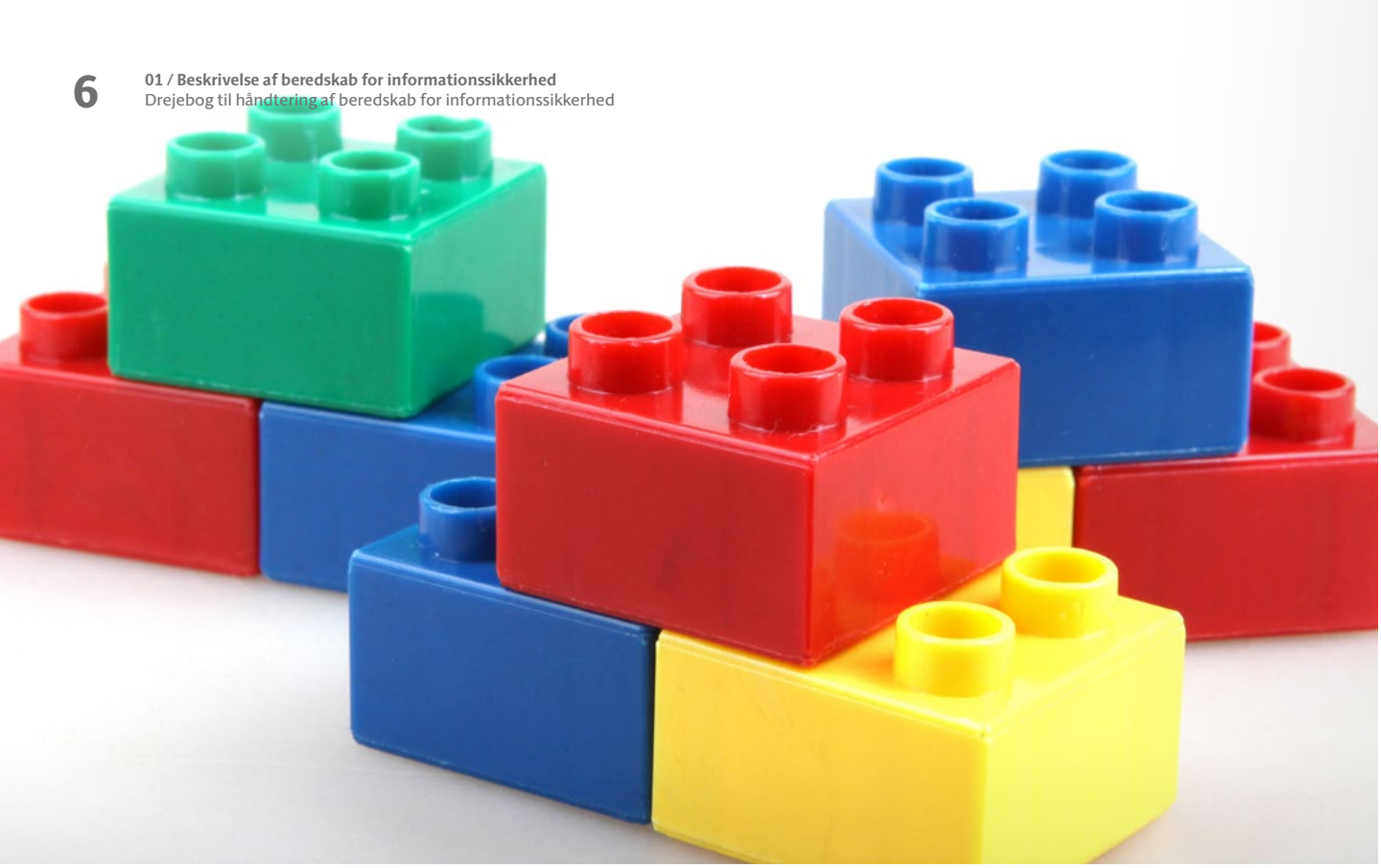
Beredskab er således en særlig sikringsforanstaltning, der skal tages i brug, når de almindelige procedurer ikke kan håndtere et mere alvorligt hændelsesforløb.

Tidligere har man omtalt denne type beredskab som et it-beredskab. Beredskabet skal imidlertid ikke kun håndtere hændelser på it-området, hvis der eksempelvis sker angreb eller nedbrud på it-udstyr, men også kunne håndtere sikkerhedsbrud/kompromittering af borgernes data. Derfor har KL valgt at ændre navnet fra It-beredskab til Beredskab for informationssikkerhed.

Formålet med denne drejebog er at beskrive, hvordan en kommune kan implementere, styre og vedligeholde et passende beredskab for informationssikkerhed samt håndtere eventuelle opståede hændelser.

I drejebogen henvises der til en række skabeloner, der kan være en støtte i arbejdet med at få etableret et beredskab for informationssikkerhed. Disse kan frit benyttes i kommunen og kan hentes på KL's Videnscenter.

Målgruppe
Drejebogen er henvendt til kommunens informationssikkerhedskoordinator og øvrige kommunale ansatte, der arbejder med etablering og vedligeholdelse af et beredskab for informationssikkerhed.



01 / BESKRIVELSE AF BEREDSKAB FOR INFORMATIONS-SIKKERHED

De dokumenter, der kan indgå i beskrivelsen af beredskab, dækker typisk over forskellige niveauer af dokumentation.

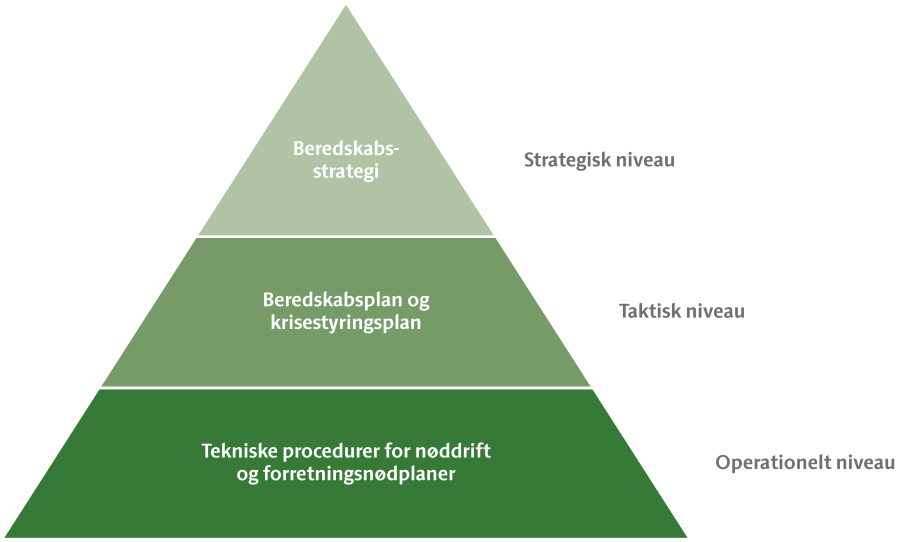
Øverste niveau fastlægger de overordnede rammer for arbejdet med og implementering af beredskabet. Hvad er det ønskede niveau for beredskabet? Hvilke forventninger og krav er der til beredskabet? De overordnede rammer kan med fordel beskrives i en beredskabsstrategi, der godkendes af topledelsen.

