MASTEROPPGAVE

Emnekode: SO330S Navn: Nina Louise Danielsen

- Det skjer ikke oss

Cybersikkerhet i norske kommuner

Dato: 16.mai.2022 Totalt antall sider: 99

NORD universitet

www.nord.no

Forord

Da er det kommet til slutten for meg for denne gang og jeg leverer endelig mitt avsluttende prosjekt som masterstudent i samfunnsvitenskap med fordypning i samfunnssikkerhet og terrorismestudier på Nord Universitet.

Først og fremst vil jeg takke veileder Harald Fardal. Takk for gode råd og støtte i denne prosessen.

En stor takk informantene som tok seg tid i en travel arbeidshverdag til å snakke med meg. Takk for hjelpen!

Jeg vil også benytte anledningen til å takke familie og venner, dere har vært utrolig god støtte gjennom hele denne perioden som har vært veldig utfordrende for meg. En spesiell takk til mor og far, dere har vært mitt anker gjennom hele denne perioden og jeg hadde ikke klart dette uten dere!

Takk til alle ulike studievenner jeg har fått på veien mot målet, dere har hver og en vært viktige for meg på veien mot målet. Jeg vil også rette en spesiell takk til Kristin, Elsa, Hege og Jeannett som i siste liten hjalp med oppgaven og ikke minst rettskrivingen.

Mai 2022

Nina Louise Danielsen

Sammendrag

Digitaliseringen fører til flere muligheter for kommunene i Norge, men også til økt sårbarhet for brudd på cybersikkerheten. Utbredelsen av digitaliseringen fører til flere cyberangrep, og de oppstår hyppigere enn før. Angrepet som skjedde på Østre Toten førte til store økonomiske konsekvenser for kommunen og risikostyringen av cybersikkerhet var mangelfull. Formålet med denne studien er å se på hvordan kommuner arbeider med cybersikkerhet, og om hendelser som angrepet Østre Toten opplevde, påvirker norske kommuner til endring. Det fører meg til problemstillingen som er:

«Hvordan er arbeidet med cybersikkerhet i norske kommuner, og har angrepet på Østre Toten ført til endringer?»

Problemstillingen blir besvart som følge av 3 forskningsspørsmål: (1) Hvordan påvirker ledelsesforankring arbeidet med cybersikkerhet? (2) Hvordan ligger risikostyring til grunn for arbeidet med cybersikkerhet? (3) Hvordan er sikkerhetskultur integrert i arbeidet med cybersikkerhet? Metoden som er brukt for å besvare disse forskningsspørsmålene er kvalitative dybdeintervjuer. Det har blitt intervjuet 10 informanter fra IT-avdelinger i kommuner, eller blant de som drifter IT for kommunene. Resultatene som samlet inn fra intervjuene vil bli diskutert i sammen med teorien. Det som kom frem i empirien ble analysert ved en innholdsanalyse. Teoriene som vil bli brukt for å diskutere resultatene er ledelsesforankring, beredskap, risikostyring, risikopersepsjon, kultur og sikkerhetskultur. Det vil forgående bli presentert teori om begrepene cybersikkerhet, risiko og kultur for videre forståelse av oppgavens temaer.

Analysen viser til at det gjennomgående i studien er at ledelsesforankring har påvirket arbeidet med cybersikkerhet i kommunene, ettersom endringer i toppledelsen har ført til endringer i det forebyggende arbeidet med cybersikkerhet. I tillegg belyser også analysen hvordan risikoforståelsen har endret seg i kommunene som følge av angrepet på Østre Toten, og av den grunn har risikostyringen av cybersikkerhet endret seg. Arbeidet med sikkerhetskultur gjeldende cybersikkerhet er komplisert, men det arbeides stadig med forbedring. Konklusjonen for oppgaven er at arbeidet med cybersikkerhet i kommunene er mangelfullt og utfordrende, men at angrepet på Østre Toten har ført til endringer.

Liste over forkortelser

Forkortelser	**Forklaring**
Digdir	Digitaliseringsdirektoratet
DSB	Direktoratet for samfunnssikkerhet og beredskap
GRPS	Global Risks Perception Survey
KINS	Foreningen for kommunal informasjonssikkerhet
KS	Kommunesektorens organisasjon
IKT	Informasjons- og kommunikasjonsteknologi
IT	Informasjons Teknologi
NOU	Norsk offentlig utredning
NSD	Norsk senter for forskningsdata
NSM	Nasjonal sikkerhetsmyndighet
NSR	Næringslivets sikkerhetsråd
NVE	Norges vassdrag- og energidirektorat
PST	Politiets sikkerhetstjeneste
WEF	World Economic Forum

Innholdsfortegnelse

Oversikt over tabeller:

Oversikt over figurer:

1.0 Innledning

Digitaliseringen i Norge fører til flere muligheter med digitale tjenester som kan virke utenkelige, men det medfører også nye utfordringer for samfunnet (Departementene, 2019, s. 6). Utviklingen av teknologi fører til at samfunnet blir avhengig av digitale tjenester og sårbarhetene for digitale trusler blir større (Departementene, 2019; Nasjonal Sikkerhetsmyndighet, 2022). Med digitaliseringen og den teknologiske utviklingen følger en økning i nettkriminalitet, hvor det kontinuerlig utvikles nye angrepsmetoder, verktøy og teknikker som gir angripere muligheten til å trenge seg inn i organisasjoners datasystemer (Bendovschi, 2015). Cyberangrep blir på daglig basis en større realitet både for store og små selskaper, så vel som enkeltpersoner. Dette fører til økt risiko for brudd på cybersikkerheten (Bendovschi, 2015).

I World Economic Forum (WEF) hevdes det at avhengigheten for komplekse digitale systemer øker, noe som kan føre til at cybertrusler kan overgå samfunnets evne til å effektivt forebygge og håndtere dem (World Economic Forum, 2022, s. 45). «Cybersikkerhetssvikt» ble ifølge en undersøkelse kalt: «Global Risks Perception Survey (GRPS)» også rangert som topp 10 risikoer som har blitt større siden starten på COVID-19 pandemien. I tillegg ble cybersikkerhetssvikt rangert som topp 5 risiko-utfordringer i Europa (World Economic Forum, 2022, s. 45). Til tross for økende grad av digital forståelse og modenhet i ulike selskap, samt økt investering i cybersikkerhet, er virksomheter fremdeles for dårlig forberedt på cyberhendelser (KPMG, 2018). I en mørketallsundersøkelse som ble utført i 2018 av næringslivets sikkerhetsråd (NSR) kommer det frem at det er stor naivitet omkring forståelse av egne verdier, konsekvenser og kostnader for virksomheten når vi snakker om cyberangrep. Tilsvarende viser det at mange har holdningen «det vil ikke skje oss» (KPMG, 2018).

NorSIS (2021) hevder at løspengevirus og andre alvorlige digitale trusler er mer aktuelt enn noen gang, både for de norske kommunene, samt små og mellomstore bedrifter. I en mørketallsundersøkelse utført av NorSIS (2021) beskrives det også at løspengevirus og andre typer cyberangrep rammer og ødelegger store summer i bedrifts-Norge hver eneste dag. Årsaken til at omfanget av dette ikke tidligere har vært kjent er at mange norske virksomheter ikke snakker høyt om angrepene når det skjer (NorSIS, 2021, s. 5). Problemet i mange av bedriftene er at flere mener de ikke er attraktive mål for nettkriminelle, men ifølge NorSIS (2021) er dette ikke tilfellet. Alle bedrifter/organisasjoner har verdier som kan videreselges, brukes til utpressing eller omsettes på en eller annen måte (NorSIS, 2021, s. 5). Med sine nesten 15 000 innbyggere er Østre Toten et eksempel på hvor totalt og nådeløst et cyber

angrep kan ramme (NorSIS, 2021, s. 5). Angrepet Østre Toten opplevde førte til store konsekvenser for kommunen, blant annet økonomiske tap og sensitiv data på avveie (KPMG, 2021; NorSIS, 2021).

1.1 Studiens tema

I risikovurderingen fra Nasjonal Sikkerhetsmyndighet (NSM) ser man en økende trusselaktivitet i cyberdomenet, både fra kriminelle og statlige aktører (Nasjonal Sikkerhetsmyndighet, 2022, s. 17). NOU: 2015: 13 beskriver at den økte digitale kompleksiteten fører til store utfordringer både lokalt og regionalt. Dette gjelder spesielt for kommunesektoren fordi det er mange små enheter som har ansvar for viktige enheter og tjenester, men som også kan ha manglende kompetanse på IKT-sikkerhet (NOU 2015: 13, s. 250).

I Politiets sikkerhetstjeneste (PST) sin trusselvurdering vil nettverksoperasjoner fremdeles utgjøre en trussel mot Norge. Operasjonene mot Stortinget i 2020 og 2021 er eksempler på svært alvorlige hendelser (Politiets Sikkerhetstjeneste, 2022, s. 7). Ifølge PST sin trusselvurdering har NSM også observert en tredobling av alvorlige hendelser med nettverksoperasjoner det siste året (Nasjonal Sikkerhetsmyndighet, 2022; Politiets Sikkerhetstjeneste, 2022).

Gjennom undersøkelsene i 2015 fra NOU og innspill fra Direktoratet for samfunnssikkerhet og beredskap (DSB) kom det frem at det var mangel på IKT-sikkerhetskompetanse, både på ledelsesnivå og for ansatte, og at dette var en utfordring for kommunene. Foreningen for kommunal informasjonssikkerhet (KINS) trakk også frem en observert sårbarhet hvor ledelsen har mange tradisjonelle ansvarsområder, og hvor IKT-sikkerhet fikk lite oppmerksomhet (NOU 2015: 13, s. 243). Dette kan begrunnes med at IKT-sikkerhet er et relativt nytt område som ikke blir prioritert på lik linje med andre oppgaver (NOU 2015: 13, s. 246). IKT-sikkerhet blir også sett på som teknisk vanskelig. Det kom også frem at mange kommuner mangler styringssystem og hadde for dårlig internkontroll (NOU 2015: 13, s. 246).

