Masteroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for samfunns- og utdanningsvitenskap
Institutt for sosiologi og statsvitenskap

Marie Berntsen

Digital sikkerhet i offentlig sektor

En komparativ studie av digital sikkerhet i kommuner i Trøndelag

Masteroppgave i Organisasjon, digitalisering, administrasjon og arbeid
Veileder: Barbara Krystyna Zyzak
Juni 2023

NTNU
Kunnskap for en bedre verden

Marie Berntsen

Digital sikkerhet i offentlig sektor

En komparativ studie av digital sikkerhet i kommuner i Trøndelag

Masteroppgave i Organisasjon, digitalisering, administrasjon og arbeid
Veileder: Barbara Krystyna Zyzak
Juni 2023

Norges teknisk-naturvitenskapelige universitet
Fakultet for samfunns- og utdanningsvitenskap
Institutt for sosiologi og statsvitenskap

NTNU
Kunnskap for en bedre verden

Sammendrag

Digital sikkerhet har fått mer oppmerksomhet etter at krigen i Ukraina førte til et økt trusselnivå. Hybride trusler vil prege fremtiden, hvilket gjør at offentlig sektor må forberede seg på uforutsette hendelser. Grunnet hyppig angrepsaktivitet ser kommuner seg nødt til å vektlegge digital sikkerhet i større grad. Østre Toten kommune opplevde blant annet et omfattende digitalt angrep. Dette har skapt en årvåkenhet ellers i sektoren. Formålet med oppgaven er å undersøke et digitalt sikkerhetsarbeid med tre caser i den kommunale sektoren.

Oppgaven undersøker hvordan menneskelig kompetanse kan imøtekomme dagens risikobilde. Deretter vurderes bruken av teknologi for å nå sikkerhetsmålene. Målet for oppgaven er også å avklare hvilke tiltak lederne har arbeidet med for å bedre sikkerheten. Informantenes synspunkter om arbeidet bidrar til å belyse tiltak og endringer utløst av dagens risikobilde. Oppgaven tar i bruk et teoretisk sikkerhetsperspektiv ved navn MTO. I tillegg involverer det teoretiske rammeverket litteratur om *digital governance* og resiliens. Masteroppgaven bygger på en komparativ studie, hvor semi-strukturerte intervjuer og en dokumentanalyse er benyttet. Dette fungerer som primær- og sekundærdata for oppgaven. Totalt ble ti informanter intervjuet. Funnene blir analysert på en tematisk måte, fordelt på tvers av menneskelige, teknologiske og organisatoriske faktorer. Dette skal bidra til å vurdere det digitale sikkerhetsarbeidet i et helhetlig rammeverk.

Resultatene indikerer at kommunene sliter med å tilpasse seg et helhetlig arbeid som sørger for god sikkerhetsstyring og internkontroll. Kapasiteter og ressurser varierer, og dette kan skape utfordringer for kommuner i å håndtere digital transformasjon og komplekse systemer. Likevel indiker funnene at flere tiltak er iverksatt, som opplæringskampanjer og innstramminger på teknisk nivå. Dette kan vurderes som fremskritt i arbeidet med digital sikkerhet. Studiet anbefaler at kommunene bør ha et mer bevisst forhold til læring og risikostyring. På denne måten kan de enklere se verdien av ulike sikkerhetstiltak som for eksempel beredskapsøvelser. I tillegg er det nødvendig å benytte en helhetlig tilnærming som fordeler ansvar til flere deler av organisasjonen enn kun IT-avdelingen. Avslutningsvis er det viktig å ivareta en åpen og tillitsfull kommunikasjon mellom ledere og ansatte for å etablere en sikkerhetskultur.

Abstract

Digital Security has recently received increased attention, particularly due to elevated cyber threats triggered by the war in Ukraine. Hybrid threats will shape the future, requiring the public sector to prepare for unforeseen events. The frequent occurrence of cyber-attacks has forced municipalities to recognize the importance of focusing more on digital security. For instance, Østre Toten municipality experienced a serious digital attack, and this raised awareness within the municipal sector.

This study examines how human competence can address the current risk landscape and evaluates how technology is utilized to achieve security goals. Consequently, the study aims to identify the measures implemented by leaders to improve the security. The views of the informants clarify the actions and changes prompted by the current risk landscape.

The study utilizes a theoretical security perspective called MTO (Human, Technology, Organisation). In addition, the theoretical framework involves other concepts such as digital governance and resilience. The master thesis is a comparative study, involving semi-structured interviews and a document study. The study therefore combines both primary and secondary data. A total of ten informants participated in the study. The findings are analyzed thematically across human, technological, and organizational factors to assess the work within digital security.

The results indicate that municipalities struggle to adapt a holistic work that ensures efficient security management and internal control. Capacities and resources vary, posing challenges for municipalities in handling digital transformation and complex systems. However, the findings suggest that several measures have been implemented, such as training campaigns and enhancing of the technical security. These measures can be regarded as progress in the field of digital security. The study suggests that municipalities should take a more conscious approach to learning, as well as risk management. Such an approach can enable them to recognize the value of various security measures, such as emergency drills. Additionally, it is necessary to adapt to a holistic approach that distributes responsibilities to multiple sections of the organization rather than solely rely on the IT department. Finally, it is crucial to maintain open and trusting communication between leaders and employees to establish a security culture.

Forord

Masteroppgaven markerer slutten på fem år som student på Norges teknisk-naturvitenskapelige universitet (NTNU). Arbeidet er en avsluttende oppgave på studieprogrammet master i «Organisasjon, digitalisering, administrasjon og arbeid» ved NTNU Dragvoll. Det har vært spennende og givende å tilhøre det første kullet noensinne på denne masteren. Jeg er takknemlig for at programmet ble opprettet og at det har gitt oss muligheten til å tilegne oss tverrfaglig kompetanse som er nyttig både for arbeidslivet og akademia.

Jeg kjenner på flere følelser idet jeg skriver dette forordet. Jeg har trivdes som student, og det blir trist å se min akademiske karriere gå mot slutten. Likevel venter nye erfaringer i jobben som rådgiver i Digitaliseringsdirektoratet. Jeg håper og tror at kunnskapen jeg har tilegnet meg gjennom masteroppgaven kan tas med videre inn i arbeidslivet. Det er motiverende å muligens kunne bidra til forskningsfeltet om digital sikkerhet, samtidig som det også kan være til nytte for aktuelle kommuner som oppgaven fokuserer på.

Selv om oppgaven er skrevet alene, er det mange som fortjener en takk for å ha hjulpet meg på veien. Først vil jeg takke mine medstudenter som jeg har blitt gode venner med. Takk for at dere har lært meg mye og for gode stunder både på lesesal, i lunsjpauser og i det «virkelige» livet.

Jeg vil også rette en takk til søster Line Berntsen og barndomsvenninne Agnes Linnea Gärtner Davidsen for korrekturlesing. Samt en takk til min studievenninne fra sosiologi-bachelor, Mona Eskeland som også har tatt seg bryet til å lese oppgaven og kommet med faglig råd og inspirasjon. Videre ønsker jeg å takke Markus Jacobsen for uendelig støtte, selv når alt jeg prater om er masteroppgaven. Takk til familien min som også har lyttet til mine resonnementer om temaet.

Jeg må også rette en stor takk til Elin E. Sotberg Harder, min tidligere sjef i sommerjobb i DigiTrøndelag. Det har vært en ære å skrive for Trondheim kommune. Elin har bidratt med rekruttering av informanter, «brainstorming» av problemstilling og fungert som en møtekoordinator. I tillegg var hun alltid tilgjengelig for å svare på mine spørsmål og bidro sterkt i at jeg kom tidlig i gang med arbeidet. Det har vært ekstra motiverende å skrive om den valgte tematikken når det også ble fremstilt som viktig for kommunene. Dermed rettes en stor takk til informantene som har deltatt. Jeg har oppnådd god forståelse av teamet, takket være deres ekspertise og erfaringer. Jeg setter stor pris på at dere har deltatt og investert tid i prosjektet.

Til slutt vil jeg takke min veileder Barbara Zyzak for å ha vist stor interesse i oppgaven og tatt alle mine ideer på alvor. Vi hadde allerede møter om oppgaven høsten 2022 da jeg var på utveksling i Firenze. Jeg må takke deg for motiverende tilbakemeldinger og for at du inspirerte meg til å jobbe målrettet. Som veileder og programleder på masteren har du delt mye av din kunnskap og dermed gjort meg trygg på egne akademiske evner.

Trondheim, juni 2023
Marie Berntsen

Innholdsfortegnelse

Figurer

Tabeller

Forkortelser

KS	Kommunesektorens organisasjon
MTO	Mennesker, teknologi og organisering
IKT	Informasjons- og kommunikasjonsteknologi
IKS	Interkommunalt samarbeid
OECD	Organisation for Economic Co-operation and Development
Digdir	Digitaliseringsdirektoratet
NSM	Nasjonal sikkerhetsmyndighet
IRGC	International Risk Governance Council
ROS	Risiko- og sårbarhetsanalyse

1. Innledning

Det er et større behov for nasjonal- og digital sikkerhet i verdenssamfunnet i dag, også blant kommunene i Norge. Nasjonal sikkerhet utfordres av teknologi-utviklingen fordi virksomheter blir avhengig av nye tjenester. Bevissthet og kompetanse om trussel- og risikobildet er for svak. Nasjonal sikkerhetsmyndighet (NSM) mener dermed at ledere i offentlig sektor har et stort ansvar (NSM, 2022). Økende digitale trusler sørger for signifikante økonomiske og sosiale konsekvenser for offentlige og private organisasjoner, men også for individer. Noen av disse konsekvensene er angrep i form av tjenestenekt og sabotasje, forstyrelser i systemer, finansielle tap, skade på organisasjoners rykte og mangel på tillit fra brukere (OECD, 2015). Pandemien bidro blant annet til å skape et historisk skifte av digital transformasjon. Det innebærer en prosess som tar sikte på å utnytte digitale data og nye teknologier, for å blant annet muliggjøre endringer og effektivitet i en organisasjon (Osmundsen, Iden & Bygstad, 2018). Hyppig bruk av hjemmekontorløsninger skapte nye utfordringer og muligheter. Pandemien og krigen i Europa har endret dagens sikkerhetspolitiske situasjon, hvor komplekse digitale verdikjeder gjør sårbarheter mer krevende å oppdage enn før (Riksrevisjonen, 2023; NSM, 2022a).

I dag har uønskede hendelser og sikkerhetsbrudd blitt daglige nyheter. Det eksisterer en sammenheng mellom den optimistiske diskursen om digital transformasjon og den langt mer pessimistiske opplevelsen av digital sikkerhet. Likevel har utfordringer fått mindre oppmerksomhet i forskningsfeltet (Grøtan, Antonsen & Haavik, 2022). Disse kontrastene bør utforskes nærmere da det er synlig at bak innføringen av ny teknologi følger et etterslep av beskyttelsestiltak. Det kan forstås som et regelvakuum der teknologien utvikler seg raskere enn lovverket (Bergsjø, Windvik, & Øverlier, 2020, s. 51). Dette er ikke bare et teknisk problem, men sosio-tekniske utfordringer. Organisasjoner må ha evnen til å håndtere kombinasjonen av gammel og ny teknologi, samt nye måter å arbeide på, i en verden preget av uforutsette endringer (Lips, 2020).

Dagens risikobilde

Kommunesektorens organisasjon (KS) publiserte i mars 2022 et infobrev om digital sikkerhet da det kan forventes «økt aktivitet av svindel, nettfisking og sosial manipulering i tiden fremover». KS og Kommunal- og distriktsdepartementet rådet derfor kommunene i Norge til å vurdere egen sikkerhet- og sårbarhetsituasjon (KS, 2022). I desember 2021 opplevde Nordland fylkeskommune at skadevare hadde trengt igjennom brannmuren til datasystemene. Dette gikk spesielt utover skolene i fylket og deres datasystemer, i tillegg havnet personinformasjon på avveie og fylkeskommunen var i flere uker uten digitale løsninger (Regjeringen, 2022; NRK, 2021). Østre Toten ble rammet av et omfattende løsepengevirus i januar 2021, som også fikk stor oppmerksomhet. Østre Toten kommune virket lite rustet til å møte digitale angrep og trengte hjelp til å utføre risikovurderinger. Mange ansatte måtte jobbe med penn og papir i lang tid. Det ble anslått at kommunen tapte omtrent 35 millioner kroner på angrepet, i tillegg fikk de et overtredelsesgebyr på fire millioner kroner av Datatilsynet. I undersøkelse av saken ble det funnet flere grunnleggende mangler i sikkerheten (NRK, 2021; Datatilsynet, 2022). Dette har trolig alarmert sikkerhetsbevisstheten i kommunal sektor, noe som vil undersøkes nærmere i oppgavens analysekapittel.

Flere angrep på kommuner har vært av omfattende karakter. I år avdekket politiet i Finnmark datainnbrudd eller forsøk på dette i flere kommuner. Sikkerhetsansvarlig i Hammerfest kommune poengterer at slike angrep har blitt den nye normalen, forskjellen fra tidligere er derimot at det er mindre «gutteromshackere» og at det nå kan være stater som står bak. Det eksisterer mer bevissthet på at «dataangrep kan være ledd i moderne krigføring» (Steine et al., 2023). Dette fenomenet, kalt *hybride trusler*, vil prege framtiden. Hybride trusler innebærer at angriper tar i bruk både konvensjonelle og irregulære trusler for å nå et mål. Målet kan blant annet være et ønske om å påvirke et valg gjennom propagandatrusler eller drive nettmanipulering gjennom cyberoperasjoner. Hybride trusler er utfordrende å håndtere fordi de kombinerer ulike elementer og kan være godt skjult. På denne måten hviskes det tradisjonelle skillet mellom fred og væpnet konflikt ut (NSM, 2022; Departementene, 2019).

Nasjonal agenda
Proposisjon 78 S fremmer behovet for å øke motstandsdyktigheten mot digitale angrep i kommunal sektor, med særskilt fokus på små og mellomstore kommuner. Dermed ble det foreslått endringer i statsbudsjettet. I 2022 satt Stortinget av totalt 50 millioner kroner til en styrking av IKT-sikkerhet i kommunal sektor. Forslagene er en reaksjon på krigen i Ukraina. Blant annet er en felles myndighetsportal et nytt initiativ til virksomheter og kommuner for å få råd om digital sikkerhet (Prop. 78 S (2021-2022), ss. 10-18). I februar 2022 ble det avholdt et møte med omkring 200 av landets kommuner. Det ble tydelig formidlet at digitale angrep på kommuner kan ha alvorlige konsekvenser. Kommunenes økonomiske utfordringer har gjort det krevende å tilstrekkelig sikre egne nettverk og systemer. Møtet la fram at det kan forventes flere digitale angrep i form av utpressing, såkalte løsepengevirus. Det er dermed satt av ressurser til å begrense digitale skader og skape en felles innsats blant kommunene (Justis- og beredskapsdepartementet & Kommunal- og distriksdepartementet, 2022).

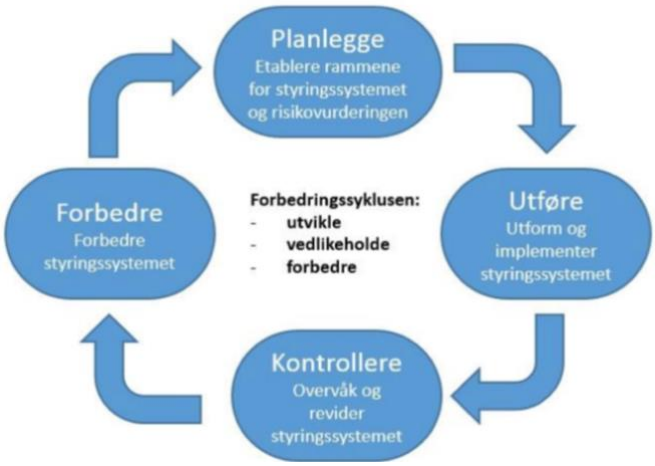
I februar 2023 ble det publisert en rapport av Riksrevisjonen som legger særlig vekt på ansvaret som justis- og beredskapsdepartementet har på samordningen mellom offentlige etater innenfor digital sikkerhet. De kritiserer arbeidet som departementet har lagt ned, særlig samordning av roller, ansvar og krav. Justis- og beredskapsdepartementet mangler oversikt over den nasjonale digitale sikkerhetstilstanden (Riksrevisjonen, 2023). Nivået av kritikkverdighet som rapporten utlyser synliggjør diverse utfordringer som kommuner måtte ha. Dette blir mer forståelig ettersom de øverste organene av samfunnet ikke ivaretar sitt pådriveransvar i arbeidet med digital sikkerhet.

1.1. Bakgrunn (standarder og veiledere)

Det eksisterer noe lovverk innen digital sikkerhet som vil være forekommende gjennom oppgaven (se forklaring i Vedlegg F). Digital sikkerhet har den siste tiden fått økende oppmerksomhet. 68% av statlige virksomheter og 65% av kommuner har opplevd diverse forsøk på identitetstyveri. Kommuner opplever også andre sikkerhetsproblemer: 19% har opplevd at virksomhetens IKT utstyr har kommet på avveie og 18% har erfart data-sammenbrudd (Digdir, 2022). I 2022 opplevde 16,4% av kommunene i Norge uautorisert tilgang til sine systemer (SSB, 2022). Mange brukere av offentlige tjenester er bekymret for at personlig informasjon skal komme på avveie. Dette kan forekomme idet en offentlig etat blir angrepet (Digdir, 2022). For å ivareta tillit til offentlig sektor, er det helt nødvendig å beskytte personlig informasjon.

I følge eForvaltningsloven §15 og anbefalinger av Digdir (2020) er det gunstig å være kjent med ISO standardene, spesielt 27000-serien. Den oppdaterte versjonen ISO27001 fra 2022 er er et dokument på 19 sider (ISO, u.d.). Grunnet standardens lengde og kompleksitet skal jeg ikke gå nærmere inn på dette, men heller oppsummere digitaliseringsdirektoratets internkontrollveileder som uthever det viktigste av ISO27001. Den sier blant annet at et styringssystem for informasjonssikkerhet skal sikre nødvendig konfidensialitet, integritet og tilgjengelighet til informasjonen til virksomheter. Innføringen av et styringssystem skal bygge på virksomhetenes ulike behov og mål, samt virksomhetens størrelse, struktur og arbeidsprosesser. For å oppfylle målene og kravene i lovverket om informasjonssikkerhet må en planlegge, implementere og kontrollere. Toppledelsen må sørge for at dette gjennomføres, og etablere en informasjonssikkerhetspolicy som inneholder tydelig mål og krav. Eksterne og interne aktører som er relevant i arbeidet bør redegjøres for. Ansvar skal være delegert utover i organisasjonen og styringssystemet skal dokumenteres (Digdir, u.d.).

Ifølge virksomhet-sikkerhetsforskriften §3 (2019) skal en virksomhet som omfattes av sikkerhetsloven etablere et styringssystem for sikkerhet. Likevel er offentlige virksomheter i Norge ikke pålagt å følge ISO-standarden (Digdir, u.d.) Figur 1 nedenfor er en illustrasjon på sikkerhetsstyring (NSM, 2021).



Figur 1: Nasjonal Sikkerhetsmyndighet (2021). *Veileder i sikkerhetsstyring.*

Justis- og beredskapsdepartementet mener NSM Grunnprinsipper for IKT-sikkerhet og digitaliseringsdirektoratets veileder er mest naturlig å rette seg etter (Riksrevisjonen, 2023). NSM har i flere tiår utviklet sikkerhetstiltak hvor grunnprinsipper for IKT-sikkerhet er organisert gjennom fire hovedområder: (1) Identifisere og kartlegge, (2) beskytte og opprettholde, (3) oppdage og (4) håndtere og gjenopprette. Den første kategorien innebærer å tilegne forståelse om virksomheten som styringsstruktur, ledelsesprioriteringer, leveranser, IKT-systemer og brukere. En slik oversikt er nødvendig for å kunne prioritere sikkerhetsbehov og risikostyring. Den andre kategorien handler om å opprettholde en sikker og trygg kommunikasjon mellom to systemer. Videre er det nødvendig å oppdage sårbarheter, trusler og etablere sikkerhetsovervåkning for å kunne fjerne kjente sårbarheter. NSM presiserer at målet er å stadig oppdage avvik fra normaltilstanden. Dermed bør normaltilstanden gjenopprettes ved at sikkerheten forbedres på grunnlag av tidligere erfaring (NSM, 2020).

1.2. Tema og formål

Oppgavens tema er digital sikkerhet i offentlig sektor. Formålet med masteroppgaven er å undersøke dagens arbeid med digital sikkerhet med særlig hensyn til kommuner i Trøndelag. Det er spesielt viktig å se hvordan ledere tilpasser seg dagens risikobilde og om de iverksetter endringer og tiltak på bakgrunn av dette. I startfasen av masterprosjektet ble det avholdt møter med samarbeidspartner i Trondheim kommune. I november 2022 og januar 2023 ble det gjennomført møter med ansatte fra Trondheim kommune, Fosen IKT, Midtre Gauldal kommune og KS. Oppgavens omfang ble diskutert og deltakere ble formelt invitert til intervju. Flere syntes oppgavens tema var interessant og ville gjerne være en del av prosjektet.

To begreper er spesielt viktige for temaet i masteroppgaven: digital sikkerhet og risiko. Risiko må ikke forveksles med krise, til tross for sammenhengen mellom dem. En krise er en alvorlig hendelse som medfører en endring fra normaltilstand til en hendelse med uønskede problemer. Det er en krevende situasjon som må løses med ressurser og organisering (Engen et al., 2021). Risiko er effekten av usikkerhet på diverse målsettinger. En tradisjonell beskrivelse av risiko innenfor økonomi og naturvitenskap er en matematisk kombinasjon mellom sannsynlighet og konsekvens (Engen et al., 2016). Innenfor samfunnsvitenskap og sikkerhetsmiljøer er en slik tilnærming lite tilstrekkelig. Det er nærmest umulig å sette et kvantifiserbart tall på når en trusselaktør går til angrep. Det er dog essensielt å ta hensyn til usikkerhet når en skal gjennomføre risikovurderinger. Ved å synliggjøre verstefallsscenario og adressere manglende informasjonsgrunnlag kan ledere ta bedre informerte avgjørelser (OECD, 2015; Bergsjø et al., 2020).

I denne masteroppgaven har jeg valgt å benytte begrepet *digital sikkerhet*, selv om begreper som *informasjonssikkerhet* og *cyber-sikkerhet* også er vanlig i dagligtalen og akademia. Jeg har valgt digital sikkerhet fordi det kan fungere som et overordnet begrep, og har tilhørighet med digital transformasjon. Begrepet digital sikkerhet vil nærmere redegjøres for i teorikapittelet. Følgelig vil oppgavens avgrensninger presenteres, samt hvilke spørsmål masteroppgaven skal forsøke å besvare.

1.3. Avgrensning, problemstilling og forskningsspørsmål

I denne oppgaven skal jeg undersøke hvordan arbeidet med digital sikkerhet i offentlig sektor fungerer, ved å ta utgangspunkt i to kommuner og et kommunesamarbeid i Trøndelag. Trondheim kommune, Midtre Gauldal kommune og Fosen IKT (interkommunalt samarbeid) har blitt med i prosjektet. Fosen IKT er en meta-organisasjon, da medlemmene er aktører fra andre organisasjoner (Ahrne & Brunossen, 2005). De tre casene blir derfor referert som organisasjoner i oppgaven. I tillegg inkluderes to representanter fra KS. Disse deltakerne reflekterer et bredt perspektiv på det digitale sikkerhetsarbeidet i kommunal sektor. KS er bindeleddet for landets kommuner og fylkeskommuner og har dermed god oversikt over diverse utfordringer kommunene møter. Samarbeidspartner ønsket å inkludere innspill fra KS. Dette kan leseren finne mer informasjon om i oppgavens metodekapittel.

Det som er utfordrende når en tar for seg et dagsaktuelt og komplekst tema er å avgrense oppgavens omfang. Oppgaven kunne hatt et nasjonalt fokus, men dette ble vurdert som noe ambisiøst for et selvstendig verk. Som nevnt er det også nødvendig å rette søkelys mot kommuner for å bedre den nasjonale sikkerheten. Det ble dermed gjort

et valg om å ta for seg kommunal sektor. Sikkerhet er et stort tema i seg selv, og kan overføres til mange ulike virksomheter og situasjoner. I lys av dagens risikobilde har det blitt valgt å vurdere sikkerheten i en digital sfære. Blant annet kan kultur, kryptografi, personvern, lover, programvare og overvåkning være sentrale emner (Bergsjø et al., 2020). Denne oppgaven har et mindre fokus på disse, og risiko har fått større plass. Med utgangspunkt i oppgavens tema og formål er følgende problemstilling formulert:

Hvilke endringer og tiltak har dagens risikobilde utløst i kommunal sektor?

Det tas utgangspunkt i tre hovedkategorier inspirert av et klassisk sikkerhetsperspektiv i litteraturen med navnet MTO-perspektivet (Schiefloe, 2017). I perspektivet vurderes menneskelige, teknologiske og organisatoriske forhold, hvordan disse spiller sammen og påvirker hverandre og sikkerheten i en organisasjon. Nye teknologiske løsninger fikk en større rolle i sikkerhetstenkning fra 1960-tallet. Det har vært særlig gjeldende for ingeniører og har hatt stor betydning for utviklingen av sikkerhet. Menneskelige faktorer ble mer sentralt utover 70-tallet og det er særlig kognitive begrensninger og hvordan mennesker håndterer systemene rundt seg som har engasjert forskningsbildet. Følgelig presiserer studier om organisatoriske forhold hvordan sikkerheten påvirkes av ledelse, samhandling og strukturering av arbeidet. Organisasjonsperspektivet ble mer gjeldende på 90-tallet (Kongsvik, 2013, s. 14). Perspektivet vil undersøkes nærmere i oppgavens teoridel. For å bidra til å svare på problemstillingen vil det utformes tre forskningsspørsmål som tar utgangspunkt i MTO-perspektivet:

1. Hvordan kan *menneskelig* kompetanse møte dagens risikobilde?
2. Hvordan benyttes *teknologi* for å nå sikkerhetsmålene?
3. Hvilke tiltak gjør lederne i *organisasjonen* for å forbedre sikkerhetsarbeidet?

Det valgte perspektivet er noe omfattende, men det er viktig å ta hensyn til alle de tre elementene. Perspektivet tyder på at uønskede hendelser best kan studeres med et helhetlig utgangspunkt, det vil si at det sjelden er kun én enkelt årsak som har forårsaket en situasjon (Kongsvik, 2013). Jeg skal se på temaet med en samfunnsvitenskapelig tilnærming, ikke et rent teknisk perspektiv. Dette vil nærmere redegjøres for i kapittelet om tidligere forskning. For å avgrense vil kategorien om mennesker vurdere effekten av kompetanse. Kategorien om organisering fokuserer på ledelse og tiltak. Videre vil kategorien om teknologi legge vekt på sikkerhetsmål i lys av digital transformasjon. Bruken av perspektivet var også et ønske fra samarbeidspartner.

1.4. Disposisjon

Videre vil kapittelet om tidligere forskning ta for seg digital sikkerhet først gjennom et internasjonalt og overordnet blikk, før tematikken spisses opp mot Norge og kommunal sektor. Deretter følger kapittelet om teori og begrepsavklaring. MTO-perspektivet, *digital governance* og resiliens vil utforskes nærmere. Oppgavens metodedel gir innsikt i de ulike metodiske valgene som ble tatt underveis, og i analysen blir de empiriske funnene presentert tematisk. I oppgavens diskusjon vil funnene fra intervjuene og en dokumentanalyse ses i lys av de teoretiske perspektivene. Deretter vil hovedfunn trekkes frem og benyttes til å besvare problemstillingen samt forskningsspørsmålene. Videre diskuteres oppgavens relevans og begrensninger. Avslutningsvis presenteres et forslag til videre forskning og anbefalinger til organisasjonene.

2. Tidligere forskning

I dette kapittelet vil jeg presentere tidligere forskning på digital sikkerhet, og utforske hvor det er behov for mer kunnskap. Digital sikkerhet vil bli undersøkt i en generell kontekst, men vil senere begrenses til å omhandle offentlig sektor. Det eksisterer mye forskning som er relevant for det utvalgte temaet. Nedenfor vil en se hvordan forskningsfeltet rundt digital sikkerhet har utviklet seg og blitt mer fremtredende. Deretter vil oppgaven snevre inn forskningen på nasjonalt og kommunalt nivå, som er viktig for å kunne besvare den endelige problemstillingen.

En systematisk litteraturgjennomgang har tatt for seg eksisterende forskning innenfor et spesifikt fagfelt eller tema (Christoffersen, Johannessen & Tufte, 2016). Tilgjengeligheten som internett og teknologi har sørget for gjør det enklere å finne eksisterende litteratur om diverse samfunnsvitenskapelige fenomener. Målet med en litteraturstudiet er å bidra med kunnskap og indentifisere forskningshull (Knopf, 2006). For å komme frem til relevant tidligere forskning har det blitt benyttet teoretiske og empiriske kilder, blant annet fra offentlige institusjoner i Norge som Riksrevisjonen og Digitaliseringsdirektoratet. I tillegg har jeg valgt å inkludere forskning fra internasjonale organisasjoner, som OECD og International Risk Governance Council (IRGC). Det er forskning om digitalt sikkerhetsarbeid som har fått størst oppmerksomhet i litteraturgjennomgangen. Risiko ses på som et viktig element innenfor dette. Kapittelet er delt inn i 3 nivåer: internasjonalt, nasjonalt og kommunalt. Prosessen bak litteratursøket vil nærmere redegjøres for i underkapittelet 4.2.4. om dokumentstudie.

2.1. Internasjonalt nivå

Den raske utviklingen av informasjons- og kommunikasjonsteknologi (IKT) fører til høy grad av integrasjon og kobling av systemer. Rasmussen (1997) skrev at mange studier har fokusert på de teknologiske farekildene, men det er like viktig å undersøke samspillet mellom de sosiale og teknologiske systemene i en organisasjon. Sosiologen Charles Perrow hevdet at ulykker er unngåelig, spesielt der organisasjoner må håndtere kompleks teknologi. Komplekse interaksjoner er forekommende i systemer der komponenter har flere funksjoner og derfor kan svikte i flere retninger samtidig. Mennesker forutser ikke disse interaksjonene, og når de først oppstår forstår de ikke hvordan de skal svare på dem. Hvis teknologien også er tett koblet, som vil si at feil forplanter seg raskt og uhindret gjennom hele systemet, vil feilene eskalere til en systemulykke. Perrow kalte dette *Normal Accident Theory* (Rijpma, 1997). Jeg skal dermed utforske interaksjonen mellom mennesker, teknologi og organisering, noe som er viktig for å forstå samspillet i komplekse systemer (OECD, 2015).

I kontrast til Perrows teori om normale ulykker viser *high reliability theory* at organisasjoner som har komplekse systemer kan benytte effektiv risikoreduserende strategi som redundans (Rijpma, 1997). Redundans kan være gjennom teknologiske reservesystemer i tilfeller der et system slutter å fungere (Schiefloe, 2017). Perrow mente at hovedutfordringen med komplekse systemer er at de krever både desentralisert og sentralisert ledelse på en og samme tid. Det er utfordrende å tillate operatører betydelig beslutningsmyndighet på den ene siden og sikre rigid kontroll og styring på den andre siden (Rijpma, 1997). I nyere forskning blir resiliens ansett som viktig. Blant annet tilsier litteraturen at ledere kan balansere regelstyring med tilpasningsevne. Resiliens er evnen et system eller en organisasjon har til å justere sin funksjon før, under eller etter

endringer og forstyrrelser, og på denne måten opprettholde nødvendige operasjoner (Hollnagel, Leonhardt, Licu, & Shorrock, 2015).