Der findes en skabelon for "Beredskabsstrategi for informationssikkerhed", som kan anvendes til at understøtte udarbejdelse af strategien. Skabelonen findes på KL's Videnscenter.

Når de overordnede rammer er på plads, kan den operationelle udmøntning af strategien beskrives særskilt i en beredskabsplan for informationssikkerhed. Beredskabsplanen beskriver bl.a. målsætning for retablering, beredskabsorganisation, eskaleringsprocedure, krisestyring, nøddrift og normalisering. Beredskabsplanen skal godkendes af Informationssikkerhedsudvalget og være tilgængelig for relevante personer i organisationen.

Der findes en skabelon for "Beredskabsplan for informationssikkerhed", som kan anvendes til udarbejdelse af beredskabsplanen. Skabelonen findes på KL's Videnscenter.

› **Figuren viser hierarkiet mellem de forskellige dokumenter i beredskabet for informationssikkerhed**



Sammenhæng med øvrigt beredskab
Beredskab for informationssikkerhed hænger sammen med de beredskabsaktiviteter, der ikke direkte vedrører håndteringen af hændelser på kommunens informationsaktiver. Det er fx håndtering af tilskadekomne medarbejdere, situationer med ødelagte bygninger, evakuering osv., hvor det kommunale redningsberedskab (også kaldet brandvæsen) skal kunne yde en forsvarlig indsats. I nogle kommuner er der et tæt samarbejde om beredskabsplaner mellem det kommunale redningsberedskab og beredskabet for informationssikkerhed.

Planerne skal koordineres, da det i de fleste organisationer er de samme fælles centrale ressourcer, der trækkes på:

- Nogle medarbejdere kan have roller i flere dele af beredskabet, ikke mindst visse ledende medarbejdere, der ofte vil have et bredt funderet ansvar i en beredskabssituation. Ansvarlige kan desuden være fraværende ved en beredskabssituation, og substitut/stedfortræder skal i det tilfælde være udpeget og til rådighed.
- Fysisk ødelæggelse af bygninger mv. kan berøre bygningsdele, der er særligt kritiske i relation til informationsaktiver – fx et serverrum. Beredskabsplanen skal her gennem koordinering med beredskabet for bygningerne sikre, at de nødvendige fysiske rammer til at drive teknikken videre kan etableres. Det øvrige beredskab skal retablere de fysiske rammer, inventar m.m., så medarbejderne kan genoptage arbejdet.
- Endelig kan der være rent logistiske aspekter, der skal være koordinerede. Det kan være spørgsmål om, hvor beredskabsledelsen skal samles, og hvilket kommunikationsudstyr der skal være til rådighed, forplejning mv.

Det er desuden vigtigt, at der sikres koordinering og kommunikation mellem beredskabsplanen for informationssikkerhed og forretningsnødplanerne.

En forretningsnødplan skal beskrive, hvordan kritiske forretningsprocesser eller opgaver skal håndteres i en situation, hvor den almindelige it-understøttelse ikke er til rådighed, fx at ESDH-systemet er ramt af en alvorlig hændelse og derfor ikke er til rådighed for medarbejderne. I en sådan situation vil løsningen ofte være manuelle arbejdsgange eller midlertidig ibrugtagning af andre it-værktøjer.

Forretningsnødplaner vil ofte være udarbejdet i forbindelse med, at der er sket en risikovurdering af kritiske forretningsprocesser. Her vil forretningsnødplanen typisk være en del af de beskrevne foranstaltninger til håndteringen af risici. Det er vigtigt, at der som minimum findes forretningsnødplaner for alle kommunens kritiske forretningsprocesser, eksempelvis forretningsprocesser der kan påvirke liv eller død.

Hvis der i forbindelse med risikovurderingen ikke er blevet beskrevet forretningsnødplaner med retningslinjer for understøttende it-systemer i tilfælde af systemnedbrud, kan skabelon for "Nødplan bilag B.x" anvendes til udarbejdelse og dokumentation af disse. Skabelonen findes på KL's Videncenter.

02 / IT-BEREDSKAB OG EKSTERNE LEVERANDØRER

Når driften af kritiske it-systemer eller it-infrastruktur er udliciteret til en ekstern leverandør (herunder også it-systemer varetaget af KOMBIT), vil leverandøren i de fleste tilfælde også skulle varetage de praktiske opgaver med at retablere i en beredskabssituation.

Leverandøren har således en central rolle i beredskabet, og det er derfor vigtigt, at man i organisationen tager stilling til følgende spørgsmål:

- Hvilket beredskab skal leverandøren have?
- Hvordan skal de planlægningsmæssige opgaver fordeles?
- Hvordan skal der kommunikeres i en beredskabssituation?