1.2 Bakgrunn

Østre Toten opplevde 9.januar 2021 et cyberangrep som førte til store økonomiske tap for kommunen, og ifølge NRK (2021) var nok dette det største hackerangrepet Norge noensinne har erfart mot en kommune (Kessel & Røsrud, 2021). Store deler av Østre Toten sine systemer og informasjon ble kryptert og gjort utilgjengelige som følge av en angriper kom seg inn på kommunens IT-systemer (NorSIS, 2021). KPMG (2021)har vurdert forholdene for

kommunen i etterkant hvor flere av systemene, spesielt sikkerhetsstyringen, var svak eller mangelfull (KPMG, 2021, s. 2). Rapporten baserte seg på muntlig informasjon ettersom det var manglende tilgjengelighet på dokumentasjon etter angrepet. I denne rapporten ble det gjennomført en praktisk beskrivelse av hvordan Østre Toten kommune jobbet med IKT-sikkerhet og informasjonssikkerhet (KPMG, 2021, s. 24, 25). Vurderingen av kommunens sikkerhetstilstand forut for angrepet, var at sikkerhetsstyringen har vært mangelfull og sikkerhetstiltak har virket tilfeldige. Resultatene viste til at Østre Toten i liten grad hadde fulgt NSMs grunnprinsipper for cybersikkerhet. I tillegg beskrives det i rapporten manglende kompetanse og forståelse hos både ledere og medarbeidere (KPMG, 2021, s. 24, 25). KPMG (2021) kommenterer også hvordan manglende kultur påvirket sikkerhetsarbeidet i kommunen. Det viser også til at det ikke i tilstrekkelig grad arbeides med kompetanseutvikling og sikkerhetskultur i norske kommuner. Dette er med på å utgjøre hindringer i arbeidet med informasjonssikkerhet (KPMG, 2021, s. 24, 25).

I en kartlegging utført av Helsetilsynet (2020) har det blitt undersøkt hvordan sykehusene er forberedt på å håndtere IKT-bortfall. Undersøkelsen er gjennomført ved 17 virksomheter i spesialhelsetjenesten og handler om hvordan de har vurdert risikoen for forsvarlig helsehjelp ved bortfall av viktige IKT-systemer. Det ble også undersøkt hvorvidt virksomhetene var forberedt på nedetid. Funnene viste til at virksomhetene i sammenheng med leverandører har utfordringer i arbeidet med ansvarsfordeling av risikovurderinger. Komplekse organisasjoner fører til at ansvarsfordelingen blir for komplisert og at dette burde arbeides med. Svake planverk for krisehåndtering ved bortfall av IKT-systemer og lite øvelsesrutiner var ikke tilstrekkelige sett i sammenheng med tekniske løsninger (Helsetilsynet, 2020, s. 5, 6).

Videre i undersøkelsen formidler Helsetilsynet (2020) at det ved bortfall av IKT-systemer må det utføres undersøkelser på pasienter uten å vite tidligere sykehistorikk eller informasjonen til pasientene. Det var også fare for svikt i forsvarlig helsehjelp dersom IKT-bortfall varte i lengre tid. Virksomhetene hadde i flere tilfeller risikoanalyser i forhold til det tekniske. Risikoanalysene inkluderte ikke konsekvenser av IKT-bortfall, og de var ikke forberedt på å håndtere langvarig bortfall av IKT-systemer. Videre funn viste at det ikke hadde blitt gjennomført øvelser for ansatte ved bortfall av IKT-systemer. Det blir også presentert i studien at helsevesenet arbeider for å utvikle planer for krisehåndtering og sørge for at det blir øvd i henhold til disse planene. Virksomhetene formilder videre at det er utfordrende å lage beredskapsplaner i henhold til IKT-bortfall. Å drive et sykehus uten IKT-støtte og

konsekvensene av det var ikke noe sykehusene hadde tatt stilling til. De var dermed ikke forberedt på å håndtere langvarige IKT-bortfall (Helsetilsynet, 2020, s. 5, 6).

1.3 Formål og problemstilling

Angrepet på Østre Toten og undersøkelsen utført av Helsetilsynet har ført til formålet med denne studien. Formålet er å se på hvordan kommunene i Norge arbeider med cybersikkerhet og om cyberangrepet på Østre Toten i januar 2021 har ført til endringer i kommunene. Studien skal bidra til å belyse hvilke utfordringer kommunene står ovenfor i arbeidet med cybersikkerhet, samt om hendelser fører til endring i kommunene. Dette kan bidra til å få et mer oversiktlig bilde på hvordan kommuner arbeider med cybersikkerhet på tross av de ulike sektorene. Derav problemstillingen:

«Hvordan er arbeidet med cybersikkerhet i norske kommuner, og har angrepet på Østre Toten ført til endringer?»

Som fører meg videre til forskningsspørsmålene:

Forskningsspørsmål 1: Hvordan påvirker ledelsesforankring arbeidet med cybersikkerhet?

Forskningsspørsmål 2: Hvordan ligger risikostyring til grunn for arbeidet med cybersikkerhet i kommunene?

Forskningsspørsmål 3: Hvordan er sikkerhetskultur integrert i arbeidet med cybersikkerhet?

Problemstillingene i sammenheng med forskningsspørsmålene vil bli besvart gjennom en kvalitativ metode. Svarene i sammenheng med teori vil diskuteres og analyseres for å frembringe konklusjon på oppgaven.

1.4 Avgrensinger

For å tydeliggjøre studien og som følge av tid og ressurser vil det være viktig å avgrense temaet. Det finnes forskjellige fremgangsmåter for en kommune å jobbe med cybersikkerhet, og flere ulike sektorer innenfor kommunen som muligens har ulike perspektiver på samme tema. Derfor vil det i denne studien bli sett på et overordnet bilde i kommunene om hvordan de arbeider med cybersikkerhet med hovedsakelig fokus på risikopersepsjon før og etter Østre Toten. I tillegg til ledelsesforankring av cybersikkerhet går oppgaven inn på hvilke endringer som har blitt utført, hvilke utfordringer de har i arbeidet med cybersikkerhet samt hvordan sikkerhetskulturen er.

På bakgrunn av dette vil den tekniske delen av arbeidet med cybersikkerhet ikke bli prioritert ettersom det er noe som kan kreve sikkerhetsklarering og fordi de ansatte muligens har taushetsplikt. Fordi virksomhetsledere i kommunen sannsynligvis ofte har det travelt, og fordi det vil være for tidskrevende å skulle få tak i mange ledere, vil det avgrenses til å kun se på informanter som jobber innenfor IKT-avdelinger. Det vil heller ikke bli snakket med de som jobber i beredskapsavdelingen på grunn av manglende tid og ressurser. Ettersom undersøkelsen handler om å få et oversiktlig bilde, vil det ikke bli gått inn på detaljer i de ulike delene.

1.5 Oppgavens struktur

Oppgaven er delt inn i 8 deler. Strukturen vil presenteres her for at det skal bli lettere for leseren å forstå sammenhengen.

Kapittel 1 har gitt en presentasjon av tema og bakgrunn for valg av tema. Videre har problemstillingen og tilhørende forskningsspørsmål samt formålet med studien blitt presentert. Til slutt har det blitt redegjort for de avgrensningene som tilhører studien.

Kapittel 2 knytter temaet til konteksten. Innenfor dette kapittelet vil det også komme frem hvordan kommunen organiseres, og hvilket trusselbilde de står ovenfor.

Kapittel 3 beskriver oppgavens teoretiske rammeverk. Teoriene som vil bli presentert her er forskning på temaet, cybersikkerhet, sårbarheter, risiko, risikopersepsjon, risikostyring, beredskap, ledelsesforankring, kultur og sikkerhetskultur.

Kapittel 4 går inn i detaljer om metoden som er brukt for å gjennomføre studien. Her vil de metodiske valgene som er gjort utdypes, og en vurdering av oppgavens gyldighet og etiske betraktninger beskrives.

Kapittel 5 viser til de empiriske funnene med likheter og ulikheter for temaene som fremsto i analysen.

Kapittel 6 utarbeider diskusjonen av forskningsspørsmålene for å kunne svare på problemstillingen. Her blir empirien satt sammen med teorien som jeg redegjør for i kapittel 3.

Kapittel 7 belyser de viktigste elementene til stede i diskusjonen og former konklusjonen av oppgavens problemstilling. Videre vil jeg fokusere på temaer som kan eller bør forskes videre på.

2.0 Kontekst

Kommuner er komplekse organisasjoner med flere ulike sektorer. I dette kapitlet blir konteksten av studiet presentert i lys av sårbarheter kommuner står ovenfor, hvordan kommuner er organisert og hvilke cyberangrep som kan ramme. Dette kapittelet skal bidra med å få innsikt i trusler kommunene står ovenfor, samt hvordan kommuner har en komplisert organisasjon og hvordan trusselbildet da fremstår for kommunene.

2.1 Kommunens organisering og drift

Jacobsen (2009) beskriver de ulike oppgavene norske kommuner i Norge har. En av de mest sentrale oppgavene er tjenesteyting, deriblant; helsetjenesten, omsorgstjenesten, sosialtjenester, grunnskole og voksenopplæring, oppvekstmiljø, lokale veier, vanntilførsel, søppeltømming og kloakk, kirker og kirkegårder (Jacobsen, 2009, s. 50-53). De fleste kommunale oppgaver ivaretas normalt sett av kommunens egen driftsorganisasjon. Unntaket er når det er tekniske tjenester, støttefunksjoner der interkommunale løsninger er utbredt, som renovasjon og delvis innkjøp, eller tjenester som i dominerende grad blir ivaretatt av private aktører (Hovik & Inger Marie, 2004, s. 11). Det har også tidligere vært endringer på organiseringen av kommuner. Endringene som ble foretatt på 90-tallet var først og fremst for å møte kravet om høyere produktivitet og mer tjenester for hver krone (Hovik & Inger Marie, 2004, s. 13).

De mest ressurskrevende oppgavene er knyttet til helse, sosial og skole, som i en gjennomsnittlig kommune står for ca. 75 % av kommunens totale utgifter. Kommuner har også andre sentrale oppgaver som blant annet forvaltningsoppgaver og utviklingsoppgaver (Jacobsen, 2009, s. 50-53). I likhet med andre større organisasjoner har også kommunen en intern administrasjon knyttet til ulike former for planlegging, personalforvaltning, personalutvikling, økonomistyring og organisasjonsutvikling (Jacobsen, 2009, s. 50-53). Figur 1 under viser hvordan oppgavene til kommunen er fordelt og hvilke oppgaver som er mest ressurskrevende.

