DIGITALISERINGSSTYRELSEN

Vejledning til kommunikation i en beredskabssituation

Januar 2022

2022

Indholdsfortegnelse

Formålet med denne guide er at give råd og anbefalinger til, hvordan myndigheder kan styre deres kommunikation i en beredskabssituation. I guiden finder du råd og anbefalinger til, hvordan myndigheden kommunikerer til følgende interessenter:

- Medarbejdere
- Andre offentlige organisationer
- Eksterne leverandører
- Den brede offentlighed: Borgere, virksomheder og medier

Guiden er til dig, der har ansvaret for at styre din myndigheds kommunikationsaktiviteter i en beredskabssituation. Det kunne være den kommunikationsansvarlige i beredskabsorganisationen, men det kunne også være medarbejderen, der har ansvaret for at vedligeholde beredskabet i fredstid.

Her kan du læse mere: På sikkerdigital.dk finder du flere materialer, der kan støtte arbejdet med beredskabsstyring. I Etablering og vedligeholdelse af et beredskab med fokus på informationssikkerheden finder du mere hjælp til, hvordan man etablerer og vedligeholder et beredskab. Du finder også et værktøj, der kan benyttes til at foretage løbende målinger af ens beredskab samt en vejledning til benyttelse af værktøjet. Endelig finder du skabeloner til beredskabsplaner og beredskabsspil til afprøvning af beredskabet,

1. Indledning

Et af hovedelementerne til en succesfuld styring af beredskabet i en krise er at sikre en passende kommunikation til alle relevante interessenter, i rette tid og med det rette indhold.

Kommunikation skal sikre, at organisationens interessenter informeres så godt om situationen, at forvirring og rygter minimeres mest muligt. Det vil også forebygge et unødigt stort antal henvendelser og unødig forbrug af tid og kræfter, som kunne være anvendt til at håndtere selve krisen.
Kommunikation skal også sikre, at interessenterne får de fornødne oplysninger til at minimere eventuelle følgevirkninger og til at kunne etablere eventuelle alternative løsninger.

Det er derfor vigtigt, at beredskabsplanen udpeger en eller flere ansvarlige for styringen af både eks- tern og intern kommunikation i hele beredskabsforløbet. Beredskab for kommunikation skal i lighed med andre dele af beredskabet afprøves jævnligt, så der er opmærksomhed om og erfaring med udførelse af opgaverne i en krise.

Hvis organisationen først er ved at tilrettelægge sin beredskabskommunikation, eller hvis organisationen ønsker at gentænke sin beredskabskommunikation, er det en god idé først at gøre sig nogle strategiske overvejelser om kommunikationen:

- Hvem skal der kommunikeres til (interessentkortlægning)?
- Hvor åben eller lukket ønsker man at være som organisation?
- Er der forskel på, hvor åben/lukket man vil være ift. forskellige interessenter (andre myndigheder, borgere, leverandører)?

2. Roller og ansvar i beredskabskommunikationen

I det omfang det er muligt, bør rollerne udfyldes af personer, der udfører lignende kommunikationsopgaver i daglig drift, da varetagelsen kræver erfaring og øvelse, ikke mindst i pressede situationer.

Nedenstående tabel giver et vejledende overblik over de typiske rolleindehavere og en mulig fordeling af deres ansvar i relation til kommunikationen med væsentlige interessenter i en beredskabssituation. Afhængigt af organisationens interessentkortlægning kan kontaktpersoner på de forskellige interessentgrupper defineres og besluttes på forhånd.