Videre har sikkerhet alltid vært en kritisk risikofaktor, mens digital sikkerhet og personvern har fått mer oppmerksomhet i nyere tider (IRGC, 2015). Internasjonal forskning presiserer at organisasjoner som er avhengig av digitale systemer må forberede seg på å oppleve hybride trussel-scenarioer (Loonam et al., 2022). Det er derfor et sterkt behov for forskning om organisatoriske prosesser som bedrer den digitale sikkerheten i dag. Grøtan et al. (2022) mener at bruken av sosio-tekniske perspektiver som MTO kan utnyttes mer. Det er også henvist til lite forskning på sammenhengen mellom digital transformasjon og digital sikkerhet som fagfelt. I tillegg tar resilienslitteraturen i liten grad opp lederansvar (Hollnagel, 2022). Jeg forsøker dermed å benytte MTO-perspektivet for å utforske de nevnte sammenhengene. Digital sikkerhet er ikke bare et teknisk problem, men en institusjonell og sosial utfordring (OECD, 2022a).

Det er mer behov for studier om roller og ansvar i offentlig sektor, da eksisterende litteratur ofte handler om privat sektor. Ved å avklare ansvarsfordelinger vil en enklere kunne adressere problemer ved risikostyring. En utfordring som dukker opp er at tradisjonelle målinger på risiko ofte er hentet fra banksektoren, noe som kan være krevende å overføre til andre sektorer (Ahmeti & Vladi, 2017). Det kan være utfordrende å finne sannsynligheten på risiko i en digital verden som stadig er i endring. Dessuten har teknologien innebygde sårbarheter som kan være vanskelig å oppdage før de blir utnyttet, såkalte nulldagssårbarheter (Bergsjø et al., 2020). Det internasjonale nivået peker på behovet for et bredere forskningsomfang, som også inkluderer tverrfaglig arbeid om organisatoriske, sosiologiske, økonomiske, juridiske og psykologiske faktorer så vel som teknologiske (IRGC, 2015). Forskningshullene tilsvarer en svak helhetlige forståelse og bruk av sosio-tekniske perspektiver, og manglende fokus på ansvaret som ledere har (Grøtan et al., 2022; Loonam et al., 2022; OECD, 2022a). Til slutt er det nødvendig med mer forskning som ser sammenhengen mellom digital transformasjon og digital sikkerhet. Masteroppgaven vil dermed forsøke å fylle disse hullene, ved å sette søkelys på ledelse og digital transformasjon i offentlig sektor gjennom et sosio-teknisk perspektiv.

2.2. Nasjonalt nivå

I Norge har det nylig vært observert at taktskifte i cyberaktivitet. Fra 2019 til 2021 har NSM sett en tredobling av antall alvorlige angrep (NSM, 2022). Almklov, Antonsen, Størkersen og Roe (2018) mener at det krever samarbeid mellom fagfolk for å skape en god digital sikkerhet. Informasjonsbeskyttelse, personvern, sikkerhet og pålitelighet må balanseres. En må kunne bevege seg utover de veletablerte siloene for sikkerhet, noe som utgjør en viktig forskingsutfordring innenfor vitenskaps-, ingeniør- og risikostyringsmiljøene. Norsk forskning utpeker også tilpasningsevne, resiliens som «den nye vinen innen sikkerhet» (Grøtan, 2017, s. 85). Grøtan fremhever at sikkerhet kan og bør integreres som en helhetlig del av ledelsen. I det ledelse knyttes til sikkerhet må en ta ansvar og forholde seg til noe som ofte er både ubehagelig og uønsket. Det er særlig viktig at ledere utvikler evnen til å kjempe videre etter et nederlag. Ledelsen har dermed et ansvar for å identifisere hva som gikk galt og iverksette tiltak som skaper gunstig endring. Dette kan skje dersom ledere utforsker en balanse mellom etterlevelse og tilpasningsevne og skaper et fleksibelt samspill med de ansatte (Grøtan, 2017).

Samhandling med systemer og personell utenfor egen organisasjon endrer mulighetene for koordinert arbeid. Dette samsvarer også med den nasjonale strategien om *én digital offentlig sektor* hvor «det digitale sikkerhetsperspektivet må sees i et helhetlig perspektiv, på tvers av sektorer og forvaltningsnivåer, og i sammenheng med det øvrige arbeidet for samfunnssikkerhet» (Kommunal- og moderniseringsdepartementet, 2019, s. 96). Ambisjonen om økt digitalisering i offentlig sektor henger derfor tett sammen med nasjonal strategi for digital sikkerhet (Departementene, 2019). Likevel er samordningen på nasjonalt nivå noe utfordrende. Rapporten fra Riksrevisjonen (2023) finner at statsforvalternes tilsyn med kommunene i liten grad omfatter arbeidet med digital sikkerhet. Justis- og beredskapsdepartementet har ikke hatt særlig oppmerksomhet på kommunesektoren. Det er dermed lite oversikt over hvem som skal ha særskilt ansvar for tilsyn av digital sikkerhet.

Tidligere sikkerhetsforskning i Norge benytter MTO-perspektivet, men omhandler som regel fysiske ulykker blant annet fra petroleumsindustrien, kjernekraftverk eller flykontrollsentre (Kongsvik, 2013; Schiefloe, 2017). Som presentert på internasjonalt nivå, krever digital sikkerhet å bli vurdert i lys av et helhetlig rammeverk. For å oppsummere ser en at tidligere forskning om digital sikkerhet i Norge også mangler bruk av sosio-tekniske perspektiver (Grøtan et al., 2022). Resiliens-begrepet har blitt en sentral del av sikkerhetsforskningen, særlig i sammenheng med forskning om ledelse. I tillegg er det gunstig å se forbi allerede etablerte siloer i offentlig sektor. Dermed er det et behov for mer forskning om dette for å nå målet om én digital offentlig sektor.

2.3. Kommunalt nivå

Grøtan et al. (2022) hevder at det er mer behov for empirisk forskning av mer «normale» eller «vanlige» organisasjoner som strever med forventningene og behovene som følge av digital transformasjon. Som nevnt har mye av fokuset ligget hos spesifiserte bransjer eller banksektoren. I denne oppgaven vurderer jeg en kommune for å være en såkalt «normal» organisasjon, men likevel kompleks. Tidligere forskning viser tendenser til svake sikkerhetsorganisasjoner og at mange kommuner mangler et styringssystem på informasjonssikkerhet (Digdir, 2020).

Rapporten fra Digdir (2020) poengterer at det er store forskjeller på kommuner. En stor andel av kommuner har et lite IKT-miljø som også skal løse mange andre oppgaver parallelt med sikkerhet. I tillegg er det observert mangelfull bevissthet på det særegne ansvaret som ledere har. Undersøkelsen av Riksrevisjonen (2023) viser at kommunene opplever sikkerhetsarbeidet som utfordrende, spesielt er mengder av ulike retningslinjer omfattende og delvis uoversiktlig. Når begrepsbruk varierer er det også utfordrende for den enkelte kommune å forstå hva som forventes av dem (Riksrevisjonen, 2023).

Digdir (2020) mener at kommunene bør innføre styrende dokumenter for å forankre ledelsene og skape internkontroll. Likevel kom det tydelig frem i Riksrevisjonen (2023) sin undersøkelse at flere kommuner finner det utfordrende og urealistisk å forholde seg til Digitaliseringsdirektoratets veiledning for internkontroll. Dette peker i retning av mangelfull organisering som muliggjør tid til å utvikle grundig styringsprosesser. Det er dermed behov for en undersøkelse som legger vekt på organisatoriske faktorer. Menneskelige og teknologiske elementer er viktig for å forstå de organisatoriske utfordringene og vurdere dette i et helhetlig rammeverk (Schiefloe, 2017).

2.3.1. Trøndelag

En undersøkelse gjort i regi av DigiTrøndelag viser at kommunene i Trøndelag har størst utfordringer med ressurser for sikkerhetsarbeidet. Blant annet er tid og ressurser for opplæring mangelfull. Rapporten nevner også at det er svært få som har implementert beredskapsplaner (Buan, 2021). Beredskap handler om å forberede seg på å håndtere ulike typer nødssituasjoner (Engen et al., 2021). Mangelfull opplæring er et interessant funn og det har dermed blitt valgt å se på kompetanse innenfor kategorien om mennesker. I tillegg er det ønskelig å gjøre en videre oppfølging av disse funnene, derfor har spørsmålet om beredskapsplaner også blitt inkludert i egen intervjuguide.

Digitaliseringsdirektoratet har sett funn som indikerer at spesielt små og mellomstore kommuner ikke har god nok internkontroll og styring på informasjonssikkerhet. Kommunestørrelse kan dermed ha betydning i arbeidet med informasjonssikkerhet. I tillegg gjennomfører store kommuner oftere aktiviteter som skal heve kompetansenivået på de ansatte (Riksrevisjonen, 2023). Et slikt funn styrker valget om å inkludere kommuner med ulike størrelser i masteroppgaven. På denne måten kan en få dypere forståelse for hva som utgjør forskjellene i kommunal sektor. På grunnlag av tidligere forskning fra DigiTrøndelag (Buan, 2021) ser en behovet for hjelpende tiltak og klare retningslinjer som kommunene kan benytte. Studien fant manglende bruk av overvåkningssystemer som kan oppdage inntrengingsforsøk og penetrasjonstester. Disse manglene har jeg valgt å plassere innenfor kategorien teknologi, og vil dermed følge opp noen av de tekniske utfordringene i samtale med informanter.

Buan (2021) viser at kun 32% av kommunene har en informasjonssikkerhetsleder, og av disse oppgir flertallet at en slik rolle er svært liten. En omfattende studie av Sopra Steria (2021) for informasjonssikkerhet og personvern i Trondheim kommune viser at roller og ansvar er noe uklart, der ansatte ikke alltid vet hvor eller til hvem de skal rapportere hendelser. Kommunen mangler organisatorisk prioritering på digital sikkerhet, noe som svekker Trondheim kommunes ambisjoner om digitalisering. Rapporten legger vekt på at informasjonssikkerhet tradisjonelt har vært forbundet med teknologi, noe som fortsatt preger organisasjonen. Det kreves en tydeligere sikkerhetskultur med rapportering, dokumentering og systematisering av risikovurderinger, noe som er avgjørende for en god internkontroll (Sopra Steria, 2021). Det er valgt å gi et ekstra blikk mot ledelsen og ansvarsfordelinger innen kategorien organisering. For å oppsummere viser tidligere forskning om kommunal sektor at utfordringer rundt digital sikkerhet er påvirket av kommunenes størrelse og tilgjengelige ressurser. Samtidig vil mangelfull organisering og sikkerhetsforståelse gjøre det krevende å prioritere tid til styring og internkontroll (Digdir, 2020; Riksrevisjonen, 2023). Dagens risikobilde setter digital sikkerhet på dagsorden. Likevel sørger forvirrende begrepsbruk og ulike retningslinjer for at kommunene strever med å finne gode organisatoriske løsninger.

2.4. Oppsummering

Kapittelet viser at digital sikkerhet nylig har fått et større fokus både internasjonalt og nasjonalt, og rikere forankring innen ulike forskningsmiljø. Samtidig er det nødvendig med organisatoriske og sosiologiske tilnærminger som inkluderer flere faktorer enn kun det teknologiske. Det er et behov for mer forskning på risikostyring i offentlig sektor, særlig på roller og ansvar. Samarbeid mellom fagfolk, ledere og bevegelse på tvers av siloer er sett på som viktig for å lykkes med en bedre digital sikkerhet. Dagens risikobilde legger føringer for endringer av sikkerhetsstyring og kommuner må være mer på vakt enn tidligere. Masteroppgaven skal bidra med kunnskap for å fylle de presenterte forskningshullene. Det kan dermed være viktig å kartlegge ulike utfordringer blant kommuner for å bedre den nasjonale digitale sikkerheten.

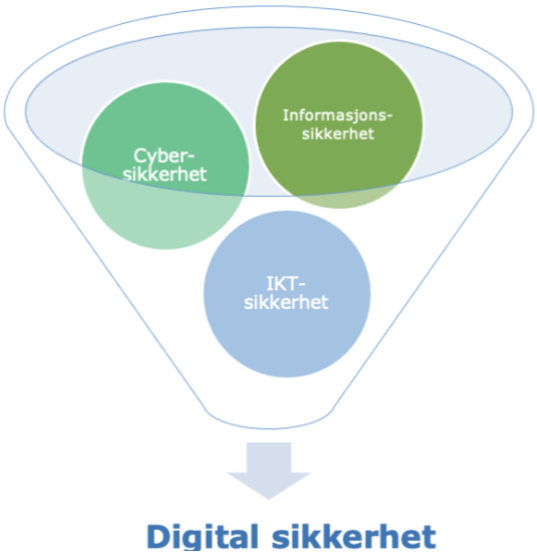
Leseren kan finne Tabell 1 i Vedlegg B som visualiserer og oppsummerer arbeidet med tidligere forskning. Funnet av disse referansene har skapt progresjon i videre datainnsamling for oppgavens teoridel. Flere av forfatterne vil være fremtredende videre i masteroppgaven. Blant annet er forskning av Grøtan et al. (2022), Loonam et al. (2022), Bergsjø et al. (2020), Kongsvik et al. (2018) og Hollnagel (2022) hyppig brukt.

3. Teori og begrepsavklaring

I dette kapittelet vil utvalgt teori og begreper danne grunnlaget for å besvare oppgavens problemstilling. MTO-perspektivet vil være sentralt gjennom hele oppgaven og sees i relasjon med temaet om digital sikkerhet. *Digital governance* er viktig for å forstå nye styringsinitiativer i offentlig sektor, og vurderer både positive og negative konsekvenser av digital transformasjon. Her vil ledelse, samskaping og risiko være sentralt. Resiliens forklares deretter for å belyse et fornyet blikk på arbeidet med sikkerhet, selv i en digital sfære. Masteroppgavens diskusjon i kapittel 6 vil bygge videre på den utvalgte teorien.

Det eksisterer noe begrepsforvirring innenfor digital sikkerhet som følgelig vil forklares nærmere. *IKT-sikkerhet* handler om «beskyttelse av IKT-systemene, samvirket mellom systemene, tjenestene som leveres av systemene eller informasjon som behandles i systemene» (NOU 2018:14, kap. 2). *Informasjonssikkerhet* innebærer sikring av informasjonens konfidensialitet, integritet og tilgjengelighet. Det vil si at informasjonen ikke blir kjent for uvedkommende, at informasjonen ikke blir endret og at det er tilgjengelig for autoriserte ved behov (Datatilsynet, 2018). Begrepet overlapper med cybersikkerhet, likevel vil cybersikkerhet inkluderer mer enn kun beskyttelse av informasjonsressurser (Loonam et al., 2022). Cybersikkerhet omfatter «tiltak for beskyttelse mot reelle og potensielle trusler som kanaliseres via IKT-infrastruktur» (Regjeringen, 2010, s. 21).

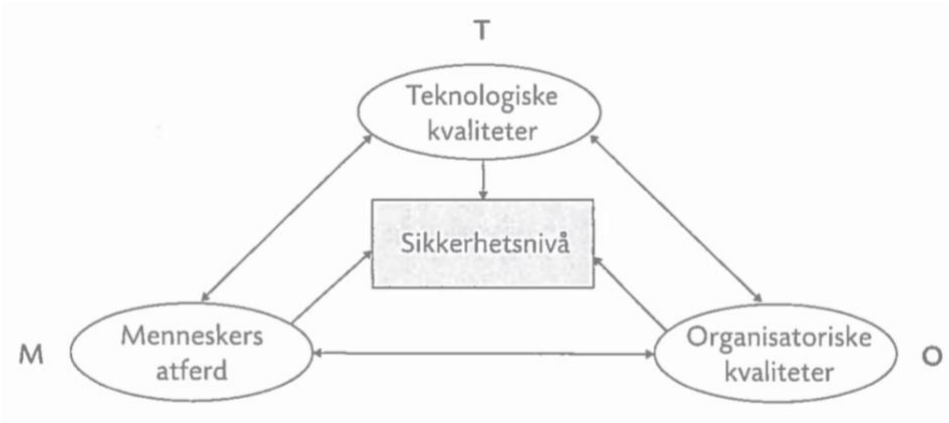
Begrepet *digital sikkerhet* benyttes i denne oppgaven fordi det kan fungere som et paraplybegrep for de ulike oppdelingene nevnt ovenfor (Figur 2). Begrepene brukes ofte synonymt med hverandre og kan derfor være vanskelig å skille. Digital sikkerhet handler om «beskyttelse av alt som er sårbart fordi det er koblet til eller på annen måte er avhengig av informasjons- og kommunikasjonsteknologi» (Bergsjø et al., 2020, s. 18). OECD benytter begrepet digital sikkerhet. Det brukes i stedet for cyber-sikkerhet da begrepet referer til økonomiske og sosiale aspekter ved cyber-sikkerhet, og ikke rent tekniske forhold. Begrepet «digital» har også sterk tilhørighet med digital transformasjon og digitale teknologier. Det handler om å skape tillit og maksimere muligheter fra IKT (OECD, u.d.). Målet med digital sikkerhet er å opprettholde sikkerhetsmålene om konfidensialitet, integritet og tilgjengelighet og å redusere uønskede hendelser til et akseptabelt nivå (Bergsjø et al., 2020, s. 21; OECD, 2022).



Figur 2: Egenlaget illustrasjon over begreper.

3.1. MTO-perspektivet

Det valgte perspektivet for denne masteroppgaven er MTO: Mennesker, teknologi og organisering (Schiefloe, 2017). Sikkerhet dreier seg om et samspill mellom slike forhold. Dermed vurderes det som gunstig å benytte MTO i oppgavens utforskning av digital sikkerhet i kommunal sektor. Elementene som inngår i en virksomhet, er relatert til hverandre og danner en helhet som skiller seg ut fra en organisasjon til en annen. En slik tenking legger føringer for at de ulike systemene i en virksomhet påvirker hverandre og er avhengig av hverandre. Målet ved å bruke et MTO-perspektiv er dermed at menneskelige, teknologiske og organisatoriske faktorer skal vurderes på lik linje (Kongsvik, 2013). Det har lenge vært akseptert at suksessen til organisasjonsaktiviteter bestemmes av hvor godt organisasjonen, menneskene og teknologien støtter hverandre, selv om denne ideen har fått ingen eller liten oppmerksomhet i det siste tiåret (Xu & Lu, 2022). Teorien til Perrow om normale ulykker gjorde at systemperspektivet ble aktualisert, spesielt for «inkluderingen av organisatoriske forhold» (Kongsvik, 2013, s. 78). Figuren nedenfor visualisere sammenhengen i MTO-perspektivet.



Figur 3: MTO-perspektivet funnet i Schiefloe (2017).

Figur 3 viser at det trengs et samspill mellom MTO for å opprettholde et akseptabelt sikkerhetsnivå. *Teknologien* er svært viktig for sikkerheten da den må være pålitelig og driftssikker (Schiefloe, 2017). I det digitale landskapet må også teknologien fungere som en barriere for å beskytte mot angrep. Digitalisering hjelper virksomheter med å bruke informasjonsteknologi. I tillegg sørger det for utnyttelse av gevinstene et digitalisert samfunn gir. Baksiden ved digitalisering er derimot mistillit til digitale tjenester og økende frykt for datakriminalitet (Bergsjø et al., 2020). Avgjørende for sikkerheten er blant annet at den teknologiske kapasiteten er tilstrekkelig og at det eksisterer redundans som ved bruken av reservesystemer (Schiefloe, 2017).

For å vurdere ulike nivåer som kan ha betydningen for sikkerheten er det nødvendig å undersøke de *menneskelige* faktorene. M-faktoren defineres som «atferd der utfallet av atferden kan ha direkte eller indirekte konsekvenser for sikkerheten i en operasjon eller aktivitet» (Schiefloe, 2017, s. 285). Rundt 1960-tallet ble det erkjent at en god tilpasning mellom teknologi og menneske var viktig for arbeidslivet. Tilpasningen skulle bedre arbeidsresultater innenfor områder som produktivitet, trivsel og sikkerhet (Kongsvik et al., 2018a). Mennesker er innebygd i sine organisasjoner, på den måten at de fungerer som kollektive aktører for å oppnå spesifikke mål, drive prosesser videre og etablere en kultur (Xu & Lu, 2022). Menneskelige feilhandlinger er noe som stadig omtales i

litteraturen. Tidligere forskning var opptatt av hvordan mennesker gjør feil, men har med tiden skiftet fokus til hvorfor mennesker gjør feil. Kompetanse og kunnskap kan trekkes frem som sentralt for å unngå feilhandlinger (Kongsvik et al., 2018a).

Ofte er det menneskelige feil en utpeker som hovedfaktoren for sikkerhetssvikt i en organisasjon, det er dog viktig å vurdere årsakene bak, i et mer helhetlig rammeverk. Slike bakenforliggende forhold faller ofte inn under O-faktoren, de *organisatoriske* forholdene. Det kan være manglende opplæring, uklare rutiner, utgåtte systemer, fraværende ledelse, manglende risikovurderinger, fraværende kommunikasjon eller svak sikkerhetskultur. Det kan være utfordrende å finne en forklaringsårsak på et sikkerhetsbrudd. I tillegg er sikkerhetsanalyser komplekse å utføre innen O-faktoren. En må se de organisatoriske faktorene i forhold til hverandre og vurdere hvordan de utgjør en felles organisatorisk kontekst (Schiefloe, 2017). Det krever inngående innsikt i en organisasjon for å vurdere samspillet mellom menneskelige, teknologiske og organisatoriske forhold. Kongsvik (2013) hevder at dette kan være en utfordrende oppgave som krever gode analytiske evner. MTO-analyser benyttes ofte i forbindelse med ulykkes-granskninger. Det er riktignok ikke dette som er formålet i denne masteroppgaven. Det er tydelig at MTO-tenking bidrar til å skape en helhetlig forståelse av strukturene i en virksomhet, som påvirker dets sikkerhetstilstand.

Videre vil **digital sikkerhet** ses i lys av MTO-perspektivet. Khando et al (2021) skriver at et stort antall av hendelser knyttet til digital sikkerhet skyldes utnyttelse av menneskelige svakheter som direkte eller indirekte forårsaker de fleste sikkerhetshendelser. Mange offentlige organisasjoner i dag støtter seg på digitale styringer og initiativer (digital governance). Det er dermed kritisk å øke de ansattes bevissthet rundt digital sikkerhet for å beskytte mot uønskede hendelser. Det er ikke nødvendigvis slik at digitale ferdigheter er noe en får gjennom utdanning. Opplæring er likevel viktig, og må prioriteres som et sikkerhetstiltak i organisasjoner (Bergsjø et al., 2020). Mennesket kan i realiteten fungere som en ressurs. Innenfor en resilient tankegang er mennesker helt nødvendig når noe uventet oppstår, da de har evnen til å benytte egen situasjonsforståelse for å tilpasse seg omgivelsene. Digitalisering har sørget for at kompleksiteten i mange systemer har økt. Dette kan ikke kun håndteres med satte prosedyrer, det krever også menneskelige evner (Kongsvik et al., 2018; Bergsjø, 2020). Digital transformasjon forsterker behovet for læring og kompetansebygging innad i organisasjoner, da menneskelige ferdigheter ikke overskygges av teknologisk utvikling (Grøtan et al., 2022).

Mange organisasjoner mislykkes i å beskytte seg mot angrep eller trusler fordi de kun lener seg på tekniske løsninger, likevel spiller teknologien en sentral rolle (Khando et al., 2021). *Phishing* og andre svindelteknikker er tilstedeværende trusler. Det kan sees på som en kontinuerlig kamp på ulike nivåer, der alt fra leverandører til nasjonale virksomheter kjemper mot individer som stadig finner opp nye tilnærminger for å utnytte sårbarheter (Grøtan et al., 2022). For å nå robusthet kan en benytte ulike teknologier som sikkerhetsovervåkning, identifikasjon og autentisering (Bergsjø et al., 2020). Det må også tas hensyn til organisasjoners evne til å håndtere kombinasjonen mellom gammel og ny teknologi, samt skape struktur i arbeidet rundt teknologien. Digital transformasjon forsterker forventningen om at uventede hendelser sannsynligvis ikke kommer i form av rene tekniske feil (Grøtan et al., 2022). Historisk sett har IT-avdelingen i en virksomhet hatt ansvar for den digitale sikkerheten. Et slikt ansvar kan i

dagens situasjon ikke lenger overholdes til IT-avdelingen alene, og et av de viktigste elementene i digital sikkerhet er kravet om risikostyring (Bergsjø et al., 2020).

En effektiv organisatorisk strategi kan fungere som et godt virkemiddel for å oppnå resiliens og styrke sikkerheten. Det bør derfor være tydelige forankrede roller og ansvar i organisasjonen for å etablere klare retningslinjer for de ansatte (Khando et al., 2021; Loonam et al., 2022). Ledelse er sentralt innen O-faktoren. Det er viktig at ledelsen sørger for opplæring av ansatte, generering av tillit, engasjement og strategiske mål. Videre er det viktig å skape organisatoriske verdier gjennom felles formål og samarbeid. På denne måten oppstår en sikkerhetskultur (Potrich, Selig, Matos, & Giugliani, 2022). I tillegg er lover og regler, sikkerhetstiltak og risikovurderinger viktige organisatoriske elementer som ledelsen må vedlikeholde (Bergsjø et al., 2020). Det er synlig at MTO-perspektivet kan bidra til å forstå komplekse utfordringer innenfor digital sikkerhet. Følgelig vil en utdypelse av *digital governance* utforske hvordan organisatoriske elementer blir påvirket av økende grad av digitalisering.

3.2. Digital Governance

Digitalisering og teknologiske innovasjoner har blitt en integrert del av hvordan offentlige organisasjoner styres i dag. Digitalisering er en forutsetning for digital transformasjon (Mergel, Edelmann & Haug, 2019; Lips, 2020) og kan forklares som «prosessen med å benytte digital teknologi til å endre på en eller flere sosio-tekniske strukturer» (Osmundsen, Iden & Bygstad, 2018, s. 10). *Digital governance* er et integrert system av sosio-tekniske dimensjoner og digitale regjeringsinitiativer. Bruken av digitale teknologier og data har stor påvirkning på myndigheters kjernefunksjoner, strukturer, prosesser og forhold til innbyggere, i tillegg til andre interessenter og virksomheter. Det gir rom for å tenke annerledes og implementere nyttige løsninger (Lips, 2021). Vellykket transformasjon av offentlige tjenester finner sted i organisasjoner med klare retningslinjer støttet av effektive ledere, høyt utdannede ansatte og aktive velinformerte borgere (Milakovich, 2022). Innenfor et *digital governance* er teknologi og arbeid godt inngrodd i hverandre og i uendelig endring. Denne sammenfiltringen av teknologisk fremgang og utviklingen av arbeidsprosesser er kjernen i vellykket digital transformasjon (Grøtan et al, 2022).

I en moderne styring kreves kompetente mennesker, robuste teknologier og organisatorisk forankring. Likevel er de fleste offentlige etater lite fleksible og mangler standardiserte styringssystemer. Ifølge den «nye normalen» ligger ikke ansvaret lenger hos teknologi-eksperter, men hos alle offentlige tjenesteansatte (Milakovich, 2022). I dag finnes en form for *hybrid digital governance*, det vil si at nye reformer og systemer blir kombinert med eldre systemer. Ledelse er en av de mest kritiske områdene for å lykkes i det hybride landskapet. Det innebære å håndtere nye problemer og barrierer. De må også skape kontroll over et komplekst nettverk, så vel som tilpasninger i og mellom systemer. Ledere bør muliggjøre samskaping mellom sektorer og på denne måten sørge for et læringsmiljø hvor de ulike aktørene kan skape effektive løsninger (Lips, 2021). Samskaping kommer fra det engelske ordet *co-creation*, og kan forstås som «[...] utviklingen av nye tjenester, produkter eller nye politiske tiltak, altså en form for innovasjon i fellesskap mellom flere aktører (Rommetvedt, 2023).

Wilson og Mergel (2022) forklarer at forskning om digital governance viser til en variasjon av barrierer. Strukturelle barrierer er spesielt fremtredende og inkluderer

teknologiske barrierer som kompleks infrastruktur, mangel på interoperabilitet og datatilgang. I tillegg finnes organisatoriske barrierer som mangel på strategi, menneskelige ressurser, digitale ferdigheter og kapasiteter til ledere. Silo-organisatoriske ordninger er også problematisk i en slik sammenheng (Almklov et al., 2018). Wilson og Mergel (2022) fant at kapasitet og ressurser er mest utfordrende. I tillegg strever offentlig sektor med å ansette folk med tilstrekkelig kompetanse, grunnet konkurranse med privat sektor. Kulturelle barrierer som fornektelse av risiko, manglene sikkerhetsbevissthet, byråkratisk kultur og frykt for forandringer preger offentlig sektor. Det er tydelig at digital governance har skapt muligheter for innovasjon, samskaping og utvikling i offentlig sektor. Likevel eksisterer flere barrierer og utfordringer som følge av en digital transformasjon. Følgelig vil masteroppgaven gå nærmere inn på et av barrierene, som også påvirker muligheten for gunstig intern- og styringskontroll, nemlig risikostyring (Digdir, u.d.).

3.2.1. Risikostyring

Risikostyring anses å være et verktøy for governance (styringsverktøy) som brukes til å støtte politiske valg og beslutningstaking. Risikostyring har kun blitt behandlet i minimal grad i akademisk litteratur, spesielt om implementeringen av risikostyring på ulike organisasjonsnivåer i offentlig sektor (Bracci et al., 2021). Den tradisjonelle forståelsen av risiko er: risiko = sannsynlighet x konsekvens. Risikonivået bestemmes av sannsynligheten for at en hendelse skjer og på bakgrunn av de mulige konsekvensene som en hendelse har. I flere arbeidslivsammenhenger kan dette være utfordrende (Kongsvik, 2013). Det vil være umulig å fjerne all risiko, og det vil alltid eksistere restrisiko (Ahmeti & Vladi, 2017). En mer pragmatisk forståelse av risiko er derfor fravær av uakseptabel risiko, der det er ønskelig å redusere risikoen til et akseptabelt nivå (Kongsvik, 2013).

Usikkerhet er en sentral dimensjon av risiko, særlig i forbindelse med en nyere forståelse av begrepet. Usikkerhet kan bekjempes med mer kunnskap; likevel er det ingen i vitenskapens lov som kan se inn i fremtiden. Derfor må en benytte etiske og politiske vurderinger for å kompensere for usikkerheten som eksisterer. Det er vanlig at organisasjoner utfører risiko- og sårbarhetsanalyser (ROS) som bygger på en fare som eksisterer, men slike analyser kritiseres for å bli for kompliserte til praktisk bruk (Engen et al., 2016). Det er likevel viktig å forstå at risiko ikke alltid peker mot uønskete hendelser. Noen kan se på et fenomen som en trussel, mens andre kan se på det som en mulighet. Derfor bør organisasjoner vurdere sine egne ferdigheter, mål og verdier for å definere hva risiko betyr for dem (Ahmeti & Vladi, 2017). Et samfunn preget av endringer skaper et behov for kontinuerlig oppdatering av kunnskap. Et felles språk og forståelse om sikkerhet hjelper den enkelte med å analysere mulige trusler. Risiko- og sikkerhetsarbeidet er dermed en kontinuerlig prosess som krever tilpasset planlegging, regulering og håndtering på tvers av fagfelt og arbeidsområder (Engen et al., 2016).

Risikostyring i offentlig sektor er komplekst, hovedsakelig som følge av det store utvalget av involverte parter og politisk innflytelse. Utfordringer som offentlig sektor møter på i forbindelse med risiko er blant annet ledere som mangler kunnskap om risikostyring og organisasjonsutvikling. I tillegg er begrenset risikokultur fremtredende (Amheti & Vladi, 2017). Det kan bemerkes at utfordringene med ledelse og svak risikokultur samsvarer med barrierene utpekt over (Wilson & Mergel, 2022). Likevel er risikostyring viktig for å oppnå strategiske mål og mer effektiv ressursbruk. Det bør gjøres ved å allokere risikoer til de som best kan håndtere dem, for eksempel gjennom offentlig-privat partnerskap. I

lys av disse bemerkningene er det nødvendig å utvikle en sikkerhetskultur som skaper større bevissthet om risikospørsmål hos alle aktører. Risikostyring bør bli en organisasjonspraksis som tillater organisasjonslæring. Med utgangspunkt i dette er det viktig å lære av egne feil for å fremme innovasjon i offentlig sektor (Bracci et al., 2021). Verdien av å lære er sentral i litteraturen om resiliens.