Figur 1: Kommunale oppgaver (Jacobsen, 2009, s. 52).

Videre er kommunen som organisasjon finansiert gjennom at innbyggere og Norge som land betaler inn politisk bestemte summer til fellesskapet, som igjen går ut som tjenesteyting fra kommunen (Jacobsen, 2009, s. 56). Det er ulike måter en kommune er organisert på, men flertallet av kommunene i Norge har delegering av beslutningsmyndighet fra et kommunestyre eller administrasjonssjef/rådmann (Jacobsen, 2009, s. 85). Videre i oppgaven, uavhengig av hvordan kommunene har organisert ledelsen, vil den øverste ledelsen (administrasjonssjef, kommunestyre og rådmann) bli omtalt som toppledelsen.

2.2 Trusselbildet for kommuner

I rapporten til Kommune-CSIRT (2020) hevdes det at nye digitaliseringsprosjekter gjør at angrep mot digitaliserte tjenester vil øke. Angrepene i offentlig sektor fortsetter i uforminsket styrke, både mot epostkontoer, internetteksponerte tjenester og mot hjemmekontorløsninger (Kommune-CSIRT, 2020). Hensikten med angrepene i offentlig sektor er både å stjele innloggingsdetaljer, kryptering av data for å drive med utpressing samt spionasje mot myndigheter (Kommune-CSIRT, 2020). Når kommuner blir utsatt for et cyberangrep slik som angrepet på Østre Toten, betyr det at kommunen blir utsatt for en uønsket hendelse. «En uønsket hendelse er en hendelse eller handling som kan føre til skade på et eller flere verdiobjekt, hvis det ikke er installert effektive barrierer eller sikkerhetsfunksjoner i analyseobjektet, eller hvis det ikke på annen måte gripes inn slik at utviklingen av hendelsen

stoppes» (Rausand & Utne, 2022, s. 29). I figur 2 nedenfor blir det presentert hvordan en uønsket hendelse foregår.

.

Figur 2. Hendelse med årsak og virkning (Rausand & Utne, 2022, s. 29).

Det finnes to ulike typer uønskede hendelser. En utilsiktet uønsket hendelse kan for eksempel være bortfall av strøm på grunn av teknisk svikt (Rausand & Utne, 2022, s. 30). Tilsiktede uønskede hendelser er en uønsket hendelse eller handling som er forårsaket med hensikt av en person eller gruppe (Rausand & Utne, 2022, s. 30). Dette vil bli brukt videre i oppgaven for å se hvordan kommunene kan bli utsatt for uønskede hendelser.

Innenfor utilsiktede hendelser som kan påvirke kommunens cybersikkerhet er naturhendelser en av dem. Mye nedbør, vind eller storm generelt kan føre til bortfall av strøm i kommunene (NOU 2015: 13, s. 52). Andre utilsiktede hendelser kan være menneskelig svikt, som at mennesket ikke forstår systemene og ikke klarer å holde på gode sikkerhetsrutiner eller holdninger til sikkerhetsarbeidet. Organisatorisk svikt kan også være en årsak til utilsiktede hendelser i en kommune. Årsaken til dette kan for eksempel være at organisasjoner ikke forstår hvilke verdier de besitter og dermed ikke beskytter de viktigste tjenestene, eller at det er generelt manglende kunnskap om cybersikkerhet (NOU 2015: 13, s. 53).

Tilsiktede hendelser kommuner står ovenfor er IKT-kriminalitet, cyberangrep (digitale angrep), spionasje og terror (NOU 2015: 13, s. 54). Individer eller grupper av ulike trusselaktører har forskjellige motiver for å utføre tilsiktede hendelser på kommuner. Motivene er varierende, og de kan være alt fra økonomisk vinning til politisk press. Angrepene er ulike, men jeg vil nedenfor presentere typiske cyberangrep eller IKT- angrep en kommune kan stå ovenfor (NOU 2015: 13, s. 54). Cyberangrep blir definert varierende i litteraturen. I studien til Hathaway (2012) diskuteres det forskjellige måter å forstå et cyberangrep på. Hathaway (2012) forholder seg til denne definisjonen: «Et cyberangrep

består av enhver handling utført for å undergrave funksjonene til et datanettverk for å nå et politisk eller nasjonal sikkerhetsformål» (Hathaway et al., 2012, s. 826). Ifølge Rausand og Utne (2020) blir et cyberangrep forklart som: «Cyberangrep er der trusselaktøren utfører angrepet via et datanettverk. I dette tilfellet kan trusselaktøren befinne seg hvor som helst. Et cyberangrep kan også kalles et IKT-angrep» (Rausand & Utne, 2022, s. 38). Beskrivelsen til Rausand og Utne (2022) vil bli brukt videre som følge av oppgavens tema. Cyberangrep blir også ofte brukt som et synonym til dataangrep, men det vil kun bli brukt cyberangrep i denne studien (Rausand & Utne, 2022, s. 278). Ifølge Bendovschi (2015) har ulike typer cyberangrep blir studert og definert. De ulike typene vil bli presentert nedenfor for å få en forståelse av hvilke cyberangrep kommunene kan bli utsatt for:

«Man in the middle attack»- er et angrep som oppstår når det er kommunikasjon mellom to parter. Disse partene kan bli forstyrret av en angriper, som fører til at meldingen blir sendt til angriperen, før den kommer til planlagt mottaker (Bendovschi, 2015). Ved et angrep som dette kan konsekvensene bli at angriperen får tilgang til sensitiv informasjon eller endrer meldingen (Bendovschi, 2015).

«Brute force-angrep»: Angriperen vil ha tilgang på beskyttet informasjon (f.eks. passord, kryptering) og prøver igjen og igjen frem til riktig nøkkel er funnet og man får tilgang på informasjonen (Bendovschi, 2015).

-«DDoS (Distributed Denial of Service)» er et angrep som består av å ødelegge tilgjengeligheten av data, hvor det da blir oversvømt på f.eks. en server med beskjeder og serveren blir ubrukelig (Bendovschi, 2015).

-Skadevare(«Malware»): Her benytter angriperen de tekniske sårbarhetene for å oppnå tilgang og rettigheter til teknisk utstyr. Skadevare blir ofte presentert som en spredningsform, som virus, orm, løspengevirus, bakdør eller trojansk hest (Bendovschi, 2015; NOU 2015: 13).

-«Phising» angrep er en teknikk som handler om at angriperen stjeler privat informasjon fra brukere gjennom å bruke en maske i en pålitelig kilde, som for eksempel e-post fra en sjef i sin egen organisasjon (Bendovschi, 2015).

-«Social Engineering» er et generelt begrep som brukes for å beskrive teknikker som blir brukt for å få tilgang til ulike deler, via mennesker (Bendovschi, 2015).

3.0 Teori

I dette kapittelet presenteres ulike teoretiske perspektiver og begreper som bidrar som utgangspunkt for det empiriske materialet som har blitt samlet inn. Teorigrunnlaget utgjør et rammeverk som vil brukes for å belyse problemstillingen sammen med forskningsspørsmålene. Det vil først bli presentert forskning på temaet for å belyse hva som er forsket på i lignende temaer og hva som finnes innen forskningsfeltet. Etterfølgende vil det bli presentert teorier om begrepene sårbarheter, cybersikkerhet og risiko som brukes for å diskutere hvordan kommunene jobber med cybersikkerhet. Til slutt fremstilles det teoretiske grunnlaget av risikopersepsjon, risikostyring, ledelsesforankring, kultur og sikkerhetskultur.

3.1. Forskning på temaet

I studien gjennomført av Choodakowska, Kandula og Przybylska (2022) ble det undersøkt hvorvidt kommuner i Polen har innført retningslinjer angående cybersikkerhet. Funnene tilsier at flertallet av kommunene har implementert tilstrekkelig informasjonssikkerhet som blir gjennomgått i en årlig revisjon. Det viser likevel til at flere av kommunene ikke har iverksatt forebyggende tiltak for å unngå brudd på cybersikkerheten (Choodakowska, Kandula & Przybylska, 2022). Studien viser til at det er manglende bevissthet omkring nettkriminalitet og mangel på kunnskap om lovverk i den forbindelse (Choodakowska et al., 2022).

Videre formidles det i studien til Choodakowska et al. (2022) at kommunene, som hadde liten forståelse på cyberangrep, heller ikke hadde utført risikoanalyser for sannsynligheten for å miste informasjon. Flere av kommunene var likevel delvis forberedt på cyberangrep. Likevel viser funnene at det var en del av kommunene som ikke hadde gjennomført tiltak for å være forberedt på cyberangrep. Årsakene til at kommunene ikke var forberedt på cyberangrep var at ansatte ikke var opplærte, det var manglende bevissthet om trusler samt mangel på økonomiske ressurser. Det var også mange av kommunene som manglet retningslinjer til arbeidet med cybersikkerhet. Resultatene i undersøkelsen av kommunene i Polen var at det var et økt behov for forbedring av cybersikkerheten. Blant annet bør kommunene få tilført mer økonomiske ressurser, økt kunnskap blant ansatte og bedre teknisk sikkerhet (Choodakowska et al., 2022).