	Intern kommunikation: Medarbejdere	**Ekstern kommunikation: Andre offentlige organisationer**	**Ekstern kommunikation: Leverandører**	**Ekstern kommunikation: Borgere, medier og virksomheder**
Topledelse	Godkender kommunikation om forhold, der har betydning for arbejdsopgaver og ansættelsesforhold.	Bestiller og godkender kommunikationsstrategi for kommunikation til andre offentlige organisationer.	Godkender kontraktlige dispositioner omkring kommunikation.	Godkender kommunikationsstrategi for kommunikation med offentligheden. Godkender evt. skuffemeddelelser. Godkender indhold og timing af bud- skaber, som løbende sendes ud.
Kommunikationsansvarlig	Inputgiver til HR-chef.	Varetager kommunikation på ledelsesplan i forhold til andre offentlige organisationer, som er berørt af krisen.	Rådgiver og sparringspartner på det kommunikationsfaglige.	Koordinerer varetagelsen af kommunikation med offentligheden blandt kommunikationsmedarbejderne.
HR-ansvarlig	Giver input til kommunikationsansvarlige om forhold, der har betydning for ansættelsesforholdet.			
Beredskabskoordinator	Varetager kommunikation om retableringsindsatsens fremskridt.	Varetager kommunikation med beredskabskoordinatorer hos andre offentlige organisationer	Koordinerer varetagelsen af den løbende kommunikation, som er nødvendig af hensyn til den overordnede håndtering af krisen.	Giver input til den kommunikationsansvarlige om retableringsindsatsens fremskridt.
Linjeledelse	Varetager kommunikation om iværksættelse af forretningsnødplaner.		Varetager eventuel kommunikation om funktionelle forhold i relation til forretningssystemer.	
Retableringsteams		Varetager en eventuel kontakt på det tekniske plan.	Varetager kontakt på det tekniske plan	

	Intern kommunikation: Medarbejdere	Ekstern kommunikation: Andre offentlige organisationer	Ekstern kommunikation: Leverandører	Ekstern kommunikation: Borgere, medier og virksomheder
Helpdesk[1]	Varetager kommunikation om retableringsindsatsens fremskridt.	Kommunikationsansvarlig koordinerer ekstern kommunikation	Varetager initial kontakt ved konstatering af den hændelse, der udvikler sig til en beredskabssituation.	

Flere af skemaets forslag er uddybet i nedenstående afsnit under overskriften *Hvem er ansvarlig for kommunikationen*?

[1] Mange offentlige organisationer har outsourcet it-servicedesk/helpdesk. I så fald skal dens rolle i en beredskabssituation aftales i leverandørkontrakten. Er det ikke muligt, må de anførte opgaver fordeles på interne rolle- indehavere

3. Intern kommunikation til medarbejdere

Formålet med kommunikation til medarbejderne er at sikre, at organisationen så hurtigt og let som muligt kan komme tilbage i normal drift eller etablere midlertidig drift. I visse tilfælde kan kommunikationen til medarbejderne også være afgørende for at begrænse konsekvenser af hændelsen.

Ved større kriser (fx systemnedbrud) kan et større antal medarbejderes arbejde blive berørt. Det er vigtigt, at de rette medarbejdere får faktuelle og informative beskeder hurtigt om situationen.

3.1 Hvad skal kommunikeres?

Først og fremmest bør det overvejes, hvilke medarbejdere der er mest berørt af hændelsen, så kommunikationen til netop dem med det største behov prioriteres og håndteres først. Afhængig af situationen kan det også overvejes, om det er hensigtsmæssigt at kommunikere til hele organisationen. Hvis nyheden om krisen fx har pressens interesse, bør alle medarbejdere som minimum være informeret på samme niveau som pressen.

Dernæst skal det kommunikeres:

- Hvordan medarbejderne skal forholde sig og agere under nedbruddet. Dette afhænger af, hvor kritisk det ramte område er (fx et it-system) og af de forretningsnødplaner, der eventuelt knytter sig til det.
- Hvad medarbejderne skal holde fortroligt/må kommunikere videre om hændelsen. Det skal dels vurderes, hvor meget af krisesituationen, der skal kommunikeres til medarbejderne. Dels skal det tydeliggøres, hvis dele af de kommunikerede oplysninger er fortrolige af hensyn til forretningen, samarbejdspartnere eller samfundets sikkerhed. Informationer om flytning af medarbejdere: De afdelinger, der indgår i en plan for flytning til ny lokation, skal have praktiske informationer om tid, sted, og hvad der skal medbringes. Informationer om forretningsnødplaner: De afdelinger, der indgår i forretningsnødplaner, skal instrueres i evt. nye eller ændrede arbejdsgange. De, der af relevante årsager ikke er omfattet af forretningsnødplanen, skal orienteres om hvordan de skal forholde sig under de nye omstændigheder.