3.3. Resiliens

Resiliens er den kapasiteten et system har til å motstå og tilpasse seg forventede og uforventede forstyrrelser, og til å gjenopprette funksjonaliteten etter alvorlige påkjenninger (Hollnagel, 2022). Safety I og Safety II er to perspektiver som har preget sikkerhetsforskning. Perspektivene vil ikke være fokuset for denne masteroppgaven, da innholdet og oppgavens omfang må begrenses. Det er likevel nevneverdig at et skifte har oppstått hvor en er mindre opptatt av regler fra et Safety I perspektiv, og heller setter søkelys på å bygge resiliens i Safety II. Hovedpoenget er at en trenger balanse mellom regler (etterlevelse) og resiliens (tilpasningsevne) for å ivareta sikkerheten. Regler setter rammer for hva som er akseptabelt innen en organisasjon, det er likevel viktig at reglene gir rom for tilpasning. Ledere må dermed ha god forståelse av lovverket, for å unngå bøter og omdømmetap, men også for å vite når verdien av resiliens er nødvendig (Kongsvik, et al., 2018).

Resiliens-begrepet har gjennomgått endringer over tid, fra å fokusere på risiko og trusler til å omhandle hvordan systemer blir utført under skiftende omgivelser, inkludert ytelse under hverdagslige forhold (Hollnagel, 2022). Hollnagel (2009) introduserte fire evner for å operasjonalisere resiliens-begrepet. Den første utgjør potensialet til å *respondere* på forandringer, trussler og muligheter. For organisasjoner kan det være å annerkjenne oppståtte konflikter. Et resilient system tilpasser sin funksjon for å passe inn i de nye forholdene og responderer deretter. Den andre evnen er å *observere*. Observasjon skaper oversikt over endringer som kan påvirke en organisasjon både positivt og negativt. Den tredje evnen går ut på å *lære*, noe som er essensielt for å mestre alle de fire evnene. Dersom en ikke lærer fra tidligere hendelser, både det som gikk bra og galt, vil tilpasning og endringer mislykkes. Til slutt må en *forutse*, altså vurdere hva som kan skje i fremtiden. Når en forutser, bør en vurdere hvordan interne og eksterne forhold kan endre seg og hvordan dette kan påvirke organisasjonens opptreden. Hver evne er viktig i seg selv, men har størst effekt når de samhører med hverandre (Hollnagel, 2022).

Resiliens skal bidra til at menneskene utvikler nye ferdigheter og driver fram en organisasjonsutvikling (Bergsjø et al., 2020; Hollnagel, 2022). Digital transformasjon introduserer nivåer av kompleksitet og sårbarheter, og gjør at resiliens får fornyet kraft i dagens samfunn. Grøtan et al. (2022) mener at ved å plassere mennesker i sentrum for transformasjoner kan vi trolig oppnå et resilient samfunn. Digital transformasjon har mulighet til å endre og påvikre mennesker, organisasjoner og sammfunet for øvrig. I dag har digital transfomasjon en høy hastighet og er allestednærverende. Begrepet *cyber-resiliens* blir dermed relevant. Det er evnen til å reagere hensiktsmessig på forstyrrelser, opprettholde og redusere risikoen som følger av digital transformasjon. Problemet med digital transformasjon er at den ikke er demokratisk. Det kan dermed oppstå kamp om ressursene. Noen organisasjoner kan ha tilgang til de beste teknologiske løsningene, som lett kan fremskynde motstandskraft, mens andre må lære å være robuste uten hjelpemidler (Grøtan et al., 2022).

Grøtan (2017) stiller seg noe kritisk til assosiasjonene som forbindes med resiliens. Begrepet kan gi lite mening hvis det ikke forekommer en form for overraskelse som må håndteres. Det er ikke ønskelig at masteroppgaven skal fremme mindre ressursbruk på risikostyring og forebygging av kriser. Potensialet for resiliens krever initiering av ledelsen, forpliktende samarbeid og menneskelig intuisjon. Organisasjoner bør dermed sikre kontroll og planlegging, men være klar over at uforutsigbarheten som følger av digital transformasjon krever tilpasningsevne. Det kan ses i relasjon med Perrows krav om desentralisering og sentralisering i komplekse systemer (Rijpma, 1997).

3.3.1. Cyber-resiliens

Cyber-resiliens kan i enkel forstand forstås som å forbedre digital sikkerhet. Likevel forklarer Grøtan et al. (2022) at det mangler avklaring og avgrensning av begrepet som en handlingsteori. Cyber-resiliens har et fokus på sosio-teknisk praksis, styringsstrukturer og kulturelle betydninger av risikofellesskap, som sees i sammenheng med digital transformasjon (Grøtan et al., 2022). For å skape en kultur preget av resiliens innenfor digital sikkerhet må ledelsen sammen med de ansatte etablere et miljø preget av åpenhet og tillit, hvilket er essensielt for å bekjempe digitale trusler. Andre faktorer for å skape resiliens er å sørge for at digitale strategier er i tilhørighet med virksomhetens andre strategier og at resiliens vurderes som en viktig kompetansefaktor innen organisasjonen. Cyber-resiliens skal ikke behandles som et IT-prosjekt, da slike prosjekter kan forvitre når nye initiativer finner sted (Loonam et al., 2022).

MTO-perspektivet er relevant for cyber-resiliens, spesielt når en referer til beslutninger tatt av ledere, og hvilken effekt dette kan ha for den digitale sikkerheten. Ren teknologisk resiliens vil feile da den menneskelige faktoren er svært nødvendig. Selv ikke kunstig intelligens kan utfordre menneskelig erfaring og oppfinnsomhet som kreves for å forutse og håndtere uventede hendelser (Grøtan et al., 2022). En helhetlig forståelse av systemene er dermed elementært for å oppnå resiliens. Organisasjoner bør utvide eget nettverket ved å sikre at alle enheter forstår den digitale sikkerhetsstrategien og oppfyller standardene for å beskytte tjenestene. Videre må en sikre at *governance* strukturer er på plass og at ansvarsfordeling er tydeliggjort. Det er også strategisk å prioritere kritiske data og verdier. Dette kan gjøres ved å gjennomføre *benchmarking*-øvelser, som vil si å vurdere prosesser og praksis gjennom sammenligning med andre organisasjoner. De ansatte skal ha et direkte rapporteringsforhold til strategiske ledere. Dette gjør det mulig å kommunisere på en effektiv og åpen måte (Loonam et al., 2022).

Å utføre handlinger på en resilient måte kan tolkes ulikt. Dersom forsøket på resiliens mislykkes, bør ledere ha vurdert mulige samfunnskonsekvenser og ringvirkninger av skadeomfanget. Det skal dermed ikke hevdes at målet om resiliens er en enkel tilnærming for organisasjoner, men det er likevel viktig i en tid preget av digitalisering. Cyber-resiliens bør ifølge Grøtan et al. (2022) søke etter en balanse mellom realistiske ambisjoner om tilpasningskapasitet og teknologiske- og operasjonelle risikoer. På denne måten skal resiliens bidra til å identifisere en forsvarlig hastighet på digital transformasjon. Digital sikkerhet er ekstremt viktig for organisasjoner, med de mangler likevel kunnskap om hvordan ledere kan støtte mer effektive og resiliente prosesser (Loonam et al., 2022).

4. Metode

Formålet med dette kapittelet er å beskrive den metodiske fremgangsmåten som har blitt brukt i studien, og hvordan denne påvirker tolkningen av de empiriske funnene. Jeg vil også diskutere metodiske implikasjoner for å sikre prosjektets transparens, med hensikt om å gi leseren god innsikt i forskningen. På denne måten kan leseren ta stilling til og vurdere forskningens kvalitet (Tjora, 2018). Jeg vil først beskrive forskningstilnærmingen, deretter datagrunnlag og innsamling av data. Videre vil jeg redegjøre for det endelige utvalget av informanter, samt hvordan intervjuene ble gjennomført. Til slutt diskuteres den valgte analysen av dataen, i tillegg til at forskningens kvalitet vil vurderes. Masteroppgaven har fått godkjent forskningstillatelse av NSD (Vedlegg A).

4.1. Forskningstilnærming

Forskningstilnærmingen innebærer valg av metode og forskningsprosess. En viktig del av arbeidet med en empirisk forskningsstudie er å samle data om fenomenet som undersøkes. Datainnsamling kan foregå på en numerisk måte, gjennom spørreskjemaer og statistikk, kalt kvantitativ metode. I masteroppgaven er det derimot benyttet en kvalitativ tilnærming. Jeg har gjennomført semi-strukturerte intervjuer, i tillegg til at to informanter har blitt intervjuet samtidig, som faller innenfor kategorien fokus-gruppe (Johannesson & Perjons, 2014). Arbeidet med datainnsamling og informanter vil bli nærmere forklart i delkapittelet 4.2. Gjennom en dokumentstudie blir fire av de empirinære kildene i tidligere forskning inkludert (Tabell 4, kap. 4.2.4). To av dem er interne dokumenter som ble tilsendt av Trondheim kommune 15.11.2022. Blandingsmetoden som er valgt viser til prinsippet om triangulering, som handler om å se på det samme fenomenet fra ulike perspektiver (Johannesson & Perjons, 2014).

Det kan være vanskelig å kategorisere forskningstilnærmingen som enten deduktiv eller induktiv. Arbeidet med empiri startet tidlig da det ble avholdt introduksjonsmøter med informantene. Tidlig arbeid med empiri stemmer overens med en induktiv tilnærming (Midré, 2009). Likevel ble det foreslått å se på mennesker, teknologi og organisering. Jeg knyttet dette opp mot MTO-perspektivet. Det eksisterte dermed noen ideer om hva slags forskning og teorier som kunne blitt utforsket nærmere. Dette samsvarer med en deduktiv tilnærming (Knutsen, 2018).

En mer passende tilnærming til datainnsamlingen for denne oppgaven er en abduktiv metode, i og med at forskningsprosessen har vekslet mellom empiri og teori (Vassenden, 2018). Det kan derfor sies at jeg har vært inspirert av utsagnet om å ikke være en teoretisk ateist (induktiv tilnærming) eller monoteist (deduktiv tilnærming), men heller sikte mot å være en teoretisk informert agnostiker (abduktiv tilnærming) (Timmermans & Tavory, 2012, s. 169). Abduksjon skiller seg fra induksjon og deduksjon, men kombinerer trekk ved begge typer logiske slutninger. Det vil si at det observerte fenomenet ikke inneholder en forklaring i seg selv (induksjon), og det utgjør heller ikke et nytt tilfelle av en allerede kjent regel og/eller teori (deduksjon). Det forklares heller som en kombinasjon av begge tilnærmingene (Vila-Henninger et al., 2021). Denne tilnærmingen har skapt dynamikk i arbeidet og var et bevisst valg for å unngå å se seg blind på mengder med teori eller datainnsamling. Jeg har dermed vurdert det som positivt å heller arbeide med begge deler parallelt og stadig gjøre revurderinger på hva som egner seg best for oppgaven.

4.1.1. Komparativ case-studie

En case-studie fokuserer på én instans av et fenomen som skal undersøkes, i tillegg til å gi en dyptgående beskrivelse og innsikt i det som studeres (Yin, 2018). Kompleksitet er avgjørende for en vellykket case-studie, ettersom den undersøker flere faktorer, hendelser og relasjoner som oppstår i virkeligheten (Johannesson & Perjons, 2014). Masteroppgaven faller innenfor kategorien komparativ case-studie da de tre analyseenhetene (Tabell 2 i kap. 4.1.2.) sammenlignes opp mot hverandre. Et komparativt design innebærer å studere variasjoner ved å sammenligne flere caser (Bukve, 2021). Det er hovedsakelig de ulike sikkerhetstiltakene som vil sammenlignes. Å studere tre caser kan trolig styrke forskningsgrunnlaget, men det kan være utfordrende å oppnå en dyp forståelse for hver enkelt organisasjon. Beslutningen om å rette forskningen mot kommunal sektor kan derimot ha bidratt til en generell forståelse for hvordan kommuner arbeider med digital sikkerhet i dag.

I motsetning til flercasestudier vil en komparativ studie ikke bare se på fellestrekk, men også hvordan og hvorfor de varierer. I de fleste tilfeller bør en nøye seg med få caser, da det kan være krevende å utforske mange aspekter i en case (Bukve, 2021). Jeg har dermed vurdert tre caser som tilstrekkelig. To informanter fra KS har også blitt intervjuet, noe som kan bidra med flere perspektiver på kommuner i Norge. På denne måten kan forskningen trolig generaliseres i større grad, da flere synspunkter og erfaringer er inkludert. Som forsker kan en velge å studere kontrasterende eller homogene caser (Thiel, 2022). Valget om å inkludere en stor kommune, en mindre kommune og et kommunesamarbeid viser til kontraster i utvalget. Det gjør det mulig å se om variasjonene avhenger av kommunestørrelse eller andre faktorer. Denne strategien kalles *most similar/most different* (Seawright & Gerring, 2008). Utvalget er like ettersom de tilhører kommunal-sektor og jobber med digital sikkerhet, men er noe ulike i form av organisering og størrelse.

4.1.2. Presentasjon av case

Følgelig vil jeg kort presentere oppgavens caser med hensikt om å se størrelsesforskjeller blant organisasjonene. I denne oppgaven har jeg valgt å benytte en tredelt størrelsesgruppering av SSB. Små kommuner anses å ha mellom 0-4 999 innbyggere. Deretter har en mellomstor kommune mellom 5000-19 999 innbyggere. En stor kommune har minst 20 000 innbyggere (Kringlebotten & Langørgen, 2020). Trondheim er den største kommunen i dette utvalget (Trondheim Kommune, 2023). Midtre Gauldal anses som en mellomstor kommune (SSB, u.d.). Fosen IKT er et interkommunalt samarbeid (IKS). Fosen IKT har en aktiv rolle innen digitalisering og «de har ansvaret for å bygge opp og drifte felles IKT-infrastruktur» (Fosen IKT, u.d.). De fire kommunene som utgjør Fosen IKT er Osen kommune, Åfjord kommune, Indre Fosen kommune og Ørland kommune (SSB, u.d.). Fosen IKT består av et samarbeid mellom små- og mellomstore kommuner. De kan dermed belyse problemstillinger som berører alle de deltakende kommunene.

Organisasjon	Størrelse (innbyggertall)	Organisering
Trondheim kommune	212 660 (pr. 2023)	Kommune
Midtre Gauldal kommune	6 115 (pr. 2023)	Kommune
Fosen IKT	Osen kommune: 904 (pr. 2022) Åfjord kommune: 4 252 (pr. 2022) Ørland kommune: 10 472 (pr. 2022) Indre Fosen: 9 977 (pr. 2022)	Interkommunalt samarbeid (IKS)

Tabell 2: Masteroppgavens valgte caser med innbyggertall

4.2. Datagrunnlag og datainnsamling

Ifølge Johannesson og Perjons (2014) er semi-strukturerte eller ustrukturerte intervjuer bedre når en skal undersøke komplekse saker, da informanten kan utrykke sine tanker på en friere og mer ustrukturert måte. Som redegjort for i tidligere forskning er digital sikkerhet svært komplekst, spesielt når organisasjoner i stor grad er avhengig av teknologi (Grøtan et al., 2022). For å sikre et nyansert datagrunnlag som kan representere virkeligheten, ble det valgt å inkludere flere kommuner enn kun Trondheim kommune. En mindre kommune vil trolig ha andre utfordringer og forutsetninger i arbeidet med digital sikkerhet. Intervjuene fungerer som primærdata for oppgaven.

4.2.1. Utvalg og rekruttering

Rekruttering ble gjennomført fra midten av november 2022 til januar 2023. En svært behjelpelig samarbeidspartner fra Trondheim kommune fant de første informantene. I møter med disse informantene spurte vi om de kjente til andre mulige kandidater. Det ble dermed iverksatt en delvis snøballmetode for rekruttering. Det ble gjort et strategisk utvalg av informanter (Tjora 2018). Informantene som ble kontaktet har lederstillinger eller et særskilt ansvar innen sikkerhet. Blant annet har kommunale toppledere og IT-ledere blitt intervjuet. Jeg har likevel valgt å ikke spesifisere navnet på de ulike stillingene, grunnet anonymitet. De tre utvalgte casene har vist både engasjement og nysgjerrighet til den utvalgte tematikken om digital sikkerhet. Intervjuene ble utført i perioden 13.02.2023 – 06.03.2023. Det endelige utvalget består av 10 informanter (9 intervjuer).

4.2.2. Utforming av intervjuguide

Intervjuguiden ble utformet i flere etapper og revidert i samarbeid med veileder. Intervjuguiden er basert på de tre kategoriene som utgjør MTO-perspektivet. Innenfor kategorien om organisering ble det stilt flere spørsmål som ble strukturert i underkategorier: spørsmål om omgivelsene, spørsmål om samarbeid og spørsmål om ledelse. En tematisk inndeling gjør det lettere for både intervjueren og informantene å ha kontroll på spørsmålene (Tjora, 2018). I utviklingen av intervjuspørsmålene så jeg igjennom dokumenter tilsendt av samarbeidspartner. Det var informasjon fra NSM, KS, DigiTrøndelag og Sopra Steria som fungerte som hjelpemiddel. I tillegg tok jeg noe inspirasjon fra et spørreskjema fra Digdir sin *Veileder for kartlegging av digital sikkerhetskultur* (Digdir, u.d.). Utfordringen lå i å lage så åpne spørsmål som mulig (se Vedlegg D1/D2).

4.2.3. Gjennomføring av intervju

Når en gjennomfører et intervju, bør en være klar over at sine egne personlige interesser kan påvirke deltakerne. Informanter kan være mindre villig til å fullstendig oppgi informasjonen til noen som er veldig ulik dem selv. Dette kan for eksempel være i form av alder og kjønn (Johannesson & Perjons, 2014). Det er forskjeller mellom meg som forsker og de kommuneansatte, men den overordnede opplevelsen var likevel at informantene var åpne og villig til å dele. Ifølge OECD (2015) skal digital sikkerhet være basert på etiske forhold som respekterer og anerkjenner de legitime interessene til andre, og samfunnet som helhet. Organisasjoner bør dermed sikte mot å være transparente om deres praksis for håndteringen av digital sikkerhet.

De fleste intervjuene ble gjennomført digitalt over Microsoft Teams. To av intervjuene ble gjennomført fysisk. Det første tok sted på kontoret til informanten og det andre i et møterom hos Trondheim kommune. Dette er steder som informantene har god kjennskap til, noe som hadde til hensikt om å skape et nivå av komfort for deltakerne. De resterende syv intervjuene ble gjennomført digitalt, da dette var mest gunstig for deltakerne, som er både begrenset gjennom tid og geografiske avstander. Jeg vurderer ikke dette som noe negativt for forskningen. Det skal likevel nevnes at tekniske problemer som dårlig lyd er noe forekommende, som kan ødelegge flyten i intervjuet. Heldigvis oppsto slike problemer kun et fåtall ganger. Det kan også oppstå problemer når to informanter skal bli intervjuet sammen. Kandidatene i fokus-gruppe intervjuet har ulike stillinger, men jobber ofte sammen. De mente derfor at de kunne utfylle hverandre på de tre kategoriene (MTO). Fokus-gruppe tillater interaksjon mellom deltakerne, noe som gjør at de kan inspirere hverandre og tilføye hverandres tanker om temaet (Johannesson & Perjons, 2014). Informantene var dyktige på å la hverandre snakke og deretter formidle sine egne tanker.

Det er ønskelig at en kvalitativ tilnærming, bestående av 10 informanter (se Tabell 3), skal fungere som et verktøy for å utnytte systematisk bruk av MTO-perspektivet, i tillegg til å øke troverdigheten til masteroppgaven som helhet. Dette gjøres ved å stille et bredt spekter av åpne spørsmål til informantene (Tjora, 2018). Intervjuene ble tatt opp ved bruk av diktafon. Informantene ble opplyst om opptaket på forhånd og ble påmint dette rett før intervjuet startet. Tabellen nedenfor viser en oversikt over informantene, noe som gjør det lettere for leseren å forholde seg til informasjonen i analysen. Jeg velger å oppgi navn på kommunene ettersom deltakerne stiller som gode eksempler på åpenhet ved å ta del i forskningen. Andre virksomheter kan følge opp forskningen, ta kontakt og eventuelt høre om mulige fellesløsninger. I tillegg kan det være nyttig informasjon for et digitaliseringsnettverk som DigiTrøndelag, som arbeider med felles informasjonsutveksling for å oppnå et digitalt løft for kommunene i Trøndelag (DigiTrøndelag, u.d.).

Deltaker	Organisasjon	Samtaletid
Informant 1	Trondheim kommune	51 min
Informant 2	Trondheim kommune	1 t og 30 min
Informant 3	Trondheim kommune	42 min
Informant 4	Fosen IKT	59 min
Informant 5	Fosen IKT	50 min
Informant 6	Midtre Gauldal kommune	49 min
Informant 7	Midtre Gauldal kommune	60 min
Informant 8	Midtre Gauldal kommune	60 min
Informant 9	Kommunesektorens organisasjon (KS)	35 min
Informant 10	Kommunesektorens organisasjon (KS)	1 t og 20 min

Tabell 3: Oversikt over informanter

4.2.4. Dokumentstudie

En dokumentstudie fungerer som sekundærdata for masteroppgaven. Ved å bruke dokumenter som data kan en samle mer informasjon på kortere tid. Det kan derimot være vanskelig å bedømme dokumentenes troverdighet. Likevel er det statlige dokumenter og interne organisatoriske dokumenter som er benyttet, noe som anses som troverdig (Johannesson & Perjons, 2014). De fire utvalgte dokumentene til analysen utpekte seg i underkapittelet 2.3. om kommunal sektor og vil derfor ses i sammenheng med intervjuene. Arbeidet begynte med et litteratursøk som skapte grunnlaget for kapittelet om tidligere forskning. Litteratursøket har blitt gjennomført på digitale plattformer som Oria, Google Scholar og Scopus i perioden januar til mars 2023. For å samle inn informasjon ble det benyttet søkeord både på engelsk og norsk som «digital sikkerhet», «digital governance and risk management», «risikohåndtering» og «cyber security». Etter et bredt søk ble søkekriterier relatert til offentlig sektor benyttet. Jeg forsøkte å anvende artikler publisert fra 2015 og utover. Kun noen få eldre verk har blitt benyttet.

Masteroppgaven har favnet bredt i innhentingen av informasjon for å reflektere MTO-perspektivets omfang. Det har vært ønskelig å identifisere utfordringene som følger av økt digitalisering og behovet for mer sikkerhet. I tillegg til de elementer som faller innenfor de tre nevnte kategoriene. Det er dermed hentet inn litteratur fra ulike fagdisipliner for å vise til bredden i omfanget av digital sikkerhet, noe som ble strukturert ut ifra internasjonalt, nasjonalt og kommunalt nivå, fremvist i kapittelet om tidligere forsking. Alle artiklene benyttet er fagfellevurdert. Forskningsartikler i faget *organisasjon og sikkerhet* SOS2017 og en innføringsbok i faget *informasjonssikkerhetsstyring* INFT2001 på Norges-tekniske naturvitenskapelige universitet (NTNU) har blitt benyttet. Tilgangen på slik informasjon har skapt grunnlaget for videre datainnsamling, og kan forklares gjennom *snøballmetoden* (Tjora, 2018). Bruken av tilgjengelig informasjon gjennom egen utdanning kan trolig styrke påliteligheten til kunnskapen som formidles. Det er empirinære kilder som benyttes i dokumentstudiet. Disse ble funnet gjennom samarbeidspartner, utforsking av Digdir sin nettside og nettsøk. Tabellen under oppsummerer innholdet i de fire dokumentene som benyttes i analysen, og er et sammendrag av den mer omfattende visualiseringen (Tabell 1) i Vedlegg B.

Empirinære kilder	Tittel	Innhold
Digitaliseringsdirektoratet (Digdir) (2020)	Arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner	- Svakheter i styring og kontroll av informasjonssikkerhet. - Små og mellomstore kommuner trenger mer hjelp med informasjonssikkerhetsstyring - Få beredskapsøvelser, manglende kompetanse og forståelse hos både medarbeidere og ledere
Buan (2021)	Sluttrapport - Felles løft på informasjonssikkerhet og personvern. DigiTrøndelag (unntatt offentligheten)	- Modenhetskartlegging i regi av DigiTrøndelag. - Mål: løfte informasjonssikkerheten i kommunene. - Utfordringer: ressurser, rollefordelinger, opplæring, personvernregelverk og risikohåndtering
Sopra Steria (2021)	Informasjonssikkerhet og personvern i Trondheim kommune (unntatt offentligheten)	- Arbeid med informasjonssikkerhet krever en helhetlig tilnærming - Kommunen har ikke kapasitet til å håndtere sikkerhetssituasjonen. - Risikoreduserende tiltak er mangelfullt, og forvaltningsoppgaver/rutiner er ikke prioritert.
Riksrevisjonen (2023)	Myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor	- Kritikk til justis- og beredskapsdepartementet for manglende oppfølging av *Nasjonal strategi for digital sikkerhet.* - Svak samordning av roller, ansvar og krav som gjør arbeidet med digital sikkerhet utfordrende.

Tabell 4: Dokumentstudie med fire empirinære kilder

4.3. Arbeid med analysen

Jeg har valgt å ta utgangspunkt i en tematisk analyse forklart av Johannessen, Rafoss og Rasmussen (2020) for å skape oversikt over det samlede datamaterialet. Tematisk analyse er en av de mest grunnleggende tilnærmingene i kvalitativ metode, i tillegg er den fleksibel å benytte (Johannessen, et al., 2020). Det vurderes dermed som gunstig å bruke en analyseform som ikke er for komplekst i omfang, når det er mange elementer som skal undersøkes. Basert på en veiledning for MTO-analyser som utpeker tematiske punkter velger jeg å dekke opplæring og kompetanse (M), krav og prosedyrer (T), organisering av arbeidet, ledelse og endringsrutiner (O) i oppgaven (Kongsvik, 2013).

Tematisk analyse innebærer å identifisere temaer i datamaterialet, som vil si å gruppere data med viktige fellestrekk inn i ulike kategorier. Deretter skal temaene som identifiseres benyttes til å besvare oppgavens problemstilling og forskningsspørsmål (Johannessen et al., 2020). De overordnede kategoriene (MTO) var utgangspunktet for grupperingen av dataen (deduktiv tilnærming). Ut ifra dette oppsto undertemaer som for eksempel «mennesker som feilkilde» for å skape orden i en stor mengde data. På denne måten ble unødvendig informasjon utelukket (induktiv tilnærming). Koding har dermed blitt benyttet med mål om å finne essensen i materialet, redusere volumet og danne grunnlag for idégenerering. Kodene skal samsvare med utsagnene fra intervjuene, dermed blir sitater uthevet i kapittel 5. Empiriske resultater (Tjora, 2018). Dette kan forstås som abduktiv koding der en arbeider i etapper ved å starte med en deduktiv og

teoretisk tilnærming, før en videre skaper induktive koder gjennom grupperinger og tekstreduksjon (Vila-Henninger, et al., 2021).

Tematisk analyse kan forstås som en teoriuavhengig tilnærming. Det er en oppskrift på hvordan en skal analysere dataen, uten å tilføye spesifikke ideer om hva en skal se etter. Derfor må forskeren ha godt nok kjennskap til teorier på feltet for å ikke overse interessante funn (Johannessen et al., 2020). Jeg gjennomførte dermed et grundig arbeid med teori og tidligere forskning før dataen skulle analyseres. En tematisk analyse kan følge en stegvis prosess. Første steg var å transkribere ni omfattende intervjuer. Allerede her ble det tatt noen notater underveis for å skape oversikt over helheten av et intervju. Deretter ble materialet kodet med ulike farger. Det ble vurdert å benytte et program som NVivo, likevel gjorde jeg arbeidet manuelt for å sikre nøyaktighet og kontroll over datamaterialet. Innfall og ideer ble også notert i denne fasen. Materialet ble lest tre til fem ganger. Dermed utviklet kodene seg til å bli mer presise og sammenhengende, sett i lys av forskningsspørsmålene. Det er abduktiv koding som bidrar til å utvikle forskerens innledende teoretiske rammeverk (Vila-Henninger et al., 2021).

Det tredje steget innebærer å kategorisere dataene og sette dem sammen til en større enhet. En kan sortere inn i bokser hvor det tas utgangspunkt i det forskeren ønsker svar på. Jeg utviklet et digitalt tankekart og tabeller for å utføre dette. I hver boks skal det være data som har ting til felles. Det er enklere å gjennomføre dersom en er klar over hva oppgaven ønsker å svare på. Dette er en prøve- og feile-metode der en justerer underveis. Det fjerde og siste steget er rapportering av temaene som skrives frem i analysen. Her kan en trolig oppdage nye og spennende sammenhenger i datamaterialet. Formålet er å skrive frem svarene til forskningsspørsmålene. Dette vil gjøres med en ryddig struktur hvor temaer og undertemaer tydelig presenteres og viser til relevante utsagn fra intervjuene (Johannessen et al., 2020). De valgte dokumentene har blitt kodet på samme måte som intervjuene.

4.4. Forskningens kvalitet

I følgende delkapittel vil forskningen vurderes i et kritisk lys. Indikatorene reliabilitet, validitet og generaliserbarhet benyttes for å vurdere styrker og svakheter ved forskningsmetoden (Tjora, 2018). Reliabilitet, også kalt pålitelighet handler om studiens nøyaktighet og sammenheng. Dersom målene er gjort på en systematisk og grundig måte, er det sannsynlig at resultatene ikke forblir tilfeldige, men viser et representativt bilde. Nøyaktighet har blitt sikret ved å stille presise oppfølgingsspørsmål og få svar på det en faktisk studerer. I en kvalitativ studie er sammenheng, altså replikasjon, vanskeligere å oppnå (Thiel, 2022). Det er ikke sikkert at liknende studier på andre kommuner i landet vil gi de samme resultatene. Tjora (2018) skriver at reliabilitet avhenger av sammenheng i forskningsprosessen. Jeg har dermed tydeliggjort hvordan datagenerering gjennom transkribering og koding har blitt gjennomført. I en kvalitativ studie er det ikke like vanlig å ta for seg ren validitet og reliabilitet, men heller se det i lys av andre begreper som forståelighet (reliabilitet), overførbarhet (ytre validitet) og troverdighet (indre validitet). Hvis studien er forståelig, kan den bli repetert og benyttet av andre forskere. Hvis den er overførbar, kan resultatene generaliseres. Samtidig kan en stole på oppgavens konklusjoner om studien også er troverdig (Thiel, 2022).

Validitet, også kalt gyldighet, går ut på å finne logisk sammenheng mellom problemstillingen og utformingen av prosjektet. (Tjora, 2018). Dette gjøres ved å se dataen i lys av oppgavens teorikapittel, samt inkludere en dokumentstudie som bidrar til å sammenligne egen forskning med tidligere funn. Validitet kan deles inn i to kategorier: indre og ytre validitet. Indre validitet viser til hvorvidt forskeren faktisk har svart på det det som skulle undersøkes. Det som har betydning er om teoriene er tilstrekkelig operasjonalisert og samsvarer med mønstre i dataen (Bukve, 2021; Thiel, 2022). Ytre validitet beskriver graden av generaliserbarhet (Johannesson & Perjons, 2014). Som nevnt kan det være utfordrende å generalisere forskningen til å gjelde for alle kommuner i landet. Likevel kan en forhåpentligvis få dypere innsikt i temaet. Opplevelsene til de tre casene kan muligens gjenspeile hvordan andre kommuner, med lignende størrelse og form for organisering, arbeider med digital sikkerhet. Tjora (2018) mener generaliserbarhet ikke bør begrenses til overførbarhet eller statistisk generalisering. Masteroppgaven kan heller peke mot en moderat generalisering der forskeren selv skal beskrive i hvilke situasjoner resultatene er gyldige.