I Ruuds (2011) masteroppgave studeres det hvordan bruken av IKT i kommunene øker og hvordan dette stiller store krav til sikkerhet. Ruud (2011) studerte hvordan man som innbygger kan være sikker på at kommunen forvalter sensitive opplysninger på en sikker måte, og hvilke rutiner og sikkerhetssystemer som har blitt etablert for at personvernet skal bli

ivaretatt. Ruud (2011) spør videre: Hvilke faktorer er det som bidrar til, eller hindrer en sikker behandling av sensitive opplysninger i kommunen? Det ble gjort en kvalitativ studie med intervjuer av åtte personer delt på fire kommuner. Ruud (2011) oppdaget at det var mangelfullt på rutiner, og at det i alle kommunene manglet en overordnet beskrivelse av hvordan personvernet skulle ivaretas. Noen av kommunene påpeker at de hadde rutiner, men disse var ikke nedskrevet (Ruud, 2011). Funnene i studien til Ruud (2011) viste at mangel på kontroll av opplysningene som ble lagt inn om enkelte pasienter var noe av det mest oppsiktsvekkende. I tillegg til det var det ingen rutiner på hvordan man kunne vite at opplysningene som lå inne i fagprogrammene var korrekte. Noen av kommunene hadde også opplevd opplysninger som var lagt inn ukorrekt. Videre forteller Ruud (2011) at kommunene hadde få avvikssystemer og at flere av brukerne som skulle benytte seg av systemene ikke hadde fått god nok opplæring. Konklusjonen i undersøkelsen var at det var store mangler i arbeidet med personopplysninger (Ruud, 2011).

Cheng og Groysberg (2019) har gjennomført en studie for å finne ut av hvorfor styret i bedrifter ikke klarer å håndtere cybertrusler. Cybersikkerhet blir forstått som en av de største utfordringene ledere har i dag (Cheng & Groysberg, 2019, s. 39-40). Ifølge Cheng og Groysberg (2019) er spørsmålet om cybersikkerhet et av de viktigste politiske spørsmålene som blir stilt til styrer, kun etterfulgt av økonomi og miljøkrav. I undersøkelsen utført i samsvar med «Woman Corporate Directors», med Spencer Stuart og forskeren Deborah Bell, ble det spurt ledere om hvilke risikoer de bekymrer seg mest for og da ble cybersikkerhet et nedprioritert tema. Det de bekymret seg mest for var risikoer angående miljøkrav eller omdømmet, og lederne var mer forberedt på å håndtere disse risikoene. Videre viser funnene at ledere i organisasjoner ikke forstår de omfattende og langsiktige skadene cyberangrep kan påføre organisasjonene deres. Resultatene i studiene var at ledere mangler prosessene og ekspertisen for å henvende seg til cyberangrep (Cheng & Groysberg, 2019, s. 39-46).

Wirtz og Weyerer (2017) har undersøkt hvordan offentlige myndigheter oppfatter og håndterer cyberangrep. Studien undersøker offentlige ansattes holdninger til cybersikkerhet i offentlig sektor. Den omtaler også prosessene og tiltakene som er på plass for å beskytte sensitive myndighetsdata og behandle dem på en sikker måte for personvern og overholdelse av regelverk (Wirtz & Weyerer, 2017). I undersøkelsen ble det laget en utforskende ekspertundersøkelse og epost invitasjoner ble sendt ut til direktøren for offentlige myndigheter på kommunalt, regionalt, statlig og nasjonalt nivå i Tyskland. Det ble forespurt om den kunne videresendes til IT-ansvarlige for å delta i studien. Datainnsamlingen ble utført

ved hjelp av en selvadministrert internett-undersøkelse i 2015. Wirtz og Weyerer (2017) forteller at denne studien bidrar til å øke forståelsen av hvordan offentlige ledere oppfatter og håndterer digitale trusler. I studien kommer det frem at offentlige myndigheter viser stabilitet i form av effektive sikkerhetstiltak. Cyberangrep oppleves som en alvorlig trussel og det blir avslørt åpenbare svakheter i det offentlige. Wirtz og Weyerer (2017) beskriver videre hvordan det er sterkt potensiale for forbedring. Ettersom det digitale rommet («Cyber-Space») stadig er i endring, er det viktig at offentlig ledelse er klar over og oppdatert på alle typer tiltak som fører til beskyttelse av det digitale rommet. Det er også viktig å iverksette disse (Wirtz & Weyerer, 2017). I denne forbindelse viser studien at offentlig forvaltning bør ta tak i den observerte mangelen på beredskapstiltak og forbedre det for å kunne garantere cybersikkerhet. Selv om aspektene som er presentert tar for seg det operative nivået, bør likevel offentlige myndigheter ta ansvar for cybersikkerhetsrelaterte spørsmål. Kommunene må også sørge for nok ressurser og ta ansvar for at de har betingelser der de er i stand til å forbedre arbeidet med cybersikkerhet (Wirtz & Weyerer, 2017).

3.2 Cybersikkerhet, IKT-sikkerhet og informasjonssikkerhet

Chapmen & Reitel (2021) hevder at ordet «cybersikkerhet» ble brukt for første gang i 1989, og ble den gang definert som: «eventuelle tiltak som gjøres for å beskytte data eller et datasystem mot uautorisert adgang eller angrep» (Chapman & Reithel, 2021, s. 439). Branch (2021) viser i sin studie hvordan begrepet cybersikkerhet har blitt konstruert på ulike måter av språk og hvordan eksisterende litteratur viser til at fokuset går utover det tekniske og strategiske perspektiver (Branch, 2021). Lewallen (2021) forteller i studien at teknologi kan skape nye problemer. Årsaken til at teknologi kan skape flere problemer er at den er i stadig endring, og at flere ting tilkobles til internett. Eksempler på dette er; smarte hus, mobiltelefoner og andre deler som blir sårbare for cyberangrep, og dermed utvides begrepet cybersikkerhet (Lewallen, 2021, s. 1047). Armenia, Ferreira Franco, Nonino, Spagnoli og Medaglia (2019) mener at cybersikkerhet handler om mer enn bare teknologi. Det inkluderer også å se på lovlige og formelle oppgaver og prinsipper av sosiale interesser (Armenia, Ferreira Franco, Nonino, Spagnoli & Medaglia, 2019, s. 411). Craigen et al., (2014) foreslår følgende definisjon basert på nøkkelbegreper i eksisterende litteratur:

«Cybersikkerhet er organiseringen og samlingen av ressurser, prosesser og strukturer som brukes for å beskytte cyberrommet og cyber-aktiverte systemer som ikke stemmer overens med eiendomsretten» *(Craigen, Diakun-Thibault & Purse, 2014, s. 17).*

I studien til Von Solms og Van Niekerk (2013) blir det undersøkt ulike definisjoner av IKT-sikkerhet og informasjonssikkerhet for å se på hvordan cybersikkerhet skiller seg fra disse begrepene. Det blir tydelig i den forstand at cybersikkerhet handler mer om eiendeler som skal bli beskyttet, som kan være alt fra samfunnets interesser, personer, husholdningsapparater eller nasjonal infrastruktur (von Solms & van Niekerk, 2013). Mens IKT-sikkerhet ligger mer i beskyttelse av systemer som er teknologibasert, hvor kommunikasjon er lagret eller overført via internett. Informasjonssikkerhet handler om sikring av informasjonen, og at det skal behandles konfidensielt og med integritet (von Solms & van Niekerk, 2013). Informasjonssikkerhet er det samme som å sikre all informasjon, uavhengig om den er digital eller ikke (NVE, 2017, s. 15). Norges vassdrag- og energidirektorat (NVE) (2017) beskriver i rapporten hvordan IKT-sikkerhet handler om å sikre det som omhandler informasjons- og kommunikasjonsteknologi, som for eksempel maskinvare og programvare. Cybersikkerhet derimot er beskyttelse mot ting som er sårbare via IKT (NVE, 2017, s. 15). Likevel er ikke IKT-sikkerhet alene det som behøves for å oppnå cybersikkerhet. For å oppnå cybersikkerhet er det viktig med fysisk adgangskontroll, konsekvensreduserende tiltak, økt kompetanse og bevisstgjøring avgjørende (NVE, 2017, s. 15).

Ifølge Von Solms og Van Niekerk (2013) handler cybersikkerhet om alt som kan nås via cyberrommet, og kan dermed ikke ses på som et synonym for IKT-sikkerhet og informasjonssikkerhet. Langø og Sandvik (2013) hevder at cybersikkerhet er «trusler mot individer, organisasjoner og samfunn gjennom det digitale rommet. Cyberangrepene eller truslene kommer på ulike måter» (Langø & Sandvik, 2013, s. 221). Von Solms og Van Niekerk (2013) mener at cybersikkerhet handler om å sikre funksjoner i cyberrommet, uavhengig av om det er individer, organisasjoner eller nasjoner. På bakgrunn av dette har Von Solms og Van Niekerk (2013) definert cybersikkerhet som:

«Beskyttelse av det digitale rommet, elektronisk informasjon, IKT som beskytter det digitale rommet, og brukerne av det digitale rommet i sin personlige, samfunnsmessige og nasjonale kapasitet, inkludert alle deres interesser, enten materielle eller immaterielle, som er sårbare for angrep som oppstår i det digitale rommet» (von Solms & van Niekerk, 2013, s. 101).

Definisjonen viser at cybersikkerhet er mer omfattende enn det IKT-sikkerhet eller informasjonssikkerhet handler om (von Solms & van Niekerk, 2013). På bakgrunn av denne studiens tema, vil denne definisjonen bli brukt gjennomgående i studien fordi den omfatter det

menneskelige elementet, samt nasjonale interesser, som er relevant for videre forklaring av cybersikkerhet i denne oppgaven. Videre nevnes det i studien til Von Solms og Van Niekerk (2013) at informasjonssikkerhet og IKT-sikkerhet kan være de underliggende årsakene til sårbarheter i cybersikkerhet. Figur 3 under viser hvordan ulike trusler kan påvirke ulike sårbarheter, og blant disse er IKT-sikkerhet og informasjonssikkerhet:

Figur 3 : Cybersikkerhet (von Solms & van Niekerk, 2013, s. 99).

3.2.1 Styring av cybersikkerhet

Galinec, Možnik og Guberina (2017) mener å redusere sårbarheter er viktig i arbeidet med cybersikkerhet. Et viktig problem i samfunnet som kommer frem i studien til Galinec et al. (2017) er at det trengs bedre opplæring av cybersikkerhet og flere typer utdanning innen cybersikkerhet (Galinec, Možnik & Guberina, 2017, s. 284-285). Marvell (2015) forteller videre at det er viktig for organisasjoner å ha hele bildet på cybersikkerhet i organisasjonen. Dette innebærer hvilke trusler organisasjonen står ovenfor, hvilke trusler som aksepteres av organisasjonen og hvem er ansvarlig (Marvell, 2015, s. 26). For organisasjoner er det også viktig å hele tiden være oppdatert på trusselbildet i arbeidet med cybersikkerhet, ettersom det endrer seg hele tiden (Marvell, 2015, s. 26). Styring av cybersikkerhet handler om prosesser, planlegging og budsjettering av ressurser, og er en viktig del av cybersikkerhetsarbeidet (Marvell, 2015, s. 26).

