UiT Norges arktiske universitet

Fakultet for naturvitenskap og teknologi / Institutt for teknologi og sikkerhet

Hvordan skape mening av det usynlige

Et teoretisk rammeverk for sensemaking under dataangrep.

Einar Lohne Bjøru

Masteroppgave i samfunnssikkerhet - SVF-3920 – 31.05.2023.

Ord: 16.596

UiT

NORGES
ARKTISKE
UNIVERSITET

Sammendrag

Dataangrep er en økende trussel blant organisasjoner og virksomheter i Norge. Et ekstra element i dette er at trusselen er vanskelig å se og forstå for aktører som ikke er utdannet eller har kompetanse på det tekniske fagfeltet. Problemstillingen for denne studien tar for seg hva som er viktig for at offentlige organisasjoner skal kunne forstå og formidle omstendighetene under et dataangrep. Studien presenterer et teoretisk rammeverk med utgangspunkt i sensemaking-teorien. Formålet er å skildre hvordan de tilhørende konseptene tillit, meaning-making, framing og transparens spiller inn på sensemaking-prosessen. Det argumenteres for at dette rammeverket bidrar, som et verktøy, til å kunne analysere offentlige organisasjoners forståelse, håndtering og kommunikasjon under et dataangrep. Med utgangspunkt i Nordland fylkeskommunes dataangrep desember 2021, argumenterer studien videre for at spesielt tillit er nødvendig for en god sensemaking-prosess. I sammenheng med dette viser rammeverket hvordan framing og transparens – i samspill med sensemaking – er med på å gi grunnlag for meaning-making.

Forord

Seks år med studietid er ved veis ende. En vei som har gått via Bergen, Kairo, København og til slutt – Tromsø. Jeg er utrolig glad for at jeg til slutt endte opp med å satse på en master i samfunnssikkerhet, og ser tilbake på tiden som givende.

En takk til veileder Christer Pursianen, som har gitt flere timer til meg enn han har behøvd. Etter hvert møte har jeg kunnet gå tilbake til skrivingen med fornyet tro på at oppgaven blir fullført, og et produkt jeg har tro på.

Utover det vil jeg takke mine medstudenter ved UiT – både de jeg har blitt kjent med fysisk og digitalt. De sørget for at jeg fikk en forkjærlighet for faget, og at slutten på studenttilværelsen ble en gøy tid. Takk til Nordland fylkeskommune som har bidratt som case til denne studien. På hjemmebane; Takk til Mathilde, som i denne tiden sørger for at vår felles drøm får vokse til. Takk også til mine søsken og foreldre – som svarer positivt på mine sporadiske innfall om studie- og jobbideer. En siste, ekstra takk går til Emil Engen Granås, som har vært en god venn i tykt og tynt de siste seks år, og som alltid stiller opp – enten det er lange samtaler i tunge stunder, eller som korrekturleser av denne oppgaven.

God lesing.

- Einar Lohne Bjøru
Mai, 2023

Innholdsfortegnelse

1 Introduksjon

Dataangrep er en økende tendens i verden i dag, og i Norge er offentlige forvaltningsorganer blant de som er særlig utsatt for angrep. Det er ikke et spørsmål *om* det blir et datarelatert angrep, men *når.* Da er statlige organisasjoner tvunget til å tolke og forstå store mengder informasjon, og ivareta en gruppe av ulike parter (Naseer et al., 2021). Med en stadig digitalisering av samfunnet vil derfor mange statlige ansatte være avhengig av å bruke digitale hjelpemidler og internett som arbeidsverktøy. Virksomheter har derfor et ansvar for å ivareta sikkerheten til IT-relatert informasjon. Samtidig er det en mangel på kompetanse rundt dataangrep og cyberkriminalitet, og samfunnet er nå avhengig av en teknologi som er dårlig - om i det hele tatt - forstått av sine brukere (*Nasjonalt digitalt risikobilde 2022*, 2022; Naughton, 2016). Politikere, byråkrater, borgere og andre berørte parter er avhengig av teknologi de nødvendigvis ikke innehar nok kunnskaper til å kunne ta avgjørelser med. De som sitter med kunnskapen til IT-relaterte tjenester, har heller ikke nødvendigvis den totale innsikten til å kunne fatte avgjørelser som er gunstig for hele organisasjonen (Happa & Fairclough, 2016). Det medfører at raske avgjørelser tas av organisasjoners ledelse for å unngå at det blir store konsekvenser av et dataangrep, til tross for mangelfull informasjon og tidspress (Lakshmi et al., 2021). Denne kompleksiteten danner grunnlaget for denne masteroppgaven, der det vil det være interessant å ta en nærmere kikk på hvordan ledelsen i offentlige forvaltningsorganer forstår situasjonen som utfolder seg, og deretter formidler videre til de berørte parter, eller interessenter, ved eventuelle angrep. Studien presenterer et rammeverk for hvordan situasjoner forstås, med utgangspunkt i sensemaking-konseptet (Boin et al., 2021). Videre vil den trekke frem noen sentrale elementer som bør være til stede for å kunne forstå et dataangrep utfolde seg, og handle raskt deretter. Studien tar utgangspunkt i angrepet mot Nordland fylkeskommune i desember 2021. Her analyseres prosessen for hvordan sentral kriseledelse i organisasjonen raskt kom frem til en drastisk avgjørelse om å koble hele organisasjonen fra internett – som senere skulle vise seg å være avgjørende for at fylkeskommunen ikke fikk større konsekvenser av dataangrepet. Studien ser også på hvordan kommunikasjon spilte en rolle i situasjonen.

Videre i dette introduksjonskapittelet vil problemstilling og avgrensninger bli presentert, før et dypdykk i studiens utgangspunkt. Deretter vil resten av studiens struktur bli presentert.

1.1 Problemstilling

Problemstillingen for studien er:

> *Hva er viktig for at offentlige organisasjoner skal kunne forstå og formidle omstendighetene under et dataangrep?*

Denne innfallsvinkelen vil kunne gi en forståelse, og danne grunnlag for et teoretisk rammeverk for hvordan organisasjoner kan legge til rette for å håndtere situasjoner i fremtiden. Statlige organisasjoner i Norge bør ha nødvendig kompetanse til å både håndtere slike kriser – men også kommunisere dem. Nordland fylkeskommune ble på tampen av 2021 rammet av et dataangrep. Dette førte til at kriseledelsen raskt fattet beslutningen med å stenge ned hele nettverket i organisasjonen. Til tross for at man da utsatte over 3000 ansatte, og opp mot 15.000 andre berørte, i form av å ikke ha tilgang til arbeidsredskapene sine, høstet de ros for sin avgjørelse av myndigheter og fagkompetente nettverk. Denne studien har som formål å skape en utdypende forståelse av hvor komplisert krisehåndtering og kommunikasjon er ved å se på hva som ledet opp til at fylkeskommunen nådde sin avgjørelse. Studien vil også deretter vise hvilke faktorer som ligger til grunn for de avgjørelsene som faktisk tas i slike situasjoner.

1.2 Avgrensninger

Der andre kriser, som pandemi og naturkatastrofer, i seg selv kan være mer fysisk og forklarende på hva som er situasjonen, viser litteraturen at dataangrep her har en ekstra utfordring. Dette gjelder det å ha nødvendig kompetanse for å forstå situasjonen når den utfolder seg, samt kommunisere hendelsene videre til berørte parter. I et mangfold av relevant litteratur, teori og empiri, har denne studien identifisert et hovedkonsept i *sensemaking*[1], som kan kaste lys over problemstillingen. For å gå nærmere inn på hvordan denne prosessen var i Nordland fylkeskommune, vil konsepter som *meaning-making, framing, tillit* og *transparens* bli benyttet – inkludert i et rammeverk, som illustreres i kapittel 3. Med dette som utgangspunkt, vil man kunne få et innblikk i hvilke elementer som gjorde at ledelsen i fylkeskommunen forsto hva som var i ferd med å utfolde seg, og hvordan de videre valgte å agere. Men denne studien viser at sensemaking-konseptet har behov for mer utfyllende og komplementerende konsepter for å kunne forklare hele fenomenet som studeres. Derfor søker

[1] Da litteraturgjennomgangen ikke har vist til noen gode oversettelser av «sensemaking», «framing» og «meaning-making» til norsk, vil det engelske ordet bli benyttet i studien.

denne studien å presentere et teoretisk rammeverk, med mål om å kunne gi en dypere forståelse av hvordan organisasjoner kan håndtere situasjoner hvor dataangrep er relatert.

Grunnen for dette utgangspunktet, er som Happa og Fairclough (2016) nevner, at en organisasjons ledelse vil ha ulike utgangspunkt og føre til en ulik forståelse og ulike tilnærminger til løsning på problemet. Samtidig som tekniske vurderinger må legges til grunn, er det også en politisk, organisatorisk og finansiell kontekst som må vektlegges når man skal komme til beslutninger. Ved å ikke benytte seg av ressurser som har nødvendig kompetanse, vil det oppstå en slik dynamikk i kriseresponsen som igjen vil gjøre at nødvendige tiltak ikke blir iverksatt. Å både forstå, og kommunisere, hendelsen er derfor utfordrende.

1.3 Litteratur og forskningsspørsmål

En gjennomgang av litteraturen, som vil bli presentert i kapittel 2, viser et mangfold av hvordan angrepsrammede organisasjoner håndterer slike angrep. Tillit og samarbeid, både til hverandre i ledelsen, men og på tvers av hierarki, er et gjennomgående tema. Diers-Lawson et al. (2021) sine funn påpeker at en proaktiv holdning til en god relasjon med folk i organisasjonen vil gi en større effekt i krisekommunikasjonen, og at kommunikasjonen bør inneholde organisasjonens kompetanse og omsorg, samt identitet. I spørsmålet om skyldfordeling under kommunikasjonen med berørte parter, tenderer organisasjoner til å legge skylden på den eksterne aktøren som utfører angrepet, mens teoretikere påpeker at det er formålstjenlig for en organisasjon å ta skyld selv overfor interessenter og ivaretakelse av omdømme, uttrykke beklagelse overfor berørte parter, samt vise empati og forståelse for den vanskelige situasjonen. I tillegg viser litteraturen til transparens som et virkemiddel for å skape tillit til organisasjonens håndtering av krisen, og samtidig ha en avskrekkende effekt på potensielle aktører som kan være truende til å utføre samme type angrep. Dette blir enda mer innfløkt hvis man tar med Kaschner (2022) sitt perspektiv på dataangrep, der argumentasjon om at det kan være grunner for å holde tilbake informasjon, grunnet lov- og sikkerhetsmessige hensyn. Dette gjør informasjonsdeling til en krevende øvelse.

Litteraturen viser til en del teoretiske gjennomganger av hvordan man oppdager og forstår dataangrep, og hvordan kommunikasjonen går videre. Det er likevel et mangelfullt grunnlag av empiriske gjennomganger av hvorfor ledelsen agerer slik de gjør i gitte situasjoner som innebærer angrep på cybernettverket. Problemstillingen er avgrenset til ledelsens respons ved krisetilfeller, og hvordan de selv kommuniserer og forstår situasjonen som utfolder seg, og hvordan de videre kommuniserer hva som skjer til andre relevante parter. Studien baserer seg

på to forskningsspørsmål ut fra problemstillingen, der det ene spørsmålet har et sub-spørsmål, grunnet samme tematikk. Første spørsmål er å undersøke hva som gjorde at ledelsen ved organisasjonen forsto at dataangrepet var av en så alvorlig art at drastiske tiltak måtte til. Under dette kommer også spørsmålet om hvilken mellom-menneskelige relasjoner gjorde at kriseledelsen forsto alvorligheten av dataangrepet. Som et siste forskningsspørsmål, undersøker studien på hva som var organisasjonens hovedfokus når det gjaldt formidling og kommunikasjon til de som er berørt av hendelsen.

Forskningsspørsmålene dreier seg om mellom-menneskelige faktorer, kommunikasjonen, og spør konkret om hvilke elementer som gjorde at ledelsen forsto at det var snakk om mulig krise, og hva de selv valgte å fokusere på i videre kommunikasjon med omverdenen.

1.4 Studiens utgangspunkt

Dataangrepet i Nordland fylkeskommune danner grunnlaget for analysen i denne studien. Dette underkapittelet er basert på informasjon fra fylkeskommunens egne nettsider og pressemeldinger, samt nyhetsartikler som rapporterte om angrepet, og rapporter fra eksterne firma og fagmyndigheter. Konklusjonen til sistnevnte er at fylkeskommunens reaksjon var avgjørende for at situasjonen ikke fikk et større konsekvensomfang enn det som kunne vært. Men det er viktig å legge grunnlaget for hva det skal snakkes om. For å definere dataangrep, eller cyberangrep, tar denne forskningen utgangspunkt i Kaschner (2022) sin forklaring. Den forklarer at IT-systemer spiller en sentral rolle i beskyttelse av informasjonssikkerhet, som konfidensielle opplysninger, integritet og kommunikasjonen mellom deltagere i systemet. Et angrep eller brudd på sikkerheten til dette systemet, vil da kunne utvikle seg til en krisesituasjon der liv kunne stå på spill, eventuelt opplysninger som kan skade strategiske mål, omdømme eller organisasjonens videre drift og overlevelse. Chayes (2015) argumenterer for at det er viktig for en definisjon å skille mellom det som er et angrep som rammer staten på en skadelig måte, og angrep som er kommersielt tyveri eller spionasje, og fremhever en definisjon som sier at et cyberangrep er et angrep som innbefatter en handling som underminerer et datanettverks funksjonalitet i et politisk eller nasjonalt sikkerhetsøyemed. Da disse definisjonene er på et overordnet nivå, kan man se på Mehdi (2014) sin konseptualisering av dataangrep, for å få et blikk på dets egenskaper – som forfatteren sier består av fem punkter. Dette innebærer i) aktører involvert, som minst er to – angriper og den angrepne; ii) den angripende aktørs mål med angrepet, hvilke eiendeler den er ute etter fra den andre part; iii) motivasjon, som informasjon, penger og data; iv) effekten av angrepet; v)

lengde på angrepet. Organisasjoner vil gjerne ha systemer og prosesser for hvordan svare på dataangrep som kan true sikkerheten deres (Ahmad et al., 2020). Standardiserte verk, slik som International Organization for Standards (ISO), er med på å gi organisasjoner verktøy og retningslinjer de kan implementere i organisasjonen, og etter hvert kan ulike hendelser og erfaringer være med på å finjustere hvilken respons som fungerer best. Derfor er mesteparten av undersøkelser rettet mot hvordan å effektivisere prosessen, men få undersøkelser har sett på hvordan prosessen påvirkes av interaksjoner mellom organisasjon, teknologi og individer – noe Lakshmi et al. (2021) adresserer. Denne studien forsøker å komme med et bidrag på dette, noe som vil illustreres i neste kapittel.

22. og 23. desember 2021 ble Nordland fylkeskommune rammet av et dataangrep, fra ukjent aktør. Datasystemene ble rammet av skadevare som kom forbi brannmuren til organisasjonen (Budalen, 2021). Angrepet medførte at fylkeskommunens nettverk ble stengt for omverdenen den 23. desember 2021. Folk utenfor fylkeskommunal lokasjon kunne da ikke få tilgang til organisasjonens systemer. Ifølge fylkeskommunens egne nettsider, forklares det at 18.000 mennesker kunne være berørt av angrepet, noe som inkluderer ansatte, elever i videregående skole, fagskole, nettskole og lærlinger (Forsland, 2022). Den 14. januar 2022 slapp fylkeskommunen en pressemelding angående innbruddet, der de bekreftet at personopplysninger til disse 18.000 menneskene kunne være på avveie. Dette innebar informasjon om fødselsnummer, navn, telefonnummer, e-postadresser og brukernavn i organisasjonen (Willasen, 2022).

I pressemeldingen kom det frem at fylkeskommunen formidler beskjeden fordi de ønsker å være føre var, da de som utførte angrepet hadde fått innhentet en mindre mengde data i tidsrommet fra angrepet skjedde til nettverket ble stengt ned – i tillegg til at opplysninger om at systemene var utilgjengelige utenfor fylkeskommunale bygg, og at det ville blitt grundig gjennom før gjenopprettelse (Willasen, 2022).

19. januar 2022 annonserer fylkeskommunen i blant annet Bodøposten at de trinnvis gjenåpner systemene (Andreassen, 2022). Til da hadde de gjenåpnet tidsstyrt internett for videregående skoler, deretter lønns- og faktura-betaling. 18. juni legger Dagbladet ut en artikkel i samarbeid med Kommunal Rapport, der de intervjuer en fylkesdirektør i organisasjonen. Her beskrives det at ansatte hadde vært uten nett i flere uker og at angrepet var stadig under etterforskning (Frigård, 2022). Der uttaler de at de ikke vet hvem som står bak angrepet, men at det er spor til utlandet. Et arbeid med å styrke sikkerheten, forbedre

overvåkingen av nett-trafikken, ble utført i etterkant, og fylkesdirektøren uttaler til avisen at de har gjort erfaringer som viser hvor avhengig de er av IKT-strukturen for å sikre sin levering av tjenester (Frigård, 2022). I samme artikkel opplyser politiet at spor tyder på at angrepet kom fra utlandet, og at angrepet virker å ha blitt avbrutt. Fylkesdirektøren sier til dette at fylkeskommunen oppdaget angrepet raskt og at det bidro til å redusere skadeomfanget. De hadde et sikkerhetsnett som gjorde at de oppdaget de som angrep systemet, og svarte med å stenge ned nettet umiddelbart. Ansatte mistet tilgang på internett over en lang periode, men organisasjonen tror likevel at handlingen reduserte skadeomfanget av angrepet (Frigård, 2022). I etterkant har både Datatilsynet og IT-sikkerhetsfirmaet Mnemonic avlagt konklusjoner om arbeidet. Førstnevnte viste i sin saksavslutnings-melding at fylkeskommunen oppdaget hendelsen tidlig nok til at man kunne sette inn skadebegrensende tiltak (Datatilsynet, 2022). IT-sikkerhetsfirmaet Mnemonic, som ble leid om som konsulterende part underveis i angrepet, konkluderer med lignende formuleringer i sin rapport. Deres konklusjon sier fylkeskommunens reaksjon, med nedstengingen, var «avgjørende for at angrepet ikke fikk større konsekvenser» (Mnemonic, 2022).

Med dette som utgangspunkt, er det interessant å se videre på hva som gjorde at denne tilnærmingen, samt reaksjonen, fra fylkeskommunen var av så avgjørende art, og hvilke forhold innad i organisasjon og ledelse som muliggjorde et rask fattet beslutning fra fylkeskommunen som i ettertid viste seg å være utslagsgivende i å begrense skadeomfanget av dataangrepet.