Medarbejderne skal løbende opdateres om, hvordan det står til – dvs. skrider situationen frem, eller er status den samme som tidligere. Hvor tit, man vælger at kommunikere, skal besluttes af ledelsen. Både for ofte og for sjælden kommunikation er ikke at foretrække. Denne del af kommunikationen kan med fordel varetages af topledelsen, hvis der er egnede kommunikationskanaler til rådighed.

3.2 Kommunikationskanal

Når der er tale om en krise, der vedrører organisationens it-understøttelse, vil man ofte benytte de samme kommunikationskanaler som ved driftsforstyrrelser og andre mindre hændelser. Hvis medarbejderne er vant til at holde sig opdateret via en it-service eller webside på organisationens intranet, vil det også være den oplagte kommunikationskanal i en beredskabssituation. Hvis it-servicedesk eller helpdesk-funktionen er outsourcet til en leverandør, anbefales det i leverandørkontrakten at præcisere dens rolle i beredskabssituationer – ikke mindst vedrørende intern kommunikation.

Hvis der som følge af beredskabssituationen ikke er adgang til intranettet, eller hvis det er afgørende, at medarbejderne får besked straks, kan det overvejes at sende beskeden direkte på telefon eller mail til de relevante afdelinger. Der kan alternativt iværksættes telefonkæder til chefer, som kan kommunikere mundtligt med de medarbejdere, der er fysisk til stede. Aftaler om og afprøvning af alternative kommunikationskanaler bør indgå i kommunikationsberedskabets etablering og vedligehold.

Det skal overvejes, om nogle af de skriftlige meddelelser i beredskabssituationen skal formuleres på forhånd (et såkaldt skuffeberedskab), og om de operationelle nødplaner og kommunikationsplaner skal printes i fysisk form eller lægges på USB-sticks, som opbevares sikkert hos den kommunikationsansvarlige, beredskabskoordinatoren eller andet steds.

Det er vigtigt at gemme dokumentation for udsendt kommunikation, samt beslutninger herom til efterfølgende evaluering.

4. Kommunikation til andre offentlige organisationer

Det er ikke ualmindeligt, at offentlige organisationer kan blive påvirket af en krise i en anden offentlig organisation. Det kan være tilfældet for de myndigheder, der stiller it-tjenester til rådighed for hinanden. Tjenester, der stilles til rådighed mellem organisationer, kan let resultere i mistet tilgængelighed flere steder, hvis de fejler alvorligt. Derfor er det vigtigt, at den systemansvarlige myndighed sikrer kommunikationen til de myndigheder, som er afhængige af systemet. Vice versa hvis en myndighed er afhængig af et system, som en anden myndighed er ansvarlig for, er det vigtigt, at der etableres en kontaktperson til den myndighed.

Udveksler myndighederne data med hinandens tjenester, kan der også være behov for at afstemme kommunikationsansvaret i tilfælde af en krise, hvor flere parter er berørte.

4.1 Hvem er ansvarlig for kommunikationen?

Hvis der er tale om flere forskellige organisationer, kan det være relevant at uddelegere ansvaret mel- lem flere kontaktansvarlige. Det kan eventuelt være de samme medarbejdere, som i det daglige varetager kontakten med disse samarbejdspartnere. Hvis ansvaret fordeles, bør det dokumenteres i beredskabsplanen.