3.3 Sårbarheter

Sårbarheter i en organisasjon blir ofte omtalt som et svakt punkt eller en svak egenskap- i et analyseobjekt som kan utnyttes av trussel-aktører i et cyberangrep (Rausand & Utne, 2022, s. 403). Sårbarheter kan defineres som: «Et uttrykk for de problemene et system vil få med å

fungere når det utsettes for en uønsket hendelse, samt de problemene systemet får med å gjenoppta sin virksomhet etter at hendelsen er inntruffet» (NOU 2000: 24, s. 18; Rausand & Utne, 2022, s. 38). Denne definisjonen vil følge denne studien ettersom det er et begrep som forklarer hvordan organisasjoner bør drive med cybersikkerhet. Det vil også bli brukt som en terminologi forståelse relatert til oppgavens studie.

Ifølge Aven (2011) defineres sårbarhet som: «Manifestasjon av systemets iboende tilstander som kan utsettes for en naturlig fare eller utnyttes til å påvirke systemet negativt» (Aven, 2011, s. 505). Det finnes 3 ulike deler sårbarheter kan deles opp ifølge Rausand og Utne (2022):

Teknologiske sårbarheter	**Organisatoriske sårbarheter**	**Menneskelige sårbarheter**
1. IKT-sårbarheter:	Det settes ikke av nødvendige ressurser til sikkerhet	Svak forståelse av hvor viktig sikkerhet er for virksomheten
Mangelfull tilgangskontroll til IKT-systemene	Manglende måleparametere for sikkerhet	Mangelfull forsiktighet med å oppgi brukernavn og passord
Mangelfull installasjon av sikkerhetsoppdateringer	Mangelfull oversikt over nettverkets oppbygning	Bruk av standardpassord og gjenbruk av passord
Sluttbrukere har administrasjonsrettigheter	Mangelfull kontroll av ansattes bruk og bytting av passord	Ukritisk bruk av sosiale medier i jobben
Manglende bruk av brannmurer	Mangelfulle beredskapsplaner og/ eller øvinger i bruk av disse	Ukritisk åpning av ukjente nettsider
2. Fysiske sårbarheter	Manglende krav til sikkerhetskompetanse	Ukritisk åpning av vedlegg til eposter
Manglende sikring i bygningsskallet, dører,	Mangelfulle rutiner for sikkerhetskopiering	

vinduer og låser mot innbrudd.		
Manglende bruk av alarmsensorer og fjernsynsovervåkning for å avdekke innbrudd	Mangelfull håndheving av forbud om bruk av privat utstyr i jobben.	
Bruk av adgangskort med dårlig sikkerhetsteknologi		

Tabell 1: Sårbarheter (Rausand & Utne, 2022, s. 404).

3.4 Risiko-konseptet

Fordi det finnes ulike forståelser av begrepet risiko vil det her bli presentert de ulike perspektiver som videre grunnlag for oppgavens tema. Vatnelid (2018) beskriver risiko som et begrep som brukes for å beregne hvor sannsynlig det er at en hendelse skjer, og hvilke konsekvenser denne hendelsen kan ha. Hvor sannsynlig det er sier noe om hvor ofte det skjer, og konsekvenser sier noe om resultatet (Vatnelid, 2018, s. 17) Ifølge Aven og Renn (2010) er risiko noe som følger oss hele tiden så lenge man har noe en verdsetter, og dette fører til beslutninger i nærhet av usikkerhet (Aven & Renn, 2010, s. 1). Videre beskriver de at det ikke finnes en felles definisjon eller enighet om hvordan risiko defineres. I risikolitteraturen beskrives det at risiko blir brukt som en begrep om en forventet verdi, en sannsynlighetsfordeling, som usikkerhet og som en hendelse (Aven & Renn, 2010, s. 2). På en annen side blir risiko forstått som en måte å analysere usikre konsekvenser av fremtidens utvikling og endring i samfunnet (Aven & Renn, 2010, s. 2). Aven og Renn diskuterer ulike perspektiver av risiko (Aven, 2008b, 2015; Aven & Renn, 2010). Aven (2015) hevder at det er to veldig ulike definisjoner på risiko i forhold til fagområder. Aven (2015) viser til at ingeniører definerer risiko slik: «Risiko=forventet tap (multiplisert med sannsynlighet)» (Aven, 2015, s. 41). Den andre definisjonen fra et økonomiperspektiv er: «Risiko= usikkerhet rundt forventningsverdien» (Aven, 2015, s. 41).

Aven (2015) beskriver hvordan det har blitt en økt allmennforståelse av at risiko er mer enn forventningsverdier, og det har også endret seg i ingeniørmiljøene, som viser til at risiko er mer en kombinasjon av mulige konsekvenser og sannsynlighetene det medfører. Ved endring i perspektivene til ingeniørmiljøene, viser det til at skillene mellom perspektivene til økonomene og ingeniørene blir mindre. Derimot handler det mer om forventningen av en

hendelse for økonomene, hvilket betyr at de ulike perspektivene likevel er forskjellige (Aven, 2015, s. 41). En litt mer generell definisjon fra Aven og Renn (2015) fra det økonomiske perspektivet er: «Risiko er kombinasjon av konsekvensene C av aktiviteten og tilhørende usikkerhet U (Vi vet ikke hva C vil bli)» (Aven, 2015, s. 42).

Ifølge Aven (2015) er det to hovedkomponenter knyttet til risiko ved en aktivitet:

1) Konsekvensene av aktiviteten.

2) Usikkerhet om disse - hva vil konsekvensene bli.

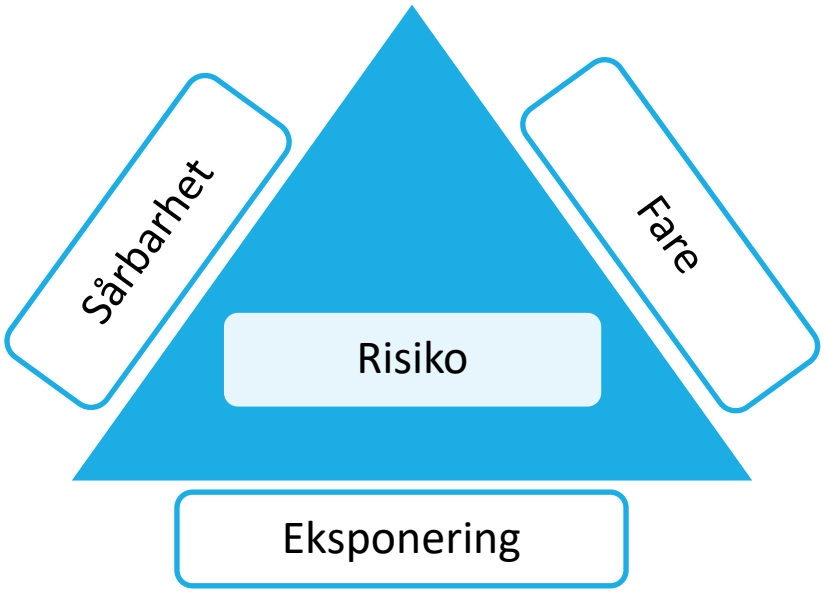
Dette er to komponenter som til sammen utgjør risiko (Aven, 2015, s. 42). Sannsynlighet kommer inn i det overnevnte bilde i forhold til hvor stor risikoen er (Aven, 2015, s. 42). En enda mer generell definisjon på risiko beskrives av Aven & Renn (2010) som:

«Risiko referer til usikkerheten om og alvorligheten av hendelser og konsekvenser (eller resultater) av en aktivitet med hensyn til det mennesker verdsetter» (Aven & Renn, 2010, s. 3)

Disse definisjonene viser likheter i den forstand at risiko i litteraturen beskrives som forventet verdi, sannsynlighet av distribusjon og som en usikkerhet og hendelse (Aven & Renn, 2010). Engen, Kruke, Lindøe, Olsen, Olsen og Pettersen (2016) beskriver at risiko «er hvordan hendelser (som kan eller kunne ha skjedd) påvirker det samfunnet vi lever i, og hvordan bestemte handlinger kan endre forløpet av en hendelse» (Engen, Kruke, Lindøe, Olsen, Olsen & Pettersen, s. 79). Definisjonene forteller oss at det er et forhold mellom mulige hendelser og valgte hendelser (Engen et al., 2016, s. 79). Pritchard (2015) beskriver et tradisjonelt syn, der risiko handler om en hendelse som kan oppstå og at hvor ofte denne hendelsen oppstår er basert på sannsynlighet av tidligere hendelser og miljøhensyn (Pritchard, 2015, s. 7). Utover dette viser studien til Pritchard (2015) at risiko kan være en følelse av hvor stor en sannsynlighet er i forhold til at en hendelse oppstår. Usikkerheten er imidlertid at denne sannsynligheten er ukjent (Pritchard, 2015, s. 7).

Til tross for at risiko ikke er det samme som risikopersepsjon (som vil bli presentert senere i oppgaven) krever det vurdering å bestemme risiko (Pritchard, 2015). For eksempel; selv om det er liten sannsynlighet for at noe vil skje, kan konsekvensene bli katastrofale dersom det skjer. Å reise med fly illustrerer dette; sannsynligheten for en flystyrt er liten, men konsekvensene i tilfelle et krasj er store. Selv om mange mennesker er ukomfortable med å fly på grunn av konsekvensene ved en ulykke, ser ikke de fleste på det å fly som en høy risiko (Pritchard, 2015, s. 6, 7). Dette eksempelet understreker også prinsippet om at risiko i stor

grad avhenger av individuell oppfatning (Pritchard, 2015, s. 7). Forståelsen av en gitt risiko er sammensatt av tre grunnleggende elementer; hendelsen, sannsynligheten og alvorlighetsgraden (eller virkningen). Hendelsen er beskrivelsen av risikoen slik den kan oppstå (Pritchard, 2015, s. 7). Sannsynligheten for og virkningen av en flyulykke fra en høyde på 30 000 fot kan være katastrofale hvis det først skjer (Pritchard, 2015, s. 7).