En kan kritisere kvalitativ forskning for å være for subjektiv. Det er forskerens egne tolkninger som blir lagt frem, noe som gjør at bias, altså skjevheter i forskningen, kan forekomme. Likevel kan en gjøre visse handlinger for å sikre reliabilitet og validitet. Stegene som ble tatt underveis bør dokumenteres, og det kan være gunstig å få noen til å se over arbeidet med analyse og koding (Thiel, 2022). Dette har blitt gjort ved at veileder har kommentert oppgaven og forskningsprosessen. Valget om å ha tre caser i stedet for én kan styrke oppgavens validitet da et større utvalg enklere kan generaliseres til samfunnet for øvrig. Likevel kan noen vurdere antallet caser som for lite, noe som kan true forskningens reliabilitet og validitet. Det er derfor gunstig å samle mer informasjon ved bruk av triangulering, gjennom ulike datakilder og metoder. Case-studier er en svært intensiv form for forskning som kan ta lang tid (Johannesson & Perjons, 2014; Thiel, 2022). Det ble dermed vurdert å utelukke andre kommuner i Norge og heller inkludere to informanter fra KS for å få et overordnet perspektiv på kommunal sektor.

5. Empiriske resultater

I det følgende kapittelet skal oppgavens datamateriale analyseres. Innholdet vil først fordeles på bakgrunn av de tre kategoriene som utgjør MTO-perspektivet. Deretter, for å underbygge funn, vil både utdrag fra intervjuer og relevant informasjon fra dokumenter inkluderes. Det er de utpekte dokumentene fra Digdir (2020), Riksrevisjonen (2023), DigiTrøndelag (Buan, 2021) og Sopra Steria (2021) som benyttes for å komplementere funnene fra intervjuene. Masteroppgavens forskningsspørsmål fremtrer i underkapitlene og vil ses i sammenheng med det empiriske datamaterialet. Både det som fremtrer som utfordrende og positivt blant analyseenhetene vil løftes opp i kapittelet, og organisasjonene vil sammenlignes fortløpende.

5.1. Mennesker

M-faktoren i forbindelse med digital sikkerhet fremtrer som spesielt viktig for alle organisasjonene, på den måten at det har oppstått en økt oppmerksomhet i lys av dagens risikobilde. Kompetanseheving og bevissthet om digitale trusler er noe informantene trekker frem som viktig for å bedre sikkerhetsarbeidet. Digdir utpeker kompetanse som «samlede kunnskaper, ferdigheter, evner og holdninger som gjør det mulig å utføre aktuelle oppgaver i henhold til definerte krav og mål» (Digdir, 2020, s. 20). M-faktoren vil betraktes i lys av to temaer: *mennesker som feilkilde* og *mennesker som ressurs*. Deretter vil fremstillinger fra datamaterialet benyttes til å besvare det første forskningsspørsmålet: hvordan kan menneskelig kompetanse møte dagens risikobilde?

Mennesker som feilkilde

Ved samtale med informantene diskuteres fenomenet menneskelige feil. Alle deltakerne er kjent med begrepet og reflekterer over situasjoner som resulterer fra uønskede handlinger. Dette blir eksemplifisert av informant 6. Det kan være flere grunner til at mennesker handler på en uønsket måte, noe som gjør det nyttig å vurdere interne årsaker. Informant 1 retter samtalen mot deres strategi for å håndtere slike hendelser.

> *Noen går fra kontorene sine uten å stenge ned pc-en sant, der du kan liksom bare trykke på så starter pc-en uten at du må inn med passord. [...] Men du kan jo bygge inn teknologiske forutsetninger som demper virkninger av menneskelige feil da selvsagt, men ikke hundre prosent. (Informant 6)*

> *Vi har oppdaget ting som har vært lagret på våre servere som inneholder sånn 'fake news' om politiske forhold, og da er vi ganske gode til å finne ut hvem det er som har gjort det [...] Så er det ikke alltid vi forteller eller gjør den ansatte oppmerksom på at vi har sett det her [...] Sånn at det blir en annen krets av informasjon om hva som har skjedd, enn det som er vanlig ellers når en ansatt gjør noe den ikke bør gjøre. (Informant 1)*

I noen tilfeller blir den menneskelige faktoren et forstyrrende element i arbeid med å bevare sikkerheten. Undersøkelsen av DigiTrøndelag vurderer svak opplæring i kommunene som bekymringsfullt ettersom kriminelle ofte handler igjennom mennesker (Buan, 2021, s. 11). Det er blant annet viktig at de ansatte er innebefattet om eget ansvar og at tidsrommet for å motvirke skader er begrenset. Åpenhet om det som gikk galt er viktig for å raskere redusere skadeomfanget.

> *Så en sikkerhetshendelse starter ofte med en slags menneskelig feil faktisk, at de gjør noe dumt. Så da er det viktig å ha en kultur hvor man tør å varsle fort da, for den tida er jo veldig kritisk.* (Informant 4)

Ifølge Riksrevisjonen er det nødvendig med mer kompetanse og kapasitet for «å etterleve et funksjonsbasert regelverk fordi virksomhetene selv må vurdere risikoen og finne fram til sikkerhetsløsninger» (Riksrevisjonen, 2023, s. 15). Bevisstgjøring og opplæringsprogrammer er noe som skal motvirke menneskelige feil, i tillegg til å etterleve krav og regler. Utsagnene under viser at erfaring fra tidligere hendelser i liten grad blir anvendt til opplæring av ansatte. Funnene indikerer dermed at organisasjonene burde hatt et mer bevisst forhold til læring:

> *Vi har hatt noen hendelser opp igjennom årene som virkelig, ikke bare skulle vært til læring for oss selv, men også andre kommuner, men i liten grad har vi greid å få til det. (Informant 2)*

> *Vi snakker vel ikke så mye om sånne hendelser, vi bruker det kanskje heller ikke så mye for å opplyse andre i opplæringsmetode, som vi burde, men det gjelder å anonymisere da for å ikke henge ut folk. (Informant 7)*

> *Vi håndterer jo sak for sak holdt jeg på å si og løser det i hvert enkelt tilfelle, også om det blir brukt til noe opplæringsprogram etterpå, utover det vi eventuelt deler av informasjon [...] det vet ikke jeg. (Informant 5)*

Når menneskene i organisasjonen ikke har tilstrekkelig kompetanse om digital sikkerhet, resulterer det ofte i at de som jobber med det tekniske må ta et større ansvar. Et fellestrekk blant kommunene er at et kompetent IT miljø sørger for at sikkerheten overholdes til et akseptabelt nivå. Det utelukker ikke delvis frustrasjon over manglende kunnskaper, spesielt blant toppledelsen. Dokumentstudiet av Digdir fremhever at manglende forståelse og kompetanse hos ledere resulterer i svak sikkerhetskultur, og utgjør et av de største hindrene for arbeidet med digital sikkerhetskompetanse (Digdir, 2020, s. 3). Informant 5 har tidligere observert distansert forståelse blant kommunale toppledere:

> *Litt sånn historisk har de hatt litt for lite fokus på det og tenker at kanskje det der er noe de bare fikser på IT. Ja, så jeg vet ikke, det går vel egentlig litt på kompetanse [...] de tenker ikke på det nok kanskje, at det er et ansvar de har. (Informant 5)*

Det trekkes derfor frem at det fortsatt kreves mye arbeid for å nå et høyere kompetansenivå i hele organisasjonen og på tvers av siloer. Kommunene er i noen grad preget av et teknologi-drevet fokus, som gjør at M- og O-faktoren må vike. Rapporten fra Riksrevisjonen ser at en felles forståelse er viktig, blant annet er arbeidet med sikkerhetsloven en kontinuerlig prosess som rommer flere samfunnsområder. Varierende begrepsbruk på nasjonalt nivå, for eksempel i ulike veiledningsmateriell, kan gjøre det krevende for folk å forstå hva de ulike anbefalingene innebærer (Riksrevisjonen, 2023, s. 62). Informant 2 utrykker frustrasjon over svak kompetanseutvikling og felles forståelse.

> *Jeg må jo si direkte pinlig. Jeg syntes det er stusselige greier. Jeg må være ærlig på det. Altså misforstå meg rett, vi har ganske mye på plass [...] enkelte ganger blir jeg nesten stående målløs når jeg skjønner at folk ikke har noe kompetanse på sikkerhetstenking [...] med en gang når jeg spør hva har du gjort for å sikre den informasjonen som ligger her nå, for at den skal være tilgjengelig og ikke endret av uvedkommende [...] Da blir de stående helt paff. Og den organisasjonen da som skulle tatt vare på det her, det er ikke noe mye å skryte av, spør du meg da. (Informant 2)*

I 2021 fant Sopra Steria at 88% av alle de spurte ser behov for å bedre sin kompetanse på personvern og informasjonssikerhet. Det kan tyde på at utfordringene relatert til kompetanse fortsatt er gjeldende for Trondheim kommune. Sopra Steria (2021)

fremhever at kommunen har et personell som får til mye, men at de mangler dedikasjon og prioritering av omgivelsene. Et annet element som særlig trekkes opp er rekruttering av ny kompetanse. Fosen IKT og Midtre Gauldal kommune, som er mindre i størrelse enn Trondheim kommune, har færre forutsetninger for å rekruttere nye medarbeidere. Fosen IKT mener det også kan være utfordrende å få folk til å engasjere seg i sikkerhet, noe som samsvarer med funn fra DigiTrøndelag. Kommunene syntes det er vanskelig «å nå ut til de ansatte og å gjøre opplæringen relevant og interessant» (Buan, 2021, s. 11). Det er riktignok slik at Trondheim kommune også finner dette utfordrende. Informant 3 hevder at kompetanse i markedet er spesielt krevende:

> *Så det er nok hovedproblemet, vi prøver jo konstant å rekruttere og bygge opp kompetanse, men sånn som det er nå så er det for lite kompetanse i markedet. Og den kompetansen som er der ute er for dårlig. Det er jo et problem det og at det er for mange inkompetente som kommer inn i sånne posisjoner. (Informant 3)*

Likevel poengterer rapporten fra Riksrevisjonen at Regjeringen fra 2015 til 2019 tildelte «midler til nesten 1600 nye studieplasser i IKT-relaterte fag ved universiteter og høyskoler, inkludert IKT-sikkerhet [...] antall uteksaminerte kandidater innenfor digital sikkerhet økte med 114 prosent i perioden 2014–2021». Rapporten tyder på at det kan ta tid før en ser den fulle effekten av endringene i akademia, noe som kan forklare Trondheim kommunes vanskeligheter med rekruttering.

Mennesker som ressurs

Det er like så viktig å trekke frem at de tre organisasjonene også anser mennesker som en ressurs. Ifølge Riksrevisjonen (2023) kan kompetansesatsing være et resultat av Regjeringens bidrag med 50 millioner kroner. En del av nyere tiltak i de tre organisasjonene faller innenfor kategorien mennesker og går ut på å styrke kunnskapen om digitale trusler og sikkerhetsatferd. Dette tyder på at organisasjonene er bevisst på egne mangler og ser nødvendigheten av å bedre kompetanseutviklingen. Det er likevel noe mangelfull kontinuitet i dette arbeidet. Informant 3 mener flere ansatte bør bli opplært tidlig.

> *Eneste vi har er egentlig at vi dessverre kjører sånne e-læringskurs i forbindelse med nasjonal sikkerhetsmåned [...] Så har vi ambisjoner om å gjøre noe gjennom onboarding-prosesser. (Informant 3)*

Trondheim kommune har opplæring i form av e-post kampanjer, noe som også er forekommende hos Midtre Gauldal og Fosen IKT. Testene handler til dels om å motstå fristelsen av å trykke på en lenke, dermed unngå å bli lurt. Det kan vurderes som et godt steg på veien til å utnytte menneskelige evner og forberede de ansatte på digitale angrep. Blant annet gjennomførte Midtre Gauldal kommune nylig en slik informasjonskampanje:

> *Før var det å trykke på en lenke det artigste som fantes fordi det kunne oppstå noe spennende, men man tenker jo annerledes nå, nå har man sett konsekvensene. [...] Jeg var litt deprimert når vi gjorde den testen da [...] Jeg håpet at det skulle være null som skulle trykke på den linken, men det var det ikke. (Informant 7)*

Det kan tyde på at kommunen fortsatt har en jobb å gjøre. Blant annet erkjenner alle informantene fra Trondheim kommune at de trenger et mer systematisk arbeid for å øke sikkerhetskulturen ut i organisasjonen. De arbeider i disse tider med å ansette spesifisert kompetanse innenfor personvern og informasjonssikkerhet. Fosen IKT er opptatt av å

bevare kompetansen som eksisterer i eget hus og sender i den anledning de ansatte på Microsoft sikkerhetskurs. Informantene fra Fosen IKT trekker frem at de har begynt å fokusere mer på kompetanseheving i gjennomføring av kriseøvelser, og anser dette som en gunstig måte å lære på.

> *Så i kriseøvelser som vi skal ha nå, det er jo viktig da for kompetanseheving. For der blir det jo i forkant sendt ut sånne falske 'phishing-mailer' da for å se om de går på. (Informant 4)*

Riksrevisjonen trekker frem at «under halvparten av de små og mellomstore kommunene gjennomfører kompetansehevende aktiviteter minst én gang i året, og at store kommuner gjør dette i større grad enn små og mellomstore kommuner» (Riksrevisjonen, 2023, s. 65). Samtalen med informantene fra Fosen IKT og Midtre Gauldal utfordrer delvis denne informasjonen. Det virker som at de mindre kommunene i dette utvalget har et forsterket blikk mot å bedre M-faktoren, og omtaler flere konkrete tiltak for kompetanseheving. Undersøkelsen av DigiTrøndelag oppga at opplæring er noe som både de små og store kommunene er forholdsvis dårlige på, de er heller ikke fornøyde med programmet de har i dag (Buan, 2021, s. 11). Med utgangspunkt i datagrunnlaget fra intervjuene, kan det virke som at det har skjedd vesentlige endringer på dette feltet. Alle organisasjonene har riktignok en lang vei å gå.

5.1.1. Hvordan kan menneskelig kompetanse møte dagens risikobilde?

Det er synlig at kompetanse er viktig for alle de tre organisasjonene. I tillegg forstår deltakerne at dette vil kreve et kontinuerlig arbeid. Alle informantene opplevde at de har en åpnehetskultur, på den måten at en kan innrømme feil. Informant 3 presiserer dette:

> *Innenfor min enhet har vi i hvert fall en åpenhetskultur, det er ingen som blir hugget hodet av fordi de har gjort noe feil. Trenger ikke gjøre samme feilen tre ganger, man kan kanskje lære litt underveis. (Informant 3)*

Åpenhet anses som viktig slik at medarbeidere og ledere kan lære av egne feil. Likevel kan lærdom fra tidligere erfaringer brukes mer aktivt. E-post kampanjer oppleves som positivt og gjør at menneskene trår mer varsomt. På denne måten kan menneskene møte dagens risikobilde med økt bevissthet om digitale angrep. Riktignok kan det virke som at slike kampanjer ikke alene kan sørge for økt kollektiv kompetanse. Det er trolig at et endret trusselnivå krever mer fra kommunene. Samtalene med informantene tydeliggjør et endret mediebildet som hovedårsak bak en økt bevissthet. I tillegg kan erfaringer fra andre kommuner også påvirke dette. Ifølge Riksrevisjonen fikk angrepet på Østre Toten «tydelig fram de konkrete konsekvensene av et digitalt angrep og fører dermed til at arbeidet med digital sikkerhet får økt oppmerksomhet» (Riksrevisjonen, 2023, s. 84). Dette gjør at flere ansatte søker mer informasjon og bedre forstår hva dagens sikkerhetspolitiske situasjon kan kreve av dem.

> *Jeg tror at de ansatte på veldig mange nivå i organisasjonen er blitt kjent med hvilke konsekvenser det kan få, når ting går galt. [...] ikke nødvendigvis fordi alle har hørt om det som skjedde på Toten, men fordi det har vært så mye omtale om det generelt, disse angrepene. Og begrepet hybrid krigføring har blitt kjent blant mange. (Informant 1)*

> *Ja aktørene de leser vi jo en del om i media da, og hvordan forberede seg på dem, det er jo en del tekniske ting, men også å prøve å øke bevisstheten til brukeren da. (Informant 4)*

Forståelse om et endret miljø som er preget av flere trusler anses som nødvendig for den digitale sikkerheten. Likevel eksisterer visse utfordringer, blant annet kan det være

krevende å oppnå atferdsendringer. Informant 1 reflekterer over motstand som kan sette en stopper for menneskelig utvikling:

> *Jeg tror at for at det skal skje atferdsendringer så må den måten vi gjorde ting på før ikke virke lenger. (Informant 1)*

Dette kan ses på som en utfordring for ledere som strever med å få med seg hele organisasjonen i digitale transformasjonsprosesser. Informant 1 trekker derfor frem at en ny stilling som personvernombud skal ha rett kompetanse og drive opplæring ut i organisasjonen. Midtre Gauldal kommune ser også behovet for mer lærdom. I tillegg legger kommunen vekt på ansvaret som ledere har og ser at forbedringer har skjedd gjennom erfaringer fra pandemien. Kommunen ser også verdien av felles kompetanseløft i Trøndelag:

> *Det må løftes opp som et tema, du kan ikke bare ta det for gitt. Da tror jeg mange vil si at det blir mer fokus på at kanskje kommunene må løse flere ting sammen på digi-området. (Informant 6)*

Informantene fra KS understreker også poenget om samarbeid og anser dette som verdifullt for kommunene i Norge. De ser behovet for å heve kompetansen, spesielt i forhold til atferdsendringer. KS kan være en pådriver for samarbeid i kommunal sektor:

> *Det flere har sagt er at det er godt å ha et miljø å spille på. Så det kan være med å løfte kompetansen [...] tilbudt noen sånne e-læringskurs knyttet til personvern, og det er tilgjengelig for absolutt alle. Til sist holder vi på med å etablere et sånt kompetanseprogram, med korte videoer og refleksjonsoppgaver. (Informant 9)*

Fosen IKT er den eneste organisasjonen i dette utvalget som aktivt bygger på et samarbeid mellom kommuner. Informasjonsdelingen på tvers av kommuner gjør at de kan hjelpe hverandre til å håndtere sikkerheten. Fosen IKT er primært et teknisk miljø uten direkte opplæringsansvar. Samtidig ser de behov for å spre kompetanse ut til de fire kommunene, noe som kan fremme et samspill mellom menneskelige og teknologiske kapabiliteter.

> *Det er jo nesten litt drøyt å kalle det opplæring, men så er det jo det læll [...] men utover det har vi ikke hatt noe opplegg på informasjonssikkerhetskursing, utenom små snutter og sånt som vi deler. Hvis vi ser sårbarheter og sånt informerer vi om det. Det er mer bevisstgjøringsarbeid egentlig. (Informant 5)*

Oppsummert er det enighet blant informantene om at arbeid med kompetanseprogrammer øker bevissthet, og gjør mennesker bedre i stand til å møte dagens risikobilde. Endringer i mediebildet gjør at flere forstår konsekvensene av et digitalt angrep. Det trengs likevel kontinuerlig arbeid for å løfte kompetansen i hele organisasjonen. I tillegg er det spesielt viktig at toppledelsen er involvert i sikkerhetsarbeidet og har tilstrekkelig forståelse om ansvaret som kreves av dem. Dette virker fortsatt noe mangelfullt blant informantene. Digdir (2020) mener at spesielt små og mellomstore kommuner trenger hjelp med kompetansehevende aktiviteter. Det kan virke som at dette også gjelder for Trondheim kommune. Det gjennomføres sporadiske tiltak blant alle organisasjonene, men det er usikkert om dette er tilstrekkelig for å håndtere dagens risikobilde.

5.2. Teknologi

Funn fra intervjuene indikerer at T-faktoren er det mest overkommelige området i det digitale sikkerhetsarbeidet. Det er heller M- og O-faktoren som er utfordrende. I denne delen av analysen skal det teknologiske arbeidet vurderes. Viktigheten av samspill mellom mennesker og teknologi har allerede blitt etablert. Analysen vektlegger dermed hvordan de ulike delene som utgjør MTO-perspektivet overlapper og komplimenterer hverandre. Resultatene tyder på at teknologi ikke er nok for å øke sikkerheten i en organisasjon. Underkapittelet nedenfor vil forsøke å besvare forskningsspørsmålet om teknologi: Hvordan benyttes teknologi for å nå sikkerhetsmålene?

Teknologi i lys av digital transformasjon

I rapporten fra Riksrevisjonen vurderes endringene av den nye sikkerhetsloven som noe kompleks. Tidligere var det kun konfidensialitetsbehovet som var av betydning. Derimot omfatter den nye loven «både informasjon som er sikkerhetsgradert, og som må beskyttes av konfidensialitetsbehov, og informasjon som må beskyttes av integritets- og tilgjengelighetsbehov» (Riksrevisjonen, 2023, s. 48). Informant 7 forklarer hvordan sikkerhetsmålene påvirker arbeidet med teknologi:

> *Konfidensielt er jo det som ikke andre skal få se [...] man hindrer utenforstående å komme inn i våre systemer. Det har vi, med passord og tofaktorautentisering og brukernavn. Vi har brannmurer som hindrer utenforstående å komme inn i systemene [...]*
> *Men tilgjengelighet da, er jo at alt skal surre og gå og at det ikke stopper opp [...] da har vi veldig høy grad av redundans. En server kan ha opp til fire forskjellige strømforskyvninger for å ha tre reservere i tilfelle en ryker [...] Det tredje da, er jo at vi har sikret dataen så den ikke kommer på avveie. Vi har back-up-system som er ganske avansert, lagret på vårt eget serverrom, men også en annen plass. Hvis serverrommet vårt brenner opp har vi i hvert fall dataen klar, det er vel de teknologiene vi har. (Informant 7)*

Med utgangspunkt i utsagnet over kan det virke som at informanten fra Midtre Gauldal har god kontroll over de teknologiske verktøyene som kommunen benytter. Informant 2 hevder at det er lite kunnskap og forståelse generelt om sikkerhetsmål og bruken av teknologi:

> *Det er såpass få i Trondheim kommune som kan svare på det [...] De skjønner ikke det at konfidensialitet og tilgjengelighet faktisk skal kunne vektes mot hverandre, ikke sant. Og gjennom den gamle sikkerhetsloven, som var helt på konfidensialitet, så er det jo mange som har hatt med seg en grunnordning om at sikkerhet, det er å pakke inn informasjon. Så glemmer de at det skal jo være tilgjengelig for flere og at det skal helst være til å stole på. Så bare det at du deler det i tre, tror jeg du får mange måpende blikk av rundt omkring, dessverre. (Informant 2)*

Dette samsvarer med funn som ble redegjort for i M-faktoren: kommunene mangler en helhetlig forståelse og et felles språk. En av utfordringene som blir fremhevet med teknologien er balanse mellom gamle og nye systemer. Funnene fra intervjuene indikerer at dette hovedsakelig er en problemstilling blant de mindre kommunene. Informant 5 forklarer hvordan dette utspiller seg i praksis:

> *Jeg kaller det gammel morro. Vi har veldig mange systemer som har vært i drift i en del år også driver vi til enhver tid og prøver å fornye oss og digitalisere [...] Sånn digital transformasjon som er på gang i det siste. [...] det er ikke bestandig at alle data blir flyttet over i det nye systemet, for det kan være omfattende å gjøre og det tar tid, koster mye penger. Så vi ender opp med en infrastruktur som er ganske sånn kompleks da fordi at vi innfaser ganske mange nye systemer, selv om vi holder det gamle i live en stund. (Informant 5)*

Informant 7 presiserer utfordringer med komplekse systemer, hvor mange avhengigheter påvirker hverandre. Dette peker på samspillet mellom M-faktoren og det høye konsentrasjonsnivået som kreves i arbeidet med teknologi:

> *Ja i en kommune spesielt, for man har så mange virksomhetsområder [...] der man skal ha fagsystemer som støtter all ting. Så det blir et veldig komplisert bilde på hvordan det skal fungere sammen. Det blir at man må holde tungen rett i munn, ikke koble ting i loop eller åpne bakdører og ting blir lagret feil [...] det er alle som jobber med IT bevisst på, så man er konsentrert om det der. Men om man har veldig lite tid og skal gjøre ferdig ting på kort tid, blir det veldig stressfaktor og man er usikker på om man gjorde ting rett. (Informant 7)*

Det blir derimot presisert av informant 3 at de trolig har et sterkere teknisk miljø enn flere av de mindre kommunene. Det skal dermed sies at funnene fra intervjuene indikerer at Fosen IKT og Midtre Gauldal også har god teknologisk kapabilitet. Informant 3 peker på utfordringen med eldre systemer og sammenligner egen kommune med Østre Toten:

> *Men når det gjelder andre kommuner har vi ikke lært så mye egentlig, for vi ser at de som blir truffet, som Østre Toten, var i en helt annen driftsituasjon enn oss, ikke sant. Vi sitter ikke med servere i kjelleren og holder på sånn som de gjør, vi var i 'Public Cloud' for lenge siden [...] det er mange av dem som blir rammet da som sitter med tekniske løsninger som egentlig er 'obsolete' for lenge siden. (Informant 3)*

I 2021 ble det vurdert at Trondheim kommune har gode muligheter «til å håndtere uønskede hendelser innenfor faktoren teknologi» (Sopra Steria, 2021, s. 42). Likevel kan utfordringer med digital transformasjon også forekomme i en stor kommune. Det kan være krevende å overholde regler og kontroll når det oppstår mer deling av data mellom ulike aktører:

> *[...] men å skrive i samme dokument og sånn, det byr på noen utfordringer. Det gjør det, hvis man deler et sånt dokument med en politiker så har du brutt kommuneloven. (Informant 1)*

Informant 9 fra KS forteller at kommunene så langt har vært utsatt for aktører som leter etter sårbarheter og deretter beslaglegger data og krever penger. Informanten hevder også at det enn så lenge ikke har vært målrettede angrep mot kommunene. Derimot viser underkapitlet om endringsrutiner til motstridende meninger om dette. Det som likevel er viktig er ifølge informant 10 å erkjenne at en er avhengig av teknologi:

> *Også sier man sånn at den teknologien, den gir deg både mulighetsrom, men har alltid sårbarhet, uansett har den en sårbarhet. Du kan ikke sikre deg hundre prosent (Informant 10)*

Det er synlig at digital transformasjon resulterer i en avhengighet av teknologi hvor en må opprettholde kontroll over komplekse systemer. Det kan dermed være noe vanskeligere å arbeide med teknologiske forutsetninger for digital sikkerhet, spesielt for kommuner som må balansere nye og gamle systemer. Følgelig vil forskningsspørsmålet om teknologi besvares.

5.2.1. Hvordan benyttes teknologi for å nå sikkerhetsmålene?

Det er flere fellestrekk blant de tre analyseenhetene når det gjelder arbeidet med teknologi. Alle informantene forteller at teknologien følges opp og utvikles jevnlig. For å sikre konfidensialitet, integritet og tilgjengelighet har Trondheim kommune arbeidet med klarering av individer, tilgangsstyring og autorisasjonsnivå. Fosen IKT har nylig tatt en gjennomgang av alle fagsystemene, og Midtre Gauldal kommune har innlemmet en ny

overvåkningstjeneste. Alle organisasjonene benytter NSM grunnprinsipper for IKT-sikkerhet, noe Sopra Steria (2021) anser som nyttig å tilpasse til egen sikkerhet. Et økt fokus på tofaktorautentisering er også fremtredende blant alle organisasjonene. De tre organisasjonene har enn så lenge klart å benytte teknologien til å bekjempe alvorlige angrep. Trondheim kommune aktiverte nye løsninger etter krigens utbrudd. Dette gikk ut på å flytte tjenester som særlig var utsatt for tjenestenektangrep. Sopra Steria (2021) bemerket blant annet at Trondheim må arbeide med å følge opp personvern i skyløsninger. Utsagnet under kan tyde på at dette har skjedd:

> *Vi har jo hatt veldig mye fokus på å få til autentisering og tilgangsstyring da. [...] Så har vi brukt mye tid på den skyreisen vår, bygd veldig sånn bevisstgjøring på hva skyløsning kan brukes til i form av lagring [...] sensitivt eller ikke sensitivt. Det har man brukt mye tid på for å få organisasjonen til å forstå at noe skal dit og noe skal i type fagsystemer. (Informant 3)*

Tilgangsstyring fremstår som særlig viktig for alle organisasjonene for å nå sikkerhetsmålene. Både informant 3 og informant 4 trekker frem arbeidet med å se lokasjonen der de ansatte logger seg på. Det vil dermed bli oppdaget hvis noen skulle befinne seg i et annet land, som gjør at de ikke får tilgang til systemer:

> *Hvis en bruker hos oss skal på utenlandstjeneste eller reise, må den varsle. For alt utenom Norge er blokkert da. (Informant 4)*

Teknologiske sikkerhetstiltak som utpeker seg i samtale med informantene er bruken av penetrasjonstester og overvåkningstjenester. Studien av DigiTrøndelag konkluderer at bare to av de spurte kommunene har gjort penetrasjonstester i løpet av de siste årene. Dette innebærer å leie inn noen som skal hacke systemene i kommunen og dermed avdekke sårbarheter (Buan, 2021, s. 16). Det ble ikke spurt hvor ofte slike tester gjennomføres, men informant 5 påpeker at det kunne vært gjort oftere:

> *Så kjører vi penetrasjonstesting, men det kunne kanskje vært gjort litt oftere etter mitt syn da, men det og er en ting som krever ressurser å gjennomføre og oppkjøringen av det etterpå ikke minst. (Informant 5)*

Fellesnevneren med det teknologiske arbeidet er at det må anses som en kontinuerlig prosess der en må være på jakt etter nye sårbarheter. Informantene fra Midtre Gauldal kommune presiserer et større fokus på redundans og back-up systemer. Dersom en oppdager et sikkerhetshull, er det ifølge informant 7 viktig å vedlikeholde systemene. I tillegg påpeker informant 4 utfordringer med å gjenopprette systemer etter et angrep:

> *[...] skulle det skje noe likevel så får vi et varsel da fra denne overvåkningstjenesten. Da må vi agere veldig raskt for å hindre at de kan ja utvikle sitt innbrudd og hindre oss fra å gå inn og gjøre ting. (Informant 7)*

> *Erfaringer fra tidligere er at vi har fått ting opp til å gå igjen, men det som har vært overraskende var kanskje at vi brukte så lang tid på å få det tilbake [...] Hadde noe rammet hele kommunen eller alle kommunene så hadde datamengden vært så stor at vi lukter mange dager og uker da. (Informant 4)*

Back-up avtaler, antivirus og brannmurer er standard teknologier som benyttes av de fleste, og skal med dette sikre redundans. Alle informantene hevder likevel at det er arbeidet rundt teknologien som innebærer flest svakheter. Det virker dermed nødvendig med bedre forståelse om hvordan teknologien fungerer, og hva digital transformasjon vil kreve av organisasjonene. Informant 4 mener at det trengs bedre kontroll på å

administrere teknologien, for å ivareta sikkerhetsloven. I tillegg eksemplifiserer informant 6 denne utfordringen med innføringen av helseplattformen:

> *Problemet der er jo å få god kontroll på å administrere hvem som har rettigheter da. Så teknologien er jo der, men det er bare regimet rundt som feiler. (Informant 4)*

> *Helseplattformen er vel egentlig beste eksempelet på at folk tror det motsatte, sant, at det er 20% organisasjon og 80% teknologi. [...] De tror jo at det bare er noen som har fått en ny datamaskin også ordner alt seg. Helseplattformen krever jo at de som skal bruke den jobber annerledes og det er det ikke alle som har fått med seg heller. (Informant 6)*

Funnene indikerer at det er nødvendig med et samspill mellom mennesker, teknologi og organisering. Dette kan forstås som at sterk teknologisk kapabilitet er avhengig av styringsstrukturer. Det kan virke som at alle organisasjonene har et kompetent teknisk miljø som sørger for at sikkerhetsmålene overholdes. Det er likevel slik at arbeidet blir utfordret av en økende digital transformasjon og manglende administrering. Dette vil følgelig utforskes nærmere gjennom vurdering av organisasjonenes O-faktor.