1.5 Studiens oppbygging

Videre vil tidligere forskning og det teoretiske rammeverket bli beskrevet. Metodekapittelet forklarer hvorfor en casestudie ble gjort for å svare på problemstillingen, og viser til utvalget og prosessen til det. Deretter vil funnene bli presentert, samt en diskusjon opp mot rammeverket som er utviklet. Studien konkluderer med at tillit er en essensiell del av prosessen for å kunne både forstå og handle i en krise man ikke har oversikt over selv, og videre hvordan både kommunikasjonen og transparensen innad i kriseledelsen påvirket hvordan organisasjonen handlet videre når de skulle kommunisere ut til omverdenen.

2 Teori og begreper

For å kunne utrede hva som gjør at man forstår en ukjent situasjon, vil sensemaking være en teoretisk innfallsvinkel som vil kunne kaste lys på disse spørsmålene. Samtidig krever problemstillingen og forskningsspørsmålene å knytte andre konsepter inn mot sensemaking. Denne studien presenterer derfor et teoretisk rammeverk, bestående av sensemaking som det teoretiske utgangspunktet, men inkluderer andre tematiske konsepter hentet fra relevant litteratur, herunder meaning-making, framing, transparens og tillit. Disse konseptene er relevante i samhandling med problemstillingen fordi de tillater studiet å ta i betraktning forståelsen av mellom-menneskelige relasjoner og betydningen av kommunikasjon og åpenhet i en ledelses beslutningsprosess.

Videre vil disse teoriene og konseptene diskusjon i litteraturen fremheves, og hvilken relevans det har for denne studien. Til sist i kapittelet vil en illustrasjon av det teoretiske rammeverket bli presentert gjennom en modell som viser hvordan tillit er nødvendig for sensemaking-prosessen, og hvordan framing og transparens er tilhørende til sensemaking-prosessen og danner grunnlag for meaning-making.

2.1 Sensemaking

Studien tar utgangspunkt i sensemaking-prosessen rundt kriser og kriseledelsens valg av respons og kommunikasjon. Krise-begrepet er diskutert i mange sammenhenger. Denne studien vil ta utgangspunkt i definisjonen av krise som en hendelse som har potensial til å skade viktige verdier og truer viktige verdier og svekke muligheten for organisasjoner til å utføre viktige funksjoner (NOU 2000: 24, 2000). Det er også viktig å trekke frem behovet for kritisk beslutningstaking, som Engen et al. (2016) trekker frem. I et sensmaking-perspektiv, der sensemaking bunner i å forstå hva som skjer – når det skjer, benytter Weick (1988) karakteriseringen av krise som en konsekvens med lav eller høy sannsynlighet til å true en organisasjons målsettinger. Studien vil ta utgangspunkt i denne definisjonen, hvor Weick (1995) videre beskriver konseptet som å konstruere en mening av hva som skjer. Han beskriver det som en prosess for hvordan, hvorfor og med hvilke verktøy man kan lage mening, og samhandle for å oppnå en felles forståelse som kan rasjonalisere handlinger som blir gjort. Gjennom konseptet blir situasjoner kommunisert til å faktisk eksistere, og sensemaking er derfor et spørsmål om kommunikasjon og språk (Weick et al., 2005). Med det menes at kommunikasjon spiller en vesentlig rolle i sensemaking-prosessen. Brown et al. (2015) forklarer sensemaking skjer når man prøver å forstå hendelser som er uoversiktlige og

forvirrende, og tilskriver betydninger for å kunne forklare hva som foregår. I denne prosessen oppstår intersubjektive forståelser av situasjonen, som gir grunnlag for beslutningstaking (Lakshmi et al., 2021). Maitlis og Sonenshein (2010) tar Weicks konseptualisering videre inn i krisesammenheng, som gir flere interessante syn på konseptet. Det ene er at en blind positivisme og offentlig evaluering rundt en krisesituasjon vil føre til at det kan utfolde seg til det verre. Forfatterne viser til forskning som tilsier at man bør ha en pessimistisk tilnærming til krisen for å sikre at relevante parter ikke misforstår situasjonen. I etterkant av en krise, derimot, vil en positiv sensemaking være med på å kunne sikre adekvat gjenopprettelse av systemet eller organisasjonen. Pursianen (2018) poengterer Weicks opprinnelige tanker rundt sensemaking ved å fremheve at en krise som oppstår vil kreve handling, og at dette kan føre til at handlingen i seg selv kan være med på å forverre krisen. Boin et al. (2021) argumenterer videre for at en krise håndteres mest effektivt når den blir oppdaget, tolket, forstått og så håndtert på proporsjonalt vis i henhold til kriseforløpet. Viktigheten av å ikke håndtere krisen på proporsjonalt vis, kan føre til både underreaksjon, ved at de riktige menneskene ikke legger merke til risiko, trusler og verdier som står på spill. Dermed vil ikke responsen til en krise være adekvat, og man kan oppleve «for lite – for sent»-tiltak. Dette kan også ses på i motsatt tilfelle, hvor ledere kan agere i stor skala på små trusler, som kan oppfattes som en overreaksjon. Videre sier forfatterne at sensemaking er kritisk gjennom hele krisen, da det gir beslutningstakere en rettesnor på hva de bør følge med på av utvikling i krisen, samt hvilke handlinger som bør utføres. Og som nevnt over, kan handlinger i seg selv kan være med på å utvikle krisen. Cornelissen et al. (2014) benytter sensemaking-teori i sin studie i å finne ut hva som gjør at individer i fellesskap kan improvisere, tenke bredt og være åpen for nye tanker mens situasjonen utfolder seg, i stedet for å holde seg til en, enkelt forståelse. Funnene deres tilsier at kommunikasjonen og språket som blir brukt er avgjørende for hvordan kollektivet agerer i situasjonen.

2.2 Tilknyttede konsepter

Under vil analysen ta utgangspunkt i de tilknyttede konseptene tillit, framing, transparens og meaning-making. Deretter vil disse konseptene bli sammenfattet i et teoretisk rammeverk for videre analyse.

2.2.1 Tillit

Det er også et element av tillit i sensemaking-prosessen. Tillit, som i denne sammenheng kan defineres som troen på at ingen part i en sak vil ta utnytte av hverandres sårbarhet, blir

akkumulert og bygget trinnvis gjennom prosesser (Adobor, 2005). En organisasjon med tillit mellom ledelse og ansatte sørger for en effektiv organisasjon, og kan legge til rette for et godt samarbeid som leder til gode prosesser for å ta avgjørelser (Fragouli, 2019). Adobor (2005) argumenterer for at de umiddelbare forventningene man har til en motpart i en felles situasjon, er en viktig del av det å skape og bygge tillit. Dermed kan man se på tillit i form av sensemaking, da sistnevnte baserer seg på hvordan man umiddelbart forstår en ukjent situasjon, og hvor aktører har lite informasjon å gå på isolert sett, vil forventningene til hverandre være med på å forme forståelsen av hva som skjer. Tillit er ikke bare med på å skape en kommunikasjon og interaksjon mellom medlemmer av en organisasjon, men også være medvirkende til at organisasjonen når sitt mål. Med den forståelsen i grunn, legger Yu et al. (2022) opp til at tillit er en avgjørende forutsetning for sensemaking-prosessen. Forfatterne gjorde undersøkelser på virtuelle team som måtte nå raske avgjørelser for sin organisasjon under de stadige skiftende forhold av pandemien, og fant at individer som greide å skape tillit fort nok til sine kolleger, var med på å skape gode sensemaking-prosesser. Når man da skal ta avgjørelser som baserer seg på å ta en sjanse basert på andre sine forståelse av situasjonen, iverksettes utøvelsen av opparbeidet tillit (Jagd & Fuglsang, 2016). Spreitzer og Mishra (1999) påpeker at en leder tar risiko for å miste kontrollen ved å inkludere ansatte i avgjørelses-prosessen, men at ansatte som har spesialkompetanse kan sørge for å ta avgjørelser som er bedre for situasjonen som har oppstått. Forfatterne argumenterer imidlertid for at en leder som klarer å inkludere ansatte, vil heve organisasjonens prestasjon.

2.2.2 Framing

Framing i sensemaking er å velge ut og fremheve noen elementer fra hendelser eller temaer, og knytte dem sammen for å fremstille en spesifikk tolkning, evaluering eller løsning (Entmann, 2004). Framing, som kan beskrives som innramming av situasjonen, tilbyr derfor en forståelse og mening på det som kan oppfattes som en fryktinngytende og forvirrende hendelse, og er en viktig prosess for myndigheter som opplever kriser (Olmeda, 2008). Resodihardjo (2020) forteller at viktigheten av framing i krisesituasjoner er for at man skal kunne definere hvem som er ansvarlig for krisen, skaden som er skjedd og om hendelsen var en enkelthendelse eller om det var en del av et større problem. Derfor anses framing som essensielt, og de som er involvert i hendelsen er ute etter å tilpasse kommunikasjonen slik at det passer deres egne interesser og behov (Pursianen, 2018). Som Cornelissen et al. (2014) beskriver det, brukes ikke ordvalg nødvendigvis for å beskrive og gi mening til et tema, men heller å skape en større bakgrunnsforståelse, som kan gi en veiledning til tolkning og

handlinger. Når individer gjennomfører denne prosessen i fellesskap, som i en kriseledelse, dannes et felles grunnlag for forståelse, og hva som er forventet av hver av dem (Cornelissen et al., 2014). Når det angår språk i sensemaking-prosessen, har også Whittle et al. (2023) gjort omfattende arbeid på å danne et teoretisk grunnlag for nettopp dette. Forfatterne argumenterer for at språk og kommunikasjon er med på å «ramme inn» forståelsen for enkeltindivider i en gitt situasjon.

Knight og Nurse (2020) argumenterer for at det finnes ulike tilnærminger til hvordan legge frem situasjonen for berørte parter og publikum i et sensemaking-perspektiv – for å gi en ramme for forståelse av hva som skjer. Happa og Fairclough (2016) mener at konsekvensen av å ikke ha samme utgangspunkt eller referansepunkt rundt hendelsen medfører hver enkelt aktør i en organisasjon får sin egen oppfatning av nødvendig løsninger til dataangrepet. De argumenterer for at mangelen på kunnskap som behøves for å oppnå en slik felles tilnærming, som igjen vil føre til nødvendige tiltak, oppstår for at organisasjoner ikke benytter seg av ressurser som har den nødvendige kunnskapen om temaet. For å nå en avgjørelse på hvordan håndtere dataangrep, og nå en felles tilnærming, har forfatterne fremstilt en modell ut fra tre antagelser. Først må man se på dataangrep holistisk, og ikke kun av teknisk art. Videre må man involvere et bredt spekter av medlemmer i organisasjonen, for å kunne effektivt kommunisere seg frem til en felles beslutning. Som siste punkt må man etablere en felles forståelse av situasjonen, ettersom et angrep har konsekvenser for ulike ledd i organisasjonen, og ikke kun det tekniske.

Ut fra disse punktene ønsker forfatterne å skissere en modell som gjør at de som er rammet av dataangrep kan oppnå en felles forståelse, når det kan være politikere og byråkrater involvert, utover tekniske fagfelt. Fra en felles forståelse, på tvers av fagfelt og interesser, kan man utøve den mest passende og treffende beslutningen for å håndtere et dataangrep.

2.2.3 Transparens

Transparens, eller åpenhet, kan defineres som den opplevde kvaliteten på informasjonen som er bevisst delt fra en avsender, og er essensielt for organisasjoners tillit (Schnackenberg & Tomlinson, 2016). Aoyama et al. (2020) tydeliggjør hvordan krisekommunikasjon under cyber-hendelser burde samkjøres med hvordan man responderer på krisen gjennom valgt krisehåndtering. Gjennom sin case-studie av Norsk Hydro trekker de frem åpenhet som en viktig faktor i kommunikasjonen, og hvordan det både skaper og bearbeider tillit mellom organisasjonen og berørte parter. Forfatterne argumenterer for at bedrifter og organisasjoner

bør være mer tilbøyelig til å dele informasjon – også via sosiale medier – da dette skaper en jevnlig interaksjon med medlemmer av organisasjonen og øvrig publikum, i tillegg til å motvirke tidligere tendenser som innebar å holde informasjonen internt, eller interessenter med tette relasjoner til organisasjonen. Aoyama et al. (2020) mener agile organisasjoner deler informasjon mellom ulike nivå og ansvarsområder, og at en slik strategi øker situasjonsforståelsen og effektiviteten i videre krisehåndtering.

I kriserespons-rammeverket utviklet av Knight og Nurse (2020) argumenteres det for at det er viktig å informere publikum så fort som mulig, da det blant annet vil forsterke tilliten til kriseledelsen, samt adressere bekymringene til de som er påvirket. Rammeverket viser også til hvordan man bør adressere relevante aktører, både gjennom direkte kommunikasjon som e-post, nettside og SMS/telefon – samt mer indirekte metoder som sosiale og tradisjonelle medier. Disse formene for kommunikasjon er effektivt da det er henholdsvis mer personlig og direkte mot aktørene, og gir mulighet til å kunne agere raskere hvis feilinformasjon skulle bli spredd. I tillegg kan man se på Egloff (2020) sitt argument om å gå ut offentlig med informasjon som et ledd i å finne gjerningsaktør for cyberangrep, som et virkemiddel til å avskrekke andre land eller aktører til å gjennomføre angrep. Kuipers og Schonheit (2022) argumenterer også for at proaktiv transparens i kommunikasjonen rundt hendelsen er essensielt for å redusere omdømmetap etter et datainnbrudd.

Transparens er dog en tilspisset situasjon når det angår dataangrep. Som Kaschner (2022) argumenterer, er kommunikasjon en av tommelfingerreglene når det kommer til kriserespons. Både fordi det avgjør hvem som snakker med hvem, og gjennom hvilke kanaler kommunikasjonen går. Forfatteren poengterer at åpenhet rundt hendelsen er et viktig premiss for noen aktører, eksempelvis media og reguleringsmyndigheter, mens det for andre aktører som organisasjoners lovavdelinger og sikkerhetspersonell er premisset basert på å være mer tilbakeholden hvor det gjelder deling av informasjon. Samtidig som myndigheter ønsker å bli mer tilgjengelig via moderne teknologi, blir man da mer eksponert, og Macmanus et al. (2013) forteller at lokale myndigheter med tilgang på sensitiv informasjon havner i en spagat for å prøve å tilfredsstille denne balansen mellom å være åpen og transparent, mot det å beskytte sensitive opplysninger. Samtidig, som Bannister og Connolly (2011) argumenterer for, så kan for mye åpenhet føre til for mye informasjon og forvirring, som igjen kan føre til stor usikkerhet blant befolkningen.

2.2.4 Meaning-making

Når samfunn møter på krisetilstander er kommunikasjon særdeles viktig, noe meaning-making kan gi en teoretisk innfallsvinkel på. Organisasjonens medlemmer, tilknyttede partnere og innbyggere for øvrig er interessert i å vite hva som skjer, og hva som gjøres av beskyttende tiltak og hva de selv kan gjøre for å beskytte seg selv. Meaning-making handler dermed om kommunikasjonen rundt hendelsen, og hvordan myndighetene kan ramme inn forståelsen av situasjonen i kommunikasjonen til interessenter og andre i offentligheten. Boin et al. (2021) forklarer meaning-making-prosessen som styresmakters måte å ramme inn en fortelling om hva som foregår, i et forsøk på å påvirke berørte parter sin forståelse av situasjonen som truer dem. Forfatterne deler funksjonen av meaning-making inn i tre deler. Den første, instrumentelle funksjonen er å få støtte til tiltak gjennom å gi et narrativ som gjør at folk forstår tiltakene. Videre viser de til en styrkende funksjon, som går på å hjelpe folk å gjøre informerte valg i krisesituasjonen. Det er også en politisk funksjon, som går på å underbygge legitimitet ved å fremme eller utfordre befolkningens tillit til myndigheter, samt deres tillit til institusjoner, systemer og prosesser.

Berg og Kuipers (2022) argumenterer for at det er særdeles vanskelig å kommunisere ut og få folk til å forstå hva som foregår, når trusselen er usynlig og kilden til angrepet er uklart. Der andre kriser kan være synlig, og man kan forstå alvorlighetsgraden ved å se hva krisen går ut på fysisk, er ikke det samme tilfellet under dataangrep, og man kan være usikker på hva konsekvensen er. Som et ledd i dette, kan kriseledelsen ende opp med å simplifisere hendelsen med en metaforisk sammenligning fra fysiske hendelser. Dette kan være risikabelt, da litteraturen viser at det kan medføre en misvisende beskrivelse av hva som faktisk foregår, og vil kunne være med på å gjøre vondt verre. Å få en debatt rundt cyber-trusler vil kunne gi et vokabular og en forståelse for dataangrep som ledere kan benytte som vil øke sjansen for at publikum og andre interessenter blir beroliget og forstår tiltakene som settes i verk. Helsloot og Groenendaal (2017) viser til i sin studie, at meaning-making er det viktigste redskapet for hvordan man oppfattes som leder i kriser. Forfatterne argumenterer for at ledere som evner å utføre meaning-making mens krisen utfolder seg, blir ansett som gode, kompetente ledere – til tross for at ingen avgjørelser eller handlinger nødvendigvis har blitt utført i kriseresponsen.

Når det angår kommunikasjon med berørte parter etter dataangrep, viser Bentley et al. (2018) til kvantitative undersøkelser som studerer beklagelsens innhold. Angående cyberangrep er det tendenser til at man ikke tar på seg skyld selv, men heller retter det mot den eksterne

aktøren som har foretatt angrepet. Forfatterne sier videre at den empatiske tilnærmingen til de som er rammet uteblir i større grad når det angår dataangrep, noe de argumenterer for ville vært formålstjenlig – også i måten de formulerer sine henvendelser og beklagelser, for å vise respekt ovenfor berørte parter og styrke relasjoner med kunder og interessenter.

Kuipers og Schonheit (2022) følger opp Bentley et al. (2018) sin forskning, og argumenterer for at kommunikasjonen i kriser påvirker omdømmet. Her viser de til hvordan man kan instruere informasjonen for å beskytte de som er berørt av hendelsen, og justere kommunikasjonen slik at man informerer publikum om hva organisasjonen gjør for å forhindre videre hendelser, som for eksempel angrep – og gi støtte og sympati til berørte parter. De argumenterer for at å erkjenne skyld og komme med beklagelser og kompensasjonsordninger, gir en mye mer positiv effekt på omdømmet etter datainnbrudd, heller enn å fornekte eget ansvar og skylde på eksterne faktorer. Dette viser også Sapriel (2021) til, som i sin analyse etter dataangrepet på hotellkjeden «Marriott» påstår at mangelen på transparens, eller åpenhet, og empati mot interessenter som var berørt av angrepet, gjorde interessentene mer frustrert og skapte en mangel på tillit. Her vises det til analysen av responsen til angrepet mot Norsk Hydro, der organisasjonen umiddelbart satte i gang med kommunikasjon rettet mot ansatte og media gjennom pressekonferanser, samt aktiv kontakt med viktige interessenter.