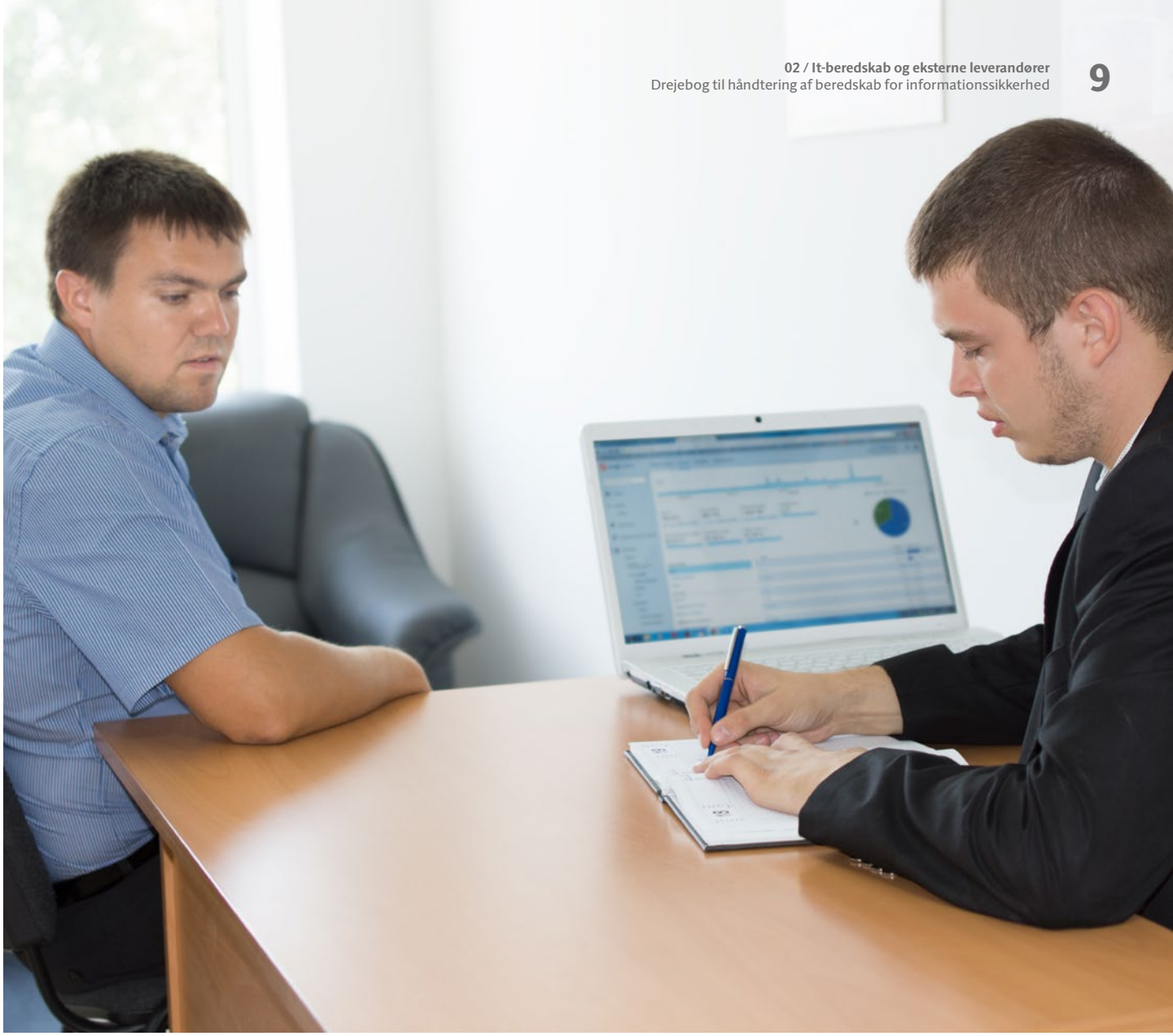
Resultatet af disse overvejelser er typisk indeholdt i kontrakten og bør resultere i en operationel plan for styring af leverandører, der er en integreret del af beredskabsplanen. Den skal bruges, hver gang en hændelse, som kræver aktivering af beredskabet, rammer aktiver, der helt eller delvist er underlagt eksterne leverandørers driftsansvar.

Stil krav til leverandørens beredskab
Beredskabet for leverandørens systemer eller infrastruktur skal aftales med leverandøren. Dette sket typisk i forbindelse med kontraktindgåelse via aftaler om SLA og support. Hvis ikke forventningerne er afstemt, er der risiko for, at leverandørens beredskab ikke er tilstrækkeligt i forhold til kommunens behov, eller at kommunen på den anden side har for høje omkostninger til en unødvendig ydelse. Udgangspunktet for at definere kravene til leverandørens beredskab bør være en risiko- og konsekvensanalyse, samt kommunens overordnede strategi for beredskabet.

Når kommunens krav til beredskabet for informationssikkerhed er fastlagt, kan den konkrete implementering aftales med leverandøren. Større driftsleverandører tilbyder ofte forskellige niveauer af beredskab.

Når der er aftalt en passende implementering af beredskabet, er det vigtigt løbende at afprøve beredskabets effektivitet. Frekvens, omfang og øvrige praktiske forhold vedrørende afprøvningen skal aftales med leverandøren.

De eksplicitte krav til beredskabet og øvrige sikkerhedsforhold skal være dokumenteret via leverandøraftaler og databehandleraftaler, da det er afgørende for retableringsløsningerne, at fx maksimalt datatab, reetableringstider og evt. datas kategorisering jf. Databeskyttelsesforordningen fremgår.



Aftal snitflader og opgavefordeling
Selvom leverandøren løser de operationelle opgaver, vil begge parter som udgangspunkt have opgaver i forbindelse med planlægningen af beredskabet. Opgaverne bør specificeres, så det kan aftales, hvem der har ansvaret for at udføre dem, fx:

- Hvem har ansvaret for at aktivere beredskabet?
- Hvem har ansvaret for at vedligeholde kontaktoplysninger?
- Hvem har ansvaret for at vedligeholde eventuel dokumentation?

Hvis leverandøren varetager driften af systemer, som er fysisk placeret i kommunens lokaler, kan der være andre praktiske forhold, der bør tages stilling til, fx adgangs- og godkendelsesprocedurer mv. Hvis en kritisk forretningsapplikation er afhængig af mere end 1 leverandør (fx en driftsleverandør og en applikationsleverandør), bør de gensidige snitflader i en beredskabssituation mellem leverandørerne gennemgås og aftales.

Opgavefordelingen bør beskrives og godkendes af begge parter.

Kommunikation med leverandøren i en beredskabssituation
Udover de planlægningsmæssige opgaver bør fordelingen af de operationelle opgaver i en beredskabssituation også aftales. Selve opgaverne ved retableringen vil i de fleste tilfælde blive udført af driftsleverandøren. Men det er også vigtigt at få aftalt kommunikationsvejene mellem parterne.

Kommunikationen bør planlægges, så der både tages højde for situationer, som opdages/eskaleres hos kommunen og hos leverandøren. Udover at aftale hvem, der skal kontakte hvem, bør man også overveje, om der er aktiviteter, som kræver en forudgående accept fra kommunen.