4.2 Hvad skal kommunikeres?

- Aktivering af nødplaner: I starten af en beredskabssituation vil der være et stort behov for at kommunikere til de afhængige myndigheder, at en alvorlig hændelse medvirker at væsentlige forretningsprocesser ikke kan understøttes, samt hvad tidshorisonten for genetablering af normaldrift er. Myndighederne kan derved bedre vurderer, om de skal aktivere egne nødplaner.
- Resultat af fejlsøgninger: Dernæst bør myndighederne holdes opdaterede om genetableringen af normaldrift.
- Aftaler om løbende statusopdateringer: Når fejlen er fundet, og beredskabsarbejdet overgår til retablering eller rettelse i de konkrete systemer, skal der aftales med de andre berørte parter, hvor ofte man ønsker statusopdateringer på, hvordan løsningen skrider frem.

4.3 Kommunikationskanal

Med mindre e-mail, almindelig telefoni eller andre foretrukne kommunikationskanaler er berørt af hændelsen, vil disse som regel benyttes som kommunikationskanal Alternativt kan benyttes (og afprøves på forhånd) krypterede sms-tjenester, beredskabstelefoner, bude mm.

4.4 Hvornår skal kommunikationen ske?

Hvis flere offentlige organisationer skal kontaktes, er det væsentligt at danne sig et overblik over, hvem der er mest påvirket af hændelsen. Er der fx tale om et utilgængeligt system, skal det på forhånd være afklaret, hvilken organisation der har den laveste målsætning for genetablering (RTO) i forhold til det ramte system. Jo mere kritisk systemet er for samarbejdspartneren, jo vigtigere er det at give besked straks.

Der kan udarbejdes en tidsplan, så den ansvarlige for kommunikationen får lettere ved at holde styr på beslutninger. Tidsplanen kan ligeledes anvendes til logning af aktiviteter.

4.5 Skabelon til ekstern kommunikation til andre offentlige organisationer

	Hvem	Besked	Kanal	Tidspunkt
Eksternt				

5. Ekstern kommunikation til driftsleverandør(er)

Ud over de planlægningsmæssige opgaver bør fordelingen af de operationelle opgaver i en beredskabs- situation også aftales med leverandører af it-services. Selve opgaverne ved retableringen vil i de fleste tilfælde udføres af den leverandør, som varetager driften. Men det er vigtigt at få aftalt, hvordan kommunikationen mellem parterne skal foregå.

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

De konkrete aktiviteter i forhold til styring af leverandøren i en beredskabssituation bør planlægges og beskrives i en handlingsplan. Et eksempel herpå findes i *Skabelon til it-beredskabsplan.*

5.1 Hvem er ansvarlig for kommunikationen?

Det skal besluttes, hvem der har kontakten til leverandøren. Det er naturligvis en fordel, hvis denne er udpeget på forhånd.

Den initiale kontakt finder som regel sted mellem it-ansvarlige medarbejdere som en del af den almindelige håndtering af driftshændelser, inden det endeligt er konstateret, at der er tale om en beredskabs- situation.

Så snart det står klart, at situationen er alvorlig, bør kommunikationen eskaleres til beredskabskoordinatoren hos henholdsvis organisationen og leverandøren. De bør være udpeget på forhånd og fremgå af driftsaftalen.

Efterfølgende kan kommunikationen falde tilbage på et teknisk plan i selve retableringsfasen. Det er væsentligt, at ansvaret for denne del af kommunikationen ligger hos medarbejdere, der har relevant teknisk og forretningsmæssig viden. Hos organisationen vil den derfor blive varetaget af de medarbejdere, som er fagligt ansvarlige for de nedbrudte it-services, eller som anvender dem i det daglige arbejde.

Under hele beredskabsforløbet vil kommunikationen veksle mellem de to niveauer afhængig af karakteren af det, der kommunikeres om.