Figur nr. 4: Risikotrekanten (Crichton, 2008, s. 122).

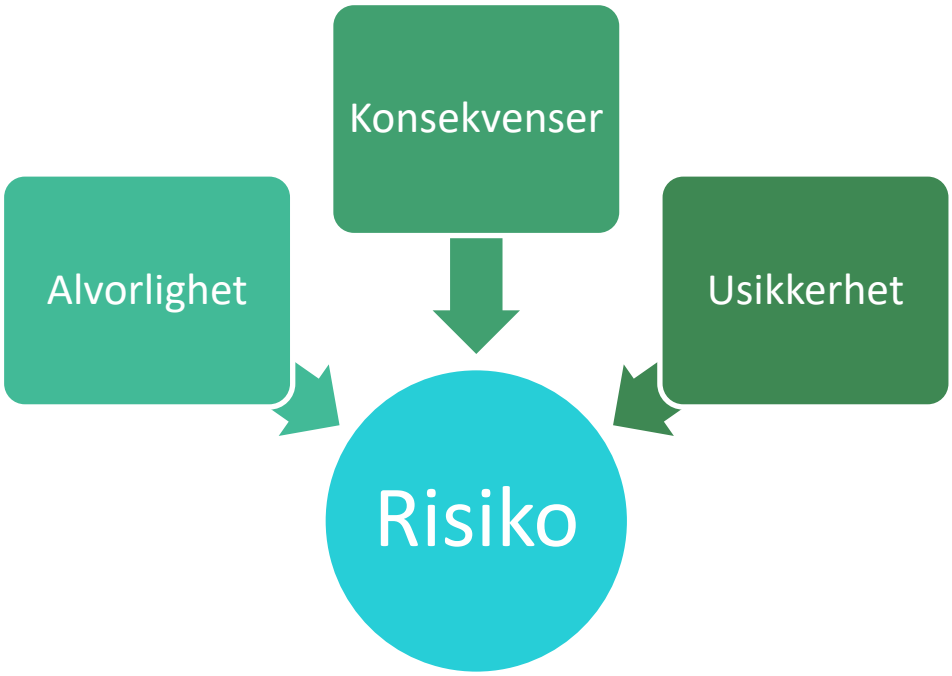
Crichton (2008) har laget en modell for å beskrive et perspektiv på risiko. Ifølge Crichton (2008) kan risiko forklares ved en modell kalt risikotrekanten som vist ovenfor. Crichton (2008) beskriver hvordan man ikke lenger kan bruke tidligere hendelser for å forutsi risiko (Crichton, 2008, s. 122, 123). Årsaken er at samfunnet og klimaet stadig er i endring. En vil dermed ikke kunne beregne risiko basert på tidligere hendelser fordi man kan ikke forutse at disse hendelsene skjer, og at utfallet er det samme som før (Crichton, 2008, s. 122, 123). De ulike sidene som vist i figuren ovenfor er: eksponering, fare og sårbarhet, og det vil være unødvendig å analysere hver av disse fordi de endrer seg på forskjellige måter. Arealet i trekanten representerer risiko (Crichton, 2008, s. 122, 123). Crichton (2008) hevder at hvis en av disse sidene mangler vil det ikke være noen risiko.

Crichton (2008) beskriver hvordan risiko kan reduseres ved å se på hver og en av sidene på trekanten og finne de mest kostnadseffektive tiltakene som kan gjennomføres for å redusere

risikoen. Et eksempel på dette kan være å redusere sårbarheter i systemer, som for eksempel jevnlig oppdatering av sikkerhetssystemene. Sårbarheten vil dermed bli redusert, og ifølge modellen vil risikoen ikke være der eller mindre grad av risiko (Crichton, 2008, s. 122, 123). For individer uten kompetanse vil hvor ofte en hendelse oppstår og alvorlighetsgrad vanligvis være forbundet med fare. Det kan være f.eks. hvor lett man blir smittet av en sykdom og hvor alvorlig sykdommen kan være (Crichton, 2008, s. 122, 123). Risikotrekanten er basert på flere definisjoner, det vil her bli presentert en definisjon som forklarer risikotrekanten: «Risiko avhenger av fare, sårbarhet og eksponering. Hvis noen av disse elementene mangler er det ingen risiko» (Crichton, 2002, s. 126)

Videre vil denne oppgaven basere seg på perspektivet til Aven & Renn (2010, 2015) ettersom de fokuserer mer på usikkerhet, sannsynlighet og konsekvenser som vises i figuren nedenfor. Figur 5 viser hvilke aspekter som er viktige i måten å forstå begrepet på. Risikokonseptet til Aven og Renn er det som blir brukt videre i oppgaven fordi innenfor cybersikkerhet kan konsekvensene av angrep være store og dermed er det viktig å få med hvordan konsekvenser og sannsynlighet påvirker hvordan mennesker forstår risiko. På bakgrunn av dette vil definisjonen brukt for denne oppgaven være:

«Risiko referer til usikkerheten om og alvorligheten av hendelser og konsekvenser (eller resultater) av en aktivitet med hensyn til det mennesker verdsetter» (Aven & Renn, 2010, s. 3).



Figur 5 : Risiko (Aven & Renn, 2010).

3.5 Risikopersepsjon:

Vatnelid (2018) skiller mellom subjektiv risiko og objektiv risiko om måten mennesker forstår risiko. Subjektiv handler om hvordan mennesker selv opplever risiko, mens objektiv er ofte basert på statistikk (Vatnelid, 2018, s. 19). Ifølge Vatnelid (2018) er risiko forstått ulikt som følge av opplevelser, personlig kontroll samt kunnskap om sannsynlighet og konsekvens. I tillegg mener Vatnelid (2018) at måten risiko forstås på har mye med tidsperspektivet å gjøre, som for eksempel at risikoen verden opplever med skade av naturen og store konsekvenser, men det er lenge til det vil skje (Vatnelid, 2018, s. 19-20). Ifølge Aven og Renn (2010) er forståelsen av risiko når individer selv vurderer risiko som inkluderer personlige og sosiale egenskaper, opplevd personlig kontroll og om man har erfaring med risikosituasjonen (Aven & Renn, 2010, s. 10). Enklere sagt, hvordan folk flest opplever, forstår og håndterer risiko og farer er risikopersepsjon (Njå, Sommer, Rake & Braut, 2020, s. 44-45). For at organisasjoner skal redusere risiko, er det viktig at de forstår hvordan mennesker sosialt eller kulturelt skaper sin egen risikoforståelse (Njå et al., 2020, s. 44-45). Videre forklarer Njå et al., (2020) at risikoopplevelse påvirker strategier for akseptabel sikkerhet, som for eksempel kan et individ velger å drikke alkohol, selv om det har vist til skadelige helseeffekter, så lenge en selv tar valget om risikoen.

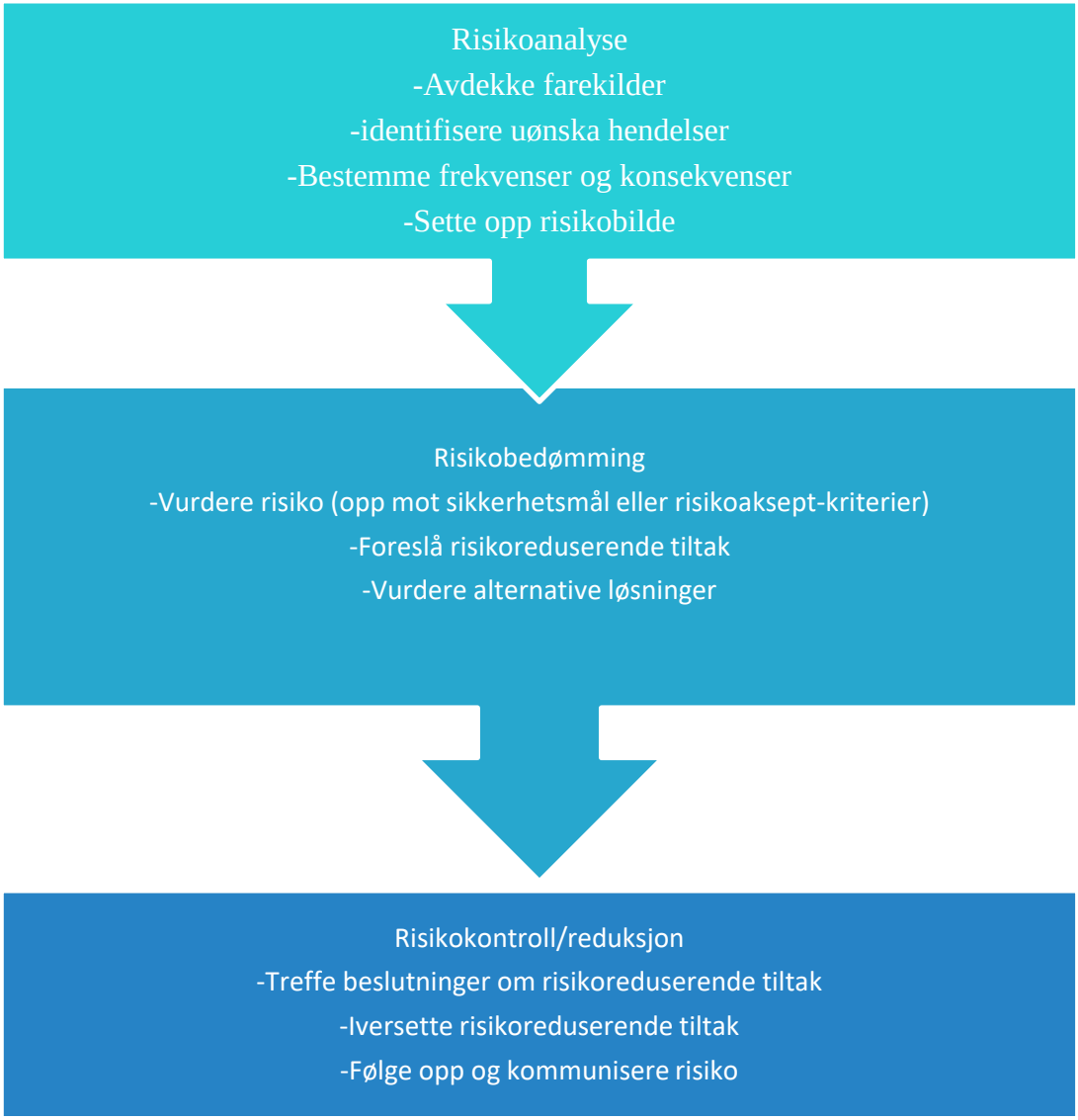
Ifølge Sjoberg (2000) er risikopersepsjon et fenomen for å søke etter forklaring og fenomenet er vanskelig å forstå. I studien kommer det frem at flere faktorer påvirker risikopersepsjon (Sjoberg, 2000). I kulturell teori om risikopersepsjon forklares det som en refleksjon av den sosiale situasjonen et individ befinner seg i (Sjoberg, 2000). Pidgeon (1998) oppdaget at studier i samfunnsvitenskap om risikopersepsjon har vist hvordan risiko ikke bare handler om sannsynligheten for at en hendelse skal inntreffe, men mot et rammeverk for å forstå hvordan risikoer representeres og kommuniseres, og hvordan det er innrammet i sosiale prosesser har mye å bety for forståelsen av risiko (Pidgeon, 1998). Det psykometriske paradigmet ble utviklet av Paul Slovic på 1960-tallet, og blir fremdeles brukt for å beskrive hvordan mennesker forstår risiko på ulike måter (Slovic, Fischhoff & Lichtenstein, 2005). Slovic, Fischhoff og Lichtenstein (2005) mener paradigmet beskriver hvorfor denne forståelsen er forskjellig mellom eksperter, lekfolk og mellom ulike sosiale og kulturelle grupperinger. Grunnlaget i denne modellen er at individer subjektivt definerer risiko. Modellen viser hvordan mennesker ofte blir påvirket av kulturelle, organisatoriske, psykologiske og samfunnsmessige faktorer når en skal bestemme om det er en risiko. Den utpeker hvordan individer er villige til å akseptere risiko hvis de har kontroll på hendelsen de blir utsatt for,