5.3. Organisering

O-faktoren er spesielt omfattende å analysere da det er mange ulike elementer som spiller inn i arbeidet med digital sikkerhet. Denne delen av oppgaven er dermed inndelt i flere underkapitler. Mot slutten av kapittelet vil forskningsspørsmålet om organisering bli besvart: Hvilke tiltak gjør lederne i organisasjonen for å forbedre sikkerhetsarbeidet? Som nevnt i oppgavens metodekapittel er det ulike temaer som kan vurdere de organisatoriske kapabilitetene. I samsvar med forslag til tematiske punkter i MTO-analyser vil organisering av arbeidet, ledelse og endringsrutiner utforskes nærmere (Kongsvik, 2013). Nedenfor er roller og sikkerhetsstyring, beredskapsøvelser og samarbeid uthevede elementer. Dette er områder som blir diskutert blant informantene, i tillegg til å være sentralt i de fire utvalgte dokumentene.

5.3.1. Organisering av arbeidet

Roller og sikkerhetsstyring

Informantene har god forståelse for at digital sikkerhet krever et endeløst organisasjonsarbeid, i den forstand at teknologiske forutsetninger ikke er nok for å ivareta sikkerheten. Likevel oppleves O-faktoren som mest krevende. I rapporten til Sopra Steria (2021) oppfattes Trondheim kommunes rollebaserte tilnærming til informasjonssikkerhet som delvis fragmentert og utfordrende. I samtale med alle informantene fra de tre organisasjonene blir det presisert at kommunedirektøren har det overordnede ansvaret. I Trondheim kommune er det organisasjonsdirektøren som har ansvaret for det digitale domenet. Videre blir ansvaret delegert ned til IT-sjefen. Dersom det skjer en alvorlig hendelse, vil sikkerhet- og beredskapssjefen få beskjed. Kommunen har også informasjonssikkerhetsrådgiver og personvernombud. En av de største utfordringene med rollefordeling blir utpekt av informant 3:

> *Så er det jo generelt sett for lite ressurser rundt omkring i organisasjonen til å ivareta på en måte det store ansvaret som påligger hvert virksomhetsområde da. Så per i dag er det nok best organisert ifølge teknisk sikkerhet. (Informant 3)*

Midtre Gauldal kommune har organisert arbeidet med utgangspunkt i forankring av roller og årlige ledelsesgjennomganger, noe som har gjort kommunen mer selvsikker på evnen til å oppnå en funksjonell vurdering av risiko.

> *IKT-sjefen som har det daglige, så er det jo kommunalsjef da [...] også vi har gjort det sånn, en IKT-strategi og en digitaliseringsstrategi som forankrer hva vi skal jobbe etter [...] Det er en i staben da, som er sikkerhetsansvarlig også har vi personvernansvar, så fordelt de rollene som vi må ha da. (Informant 6)*

Gjennom å utpeke sentrale roller, ansvar og krav kan organisasjoner oppnå mest mulig effektiv bruk av ressurser (Riksrevisjonen, 2023). Ifølge informant 10 fra KS er det viktig at arbeidet ses i sammenheng med digitalisering. Det kan dermed vurderes som positivt at informant 6 nevner digitaliseringsstrategien. Selv om kommunen har fordelt sikkerhetsansvaret, presiserer informant 7 at mye av det praktiske arbeidet fortsatt blir gjort av IT-teknikerne. Det tyder på at arbeidet med digital sikkerhet enda ikke er fullstendig og helhetlig forankret i organisasjonen, noe som blir forklart av informant 8:

> *Men det var jo det organisatoriske som du spør om, og da føler jeg at informasjonssikkerhet er egentlig noe som skjer i bakgrunnen, selv om det angår alle. (Informant 8)*

Fosen IKT har også fordelt ansvar ut til enkelte roller, i tillegg til å ha en krisestab. Dersom noe i de fire kommunene oppfattes som kritisk, får alle de ansatte i Fosen IKT varsel. Samarbeidet er derfor nyttig for å avdekke mulige angrep hos kommunene. Informantene hevder likevel at organiseringen ut i de fire kommunene mangler god forankring:

> *IT-leder i Fosen-IKT som er ansvarlig for informasjonssikkerheten i avdelingen vår og i hver kommune så er det jo egentlig kommunedirektør [...] som har det øverste ansvaret. Men utover det så er det litt sånn ymse med folk som har dedikerte roller som jobber med informasjonssikkerhet. (Informant 5)*

For Fosen IKT virker det utfordrende å ha kontroll på O-faktoren blant alle de fire kommunene, det er heller ikke deres oppgave, men vurderes likevel som nødvendig for å bedre det øvrige sikkerhetsarbeidet. Det er ikke alle kommunene som har utfylte roller på informasjonssikkerhet, personvern og beredskap, noe som går utover effektiv kommunikasjon på tvers av samarbeidet. Begge informantene fra Fosen IKT legger vekt på at det er en kamp om ressurser.

> *Det er jo litt problemet i mindre kommuner at de ikke har ressursene på alle disse rollene, og om noen får den rollen som er kanskje 100% jobber på arkivet eller andre ting, så da blir det jo arkivet som personen egentlig jobber med. (Informant 4)*

Internkontroll er en viktig faktor for å lykkes med det digitale sikkerhetsarbeidet, og bør være en integrert del av organisasjonens helhetlige styringssystem (Digdir, 2020). Informantene fra Trondheim kommune presiserer blant annet at svak risikooppfattelse går utover sikkerhetsstyringen:

> *Internkontrollen i Trondheim kommune den er ikke all verdens. Styringssystemene i Trondheim kommune er heller ikke all verdens. Så det er stort forbedringspotensial, og i det da er det litt lenger vei enn det burde ha vært, både det med risikostyring og risikotenking. (Informant 2).*

Sopra Steria fant at mange ansatte utfører risikovurderinger, men at det mangler etablerte arbeidsprosesser for å systematisere dette (Sopra Steria, 2021, s. 30). Digdir (2020) uthever at styrende dokumenter er en viktig del av sikkerhetsarbeidet og råder

kommunene til å forholde seg til internasjonale standarder som ISO 27001, ved etablering av internkontroll. Ingen av organisasjonene har implementert standarden til eget bruk og forholder seg heller til anbefalinger fra statlige aktører. Fosen IKT anser standarden som for kompleks. Det har også vært noe krevende for Trondheim kommune.

> *Vi baserer oss på det som kommer fra NSM, eksempelvis så for en tid tilbake var det beslutta at vi skulle ha ISO 27001 styringssystem for informasjonssikkerhet [...], men vi hadde ikke nok ressurser til å jobbe med det styringssystemet. Det endte opp med at vi satt der med et styringssystem som ikke var brukt og da har det jo ingen verdi. (Informant 3)*

> *Det går litt på det med å få på plass et informasjonssikkerhetsstyring-system [...] Så hvis det ansvaret blir litt sånn spredt så stopper det litt opp, for folk er opptatt på andre hold [...] man må ikke jobbe med informasjonssikkerhet jevnlig for å holde julene i gang, men det kan få katastrofale konsekvenser hvis du ikke jobber nok med det. (Informant 5)*

Regjeringen skal lansere en nasjonal portal for digital sikkerhet hvor virksomheter kan få ensartede råd som passer deres behov (Riksrevisjonen, 2023). Dersom dette blir benyttet kan trolig flere kommuner få hjelp med styring og internkontroll. Det er synlig at de tre organisasjonene mangler en helhetlig plan for digital sikkerhet, noe som går på bekostning av et fullverdig styringsnivå. Ifølge Digdir (2020) er det viktig å ha en informasjonssikkerhetspolicy som beskriver mål og strategier. Det var midlertidig noe uklart om organisasjonene har innført dette i tilstrekkelig grad. Likevel har alle informantene forståelse om at et helhetlig arbeid krever mer prioritering. Informant 2 ønsker at fagrådet for informasjonssikkerhet og personvern blir tilstrekkelig investert i, noe som var en anbefaling fra Sopra Steria i 2021.

> *[...] fordi at man har et felles råd på tvers av sektorer med representant fra hver av sektorene. [...] for det første er det veldig mye informasjon på tvers med aktuelle saker og da er det en anledning for å faktisk bli litt kjent med, diskutere ulike utfordringer. Ulike sårbarheter, ulike risikoer. (Informant 2)*

Beredskapsøvelser

Riksrevisjonen undersøkte flere kommunale planer og så at digital sikkerhet får lite oppmerksomhet, på den måten at beredskapsplanene vektlegger «først og fremst risiko- og sårbarhetsanalyser, øvelser og beredskapsplanlegging i stort. I noen tilfeller omtales digitale sikkerhetshendelser» (Riksrevisjonen, 2023, s. 59). DigiTrøndelag fant at kun 31,6% av de spurte kommunene har beredskapsplaner for informasjonssikkerhet, og av disse har kun halvparten gjennomført øvelser (Buan, 2021, s. 12). Det er ingen av organisasjonene i utvalget som har beredskapsøvelser spesifikt for digital sikkerhet, i så fall gjelder dette kun for IT avdelingen og ikke på tvers av de ulike enhetene.

> *Så til spørsmålet om vi gjennomfører beredskapsøvelser. Så er jo svaret nei og hvorfor ikke, vi har ikke prioritert det, må ærlig svare på det. (Informant 1)*

> *Vi fikk for litt siden et politisk spørsmål om det gjøres i andre deler av kommunen også [...] men da fikk vi svart at det kjøres ikke noe separat innenfor hvert virksomhetsområde for det der, men de anser det for å være en del av sin ordinære beredskapsplanlegging og beredskapstesting. Så er vel sannsynligvis det å pynte litt på sannheten da. (Informant 3)*

Utsagnene over kan tyde på at Trondheim kommune erkjenner behovet for slike øvelser. Riktignok skal det bemerkes at Fosen IKT og Ørland kommune planlegger en omfattende øvelse i disse tider. Erfaringer fra en slik øvelse kan være verdifullt for samarbeidet som helhet.

Men det som er på Fosen da er at vi har Ørland kommune som virkelig har tatt tak i det da, så det kan jo bli en rettesnor for resten [...] For i det man har kommet godt i gang på sikkerhetsarbeidet og alt er på stell, prosedyrer på alt og alt er dokumentert så har vi en felles ressurs. Sånn som nå ligger vi litt på etterskudd da. (Informant 4)

Digdir mener at kommuner trenger hjelp med å gjennomføre jevnlige øvelser. Ifølge dokumentstudiet er hendelseshåndtering og øvelser «viktige kilder til forbedringer, for eksempel til bruk i risikovurderinger» (Digdir, 2020, s. 14). De ulike informantene anser beredskapsøvelser som viktig og er klar over at det er noe de burde ha:

Men det har jo aldri skjedd øvelser og det bør gjøre det. Det blir kanskje aktuelt etter vi er ferdig med nye planer. (Informant 7)

Selv om kommunene har noen planer for ulike scenarioer innenfor digital sikkerhet, blir beredskapsøvelser omtalt som utfordrende å iverksette på egenhånd:

Det er ikke så mange kommuner som har turt å gjøre det før da. Den eneste kommunen jeg vet om er Orkland kommune som gjorde det nå rett etter jul, for det var et såpass stort inngrep på kommunene. (Informant 4)

Kommunene virker likevel dyktige på å gjennomføre generelle beredskapsøvelser og ser nytteverdien av å ha et planverk. Det er dog forskjell på fysiske og digitale skader:

Der er jo kommuner drilla veldig godt på, krisearbeid da, men så kan du jo si at det er forskjell på å få tak i en gravmaskin og grave opp et rør som har gått tett da, versus at eventuelt all digital infrastruktur er nede. (6)

Samarbeid

For å imøtekomme flere av utfordringene som kommunal sektor står ovenfor kan det være nødvendig å samarbeide, både gjennom eksterne partnere og i form av interkommunale samarbeid. I samtale med informantene fra KS ble det tydelig presisert hva de ønsker at kommunene skal gjøre for å bedre det digitale sikkerhetsarbeidet:

Problemet med alle disse kommunene våre det er jo dette her, det er ulik modenhetsgrad [...] hvordan skal vi løfte samtlige kommuner for å gjøre dem mer robust. [...] skal vi gjøre det alene eller sammen, gitt kompleksiteten så mener vi at man må gjøre ting sammen. [...] Selv Bergen-kommune som er ganske stor, sier at de er for små alene til å ha 24/7 beredskap. For jo større kommune desto større infrastruktur og mer komplekst. (Informant 10)

Trondheim kommune har flere ressurser og tilgang på kompetanse, som gjør at de har sterkere sikkerhetsmekanismer på plass. Det er likevel mer utfordrende for en stor kommune å ha oversikt da infrastrukturen er omfattende. Alle de tre organisasjonene har eksterne samarbeid som «helse- og omsorgssektorens nasjonale senter for cybersikkerhet» (HelseCERT). Et slikt nettverk får ansvaret som felles responsmiljø for kommunene (Riksrevisjonen, 2023). KS er opptatt av at kommunene skal benytte slike tilbud. Statlige aktører som NSM bidrar med å analysere trusselbildet for kommunene. I tillegg er eksterne samarbeid med private aktører også forekommende. Kommunene leier inn konsulenter og har avtaler med leverandører:

Store profesjonelle aktører som Evry og Sopra Steria, og de har jo et system på det her, mye bedre enn det vi hadde internt hos oss. Det må vi bare stikke fingeren i jorda å være helt enig om. Det kommer jo med en pris selvfølgelig, men for Trondheim kommune var det et gedigent løft sikkerhetsmessig. [...] Det rimer dårlig med styringsprinsippet mitt at de som eier informasjonen også skal styre kontrollene, ikke sant. Men i praksis så fungerte det som bare

juling, inntil noen begynner å spørre da. Ikke sant som hva har vi gjort på den sida, og hvordan ser nettverket vår ut. (Informant 2)

Rapporten fra Riksrevisjonen viser at samarbeid mellom flere aktører, for eksempel mellom privat og offentlig sektor, øker kompleksiteten i verdikjeder og i digitale systemer. Det kan dermed være utfordrende for virksomheter å opprettholde oversikt (Riksrevisjonen, 2023, s. 10). Likevel syntes flere av informantene at områder som grenser mot digital sikkerhet er såpass spesialisert at det blir urealistisk å være fullstendig selvforsynt. Dermed vurderer informantene fra KS det som viktig å stille krav for å bevare internkontroll:

[...] sikkerhetsteknologien den skal hjelpe deg og den vil hjelpe deg, all over, men den vil aldri fungere helt hvis du har et dårlig system i utgangspunktet. [...] Vi må som sagt stille krav til leverandørene. (Informant 10)

Informant 9 poengterer at den vanligste formen for samarbeid innen digital sikkerhet er gjennom interkommunale samarbeid på IKT-drift. Slik som Fosen-kommunene har. Et slikt samarbeid blir også vurdert som en mulig løsning for Midtre Gauldal kommune:

Fosen IKT har jo drevet på lenge, så det er nok sånn for oss nå at vi er i en vurderingsfase om vi skal søke samarbeid. (informant 6)

Informant 6 presiserer at de har noen samarbeid. De deler blant annet personvernombud med tre andre kommuner, hvilket legger til rette for informasjonsdeling. De har tiltro til at nabo-kommunene vil komme til hjelp dersom en uheldig hendelse skulle oppstå. Informant 1 er usikker på om dette gjelder for dem:

Men Trondheim er en stor kommune så hvis vi får ordentlig angrep på våre tjenester, sånn at vi ligger nede, så er det veldig vanskelig for andre å hjelpe oss. (Informant 1)

Undersøkelsen av DigiTrøndelag vurderer det som gunstig at kommuner samarbeider. Det kan heller ikke forventes at små kommuner skal avsette store ressurser på egenhånd (Buan, 2021). Fosen IKT, som er den eneste aktøren i utvalget basert på et samarbeid, ble spurt om deres opplevelse av dette:

Men det er klart at småkommuner blir jo veldig fort veldig små skal jeg si, hvis de blir stående alene både med tanke på informasjonssikkerhetsarbeidet og den tradisjonelle IT-driften da. [...] samarbeidet om IT-drift for eksempel, så får du bygd et fagmiljø da. (Informant 5)

Rapporten av Sopra Steria (2021) viser at Trondheim kommune bør dra mer nytte fra regionsamarbeid, KS og andre kommuner. Informant 9 mener at arbeidet med digital sikkerhet i kommunal sektor er fragmentert og mangler samhandling. Dette blir også presisert i rapporten av Riksrevisjonen som vurderer graden av «samordning mellom ulike aktører som lav til moderat, da den stort sett begrenser seg til utveksling av informasjon, erfaring og kunnskap mellom aktørene» (Riksrevisjonen, 2023, s. 124). Flere av informantene nevner DigiTrøndelag og ser nytteverdien av et slikt nettverk. Regionale samarbeidsnettverk kan dermed vurderes som gunstig for både små- og store kommuner.

5.3.2. Ledelse

Med bakgrunn i viktigheten av å fordele ansvar og roller i arbeidet med sikkerhet vil det rettes et blikk mot ledelse. Informant 7 poengterer at en sikkerhetsansvarlig kan ha et blikk utenfra og stille relevante spørsmål til det daglige driftsansvaret. Funn fra intervjuene indikerer likevel at det har vært og fortsatt eksisterer en form for ansvarsfraskrivelse i kommunal sektor, da ansvar og prosjekter blir delegert videre til IT-avdelingen.

> *IT får skylda for mye. Og jeg vil jo si at IT gjør jo per i dag mer enn de skulle på den sida, fordi det ansvaret som ikke blir tatt vare på ute på enhetene, det må IT prøve å dekke opp da. (Informant 2)*

Revisjonen som ble gjennomført i Trondheim kommune sier at «arbeidet med informasjonssikkerhet og personvern anerkjennes av enkelte ledere, men mister fokus og prioritet i møte med annen kjernevirksomhet» (Sopra Steria, 2021, s. 25). Svarene som blir gitt i intervjuene gir inntrykk av en nylig oppstått prioritering av digital sikkerhet. Det er blant annet flere av informantene som applauderer helsesektoren for god innsats på feltet. I Trondheim kommune er det mange ledere og alle vil dermed ikke ha like stor interesse og forståelse for arbeidet. Riksrevisjonen (2023) trekker frem at det er krevende for flere virksomheter å vurdere hva som kan anses som akseptabelt sikkerhetsnivå. Dette blir også tydelig i samtale med informant 2:

> *Det er ikke noe felles forståelse for hva som er akseptabelt risikonivå i Trondheim kommunes ledergrupper. Det varierer fra sektor til sektor, også varierer fra sak til sak. (Informant 2)*

Riksrevisjonen (2023) fant at kommunene trenger anbefalinger om hva som kan vurderes som akseptabel risiko. I henhold til dokumentstudiet fra Digdir (2020) er det ledere sitt ansvar å ha kontroll på risikoen som følger av mål og arbeidsoppgaver. Informant 10 forteller derimot at det å gjennomføre risikovurderinger ikke er en enkel sak, spesielt innen det digitale sikkerhetsarbeidet. Informanten legger vekt på at lederne må tenke mer på konsekvenser og deretter stille krav for å øke sikkerheten. Det er likevel mulig at det kreves for mye av kommunene på dette feltet.

> *Det er vanskelig å drive med det vi kaller risikobasert tilnærming overhodet. [...] Og motparten tenker ikke om du har sikret den verdien ovenfor en annen, der er målet å bare finne. (Informant 10)*

Ifølge informant 7 har toppledelsen blitt gode på å håndtere kriser, men risiko- og sårbarhetsanalyser anses fortsatt som krevende. Utsagnene over tyder på at ledere har en del utfordringer med det digitale sikkerhetsarbeidet. Informant 10 utpeker at det er et viktig ansvar som er pålagt ledelsen, spesielt kommunedirektøren, for å ivareta internkontroll. Dette blir operasjonalisert gjennom tre spørsmål:

> *Still deg disse tre spørsmålene. Hva skjer om kommunens systemer er helt utilgjengelig og ikke til å stole på, hva gjør du da? Hvor lenge og hvilken del i kommunen kan du operere, til tross for at systemene er utilgjengelig? Og hvor skal du søke ekstern hjelp? [...] om du kan svare på de tre der har du faktisk kommet ganske langt med risikoen. (Informant 10)*

I fokus-gruppe intervjuet ser informantene ledelse i relasjon med digital transformasjon. Samtalen mellom de to informantene tar for seg ledelsens ansvar til å optimalisere arbeidsrutiner og implementere endringer:

Man vil jo helst bare arbeide slik man har gjort tidligere med det gamle systemet. Og der mener jeg at ledere, ikke IT-teknikerne, må ta tak i og bli bevisst på det der [...] (Informant 7)

Ja, det er nettopp det, også er det så mye digitale løsninger som vi har kanskje vært flinkere til å ha i hus da, men mange begynner i feil ende. De ser noen som har et program også vil de gjerne ha det i sin organisasjon, så er det kanskje ikke det vi trenger læll. (Informant 8)

Ja og det der er interessant for det kan være en kommune da som har gjort forarbeid og en utredning og anskaffet dette her, også lykkes man og det blir en suksess. Og da hører vår kommune det og vil kjøpe samme program, uten å ha egentlig skjønt hva som er gjort i forhånd, og vi mislykkes jo da. (Informant 7)

En slik problematikk blir også nevnt som forekommende i de fire Fosen-kommunene. KS-informantene reflekterer over slike utfordringer, samt en viktig verdi som kommunene må bevare:

Jeg syntes man må ta større grep sånn at man kan endre seg, og teknologien heller kommer som et tillegg. Jeg tror den største utfordringer fra vår sektor er vel egentlig å faktisk ta å utnytte av gevinstene [...] da kan man fort etablere mye risiko om man ikke har tenkt igjennom det før man tar i bruk noe nytt. (Informant 9)

Sikkerhet handler om kun en ting. Og det er tillit. [...] Jo mindre tillit, mer kontroll. Og hvor mer kontroll jo mer ressurser må du bruke. (Informant 10)

5.3.3. Endringsrutiner

Det er flere endringer som har oppstått blant organisasjonene. Med hensyn til masteroppgavens problemstilling er det endringer som et resultat av dagens risikobilde som har vært mest relevant. Politikerne prioriterer mer ressurser, noe som utgjør en forskjell i arbeidet med digital sikkerhet i kommunal sektor:

For det første så påvirker det politikernes vilje til å prioritere ressurser til å jobbe med det området. [...] Det er ofte veldig lett for politikere og prioritere mest penger til skole eller helse, og ikke til noen som sitter og planlegger for noe man ikke håper skal skje. [...] du merker en forskjell, at nå går det an å snakke om det her, og mottaket er helt annerledes. Men også ellers i organisasjonen, man skjønner at det her er hensyn som vi må ivareta. (Informant 1)

Temaet digital sikkerhet har blitt mer vesentlig enn før. Informant 1 trekker også frem at en større uro er synlig blant befolkningen. Særlig invasjonen av Ukraina har preget kommunal sektor. Situasjonen krever årvåkenhet i den forstand at en lettere kan begå feil, når det er økt aktivitet på flere områder. Trondheim kommune har dermed gjort teknologiske innstramminger:

Akkurat i forhold til krigen i Europa, på grunn av den da så har det jo vært gjort vesentlige endringer. På teknisk og operativt nivå igjen, det har vært strammet inn veldig mye. [...] Det som skjedde da, de advarslene og anbefalingene som kom nasjonalt fra, ga oss jo dekning for å gå til politisk og be om mer penger for å gjøre mer. (Informant 3)

Informantene reflekterer over et økt trusselnivå der det er faren rundt Russland som utpeker seg. Alle kommunene opplever hyppige angrep på sine systemer, men foreløpig ikke av alvorlig grad. Likevel forstår informantene at de ikke kan være helt trygge. Alle informantene nevner både direkte og indirekte at endrede omgivelser, som følge av pandemien og krigen i Europa, har blitt den nye normalen. En konsekvens at dette er at

individer blir vant med en høyere usikkerhet og dermed aksepterer en slik risiko i hverdagen.

> *Det er ikke så rart da å tenke at russerne faktisk på statlig nivå i flere år, i hvert fall etter invasjonen på Krim, har de bevisst drevet hybride angrep mot Norge og til og med Trondheim som kommune. Men vi har vent oss til det på en måte, vi har liksom justert oss litt, bare justert skalaen. Ja, det er den nye normalen. (Informant 2)*

Det er også noen kontrasterende meninger blant informantene, hvor ikke alle er like skråsikre på om det i dag eksisterer målrettede angrep mot kommunen eller ikke:

> *Vi forbereder mer generelt. [...] per i dag er det ikke noe grunnlag for å peke på at Trondheim kommune er noe sannsynlig mål for Russland eksempelvis. (Informant 3)*

Midtre Gauldal kommune opplever økt angrepsaktivitet mot sine systemer, noe som resulterer i større bevissthet blant ansatte og ledere. Under pandemien fokuserte kommunen på å oppnå sikker kommunikasjon, og måtte med dette sørge for å innlemme tofaktorautentisering. Flere ansatte trengte tilgang til datasystemene da det ble økt bruk av hjemmekontorløsninger. Endringer gjennom deling av data og bruken av nye verktøy som teams var ikke alltid like enkelt. I tillegg er svindelteknikker mer avanserte i dag.

> *Men vi oppdaget jo det da, vi skulle ikke si det til noen, at det ble lagret et dokument på offentlige grupper som elever kom inn på, sant. Og vet jo at det var lagret mye personopplysninger og på teams da i de gruppene der. Så ja vi kom litt på etterskudd, vi ønsker jo å være i forkant når vi ruller ut noe nytt. (Informant 8)*

> *Men de jobber på en annen måte nå, de prøver å forberede ting før de krypterer og krever løsepenger, og da har de ødelagt og gjort masse ting i forkant da. Kanskje forberedt seg i en uke eller noe, og det gir store konsekvenser, men det har vi ikke blitt rammet av enda. (Informant 7)*

Det er tydelig at det har blitt vanskeligere å oppdage svindelforsøk. Informant 7 presiserer at toppledelsen ble mer involvert i arbeidet og ga de ansatte korte og langsiktige tiltak. Dette var et resultat av brevet som kom fra KS i forbindelse med krigen i Ukraina. Det er likevel utfordrende når ressurser og kapasitet har et begrenset omfang, noe som forsterker behovet for å samarbeide med andre kommuner:

> *Det går bra og det går rundt [...] Det er jo veldig mye utviklingsarbeid på IKT, alt er på utbytting av systemer og nye muligheter, og da blir jo miljøene mer sårbare om vi skal gjøre store løft da. Så det er nok grunn over tid at vi søker samarbeid sammen med andre. (Informant 6)*

I fokus-gruppe intervjuet formidles det at digital sikkerhet tidligere har vært behandlet som noe separat, men at de nå ser et behov for å integrere det inn i det øvrige sikkerhetsarbeidet:

> *Tidligere har det vært to forskjellige ting, vi har jo hatt vårt eget regelverk rund informasjonssikkerhet. Men nå så ser vi at hele beredskapsbiten, for alle scenarioer i kommunen, da baker vi det inn i det.* Så det blir samme regelverk og samme metodikk, hvis det skjer en alvorlig hendelse som et større dataangrep i kommunen *(Informant 7).*

Pandemien var utfordrende, men det skaper også mulighet for læring. I Trondheim kommune tilpasset kriseledelsen sin arbeidsform til det nye miljøet, og dette viste seg å være vellykket. En plan er hjelpsomt, men det er også viktig å tenke utenfor etablerte

rammer, slik informant 2 forklarer. Flere av deltakerne poengterer at kommunene har blitt mer tilpasningsdyktige:

> *For oss på sidelinja var det litt sånn, ja hvorfor følger vi ikke planen også videre. Men samtidig målet var så klinkende klart. Alle hadde motivasjon for å gjøre så god jobb som mulig, så det datt på plass av seg selv. I det var det mye læring (Informant 2)*

> *De tilpasser seg situasjoner ganske så fort, om det må være digitalisering eller noe annet. Bare å se på flyktningstrømmen og Covid. (Informant 10)*

Fosen IKT har i likhet med Midtre Gauldal og Trondheim endret rutiner, spesielt på teknisk nivå, grunnet bruk av hjemmekontor under pandemien. I sammenheng med hybride angrep har det vært diskusjoner om Fosen-kommunene kan være i fare. Dagens risikobilde har dermed ført til at toppledelsen i kommunene involveres mer.

> *Så da blir det mer fokus i og med at flere snakker om det, og det kan være en problemstilling at vi kan være et interessant mål da, for eksempel for enkelte. Så det påvirker jo i høyeste grad. (Informant 5)*

Det virker som at flere har blitt mer åpne for endringer som følge av digital transformasjon og lærdom fra tidligere hendelser. I det neste underkapittelet vil nyere tiltak i de tre organisasjonene formidles, hvilket er resultat av de nevnte endringene. I den anledning vil masteroppgavens siste forskningsspørsmål bli besvart.