Dette resonnerer også med Diers-Lawson et al. (2021) sine funn, som tilsier at reaktiv respons på kriser i datainnbrudd har nær ingen effekt på forholdet mellom ansatte og organisasjonens ledelse, og at en proaktiv relasjonsbygging med relevante aktører og andre parter vil gi krisekommunikasjonen større effekt. Angående skyldspørsmålet, altså grad av skyld organisasjonen har for datainnbruddet, finner forfatterne at grad av skyld påvirker kommunikasjonen. Studien tilsier at organisasjoner som tilbyr informasjonsrik kommunikasjon, som inneholder organisasjonens kompetanse, identitet, samarbeid og omsorg, har effekt i kommunikasjonen med interessenter. Dette kan relateres til Helsloot og Groenendaal (2017) sine funn som nevnt over, som tilsier at strategier for kommunikasjon under krisen er viktigere enn lederens kommunikasjonsevner ellers. Forfatterne påstår at å utføre strategier kan gjøre at ledere som normalt ikke har gode kommunikasjonsferdigheter, vil kunne bli oppfattet som gode ledere i en umiddelbar krise.

2.3 Teoretisk rammeverk for studien

For å oppsummere, er de nevnte teoriene en inngangsport til å kunne forstå og diskutere hvordan kriseledelsen klarte å oppfatte angrepet, og hvordan man valgte å handle når det angår å kommunisere mellom ledelsen og andre relevante aktører. I dette tilfellet, har kriseledelsen i organisasjonen ulik bakgrunn, og hvert enkelt medlem har ikke nødvendigvis IKT- eller sikkerhets-bakgrunn. Dermed må man se på sensemaking i kollektiv, samarbeidende forstand, som er når folk med ulik bakgrunn må gjøre seg en forståelse av kompliserte, informasjonsrike hendelser, og komme frem til en felles handling for å møte situasjonen (Umapathy, 2010). Lakshmi et al. (2021) argumenterer for at kommunikasjonen mellom individene, sammenfaller med organisasjonen og teknologien, er hva som gjør sensemaking mulig – som igjen er med på å gi en adekvat respons på dataangrep og cyber-hendelser.

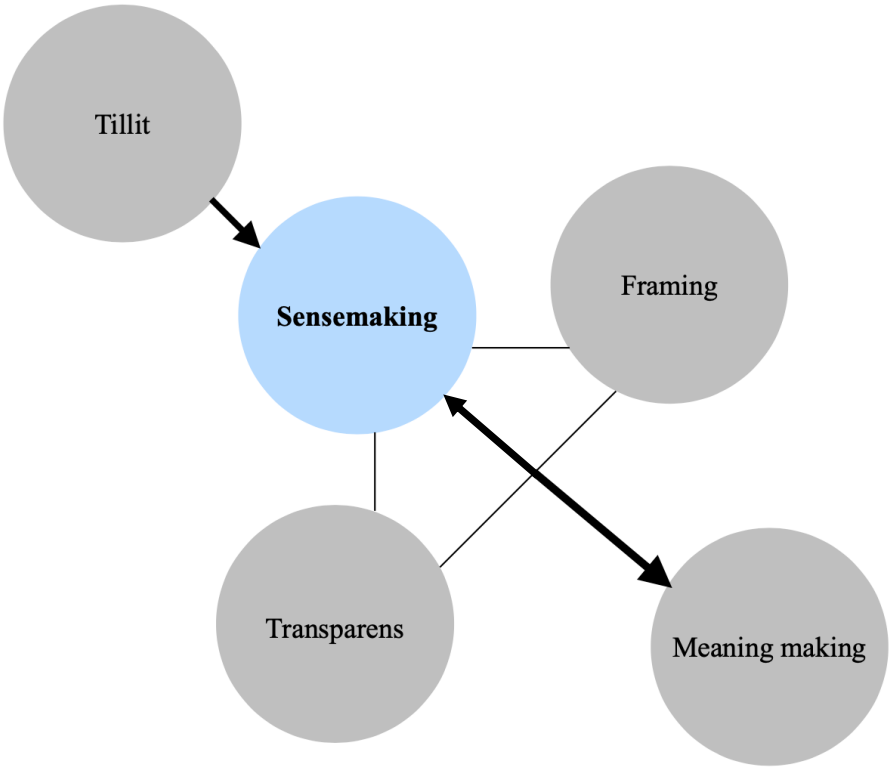
Litteraturen viser til at sensemaking under dataangrep har en spesifikk utfordring når det angår kompetanse for å forstå situasjonen når den utfolder seg. Som Happa og Fairclough (2016) nevner, vil ledelsens ulike utgangspunkt føre til en ulik forståelse og ulike tilnærming til løsning på problemet. Ved å ikke benytte seg av ressurser som har nødvendig kompetanse, vil det oppstå en slik dynamikk i kriseresponsen som igjen vil gjøre at nødvendige tiltak ikke blir iverksatt. Her spiller også tillit inn som et element verdt å undersøke i relasjon med hvordan det påvirker ledelsens prosess til å forstå hva som foregår og hvordan det påvirker beslutningene som tas deretter.

Når det gjelder kommunikasjon ut til interessenter i ettertid av et angrep, viser litteraturen til eksempler på hvordan angrepsrammede organisasjoner håndterer skyld og beklagelse i ettertid av et angrep. Empirisk tenderer organisasjoner til å legge skylden på den eksterne aktøren som utfører angrepet, mens litteraturen i stor grad er samstemte på at det er formålstjenlig for en organisasjon overfor interessenter og omdømme å ta skyld, utsende beklagelse overfor interessenter, samt vise empati og forståelse for den vanskelige situasjonen. Det er også interessant å legge til Diers-Lawson et al. (2021) sine funn, som påpeker at en proaktiv holdning til en god relasjon med interessenter vil gi en større effekt i krisekommunikasjonen, og at kommunikasjonen bør inneholde organisasjonens kompetanse og omsorg, samt identitet.

Transparens er relevant, da litteraturen viser til dette som et virkemiddel for å skape tillit til organisasjonens håndtering av krisen, og samtidig ha en avskrekkende effekt på potensielle aktører som kan være truende til å utføre samme type angrep. Et interessant perspektiv når det

gjelder dataangrep, er Kaschner (2022) sin argumentasjon om at det kan være grunner for å holde tilbake informasjon, grunnet lov- og sikkerhetsmessige hensyn. Dette gjør informasjonsdeling til en krevende øvelse.

Dette skaper et teoretisk rammeverk, som denne studien argumenterer for er en modell som kan svare på hvordan organisasjoner kan forstå hva som skjer under et dataangrep, til å både kunne ta en hurtig avgjørelse og kommunisere videre hva som foregår. Dette rammeverket baserer seg på at tillit innad i ledelsen er nødvendig for at sensemaking-prosessen raskt kan finne sted. Med dette i bunn, danner det grunnlag for hvordan situasjonen blir lagt frem og forstått innad i ledelsen, gjennom framing-prosessen, som danner grunnlag for hva som skal kommuniseres videre. Åpenhet er også et element, som kan praktiseres innad i ledelsen for å opparbeide en større forståelse – som igjen danner grunnlaget videre for meaning-making. Sistnevnte vil, med disse elementene i grunn, kunne skape et grunnlag for forståelse og valg for videre kommunikasjon ut til interessenter. Figur 3-1 illustrerer dette teoretiske rammeverket.



Figur 2-1: Teoretisk rammeverk for sensemaking-prosessen under dataangrep

3 Metode

For å kunne forstå bakgrunnen og de underliggende faktorene for at ledelsen i Nordland Fylkeskommune handlet slik de gjorde, som igjen danner grunnlag for teoriutviklingen, ble kvalitativ casestudie benyttet for å svare på problemstillingen og forskningsspørsmålene i denne studien. Denne tilnærmingen gjør det mulig å få innsikt i menneskelig atferd, og tankene bak avgjørelsene. Det vil og gi en mulighet for å kunne induktivt finne frem til gjennomgående temaer som kan gi grunnlag for teoriutforming og elementer som kan være gjenstand for videre forskning.

3.1 Forskningstilnærming: Kvalitativt casestudie

Utgangspunktet med studien er å få utarbeidet en helhetlig fremstilling av en situasjon, og skildre flere sider av situasjonen som oppstår hos flere aktører. Derfor vil en kvalitativ tilnærming være mest hensiktsmessig. Dette vil også gi en mer fleksibel tilnærming til forskningen, ettersom opplegget kan endres underveis. Dette samsvarer også med ideen om å bevege seg i dybden, og få fremmet et helhetlig perspektiv på en spesifikk, avgrenset situasjon, som Balsvik (2011) forklarer. En casestudie gir anledning til å gå grundig gjennom hendelser eller situasjoner for å undersøke fenomener som ellers ikke ville kunne bli oppdaget (Johannessen et al., 2021). Videre falt valget på enkeltcase-studie, som er hensiktsmessig når det er et kritisk tilfelle som skal undersøkes, og tilfellet kan bidra til å forstå viktige hendelser. Johannessen et al. (2021) forklarer at dette vil gi mulighet til å undersøke et fenomen fra flere sider, og gi en fyldigere beskrivelse. Denne metoden gjør det også mulig å ta en induktiv tilnærming til forskningen, som innebærer å kunne formulere teorier og hypoteser ut fra observasjonene gjort i forskningen. Dette kan være til nytte for å utvide forskningsfeltet på et relativt nytt tema som krisehåndtering under dataangrep, både for offentlige og private organisasjoner.

En kritikk mot dette valget av metodikk, er som Johannessen et al. (2021) forklarer, at man med flere caser kan se etter mønstre og fellestrekk på tvers av bransjer, relevant opp mot problemstillingen. En slik tilnærming vil være nyttig for å kunne gi teoriutformingen en sterkere forankring. Til gjengjeld vil det være særdeles tidkrevende, og for denne forskningen vil Balsvik (2011) sitt argument om å kunne gå ned i dybden på en spesifikk situasjon være mest formålstjenlig, for å deretter kunne bygge hypoteser som kan benyttes til videre forskning.

For denne studien ble det utført intervju til en casestudie. Videre vil studien først forklare utvalgsstrategi og intervjuprosess, før en nærmere beskrivelse av dataanalyseelementene.

3.1.1 Utvalg

Å intervjue relevante aktører innenfor forskningsfeltet er en god måte å tilegne seg informasjon om deres holdninger, opplevelser, følelser og meninger. Siden studien er ute etter å forstå hvorfor ledelsesfigurer oppfattet situasjonen, samt hvorfor de valgte å reagere slik de gjorde, vil man gjennom intervju kunne få frem en analyse av menneskers opplevelse av bestemte situasjoner (Brinkmann & Tanggaard, 2019; Johannessen et al., 2021). Her tas det utgangspunkt i det Brinkmann og Tanggaard (2019) referer til som en grunnregel, nemlig å intervjue relativt få individer for så å gå grundig inn i analysen av disse. Dette resonnerer også med Balsvik (2011), som sier kvalitative intervjuer baserer seg gjerne på strategiske ikke-tilfeldige utvalg, siden de som skal være en del av undersøkelsen tilhøre og representere en gruppe. Også Johannessen et al. (2021) poengterer at den gylne regelen er å intervjue nok mennesker til det ikke er noe mer informasjon å få. Sistnevnte sier også at mindre prosjekter har et utvalg på ti til femten intervjuer, men også færre eller flere, alt etter hva forskningen krever. I dette tilfellet vil det være relevant å snakke med ledelsesaktører i den gjeldende organisasjonen som skal undersøkes. Derfor ble utvalget bestående av åtte medlemmer av kriseledelsen.

I november 2022 ble Nordland fylkeskommune kontaktet for å starte prosessen med intervjuobjekter som kunne være relevante til studiens problemstilling[2]. Strategien for utvalget kan ses på som en blanding av det Johannessen et al. (2021) kaller kriteriebestemt utvalg, der informanter må inneha bestemte kriterier for å kunne delta på studien. I dette tilfellet ledelsen, og snøballmetoden, ettersom informanter ble rekruttert ved å kontakte personer som vet mye om temaet som skal undersøkes. I diskusjoner med denne kontaktpersonen i organisasjonen, ble det besluttet at de mest relevante innenfor ledelsessegmentet da krisen inntraff, var de som satt i *sentral kriseledelse* (SKL). Dette innbefatter flere aktører og roller, som politisk ledelse, direktører og rådgivere. Dette består dermed av øverste sjefer innenfor hver av organisasjonens avdelinger, samt politisk ledelse og endelig beslutningstaker. For å sikre et mest mulig representativt bilde av hvordan ledelsen

[2] Se forespørsel til Nordland fylkeskommune og samtykkeerklæring for hvert enkelt intervjuobjekt i hhv. vedlegg 8.3 og 8.4.

dermed håndterte sin kommunikasjonsprosess når krisen inntraff, endte studien opp med å intervjue informantene, også kalt respondentene, vist i tabell 1.

Tabell 1: Respondenter i studien

Hvem	**Rolle i sentral kriseledelse (SKL)**
Politisk leder	Endelig beslutningstaker
Politisk nestleder	Politisk ansvarlig for avdeling finans og organisasjon og kommunikasjon.
Direktør 1	Ansvarlig for finans og organisasjon, herunder også kommunikasjon.
Direktør 2	Ansvarlig for den avdelingen med flest ansatte og andre interessenter.
IKT-sjef	Ansvarlig for IKT. Underlagt avdelingen til *Direktør 1.*
Sikkerhetssjef	Sikkerhetsansvarlig for organisasjonen. Underlagt avdelingen til *Direktør 1.*
Kommunikasjonsansvarlig	Ansvarlig for kommunikasjon i organisasjonen, både internt og eksternt. Underlagt avdelingen til *Direktør 1.*
Rådgiver	Sikkerhetsrådgiver, som eneste ansatt hos sikkerhetssjefen.

3.1.2 Intervju

Grunnet geografisk avstand til intervjuobjektene, også kalt respondentene, ble Teams foretrukket kanal. På det viset kunne man stadig oppfatte kroppsspråket til hverandre, da kroppsspråk er med på å definere intervjusituasjonen og gjøre at både intervjuer og respondent kan bli tatt på alvor ved at man har øyekontakt (Kvale & Brinkmann, 2017). Ved gjennomføring ble det informert om bruk av lydopptaker, som ble benyttet til å ta opp lyd og senere transkribere intervjuene. På forhånd ble det gjort klart for meg at medlemmer av kriseledelsen ivaretok viktige oppgaver i arbeidssammenheng som var tidkrevende, og det ble derfor begrenset til times-lange intervju. Johannessen et al. (2021) argumenterer for at intervjuer over tjenester som Teams kan gi tilnærmet like god informasjon som fysiske intervjuer, og ble derfor gjennomført, til tross utfordringen at det kan være vanskelig å oppnå nødvendig tillit mellom intervjuer og intervjuobjekt, når man kun har en skjerm mellom seg. For dette prosjektet ble det kompensert for ved å ha e-post-kontakt i forveien, med god informasjon om hva studien omhandlet og hva studien var ute etter. I forkant av intervju ble informantene igjen informert om studiens formål, at man ikke er ute etter taushetsbelagt

informasjon, at lyd vil bli tatt opp og at de har mulighet til å trekke seg underveis. Med denne tilnærmingen, var opplevelsen at respondentene svarte etter beste evne og opplevde selv en komfortabel og tillitsfull relasjon.

Det ble benyttet semistrukturerte intervju, eller halvstrukturert intervju, som intervjuform, med begrunnelsen at informantene skal forklare sine egne erfaringer og oppfatninger, og derfor trenger større frihet. Dette gjør og at intervjueren kan stille nødvendige oppfølgingsspørsmål skulle det være nødvendig, og gjør at man kan stille oppfølgingsspørsmål som ikke er planlagt på forhånd (Brottveit & Del Busso, 2018; Johannessen et al., 2021). Det ble utarbeidet en intervjuguide, som fungerer som et veiledende hjelpemiddel for hvilke tema og spørsmål som er relevant å spørre om i intervjuet (se vedlegg 9.1). Spørsmålene ble delt opp i tematiske hovedpunkter, med fokus på intervjuobjektets forståelse og opplevelse av hva som skjedde (Brottveit & Del Busso, 2018).

En utfordring var at medlemmer av kriseledelsen har forskjellige oppgaver og ansvar i arbeidsforholdet. Eksempelvis, der noen jobbet spesifikt med sikkerhet, var andre i kriseledelsen kommunikasjonsarbeidere. Her kom det semistrukturerte intervjuformen til nytte, da den tillot å stille spørsmål som skulle dukke opp som var mer relevant for de ulike intervjuobjektene. En utfordring med dette, er at ikke alle spørsmålene man stiller får like stor relevans hos den enkelte, da de ikke nødvendigvis var tett på i de ulike fasene av krisen. For å møte denne utfordringen ble det forsøkt å stille åpne spørsmål, som var relevant for problemstillingen og spørsmålene, som omhandlet deres opplevelse av håndteringen og kommunikasjonen – og ikke organisasjonens fokus og ønskede oppnåelse. Det ble også stilt mer konkrete spørsmål for å se om respondentene faktisk oppfattet situasjonen likt og hadde samme forståelse for hva som foregikk.

Ved bruk av intervjuform, er det nødvendig å få godkjenning til å samle inn data. Søknad til Sikt, tidligere Norsk senter for forskningsdata, den 27.12.2022. Vedlagt var det et samtykkeskjema, som inneholdt informasjon om forskningsprosjektet og rettigheter respondentene har, som skulle sendes til hver respondent for signering før intervju. Godkjenning ble mottatt 20.01.2023. Deretter ble hver enkelt respondent kontaktet, som fikk invitasjon til intervju og skjema til signering. Samtlige intervju ble utført i februar måned. Meldeskjema kan leses i vedlegg 9.2.

3.2 Dataanalyse og koding

For å analysere det transkriberte materialet, ble tematisk analyse benyttet. Denne metodikken ville være til nytte for å kunne drøfte rundt på studiens problemstilling, og gjør at studien kan legge informantsvarene til grunn for analysen videre. Dette er ønskelig, da det er kriseledelsens oppfattelser og opplevelser som vil være interessant å analysere. Det er deres betraktninger som sentral for forskningen. Svarene fra de ulike respondentene ble gjenstand for sammenligning for å identifisere og analysere mønstre (Braun & Clarke, 2006; Brottveit & Del Busso, 2018). Braun og Clarke (2006) sine faser i tematisk analyse tar utgangspunkt i å først definere temaer og deres størrelse. Videre vil det for denne studien være lønnsomt å se på ulike temaer ved hele datamaterialet, fremfor kun ett enkelt tema, for å kunne forstå en helhet av datamaterialet, fremfor kun ett dybdefokus. Det vil derfor være en induktiv tilnærming til kodingen, ettersom den baseres ut fra datamaterialet (Johannessen et al., 2021).

Braun og Clarke (2006) viser en «steg for steg»-modell for hvordan analyse datamaterialet. For å lettere kunne følge disse stegene, ble de oversatt og plassert i en tabell.