istedenfor å bli utsatt for risiko der man ikke har kontroll. Det er også rikelig med begrunnelser på at selv om vitenskap og teknologi viser hva som utgjør risiko, er det likevel individer som subjektivt definerer risiko (Slovic et al., 2005).

Douglas og Wildavsky (1987) beskriver hvordan risikopersepsjon handler om hvordan mennesker utfører handlinger innenfor visse sosiale grupper, dermed bagatelliserer enkelte risikoer og vektlegger andre som et middel til å opprettholde og kontrollere gruppen (Douglas & Wildavsky, 1987, referert i Slovic, 1987, s. 281). For å kunne forstå hvordan individer tolker og reagerer på farer vil det være viktig å forstå hvordan offentlig risiko-forståelse er og hvilke prosesser som er viktige for hvordan individer forstår risiko (Knuth, Kehl, Hulse & Schmidt, 2014). I undersøkelsen til Knuth et al., (2014) blir det undersøkt om tidligere erfaring med fare påvirker måten individer ser på risiko i forhold til andre farer. Studien viser til at når individer opplever en type fare, øker det et individs opplevelse av risiko for denne faren og for andre farer (Knuth et al., 2014). Et eksempel på dette kan være hvis et individ opplever å bli utsatt for en bilulykke, påvirker dette på hvordan de ser denne risikoen, og de kan også ende opp med å se på det å kjøre båt som en større fare. Den overnevnte teorien om risikopersepsjon blir brukt videre i studien for å se om fenomenet påvirker arbeidet med cybersikkerhet i kommunene.

3.6 Risikostyring:

Risikostyring er ifølge Richard E. Chase (2015) : «implementering av retningslinjer og prosedyrer, for å overføre eller redusere identifiserte risikoer som ikke kan aksepteres av organisasjonen» (Chase, 2015, s. 28). Chase (2015) hevder at risikoovervåkning bidrar til å påvirke risikostyring, og bør derfor påvirke – direkte eller indirekte – driften og målene til sikkerhetsfunksjonen. Risikostyring vil dermed bety blant annet hvordan styret identifiserer og prioriterer risiko systematisk (Chase, 2015, s. 28). Rausand og Utne (2022) beskriver risikostyring som: «Risikostyring er en kontinuerlig ledelsesprosess som identifiserer, analyserer og bedømmer mulige risikoforhold i et system eller i en virksomhet og finner fram til og iverksetter tiltak som kan redusere mulige skadevirkninger» (Rausand & Utne, 2022, s. 93). Videre omfatter risikostyring både god virksomhetsledelse og det deles inn i tre aktiviteter: Risikoanalyse, risikobedømming og risikohåndtering/risikoreduksjon som vist i modellen nedenfor (Rausand & Utne, 2022, s. 93, 94) I likhet med dette har Aven (2015) en klar og tydelig definisjon på risikostyring som er relevant for denne studien: «Med risikostyring forstås alle tiltak og aktiviteter som gjøres for å styre risiko» (Aven, 2015, s. 13).



Figur nr. 6: Risikostyringsprosessen (Rausand & Utne, 2022, s. 6).

Presentert over i modellen er det flere deler i en risikostyringsprosess. Det som vises er at det skilles mellom risikoanalyse og risikobedømming, der disse to sammenlignes for å se hvordan farene man står ovenfor går opp mot målene og dermed mot det en bedrift ser på som akseptabel risiko (Rausand & Utne, 2022, s. 6). Vurderer man disse opp mot hverandre og muligens innfører risikoreduserende tiltak og fortsetter med å overvåke risikoen, foretas det en risikostyring (Rausand & Utne, 2022, s. 6). Njå (2020) beskriver risikostyring som en prosess der det brukes virkemidler for å kontrollere en risiko. Kunnskaper om risiko blir ofte veid opp mot andre relevante forhold som økonomi eller samfunnsmessige forhold (Njå et al., 2020, s. 22). Aven (2015) fremhever at risikostyring handler om innsikt i risikoforhold,

effekt av tiltak, grad av styrbarhet av risiko er noe av det risikostyring. Metoder, prosesser og strategier er viktig for å kunne kartlegge og styre risikoene (Aven, 2015, s. 13).

Aven og Renn (2012) definerer risikostyring «som et verktøy for å håndtere risiko ved å bruke resultatene til risikovurderingsprosessen» (Aven & Renn, 2012, s. 1563). Årsaken til at organisasjoner gjennomfører risikostyring er at de skal sikre den riktige balansen mellom utvikling av og skapelse av ideer, samt å unngå ulykker, skader og tap. Denne prosessen innebærer blant annet risikoanalyse (Aven, 2015, s. 14, 15). Rausand og Utne (2022) forklarer at risikoanalyse er en analytisk metode for å avdekke og vurdere hvilke uønskede hendelser som kan føre til skade på det som er verdi, alt fra mennesker, til miljø eller andre verdier som settes pris på (Rausand & Utne, 2022, s. 95)

I prosessen av risikostyringen omfatter det at situasjonen skal kartlegges og lage problemformulering, målformuleringer og sikkerhet (Aven, 2015, s. 13). Det gjelder å søke etter alternative løsninger som kan utføres for å oppnå mål, analyser og utredninger av disse løsningsalternativene for å se hvordan de kommer ut når det gjelder målene som er satt, og i forhold til hverandre, samt valg og gjennomføring av løsning (Aven, 2015, s. 13, 14). Det vil også være med tilbakemeldinger ved gjennomføring, evaluerings- og læringsprosesser (Aven, 2015, s. 13, 14).

Når man utfører risikostyring er det to viktige prinsipper som må forstås. Disse er Forsiktighetsprinsippet og føre-var-prinsippet (Aven, 2015, s. 103). «En grunnleggende norm eller regel innen risikostyring er forsiktighetsprinsippet som sier at forsiktighet skal være et rådende prinsipp når det er usikkerhet knyttet til hva som blir konsekvensene (utfallene)» (Aven, 2015, s. 103). Forsiktighetsprinsippet handler om at når det kommer til en risiko der konsekvensene er usikkert, skal forsiktighetsprinsipp være det man tar valg etter. Det betyr at når det er usikkerhet om hvor store konsekvensene kan bli av å ikke være forberedt på et cyberangrep, skal man likevel velge å bruke passord på datamaskinene, og ta valg etter forsiktighetsprinsippet (Aven, 2006, 2008a, 2015).

«Føre var-prinsippet er et prinsipp som innebærer at tiltak skal iverksettes, eller at en ikke skal gjennomføre en aktivitet dersom det er betydelig vitenskapelig usikkerhet (uvitenhet) knyttet til konsekvensene av aktivitetene, og disse konsekvensene anses som alvorlige.» (Aven, 2015, s. 104). Føre-var-prinsippet inneholder hvordan man skal ta hensyn til usikkerhet når det kommer til valg organisasjoner tar (Aven, 2006, s. 202). Prinsippet handler om en måte å håndtere usikkerhet i møte med valg som skal tas om hendelser som kan få

veldig alvorlige konsekvenser. Prinsippet er vanskelig å bruke, spesielt i møte med hvordan risiko forstås, men prinsippet kan brukes i møte med vitenskapelig usikkerhet, derav skal man ikke utføre en aktivitet dersom det er betydelig vitenskapelig usikkerhet tilknyttet til det (Aven, 2006, s. 202-203; 2008a).