5.3.4. Hvilke tiltak gjør lederne i organisasjonen for å forbedre sikkerhetsarbeidet?

Som nevnt i kapittelet om mennesker har ledelsen i Trondheim kommune gjennomført noen sporadiske kompetanseløft og benyttet tester i form av simulerte e-poster. I tillegg arbeider de med å ansette flere medarbeidere. Kommunene har også fått gjennomført revisjoner som ser på status av arbeidet med digital sikkerhet. Dette har skjedd ved hjelp av eksterne partnere:

> *De peker på noen sårbarheter som vi bør jobbe med videre. Det handler først og fremst om organisering og forankring av disse perspektivene lenger ut i organisasjonen, enn hos de som jobber med IT. (Informant 1)*

Med utgangspunkt i kapitlene over, later det til at arbeidet med forankring lengere ut i organisasjonen fremdeles er i startfasen. IT-avdelingen gjør mye av arbeidet og gjennomførte en øvelse på utbrudd av krypto-virus i fjor. Et mer omfattende organisatorisk tiltak ble gjennomført i april 2022. Trondheim kommune opprettet en ny enhet: sikkerhet og beredskap. Her kan flere aktører innen diverse sektorer i kommunen arbeide sammen. De ser på sikkerhet generelt, men digitale hendelser er en del av det helhetlige bildet, noe som påvirker nasjonal sikkerhet. I disse tider vurderer enheten hvilken rolle de skal spille, særlig i forbindelse med krigen i Ukraina. Ifølge Riksrevisjonen (2023) har pandemien fått konsekvenser for planlagte tiltak på det digitale område. Det er også tenkelig at de ansatte er begrenset av taushetsplikt og kan dermed ikke oppgi fullstendig informasjon om hva organisasjonen planlegger. Informant 2 nevner likevel at de har arbeidet med å klarere ansatte, noe som er viktig for en gunstig tilgangsstyring:

> *Så er det en del tiltak som allerede er gjennomført. Noe av det kan jeg nevne, som at vi har sett på en del nøkkelposisjoner og ledere i kommunen som er klarert på ulike nivå, det er typisk da konfidensielt og hemmelig i henhold til sikkerhetsloven. (Informant 2)*

Midtre Gauldal arbeider med forankring i ledelsen og kompetanseheving. Kommunen planlegger et kurs for ledere og nyansatte. I tillegg forsøker de å bedre prosesser rundt risikovurderinger:

> *Et direkte tiltak er jo egentlig det kurs-opplegget da, som vi planlegger å rulle ut jevnlig. [...] Også har vi innført noen prosedyrer som skal sikre at vi kommer i forkant, hvis vi gjør noen anskaffelser så skal vi ha det på stell, altså i prinsippet skal det bli gjort en ROS [...] Så den rutinen, den må vi holde på å skjerpe litt hele tiden, men det er et godt tiltak da for at vi skal komme i gang riktig når vi anskaffer ting. (Informant 8)*

Det er også synlig at ledelsen tar mer initiativ enn tidligere. Kommunen har blant annet innført en årlig oppsummering av sikkerhetsarbeidet. I et slikt møte ble det bestemt at Midtre Gauldal kommune skulle investere i et nytt verktøy gjennom en leverandør:

> *[...] etter en årlig gjennomgang, investerte vi i et nytt skritt opp på sikkerhet da, et verktøy rett og slett hos en leverandør, for å garantere seg bedre. [...] Da kjente vi at vi måtte opp i programvare, for å gå opp i sikkerhetsnivået. Så det var en investering. (Informant 6)*

Tiltaket blir også et samtaleemne i fokus-gruppe intervjuet. Informant 7 reflekterer over tiltaket som både positivt og nødvendig, men ønsker å presisere at arbeidet med digital sikkerhet krever mer kontinuitet:

> *Men så har man liksom forklart og forsvart en overvåkningstjeneste, for det koster penger da [...] Jeg tror at et tiltak man har gjort da kanskje er å betale litt penger også tro at man er ferdig med saken for en stund. Men IT-sikkerhet må man jobbe med kontinuerlig. (Informant 7)*

Fosen IKT har også iverksatt kompetansehevende tiltak som ble avklart i kapittelet om mennesker. Et av de største tiltakene som blir trukket frem er en beredskapsøvelse på informasjonssikkerhet. Det er i midlertidig kun en av Fosen-kommunene som har planlagt dette i samarbeid med Fosen IKT:

> *Vi har ikke hatt det tidligere, men vi skal ha en nå i Ørland kommune i mai. En stor en, og den skal jo tjenestene tas ned en hel dag på faktisk, både skytjenestene og lokale tjenester. (Informant 4)*

Følgelig befinner Fosen IKT seg i en vurderingsfase, som gjelder ansettelse av en informasjonssikkerhetsleder. Det er ikke et tiltak som er gjennomført, med det kan anses som en mulighet for å samle flere ressurser og forankre roller blant de fire kommunene. Dette er noe som også fremstår som viktig i samtale med KS-informantene, som hevder at det er nødvendig med et strategisk sikkerhetsledd. I det daglige arbeider Fosen IKT med risikovurderinger, kartlegging av systemer og observering av de fire kommunene.

> *Så vi prøver jo som sagt å få til et samarbeid på informasjonssikkerhetsleder [...] hver enkel kommune har kanskje ikke mulighet til å ha det på egenhånd, men sammen så kan det være de får på plass en sånn en da. (Informant 5).*

Funnene fra analysen påpeker en viktig endring som finner sted i alle kommunene: et økt fokus på digital sikkerhet og mer bevissthet rundt konsekvenser av digitale angrep. Flere forstår at sjansen for å oppleve uønskede hendelser er høy.

> *Også skal man ikke være arrogant heller fordi alle kan tas. Alle kan tas. Og den dagen man tror at, nei, men det er ingen som tar meg. Så, så har man tapt. (Informant 3)*

6. Diskusjon

I det foregående kapittelet ble oppgavens empiriske resultater presentert. Informantenes synspunkter om arbeidet med digital sikkerhet ble vektlagt, og en dokumentanalyse bidro til å underbygge disse funnene. Resultatene belyste et behov for å bedre kunne utnytte menneskelige ressurser gjennom læring av feilhandlinger. Deretter ble det tydelig at både kommunene og det interkommunale samarbeidet har gode teknologiske egenskaper. O-faktoren viser behov for flere øvelser og samarbeid. I tillegg er sterkere ansvarsfordeling og kunnskap om risikostyring gunstig for å styrke den digitale sikkerheten. I denne delen av oppgaven vil resultatene drøftes opp mot det teoretiske grunnlaget.

6.1. Mennesket i sentrum av digital transformasjon

I teori-kapittelet 3.3. ble det avklart at menneskelige evner er essensielt for å skape resiliens, slik at en kan tilpasse seg skiftende omgivelser og dermed være i sentrum av digital transformasjon (Grøtan et al., 2022). Den empiriske analysen viser at læring av egne feil er noe informantene anser som viktig, men at dette allikevel ikke blir håndtert på best mulig måte. Kollektiv læring på tvers av hele kommunen eller kommunesamarbeidet bør iverksettes. Med utgangspunkt i dette kan informantene etablere mer bevissthet om resiliens, med tanke på hvordan en organisasjon skal fungere under forventede og uforventede forhold.

Læring for å utvikle resiliens

En av de fire funksjonene som Hollnagel (2022) formidler er evnen til å *lære*. Det er et viktig middel for å fremme resiliens og dermed mestre de tre andre evnene om å *respondere, observere* og *forutse*. Flere av informantene hevder at menneskelige feil bør snakkes mer om. Det vil likevel være viktig å ivareta en åpen og trygg kultur, slik at de ansatte tør å innrømme avvik. Litteraturen støtter også at en åpen kommunikasjon mellom ansatte og ledere er essensielt for å håndtere digitale trusler (Loonam et al., 2022). På grunnlag av datainnsamlingen fra intervjuene, blir menneskelige feil ofte vurdert som kilden til et sikkerhetsbrudd. Slike empiriske funn gir et inntrykk av svak forståelse for andre bakenforliggende årsaker. Ifølge Schiefloe (2017) kan manglende opplæring, fraværende kommunikasjon og svak sikkerhetskultur resultere i menneskelig svikt.

Litteraturen påpeker også viktigheten av å lære av det som gikk bra (Hollnagel, 2022). Utsagnene fra analysen indikerer at alle de tre casene arbeider med å bedre M-faktoren, gjennom opplæringsinitiativ og mål om bevisstgjøring. Det er tenkelig at digital transformasjon og et økt trusselnivå har forsterket behovet for læring. Tidligere forskning har sett manglende kompetansehevende aktiviteter (Digdir, 2020). Funnene indikerer derimot at kommunene i utvalget forsøker å forbedre dette. Ifølge Kongsvik et al. (2018a) er menneskelige erfaringer nyttig i det kompleksiteten i organisasjoner øker. Flere av informantene trekker frem god tilpasningsevne som et resultat av pandemien. Dette tyder på at deltakerne har sett nytteverdien av menneskelige evner og har mulighet til å utnytte disse i håndtering av kriser. Det er likevel tenkelig at organisasjonene kan bli mer bevisst på ytelsen av slike evner, også under hverdagslige forhold og i henhold til digital sikkerhet.

Noen av informantene hevder at manglende forståelse blant toppledelsen er problematisk. Informantene fra Fosen IKT ser blant annet utfordringer med engasjement,

noe som kan påvirke prioritering fra omgivelsene i negativ retning. Tidligere forskning viser at ledere må sørge for kontroll over komplekse nettverk og digital transformasjon, og iverksette læring og samskaping i organisasjonen for å støtte resiliente prosesser (Lips, 2020; Loonam et al., 2022; Wilson & Mergel, 2022). Ulike tiltak gjennom sikkerhetskampanjer og *phishing-mailer* kan vurderes som nyttig i det digitale sikkerhetsarbeidet. Funnene tyder likevel på at dette ikke er nok for å sikre et systematisk arbeid rundt sikkerhetskulturen. Dette er synlig da alle organisasjonene kun iverksetter sporadiske kompetanseløft eller informasjonsformidling. Likevel har både Midtre Gauldal kommune og Trondheim kommune ambisjoner om å gjennomføre opplæring om digital sikkerhet, når nyansatte begynner i kommunen.

Felles mål og forståelse for å utvikle cyber-resiliens

Kompetansekampanjene fremmer et samspill mellom mennesker og teknologi. Ifølge litteraturen skal det på denne måten oppstå kollektive mål som bidrar til å etablere en kultur. Dette fremmer muligheten til å utvikle *cyber-resiliens* (Xu & Lu, 2022; Loonam et al., 2022). Det er allikevel mulig at økt bevissthet rundt svindelteknikker vil være noe utilfredsstillende. Funnene tyder på at lederne strever med å frembringe nødvendige atferdsendringer. Dette vil trolig kreve et ytterligere samspill mellom mennesker og organisering. Informantene understreker et behov for organisatoriske ferdigheter som sikkerhetsstyring og risikovurderinger. Engen et al. (2016) presiserer at menneskene må etablere et felles språk innad i organisasjoner. På denne måten vil de ansatte i kommunal sektor trolig bli bedre egnet til å imøtekomme dagens risikobilde.

Resultatene fra Trondheim kommune retter oppmerksomhet mot rekrutteringsutfordringer. Det ble hevdet at dette er et av de største problemene som kommunen har. Først eksisterer det dårlig kompetanse i markedet. Det er tenkelig at det er behov for bedre samhandling mellom akademia og arbeidslivet for å overkomme dette, likevel har endringer i studietilbud og statlige midler trolig forandret situasjonen (Riksrevisjonen, 2023). Forskning av Wilson og Mergel (2022) poengterer at konkurranse med privat sektor kan ha påvirkning på rekrutteringsmulighetene. Med utgangspunkt i en slik forklaringsvariabel kan kommunal sektor forsøke å gjøre sektoren mer attraktiv, særlig for nyutdannede som har tilegnet seg nødvendig kompetanse om digital sikkerhet. Slike utfordringer kan også overkommes med gode samarbeidsnettverk. Tidligere forskning viser at det er verdifullt å arbeide på tvers av siloer for å innhente tverrfaglig kompetanse. En kan dermed tilrettelegge for samskaping mellom sektorer i kommunen og mellom private aktører (Almklov et al., 2018; Lips, 2020).

Resultatene viser at Midtre Gauldal kommune ønsker mer samarbeid. Det er sannsynlig at en mellomstor kommune som står alene i arbeidet med digital sikkerhet har et større behov for dette, enn en stor kommune med flere ressurser. Likevel kan det være nødvendig at kommunene og kommunesamarbeidet legger til rette for økt flyt av kommunikasjon og læring på tvers av avdelinger. I tillegg kan det være gunstig å benytte tilgjengelig informasjon. Informantene fra KS nevner blant annet ulike kompetanse-tilbud som kan være til nytte for kommunene.

6.2. Teknologi som beskytter mot «det onde».

Schiefloe (2017) presiserer at den teknologiske kapasiteten må være tilstrekkelig gjennom bruk av redundans. Funnene viser at dette er noe organisasjonene har innført. I tillegg arbeider IT-avdelingene med å oppdatere og oppgradere systemer for å lukke kjente sårbarheter. Bruken av back-up systemer, tofaktorautentisering, penetrasjonstester og overvåkningstjenester er virkemidler som informantene nevner. Likevel er digitale sårbarheter og trusler et konstant bekymringselement. Dette har tilhørighet med begrepet som ble nevnt i kapittelet om tidligere forskning: nulldagssårbarheter. Slike sårbarheter har ikke blitt kjent, noe som skaper vanskeligheter i kampen mot hackerne (Bergsjø, 2020). En rask teknologisk utvikling og et etterslep av sårbarheter kan vurderes som en kamp mellom «de gode og de onde». En slik kamp vil derimot ikke være rettferdig. Dette kan ses i lys av utfordringer med risikostyring. Utsagnene fra intervjuene viser at trusselaktører alltid vil være på jakt og klare for angrep. I tillegg ble det nevnt at det tar tid å gjenopprette et system. Dette samsvarer med litteratur om at restrisiko alltid vil eksistere (Ahmeti & Vladi, 2017). Dermed blir behovet for resiliens viktig, da ansatte må arbeide med å redusere langvarige skader (Hollnagel, 2022).

Resultatene fra analysen indikerer at IT-avdelingene arbeider tett med sikkerhetsloven, ved å ivareta prinsipper om konfidensialitet, integritet og tilgjengelighet. Tilgangsstyring er et av elementene som utpeker seg i arbeidet med den teknologiske sikkerheten. Det er likevel manglende forståelse for hvilke behov som må dekkes for å oppnå sikkerhetsmålene i andre deler av kommunene. Dersom ledere får bedre forståelse av kunnskapen rundt teknologi, kan de trolig se en helhetlig sammenheng i arbeidet med digital sikkerhet. Funnet presiserer nødvendigheten av et samspill mellom mennesker og teknologi, noe som vil gi rom for produktivitet (Kongsvik et al., 2018a). Flere ledere, uavhengig av arbeidsfelt, bør dermed gjennomgå kursing innen informasjonssikkerhetsstyring. Milakovich (2022) fremhever at vellykket digital transformasjon av offentlige tjenester krever høyt utdannede ansatte. Et av utsagnene fra analysen hevdet at mange tror arbeidet består av 80% teknologi. En slik mistolkning kan redusere systemenes evne til å komplementere hverandre, noe som trolig vil svekke et helhetlig arbeid.

Forskning om digital governance sier at nye teknologier vil drive frem en organisasjonsutvikling, men ofte må nye systemer kombineres med eldre løsninger (Lips, 2020). Informantene fra Midtre Gauldal og Fosen IKT påpeker slike utfordringer. Dette kan tyde på at en stor kommune har mer kapasitet og ressurser til å håndtere omfattende teknologiske endringer. Trondheim kommune kan dermed ha kommet lenger i arbeidet med digital transformasjon. Det kan likevel oppstå forvirring og manglende kontroll, selv i Trondheim kommune, forårsaket av økt flyt og deling av data. Det er derfor viktig at ledere har god forståelse av lovverket (Kongsvik et al., 2018). Dette ansvaret er pålagt kommunedirektøren (Kommuneloven §25-1). Kompleks infrastruktur og manglende samhandling mellom ulike teknologier gjør dette mer krevende, og stemmer overens med teknologiske barrierer som forekommer i forskningen til Wilson og Mergel (2022). I tillegg vil komplekse systemer og tette koblinger, ifølge Perrow, rammes av systemfeil før eller siden (Rijpma, 1997).

De empiriske funnene indikerer at Trondheim har sterke sikkerhetsmekanismer på plass, men at systemene blir mer komplekse i en stor kommune. Utsagnene fra intervjuene

fremmer at organisasjoner må unngå å være avhengig av utdatert teknologi og muligens flytte utsatte tjenester til nettskyen. I tillegg må en være klar til å handle raskt dersom et digitalt angrep bryter gjennom de teknologiske beskyttelsesmekanismene. Teknologien kan dermed ikke bekjempe «det onde» alene. De empiriske resultatene om teknologi kan bidra til å fylle forskningshullet om sammenhengen mellom digital transformasjon og digital sikkerhet. Et kontinuerlig arbeid med teknisk sikkerhet virker forekommende blant alle organisasjonene. Det er likevel mulig at manglende øvelser på organisatorisk nivå svekker en nødvendig handlekraft, noe som vil bli nærmere utforsket i neste delkapittel. Dette kan forstyrre evnen til å *respondere* på forandringer (Hollnagel, 2022). Det er tydelig at deltakerne savner bedre forankring mellom teknologi- og organisasjonsarbeidet. Det har resultert i at teknologi-ansatte delvis har måtte bære ansvaret alene, gjennom å styrke og overvåke den teknologiske kapabiliteten, for å kompensere for mangler i M- og O-faktorene. Dette betyr ikke at en skal arbeide mindre med teknologien, men at flere må ta ansvar for å administrere styringen rundt økende grad av digitalisering.

6.3. Organisering, limet i en helhetlig tilnærming

I masteroppgaven har tre caser med ulike kommunestørrelser og strukturer blitt analysert. Ifølge litteraturen om cyber-resiliens kan det være gunstig at organisasjoner sammenlignes med andre for å vurdere hvilke prosesser og verdier en vil ta med seg videre (Loonam et al., 2022). O-faktoren er ifølge Kongsvik (2013) kompleks å utforske. Likevel kan organisering anses som limet i en helhetlig tilnærming. Tidligere forskning har fremhevet teknologien som mest sentral, men det er et behov for ytterligere forskning om underliggende forhold (Rasmussen, 1997; Schiefloe, 2017). Jeg forsøker å fylle dette hullet. I analysen ble elementer rundt organisering av arbeidet først introdusert. Følgelig vil funnene innen denne kategorien diskuteres.

Rollefordeling, beredskapsøvelser og samarbeid

Det oppfattes som at Midtre Gauldal kommune og Trondheim kommune har fordelt formelle roller. Det varierer derimot om dette er fullstendig dedikerte roller eller om aktørene har andre arbeidsoppgaver i tillegg. Fosen IKT har noe svakere rollefordeling. Det er også varierende forankring blant de fire Fosen-kommunene, som gjør at samarbeidet ikke strekker til innenfor O-faktoren. Det kan virke som at et interkommunalt samarbeid er gunstig for å styrke tekniske ressurser. Likevel vil flere elementer av digital sikkerhet kreve tilstrekkelig kommunikasjon, god ledelse og felles formål (Schiefloe, 2017; Potrich et al., 2022). Funnene fra Fosen IKT indikerer noen vanskeligheter med dette. Det er likevel tenkelig at inntreden av en informasjonssikkerhetsleder kan være et positivt tiltak. Det er synlig at mindre kommuner har færre forutsetninger for å realisere dedikerte roller. Det er likevel nevneverdig at Trondheim kommune også har vanskeligheter med å delegere ansvar ut til tjenesteområdene. Dette peker i retning av svak samordning mellom tjenesteenheter, noe som trolig krever mer kapasitet og ressurser til å arbeide med digital sikkerhet. Dette kan også signalisere at organisasjonene mangler klare retningslinjer for de ansatte og en organisatorisk strategi (Khando et al., 2021; Loonam et al., 2022).

De empiriske resultatene peker på manglende helhetlige planer, noe som trolig påvirker prioriteringen av digital sikkerhet. Ifølge Milakovich (2022) mangler offentlige virksomheter standardiserte styringssystemer, noe som også kommer frem i intervjuene. Organisasjonene har hatt vanskeligheter med å implementere ISO 27001 til eget bruk.

Slike funn samsvarer med organisatoriske barrierer som mangel på strategi og kapasitet til ledere (Wilson & Mergel, 2022). Samtidig vitner dette om at eForvaltningsforskriften §15 ikke etterfølges på best mulig måte. Det er tenkelig at det forventes for mye av kommunene. Det er ønskelig at de benytter internasjonale standarder, men slike verktøy er ofte dyre og ressursene strekker ikke til. Det kan likevel være gunstig å etablere en informasjonssikkerhetspolicy i form av dokumentering for å synliggjøre krav, ansvar og mål ut i organisasjonen.

Resultatene viser at informantene ser verdien av øvelser som trolig kan forsterke læringspotensialet for resiliens. Øvelser kan også bidra til å utvide organisasjonens nettverk, noe Grøtan et al. (2022) mener er nyttig for at flere avdelinger forstår den digitale sikkerhetsstrategien. Derimot kreves flere ressurser for å iverksette øvelser for digital sikkerhet. Det blir vurdert at disse utfordringene kan overkommes med bidrag på nasjonalt nivå. For eksempel kan aktuelle direktorater bidra med midler og planlegging for at kommunene skal lykkes med slike øvelser. Øvelser kan gi ledere trening i å vurdere mulige samfunnskonsekvenser av digitale angrep, og søke etter realistiske mål om håndtering av situasjonen. Dette fremmer en cyber-resilient tilnærming, hvor risikostyring er sentralt (Grøtan et al., 2022; Loonam et al., 2022). Informantene nevner også at det er forskjell på fysiske og digitale skader. Generelle beredskapsøvelser er muligens ikke tilstrekkelig for å forberede organisasjonen på uforventede hendelser innen det digitale domenet.

Funn fra KS-informantene indikerer at samarbeid er nøkkelen for å løse flere av utfordringene i kommunal sektor. Det virker som at organisasjonene er avhengig av hjelp fra private leverandører. Ifølge Almklov et al. (2018) må organisasjoner søke samskaping internt og ekstern for å oppnå robusthet. Digitaliseringsnettverkene kan bidra til å fremme samarbeid mellom kommuner, og ta en mer aktiv rolle i gjennomførelse av ulike prosjektrelaterte situasjoner. Likevel presiserer Riksrevisjonen (2023) at flere samarbeid kan resultere i komplekse verdikjeder. Dette kan ses på som en konsekvens av digital transformasjon, der deling av data på tvers av aktører medfører flere sårbarheter. Det stilles dermed sterkere krav til sikkerhetsstyring som å etablere et akseptabelt risikonivå (Kongsvik, 2013). Det kan være utfordrende for kommuner å vurdere risikokriterier. Derfor mener Engen et al. (2016) at ledere bør forsøke å fylle diverse kunnskapshull, i tillegg til å vurdere viktige etiske og politiske føringer. Dette kan brukes for å avgjøre hvilke verdier organisasjonen trenger å sikre.

Ledelse og aktuelle endringer

Ledelse har vært sentralt gjennom hele oppgaven og har dermed også utpekt seg i M- og T-faktoren. Det er tydelig at lederne har tatt en mer aktiv rolle enn tidligere gjennom iverksetting av kompetanseløft. Likevel må lederne også sørge for tillit og strategiske mål (Bracci et al., 2021). Funnene indikerer at det er avgjørende å ha ledere som kan operere i en digital kontekst, for å skape en læringsarena der både feil og suksesser kan deles. Resultatene fra analysen viser at det er vanskelig å definere et akseptabelt risikonivå. Tidligere forskning presiserer at flere involverte parter og byråkrati gjør risikostyring kompleks i offentlig sektor (Ahmeti & Vladi, 2017). Derimot indikerer funn at lederne har fått mer trening på dette, gjennom håndteringen av pandemien. En bør ifølge KS-informantene iverksette planer for hvordan kommunen skal håndtere at systemer blir utilgjengelig og hvor lenge en kan operere i et slikt landskap. Dette fremmer en balanse mellom etterlevelse og tilpasningsevne, noe som Grøtan (2017) anser som essensielt. I tillegg viser Perrow at komplekse systemer behøver både desentralisert og sentralisert

ledelse (Rijpma, 1997). Det kan dermed være viktig å sentralisere beslutninger for å etterleve regelverket. Samtidig bør en også tillate desentralisering for å oppnå større grad av effektivitet, ved å gi kompetente ansatte et større ansvar.

Loonam et al. (2022) presiserer at ledere må ha god forståelse av organisasjonens teknologiske kapabiliteter og tilpasningsevner. De må redegjøre for en gunstig hastighet av digital transformasjon. Deltakerne i fokus-gruppen bemerket at manglende vurderinger på nye teknologiske løsninger forekommer. Dette vil trolig forhindre en gunstig sammenfiltring av teknologi og arbeidsprosesser. Dersom gevinstene fra digitale teknologier ikke blir utnyttet, mister de verdi og organisasjoner mislykkes i å tilpasse endrede sosio-tekniske strukturer (Osmundsen et al., 2018). Endringer i en digital verden vil trolig være uunngåelig. Med hensyn til dette må tillit og en helhetlig forståelse prege sikkerhetskulturen. Tidligere forskning presiserer dermed at en må unngå å delegere alt av ansvar videre til IT-avdelingen, da dette ikke egner seg for å oppnå cyber-resiliens (Bergsjø et al., 2020; Loonam et al., 2022). Ulike sikkerhetstiltak, øvelser og tydelige strategier kan muligens bedre ledernes forståelse for risikostyring og dermed bidra til å ivareta kontroll ut i organisasjonen.

Resultatene om endringsrutiner viser at ytre faktorer som pandemien og invasjonen av Ukraina har resultert i økt prioritet av det digitale sikkerhetsarbeidet, både på lokalt og nasjonalt nivå. Kommuneansatte har dermed blitt mer oppmerksomme. Likevel sørger økt angrepsaktivitet for at kommunene må etablere mer kontroll enn tidligere. Det har gjort at de tre organisasjonene har benyttet flere ressurser på teknisk sikkerhet. Funnene indikerer at endringene har blitt «den nye normalen», noe som gjør det utfordrende å etablere objektive risikoakseptkriterier. Endringer i samfunnet har resultert i enda større grad og hastighet av digital transformasjon. Teorien tilsier at ledere må *observere* situasjonen og på denne måten skape oversikt over endringene. Følgelig må en forsøke å *forutse* hvordan endringene kan påvirke organisasjonens opptreden (Hollnagel, 2022).

Det kan være gunstig å innlemme digital sikkerhet inn i det øvrige sikkerhetsarbeidet. Ifølge litteraturen om cyber-resiliens skal digitale strategier være i tilhørighet med andre virksomhetsområder (Loonam et al., 2022). Funnene viser at et økt trusselnivå synliggjør behovet for et helhetlig arbeid, hvor en må stille krav til leverandører for å opprettholde internkontroll. Digital sikkerhet bør derfor være synlig i flere deler av kommunen, på tvers av fagfelt.

Iverksetting av tiltak

Til slutt viser funnene at lederne har iverksatt flere tiltak for å bedre det digitale sikkerhetsarbeidet. Det er særlig bemerkelsesverdig at Midtre Gauldal kommune og Fosen IKT, som har færre ressurser enn Trondheim kommune, også har iverksatt ulike sikkerhetshevende tiltak. Tiltak som direkte påvirker O-faktoren, er noe mangelfullt. Dette indikerer at det fortsatt eksisterer svak forståelse av hva digital transformasjon og digital sikkerhet krever, nemlig en helhetlig tilnærming. Resultatene viser likevel noen prioriteringer av risikovurderinger og rolleforankring. Dette anses som viktig for å bedre O-faktoren. Riktignok omtaler informantene hovedsakelig opplæringsprogrammer og innstramming på teknisk nivå. Dette skal likevel ikke misforstås som noe negativt, til tross for at flere tiltak som styrker styring- og internkontroll bør iverksettes. Fosen IKT sammen med Ørland kommune utpeker seg da de skal gjennomføre en beredskapsøvelse, noe som kan forsterke oppbyggingen av resiliens. Selv om

kommunene ikke har opplevd alvorlige digitale angrep, er det likevel viktig å øve på hvordan systemer fungerer generelt. Dette vil muliggjøre kartleggingen av funksjonene deres og sørge for at de kan motstå uforventede hendelser (Hollnagel, 2022). Det er også viktig at ledere forstår at arbeidet krever kontinuitet, selv etter at tiltak er iverksatt. Usikkerhet blant ledelsen og svak rolleforankring kan forklare at flere tiltak og planer gjenstår å se.

6.4. Oppsummering

Tidligere forskning viste at kommunestørrelse kan ha betydning for hvordan det arbeides med digital sikkerhet (Digdir, 2020; Riksrevisjonen, 2023). Funnene som har blitt uthevet i den empiriske analysen kan bekrefte dette, men påstanden kan samtidig utfordres. Midtre Gauldal kommune har en god oversikt over roller, i tillegg har lederne iverksatt flere tiltak som skal bedre den digitale sikkerheten. Fosen IKT har samlet tekniske ressurser og kompetente medarbeidere. Samarbeidet mangler et optimalt styringssystem, men de arbeider med en øvelse for å bedre dette. Trondheim kommune har flere ressurser og mer kapasitet enn de mindre kommunene i utvalget. De har derfor flere muligheter til å fordele roller og arbeidsoppgaver, noe som er synlig i arbeidet med rekruttering. Likevel kan en stor kommune bestå av komplekse systemer. Det kan derfor være utfordrende å ha oversikt og vurdere hvilke tiltak som bør prioriteres.

Tidligere forskning viste at MTO-perspektivet bør utnyttes mer, ikke bare for fysiske ulykker i bransjespesifiserte områder, men også i lys av digital sikkerhet (Kongsvik, 2013; Grøtan et al., 2022). Oppgaven har forsøkt å vise at menneskelige, teknologiske og organisatoriske faktorer påvirker hverandre. Perspektivet gir innsikt i utfordringer som kommunene har med digital transformasjon og komplekse systemer. Ledelse er sentralt i tidligere forskning, men det er ikke godt nok forankret i resiliens-litteraturen (Hollnagel, 2022). De empiriske resultatene og diskusjonen har bidratt med enda mer forskning om ledelse for å utvikle cyber-resiliens. Det er også ønskelig at funnene tilfører mer forskning på viktigheten av roller- og ansvarfordelinger i offentlig sektor. I tillegg peker oppgaven på et bredere forskningsomfang enn kun teknologiske aspekter. Til tross for at funnene har avdekket flere utfordringer i kommunal sektor, viser resultatene at kommuner også oppnår betydelige fremskritt og er på rett vei i arbeidet med digital sikkerhet. Neste kapittel vil oppsummere svarene på oppgavens problemstilling og forskningsspørsmål, samt presentere et forslag til videre forskning.

7. Avslutning

Formålet med masteroppgaven har vært å utforske et digitalt sikkerhetsarbeid med to kommuner og et kommunesamarbeid i Trøndelag som case. Dette har blitt gjort ved å ta i bruk et sikkerhetsperspektiv (MTO). I arbeidet med analysen ble det tydelig at det har oppstått et økt fokus på digital sikkerhet som et resultat av dagens risikobilde. Likevel viste analysen at arbeidet med å iverksette en helhetlig tilnærming kan være lettere sagt enn gjort. Det er spesielt utfordrende for kommuner som er begrenset i form av størrelse, kapasitet, ressurser og komplekse systemer. Innledningsvis ble oppgavens problemstilling presentert: *Hvilke endringer og tiltak har dagens risikobilde utløst i kommunal sektor?* Problemstillingen ble videre operasjonalisert gjennom tre forskningsspørsmål som tar utgangspunkt i det valgte perspektivet:

1. Hvordan kan *menneskelig* kompetanse møte dagens risikobilde?
2. Hvordan benyttes *teknologi* for å nå sikkerhetsmålene?
3. Hvilke tiltak gjør lederne i *organisasjonen* for å forbedre sikkerhetsarbeidet?

I denne delen av oppgaven skal svarene på forskningsspørsmålene oppsummeres og deretter bidra til å begrunne et endelig svar på den overordnede problemstillingen. Forskningsspørsmålet om mennesker ble fremhevet i underkapittelet 5.1.1. Der ble det redegjort for behovet for kompetanse, sett i lys av mennesker som feilkilde og mennesker som ressurs. Det er nødvendig å lære av egne feil for å utnytte menneskelige evner på best mulig måte. Dersom menneskenes kompetanse om digital sikkerhet er tilstrekkelig, kan de være bevisst på hvilke trusler som eksisterer og hvordan de skal håndtere dette. Det kan eksempelvis innebære å ikke trykke på en falsk lenke. Likevel viser oppgaven at mennesker også kan møte dagens risikobilde med et felles språk som redegjør for en helhetlig forståelse av sikkerhetsarbeidet. Dette vil trolig bedre prioritering av ulike sikkerhetstiltak. Deretter vil god ledelse gjennom generering av tillit sørge for en åpen og tydelig kommunikasjon, som er nødvendig for å forankre en sikkerhetskultur. I tillegg vil dette bidra til å redusere skadeomfanget fra oppståtte situasjoner, ved at ansatte tør å innrømme et sikkerhetsbrudd. Følgelig vil opplæringsprogrammer forsterke evnen til å fungere under hverdagslige aktiviteter, som bidrar til forebygging av uønskede hendelser. På denne måten kan menneskelig situasjonsforståelse styrke kapasiteter rundt risikostyring, og etablere en nødvendig balanse mellom regler og tilpasningsevne.

Forskningsspørsmålet om teknologi ble studert i underkapittelet 5.2.1. Teknologi benyttes på den måten at programvarer og verktøy arbeides kontinuerlig med for å sikre at de har tilstrekkelig redundans for å bekjempe sårbarheter. Det er tydelig at IT-avdelingene har mange oppgaver som de må ha kontroll over. Overvåkningstjenester, brannmurer og «back-up» systemer benyttes for å dekke sikkerhetsmålene om konfidensialitet, integritet og tilgjengelighet. Systemene må dermed være beskyttet og til å stole på. Organisasjonene sørger for flyt av data gjennom tilgangsstyring. I slike tilfeller kan teknologien benyttes til å se hvor en ansatt logger seg på fra. Det er også blitt mer forekommende med tofaktorautentisering for å etablere sikker sone. Nye og gamle systemer må ofte balanseres, grunnet en økende digital transformasjon, noe som krever tilstrekkelig oversikt. Funnene fra intervjuene indikerer at det kan være viktig å kartlegge og flytte tjenester som er spesielt utsatt for angrep til «skyen». De ulike tekniske løsningene bidrar til å overholde sikkerhetsmål, men de krever bedre styring og administrering, for å ha kontroll over komplekse systemer som finnes i en kommune.