Må leverandøren eksempelvis kontakte andre leverandører, myndigheder eller informere brugere eller borgere?

De konkrete aktiviteter i forhold til styring af leverandøren i en beredskabssituation bør planlægges og beskrives.

For systemer varetaget af KOMBIT, vil det være KOMBIT, der varetager kommunikationen med leverandøren.

03 / STYRING AF BEREDSKAB FOR INFORMATIONS-SIKKERHED

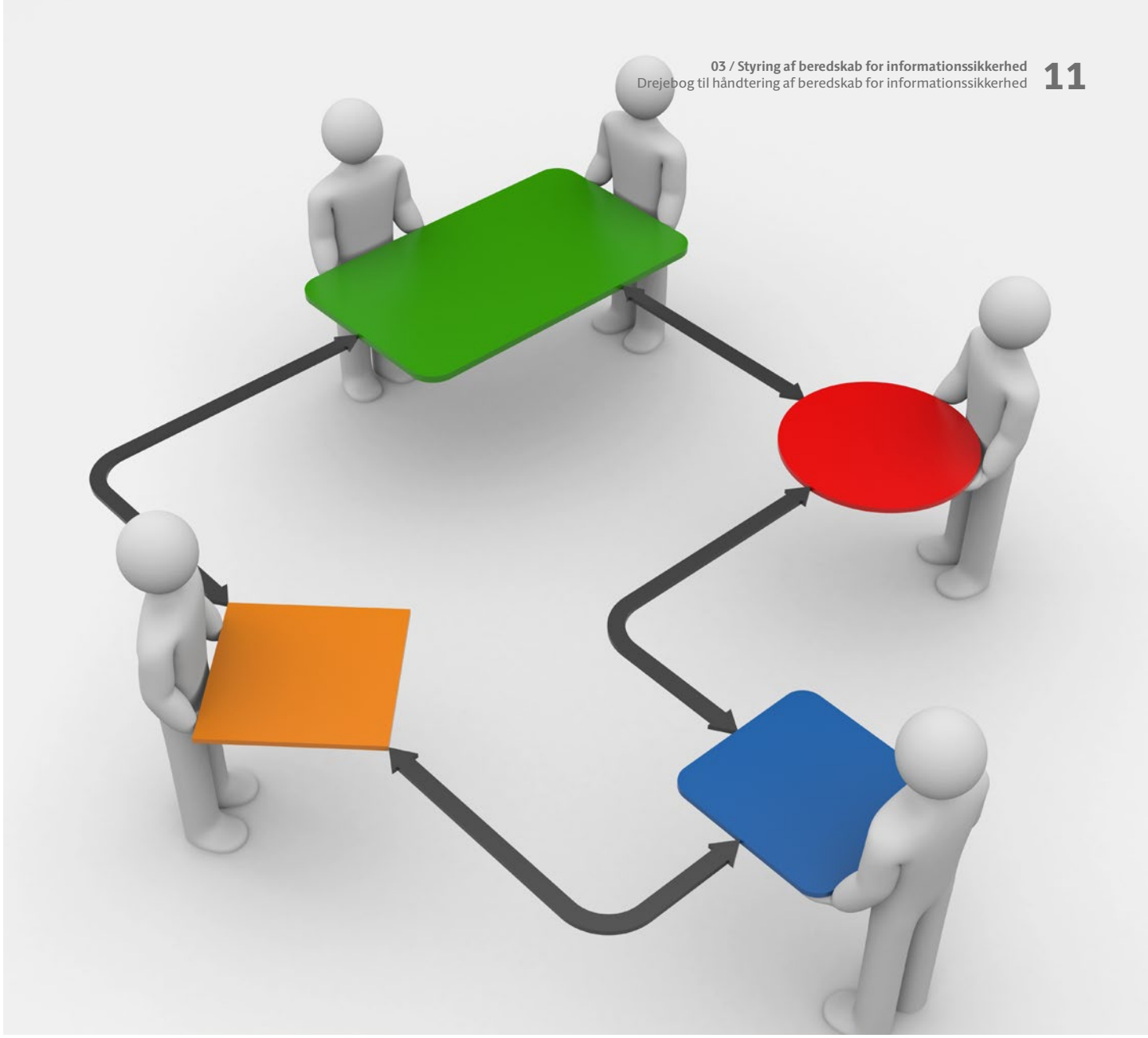
At styre kommunens beredskab for informationssikkerhed er en løbende proces. Kommunens behov vil ændres, når opgaver, forretningsgange eller it-systemer forandres, eller hvis trusselsbilledet forandres drastisk. Det betyder, at beredskabet må tilpasses.

Governance – ledelse af beredskabet
Kommunens øverste ledelse har det overordnede ansvar for beredskabet. Ledelsen skal sikre, at der etableres en hensigtsmæssig governance – eller ledelsesstruktur – af beredskabet.

Beredskabsopgaven er ikke en anden type opgave end andre ledelsesopgaver. Det betyder fx, at der skal fastsættes en målsætning for beredskabet og tildeles ansvar og tilstrækkelige ressourcer til arbejdet. Målsætningen er med til at skabe en fælles forståelse af, hvorfor beredskabet er etableret, og danner udgangspunkt for valg og udformning af de planer og konkrete aktiviteter, som implementeres. Herefter skal ledelsen desuden løbende følge op på arbejdet og tilse, at målsætningen realiseres.

De operationelle opgaver med at planlægge, implementere, teste og vedligeholde beredskabet kan uddelegeres til kommunens udvalg for informationssikkerhed eller et eksisterende beredskabsudvalg. I udvalget bør der indgå en informationssikkerhedskoordinator eller en lignende profil med de nødvendige kompetencer inden for beredskabsstyring. Udvalget vil primært have en styrende og koordinerende funktion, da planlægning af de tekniske løsninger og implementeringen heraf forudsætter særlige kompetencer, fx it-fagfolk og andre specialister.

Beredskabs- eller informationssikkerhedsudvalget bør løbende rapportere til ledelsen om status på beredskabet. Ledelsen skal informeres om evt, planlagte tiltag og forbedringer, væsentlige ændringer, udfordringer i forhold til at nå målsætningen, resultatet af øvelser mv. Rapporteringen kan være separat eller indgå i den øvrige rapportering om informationssikkerheden. Rapporteringen bør, udover at indeholde en overordnet status, også beskrive eventuelle udfordringer, anbefalinger mv. Hvis der foretages væsentlige afgrænsninger i omfanget af beredskabet, skal disse altid forelægges ledelsen.