Tabell 2: Steg-for-steg modell (Braun & Clarke, 2006)

Steg 1	Gjøre seg kjent med datamaterialet	Innebærer å transkribere og kjøre seg kjent med datamaterialet. Her noteres observasjoner og tanker om hva som kan være verdt å undersøke nærmere.
Steg 2	Generere koder fra datainnsamlingen.	Finne interessante fellestrekk i hele datasettet som kan relateres til ulike koder.
Steg 3	Identifisere temaer	Samle kodene til temaer, og gruppere temaene videre til ulike mønstre man kan oppdage.
Steg 4	Gjennomgå temaer	Kontrollere om kodene passet til innholdet, eller om man burde frembringe flere tema eller undertema, samt om det passer til datasettet i sin helhet.
Steg 5	Definere og navngi temaene	Analysere og revidere temaene og hva analysen beskriver, og deretter navngi dem til å kunne være forklarende til videre bruk.
Steg 6	Produsere sluttproduktet	Fremstilling av funnene, med passende sitater og forklarende elementer til diskusjon av analysen.

Denne listen ble fulgt relativt slavisk, og tematiseringen fant fort ut hvilke elementer som stakk seg ut, som var relevant for forskningsspørsmålene. Under vil kapittelet «Resultater» vise fremstillingen av funnene, som forklart i steg 6 i tabellen.

3.3 Reliabilitet

Reliabilitet handler om forskningens datainnsamling, og dens troverdighet, konsistens og pålitelighet (Johannessen et al., 2021; Kvale & Brinkmann, 2017). En forskers interesse og egne ønsker om utvikling kan stå sterkt i produksjonen av en studie, og dermed gjør at man kan stille spørsmål rundt forskningens funn. Reliabilitet til forskningen blir derfor viktig, og transparens spiller en nøkkelrolle i dette øyemed. Derfor vil lydopptak gjøre det lett å kontrollere faktiske opplysninger fra informanter, samt om intervjueren har stilt ledende spørsmål, også under transkribering og koding. Studien vil opplyse om underliggende, personlige forhold og vise grunnlaget for hvilke valg som er gjort underveis i studien (Kvale & Brinkmann, 2017; Tjora, 2018).

Denne studien har tatt utgangspunkt i kriseledelsen ved Nordland fylkeskommune, og gjennomført gjennom intervjuer. Den semistrukturerte intervjuformen lar intervjuet være fleksibelt, noe som i denne studien ble vist gjennom at ulike medlemmer av kriseledelsen hadde ulike prioriteringer på hva de snakket mest om. Dette kommer frem gjennom metode- og resultatkapittelet, og intervjuguiden ligger vedlagt for å sikre mest mulig transparens.

3.4 Intern og ekstern validitet

Validitet baserer seg på om en metode er egnet til å finne ut av hva forskningen er ute etter (Kvale & Brinkmann, 2017). I denne anledning skiller vi mellom intern og ekstern validitet, jamfør Johannessen et al. (2021). Denne forskningen tilstreber å ivareta validitet gjennom at problemstillinger, forskningsspørsmål og teoretiske rammeverk svarer til studiens empiriske innhold og konklusjon. Metoden som er valgt er ment å belyse temaet på en adekvat måte. Man kan se kritisk på forskningen presentert her, i den form av at man kunne valgt å intervjue alle medlemmene av kriseledelsen, eller valgt en metode som var mer komparativ. Det er absolutt en interessant innfallsvinkel, men for å utvikle et teoretisk rammeverk anså ikke denne studien det som nødvendig, da det heller kan utforskes gjennom videre forskning.

I henhold til ekstern validitet, så handler det mer om resultatene av studien kan overfører til liknende fenomen, siden all forskning har som mål å trekke slutninger utover de opplysninger som samles inn, altså en generalisering (Johannessen et al., 2021). I dette tilfellet er spørsmålet om resultatet fra denne casestudien kan overføres til en annen offentlig virksomhet. Med kun en enkelt case kan man argumentere for at det er lite generaliserende og vansker for å overføre til en annen offentlig virksomhet. Til gjengjeld har dybden i intervjuene og informasjonen gitt grunnlag for å få en dypere forståelse for hva som lå til

grunn for de valg som ble gjort. Derfor kan man argumentere for at den dybdeforståelsen man får av denne studien gjør at resultatene kan overføres til andre virksomheter. Det vil uansett oppfordres til å teste hypotesene som presenteres senere i teksten.

3.5 Etiske betraktninger

Som et kvalitativt forskningsprosjekt, får man tilgang på menneskers personlige betraktninger, og kan ende opp med å behandle sensitiv informasjon (Busso, 2018). I denne studien har man i intervjuer kunnet oppleve at respondenter har hatt mulighet til å dele taushetsbelagte opplysninger, eller opplysninger som enda var under etterforskning, uten at det nødvendigvis var hensikten. Dette er informasjon som studien ikke etterspør, og som nevnt tidligere i kapittelet, har dette blitt imøtekommet med mulighet for å lese gjennom transkribert intervju. Videre har samtykkeskjema og informasjon om studien blitt delt ut i forkant av intervju, samt at prosjektet er godkjent av Sikt. Man kan argumentere for at det kan være mulig å kjenne igjen hvem respondentene i organisasjonen er. Dette er, som oppgitt i samtykkeskjema og formidlet før intervju, forsøkt anonymisert så langt som mulig.

En annen etisk betraktning verdt å nevne, er at forfatteren av denne studien selv har jobbet i organisasjonen i en kort periode i 2022. Dette var i en separat avdeling fra de som er intervjuet til denne studien, og i en administrativ stilling som ikke underlagt noen av direktørene som er intervjuet. Undertegnede har derfor ikke hatt noen nær arbeidsrelasjon, ei heller noen relasjoner privat, til de som er intervjuet til denne studien.

4 Resultater

Studien baserer seg på teori i faglitteraturen, men også data fra et empirisk tilfelle. I dette kapittelet vil dataene for studien bli fremstilt, analysert og systematisert, før drøftingsdelen vil diskutere funnene i dette prosjektet med tidligere teori, som vil lede frem til konklusjonen (Brottveit & Del Busso, 2018). Under vil det bli delt opp i hovedtemaer som er identifisert gjennom intervjuene og relatert til forskningsspørsmålene. Dette er «forståelse for handling», «mellom-menneskelige relasjoner» og «formidling og kommunikasjon».

Flere sentrale trekk går igjen i intervjuene fra kriseledelsen ved Nordland fylkeskommune, på hvordan de forsto hva som foregikk – og hvordan de tok avgjørelser og baserte kommunikasjonen sin deretter, slik at de oppnådde det resultatet de gjorde.

4.1 Forståelse for handling: Forberedelser og erfaring

Utdanning, kompetanse og planverk – rett og slett forberedelser – var med på å håndtere situasjonen da den oppsto, ifølge respondentene. Sikkerhetsavdelingen[3] hadde, blant annet gjennom Norsk sikkerhetsmyndighet (NSM) sine grunnprinsipper for IKT-sikkerhet, trukket slutningen om at datakriminalitet kunne være noe som rammet deres organisasjon også – og var noe som skulle prioriteres. Derfor ble det halvåret i forveien en økt bevisstgjøring av dette i organisasjonen.

> *«At ting lå relativt langt framme i bevisstheten gjorde nok også at ... at man og handlet raskere enn man kanskje ville gjort hvis man hadde vært helt uforberedt».*

Dette trekkes frem som en faktor som ikke nødvendigvis kunne avverget angrepet, men som var med på å heve forståelsen av hva som foregikk.

> *«Kanskje det kan ha hatt en effekt. At man skjønner at man er forberedt på at sånne ting kan skje. Man leser jo selvfølgelig om sånne typer angrep i media, da hadde det vært noe i forkant, i Avisa Nordland tror jeg, om en sånn type angrep. Så det er en kjennskap til at dette kan skje».*

[3] Nordland fylkeskommune har ikke en offisiell sikkerhetsavdeling, men i denne studien vil benevnelsen «sikkerhetsavdeling» bli benyttet for avdelingen som jobber med sikkerhet og beredskap.

Samtidig var det mangel på planverk på spesifikke situasjoner, samt at ikke alle medlemmene var bevisst på planverk. Dette kommer til uttrykk som både positivt og mer uheldig, og vil derfor få et eget avsnitt i denne avhandlingen.

4.1.1 Utdanning og forberedelser innad i organisasjonen

På spørsmål om hva som gjorde at sentral kriseledelse forsto hva som var på gang, trekker sikkerhetssjefen frem arbeidet som ble gjort fra sikkerhetsavdelingen i forkant.

> *«Jeg opplevde at vi ble tatt på alvor med en gang, og vi fikk en kriseerkjennelse – og jeg tror alle skjønte situasjonen. Det ene skyldes nok sikkert at vi hadde vært på Fylkestinget og varslet om at det var høyt press og mye som skjer. Det andre er nok at vi hadde stått i (annen hendelse), og jobbet med denne typen problemstillinger, og snakket i kriseledelsen om hva som kan skje når denne typen ting kan skje».*

Det at sikkerhetssjefen hadde informert både kriseledelsen, men også resten av organisasjonen i forveien, tror han selv hadde en effekt på hvordan situasjonen ble mottatt. Dette får han medhold i av resten av kriseledelsen. Øverste beslutningstaker forteller at fokuset på cybersikkerhet fra både sikkerhetsavdelingen og IKT-avdelingen, gjorde at de var på tærne, og «noe mer anspent holdning» til sikkerhetsspørsmål enn tidligere. Dette arbeidet, med både Fylkestinget og Fylkesrådet, i forveien, mener en interessent at gjorde fagmiljøet var mer «på» i kriseledelsen, nettopp fordi det var gjort et arbeid på dette i forkant.

> *«I oktober så var sikkerhetssjef på fylkestinget, og orienterte fylkestinget om at nå ser vi stort press på våre systemer og den og den brannmuren, og alt sånn, at da så vi at det er et spørsmål om tid for når det blir et annet angrep. Så det var veldig langt frem fremme i pannen vår at det var mange store trusler der ute, og mye press og sårbarhet, det finnes jo hele tiden innenfor dette feltet, så jeg vil si vi var ganske ... om vi ikke var forberedt i at det forelå planverk, så var vi hvert fall mentalt ganske påkoblet på at dette kunne skje».*

Dette viser da at selv om angrepet ikke nødvendigvis kunne blitt avverget, hadde fokuset og informasjonen i forkant av angrepet muligens en effekt på forståelsen av alvoret da det faktisk skjedde.

4.1.2 Planverk

Angående planverk for kommunikasjon, beredskap og sikkerhet relatert til datainnbrudd, er det delvis ulike erfaringer om hva som fungerte og ikke. For det første var ikke alle klar over beredskapsplanverket, og det ble fremstilt som et generelt planverk.

> *«For det vi ser, er at den overordnete beredskapsplanen, den er generell, og skal like godt håndtere trafikkulykker som cyberangrep, og vi ønsket å få på plass noe enda mer spesifikt (...)Den var ikke ferdigstilt, og er enda ikke ferdigstilt, men brukte rammeverket aktivt, som vi hadde lagt til grunn, og det var tilpasset, gjennom jula, så gjennomgikk det flere ganger i romjula, og så gjennom det om det var ting vi ikke hadde tenkt på, var det ting vi måtte se nærmere på – som en sjekkliste».*

Sikkerhetsavdelingen forteller dermed at de var i gang med en mer spesifikk plan på cybersikkerhet. Selv om den ikke var ferdig utviklet, fungerte den som en sjekkliste i arbeidet, og kan tolkes dithen at et planverk var et godt attributt å støtte seg på, for å raskere kunne håndtere situasjonen. Det blir videre sagt at de skulle ønsket det var en budskapsbank tilgjengelig, for å stille mer forberedt og sikre rask og effektiv kommunikasjon. For kommunikasjonsavdelingen sin del, var det mer en fordel å ha en generell tilnærming, for å sikre fleksibilitet.

> *«For da må du lage en plan for alt fra skoleskyting til digitalt angrep til pandemi til jordskjelv til sjøldrap til busser som kjører utfor, til elever som blir drept. Du ser hvor dette bærer. Så krisekommunikasjonsplanen vår er generell, men med fleksibilitet til å tilpasse til hver enkelt hendelse. Vi har en krisekommunikasjonshandbok, som tilpasser den til hendelsen når det skjer».*

Vel og merke er ikke disse bemerkningene noe som tyder på en uenighet, nødvendigvis, men heller en bemerkning om at det er ulike metoder som kan benyttes – og at ulike fagfelt kan ha ulike preferanser.

4.1.3 Erfaring

Som et eget punkt under forberedelser, kommer egen erfaring også inn i bildet. Flere av interessentene påpeker at deres egne erfaringer, eller den til deres kolleger, spilte en rolle i håndteringen og hvordan situasjonen ble forstått. Eksempelvis, så forklares det at en pressemelding kom ut relativt raskt etter første kriseledelsesmøte, nettopp på grunn av at erfaring fra tidligere roller i mer operative enheter som sikrer at det er kort vei fra plan til

ferdig produkt. For flere av interessentene ble det påpekt at den kompetansen i kriseledelsen, fra medlemmer som tidligere har arbeidet i Forsvaret og Politiet, var med på å heve fokuset på sikkerhet og prioriteringer, som gjorde arbeidet videre mer håndterlig. En annen respondent påpeker at ens egen erfaring på IKT-feltet, gjorde at det var lettere å forstå alvoret i situasjonen.

4.2 Mellom-menneskelige relasjoner: Tillit og samarbeid

Det var tydelig i intervjusetting at medlemmene i sentral kriseledelse hadde godt kjennskap til hverandre, også i pressede situasjoner. Her trekkes både tillit til hverandre, men også til fagkompetansen og andre ledd i organisasjonen, frem. Samarbeidsrutiner var også et element flere av respondentene nevnte som en fordel.

4.2.1 Tillit

Det gjennomgående elementet for forståelse av hendelsen og dets forløp, og videre til handling, var tillit. Som en av de som gjorde innsalget til kriseledelsen, som har kompetanse på IKT, uttalte:

> *«Jeg tipper at kriseledelsen hadde sagt ja til hva som helst hvis vi bare hadde sagt at det vil vi gjøre. Men sånn er det jo fordi vi kan faget».*

Tillit ble nevnt av nærmest samtlige interessenter til hva som gjorde at de forsto alvoret i situasjonen, og handlet deretter. På spørsmål om nettopp dette, svarte blant annet en av respondentene:

> *«Jeg tror egentlig at det har mye med at man har sin tillit til at de personene som informerer oss, at de vet hva de snakker om. Man må jo basere seg på tillit til hverandre sin fagkompetanse (...) Min faglige kunnskap om IT-systemer, den vil aldri kunne bringe meg til noen konklusjoner om noe (...) Jeg tenker at for min del er det at man har tillit til fagkompetansen i ulike deler av organisasjonen. Og legger til grunn at hvis de forteller oss noe om at det har vært et datainnbrudd, så er ikke det trengt at jeg har fagkompetansen selv, eller det de har sett, jeg kan forstå at dette er alvorlig og at vi må gjøre noen tiltak».*

Dette indikerer tillit til fagpersonell og -miljø er en nøkkel hvorfor man handlet slik man gjorde, så raskt, når man ikke har kunnskapen om fagfeltet selv. Videre nevnte flere av intervjuobjektene at samarbeidet mellom kriseledelsen var såpass veletablert og satt, at de

skildret gode samarbeidsrutiner som en grunn for at forståelsen, håndteringen og avgjørelsene ble gjort raskt – som kan oppfattes som en tillit til hverandres kompetanse og forståelse.

> *«Jeg tror mye av skylden er at vi er vant til å sitte i kriseledelse sammen. Gjennompandemien, så har vi sittet i kriseledelse hver uke, stort sett, enten via sentral kriseledelse, eller lokale kriseledelser (...) Så det er nok litt av suksesskriteriene (...) Dette var et nytt møte om nytt tema».*

Mens sikkerhetssjefen hadde fri lille juleaften, kom tekstmeldingen inn som gjorde at han forsto noe var på ferde. Dette var etter at IKT-sjefen hadde samtalt med sitt vakthavende personell, som han selv omtaler som noen av de beste folkene han har i sin stab. Med den tilliten til sine ansatte, samt sin egen erfaring på feltet, gikk det via sikkerhetssjefen inn til samling av sentral kriseledelse samme dag. Dette i seg selv hadde en effekt for forståelsen av alvoret, at man ble innkalt til kriseledelse. Å ha et slikt organ gjorde at man kunne gå inn i møtet med en viss forståelse av alvor.

Deres fremlegg av situasjonen omtales av medlemmer av kriseledelsen som nøktern og alvorlig, nok til å skjønne at det måtte tiltak til, uten at det var overdramatisert.

> «*IKT-guttene vi har, de var veldig ... de tok det alvorlig. Og jeg opplevde de som ganske sånn ... normalt sett at de ikke lager mye støy, de sier ingenting. Men de på en måte ropte høyt, og vi kobler på oss mange ressurser (...) Det var jo på grunn av IKT, da, at de fortalte at dette er ikke bra».*

Tydelighet og alvorspreget gjorde inntrykk på kriseledelsen. Øverste beslutningstaker i kriseledelsen fortalte han sto og lagde grøt på lille julaften, men at den resolutte beskjeden fra sikkerhetssjefen fikk han til å handle. Hadde det vært mindre konkret og direkte, hadde han muligens gått tilbake til grøtlagingen. Han trekker frem nettopp dette som et av de viktigste grepene som ble gjort for at samtlige i sentral kriseledelse forsto alvoret:

> *«Tydelighet, ikke sant (...) Sikkerhetssjef og IKT-sjef, de kunne jo også sett på dette og sagt «nei, faen, det er jul, vi roer han litt» (...) De kunne ha underkommunisert, det gjorde de ikke».*

Denne oppfattelsen er det flere av medlemmene i kriseledelsen som deler. Dette sterke tillitsforholdet til fagmiljøet som avgjørende for å komme frem til konklusjonen om å stenge ned raskt. Men tillit var også noe som måtte gå oppover i kjeden – og være synlig på tvers, for

å få full effekt. Som en respondent forklarer, var både endelig beslutningstaker og visse direktører handlekraftige, tillitsfulle, og utviste tillit til sine ansatte og fagmiljø.

Sistnevnte forteller i sitt intervju at det ikke er noe behov for han å ta noe utdannelse eller lignende på IKT-feltet for å kunne forstå problemstillingen, nettopp fordi han har tillit til at fagmiljøet har kompetansen til å forklare konsekvensene av det tekniske som foregår. Derfor var ikke den tekniske forståelsen noe nødvendighet – det var heller en diskusjon på konsekvensen.

Disse eksemplene var bare noen som beviser hvor stor betydning tillit til fagmiljø og kolleger har for å forstå alvoret i en situasjon, og gir et grunnlag for å handle og kommunisere deretter. En av interessentene nevner at tilliten hadde blitt svekket, om IKT-avdelingen ikke hadde anbefalt tiltak, men likevel visst om faren med å holde internett oppe. Dermed hviler det et ansvar på fagmiljøet, som ikke kan bli tatt for gitt heller.