Følgelig ble forskningsspørsmålet om organisering redegjort for i underkapittelet 5.3.4. Det ble nevnt flere tiltak som lederne arbeider med. For å ha oversikt over disse er det blitt utformet en tabell som skal fremheve svaret på det siste forskningsspørsmålet. Tiltak som informasjonskampanjer, rekruttering, nye teknologiske løsninger og forankring av roller er et resultat av dagens risikobilde. Dette bidrar til å svare på den overordnede problemstillingen, om tiltak og endringer forårsaket av et samfunn i endring. Dagens risikobilde har utløst flere endringer, blant annet opplever informantene fra Fosen IKT at ledergruppene fra de ulike kommunene tar mer initiativ til å diskutere digital sikkerhet enn tidligere. I Midtre Gauldal kommune har de opplevd store endringer og mer flyt av data som har økt behovet for risikovurderinger. Dette er også gjeldende for Trondheim kommune, som har sett seg nødt til å stramme inn det tekniske nivået. Det har også oppstått endringer på politisk nivå, som har resultert i noe mer tilgang på ressurser. I tillegg har mediebildet sørget for at ansatte er mer nysgjerrige enn før og har bedre forståelse for hvilke trusselaktører som finnes. Økt angrepsaktivitet har fått lederne til å forstå at sikkerhetsarbeidet krever en helhetlig tilnærming der flere hensyn må tas. Det er blant annet formidlet et behov for mer samarbeid både internt og ekstern, særlig blant de mindre kommunene i utvalget.

De ulike tiltakene som ble presentert i kapittel 5. er visualisert i Tabell 5 i Vedlegg C. Den viser at Trondheim kommune har flere tiltak innen O-faktoren, noe som forsteker behovet for samarbeid og assistanse i de mindre kommunene. Allikevel viser oppgavens diskusjon at alle kommunene har utfordringer uavhengig av størrelse. Det er også inkludert noen planer om tiltak, da det ble formidlet at disse skal iverksettes i nærmeste fremtid. Leseren må ta høyde for at det kan være andre tiltak som organisasjonene arbeider med, men denne oppgaven har tatt utgangspunkt i det som ble fortalt av informantene gjennom semi-strukturerte intervjuer.

7.1. Forskningens relevans og begrensninger

Det er mye en kan studere innenfor sikkerhet. I arbeidet med teori og tidligere forskning fikk jeg et inntrykk av at sikkerhet er et bredt forskningsområde. Det eksisterer flere teorier og fenomener innen sikkerhet som strekker seg utover ulike fagområder og blir påvirket av forskjellige organisasjonsstrukturer. Det ble valgt å spisse tematikken til å omhandle digital sikkerhet, i henhold til eget interesseområde. I tillegg viste litteraturen at dette er i sterk tilhørighet med digital transformasjon, noe som har vært et sentralt begrep gjennom to år på masterstudiet «Organisasjon, digitalisering, administrasjon og arbeid». Det var ønskelig å utforske ulike kommunestørrelser og strukturer for å få en bred forståelse rundt oppgavens tematikk. Det var også tenkelig at et variert utvalg enklere kan generaliseres opp mot andre kommuner i landet. Likevel kan de tre organisasjonene anses som komplekse. En kommune har gjerne flere enheter med ulike organisatoriske føringer. Det kan ha medført noen begrensninger for forskningen, da det er utfordrende å få en dyptgående innsikt i alle de tre organisasjonene. Jeg har blant annet ikke inkludert perspektiver fra ansatte uten et lederansvar eller særskilt ansvar innen informasjonssikkerhet. Likevel har det blitt presentert et variert utvalg med totalt 10 informanter med ulike arbeidsoppgaver, som har bidratt til å belyse oppgavens empiriske omfang. I tillegg har informantene fra KS gitt et eksternt syn på kommunenes utfordringer, og har bidratt til å utvikle anbefalinger til kommunene.

Som nevnt i oppgavens metodekapittel kan det finnes utfordringer ved å generalisere oppgavens funn. Det er likevel slik at forskeren selv kan beskrive hvilke situasjoner

resultatene er gyldige, som viser til en moderat generalisering (Tjora, 2018). Det er tenkelig at en oversikt over sikkerhetstiltak i de tre organisasjonene kan fremme informasjonsformidling, samarbeid og innovasjon i kommunal sektor. Det kan være at organisasjonene i utvalget blir inspirert av hverandre og kan søke hjelp fra hverandre. I tillegg vil et digitaliseringsnettverk som DigiTrøndelag få innsikt i kommunenes utfordringer, og dermed vurdere egen rolle i arbeidet med digital sikkerhet. Kommunene vil trolig trenge bistand til å etablere ulike sikkerhetsløsninger og tiltak, da tilgjengelig ressurser og kapasitet kan variere.

Digital sikkerhet kan anses som et stort tema, hvor bruken av oppgavens perspektiv har sørget for aktualisering av ulike forhold. Det har blitt forsøkt å begrense oppgavens omfang, likevel innebærer et tredelt-perspektiv at mange store temaer fortjener oppmerksomhet. På grunn av begrensninger i både innhold og tid har det vært utfordrende å gi grundig behandling av hvert funn og samtidig unngå mindre relevant informasjon. Ved å bruke en dokumentstudie var det imidlertid lettere å se hvilke funn som var mest relevante. Derfor mener jeg at de ulike temaene som ble undersøkt representerer interessante funn som kan være overførbare til andre organisasjoner og interessenter.

7.2. Forslag til videre forskning

Oppgaven har pekt mot mange funn som kan bli utforsket nærmere. Det er spesielt tenkelig at problemstillinger rundt samarbeid er relevant å studere videre. Funn om samarbeid har blitt tydeliggjort i både M- og O-faktorene. Det ville vært ønskelig å intervjue en leder fra hver av Fosen-kommunene for å få innsikt i hvordan de opplever funksjonen til det interkommunale samarbeidet. Masteroppgaven måtte derimot begrenses. Videre forskning kan rette søkelys på interkommunale samarbeid eller samskaping mellom privat og offentlig sektor. På denne måten kan en i større grad vurdere hvilken effekt slike samarbeid har for kommuner og hvordan de kan optimalisere arbeidet med digital sikkerhet.

Gjennom analyse og diskusjon av datamaterialet har ledelse blitt utpekt som essensielt i arbeidet med digital sikkerhet. Resultatene peker på betydningen av «digital ledelse», som innebærer evnen til å utnytte nye teknologier og løsninger, lære raskt og tilpasse seg endringer (Lips, 2020). Dette fenomenet kan dermed utforskes mer. På denne måten kan forskningen adressere flere ledelsesegenskaper som kommunale ledere kan rette seg etter. Forskningen har vist at MTO-perspektivet er omfattende, og selv om jeg kun har inkludert noen elementer er det tydelig at disse komponentene er sammenkoblet. Det kan derfor være hensiktsmessig å benytte en konfigurasjonsbasert tilnærming for å identifisere ulike konfigurasjoner av faktorer som dekker flere elementer innenfor MTO, enn det jeg har gjort. Det er tenkelig at flere forskere som arbeider sammen kan gjennomføre dette, da det krever tid og ressurser for å få en dypere forståelse av komplekse sammenhenger.

Det kan også være nyttig å vurdere digital sikkerhet på nasjonalt nivå. Selv om Riksrevisjonens rapport fra 2023 har bidratt med slike kartlegginger, kan det likevel være gunstig å undersøke hvordan statlige organer legger til rette for at offentlig sektor kan motstå trusler som hybrid krigføring. Det kan derfor være hensiktsmessig å forske videre på dette begrepet. Avslutningsvis kan det bemerkes at masteroppgaven peker i

retning mot at dagens samfunn opplever en overgang fra fred til mer urolige tider, preget av konflikter og cyber-angrep.

7.3. Anbefalinger

Med utgangspunkt i oppgavens empiriske analyse og fremlagt diskusjon kan en utpeke noen forslag til videre arbeid med digital sikkerhet. Det kan være gunstig om Midtre Gauldal kommune og Trondheim kommune iverksetter en beredskapsøvelse for digital sikkerhet, som inkluderer flere enheter av kommunen enn kun IT-avdelingen. Dette kan blant annet bidra med risikostyring og ansvarsfordeling. Kommunene kan la seg inspirere av Fosen IKT og Ørland kommune. Det er trolig at en omfattende øvelse kan løses i samarbeid med andre kommuner, i tillegg vurderes det som relevant om DigiTrøndelag bidrar med det strategiske arbeidet rundt en slik øvelse. Dette gjør at samordningen mellom ulike aktører inkluderer mer enn bare informasjonsformidling, noe som virker nødvendig for å hjelpe kommunene. Dersom problemstillinger løses sammen, er det trolig at kommunene stiller mer forberedt til øvelser.

Det anbefales at Fosen IKT arbeider mot å forbedre kommunikasjonen ut til de fire samarbeidskommunene. Derfor er det vurdert som positivt å ansette en informasjonssikkerhetsleder. Det interkommunale samarbeidet kan også ta inspirasjon fra Trondheim kommune og innføre et fagråd som samler nøkkelpersoner fra hver av de fire kommunene. Fosen IKT er ikke forpliktet til å organisere sikkerhetstiltak i dag. Funnene fra intervjuene tyder likevel på at teknologien trenger støtte gjennom styringssystemer. Det kan derfor være nyttig for det interkommunale samarbeidet å forankre arbeidet innen M- og O-faktorene, eller å presisere tydeligere krav til de fire Fosen-kommunene.

Det oppfordres til at alle benytter menneskelige feil som en mulighet for læring og integrerer et kontinuerlig arbeid med ulike sikkerhetstiltak. Det bør også etableres et felles språk blant kommunalt ansatte, hvor alle forstår kravene som er inkludert i sikkerhetsloven. For å oppnå dette, kan det være hensiktsmessig å utvikle styrende dokumenter. I tillegg bør ledere fremme en åpen og tillitsfull kultur. Det kan også være gunstig å iverksette flere ledelsessamlinger per år for å øke involvering fra toppledelsen og bevare internkontroll. I oppgavens innledning og analysekapittel ble det presisert at Stortinget har satt av midler til å lansere en nasjonal portal for digital sikkerhet (Riksrevisjonen, 2023). Med utgangspunkt i dette kan det være relevant å benytte tiltaket og vurdere om det er et fungerende middel for kommunene.

8. Referanseliste

Ahmeti, R., & Vladi, B. (2017). Risk Management in Public Sector: A Literature Review. *European Journal of Multidisciplinary Studies, 2*(5), 323-329.

Ahrne, G., & Brunossen, N. (2005). Organizations and meta-organizations. *Scandinavian Journal of Management, 21*(4), 429-449.

Almklov, P. G., Antonsen, S., Størkersen, K. V., & Roe, E. (2018). Safer societies. *Safety Science*, 110(C), 1-6.

Bergsjø, H., Windvik, R., & Øverlier, L. (2020). *Digital sikkerhet: en innføring.* Universitetsforlaget.

Bracci, E., Tallaki, M., Gobbo, G., & Papi, L. (2021). Risk management in the public sector: a structured literature review. *The International Journal of Public Sector Management, 34*(2), 205-223.

Buan, T. A. (2021). *Sluttrapport - Felles løft på informasjonssikkerhet og personvern.* DigiTrøndelag.

Bukve, O. (2021). *Forstå, forklare, forandre.* Universitetsforlaget.

Christoffersen, L., Johannessen, A., & Tufte, P. A. (2016). *Introduksjon til samfunnsvitenskapelig metode* (Utg. 5). Abstrakt.

Datatilsynet. (2018, 30. oktober). *Iverksette styringssystem for informasjonssikkerhet.* https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/iverksette-styringssystem-for-informasjonssikkerhet/

Datatilsynet. (2022, 11. januar). *Overtredelsesgebyr til Østre Toten kommune*. https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2022/overtredelsesgebyr-til-ostre-toten-kommune/

Departementene. (2019, 30. januar). *Nasjonal strategi for digital sikkerhet.* https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhet/id2627177/

Digdir. (2020). *Arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner.* Oslo: Digitaliseringsdirektortatet. https://www.digdir.no/media/1102/download

Digdir. (2022). *Rikets digitale tilstand*. https://www.digdir.no/rikets-digitale-tilstand/opplevde-sikkerhetsproblemer/3587

Digdir. (u.d.). *Kva seier NS-ISO/IEC 27001?* https://www.digdir.no/informasjonssikkerhet/kva-seier-ns-isoiec-27001/3060

Digdir. (u.d.). *Veileder for kartlegging av digital sikkerhetskultur.* Hentet mars 2023: https://www.digdir.no/informasjonssikkerhet/veileder-kartlegging-av-digital-sikkerhetskultur/2142#overordnede_sprsml_for_kartleggingen

DigiTrøndelag. (u.d.). *Nettsider til DigiTrøndelag*. Hentet april 2023: https://sites.google.com/trondheim.kommune.no/digitrondelag/start

eForvaltningsforskriften. (2004). *Forskrift om elektronisk kommunikasjon med og i forvaltningen* (FOR-2004-06-25-988). Lovdata. https://lovdata.no/dokument/SF/forskrift/2004-06-25-988?q=eForvaltningsforskriften

Engen, O.A., Kruke, B.I., Olsen, O.E., Lindøe, P.H., Olsen, K.H., & Gould, K.A. (2016). *Perspektiver på samfunnssikkerhet.* Oslo: Cappelen Damm Akademisk. (Kap. 1, 25-54).

Engen, O.A., Kruke, B.I., Olsen, O.E., Lindøe, P.H., Olsen, K.H., & Gould, K.A. (2021) *Perspektiver på samfunnssikkerhet* (Utg. 2.). Oslo: Cappelen Damm Akademisk. (Kap. 10&11).

Fosen IKT. (u.d.). *Om oss*. Hentet april 2023: https://www.fosenikt.no/home/?page_id=5

Grøtan, T. O. (2017). Følg regelen! I S. Antonsen, F. Heldal, & S. A. Kvalheim, *Sikkerhet og ledelse* (ss. 85-106). Oslo: Gyldendal Akademisk.

Grøtan, T. O., Antonsen, S., & Haavik, T. K. (2022). Cyber Resilience: A Pre-Understanding for an Abductive Research Agenda. I F. Matos, P. M. Selig, & E. Henriqson (Red.), *Resilience in a Digital Age: Global Challenges in Organisations and Society* (ss. 205-229). Springer International Publishing. https://doi.org/10.1007/978-3-030-85954-1_12

Hollnagel, E. (2009). The four cornerstones of resilience engineering. I C. P. Nemeth, E. Hollnagel, & S. Dekker, *Resilience engineering perspectives, Volume 2*, 118-133.

Hollnagel, E. (2022). Systemic Potentials for Resilient Performance. I F. Matos, P. M. Selig, & E. Henriqson (Red.), *Resilience in a Digital Age: Global Challenges in Organisations and Society (ss.7-19).* Springer International Publishing.

Hollnagel, E., Leonhardt, J., Licu, T., & Shorrock, S. (2015). From Safety-I to Safety-II: A White Paper. *Eurocontrol*.

IRGC. (2015). *CYBER SECURITY RISK GOVERNANCE* (Workshop report). https://irgc.org/wp-content/uploads/2018/09/Cyber-Security-Risk-Governance-29-30-October-2015-Workshop-Report.pdf

ISO. (u.d.). *ISO/IEC 27001 and related standards Information security management*. Hentet januar 2023: https://www.iso.org/isoiec-27001-information-security.html

Johannessen, L.E.F., Rafoss, T.W., & Rasmussen, E.B. (2020). *Hvordan bruke teori? Nyttige verktøy i kvalitativ analyse.* Oslo: Universitetsforlaget.

Johannesson, P., & Perjons, E. (2014). *An Introduction to Design Science.* Sverie, Stockholm: Springer.

Justis- og beredskapsdepartementet & Kommunal- og distriksdepartementet. (2022, 7. februar). *Digitale angrep mot norske kommuner kan få store konsekvenser*. https://www.regjeringen.no/no/aktuelt/-digitale-angrep-mot-norske-kommuner-kan-fa-store-konsekvenser/id2900215/

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers and Security*, *106*, Article 102267. https://doi.org/10.1016/j.cose.2021.102267

Knopf, J. (2006). Doing a Litterature Review. *PS: Political Science & Politics, 39*(1), 127-132.

Knutsen, P. (2018). Gjensyn med spørsmålet om metode: En kritisk vurdering av hypotetisk-deduktiv metode (HDM) sammenlignet med induksjonsdrevne problemstillinger (IdP). *Norsk filosofisk tidsskrift, 53*(4), 198-208. https://www.idunn.no/doi/10.18261/issn.1504-2901-2018-04-03

Kommunal- og moderniseringsdepartementet. (2019, 11. juni). *Én digital offentlig sektor*. https://www.regjeringen.no/no/dokumenter/en-digital-offentlig-sektor/id2653874/?q=sikkerhet&ch=10

Kommuneloven. (2021). *Lov om kommuner og fylkes kommuner* (LOV-2021-04-23-24). Lovdata. https://lovdata.no/dokument/NL/lov/2018-06-22-83/KAPITTEL_2-1#KAPITTEL_2-1

Kongsvik, T. (2013). *Sikkerhet i organisasjoner*. Fagbokforlaget.

Kongsvik, T., Albrechtsen, E., Antonsen, S., Herrera, I. A., Hovden, J., & Schiefloe, P. M. (2018a). Mennesket som feilkilde og ressurs. I *Sikkerhet i arbeidslivet* (ss. 191-204). Fagbokforlaget.

Kongsvik, T., Albrechtsen, E., Antonsen, S., Herrera, I. A., Hovden, J., & Schiefloe, P. M. (2018). Regelstrying, etterlevelse og tilpasning. I *Sikkerhet i arbeidslivet* (ss. 205-218). Fagbokforlaget.

KS. (2022, 9. mars). *Råder kommunene til å se på it-sikkerhetstiltak*. https://www.ks.no/fagomrader/digitalisering/kompetanse-og-verktoy/informasjonssikkerhet-og-personvern/rader-kommunene-til-a-se-pa-it-sikkerhetstiltak/

Kringlebotten, M., & Langørgen, A. (2020). *Gruppering av kommuner etter folkemengde og økonomiske rammebetingelser 2020.* Oslo-Kongsvinger: Statistisk sentralbyrå.

Lips, M. (2020). *Digital Government.* Routledge.

Loonam, J., Zwiegelaar, J., Kumar, V., & Booth, C. (2022), Cyber-Resiliency for Digital Enterprises: A Strategic Leadership Perspective. *IEEE Transactions on Engineering Management, 69*(6), 3757-3770. https://www.scopus.com/record/display.uri?eid=2-s2.0-

85128078945&doi=10.1109%2fTEM.2020.2996175&origin=inward&txGid=3e83b341a6661e8a6e0ce94e3871c509

Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation: Results from expert interviews. *Goverment Information Quarterly*, *36*(4), 1-16. https://www.sciencedirect.com/science/article/pii/S0740624X18304131

Midré, G. (2009). Grounded Theory: Klassikerne, revisjonistene og den vitenskapsteoretiske diskusjonen i samfunnsfagene. *Sosiologisk tidsskrift, 17*, 240-269.

Milakovich, M. E. (2022). *Digital governance: applying advanced technologies to improve public service* (Utg.2). Routledge.

NOU 2018:14 (2018). *IKT-sikkerhet i alle ledd: Organisering og regulering av nasjonal IKT-sikkerhet*. Departementenes sikkerhets- og serviceorganisasjon. https://www.regjeringen.no/contentassets/0d408600df2f4738a9bbb85040b02b59/no/pdfs/nou201820180014000dddpdfs.pdf

NRK. (2021, 17. desember). Hacket kommune får 16 millioner kroner i statsstøtte. *NRK.* https://www.nrk.no/innlandet/ostre-toten-kommune-far-16-millioner-kroner-i-statsstotte-etter-dataangrep-1.15776277

NRK. (2021, 30. desember). Mats og 8.000 elever står uten datatilgang rett før skolestart. *NRK.* https://www.nrk.no/nordland/dataangrep-rammer-nordland-fylkeskommune-1.15789412

NSM. (2020, 15. april). *Grunnprinsipper for IKT-sikkerhet 2.0.* https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/hva-er-nsms-grunnprinsipper-for-ikt-sikkerhet/

NSM. (2021). *Veileder i sikkerhetstyring.* https://nsm.no/getfile.php/132933-1591350417/NSM/Filer/Dokumenter/Veiledere/veileder-i-sikkerhetsstyring.pdf

NSM. (2022a). *Nasjonalt digitalt risikobilde 2022.* Nasjonal sikkerhetsmyndighet & Nasjonalt cybersikkerhetssenter. https://nsm.no/getfile.php/1311995-1664550278/NSM/Filer/Dokumenter/Rapporter/NDIG%202022.pdf

NSM. (2022). *Risiko 2022.* https://nsm.no/getfile.php/137798-1644424185/NSM/Filer/Dokumenter/Rapporter/NSM_rapport_final_online_enekelt sider.pdf

OECD (2015), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document,* OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264245471-en

OECD. (2022). *OECD Policy Framework on Digital Security*. OECD Publishing, Paris. https://read.oecd-ilibrary.org/science-and-technology/oecd-policy-framework-on-digital-security_a69df866-en#page1

OECD, (2022a). *Recommendation of the Council on Digital Security Risk Management*, OECD/LEGAL/0479. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0479

OECD. (u.d.). *Digital security*. https://www.oecd.org/digital/digital-security/

Osmundsen, K., Iden, J., & Bygstad, B. (2018). Hva er digitalisering, digital innovasjon og digital transformasjon? En litteraturstudie. *NOKOBIT*, *26*(1). https://ojs.bibsys.no/index.php/Nokobit/article/view/532

Potrich, L. N., Selig, P. M., Matos, F., & Giugliani, E. (2022). Organisational Resilience in the Digital Age: Management Strategies and Practices. I F. Matos, P. M. Selig, & E. Henriqson (Red.), *Resilience in a Digital Age* (ss. 59-70). Springer International Publishing.

Prop. 78 S (2021-2022). *Endringer i statsbudsjettet 2022 (økonomiske tiltak som følge av krigen i Ukraina).* Det kongelige finansdepartementet. https://www.regjeringen.no/contentassets/8ec464ed072f4f459a3b0ad75e4637cd/no/pdfs/prp202120220078000dddpdfs.pdf

Rasmussen, J. (1997). RISK MANAGEMENT IN A DYNAMIC SOCIETY: A MODELLING PROBLEM. *Safety Science, 27*(2/3), 182-213.

Regjeringen. (2010, 1. juni). *Cybersikkerhet.* https://www.regjeringen.no/contentassets/252f869fdfac46648e41e6ca5fb0600a/cybersikkerhet_svar-med-merknader_nsm-pst-etterretningstjenesten.pdf

Regjeringen. (2022, 9. desember). *Regjeringen vil styrke nasjonal kontroll i ny stortingsmelding*. https://www.regjeringen.no/no/aktuelt/regjeringen-vil-styrke-nasjonal-kontroll-i-ny-stortingsmelding/id2950574/

Rijpma. J. A. (1997). Complexity, Thight-Coupling and Reliability: Connection Normal Accidents Theory and High Reliability Theory. *Journal of Contingencies and Crisis Management, 5*(1), 15-23.

Riksrevisjonen. (2023, 2. februar). *Myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor.* https://www.riksrevisjonen.no/globalassets/rapporter/NO-2022-2023/myndighetenes-samordning-av-arbeidet-med-digital-sikkerhet-i-sivil-sektor.pdf

Rommetvedt, H. (2023). Et lite bidrag til differensiering og presisering av det hegemoniske og tvetydige begrepet «samskaping». *Tidsskrift for velferdsforskning, 26*(1), 1-3. https://www.idunn.no/doi/10.18261/tfv.26.1.5?fbclid=IwAR2xFSgtXXBl6AXzsLHo2t3K8QtX9Mw3vrNhKQXO14rR87yeV2BGVO6SdA

Schiefloe, P. M. (2017). Pentagonanalyse: En helhetlig modell for sikkerhet i organisasjoner. I S. Antonsen , F. Heldal, & S. A. Kvalheim, *Sikkerhet og ledelse* (ss. 281-301). Oslo: Gyldendal Akademisk.

Seawright, J., & Gerring, J. (2008). Case Selection Techniques in Case Study Research. *Political Research Quarterly, 61*(2), 294-308. https://journals.sagepub.com/doi/pdf/10.1177/1065912907313077

Sikkerhetsloven. (2019). *Lov om nasjonal sikkerhet* (LOV-2018-06-01-24). Lovdata. https://lovdata.no/dokument/NL/lov/2018-06-01-24?q=sikkerhetsloven

Sopra Steria. (2021). *Informasjonssikkerhet og personvern i Trondheim kommune.* Sopra Steria.

SSB. (2022). *Digitalisering og IKT i offentlig sektor*. Hentet fra Statistisk sentralbyrå: https://www.ssb.no/statbank/table/12617/tableViewLayout1/

SSB. (u.d.). *Kommune: Midtre Gauldal (Trøndelag)*. Hentet fra Statistisk sentralbyrå: https://www.ssb.no/kommunefakta/midtre-gauldal

SSB. (u.d.). *Kommunefakta*. Hentet fra Statistisk sentralbyrå: https://www.ssb.no/kommunefakta

Steine, J.-E., Føleide, A., Wormdal, B., Sætra, G., Jakobsen , R., Larsen, H., & Bøthun, S. H. (2023, 10. februar). Etterforsker omfattende dataangrep: – Vi blir daglig utsatt for forsøk på hacking. *NRK*. https://www.nrk.no/tromsogfinnmark/etterforsker-omfattende-dataangrep_-har-bedt-om-bistand-fra-kripos-1.16292555

Thiel, S. V. (2022). *Research Methods in Public Administration and Public Management.* New York: Routledge.

Timmermans, S., & Tavory, I. (2012). Theory Construction in Qualitative Research: From Grounded Theory to Abductive Analysis. *Sociological Theory, 30*(3), 167 –186.

Tjora, A. (2018). *Kvalitative forskningsmetoder i praksis* (utg. 3.). Oslo: Gyldendal.

Trondheim Kommune. (2023, 21. april). *Befolkningsstatistikk*. https://www.trondheim.kommune.no/aktuelt/om-kommunen/statistikk/befolkningsstatistikk/

Vassenden, A. (2018). Produktive anomalier: Teoriutvikling i empirisk sosiologi. *Norsk sosiologisk tidsskrift, 2*(2), 145–163.

Vila-Henninger, L., Dupuy, C., Ingelgom, V. V., Caprioli, M., Teuber, F., Pennetreau, D., Bussi, M., Gall, C. L. (2021). Abductive Coding: Theory Building and Qualitative (Re)Analysis. *Sociological Methods & Research.* *https://journals.sagepub.com/doi/10.1177/00491241211067508*

Virksomhetsikkerhetsforskriften. (2019). *Forskrift om virksomheters arbeid med forebyggende sikkerhet* (FOR-2019-05-03-560). Lovdata. https://lovdata.no/dokument/SF/forskrift/2018-12-20-2053#KAPITTEL_2

Wilson, C., & Mergel, I. (2022). Overcoming barriers to digital government: mapping the strategies of digital champions. *Government Information Quarterly*, *39*(2), 1-11. https://www.sciencedirect.com/science/article/pii/S0740624X22000144

Xu, J., & Lu, W. (2022). Developing a human-organization-technology fit model for information technology adoption in organizations. *Technology in Society, 70*(102010).

Yin, R. K. (2018). *Case Study Reasearch and Applications Design and Methods.* SAGE Publication Inc.

9. Vedlegg

Oversikt over vedlegg:

Vedlegg A: Godkjenning av NSD

Vedlegg B: Tabell 1: oppsummering av tidligere forskning

Vedlegg C: Tabell 5: Oppsummering av tiltak eller planlagte tiltak som et resultat av dagens risikobilde

Vedlegg D1: Intervjuguide til informanter i kommuner/kommunesamarbeid

Vedlegg D2: Intervjuguide til informanter i KS

Vedlegg E: Informasjonsskriv til informanter

Vedlegg F: Kort oppsummering av sentralt lovverk

Vedlegg A

Sikt

Meldeskjema / Risikohåndtering og digital sikkerhet i offentlig sektor / Vurdering

Vurdering av behandling av personopplysninger

Referansenummer	Vurderingstype	Dato
527570	Automatisk	17.01.2023

Prosjekttittel
Risikohåndtering og digital sikkerhet i offentlig sektor

Behandlingsansvarlig institusjon
Norges teknisk-naturvitenskapelige universitet / Fakultet for samfunns- og utdanningsvitenskap (SU) / Institutt for sosiologi og statsvitenskap

Prosjektansvarlig
Barbara Zyzak

Student
Marie Berntsen

Prosjektperiode
10.01.2023 - 06.06.2023

Kategorier personopplysninger
Alminnelige

Lovlig grunnlag
Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)

Behandlingen av personopplysningene er lovlig så fremt den gjennomføres som oppgitt i meldeskjemaet. Det lovlige grunnlaget gjelder til 06.06.2023.

Meldeskjema

Grunnlag for automatisk vurdering
Meldeskjemaet har fått en automatisk vurdering. Det vil si at vurderingen er foretatt maskinelt, basert på informasjonen som er fylt inn i meldeskjemaet. Kun behandling av personopplysninger med lav personvernulempe og risiko får automatisk vurdering. Sentrale kriterier er:

- De registrerte er over 15 år
- Behandlingen omfatter ikke særlige kategorier personopplysninger;
  - Rasemessig eller etnisk opprinnelse
  - Politisk, religiøs eller filosofisk overbevisning
  - Fagforeningsmedlemskap
  - Genetiske data
  - Biometriske data for å entydig identifisere et individ
  - Helseopplysninger
  - Seksuelle forhold eller seksuell orientering
- Behandlingen omfatter ikke opplysninger om straffedommer og lovovertredelser
- Personopplysningene skal ikke behandles utenfor EU/EØS-området, og ingen som befinner seg utenfor EU/EØS skal ha tilgang til personopplysningene
- De registrerte mottar informasjon på forhånd om behandlingen av personopplysningene.