Planlægning af beredskabet
Beredskabsplanen skal sikre, at organisationens it-understøttelse kan genetableres i tilstrækkelig grad inden for en ønsket tidsperiode og/eller at alvorlige brud på informationssikkerheden håndteres. Organisationens ledelse skal fastlægge denne tidsperiode med udgangspunkt i, hvornår opgavevaretagelsen bliver truet i en grad, hvor konsekvenserne er uacceptable.

Aktivering af beredskabet behøver ikke at være begrænset til ødelæggende katastrofer, men kan overvejes delvist aktiveret, hvis hændelser medfører, at processer eller systemer opleves som værende utilgængelige eller hvis der sker et alvorlige brud på informationssikkerheden, der kræver hurtig håndtering. Herved opnås en ramme for organisering og kommunikation, som er kendt for de involverede (via test og øvelser), og som ad den vej kan sikre hurtigere normalisering.

Beredskabsplanen bør som minimum omfatte alle kritiske informationsaktiver i form af såvel data samt it-systemer. De omfattede aktiver bør opstilles eksplicit i beredskabsplanen. Aktiviteterne identificeres ved, at der gennemføres en forretningsmæssig risikovurdering, hvor deres betydning for forretningsprocesserne og deres maksimale nedetid vurderes. På baggrund heraf vurderes aktivernes kritikalitet, og der fastsættes mål for retableringstiden og eventuelt mål for tolerancen af datatab.

Defineringen af roller og ansvar i forhold til beredskabsstyring er todelt:

- En del vedrører beredskabsstyringen og håndteringen af de væsentligste planlægningsområder, herunder selve beredskabsplanen.
- En anden del vedrører roller og ansvar i en beredskabssituation.

De to vil sjældent være helt sammenfaldende.

Roller og ansvar for beredskabsstyringen vil som regel være fordelt i henhold til den almindelige organisering. Den medarbejder, der koordinerer informationssikkerheden, vil være opgaveansvarlig på selve planen. Faggrupper eller organisatoriske enheder, der har særlig viden om bestemte dele af planen, vil bidrage til den. Ledelsen eller et udvalg, der har fået delegeret kompetencen, godkender strategi og plan og sørger for opfølgning.

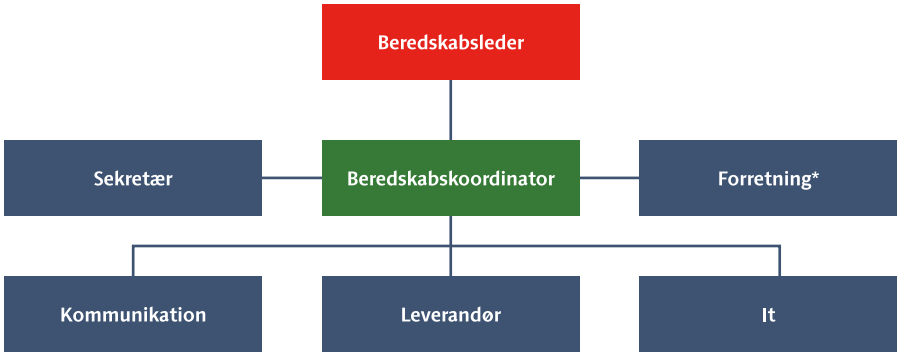
Til gengæld er det ikke ualmindeligt, at beredskabsplanen beskriver et særligt organisatorisk setup til at håndtere beredskabssituationer. Der er typisk behov for at udpege en beredskabskoordinator, der styrer slagets gang, og for at nedsætte en særlig stab til at lede situationen. Derudover er der som regel behov for en øget rapporteringsfrekvens samt for ekstraordinær kommunikation om situationen, både internt og eksternt.

Implementering af beredskabet
Implementering af et beredskab handler dybest set om at sikre, at alle forudsætninger for at kunne håndtere en beredskabssituation i henhold til beredskabsplanen er til stede. Herudover skal det periodisk kontrolleres, at forudsætningerne fortsat er til stede.

Et vigtigt element i implementeringen er sikring af de ressourcer, som er nødvendige for i praksis at udføre de operationelle aktiviteter, der er beskrevet i beredskabsplanen. Det er fx at:

- sikre adgang til reserveudstyr inden for de fastlagte frister (via leverandøraftaler, indkøb, genbrug af testmiljø mv.),
- sikre at back-up kan hentes og restores,
- sikre at der kan trækkes på de nødvendige kompetencer (internt og eksternt), hvis behovet skulle opstå. Ikke mindst beredskabskoordinatorens rolle er central. De kombinerede kompetencer inden for projektledelse, krisestyring og teknisk forståelse er kritiske, og det anbefales, at der kan trækkes på flere personer for at sikre mod personafhængighed,
- sikre adgang til nød-logistik, i det omfang planen forudsætter det (kommunikationsudstyr, mødested og -lokaler), herunder adgang til en fuldt opladet bærbar computer og mobilt bredbånd.
- sikre adgang til beredskabsplanen både elektronisk og i form af fysiske kopier, som opbevares på flere fastlagte steder.

› Figuren viser et eksempel på en beredskabsorganisation for informationssikkerhed



*Forretningsdelen kan dække over mange forskellige aktører afhængig af beredskabssituationen. Ud over de dele af forretningen, der direkte kan være ramt i kraft af nedbrud på it-systemer, kan HR, økonomi og repræsentant for kommunens ejendomscenter være deltagere i beredskabsorganisationen.

Som et led i implementeringen af beredskabsplanen bør det dokumenteres, at alle nødvendige ressourcer er på plads, og at planen derfor i det hele taget er realistisk at udføre i praksis. I denne sammenhæng er det også vigtigt med overvejelser om at returnere til normal drift, med planlægningsaktiviteter og eventuel genanskaffelse af udstyr mv.

Et andet centralt element i implementeringen består i at træne planens aktører. Alle skal kende deres rolle og de aktiviteter, de er sat til at udføre i situationen.