Denne tillitsbaserte forståelsen kommer også til uttrykk gjennom hvor godt samarbeid det er i organisasjonen, som er neste punkt.

4.2.2 Samarbeidsrutiner

Samarbeid er også en faktor som flere i kriseledelsen trekker frem, som en avgjørende nøkkel til suksess. Dette er samarbeid i og på tvers av fagavdelinger, men også innad i kriseledelsen. I sitatet over vises det til at samarbeidet mellom sikkerhetsavdelingen og IKT-avdelingen var god, og et eksempel som trekkes frem av IKT-sjefen var at da krisen inntraff, kunne sikkerhetslederen ta seg av sin del av krisehåndteringen, slik at han selv kunne holde fokus på sitt område – og at de jobbet tett videre i situasjonen. Dette samarbeidets resultat kom til syne i innsalget til resten av kriseledelsen, som vist i avsnittet ovenfor.

> *«Jeg tror nøkkelen til at mye av dette gikk bra, er at samarbeidet mellom sikkerhetsfolkene og IKT-folkene var god. Og vi klarte å selge dette til kriseledelsen, at dette er ikke snakk om at vi mister muligheten til å høre på Spotify på jobb. Vi mister tilgang på systemene våre, som fylkeskommunen er helt avhengig av. Jeg tror det er nøkkelen her. Det skal sies, at sikkerhetsavdelingen (...) og IKT, vi har møte annenhver uke, vi har faste møter (...) Vi har et veldig godt samarbeid, vi jobber i lag, og drar i lag, og har en felles retning».*

Men også innad i kriseledelsen var det et avgjørende element. Spesielt korona-pandemien, som førte til at sentral kriseledelse ble satt ofte, sier flere av interessentene gjorde kriseteamet «drillet» på å håndtere denne situasjonen også. Det var bare en ny situasjon, og de innarbeidede rutinene hjalp på når det oppsto en ukjent trussel. Det mener ett av medlemmene gjorde det hurtig å komme til hurtige avgjørelser i krisen.

> *«Jeg tror vi var mye raskere til å handle og kunne ta kjappe avgjørelser, og bruke veldig lang tid før vi måtte bestemme oss for en avgjørelse. I hvert fall i startfasen (...) der vi foretok ganske kjappe valg, vil jeg si».*

Dette samarbeidet, forklarer flere av interessentene, gjorde at prioriteringene for hvordan arbeidet videre skulle utføres ble diskutert og gjennomført på en måte som ble oppfattet som riktig. Samtidig trekkes det frem at tidlig avklaring av roller, og hvem som var beslutningstaker, var viktig å få på plass og formalisert for å unngå et beslutningsvakuum. Ved å få formalisert at øverste beslutningstaker var politisk valgt fylkesrådsleder, fikk man en tydeligere rolleavklaring. Samtidig hevdes det at det til tross for å være en stor organisasjon, med en sentral kriseledelse og en beslutningstaker på toppen, er åpne linjer og lav terskel for å si fra direkte. Dette mener øverste beslutningstaker var viktig i håndteringen, da man ikke har egen kompetanse på alle felt.

> *«Jeg har jo ikke noe utdanning eller forkunnskaper (om IKT), men tror jo at vi bevisst eller ubevisst hadde en kultur hvor vi hadde en åpen tone og åpen linje, det var ikke sånn i fylkeskommunen at alt måtte gå 100 prosent tjenestevei og be om audiens. Det fungerer ikke sånn. Det er en stor organisasjon, men ikke så stor. Det er nyttig man har.. at man har folk som føler at her kan vi slå til hvis det er noe (...) så korte linjer der, og det trur jeg er bra når noe sånn skal trøs i gang».*

Som et siste element, var det viktig for IKT-ledelsen å kunne samarbeide med kommunikasjonsenheten, og ha kommunikasjonskompetanse tett på i kriseledelsen. Det trekker IKT-sjefen frem som et eget punkt, for å sikre at noen jobbet eksternt mens fagfolket fikk tid til å jobbe med systemene som var under angrep.

4.3 Formidling og kommunikasjon: Tydelig, enkelt og åpent

Det ble tidlig klart at kommunikasjonen var avgjørende for situasjonsforståelsen, og et element i videre arbeid med temaet. Flere av interessenten påpeker at å ha åpenhet som mantra fra før av, var et veldig viktig element i videre arbeid. Men selv om organisasjonen

plikter å etterstrebe å være så transparent som mulig, var det balansegang mellom hva de faktisk kunne dele.

Samtidig var innsalget fra sikkerhetssjef og IKT-sjef viktig, i følge både dem selv og de øvrige medlemmene av kriseledelsen. Tydeligheten og den resolutte fremtoningen gjorde at det var liten tvil om at handling måtte skje. Samtidig ble det gjort forenklinger, for å ikke skape unødvendig kompliserte møter.

> *«I stedet for å fortelle hva vi hadde gjort med brannmuren, så sa vi bare at nå er internett frakoblet. Ingen kommer inn, og ingen kommer ut. That's it».*

Et annet element, som trekkes frem for hvordan de forsto at handling måtte skje, forklares med kommunikasjonen fra sikkerhetssjef og IKT-ansvarlig, altså fagkompetansen som hadde oppdaget sikkerhetsbruddet. Flere av interessentene forklarer at tydeligheten og alvoret som de to individene viste i første møtet, var med på at de både forsto alvoret og at en såpass drastisk handling måtte skje. Dette trekkes også frem av sikkerhetssjefen på spørsmålet om hva som var det viktigste grepet han gjorde innenfor kommunikasjon.

4.3.1 Transparens

Flere av interessentene trekker frem poenget med en transparent holdning til situasjonen. Ved å ha avklart på forhånd hvordan man skal forholde seg til offentlighetsloven og åpenhet til både ansatte, berørte og publikum, var ikke det en diskusjon som var nødvendig å ta i kriseledelsen. Det var allerede avklart, så man sparte tid og ressurser på å ikke diskutere dette videre.

> *«Vi hadde diskutert, og blitt enig om, at dersom vi fikk et dataangrep, så skulle vi være åpne om det. Vi er en organisasjon som forholder oss til offentlighetsloven, og det var naturlig for oss å være åpen om det. Og det gjorde at vi ikke trengte å bruke tid på den beslutningen i forhold til kriseledelsen, så det var veldig bra. (...) Det var bare: vi skal være åpne om det, og trenger ikke bruke ressurser på å skjule noe. Det var ikke noe utfordring for oss».*

Dessuten påpeker kommunikasjonsavdelingen at det gjør deres jobb mye enklere, for man trenger ikke bruke ressurser og teknikker på å dekke over ting. Fylkeskommunen som en offentlig, politisk styrt organisasjon, er avhengig av å vise de ikke skjuler noe, la flere vekt på.

> *«Det er et viktig mantra fordi (...) nummer én: vi er finansiert med skattepenger. Nummer to, vi er til for innbyggerne våre. Og vi må kunne svare på alt uansett om det er kritisk eller mindre kritisk. Så må vi kunne svare ut det, og det handler rett og slett om å legge til mer i eksistensen vår i det hele tatt. Hvis det i fylkeskommunene, som utgangspunktet er utskjelt og lite populært, skal være lukka i tillegg, så kan du bare legge ned fylkeskommunene med en gang».*

Men kommunikasjonsavdelingen påpeker at det også hadde en effekt for å skape tillit og lojalitet til publikum under krisen. Ved å ikke dekke over ting, og være ærlig, vil man kunne bygge den tilliten. En slik proaktiv åpenhet defineres som viktig, for det var bedre enn om de hadde journalister som «graver og føler de gjør avsløringer». Samtidig, som en interessent uttalte, er man av natur informasjonshungrig, og har behov for at informasjonen ligger der tilgjengelig – selv om man ikke nødvendigvis benytter seg av den.

> *«Det at vi la oss på en åpenhetslinje, hvor det var.. det var både for at vi synes det, jeg er genuint opptatt av at vi er en demokratisk folkevalgt styrt organisasjon, folk har krav på å vite hva som er, men også at det vi holder på med, det angår så mange, at den beste måten å nå ut på, er å være åpen på det».*

Det oppfattes i ettertid også som at det var viktig å ha informasjonen åpen og tilgjengelig, til tross for at det ikke nødvendigvis ble lest.

Men selv om transparens ble trukket fram som både viktig, riktig og et krav – var nærmest samtlige i kriseledelsen klar på at det var noe informasjon de måtte holde tilbake. På grunn av situasjonens alvorlighet, at hendelsen var under politietterforskning og at systemene langsomt var på vei tilbake, var infrastrukturen særdeles sårbar. Derfor var det viktig for organisasjonen å holde tilbake informasjon som kunne være av sårbar art.

> *«Og så er det mange ting vi ikke kan si. Underveis så fikk man jo indikasjoner på hva det kunne være, og vi fikk jo en del ting som vi ikke kunne gå ut med, for det var en etterforskning som pågikk, og vi ville ikke at de som har gjort dette skulle vite hvordan vi lå an. Så det var jo ikke en absolutt åpenhet».*

Som nevnt i sitatet ble ikke full åpenhet praktisert. I følge flere av intervjuobjektene var dette dog ikke en stor utfordring, da de møtte forståelse hos interessentene sine for dette da det ble

forklart at det var en politisak, og at organisasjonen dermed ikke tok på seg det ansvaret lengre.

> *«Det har alle forståelse for, da må man spørre politiet, ikke oss. Ansvarsfordeling er viktig i en krise».*

Dette var også relatert til skyldspørsmålet, da organisasjonen ikke hadde som fokus å dele ut skyld – hverken til aktøren som gjorde angrepet, eller hvis det skulle være noen i organisasjonen som hadde utført en handling som lot angrepet skje. Dermed hadde organisasjonen som mål å ivareta to behov: de berørte i organisasjonen, for å hindre ryktespredning og misforståelser om hva som har skjedd – samt å sikre en form for samholdsfølelse – og politietterforskningen. Det ble ikke et fokus, ettersom «ansvaret» ble gitt videre til politiet ved anmeldelsen.

> *«Vi var veldig bevisst på det at vi sto sammen i søla til knærne, og vi må hjelpe hverandre ut av det (...) Det er politiet som skal gjøre vurdering av skyldspørsmålet, og det er ikke vi. (...) Det er vel noe som ligger i profesjonalitet i beredskapshåndtering, og håndtere hendelsen i fokus. Vi bærer ikke frukter å fordele skyld i noe sånn».*

4.3.2 Forenkling, tydeliggjøring og metaforbruk

Flere uttrykte i intervju at det er utfordrende å skulle kommunisere ut til flere tusen brukere som ikke får tilgang til verktøyene sine, men at fokuset var å holde kommunikasjonen så enkel som mulig, uten å gå inn på de tekniske detaljene. Informasjonen som ble gitt skulle være saklig og informativt, men ikke for komplisert, for at det skal være lett å ta imot den informasjonen.

> *«Så det må jo snakke norsk til de da, sånn at de forstår det. Si at det kommer opp nå i løpet av en måneds tid, men hvis vi ikke får gjort dette her, så kommer det opp om to år. Så da forstår jo folk det på et vis. Det er de tingene. Enkelt. Snakke norsk, ikke komplisere det for mye».*

Dermed opplevde kriseledelsen at de i stor grad møtte forståelse hos sine interessenter. Det ble også forklart at de hadde prioritert direkte kommunikasjon til ansatte fra nærmeste leder, da de har gjort undersøkelser under pandemien at det er den informasjonen som blir forstått av flest – fremfor intranett, mail og andre medier. Kommunikasjons-kompetansen i

kriseledelsen fremhevet også dette poenget, og benyttet formuleringer fra kriseledelses-møtet videre i kommunikasjonen utad. Dette fordi det gjerne ble enklest, tydeligst og best mulig forklart i den settingen, og ved å notere ned formuleringene kunne kommunikasjonen utad også fremstå så tydelig og forståelig som mulig.

Samtidig var tydelighet en viktig faktor – både innad i kriseledelsen, men også ut til folk. Det ble sagt av flere at innsalget fra fagfolket var essensielt for å forstå hva som foregikk. Det som ble trukket frem var tydeligheten i budskapet fra fagfolket. Over her er også tydelighet trukket frem. At tydelig kommunikasjon fra fagfolket og sikkerhetsansvarlig var det som gjorde at alvoret sank inn, men det ble også fremhevet at tydelighet og handlekraftighet fra øverste beslutningstaker, som man i utgangspunktet har tillit til som leder. Her kommer også tydelighet i form av roller til syne. Det var et element for å sikre handling. Kriseledelsen tidligere hadde hatt tre likestilte direktører til å ta avgjørelser, kom det inn en politisk leder som endelig beslutningstaker. Det gjorde det lettere for å komme til en endelig beslutning om hvordan de skulle handle videre.

> *«Det hjalp veldig. For når du skal ut med informasjon, er det en endelig beslutningstager, og ikke tre som sitter og diskuterer på bakgrunnen. Jeg tror det hjelper alle, og ikke bare oss, å jobbe med kommunikasjon med alle som sitter i krisestaben».*

Et element som bør nevnes, med bakgrunn i teorien, er relatert til metaforbruk. For ved spørsmål om dette, ble det sagt at det ikke ble benyttet for å hindre misforståelser og kommunisere tydelig og klar informasjon. Men, en setning som ble brukt av flere, var «å dra ut pluggen», for å stenge internett. Dette påpekte de som formidlet situasjonen til kriseledelsen, uoppfordret, at ikke var det som faktisk skjedde.

> *«(...) for å si litt om det, så trekker vi ikke ut noen fysisk internettplugg, bare ... så det ikke er noen tvil om det, men det er det man sier – man tar pluggen».*

Et intervjuobjekt sa i sitt intervju, at det faktisk var det som skjedde.

> *«(...) så dro vi faktisk, bokstavelig talt, ut pluggen».*

Dette viser at det er en dissonans i forståelsen av hva som faktisk skjedde ved frakopling av internett, og fremhever at metaforbruk kan føre til ulik forståelse av hva som foregår i organisasjonen.

5 Diskusjon

Resultatene viser tydelig at tillit til de som var faglig ansvarlig, og samarbeidet i kriseledelsen, var avgjørende for at resten av organisasjonen handlet slik de gjorde – å stenge ned internett allerede etter første møte i den sentrale kriseledelsen. Men flere elementer dras også frem som sentrale. Et sterkt fokus på transparens, og en diskusjon og skolering på temaet i forveien var med på å skape en bevissthet i organisasjonen. Språk spilte en viktig rolle for de som skulle kommunisere hva som foregikk på IKT-siden, og tydeligheten enkelheten i kommunikasjonen var med på å få kriseledelsen til å handle slik fagpersonellet innen IKT og sikkerhet ønsket – og denne metoden ble fremhevet som essensiell for de øvrige medlemmene i kriseledelsen. Det skapte både en forståelse og forsterket tillit til at handlingen ble gjennomført.

Videre skal diskusjonsdelen ta utgangspunkt i forskningsspørsmålene for å diskutere funnene i analysen opp mot det teoretiske rammeverket, før kapittelet konkluderer med en gjennomgang av diskusjonen opp mot modellen av rammeverket.

5.1 Forarbeid og bevisstgjørelse

Hva gjorde at ledelsen ved organisasjonen forsto at dataangrepet var av en så alvorlig art at drastiske tiltak måtte til? At det var høy grad av tillit var hjelpsomt når krisen inntraff, men det var også et forarbeid i grunn som gjorde organisasjonen bedre forberedt på å håndtere krisen da den inntraff. Både kriseledelsens sendere og mottakere av situasjonen påpeker at det hadde vært et ekstra søkelys på datasikkerhet i månedene før dataangrepet. Dette var på grunn av høyt trusselnivå, som gjennom innlegg på fylkesting for politikere, og via interne kanaler ble formidlet til organisasjonen. Arbeidet i forkant understreker poenget til Berg og Kuipers (2022) poeng om at ledelsen med fordel kan skape debatt om datasikkerhet og -trusler i forkant av angrep, og skape en bevissthet som kan gagne organisasjonen om den skulle oppstå. Organisasjonen hadde satt datasikkerhet på dagsorden gjennom forskjellige kanaler bare måneder i forveien, noe deltagerne i denne studien fremhever som et grep som gjorde at tematikken lå klart i minnet til aktuelle parter. Dermed kunne de raskere forstå alvorligheten i hendelsen, og nødvendigheten av å svare på situasjonen. Respondentene i sentral kriseledelse fikk ikke merkbare negative tilbakemeldinger fra sine interessenter. En grunn for dette kan være at arbeidet i forveien var med på å skape en forståelse for handlingene som ble utført. Samtidig ble også samarbeidet og de innarbeidede rutinene i kriseledelsen fremhevet som en faktor av kriseledelsens medlemmer. På grunn av hyppige møter under pandemien, som

fortsatt ble avholdt på tidspunktet dataangrepet inntraff, gikk diskusjonene på tvers av fagfeltene effektivt. Happa og Fairclough (2016) sin modell presiseres hvordan man kommer frem til en felles beslutning. Dette så man også i Nordland fylkeskommunes arbeid, hvor alle var enige i beslutningen som ble tatt. Samtidig presiserte respondentene til denne studien hvor viktig det var å ha én bestemt beslutningstaker. Dette kommer ikke frem i modellen til Happa og Fairclough (2016), men er et funn som er verdt å nevne, da det var et element som flere trakk frem – deriblant beslutningstaker selv. Dette ble gjort for å hindre misforståelser, men også for å ha én beslutningstaker, og ikke flere ulike med samme beslutningsmyndighet. Her ble også den flate strukturen trukket frem som en faktor. Beslutningstaker i Nordland fylkeskommune trosset risikoen ved å miste egen kontroll ved å gå for en flatere struktur i organisasjonen, slik at det ikke var lang vei fra ansatte og opp til beslutningstaker. Man kan argumentere for at det samsvarer med Spreitzer og Mishra (1999) sine argumenter, som sier organisasjonens prestasjoner vil heves ved å inkludere ansatte med spesialkompetanse i beslutningsprosesser. Dette vil øke effektiviteten på prosessen, og gjøre slik at ledelsen kan komme frem til beslutninger og avgjørelser som er proporsjonal for krisen som oppsto. Samarbeidet på tvers av hierarki og fagfelt gjorde at prioriteringene for hvordan arbeidet videre skulle utføres ble diskutert, og gjennomført på en måte som fikk bred tilslutning i kriseledelsen. Samtidig trekkes det frem at tidlig avklaring av roller, og hvem som var beslutningstaker, var viktig å få på plass. Det å få dette formalisert var viktig for å unngå et beslutningsvakuum.