5.2 Hvad skal kommunikeres?

- Aktivering af beredskab og omfang: Det skal naturligvis sikres, at den eksterne leverandør får klar besked om hændelsen, og at leverandøren også kommunikerer klart og rettidigt den anden vej. Selve situationen skal beskrives, så alvoren og omfanget af hændelsen er tydelig. Det skal sikres på beredskabskoordinatorniveau, at leverandøren opfatter og behandler hændelsen som en beredskabssituation. Oplysninger tbf. håndtering: Leverandøren skal have alle væsentlige oplysninger til at træffe de nødvendige beslutninger.
- Støtte ang. testhandlinger mm.: Hvis leverandøren har det fulde driftsansvar for det ramte system, antages det, at leverandøren har sine egne retableringsplaner. Organisationen skal dog være klar til at udføre testhandlinger, konfigurationsændringer, prøver mv. på leverandørens anvisning.
- Orientering om øvrig retablering: Hvis den pågældende leverandør drifter en mindre del af et samlet system, vil det være relevant at give information om, hvilke tiltag til midlertidig omgåelse af problemet, der måtte være besluttet fra anden side, og som kunne have indvirkninger på retableringsindsatsen.
- Fortrolighed: Endeligt bør leverandøren informeres om, hvorvidt dele af eller hele hændelsen er fortrolig i forhold til eksterne interessenter eller eventuelt visse medarbejdere.

5.3 Kommunikationskanal

Med mindre e-mail, almindelig telefoni eller andre foretrukne kommunikationskanaler er berørt af hændelsen, vil disse som regel benyttes som kommunikationskanal. Er de utilgængelige, må organisationen forsøge at få personlig kontakt til leverandøren. Alternative kommunikationskanaler bør være overvejet og afprøvet på forhånd – fx beredskabstelefoner, krypterede sms-tjenester, bude mm.

5.4 Hvornår skal kommunikationen ske?

Hvis rettelse af fejl eller retablering af data er afhængig af leverandøren, er det naturligvis vigtigt straks at slå alarm. Hvis der er flere leverandører involveret, skal de prioriteres.

Herudover er det vigtigt at holde kommunikationskanalen åben i hele beredskabsforløbet. I bered- skabsplanen kan det være en god idé at beslutte faste statusintervaller for kommunikationen på koordinatorniveau og koordinere disse med driftsleverandørens egen beredskabsplan.

5.5 Skabelon til ekstern kommunikation med leverandører

	Hvem	Besked	Kanal	Tidspunkt
Eksternt				

6. Borgere og virksomheder

Når organisationen melder ud om en kritisk it-tjenestes nedbrud, medfører det som regel interesse og henvendelser - også fra pressen. Organisationen må forberede sig på at besvare den kritik og de spørgsmål, der følger med.

Da hændelsen kan forstyrre borgere/virksomheders drift, adgang til data eller sågar kompromittering af data, kan sikkerhedshændelser hurtigt møde stor kritik fra omverdenen. Derfor kan det være en god idé at have. Udfordringen med at kommunikere kan bl.a. bestå i at kommunikere tilpas præcist om en hændelses væsen uden at miste blik for, hvad man helt præcist ønsker at fx borgere, der ikke har den tekniske indsigt, skal gøre.

Disse udfordringer imødekommes bedst gennem forberedelse af kommunikation til borgere og virksomheder, herunder af hvordan de mere komplekse sikkerhedshændelser og beredskabsprocesser kan formidles på en måde, der skaber tillid og tryghed til organisationen.

6.1 Hvem er ansvarlig for kommunikationen?

Organisationens kommunikations- eller presseansvarlige vil ofte stå for styring af kommunikationen udadtil mod borgere, virksomheder og offentligheden generelt. Det skal besluttes, hvem der kan og må udtale sig om beredskabssituationen, og der skal udarbejdes interne instrukser herom, som er afprøvet på forhånd. Der bør være aftalt med eventuelle eksterne leverandører, at det er myndigheden, der er ansvarlig for kommunikation ud mod offentligheden.