Følgende indsatser bør udføres sideløbende:

- Beredskabskoordinatoren skal mindst en gang årligt kommunikere og forklare planen for ledelsen og alle andre centrale aktører. Ideelt set foregår dette på "en-til-en"-møder med hver rolleindehaver, hvor fokus er på dennes særlige rolle. Ved større organisationsændringer eller ændringer i bemanding bør processen gentages.
- Awarenessprogrammer og -tiltag bør som en fast bestanddel inkludere budskaber omkring håndtering af beredskabssituationer: Information om den overordnede strategi, hensigtsmæssig adfærd, kendskab til beredskabsplaner mv.
- Planen skal testes periodisk og mindst en gang årligt med deltagelse af alle væsentlige rolleindehavere. Der kan veksles mellem forskellige test typer.

Beredskabsplanen kan betragtes som implementeret, når ovenstående punkter er udført, og der samtidig findes en proces til overvågning af, at beredskabsplanen til enhver tid er operationel og velfungerende.

Løbende forbedring og opdatering
Beredskabet skal løbende vedligeholdes. Det kan være nødvendigt at foretage ændringer i beredskabet i følgende tilfælde:

- Erfaringer fra et beredskabsforløb, hvor den efterfølgende evaluering har identificeret mulige forbedringer
- Erfaringer fra en test af beredskabsplanen, hvor den efterfølgende evaluering har identificeret mulige forbedringer
- Ændringer i forudsætningerne for beredskabet (organisationen, retableringsstrategi, arbejdsgange, it-anvendelsen mv.) eller indholdet i beredskabsplanen eller forretningsnødplanen (kontaktoplysninger mv.).

Det er vigtigt at vurdere omfanget af de ændringer, der foretages i planerne. Væsentlige ændringer, som har betydning for, hvordan aktørerne skal agere, bør godkendes og udmeldes på en måde, som sikrer kendskab til de ændrede planer.

04 / TEST AF BEREDSKAB

En beredskabsplan kan ikke alene sikre en effektiv håndtering af kriser og hændelser, men den medvirker også til at skabe arbejdsrammer og give støtteværktøjer til kriseberedskabet. Det er i praksis – dvs., når der skal handles hurtigt og hensigtsmæssigt under pres – at beredskabsplanen og aktørerne skal vise sit værd. Det understreger behovet for at teste beredskabsplanen.

Målet med testen er ikke at opnå det bedst mulige resultat på dagen, men at teste planen i praksis. Hvis planen ikke testes, kan den ikke gøres bedre. Den skal virke hver dag og ikke kun på en god dag.

Test af beredskabet
Formålet med at udføre test af beredskabsplanerne er at:

- vurdere og efterprøve, at de beredskabsplaner, der er udarbejdet for organisationen, er tilstrækkelige,
- træne beredskabsplanens aktører i at udfylde deres rolle i en beredskabssituation,
- forbedre eller justere planen i forhold til ændringer i organisationens forhold, fx ændringer i risikobilledet.

Derudover er det en mulighed for at sikre, at beredskabet er integreret i organisationen og for at identificere eventuelle praktiske svagheder i de udarbejdede planer.

Det er vigtigt, at alle involverede parter i beredskabet kender deres rolle og ansvar i en eventuel beredskabssituation, og test er en proaktiv måde at skabe bevidsthed og indblik i planerne og deres effektivitet. Beredskabstesten kan foregå på flere forskellige niveauer, hvilket er beskrevet i afsnittet om testtyper.

I alle tilfælde anbefales det at udpege en testansvarlig, som ikke er en aktør i henhold til beredskabsplanen. Rollen er til gengæld at være projektleder, som bl.a. præsenterer testscenarierne for deltagerne i testen og senere kan afgøre, hvordan situationen udvikler sig på baggrund af de handlinger, deltagerne foretager sig. Den testansvarlige bør have et godt kendskab til beredskabsplanen og tilstrækkelig faglig indsigt til at kunne målrette testen til de relevante områder. Det vil som oftest være relevant at teste beredskabet 1-2 gange årligt, eller når der foretages væsentlige ændringer i beredskabsplanen for informationssikkerhed og evt. forretningsnødplaner. Vurderingen af behovet for frekvens og kompleksitet foretages af den områdeansvarlige.

I "Håndbog om test af beredskab", der findes på KL's Videnscenter, kan der læses mere om hvordan en test kan styres, planlægges og udføres.

Testtyper
Beredskabstest kan gennemføres på forskellige niveauer. Der er almindeligvis 3 typer af test med stigende kompleksitet: Skrivebordstest, simuleringstest og endelig fuldtest eller fuldskalatest.

Uanset testtype baseres testen på forskellige scenarier af typen "Hvad nu hvis... ". Scenarierne kan indeholde alt fra brand i maskinstuen, strømsvigt, læk af persondata til nedbrud på en server.

Skrivebordstest
Beredskabsorganisationen samles og gennemgår planen på baggrund af nogle forskellige scenarier, hvor man blot forestiller sig hændelserne og udviklingen i forløbet. Denne testform har mere karakter af at være en gennemgang af, hvor godt de eksisterende processer dækker en beredskabssituation, hvorvidt processerne er praktisk anvendelige samt hvor godt alle kender deres opgaver og ansvar. Mangler der noget, eller er der forhold, som har ændret sig siden sidst?

Denne type test kan også benyttes til uddannelse i beredskabsplanen.

Simuleringstest
Planen simuleres, og de forskellige aktiviteter udføres i praksis for at teste reaktionstider og udfald af de forskellige handlinger.

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.

Fuld test
Ved en fuld test gøres testen så realistisk som muligt. Her afbrydes de systemer, der fejler i henhold til scenariet, og driften forsøges genoptaget. 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. Det vil være nødvendigt at sikre sig ledelsens accept af denne test.

Planlægning og udførsel af test
Undersøg og fastlæg, hvilke områder der skal testes. Vælg herefter testtype.

Hvor realistisk skal testen være – skrivebordstest, fuld test eller simuleringstest? Hvad må den koste? Vil det sikre det bedste resultat om testen gennemføres med en ekstern facilitator, som opstiller testscenarier – eller ønsker kommunen selv at forestå testen?

Fastsæt klare mål for testen.
Målene kan defineres i forhold til de mangler, der er fundet ved tidligere test eller ved tidligere sikkerhedshændelser. Men målene kan også defineres ud fra et ønske om at teste nye scenarier, der ikke er blevet testet tidligere.

Vælg et passende testscenarie der opfylder målet
Reelt er det kun fantasien, der sætter grænser for hvilke testscenarier, der kan anvendes.