Det må også nevnes hvordan kommunikasjonen mellom partene i kriseledelsen påvirket situasjonen. Fokuset fra fagfolket innen IT- og sikkerhet var å kommunisere enkelt, tydelig og forklarende, med vekt på hva konsekvensen kan være om man ikke gjennomfører den foreslåtte handlingen. Formidlingen var et sentralt fokus for fagfolket, for å få budskapet så forståelig som mulig. Dette til tross for at det fagtekniske språket kan være komplisert. Som Cornelissen et al. (2014) fremhever hvordan man benytter et språk og kommuniserer på en måte som gjør at man kollektivt kommer frem til en beslutning for hvordan håndtere en gitt situasjon. Man kan argumentere for at det også synes i Nordland fylkeskommunes kriseledelse. Kommunikasjonen beskrives som åpen, tillitsfull og på et språk som var forståelig. Ikke nødvendigvis for å beskrive temaet, men med språk som kan gi større bakgrunnsforståelse og grunnlag for beslutningen, som Cornelissen et al. (2014) påpeker. Dette poenget kommer frem i intervjuene, der IKT- og sikkerhets-sjefen som formidlet budskapet bevisst valgte å «snakke norsk», og beskrive konsekvenser fremfor det tekniske.

Formidlingen skulle være enkel og forståelig, noe resten av intervjuobjektene og medlemmene av kriseledelsen bekrefter. De forteller videre at innsalget som ble gjort fra IKT og sikkerhetsavdelingen, var avgjørende for at de forsto alvoret og kunne fatte en beslutning. Kommunikasjonsavdelingen påpekte også at det ble notert ned hva som ble sagt i møtet, til bruk i kommunikasjonen videre. Dette forsterker også Whittle et al. (2023) sitt argument på rollen språk spiller i sensemaking-prosessen, der det er med på å kollektivt bygge rammer for en felles forståelse av situasjonen.

5.2 Helhetlig involvering og tillit

Hvilken rolle spilte mellom-menneskelige relasjoner i at kriseledelsen forsto alvorligheten av dataangrepet? Som respondentene i denne studien forklarte, var ikke kunnskapsnivået om IT-relaterte utfordringer nødvendig så høyt. Dermed var de avhengig av spesialister på fagfeltet. Dette samsvarer med Happa og Fairclough (2016) sine betraktninger. Man vil feile i å komme frem til én enkelt avgjørelse i ledelsen, dersom man ikke henter inn nødvendig kunnskap for å oppnå en samlet forståelse. Respondentene i denne studien påpeker at det var tillit til fagkompetansen de lente seg på. Til tross for at de individuelt hadde kunnskapshull om IT-relaterte sikkerhetsutfordringer, hentet de inn nok informasjon fra fagkompetansens innsalg til at de tok den avgjørelsen som var nødvendig. Forfatterne peker på sin egen modell for å nå en kollektiv tilnærming sensemaking rundt dataangrep: en holistisk tilnærming til angrepet, bred involvering av medlemmer av organisasjonen og behovet for å nå en felles forståelse av situasjonen.

Dette speiles i Nordland fylkeskommunes fremgangsmåte. Ved å involvere hele kriseledelsen, som består av direktører fra hvert av de forskjellige ansvarsområdene, fagkompetanse innenfor både IT, sikkerhet og kommunikasjon, og de to øverste politiske lederne, kunne man få samme informasjon å handle etter. Med andre ord var et bredt spekter av involverte parter inkludert. Deretter kunne de effektivt kommunisere imellom seg for å komme frem til en beslutning. Dette gjorde at de kunne fatte en rask avgjørelse, og fylkeskommunen valgte deretter å sende ut første melding om informasjon umiddelbart etter første krisemøte. Dette begrunnes med at de ville informere så fort som mulig at noe var på gang, selv om ikke all informasjon var tilgjengelig. For kriseledelsen var det en prioritet å få ut informasjon så fort som mulig. Dette ble gjort med SMS, samt at det ble påpekt at den største suksessen med å nå ut til alle var å gi direkte informasjon fra nærmeste leder. Dette stemmer overens med Knight og Nurse (2020) sine funn om at mer direkte og personlig kommunikasjon har størst effekt

hos de man ønsker å nå. Dette samsvarer også med Boin et al. (2021) argument relatert til sensemaking, om at en krise håndteres mest effektivt når de riktige menneskene oppdager en trussel på en verdi, og deretter tolket og forstått. Man kan argumentere for at kombinasjonen av at de rette menneskene så trusselen også evnet å formidle det videre slik at avgjørelser ble tatt raskt. Det var en villet strategi å gå høyt ut i møte med trusselen, for så heller å de-eskalere etter hvert, for å unngå «for lite – for sent»-tiltak. Dermed svarte man på krisen på adekvat vis.

For å komme frem til en slik respons, er man også avhengig av tillit. Yu et al. (2022) forklarer at tillit er en viktig forutsetning for å faktisk komme frem til en avgjørelse hurtig. Flere av respondentene påpeker at det var tilliten til fagmiljøet og sikkerhetsavdelingen som gjorde at de kunne handle så hurtig som de gjorde. Beskjedene fra fagavdelingen om hva som foregikk, og deres analyse, var nok til at man kunne komme frem til avgjørelsen, til tross for at individenes egen fagkompetanse på IT-feltet ikke var høy. Spreitzer og Mishra (1999) tar opp nettopp dette, der inkludering og tillit til ansatte som ikke var på samme hierarkisk nivå, førte til ønsket effekt av beslutningen. Situasjonen i Nordland fylkeskommune samsvarer dermed med deres funn. Det kan derfor argumenteres for at tillit og inkludering, ikke bare på tvers av kriseledelsen, men også videre ned på organisasjonskartet, kan føre til at man tar de nødvendige beslutningene i tilfelle av dataangrep. Øverste beslutningstaker fremhever kulturen med åpne kommunikasjonslinjer og ingen rigid tjenestevei, som et viktig element av hvordan ledelsen nådde sin avgjørelse om å stenge ned for å unngå ytterligere konsekvenser. Dette fokuset fra ledelsen kan man argumentere for at gir rom for utøvelsen av tillit mellom ledelse og ansatte, og legger til rette for et samarbeid som leder til gode avgjørelser, som Fragouli (2019) påpeker.

Dermed argumenterer denne studien for at mellom-menneskelige relasjoner i Nordland fylkeskommunes sentrale kriseledelse spilte en avgjørende rolle for forståelsen av hva som skjedde. Tillit, som Adobor (2005) påpeker, var medvirkende for at organisasjonen nådde sitt mål. Dette fordi organisasjonen la stor vekt på beskjedene som kom fra faglig hold – både IKT-avdelingen, men også sikkerhetsavdelingen.

5.3 Transparens og et forenklet budskap

Hva var organisasjonens hovedfokus når det gjaldt formidling og kommunikasjon til berørte parter? Basert på intervjuene, er det to faktorer som stikker seg ut relatert til hvordan fylkeskommunen valgte å formidle hva som hadde skjedd, og hva veien videre var. Det ene er

transparens, som flere trakk frem som det viktigste kommunikasjonsgrepet som ble gjort. Dette forklares med at de er en offentlig organisasjon, som skal etterstrebe å være åpen og tilgjengelig for publikum og skattebetalere. Dette førte også til at det ikke var nødvendig med en diskusjon om nettopp dette når hendelsen inntraff. Videre var det en måte å skape en helhetlig tillit mellom ledelsen, berørte parter og befolkning ellers. Denne åpenhetslinjen skapte også en proaktiv holdning til informasjonsspredning, som gjorde at organisasjonen etterstrebet å tilgjengeliggjøre informasjon for interessenter – både i interne kanaler, og eksternt i media.

Det er flere elementer ved dette som er nødvendig å trekke frem når man sammenligner empirien med litteraturen. Som Bentley et al. (2018) beskriver, fokuserer ikke organisasjonen å ta på noe skyld selv – men det er heller ikke et ønske eller valg om å legge skylden på andre. Dette gjelder den fremmede aktøren som utførte angrepet, så vel som eventuelt noen interne som kan ha forårsaket angrepet. Begrunnelsen for dette var at det ikke var organisasjonens ansvarsområde når forholdet hadde blitt anmeldt. Fokuset skulle heller være på de berørte parter. Dette kan man argumentere for samsvarer med både Bentley et al. (2018) og Kuipers og Schonheit (2022), som beskriver hvordan empati til de som er rammet av angrepet er viktig å formidle, både for å skape tillit til ledelsen og organisasjonen – men også for å opprettholde omdømmet. Det som Bentley et al. (2018) fremhever i tillegg, er organisasjonens beklagelse og dets innhold. Ut fra funnene i denne studien er ikke dette alltid relevant. Fylkeskommunen påsto selv at de ikke hadde noen grunn til å beklage, da de var utsatt for en kriminell handling.

Ledelsen opplevde heller ikke de store klagene fra berørte parter i organisasjonen, foruten fra politisk hold i fylkesting. Valget om å ha en proaktiv holdning, med transparens i bunn, viser at Sapriel (2021) sitt argument om at mangelen på åpenhet og empati mot interessenter som var berørt av angrepet, kunne gjøre dem mer frustrert og skapte en mangel på tillit. Respondentene i denne studien kunne ikke si de hadde fått noe særlig med tilbakemeldinger, ei heller om noe som kan minne særlig om frustrasjon eller mangel på tillit. Dette kan man argumentere for at bunner i Diers-Lawson et al. (2021) sine funn om at en proaktiv relasjonsbygging med interessenter vil gi kommunikasjonen større og bedre effekt, heller enn en reaktiv tilnærming. Dermed kan se ut som Nordland fylkeskommune valgte samme løsning som Norsk Hydro i Sapriel (2021) sin analyse, der man umiddelbart sørget for en aktiv kontakt umiddelbart for å kunne skape tillit hos ansatte og befolkning for øvrig. Litteraturen viser at dette er et viktig grep for å skape tillit og redusere tap av omdømme, som også

kriseledelsen har som et utgangspunkt, men sier også at de ikke kunne dele all informasjonen de satt på. Hendelsen var under politietterforskning, og av den grunn var det elementer som måtte tilbakeholdes. Dette kan ses i lys av Kaschner (2022) sine argumenter, om en delt forståelse av hvor viktig det er å dele all informasjon.

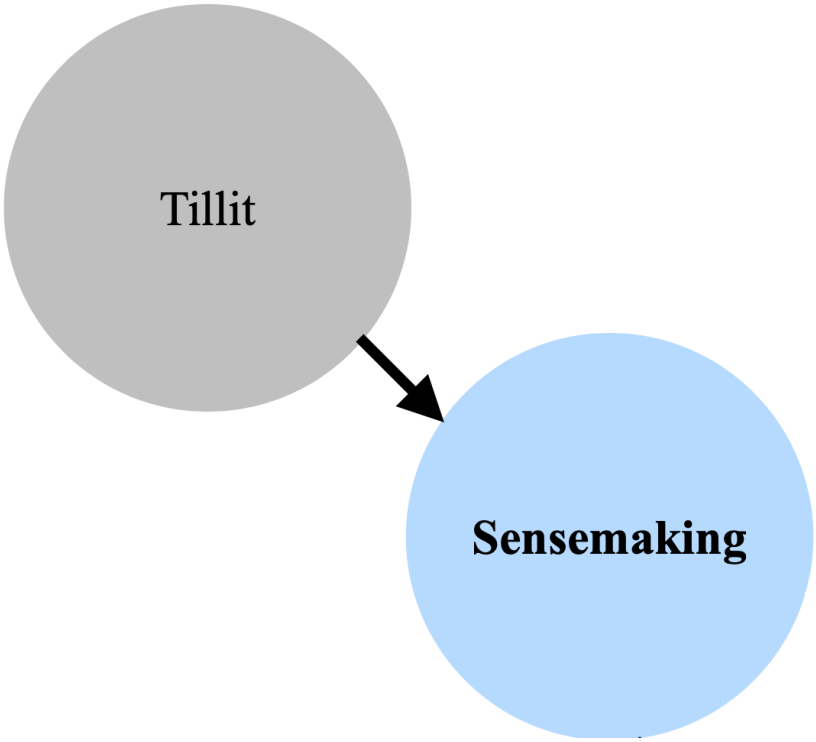
Som Berg og Kuipers (2022) argumenterer for, er det lett for ledere å ha en trang til å forenkle budskapet for mye, og gå for metaforer – noe som igjen vil kunne føre til urettmessige sammenligninger. Det ble ikke brukt metaforer i stor grad under formidlingen av angrepet til sentral kriseledelse, noe som ble begrunnet med at man skulle holde det så enkelt som mulig uten å forvirre. Dette kan argumenteres for var et viktig poeng. En forenkling, eller metafor, som ble brukt var «å dra ut pluggen», noe en respondent sa var det som «faktisk skjedde». Berg og Kuipers (2022) poeng bunner i å bruke metaforer fra den fysiske verdenen til å karakterisere det som skjer under dataangrep, og dette funnet kan utvide denne argumentasjonen, og si at metaforbruk som brukes for å karakterisere en handling også kan føre til misforståelser over hva som er den faktiske situasjonen.

5.4 Studiens bidrag til et teoretisk rammeverk

Denne studien har forsøkt å se på hvilke forhold som gjorde at kriseledelsen i Nordland fylkeskommune kom frem til hvordan de skulle respondere på den usynlige fienden et dataangrep medfører. Der andre kriser i større grad kan oppfattes enklere, enten fysisk eller med mer forståelsesgrunnlag, har dataangrep det elementet at det er i stor grad forbeholdt de med ekstra kompetanse på feltet. Dette gjør det utfordrende både ledelsen og ansatte i offentlige organisasjoner, som har flere områder de skal råde over, da de ikke nødvendigvis innehar denne kompetansen. Hvordan kan man sikre at en selv forstår hva som foregår, og deretter formidle dette videre? Sensemaking-teorien er velutviklet og diskutert mye i akademia, men rettet mot dataangrep er det stadig mye forskning som gjenstår før man får et helhetlig blikk på hvordan ledelser i både offentlige og private organisasjoner kan forstå omfanget, og handle med de nødvendige tiltak deretter. Studien har forsøkt å se på ulike argumenter innenfor sensemaking-teori, hvor enkelte også er spesifikt rettet mot dataangrep.

Denne studien kan bekrefte mye av tidligere forskning har avdekket, men også legge til noen argument som med fordel kan bli forsket videre på. Det argumenteres for at elementet av tillit mellom medlemmene av kriseledelsen, og i organisasjonen for øvrig, er underdimensjonert i forskningen. Ved et angrep av en usynlig aktør, der «hvem, hva og hvorfor»-spørsmålene forblir ubesvart, vil tillit være elementært for å kunne nå raske avgjørelser i kriseledelsen, og

dermed essensiell å kunne utføre sensemaking-prosessen. Et godt samarbeidsgrunnlag er også viktig for prosessen, som et resultat av opparbeidet tillit på tvers av hierarkisk struktur. Det fremstilles derfor som grunnlaget for hvordan ledelsen klarer å forstå hendelsen, og som et sterkt bidrag til hvorfor det ble handlet så raskt som det ble.



Figur 2: Tillits betydning for sensemaking-prosessen.

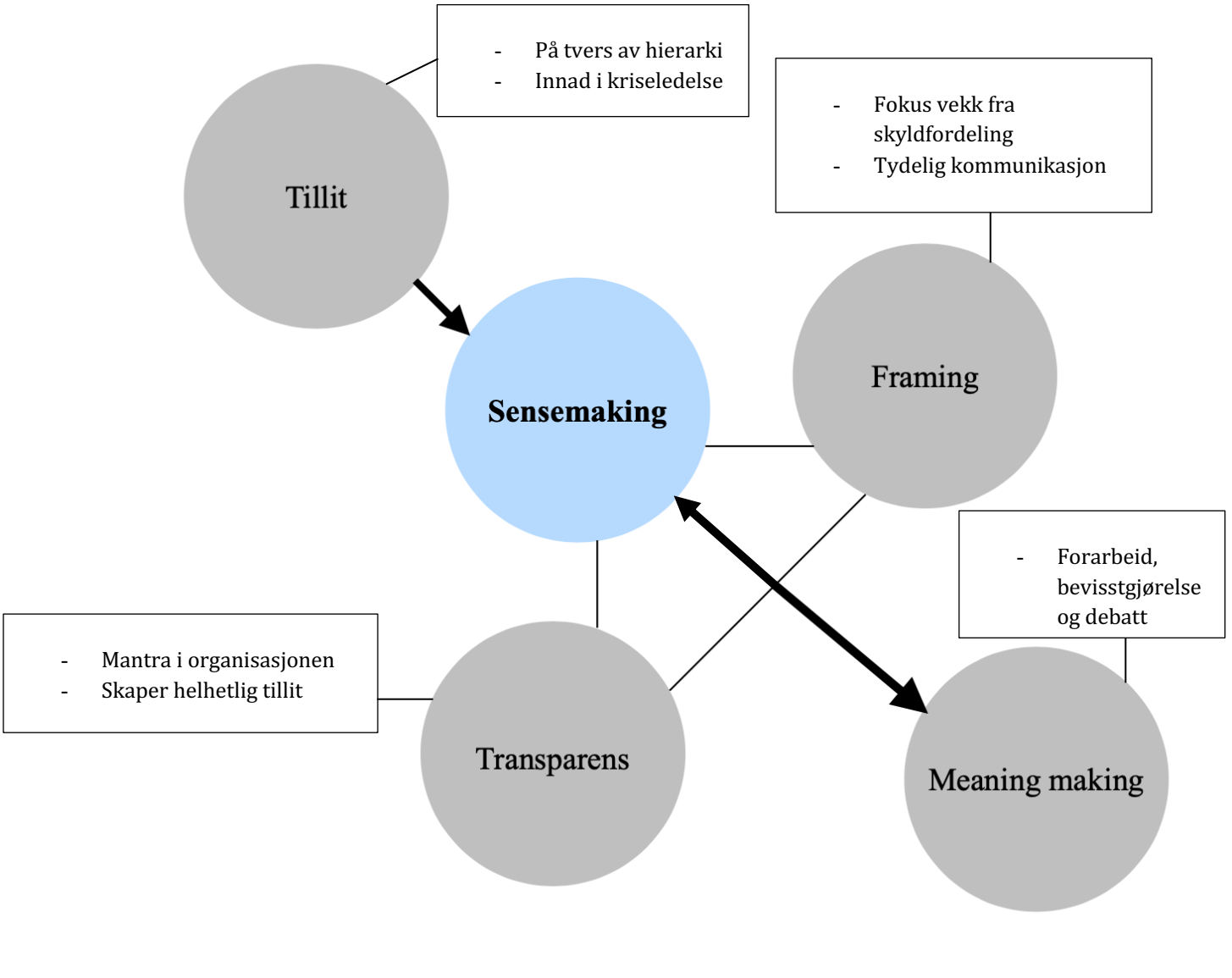
Argumentet om betydningen av tillit burde tas opp i senere forskning. Dette for å se på hva som gjør at ansatte opplever tillit til sin ledelse, til å følge og stole på de avgjørelser blir tatt. Også samarbeidsrutiner spiller inn her. For organisasjonen i denne studien var det opparbeidet god kjennskap til både sin egen, og sine kollegers, rolle i kriseledelsen. Kriseledelsen i Nordland fylkeskommune hadde nettopp lagt bak seg nesten to år med intense kriseledelsesrutiner, siden pandemien krevde jevnlige møter. Dette medførte både at tilliten vokste mellom aktørene i kriseledelsen, og hadde skapt gode samarbeidsrutiner. Dermed kan en hypotese til videre forskning være basert på at tillit og samarbeidsrutiner er essensielt for å håndtere dataangrep i offentlige organisasjoner, der ledelsen består av individer med ulik bakgrunn. Denne studien støtter også opp under Berg og Kuipers (2022) sitt argument om viktigheten av å skape en debatt, diskusjon og bevissthet rundt dataangrep – i forkant av et eventuelt angrep, er viktig i selve sensemaking-prosessen. For Nordland fylkeskommune var det et arbeid for å sette søkelys på denne trusselen i forkant av angrepet, noe flere av

respondentene i denne studien sier var med på å skape en bevissthet for alvorligheten av angrepet. Med dette som bakgrunn, kan man argumentere for at en slik bevisstgjøring var med på å skape en forståelse for alvoret i situasjonen, som gjorde at en beslutning for handling kom allerede etter første møte.