6.2 Hvad skal kommunikeres?

- Alternative muligheder og ændringer i frister: De borgere og virksomheder, som er berørt af en alvorlig hændelse, skal have besked om alternative muligheder for at få adgang til vitale serviceydelser. Hvis nedbruddet påvirker muligheden for at overholde frister, bør eventuelle fristforlængelser kommunikeres hurtigst muligt. Hvis økonomiske interesser er på spil, bør kommunikationen omfatte råd og vejledning til at begrænse et potentielt tab.
- Tidshorisont: Borgere og virksomheder bør om muligt få besked om en estimeret tidshorisont for, hvornår tjenesten igen vil være tilgængelig.
- Svar på kritiske spørgsmål: Det skal overvejes, hvordan man vil respondere på kritiske spørgsmål fra presse og borgere. I den forbindelse bør det overvejes at udarbejde skuffemeddelelser, som er tilpasset bestemte situationer eller spørgsmål og som hurtigt kan hives frem, tilpasses og sendes ud. En anden mulighed er at forberede en

presseberedskabs-FAQ, som besvarer de 10 mest sandsynlige spørgsmål.

6.3 Kommunikationsplan

Valget af kommunikationskanal kan bl.a. afhænge af beredskabskrisens størrelse, og hvor mange borgere og virksomheder, som berøres af hændelsen. Hvis det er en hændelse, som en stor del af offentligheden vil have interesse i, kan situationens tilstand formidles via en pressemeddelelse, pressekonference, TV-, radio- eller avisernes hjemmesider.

Derimod vil de hændelser, som får en mindre direkte effekt på borgerne og virksomhederne muligvis være tilstrækkeligt kommunikerede via beskeder på organisationens hjemmeside eller lignende.

6.4 Hvornår skal kommunikationen ske?

Kommunikationen bør finde sted, så snart det står klart, at en kritisk samfundsvendt it-tjeneste er berørt af en alvorlig hændelse. Det er en klar ulempe at være på bagkant af medier, sociale medier mv. Presset i form af henvendelser og negativ påvirkning af organisationens omdømme bliver hurtigt stødt stigende. Organisationen bør derfor overveje at udnytte den tidsmæssige fordel, den har i erkendelsen af krisen, til at kommunikere tidligt i forløbet – også inden ansvar og årsager til hændelsen er endeligt klarlagt.

6.5 Skabelon til ekstern kommunikation til borgere/virksomheder

	Hvem	Besked	Kanal	Tidspunkt
Eksternt	Presse			
	Borgere			
	Virksomheder			

7. Tidsplan for kommunikationsaktiviteter

Som forberedelse til en beredskabssituation bør man have gjort sig nogle tanker om, hvordan kommunikationsindsatsen planlægges og organiseres – også på timebasis, så kommunikationsplanen i praksis kan kobles til mål om maksimale nedetider.

Et forløb kan f.eks. se ud som det fremgår af nedenstående skema. Selvom forløbet i praksis vil afhænge af hændelsens karakter og mulighederne for at retablere systemerne, kan skemaet give inspiration til relevante overvejelser om, hvad der skal til for at gøre kommunikation til en naturlig del af beredskabsindsatsen.
I skemaet er der kun nævnt ét møde med beredskabsorganisationen, men det er oplagt at den kommunikationsansvarlige er med på flere møder med beredskabsorganisationen for hele tiden at gøre kommunikationen så korrekt og velovervejet som muligt.

00 00	Møde med beredskabsorganisationen
+01 00	Indsamle informationer
+02 00	Første udkast af meddelelse om beredskabssituation til hhv. intern og ekstern målgruppe
+02 30	Andet udkast af meddelelse om beredskabssituation – godkendt af teknisk specialist
+03 00	Godkendelse af kommunikationsplan
+03 30	Intern information It-informationsside Intranet
+04 00	Ekstern information Pressemeddelelse, Interview, Svar på spørgsmål, Hjemmeside

Guide til kommunikation i en beredskabssituation
Udgivet januar 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: 978-87-93073-47-0