I "Håndbog om test af beredskab" findes der i bilag A en række eksempler på testscenarier. Håndbogen findes på KL's Videnscenter.

Evaluering af testen
Efter testen afholdes en evalueringssession for at opfange læringspunkter fra de forskellige deltagere i testen.

Der udarbejdes en Beredskabsrapport til at dokumentere de erfaringer og muligheder for forbedringer, som testen har vist.

Der findes en "Skabelon for beredskabsrapport", som kan anvendes til at understøtte udarbejdelse af beredskabsrapporten. Skabelonen findes på KL's Videnscenter.

Hvem deltog og indgik i beredskabet og i afhjælpning af fejlsituationen? Hvad er de væsentligste læringspunkter fra testen?

- Hvilke ændringer skal der ske til beredskabsplanen?
- Hvilke handlingspunkter er vigtigst?
- Hvem skal informeres om resultatet af testen?

I forbindelse med udarbejdelse af beredskabsrapporten opdateres bilaget i beredskabsrapporten med handlingsplaner for områder, der skal forbedres.

Det bør sikres, at der foregår rapportering efter en test af beredskabsplaner.

Resultater fra beredskabstesten formidles til alle interessenter i beredskabsplanlægningen og særligt til ledelsen, der også godkender eventuelle handlingsplaner.

05 / IMPLEMENTERINGS-ANVISNINGER – HJÆLP TIL DEN UDFØRENDE

Det er vigtigt at være opmærksom på, at planlægning og implementering af beredskab indledningsvis starter som et traditionelt implementeringsprojekt med fast start og sluttidspunkt, men hurtigt bør opfattes som en proces, idet udarbejdelse af planer bliver genstand for periodiske tests og ændringer i bagvedliggende strategier og politikker, med heraf afledte opdateringer af beredskabet. Rollerne i beredskabet vil desuden bestå også efter den projektorienterede opstart.

Forudsætninger
Inden arbejdet med etablering af beredskabsplanerne påbegyndes, er der en række forudsætninger, der bør være styr på, dels fordi elementer i beredskabet kan være nærmest umulige at gennemføre uden, og dels fordi det kan lette udarbejdelse og implementeringen betragteligt.

Ledelsesforankring	Sikring af ressourcer og økonomi til implementeringen og den efterfølgende proces
Informations-sikkerhedspolitik	Definerer overordnet ramme for organisationens sikkerhedsarbejde
Overordnet risikovurdering	Danner grundlag for koordinering af forretningsbehov og beredskabsindsats
Fastlæggelse af beredskabsstrategi	Beskriver beredskabets overordnede mål og rammer
Identificering af kritiske forretningsprocesser	Sikrer korrekt prioritering af beredskabet, samt viser evt. behov for forretningsnødplan
Afgrænsninger	Sikrer forventningsafstemning inden detailplanlægning og implementering påbegyndes
Formidling/awareness	Sikrer commitment og fokus hos både ledelse og medarbejdere – inddrag interessenter fx via workshops

Trinvis implementering
Fra det tidspunkt, hvor de grundlæggende forudsætninger er faldet på plads, til det færdige plankompleks er udarbejdet og testet, vil der normalt gå 'en rum tid'. For at få gavn af indsatsen hurtigst muligt, kan det med fordel planlægges, så dele af planen gøres operationel fra det øjeblik indholdet er tilvejebragt, men inden koordinering og aftestning nødvendigvis har fundet sted.

Bemærk at aftestning udmærket kan gennemføres på visse delelementer, uden hele planen behøver at være færdig — herved indhentes erfaringer tidligt i forløbet, og udeståender eller begrænsninger kan hurtigere håndteres eller forelægges ledelsen.

Andre overvejelser om implementering
I forbindelse med de indledende aktiviteter er det værd at gøre sig nogle overvejelser om aspekter, der kan have indflydelse på beredskabets evne til at fungere under en hændelse, men som er svære at konkretisere eller afprøve under almindelige forhold.

Beslutningsprocessen er normalt beskrevet entydigt ud fra risikovurderingernes afledte aftaler om maksimal accepteret nedetid på et system eller proces. I praksis er det en beslutning, der kan være afhængig af mange faktorer. Det kan være tidspunktet hændelsen indtræder på, om hændelsen påvirker andre direkte eller indirekte interessenter samtidig, eller om der er forhold, der gør tilbagevenden til normaldrift særlig vanskelig. Samlet set kan det betyde, at man er villig til at acceptere en længere nedetid, for i stedet at øge indsatsen på fejlsøgning og – rettelse under de normale driftsprocedurer.

Roller og ansvar er med få undtagelser anbefalet at ligne den daglige varetagelse mest mulig af hensyn til genkendelighed. Men i praksis har det også vist sig, at nogle ledere, der i det daglige udfører deres opgaver perfekt, pludselig mister overblikket og evnen til at lede og fordele arbejdet, når vedkommende står midt i en hændelse, hvor rollen viser sig at være markant anderledes – og at der faktisk er andre personer i organisationen, uden normal ledelsesrolle, som er langt bedre til at varetage opgaverne under sådanne konditioner. En god test kan ofte belyse dette, og i en åben organisation kan der desuden ligge en aktivitet i beredskabsledelsens checkliste, hvor status og eventuel justering af organisationen kan vurderes.

Beslutningsmandat er også i forlængelse af ovenstående, et område der kan vise sig nødvendigt at have særlige retningslinjer for i en beredskabssituation, hvor man ofte opererer i døgndrift og derfor har brug for flere, der kan træffe beslutninger.

Sikkerhedsniveau og kontrol under en hændelse, hvor fx normal systemanvendelse, fysiske rammer og kontrolrutiner er påvirket, kan overvejelser om ændring af sikkerhedsniveau og løbende kontroller blive et issue.

06 / HÅNDTERING AF HÆNDELSER

Formålet med en systematisk håndtering af hændelser er at minimere risikoen for brud på fortrolighed, integritet eller tilgængelighed.