Videre avdekker denne analysen også at språk under kriseformidlingen var avgjørende, både innad i kriseledelsen, men også som et fokus til videre kommunikasjon ut i organisasjonen. I innsalget fra fagavdelingen ble det lagt vekt på et klart, tydelig og enkelt språk. Dette for å sikre en bakgrunnsforståelse for hva som skjer, hvor mye man vet og ikke – og eventuelle konsekvenser, fremfor å påpeke de tekniske detaljene. Å beskrive enkelt hva som hadde skjedd, og være åpen om at situasjonen er uavklart, og med det som grunnlag formidle at deres vurdering for best mulig utfall var å stenge ned, var delaktig i både å komme frem til avgjørelsen, men og en forståelse for situasjonen. Som en villet strategi, ble språket brukt i møtene notert ned, og formidlet videre til interessenter og berørte parter. Dette fordi språket brukt i kriseledelses-møtene var enkelt og tydelig, og dermed formålstjenlig å benytte videre. Studien argumenterer derfor for at språk spilte en rolle for hvordan det ble rammet inn en forståelse av situasjonen, som også ble benyttet i kommunikasjonen videre. Dermed trekkes transparens også inn som et tilknyttet konsept. Videre argumenteres det for at ærligheten og transparensen til fagavdelingen ble satt pris på av de øvrige medlemmene av kriseledelsen, som også sørget for at situasjonen ble forstått. For en offentlig organisasjon er åpenhet en viktig faktor. Det viser at transparens som en grunnpilar er med på å gjøre det forutsigbart for ledelsen i situasjonen, og responsen de har fått har ikke indikert at det var behov for mer åpenhet, til tross for at noe ble holdt tilbake. At eventuelle hendelser skulle behandles transparent var avklart allerede før hendelsen inntraff, så lenge det ikke gikk på tvers av politietterforskningen. I dette øyemed trekkes det også frem at det ikke ble gjort noe med skyldfordeling eller noe utfyllende beklagelser. Dette er relevant i forhold til framing-konseptet, der deler av litteraturen argumenterer for skyldfordeling og beklagelser som en mulig strategi i håndteringen av et angrep. Dette var ikke fokuset til fylkeskommunen. I stedet formidlet de situasjonen og ba om forståelse.

Av den grunn viser illustrasjonen en sammenheng mellom transparens, framing og sensemaking – en sammenheng som til sammen er med på å danne et grunnlag for å kommunisere videre til interessenter og berørte parter gjennom meaning-making. Ut fra teorien, forklarer Berg og Kuipers (2022) hvordan diskusjon og opplæring i forkant er med på å forenkle denne meaning-making-prosessen, som igjen kan kobles opp mot sensemaking-

prosessen – der en økt bevissthet i forkant av angrepet fremheves som et ledd for hvordan kriseledelsen hurtig kunne ta en avgjørelse.



Figur 3: Det teoretiske rammeverket med empiriske betraktninger.

5.5 Kritikk og videre forskning

Studien tar utgangspunkt i en casestudie som ser på hvordan kriseledelsen oppfattet, forsto og videre kommuniserte dataangrepet som traff Nordland fylkeskommune desember 2021. Ved å identifisere elementer som tillit og etablerte samarbeidsrutiner som avgjørende for sensemaking-prosessen, er dette basert på enkelte medlemmers betraktninger gjennom intervju. Studien kan dermed argumentere for at det var tillit innad i kriseledelsen, men har ingen målepunkt for tillit til ledelsen fra interessenter og andre berørte parter. Dermed skal denne forskningen være forsiktig med å konstatere at dette er riktig metode og strategi fra en ledelse å svare på dataangrep. Til gjengjeld var det ikke det denne studien baserte seg på. Denne analysen var ute etter å forstå hvilke tanker, refleksjoner og avgjørelser som ble gjort av ledelsen – og plassere det i et nytt teoretisk rammeverk, som baserer seg på eksisterende teorier, konsepter og litteratur. Dette byr opp til flere muligheter for videre forskning. Det ene er at det gir et godt grunnlag for å undersøke om strategien valgt av Nordland fylkeskommune skapte tillit, og om mangelen på mye respons på tiltakene var grunnet en komfortabel innstilling til hva ledelsen valgte, eller om det ikke ble kommunisert ut på en måte som gjorde at det skapte engasjement. Det andre er å teste denne modellen på andre organisasjoner eller virksomheter som kan ha opplevd lignende tilfeller – i tillegg til å se om den kan tilpasses til andre hendelser som ikke er dataangrep. Det vil også være interessant å studere forskjellene mellom organisasjoner og virksomheter som skal være offentlige og transparente, gjerne statlige organisasjoner, og andre som ikke har samme krav til transparens.

Videre har ikke denne studien sett på strategien rundt krisekommunikasjon isolert sett. Man kan argumentere for at forskningen ville blitt enda mer utfyllende hadde man inkludert mer krisekommunikasjons-strategier. Hadde man og sett på relevante teorier og sammenlignbare empiriske hendelser, kunne man belyst hvordan dataangrep kan kommuniseres. Som motargument til dette, har man her forsøkt å ta utgangspunkt i forståelse for kommunikasjonen, og sett på dette som et ledd i forkant av selve kommunikasjonsstrategien. Med andre ord, ikke nødvendigvis hvordan det ble kommunisert rent strategisk, men hvordan man fikk en forståelse av situasjonen nok til å kunne sette rammeverket for kommunikasjonen man ville dele med omverdenen. Som nevnt, kan dette med fordel tas med videre i andre forskningsprosjekter.

6 Konklusjon

Studien har gjennomgått hva som var viktig for at ledelsen i Nordland fylkeskommune greide å forstå situasjonen som oppsto ved dataangrepet i desember 2021, nok til å ta raske avgjørelser som i ettertid har vist seg å høste ros fra myndigheter og fagnettverk. Videre har teksten sett på hva som var viktig å fokusere på i videre formidling, gitt den usikre situasjonen. Med utgangspunkt i sensemaking-teori, presenteres det i denne studien et teoretisk rammeverk som inkluderer konseptene tillit, meaning-making, framing og transparens for å kunne identifisere faktorer som kan forklare dette fenomenet.

Rammeverket i denne studien viser hvilken rolle tillit spiller inn og kan legge til rette for sensemaking-prosessen, der veletablerte samarbeidsrutiner og en åpen linje som bryter med hierarkisk struktur var med på å bidra til at ledelsen kunne ta drastiske, men nødvendige, avgjørelser hurtig. Studien viser også hvilken rolle språk har i formidlingen – både innad i kriseledelsen, men også utad og gjennom meaning-making. Samtidig ser man hvilken betydning transparens har i diskusjonen innad i kriseledelsen i sensemaking-prosessen. Samspillet mellom disse konseptene gir spiller en betydelig rolle på hvordan man da utfører meaning-making. Studien bekrefter også viktigheten av å ha en diskurs og vokabular i organisasjonen i forkant, både til å forstå situasjonen gjennom sensemaking, men også for å lettere kunne gjennomføre meaning-making. Dermed viser rammeverket hvordan de ulike konseptene spiller på hverandre for å kunne oppnå resultatet i Nordland fylkeskommune.

Som et mer konkret svar på problemstillingen, konkluderer denne studien med at tillit, samarbeidsrutiner og et uttalt fokus og opplæring på trusselen i forkant var avgjørende for at kriseledelsen kunne forstå situasjonen nok til å utføre en så drastisk avgjørelse som å stenge internettet for å forhindre ytterligere konsekvenser av dataangrepet. Dette, i tillegg til et avklart forhold til transparens og tydelig og forklarende språk, lå til grunn for hvordan kriseledelsen kunne forstå og formidle hendelsen.

Studien presenterer også et teoretisk rammeverk, og argumenterer for at dette kan passe til flere organisasjoner i samme situasjon. Det oppfordres til å teste dette rammeverket mot andre tilfeller, for å eventuelt identifisere forbedringer eller argumenter mot rammeverket. Det identifiseres også forslag til videre forskning, og det oppfordres til å fortsette å forske på forhold rundt dataangrep, og trusselen av cybersikkerhet.

7 Litteraturliste

Adobor, H. (2005). Trust as sensemaking: the microdynamics of trust in interfirm alliances. *Journal of business research*, *58*(3), 330-337. https://doi.org/10.1016/S0148-2963(03)00077-8

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H. & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, *71*(8), 939-953. https://doi.org/10.1002/asi.24311

Andreassen, G. (2022, 19.01). Trinnvis gjenåpning etter dataangrep for Nordland fylkeskommune. *Bodøposten*. https://xn--bodposten-n8a.no/trinnvis-gjenapning-etter-dataangrep-for-nordland-fylkeskommune/

Aoyama, T., Sato, A., Lisi, G. & Watanabe, K. (2020). On the Importance of Agility, Transparency, and Positive Reinforcement in Cyber Incident Crisis Communication. *Critical Information Infrastructures Security*, 163-168.

Balsvik, E. S., Susanna Maria (2011). Introduksjon IE. Balsvik & S. M. Solli (Red.), *Introduksjon til samfunnsvitenskapene* (Bd. 2). Universitetsforlaget.

Bannister, F. & Connolly, R. (2011). The Trouble with Transparency: A Critical Review of Openness in e-Government. *Policy and internet*, *3*(1), 1-30. https://doi.org/10.2202/1944-2866.1076

Bentley, J. M., Oostman, K. R. & Shah, S. F. A. (2018). We're sorry but it's not our fault: Organizational apologies in ambiguous crisis situations. *Journal of contingencies and crisis management*, *26*(1), 138-149. https://doi.org/10.1111/1468-5973.12169

Berg, B. v. d. & Kuipers, S. L. (2022). Vulnerabilities and cyberspace: a new kind of crisis. *Oxford Research Encyclopedia Of Politics*. https://doi.org/doi:10.1093/acrefore/9780190228637.013.1604

Boin, A., McConnell, A. & t Hart, P. (2021). *Governing the Pandemic*. Springer Nature. https://doi.org/10.1007/978-3-030-72680-5

Braun, V. & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, *3*(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Brinkmann, S. & Tanggaard, L. (2019). *Kvalitative metoder : empiri og teoriutvikling* (4. utg.). Gyldendal

Brottveit, G. & Del Busso, L. (2018). *Vitenskapsteori og kvalitative forskningsmetoder : om å arbeide forskningsrelatert*. Gyldendal akademisk.

Brown, A. D., Colville, I. & Pye, A. (2015). Making Sense of Sensemaking in Organization Studies. *Organization studies*, *36*(2), 265-277. https://doi.org/10.1177/0170840614559259

Budalen, A. (2021). Frykter personopplysninger er på avveie: 18.000 kan være rammet. *NRK*. https://www.nrk.no/nordland/nordland-fylkeskommune-frykter-personopplysninger-er-pa-avveie-etter-dataangrep-1.15810697

Busso, L. D. (2018). Å bli en etisk forsker. I G. Brottveit (Red.), *Vitenskapsteori og kvalitative forskningsmetoder*. Gyldendal akademisk.

Chayes, A. (2015). Cyber Attacks and Cyber Warfare: Framing the Issues. I *Borderless Wars Civil Military Disorder and Legal Uncertainty* (s. 130-143). Cambridge University Press. https://doi.org/10.1017/CBO9781316271551.011

Cornelissen, J. P., Mantere, S. & Vaara, E. (2014). The Contraction of Meaning: The Combined Effect of Communication, Emotions, and Materiality on Sensemaking in the Stockwell Shooting. *Journal of management studies*, *51*(5), 699-736. https://doi.org/10.1111/joms.12073

Datatilsynet. (2022). *Avslutning av sak - melding om avvik - NORDLAND FYLKESKOMMUNE*. Datatilsynet.

Diers-Lawson, A., Symons, A. & Zeng, C. (2021). Building crisis capacity with data breaches: the role of stakeholder relationship management and strategic communication. *Corporate communications*, *26*(4), 675-699. https://doi.org/10.1108/CCIJ-02-2021-0024

Egloff, F. J. (2020). Public attribution of cyber intrusions. *Journal of cybersecurity (Oxford)*, *6*(1). https://doi.org/10.1093/cybsec/tyaa012

Engen, O. A., Kruke, B. I., Lindøe, P., Olsen, K. H., Olsen, O. E. & Pettersen, K. A. (2016). *Perspektiver på samfunnssikkerhet*. Cappelen Damm akademisk.

Entmann, R. (2004). *Projections of Power: Framing News, Public Opinion, and U.S. Foreign Policy*. University of Chicago Press.

Forsland, S. (2022). *Om datainnbruddet*. Nordland fylkeskommune. Hentet 02.02.2023 fra https://www.nfk.no/om-fylkeskommunen/om-datainnbruddet/

Fragouli, E. (2019). Employee Trust and Ethical Leadership Decision Making. *Behavior Studies in Organizations*, *1*, 1-12. https://doi.org/10.32038/JBSO.2019.01.01

Frigård, T. K., Torgeir P. . (2022, 18.06.2022). Dataangrep mot Nordland fylkeskommune: - Angrepet fra utlandet. *Dagbladet*. https://www.dagbladet.no/nyheter/angrepet-fra-utlandet/76352678

Happa, J. & Fairclough, G. (2016). A Model to Facilitate Discussions About Cyber Attacks. I L. G. Mariarosaria Taddeo (Red.), *Ethics and Policies for Cyber Operations* (s. 169-185) (Philosophical Studies Series). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-45300-2_10

Helsloot, I. & Groenendaal, J. (2017). It's meaning making, stupid! Success of public leadership during flash crises. *Journal of contingencies and crisis management*, *25*(4), 350-353. https://doi.org/10.1111/1468-5973.12166

Jagd, S. & Fuglsang, L. (2016). *Trust, organizations and social interaction : studying trust as process within and between organizations*. Edward Elgar Publishing.

Johannessen, A., Christoffersen, L. & Tufte, P. A. (2021). *Introduksjon til samfunnsvitenskapelig metode* (6. utg.). Abstrakt forlag.

Kaschner, H. (2022). *Cyber Crisis Management : The Practical Handbook on Crisis Management and Crisis Communication*. Springer Fachmedien Wiesbaden GmbH.

Knight, R. & Nurse, J. R. C. (2020). A framework for effective corporate communication after cyber security incidents. *Computers & Security*, *99*, 102036. https://doi.org/https://doi.org/10.1016/j.cose.2020.102036

Kuipers, S. L. & Schonheit, M. (2022). Data breaches and effective crisis communication: a comparative analysis of corporate reputational crises. *Corporate Reputation Review*, *25*, 176–197. https://doi.org/https://doi.org/10.1057/s41299-021-00121-9

Kvale, S. & Brinkmann, S. (2017). *Det kvalitative forskningsintervju* (T. M. Anderssen & J. Rygge, Overs.; 3. utg.). Gyldendal akademisk.

Lakshmi, R., Naseer, H., Maynard, S. & Ahmad, A. (2021). *Sensemaking in Cybersecurity Incident Response: The Interplay of Organizations, Technology and Individuals*. Cornell University.

Macmanus, S. A., Caruson, K. & McPhee, B. D. (2013). Cybersecurity at the Local Government Level: Balancing Demands for Transparency and Privacy Rights. *Journal of Urban Affairs*, *35*(4), 451-470. https://doi.org/10.1111/j.1467-9906.2012.00640.x

Maitlis, S. & Sonenshein, S. (2010). Sensemaking in Crisis and Change: Inspiration and Insights From Weick (1988). *Journal of management studies*, *47*(3), 551-580. https://doi.org/10.1111/j.1467-6486.2010.00908.x

Mehdi, K. (2014). Cyber-Attack Attributes. *Technology Innovation Management Review*, *4*(11). http://timreview.ca/article/846

Mnemonic. (2022). *RAPPORT MIRT-2021-12 NFK: Nordland Fylkeskommune*. Mnemonic.

Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B. & Masood Siddiqui, A. (2021). Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis. *International journal of information management*, *59*. https://doi.org/10.1016/j.ijinfomgt.2021.102334 (Article 102334)

Nasjonalt digitalt risikobilde 2022. (2022). Nasjonal Sikkerhetsmyndighet. https://nsm.no/getfile.php/1312007-1664785983/NSM/Filer/Dokumenter/Rapporter/NDIG2022_online.pdf

Naughton, J. (2016). The evolution of the Internet: from military experiment to General Purpose Technology. *Journal of Cyber Policy*, *1*(1), 5-28. https://doi.org/10.1080/23738871.2016.1157619

NOU 2000: 24. (2000). *Et sårbart samfunn— Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet*. J.-o. politidepartementet. https://www.regjeringen.no/no/dokumenter/nou-2000-24/id143248/

Olmeda, J. A. (2008). A reversal of fortune: blame games and framing contests after the 3/11 terrorist attacks in Madrid. I A. McConnell, A. Boin & P. t Hart (Red.), *Governing*

after Crisis: The Politics of Investigation, Accountability and Learning (s. 62-84). Cambridge University Press. https://doi.org/DOI: 10.1017/CBO9780511756122.003

Pursianen, C. (2018). *The Crisis Management Cycle*. Routledge.

Resodihardjo, S. L. (2020). *Crises, Inquiries and the Politics of Blame* (1. utg.). Springer International Publishing: Imprint: Palgrave Macmillan.

Sapriel, C. (2021). Managing stakeholder communication during a cyber crisis. . *Journal of Cyber Security and Mobility*, *4*, 1-8.

Schnackenberg, A. K. & Tomlinson, E. C. (2016). Organizational Transparency: A New Perspective on Managing Trust in Organization-Stakeholder Relationships. *Journal of management*, *42*(7), 1784-1810. https://doi.org/10.1177/0149206314525202

Sikt. *Informasjon til deltakarane i forskingsprosjekt*. Hentet 04.01 fra https://sikt.no/informasjon-til-deltakarane-i-forskingsprosjekt

Spreitzer, G. M. & Mishra, A. K. (1999). Giving Up Control without Losing Control: Trust and its Substitutes' Effects on Managers' Involving Employees in Decision Making. *Group & organization management*, *24*(2), 155-187. https://doi.org/10.1177/1059601199242003

Tjora, A. H. (2018). *Viten skapt : kvalitativ analyse og teoriutvikling*. Cappelen Damm akademisk.