Vedlegg B

Teoretiske kilder	Tittel	Innhold
Rasmussen (1997)	Risk management in a dynamic society: a modelling problem	Hvordan kan vi unngå alvorlige ulykker i et dynamisk samfunn? Sosiotekniske systemer er involvert i risikohåndtering, men blir presset av en rask teknologisk utvikling. Det trengs tverrfaglighet i arbeidet med risiko, samt fokus på de ulike nivåene i komplekse systemer. Tar for seg arbeidssystemer, grenser på akseptabel risiko og tilpasningsevne.
Rijpma (1997)	Complexity, Thight-Coupling and Reliability: Connection Normal Accidents Theory and High Reliability Theory.	En artikkel om en teoretisk debatt mellom to dominante retninger om utviklingen av ulykker og reliabilitet. Normal Accident Theory mener at ulykker er unngåelig i komplekse og tett koblede systemer. Derimot mener High Reliability Theory at organisasjoner kan finne gode løsninger for å motvirke uønskede hendelser, som bruken av redundans.
Kongsvik (2013)	*Sikkerhet i organisasjoner*	Boken gir en oversikt over diverse sikkerhetsteorier. Blant annet er MTO-perspektivet sentralt og tar for seg når de ulike kategoriene (mennesker, teknologi, organisering) fikk oppmerksomhet i forskningsmiljøene. En må vurdere samspillet mellom kategoriene for å bruke MTO på rett måte.
Hollnagel, Leonhardt, Licu & Shorrock (2015)	From Safety-I to Safety-II: A White Paper	Forfatterne skriver om resiliens i et Safety II perspektiv. De mener det er viktig å ikke kun se på det som gikk galt, men også det som gikk bra. Ting går riktig fordi mennesker klarer å justere sine arbeidsprosesser og tilpasse seg etter omgivelsene. Et Safety I perspektiv er ikke lenger tilstrekkelig med en verden i endring. Mennesker blir sett på som en ressurs.
Almklov, Antonsen, Størkersen & Roe (2018)	Safer societies	Arbeid med informasjonssikkerhet krever samarbeid mellom fagfolk. IKT og endringer i verden skaper et skifte i feltet «safety science». Det påvirker hvordan offentlig sektor er organisert og forfatterne peker på nødvendigheten av å arbeide forbi allerede etablerte siloer. Sikkerhet krever mer samordning og samskaping i offentlig sektor
Schiefloe (2017)	Pentagonanalyse: En helhetlig modell for sikkerhet i organisasjoner. Kap. 13 i S*ikkerhet og ledelse*	Skiller mellom ulike epoker der teknologiske, menneskelige og organisatoriske faktorer har fått størst fokus. Når ulykker inntreffer, skjer det oftest i et samspill mellom ulike faktorer. Forklarer MTO-perspektivet og benytter det for å analysere petroleumsindustrien. Tar for seg ulike elementer som er viktig innenfor MTO som teknologisk svikt, menneskelige feil og sikkerhetsstyring.
Kongsvik, Albrechtsen, Antonsen, Herrera, Hovden & Schiefloe (2018)	Mennesket som feilkilde og ressurs. Kap. 13 i *Sikkerhet i arbeidslivet*	Kjennetegn av «human factors» tradisjonen innen sikkerhetsfeltet. Det kreves et samspill mellom mennesker og teknologi. Forfatterne utforsker litteratur som omhandler menneskelige feil. De påpeker at det ofte er andre årsaker bak menneskelige feilhandlinger og at mennesker kan forhindre ulykker og styrke sikkerheten. Bør ha samskaping mellom privat sektor, offentlig sektor og innbyggere.

Grøtan (2017)	Følg regelen! Kap. 4 i *Sikkerhet og ledelse*	Resiliens får økt popularitet innen sikkerhetsforskning. Det er likevel nødvendig med en balanse mellom etterlevelse (følge regler) og tilpasningsevne (resiliens). I tillegg har ledelsen et viktig ansvar og må velge å forberede organisasjonen på noe ubehagelig og uventet. Ledelsen må skape god sikkerhet gjennom samspill med de ansatte.
Ahmeti & Vladi (2017)	Risk Management in Public Sector: A Literature Review	Forskning om risikohåndtering tar oftest for seg finans- og banksektoren. Det er dermed viktig å rette fokus mot offentlig sektor, som møter på komplekse og utfordrende hendelser i dag. Litteraturen har tidligere fokusert mest på risikoestimering og ikke hvordan disse kan bli introdusert til beslutningsprosesser i offentlig sektor.
Grøtan, Antonsen & Haavik (2022)	Cyber Resilience: A Pre-Understanding for an Abductive Research Agenda. Kap. 12 i *Resilience in a Digital Age*	Digital transformasjon gjør at kritisk infrastruktur blir et cyber-fysisk system. Overraskelser og sjokk blir et hyppig fenomen og konsepter om resiliens blir brukt i økende grad i diskurs om sårbarheter. Forfatterne diskuterer et teoretisk konsept om cyber-resiliens
Hollnagel (2022)	Systemic Potentials for Resilient Performance. Kap. 2 i *Resilience in a Digital Age*	Et system kan ikke være resilient, men det kan utvikle resiliens. Det er en pågående tilstand hvor problemer blir kontrollert grunnet kompenserende endringer. Dette er viktig for miljøer som er preget av uforventede forandringer. Forfatteren benytter fire potensialer for å yte på en resilient måte.
Loonam, Zwiegelaar, Kumar, Booth (2022)	Cyber-Resiliency for Digital Enterprises: A Strategic Leadership Perspective	Organisasjoner ser i økende grad på informasjon som deres viktigste ressurs, dermed blir informasjonssikkerhet en integrert del av organisasjonens design og prosesser. Likevel er risiko, spesielt i form av cyber angrep forekommende. Effektiv ledelse er en kritisk faktor for informasjonssikkerhet. Det mangler empirisk forskning på hvordan rollen til ledere former cyber-sikkerhetsstrategier. Forfatterne prøver å fylle dette hullet i litteraturen.
Bergsjø, Windvik & Øverlier (2020)	Digital sikkerhet: en innføring	Arbeidslivet og privatlivet har blitt avhengig av IKT-systemer og internett, dermed er det behov for kompetanse om digital sikkerhet. Norske fagfolk har dermed samarbeidet om å skrive denne innføringsboken for å gi studenter en forståelse i sentrale temaer som sikkerhetskultur, personvern, lover, risiko, sårbarhet, trusler og mye mer.
Empirinære kilder	**Tittel**	**Innhold**
International risk governance council (irgc) (2015)	Cyber Security Risk Governance	Organisasjoner er i økende grad bekymret over trusler til dataens konfidensialitet, integritet og tilgjengelighet. Trussel-aktører trenger kun å lykkes en gang, mens forsvareren må gjøre den umulige oppgaven av å være perfekt hver gang. For å sikre et komplekst system må en benytte nye strategier, dermed benytte cyber-resiliens. Digital sikkerhet må bli en integrert del av en organisasjons kjerne.
OECD (2015)	Digital Security Risk Management for Economic and Social Prosperity	OECD gir i dette heftet anbefalinger for hvordan nasjonale strategier for styring av digital sikkerhetsrisiko kan fungere. Økende digitale trusler og angrep har medbragt sosiale og økonomiske konsekvenser for offentlige og

		private organisasjoner. Dette kan gå på bekostning av tillit, og at en organisasjon kan få alvorlige skader på eget rykte. Ledelsesstrategier blir utpekt som det viktigste i arbeidet med digital sikkerhet.
Kommunal- og moderniseringsdepartementet (2019)	Én digital offentlig sektor	Regjeringens digitaliseringsstrategi som skal gi en enklere hverdag til innbyggere, næringsliv og frivillig sektor gjennom bedre offentlige tjenester. Digital sikkerhet har sterk tilhørighet med digital transformasjon og digitaliseringsstrategien
Digitaliseringsdirektoratet (Digdir) (2020)	Arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner	Undersøkelse av Digdir i samarbeid med KS. Kunnskapsgrunnlaget tar utgangspunkt i ulike dokumenter om kommuner og fylkeskommuner. De finner svakheter i styring og kontroll av informasjonssikkerhet. Det gjelder spesielt små og mellomstore kommuner. Det er få beredskapsøvinger, manglende kompetanse og forståelse hos både medarbeidere og ledere.
Buan (2021)	Sluttrapport - Felles løft på informasjonssikkerhet og personvern. DigiTrøndelag (unntatt offentligheten)	En undersøkelse i regi av DigiTrøndelag. Spørreundersøkelsen baserer seg på kommuner i Trøndelag. Målet er å løfte informasjonssikkerheten i kommunene og se hvor DigiTrøndelag kan bidra. Kommuner har utfordringer med ressurser, rollefordelinger, opplæring, personvernregelverk og risikohåndtering.
Sopra Steria (2021)	Informasjonssikkerhet og personvern i Trondheim kommune (unntatt offentligheten)	Arbeid med informasjonssikkerhet krever en helhetlig tilnærming (mennesker, teknologi og organisering). Arbeidet er preget av et teknologi-drevet fokus. Kommunen har ikke kapasitet til å håndtere sikkerhetssituasjonen. Risikoreduserende tiltak er mangelfullt, og forvaltningsoppgaver/rutiner er ikke prioritert.
OECD (2022)	Recommendation of the Council on Digital Security Risk Management	Et oppdatert skriv om anbefalinger. Anerkjenner at en ikke kan redusere all risiko og at digital sikkerhet ikke bare er et teknisk problem, men en institusjonell og sosial utfordring. Digital sikkerhet bør dermed være en høyere prioritet blant ledere og beslutningstagere.
Riksrevisjonen (2023)	Myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor	Rapport fra Riksrevisjonen til Stortinget. Det blir gitt kritikk til justis- og beredskapsdepartementet for manglende oppfølging av *Nasjonal strategi for digital sikkerhet.* Det er spesielt svak samordning av roller, ansvar og krav som gjør arbeidet med digital sikkerhet utfordrende.

Tabell 1. Oppsummering av tidligere forskning

Vedlegg C

Nr.	Tema (MTO)	Bakgrunn og begrunnelse for tiltak	Kommune/IKS
1	Kunnskap/kompetanse opplæring og bevisstgjøring (M)	Kampanje i sikkerhetsmåneden oktober: Kjørt tester i form av e-post, med hensikt å se hvor mange som trykker på en lenke, noe som indikerer at en har blitt lurt.	**Trondheim kommune**
2	Rekruttering (M)	Ansetter nytt personvernombud som kan drive opplæring ut i organisasjonen og en jurist med spesiell kompetanse på informasjonssikkerhet. I tillegg til to nye på informasjonssikkerhet for IT-avdelingen	Trondheim kommune
3	Øvelser og teknologisk løft (T)	Kjørt øvelse på utbrudd av krypto virus (2022) og strammet inn teknisk nivå etter krigens utbrudd (blant annet gjennom å flytte utsatte tjenester over i 'Public Cloud')	Trondheim kommune
4	Internkontroll og oversikt (O)	Gjennomført to revisjoner med bruk av ekstern leverandør. Blant annet Sopra Steria rapport (2021). Hensikt om å få et utenfra blikk på organisasjonen og peke ut sentrale sårbarheter.	Trondheim kommune
5	Forankring av roller og tilgangsstyring (O)	Klarert nøkkelpersoner og ledere, med hensikt om å skape oversikt over hvem som har tilgang til konfidensiell og hemmelig informasjon	Trondheim kommune
6	Organisering av arbeidet, roller og ansvar(O)	Ny enhet: sikkerhet og beredskap (opprettet april 2022). Har overordnet ansvar for sikkerhet. Forsøker i disse tider å vurdere hvilken rolle de skal ha, særlig med hensyn til den sikkerhetspolitiske situasjonen utløst av invasjonen i Ukraina.	Trondheim Kommune
1	Kunnskap/kompetanse opplæring og bevisstgjøring (M)	Informasjonskampanje med e-post tester, til slutt sendes ut en lenke, med hensikt om å se hvem som blir lurt.	**Midtre Gauldal kommune**
2	Kunnskap/kompetanse opplæring og bevisstgjøring (M)	Planlegger kurs innen digital sikkerhet for ledere og et kurs for nyansatte (ikke innført da intervjuet ble gjort).	Midtre Gauldal kommune
3	Nytt teknologisk verktøy (T)	Ny overvåkningstjeneste hvor en ekstern aktør fører logger og har en programvare som slår alarm hvis det blir datainnbrudd	Midtre Gauldal kommune
4	Tilgangsstyring/to-faktor (T)	Mer bruk av tofaktorautentisering som et resultat av pandemien og hendelsen i Østre Toten, med hensikt om å skape sikker sone ved bruk av hjemmekontor.	Midtre Gauldal kommune
5	Risikovurderinger (O)	Innført noen prosedyrer (ble ikke spesifisert hvilke) som skal skje før nye anskaffelser. Det innebærer risiko- og sårbarhetsanalyser.	Midtre Gauldal kommune
6	Forankring av ledelse (O)	Innført årlig oppsummering av sikkerhetsarbeidet (hensikt om å vurdere status og prioriteringer for neste års budsjett) og fordelt formelle roller, som en sikkerhetsansvarlig.	Midtre Gauldal kommune
1	Kunnskap/kompetanse opplæring og bevisstgjøring (M)	Fosen IKT ansatte sendes på kurs som hovedsakelig faller innenfor kategorien tekniske ferdigheter (Microsoft kurs).	**Fosen IKT**
2	Kunnskap/kompetanse opplæring og bevisstgjøring (M)	I forkant av ny kriseøvelse skal det bli sendt ut falske *phishing* mailer, med hensikt om å se hvor mange som lar seg lure. De har også kjørt ut noen videoer med hensikt om å bevisstgjøre rundt sikkerhet	Fosen IKT
3	Teknologisk løft (T)	Gjennomgang av fagsystemer (2022) med hensikt om å finne viktige verdier og sikre disse. Også benyttet mer bruk av tofaktorautentisering.	Fosen IKT
4	Beredskapsøvelse (O)	Skal gjennomføre beredskapsøvelse for informasjonssikkerhet i Ørland kommune i mai (uvisst om dette har blitt gjennomført).	Fosen IKT
5	Forankring av ledelse (O)	Planlegger å innsette en informasjonssikkerhetsleder med hensikt om å samle en ressurs for de fire kommunene (uvisst om dette har blitt gjennomført).	Fosen IKT

Tabell 5: Oppsummering av tiltak eller planlagte tiltak som et resultat av dagens risikobilde

Vedlegg D1

Intervjuguide til informanter i kommuner/kommunesamarbeid

Oppvarmingsspørsmål
- Hvor lenge har du jobbet i stillingen du har?
- Hva slags ansvarsområde har du i din organisasjon?
- Hva betyr digital sikkerhet for deg?

Organisering
- Nå skal jeg stille spørsmål som gjelder selve organiseringen rundt digital sikkerhet og risikohåndtering

Spørsmål om organisering
1. På hvilken måte har kommunen/kommunene organisert sitt sikkerhetsarbeid
    - Oppfølgingsspørsmål: hvilke metoder benytter dere i risiko og i digital sikkerhets arbeidet?
    - Har kommunen beredskapsøvinger for informasjonssikkerhet, i så fall hvorfor/hvorfor ikke?
2. Hvordan opplever dere at sikkerhetsarbeidet fungerer
    - *Hva er utfordrende når en skal vurdere og fastsette grenser for risiko?*
    - Oppfølgings: Har dere en handlingsplan/konkrete tiltak dere følger?
3. Hvilke roller er det som har ansvaret for digital sikkerhet i organisasjonen og er dette klart for de ansatte?
    - Oppfølgings: Hvem skal informeres om informasjonssikkerhetsbrudd og ta ansvar for å håndtere situasjonen?
4. Hvordan jobbes det i grensesnittet mot informasjonssikkerhet og andre former for sikkerhet og kommunal beredskap?

Spørsmål om omgivelsene:
5. Hvordan påvirker omgivelsene kommunens sikkerhetsarbeid? Her tenker jeg på siste kriser som for eks. pandemien og krigen i Europa
6. Hvordan koordineres arbeidet dersom det skulle oppstå en krisesituasjon?
    - Oppfølgingsspørsmål: Har dere erfaring med det? Hvordan er det gjort tidligere?
    - Hvilke trussel-aktører kan dere forberede dere på, hvilke typer angrep har dere erfart?
7. Hva anser du/dere som deres muligheter og utfordringer rundt digital sikkerhet og risikohåndtering sammenlignet med en større kommune som Trondheim kommune/andre kommuner?

Spørsmål om samarbeid
8. Har dere samarbeid med andre kommuner angående digital sikkerhet/informasjonssikkerhet og/eller risikohåndtering,
    - Oppfølgingsspørsmål: hvem samarbeider dere med og hvordan fungerer dette samarbeidet i praksis?

Spørsmål om ledelse
9. Er ledere forberedt på uforutsette hendelser og har ledere kompetanse/kunnskap om risikostyring?

    - Oppfølgingsspørsmål: Hvilke tiltak arbeider lederne med? Hva slags ressurser/kompetanse trenger dere? *Hva slags tidligere erfaring har dere med uforutsette hendelser?*
      Oppfølgingsspørsmål: Har dere en oversikt over mulige uønskede hendelser gradert etter risiko?
10. Hvordan tilpasser lederne seg til nye råd og retningslinjer fra KS eller andre organisasjoner da det ble alarmert om at trusselnivået i dag krever bedre digital sikkerhet?

Mennesker:

- Nå skal jeg stille spørsmål som faller innenfor kategorien mennesker

11. Hvordan bygger kommunen opp kompetansen til de ansatte når det gjelder digital sikkerhet og risiko?
    - Oppfølging: Har kommunen/(e) opplæringsprogrammer?
    - Er menneskelig feil noe som oppstår og diskuteres i kommunen?
12. Har kommunen en stilling som informasjonssikkerhetsrådgiver og/eller personvernombud? Hvis ikke, hva slags utfordringer skaper dette?
13. Hvilke kompetanse må dere søke om eksternt og hvorfor?
14. Ifølge din oppfatning, hvordan forholder de ansatte seg til digitale trusler som kan ramme kommunen?
    - Har du sett en endring?

Teknologi:

- Nå skal jeg stille spørsmål som faller innenfor kategorien teknologi

15. Hvordan sikres konfidensialitet, integritet og tilgjengelighet gjennom teknologi?
    - Hva slags utfordringer har dere med dette?
16. Hvilke løsninger og type teknologier benytter dere for å ivareta informasjonssikkerhet og personvern? (f.eks. overvåkningsteknologier, penetrasjonstester og reservesystemer)
    - Forholder dere dere til noen definerte sikkerhetskrav/prosedyrer, i så fall hvilke?
17. Hva har dere lært fra tidligere hendelser knyttet til cyber-angrep i kommunen eller fra andre kommuner som har opplevd cyber-angrep?
    - Oppfølgingsspørsmål: Hvilke utfordringer kan melde seg ved oppdagelse av nye sårbarheter?

Vedlegg D2

Intervjuguide til informanter i KS

Innledning

- Hvor lenge har du jobbet i stillingen du har?
- Hva slags ansvarsområde har du i din organisasjon?
- Hva betyr digital sikkerhet for deg?

Organisering

- Nå skal jeg stille spørsmål som gjelder selve organiseringen rundt digital sikkerhet og risikohåndtering

1. Hva skal KS gjøre for at kommuner kan bedre oppdage, forebygge og håndtere digitale angrep?
2. På hvilken måte mener dere at kommunene bør organisere sitt sikkerhetsarbeid?
    - Hvilke metoder eller prinsipper skal de benytte når det eksisterer mange ulike modeller og retningslinjer?
    - Har dere noe oversikt over det digitale sikkerhetsarbeidet i kommunene?
3. Hvordan opplever dere at sikkerhetsarbeidet fungerer i kommunene
    - Hva er utfordrende når en skal vurdere og fastsette grenser for risiko?
4. Hvordan kan kommunene tydeliggjøre roller og ansvar i sikkerhetsarbeidet?
    - Oppfølgings: Hvem skal informeres om informasjonssikkerhetsbrudd og ta ansvar for å håndtere situasjonen?

Spørsmål om omgivelsene:

5. Hvordan påvirker omgivelsene KS sitt arbeid med å bistå kommunene med digital sikkerhet? Her tenker jeg på siste kriser som for eks. pandemien og krigen i Europa.
    - Oppfølgingsspørsmål: Har dere sett en endring blant kommunene i Norge?
6. Hvilke typer trussel-aktører bør kommunene være forberedt på?
    - Hvilke angrep har dere erfart at kommunene trenger hjelp med?
    - Hvordan bruker dere trusselvurderinger og erfaringer fra hendelser fra andre aktører? (f.eks. sykehusene i Norge som ble truet av russiske hackere nå nylig, eller hendelsen i Østre Toten)

Spørsmål om samarbeid

7. Hvordan kan interkommunale samarbeid eventuelt bedre den digitale sikkerheten?

Spørsmål om ledelse

8. Har dere noen tilbud/kurs/opplæring for kommunale ledere, f.eks. kurs om risikostyring eller lignende?
9. Er ledere i kommuner forberedt på uforutsette hendelser og har ledere tilstrekkelig kompetanse/kunnskap om risikostyring?
    - Oppfølgingsspørsmål: Hva slags ressurser/kompetanse behøves?
10. Opplever dere at lederne tilpasser seg nye råd og retningslinjer fra KS (f.eks. NPISK tiltakene)?
    - Oppfølgingsspørsmål: Hvordan skal NPISK hjelpe kommunene?

Mennesker:

- Nå skal jeg stille spørsmål som faller innenfor kategorien mennesker

11. Hvordan bør en kommune bygge opp kompetansen til de ansatte når det gjelder digital sikkerhet og risiko?
    - Oppfølging: Hvem har ansvar for opplæring av kommunale ansatte?
12. Dersom en kommune ikke har en informasjonssikkerhetsrådgiver og/eller et personvernombud, hva slags utfordringer skaper dette?
13. Etter din oppfatning, hvordan forholder kommune-ansatte (spesielt ledere) seg til digitale trusler som kan ramme kommunen?

Teknologi:

- Nå skal jeg stille spørsmål som faller innenfor kategorien teknologi

14. Hvordan sikres konfidensialitet, integritet og tilgjengelighet gjennom teknologi?
    - Hva slags utfordringer har kommuner med dette i dag?
15. Hvilke løsninger og type teknologier anbefaler dere at kommuner benytter for å ivareta informasjonssikkerhet og personvern? (f.eks. overvåkningsteknologier, penetrasjonstester og reservesystemer)
16. Hva har dere lært fra tidligere hendelser knyttet til cyber-angrep fra andre kommuner som har opplevd dette?

Vedlegg E

Informasjonsskriv til informanter

Vil du delta i forskningsprosjektet

«Komparativ studie om digital sikkerhet i offentlig sektor»

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å *undersøke hvilke endringer og tiltak dagens risikobilde har utløst i kommunal sektor.* I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Temaet for masteroppgaven er risikohåndtering og digital sikkerhet. Formålet er å se hvilke holdninger og tiltak dagens risikobilde har utløst i kommunal sektor, og vurdere utfordringer som kommunene møter på når omstillinger og endringer skjer i takt med en digital transformasjon. Det er ønskelig å finne ut hvilke tiltak kommunene gjør og om kommunene kan lære fra hverandre. Holdninger rundt digital sikkerhet er sentralt for oppgaven hvor målet er å bedre sikkerhetsbevissthet generelt, men spesielt for offentlig sektor. Verdens utvikling i dag peker på et enda større behov for nasjonal sikkerhet også blant kommunene. Nasjonal sikkerhet utfordres av teknologi-utviklingen fordi vi gjør oss avhengig av nye tjenester, og fordi nye sårbarheter oppstår. Bevisstheten og kompetanse om trussel- og risikobildet er for svak, og ledere i offentlig sektor har et stort ansvar. Dermed er masteroppgavens utvalgte tema svært aktuelt.

Hvem er ansvarlig for forskningsprosjektet?
NTNU Institutt for sosiologi og statsvitenskap er ansvarlig for prosjektet.

Det samarbeides også med Universitetskommunen (Trondheim kommune), der Elin E. Sotberg Harder (Programleder DigiTrøndelag og Rådgiver Kommunedirektørens fagstab) er problemeier for oppgaven.

Hvorfor får du spørsmål om å delta?
Du får spørsmål om å delta fordi din kompetanse og erfaring er relevant for oppgaven. Utvalget er bestemt i samarbeid med Elin Sotberg Harder fra Trondheim kommune. Du ble dermed invitert til deltakelse gjennom henne. Det var ønskelig fra samarbeidspartner å intervjue flere kommuner i Trøndelag i tillegg til kommunesektorens interesseorganisasjon for å inkludere ulike nivå innen kommunal sektor

Hva innebærer det for deg å delta?
Utvalgt metode består av semi-strukturerte intervjuer. Du kan selv velge passende sted for intervjuet. Intervjuet tar gjerne sted fysisk om mulig, men kan også gjennomføres digitalt via Google Meet, Microsoft Teams eller Zoom. Opplysningene registreres gjennom lydopptak/ evt. videopptak dersom digitalt intervju gjennomføres.

- Hvis du velger å delta i prosjektet, innebærer det at du deltar på intervjuet. Det vil ta deg ca. 60 minutter. Spørsmålene er strukturert gjennom tre hovedkategorier: organisering, menneske og teknologi. Spørsmålene omhandler arbeid med digital sikkerhet og risikohåndtering hvor ledelse, samarbeid, omgivelser (dagens risikobilde), kompetanse, teknologiske løsninger og håndtering av uønskede hendelser er i fokus.

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli

slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

Opplysningene om deg vil kun bli brukt til formålene som beskrives i dette skrivet. Opplysningene blir behandlet konfidensielt og i samsvar med personvernregelverket. Det er kun student (Marie Berntsen), veileder (Barbara Zyzak) og problemeier (Elin E. Sotberg Harder) som vil ha tilgang til opplysningene, som navn på vedkommende, (mailadresse) og stilling. Navnet og kontaktopplysningene dine vil jeg erstatte med en kode som lagres på egen navneliste adskilt fra øvrige data. Under transkriberingen anonymiseres opplysninger som kan identifisere deg som person. Etter dette slettes lydopptaket. Det vil ikke være noen opplysninger som kan knyttes til deg som person i den ferdige masteroppgaven.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?
Opplysningene anonymiseres når prosjektet avsluttes/oppgaven er godkjent, noe som etter planen er ca. 6. Juni 2023. Da blir opptakene slettet i tillegg til liste med navn og stilling. Dersom oppgaven skal jobbes videre med, for en oppfølgingsstudie eller senere forskning, vil personopplysningene oppbevares maks 2 år etter startdato (10.01.2022) på prosjektet.

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:
- innsyn i hvilke personopplysninger som er registrert om deg, og å få utlevert en kopi av opplysningene,
- å få rettet personopplysninger om deg,
- å få slettet personopplysninger om deg, og
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger.

Hva gir oss rett til å behandle personopplysninger om deg?
Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra NTNU, Institutt for sosiologi og statsvitenskap har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Hvor kan jeg finne ut mer?
Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:
- NTNU Institutt for sosiologi og statsvitenskap, ved veileder
  - Veileder: Barbara Zyzak, mob. 96744330, barbara.k.zyzak@ntnu.no
  - Student: Marie Berntsen, mob. 90173632, mariebernt@msn.com
- NTNUs personvernombud: Thomas Helgesen, tlf 93 079 038, thomas.helgesen@ntnu.no

Hvis du har spørsmål knyttet til NSD sin vurdering av prosjektet, kan du ta kontakt med:
- NSD – Norsk senter for forskningsdata AS på epost (personverntjenester@nsd.no) eller på telefon: 55 58 21 17.

Med vennlig hilsen

Barbara Zyzak (Førsteamanuensis/veileder)

Marie Berntsen (Masterstudent)

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *Komparativ studie om risikohåndtering og digital sikkerhet i offentlig sektor*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☐ å delta i intervju
- ☐ at mine personopplysninger lagres etter prosjektslutt, til senere forskning/oppfølging hvis aktuelt

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

---

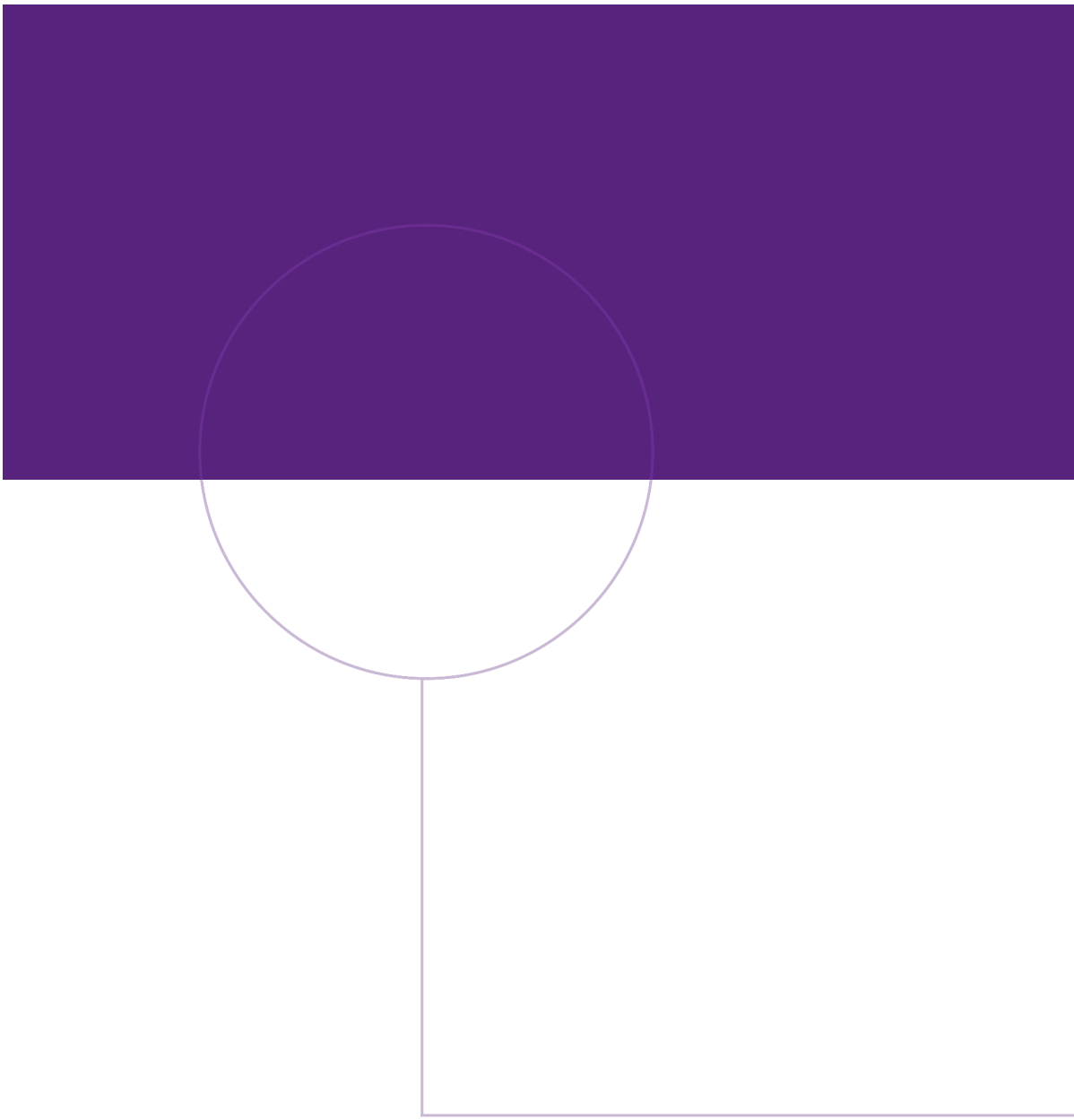
(Signert av prosjektdeltaker, dato)

Vedlegg F

Kort oppsummering av sentralt lovverk
Sikkerhetsloven §1-1 som trådte i kraft fra 1. januar 2019 skal bidra til 1) å trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser, 2) å forebygge, avdekke og motvirke sikkerhetstruende virksomhet og 3) at sikkerhetstiltak gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn. Sikkerhetsloven gjelder for statlige, fylkeskommunale og kommunale organer, i tillegg kan den gjelde for andre virksomheter som behandler sikkerhetsgradert informasjon (Sikkerhetsloven, 2019, §1-1).

Ifølge Kommuneloven §25-1 (2021) skal kommuner og fylkeskommuner «ha internkontroll med administrasjonens virksomhet for å sikre at lover og forskrifter følges. Kommunedirektøren i kommunen og fylkeskommunen er ansvarlig for internkontrollen. Internkontrollen skal være systematisk og tilpasses virksomhetens størrelse, egenart, aktiviteter og risikoforhold». Det løftes blant annet opp i denne loven at kommunedirektøren skal avdekke og følge opp avvik og den gjeldende risikoen.

eForvaltningsforskriften §15 (2004) er også sentral for den digitale sikkerheten. Loven sier at offentlige virksomheter skal ha beskrevet «mål og strategi for informasjonssikkerhet i virksomheten [...] Forvaltningsorganet skal ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem». Digitaliseringsdirektoratet har blitt utnevnt til å gi anbefalinger på området etter eForvaltningsforskriften.



NTNU

Kunnskap for en bedre verden