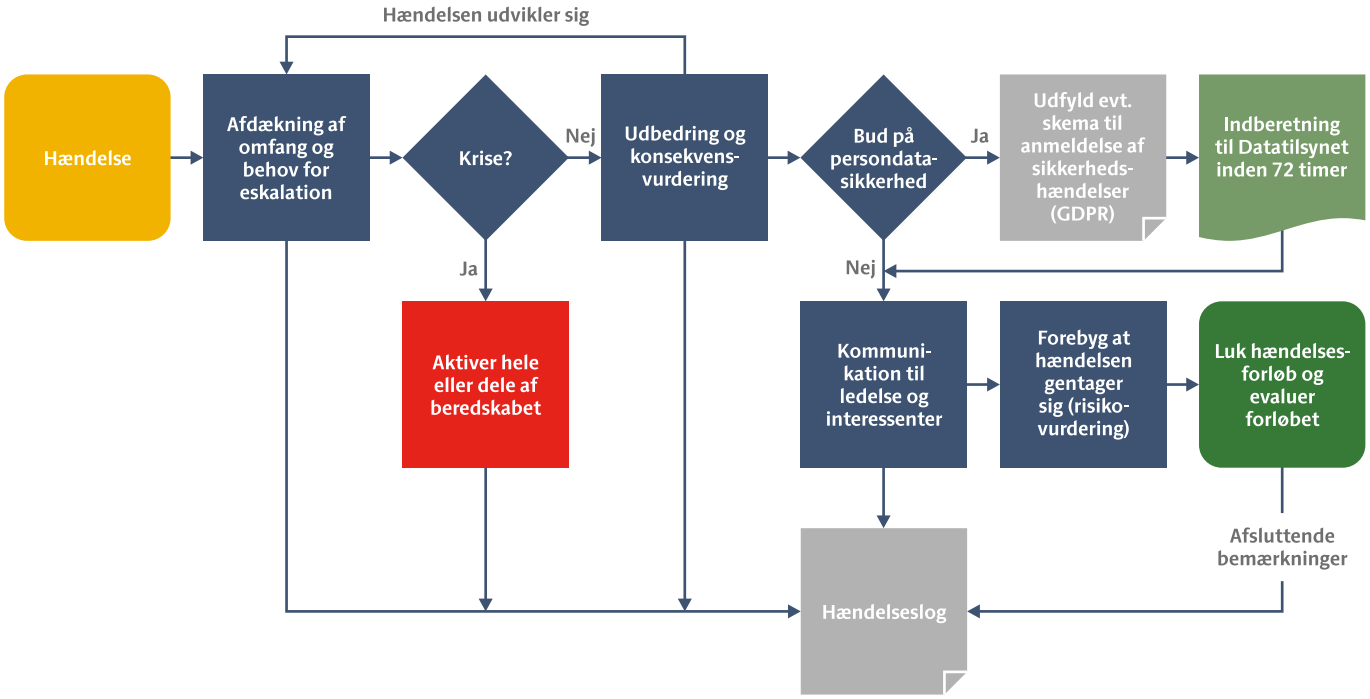
Hvis der konstateres sikkerhedsmæssige svagheder eller brud på sikkerheden, er det vigtigt, at der hurtigt rettes op på det, for at begrænse tab og hindre udnyttelse. Især når der er mistanke om brud på sikkerheden, er det vigtigt, at der handles hurtigt for at kunne begrænse eventuelle følgevirkninger. Afgørende for måden at håndtere hændelser på (og effekten af denne håndtering) er, at processen er systematisk, nem at gå til og at rapportering sker hurtigst muligt, dvs. senest umiddelbart efter eventuelle skadesbegrænsende aktiviteter er gennemført.

Den dataansvarlige skal i tilfælde af brud på persondatasikkerheden uden unødig forsinkelse og om muligt inden 72 timer foretage anmeldelse af bruddet til Datatilsynet via Virk.dk, med mindre det er usandsynligt, at bruddet medfører en risiko for personers rettigheder eller frihedsrettigheder. For at anmelde brud via Virk.dk skal NemID medarbejdersignatur anvendes.

Se i øvrigt Datatilsynets vejledning vedr. håndtering af brud på persondatasikkerhed.

Proces for hændelseshåndtering
Procestegningen nedenfor giver et bud på en tjekliste for den ansvarlige i en konkret håndteringssituation. Der bør dog altid være en vurdering af relevansen af aktiviteterne, herunder om der skal bringes flere eller andre aktiviteter og/eller aktører i spil.

› **Figuren viser et eksempel på proces for hændelseshåndtering**



Sørg for systematik i håndteringen af hændelser

Før hændelsen opstår

- Der bør beskrives retningslinjer overfor medarbejderne, så de ved hvem de skal kontakte, og hvordan de skal agere, hvis de oplever en hændelse.
- Der bør beskrives retningslinjer for, hvem der har ansvaret for eskalation af en hændelse og hvornår en hændelse eskaleres. Hvis en hændelse eksempelvis ikke er forretningskritisk og kan afklares indenfor en rimelig tid via de normale procedurer, bør en eskalering til beredskabstilstand undgås.
- Specifikke interessenter, aktører og aktiviteter i forbindelse med rapportering af sikkerhedshændelser bør beskrives i den enkelte organisation.
- Der bør oprettes faste kanaler for rapportering. Dette sikrer, at en sikkerhedshændelse altid kan rapporteres, den rette information indsamles og de rette aktører involveres.

Når hændelsen sker

- Vurderes hændelsen at have karakter af krise, følges gældende retningslinjer for beredskab.
- Informationer om sikkerhedshændelsen bør af hensyn til løsning og en eventuel retslig efterforskning opbevares med angivelse af tidspunkt og i elektronisk form.
- Alle rapporterede informationer bør behandles efter en vurdering af fortrolighed og integritet på en sådan måde, at medarbejdere og andre kan være sikre på, at informationerne ikke eksponeres unødigt.
- Der bør beskrives formelle retningslinjer for, hvornår en hændelse vurderes som afsluttet.

Efter hændelsen

- Systemejeren/risikoejeren bør indsamle beviser for outsourcede systemer i samarbejde med driftsleverandøren, hvis hændelsen er opstået forsætligt.
- Efter hver sikkerhedshændelse bør det vurderes, om der er behov for at iværksætte et forløb, der sikrer relevant erfaringsopsamling og forebyggende indsatser via en risikovurdering, fx i form af tekniske eller styringsmæssige ændringer.

It-kriminalitet er en sag for politiet

Målrettede it-kriminelle angreb bør politianmeldes og efterforskes. Som minimum bør muligheden for en politimæssig efterforskning overvejes.

KL
Weidekampsgade 10
2300 København S
Tlf. 3370 3370
kl@kl.dk
www.kl.dk
@kommunerne

Produktionsnr. 830851
ISBN 978-87-93950-71-9-pdf