Umapathy, K. (2010). *Requirements to support Collaborative Sensemaking*. University of North Florida. https://www.researchgate.net/publication/228437674_Requirements_to_support_Collaborative_Sensemaking

Weick, K., Sutcliffe, K. & Obstfeld, D. (2005). Organizing and the Process of Sensemaking. *ORGANIZATION SCIENCE*, *16*, 409-421. https://doi.org/10.1287/orsc.1050.0133

Weick, K. E. (1988). ENACTED SENSEMAKING IN CRISIS SITUATIONS[1]. *Journal of management studies*, *25*(4), 305-317. https://doi.org/10.1111/j.1467-6486.1988.tb00039.x

Weick, K. E. (1995). *Sensemaking in organizations*. Sage.

Whittle, A., Vaara, E. & Maitlis, S. (2023). The Role of Language in Organizational Sensemaking: An Integrative Theoretical Framework and an Agenda for Future Research. *Journal of management*, 01492063221147295. https://doi.org/10.1177/01492063221147295

Willasen, T. E. (2022, 14.01.). *Dataangrepet mot Nordland fylkeskommune: Kan ikke utelukke personopplysninger på avveie (14.1.2022)* https://www.nfk.no/aktuelt/dataangrepet-mot-nordland-fylkeskommune-kan-ikke-utelukke-personopplysninger-pa-avveie-14-1-2022.50296.aspx

Yu, X., Shen, Y. & Khazanchi, D. (2022). Swift Trust and Sensemaking in Fast Response Virtual Teams. *The Journal of computer information systems*, *62*(5), 1072-1087. https://doi.org/10.1080/08874417.2021.1978114

8 Vedlegg

8.1 Vedlegg 1: Intervjuguide

Huskeliste i forkant:

- Lydopptaker / lyd blir tatt opp. Informer.
- Gjengi sentrale ting fra informasjonsskrivet: taushetsbelagte opplysninger unngås, frihet til å trekke seg.
- Pause midtveis.

Del 1: Informasjon om informanten

- Navn, alder, stilling.

    - Hvor lenge har du innehatt stillingen og vært i organisasjonen?

- Hva er/var dine hovedoppgaver?

- Hva er din bakgrunn? Har du utdanning / arbeidserfaring med IT, og IT-sikkerhet? Hva med krisehåndtering eller kommunikasjon?

Del 2: Organisasjonen

- Hvordan vil du beskrive din organisasjon sin plan for krisehåndtering på generelt grunnlag?

- Hvordan opplever du kompetansen på IT-sikkerhet i organisasjonen før angrepet?

    - Og i etterkant?

- Hvordan opplever du at ansatte i organisasjonen sin forståelse av IT-relaterte tjenester, og terminologi?

    - Hva med din egen?

- Var dette noe dere tenkte på da dere skulle håndtere krisen og kommunisere den?

Del 3: Før krisen

- Har dere noen gang opplevd dataangrep eller hatt øvelser?

- Hadde dere en plan i tilfelle dette skulle skje?

- Hadde dere også en kommunikasjonsstrategi i tilfelle dataangrep?

- Hvordan opplevdes disse faktorene i etterkant?

Del 4: Når krisen var i gang

- Når fikk du beskjed om dataangrepet?

- Hvordan ble beskjeden oppfattet av deg første gang du hørte om det?

    - Hva gjorde at du forsto alvoret?

    - Noen spesiell setning, metafor eller eksempel som gjorde at du forsto det?

- Hva var din første handling?

- Hva var organisasjonens første handling?

- Hvordan opplevde du krisestabens forståelse av det som foregikk? Virket det som alle var på samme linje, eller virket det som det var ulik forståelse av hva som skjedde?

    - Var det noe som oppklarte det?

- Hvordan påvirket det situasjonen?

Del 5: Tema: Krisehåndtering

- Var det en tydelig rolleavklaring i krisehåndteringen?

    - Fungerte dette?

- Oppsto det noen misforståelser eller konflikter under håndteringen?

- Var det noen elementer som gjorde at du forsto at angrepet var av såpass alvorlig art at nettet måtte stenges ned?

- Fortell gjerne litt om din opplevelse av håndteringen av dataangrepet.

Del 9: Tema: Krisekommunikasjon

- Hva var forskjellen på den interne og eksterne kommunikasjonen under hendelsen?

    - Hva var viktig å tenke på overfor de ansatte?

    - Hvilken effekt hadde det?

- Hvordan forholdt dere dere til kommunikasjonsstrategien?

    - Hvis avvik: hvordan og hvorfor?

- Ble det valgt en felles strategi for hvordan dere ønsket å formidle det som skjedde?

    - Hvordan kom dere frem til dette? Funket det?

- Hva opplever du var organisasjonens fokus når dere skulle formidle hva som hadde skjedd?

    - Ble det gjort noen bevisste valg for å forenkle?

    - Brukte dere metaforer?

        - Hvis så, hvilke?

        - Virket det?

    - Holdt dere noen informasjon tilbake?

        - Hva var avveiningen mellom åpenhet og tilbakeholde informasjon?

        - Virket det?

- Valgte dere å skylde på aktøren, eller å beklage selv?

    - Hva var grunnen til det valget?

    - Virket det?

- Hva var vurderingen om dere skulle gå ut offentlig med kilden til angrepet?

    - Hvorfor endte dere med den endelige avgjørelsen av dette?

- Hva var ditt fokus når du skulle kommunisere videre hva som hadde skjedd?

    - Hvordan ble det oppfattet?

- Hvordan opplevde du denne kommunikasjonshåndteringen virket?

    - Hva var bra / Hva ville du gjort noe annerledes neste gang?

Del 11: Etter krisen

- Ble det gjennomført noen form for evaluering av krisehåndteringen og kommunikasjonsstrategien i etterkant?

    - Hva kom dere her frem til?

- Endret din forståelse av alvorlighetsgraden seg underveis eller i etterkant?

    - I så fall, hvorfor?

- Hvordan har responsen fra interessenter vært?

- Drar dere noen lærdom på krisehåndteringen?

- Hva med i krisekommunikasjonen?

- I dine øyne – hva var det viktigste grepet dere gjorde innenfor krisekommunikasjon?

- Er det noe angående forståelsen av angrepet, krisehåndteringen eller kommunikasjon som jeg ikke har spurt om, som du tenker jeg bør få med?

Takk for din deltakelse!

8.2 Vedlegg 2: Meldeskjema til NSD

Sikt

Meldeskjema / Master: Samfunnssikkerhet. / Eksport

Meldeskjema

Referansenummer
128806

Hvilke personopplysninger skal du behandle?

- Navn (også ved signatur/samtykke)
- E-postadresse, IP-adresse eller annen nettidentifikator
- Lydopptak av personer
- Bakgrunnsopplysninger som vil kunne identifisere en person
- Politisk oppfatning

Beskriv hvilke bakgrunnsopplysninger du skal behandle

Stillingstittel og rolle ved organisasjon i offentlig sektor / arbeidssted.

Prosjektinformasjon

Prosjekttittel

Master: Samfunnssikkerhet.

Prosjektbeskrivelse

Masteroppgave om dataangrep i offentlig sektor.

Dersom personopplysningene skal behandles til andre formål enn behandlingen for dette prosjektet, beskriv hvilke

Ikke aktuelt.

Begrunn hvorfor det er nødvendig å behandle personopplysningene

- Hvilken rolle ledelse spiller i krisesituasjoner.
- Hvem som sitter med ansvar.

Ekstern finansiering
Ikke utfyllt
Type prosjekt
Studentprosjekt, masterstudium

Kontaktinformasjon, student
Einar Lohne Bjøru, ebj065@uit.no, tlf: 41214542

Behandlingsansvar

Behandlingsansvarlig institusjon
UiT Norges Arktiske Universitet / Fakultet for naturvitenskap og teknologi / Institutt for ingeniørvitenskap og sikkerhet

Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)
Christer Pursianen, christer.h.pursiainen@uit.no, tlf: +4777660387

Skal behandlingsansvaret deles med andre institusjoner (felles behandlingsansvarlige)?
Nei

Utvalg 1

Beskriv utvalget

Ledere, politisk og administrativt, ved statlig organisasjon.

Beskriv hvordan rekruttering eller trekking av utvalget skjer

Rekrutteres via kontaktperson i organisasjonen, med kjennskap til hvem som er relevant for forskningsspørsmålet. Hvert enkelt individ i utvalget får da en personlig henvendelse, med infoskriv om oppgaven og bes skrive under på deltakelse.

Alder
22 - 70

Personopplysninger for utvalg 1

- Navn (også ved signatur/samtykke)
- E-postadresse, IP-adresse eller annen nettidentifikator
- Lydopptak av personer
- Bakgrunnsopplysninger som vil kunne identifisere en person
- Politisk oppfatning

Hvordan samler du inn data fra utvalg 1?

Personlig intervju

Vedlegg

Intervjuguide.docx

Grunnlag for å behandle alminnelige kategorier av personopplysninger
Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)

Grunnlag for å behandle særlige kategorier av personopplysninger
Uttrykkelig samtykke (Personvernforordningen art. 9 nr. 2 bokstav a)

Redegjør for valget av behandlingsgrunnlag

Informasjon for utvalg 1

Informerer du utvalget om behandlingen av personopplysningene?
Ja

Hvordan?
Skriftlig informasjon (papir eller elektronisk)

Informasjonsskriv

Samtykkeerkl_ring forskningsprosjekt_ny.docx

Tredjepersoner

Skal du behandle personopplysninger om tredjepersoner?
Nei

Dokumentasjon

Hvordan dokumenteres samtykkene?

- Manuelt (papir)

Hvordan kan samtykket trekkes tilbake?

Samtykket kan trekkes tilbake ved å ta kontakt med meg.

Hvordan kan de registrerte få innsyn, rettet eller slettet personopplysninger om seg selv?

Informantene kan få innsyn, rettet og slettet opplysninger om seg selv ved å ta kontakt med meg.

Totalt antall registrerte i prosjektet
1-99

Tillatelser

Skal du innhente følgende godkjenninger eller tillatelser for prosjektet?
Ikke utfyllt

Behandling

Hvor behandles personopplysningene?
- Maskinvare tilhørende behandlingsansvarlig institusjon

Hvem behandler/har tilgang til personopplysningene?
- Student (studentprosjekt)
- Prosjektansvarlig

Tilgjengeliggjøres personopplysningene utenfor EU/EØS til en tredjestat eller internasjonal organisasjon?
Nei

Sikkerhet

Oppbevares personopplysningene atskilt fra øvrige data (koblingsnøkkel)?
Ja

Hvilke tekniske og fysiske tiltak sikrer personopplysningene?
- Personopplysningene anonymiseres fortløpende
- Andre sikkerhetstiltak

Hvilke

Dataene vil bli avidentifisert. Det innebærer at navnet og kontaktopplysningene til informantene
vil bli erstattet med en kode som lagres på egen navneliste adskilt fra øvrige data.
Dataene skal oppbevares trygt bak to låsbare enheter. I forhold til forrige punkt om hvor opplysningene skal behandles, er jeg litt usikker på om det blir på maskinvare tilhørende behandlingsansvarlig institusjon eller på private enheter. Dersom det blir på private enheter skal det, som tidligere nevnt, i samsvar med personopplysningsloven oppbevares bak to låsbare enheter (låst skap og låst dør).

Varighet

Prosjektperiode
01.01.2023 - 01.06.2023

Hva skjer med dataene ved prosjektslutt?
Data anonymiseres (sletter/omskriver personopplysningene)

Hvilke anonymiseringstiltak vil bli foretatt?
- Personidentifiserbare opplysninger fjernes, omskrives eller grovkategoriseres
- Lyd- eller bildeopptak slettes

Vil de registrerte kunne identifiseres (direkte eller indirekte) i oppgave/avhandling/øvrige publikasjoner fra prosjektet?
Ja

Begrunn

Personer vil ikke kunne bli identifisert med navn, men organisasjonen som er case vil være navngitt. Derfor vil det være kjent at personene er blant ledelsesaktørene i denne organisasjonen under kriser. Det vil dog ikke bli kjent hvilken leder som gir hvilken informasjon.

For å holde dette etisk forsvarlig, gjøres det oppmerksom på i informasjonsskrivet, gjennom punktet anonymisering:

"Anonymisering

Gjennom forskningsetiske prinsipper skal deltagere i studier være anonymisert i tilstrekkelig grad. Dette vil etterstrebes, men rolle og arbeidssted vil være nødvendig å sitere for å kunne beskrive hvilken rolle man hadde i situasjonen som utfoldet seg under angrepet.

Ved samtykke til dette, blir det gitt mulighet til å få oversent transkribert intervju som skal benyttes til forskningen, og evt. komme med rettelser, tilbakemeldinger – eller trekke intervjuet, før videre arbeid med studien blir utøvd".

Tilleggsopplysninger

Ang. politisk oppfatning: En av organisasjonene som forespørres å stille med informanter, har en struktur som gjør øverste leder til en politisk figur.

8.3 Vedlegg 3: Forespørsel til Nordland fylkeskommune

Forespørsel til Nordland Fylkeskommune:

I hht. fremdriftdsplan for levering av oppgave, er datainnsamling satt til desember/januar.

Med forståelse for at fylkesting avholdes i starten av desember, foreslår jeg dager påfølgende uke som forslag til start. Dette er satt opp i tabell under. I stedet for bestemte dager, forsøker på å gi spillerom på uker. Nærmere tidspunkt kan jeg avtale med intervjuobjekt, om ikke det allerede er noen ønsker som foreligger.

Et intervju har tidsramme på 1 time, men kan også ta kortere/lengre tid, alt avhengig av tidsplan til intervjuobjekt og informasjonsinnhold.

Når det gjelder intervjuobjekter, har denne oppgaven et ledelsesfokus på krisehåndtering. Derfor er jeg interessert i å snakke med de som har stillinger som innbefatter en rolle krisestab. Dette inkluderer både administrativ og politisk ledelse. Jeg er også interessert i å intervjue de som oppdaget dataangrepet, og kommunikasjonsansvarlig i organisasjonen.

Datoer	Navn og stilling	Evt. forslag til dato
12.- 16. desember		
19.- 23. desember		
2.- 6. januar		

Skulle ikke disse datoene passe for relevante aktører, er det ingen problem å finne alternative datoer for min del.

I tillegg til intervju, benytter jeg dokumenter for analyse. Dette er eksempelvis pressemeldinger og nyhetsartikler som ligger ute. Skulle dere ha dokumenter, som interne mailer, tekstmeldinger eller andre dokumenter som kunne vært relevant mtp. krisehåndtering og -kommunikasjon, og som ikke er unntatt offentlighet, er jeg også interessert i dette.

Jeg sier takk for at dere ønsker å delta i dette prosjektet, og ser frem til å dele resultatet med dere etter levering av masteroppgaven.

Mvh

Einar Lohne Bjøru
Student, Samfunnssikkerhet v/ UiT Norges Arktiske Universitet

8.4 Vedlegg 4: Samtykkeerklæring

Samtykkeerklæring til forskningsprosjekt

«Krisehåndtering og kommunikasjon: Dataangrep i offentlig sektor»

Av Einar Lohne Bjøru, masterstudent i Samfunnssikkerhet v/UiT Norges arktiske universitet.

Du har blitt forespurt om å delta i en masterstudie som omhandler dataangrep i din virksomhet, eller en virksomhet du hadde tilknytning til når dataangrepet fant sted. Studien ser på krisehåndtering, og et spesielt fokus på kommunikasjon. Studien skal undersøke hvilke faktorer i kommunikasjonen i ledelsen som gjorde at man forsto alvoret i situasjonen, og hvordan man valgte å håndtere informasjonen videre til interessenter. Studien gjennomføres som en del av masteroppgave i studiet Samfunnssikkerhet, ved institutt for teknologi og sikkerhet ved UiT Norges arktiske universitet.

Frivillig deltakelse

Å delta i studien baserer seg på frivillighet. Du som informant kan derfor trekke deg fra deltakelse i studien på hvilket som helst tidspunkt, som også innebærer retten til å avbryte i intervjusituasjon – samt trekke tilbake informasjon.

Intervju og taleopptak

Intervjuet er planlagt til å ta maks 1 time. I intervjusituasjon vil taleopptaker bli benyttet, for deretter å bli transkribert. Dette for å kunne sitere det som blir sagt på en nøyaktig måte. I ettertid vil opptakene av intervjuet bli ivaretatt på ekstern harddisk og kun i forskerens eie. Det samtykkes dog til at veileder Christer Pursianen, professor ved UiT Norges Arktiske Universitet, vil kunne ha tilgang til transkriberingen for å kunne utfylle sin rolle på best mulig måte. Etter innlevering av masteroppgaven, vil opptakene bli slettet (juni 2023).

Anonymisering

Gjennom forskningsetiske prinsipper skal deltagere i studier være anonymisert i tilstrekkelig grad. Dette vil etterstrebes, men yrkestittel og arbeidssted vil være nødvendig å sitere for å kunne beskrive hvilken rolle man hadde i situasjonen som utfoldet seg under angrepet. Ved samtykke til dette, blir det gitt mulighet til å få oversent transkribert intervju som skal benyttes til forskningen, og evt. komme med rettelser, tilbakemeldinger – eller trekke intervjuet, før videre arbeid med studien blir utøvd.

Taushetsbelagte opplysninger

Oppgaven er ikke ute etter å få informasjon som er taushetsbelagt.

Personopplysninger

Ved å samtykke til å delta som informant, vil du få rett til å sende klage til personvernombudet eller datatilsynet hvis du mener behandlingen av dine personopplysninger ikke er tilfredsstillende.

Så lenge du kan identifiseres i datamaterialet, har du rett til[4]:

- innsyn i hvilke opplysninger som handler om deg, og å få utlevert en kopi av opplysningene
- å få rettet opplysninger om deg som er feil eller misvisende
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Ved å skrive under på dette dokumentet, er du kjent med overnevnte informasjon.

Kryss av for om yrkestittel/stilling og arbeidssted kan benyttes i oppgaven:

Ja O Nei O

Kryss av for om fullt navn, i tillegg til yrkestittel/stilling og arbeidssted, kan benyttes i oppgaven:

Ja O Nei O

Jeg er blitt kjent med informasjonen rundt oppgaven, og gir herved mitt samtykke til å delta i intervjuet:

---

[4] Utarbeidet fra Sikts mal for informasjonsskriv Sikt. *Informasjon til deltakarane i forskingsprosjekt*. Hentet 04.01 fra https://sikt.no/informasjon-til-deltakarane-i-forskingsprosjekt.

Sted og dato _____

Signatur _____