3.7 Beredskap

Dersom en alvorlig situasjon eller ulykke inntreffer, betyr beredskap at man skal være forberedt og klar til innsats (Rausand & Utne, 2022, s. 42). På bakgrunn av denne studien, vil Rausand og Utne (2022) sin definisjon bli brukt for å gjennomgående diskutere beredskap i forhold til cybersikkerhet i kommunene:

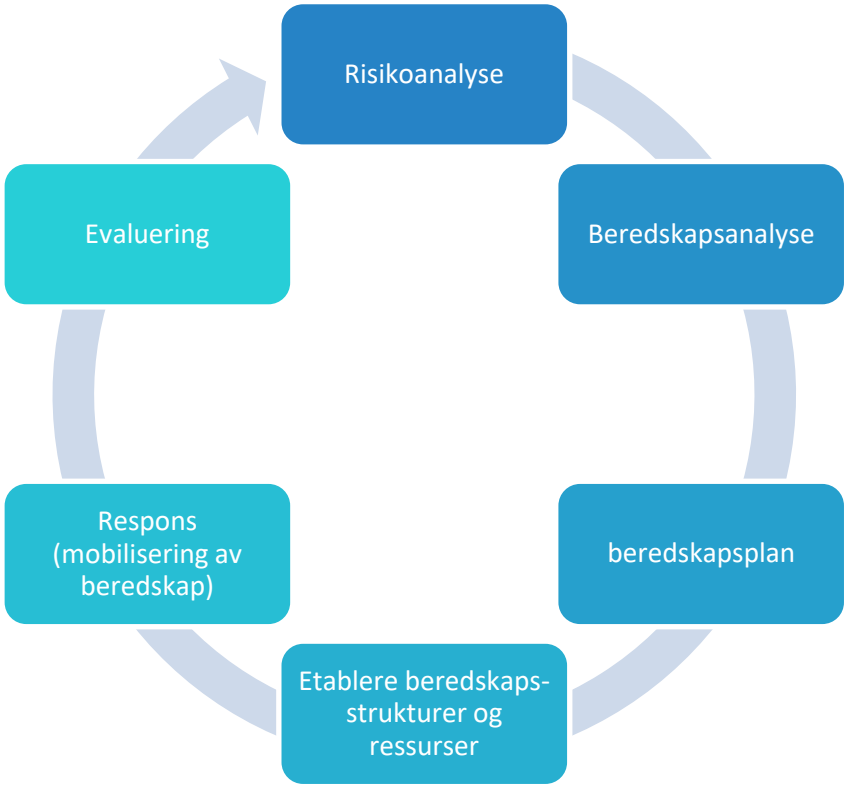
«Planlagte og forberedte tekniske, operasjonelle og organisatoriske tiltak som kan iverksettes under ledelse av beredskapsorganisasjonen hvis det inntreffer uønska hendelser, slik at konsekvensene blir minst mulig» (Rausand & Utne, 2022, s. 42).

I studien til Mehiriz og Gosselin (2016) viser det seg at flere kommuner har god beredskap når det kommer til uvær. Derimot viste det seg at kommunene som hadde mangelfull eller svak beredskap for uvær var mindre forberedt på å håndtere uvær (Mehiriz & Gosselin, 2016). Ettersom beredskap handler om å redusere eller håndtere skadevirkninger som ulykker kan føre til, vil en velfungerende beredskap gjøre at man er forberedt hvis en ulykke skulle skje (Rausand & Utne, 2022, s. 42). Hensikten med beredskap er å kunne enten avvikle ulykker eller redusere konsekvensene av en ulykke (Rausand & Utne, 2022, s. 42). Ifølge Rausand og Utne (2022) vil det være viktig å ha beredskap for ulike typer ulykker, og det bør planlegges for som følge av en risikoanalyse og resultatene presentert der. Studien til Mehiriz og Gosselin (2016) viser også at når det er høy risiko for vær-relaterte ulykker, påvirker det hvor god beredskap kommunene har for denne risikoen.

Njå, Sommer, Rake og Braut (2020) beskriver at beredskap omfatter både tekniske, organisatoriske og operasjonelle tiltak. Hensikten med disse tiltakene er å hindre at en faresituasjon utvikler seg til en ulykkessituasjon, eller så skal tiltakene hindre eller redusere mulige skader av ulykker som har oppstått (Njå et al., 2020, s. 262). Njå et al. (2022) definerer beredskap som:

«Alle tiltak som skal bidra til å hindre at farlige situasjoner får utvikle seg til ulykker, eller tiltak som skal redusere konsekvensene av inntrufne ulykkeshendelser» (Njå et al., 2020, s. 53).

Engen et al., (2016) presenterer en teori på hvordan beredskap bør foregå, og det er fire faser som inngår i disse. Den første fasen handler om starten av beredskapsplanleggingen og er presentert av Perry og Lindell (2003): I den første fasen er det veldig viktig å ha nøyaktig kunnskap om trusselen en organisasjon står ovenfor og hva som kan være sannsynlige menneskelige reaksjoner (Perry & Lindell, 2003). For å få nøyaktig kunnskap om trusselen, er det viktig med en grundig farevurdering og en sårbarhetsanalyse (Perry & Lindell, 2003). I den andre fasen av beredskap kreves det å lage en ramme for hvilke hendelser som det bør bli laget beredskap for, i tillegg tilpasse størrelse av beredskap for disse hendelsene (Engen et al., 2016, s. 280). Fase tre i en beredskapsplan er at det skal bli dokumentert beredskapen som det blir etablert for, som betyr utstyr som behøves, organisering og ressurser. Det blir gjort på bakgrunn av analyser gjort i forkant (Engen et al., 2016, s. 280). Den siste delen av de fire fasene handler om relevant trening og øving, samt mobilisering i krisesituasjoner. Det kan gi grunnlag for evaluering av beredskapen som er etablert (Engen et al., 2016, s. 280). Engen et al., (2016) fremhever at beredskap handler om å etablere ressurser og fullmakter som kan benyttes for å håndtere ulike uønskede hendelser (Engen et al., 2016, s. 280).



Figur 7: Faser i beredskapsarbeid (Engen et al., 2016, s. 284)

Framstilt i figur 7 ovenfor, viser at det er flere faser i beredskapsarbeidet. Først og fremst i beredskapsfasene er det viktig med etablering av akseptkriterier for ulike risikoer organisasjoner står ovenfor, samt vil det å gjennomføre risikoanalyser være grunnleggende for å etablere kunnskap om trusler man står ovenfor, og kartlegge samt beskrive risikoen (Engen et al., 2016, s. 283).

I en virksomhet er det som kalles akseptkriterier det som er akseptabelt risikonivå for en risiko organisasjonen står ovenfor. For å beskrive risiko bruker man en systematisk prosess, risikoanalyse. I prosessen av en risikoanalyse, tas det utgangspunkt i noen identifiserte farer eller trusler for så å gjennomføre årsaks- og konsekvensanalyser av disse og etablere et risikobilde (Engen et al., 2016, s. 284). I en årsaksanalyse blir det analysert og identifisert mulige årsaker til at uønskede hendelser oppstår, og vurdere sannsynligheten for at det skjer. Konsekvensanalyse handler om at det gjøres en gjennomgang av mulige konsekvenser som en uønsket hendelse kan medføre (Engen et al., 2016, s. 284).

Risikoanalysen bidrar med et viktig grunnlag videre til beredskapsanalysen, og det er identifikasjon av farer eller trusler, som hjelper til å etablere et register over utvalgte uønskede hendelser som man skal bygge beredskap for å håndtere (Engen et al., 2016, s. 283, 284). I en beredskapsanalyse er det registrert ulike uønskede hendelser (definerte fare- og ulykkessituasjoner) av ulikt omfang og størrelse. Det beredskapsanalysen og risikoanalysen skal resultere i er en oversikt over aktuelle farer som organisasjoner skal forberede seg på å håndtere, de skal resultere i å si noe om ressursbehovene i forbindelse med beredskap (Engen et al., 2016, s. 283, 284). Det neste steget som vises i modellen ovenfor i figur 6 er respons. I denne prosessen vil det etableres kunnskap om tilgjengelige ressurser til beredskap i organisasjonen. I den siste fasen som vist i modellen kalt evaluering skal det tas lærdom av de virkelige hendelsene som finner sted eller som man trener og øver på. Lærdommen her brukes videre til oppdatering av analysene, dokumentasjon og øvelser (Engen et al., 2016, s. 284).

3.8 Ledelsesforankring

Det er flere ulike studier hvor det henvises til ledelsesforankring for at det forebyggende sikkerhetsarbeidet skal kunne fungere. Det gjelder også i forbindelse med flere andre temaer hvor organisasjoner har hatt suksess, som for eksempel innenfor ulike prosjekter. Den samme teorien vil bli brukt som bakgrunn for studiens tema for å se om arbeidet med cybersikkerhet blir påvirket av ledelsesforankring. Temaet om ledelsesforankring kommer tydelig frem i studien utført av Uchendu, Nurse, Bada og Furnell (2021). I studien hevdes det at den mest

diskuterte faktoren for å opprettholde en positiv sikkerhetskultur er ledelsesforankring. Det var 34 studier gjennom de 10 siste årene som nevnte viktigheten av ledelse og forventninger av ledelsen for å sikre at en organisasjon er i forkant når det gjelder sikkerhet, og dens kultur (Uchendu, Nurse, Bada & Furnell, 2021). Videre formidles det i studien at toppledelsens støtte har dukket opp konsekvent gjennom en tiårsperiode av dokumentene som er blitt gjennomgått (Uchendu et al., 2021). Uchendu et al., (2021) diskuterer flere årsaker på hvorfor det er viktig at ledelsen gir støtte i arbeidet med en god cybersikkerhetskultur. Da disse årsakene er; uten støtte fra ledelsen vil sikkerhets-initiativer kanskje ikke virke viktige for ansatte i forhold til deres daglige oppgaver. Det er med støtte fra ledelsen at det blir satset mot kultur for cybersikkerhet, men også for å sikre at ressursene administreres riktig (Uchendu et al., 2021). Ma, Liu, Appolloni og Liu (2021) beskriver hvordan toppledelsen har en rolle i å støtte miljøvennlige tiltak. Det formidles videre: for at en organisasjon skal bli mer miljøvennlig er det viktig med ledelsesforankring og toppledere har mulighet til å påvirke holdninger til ansatte gjennom øvelser. Ledelsesforankring er den viktigste funksjonen for praksisen i organisasjonsmiljøet (Ma, Liu, Appolloni & Liu, 2021).

Aven (2008a) mener at for å ha suksessfull risikostyring er det viktig med ledelsesforankring, og det betyr at toppledelsen er involvert i prosessene (Aven, 2008a). Von Soms og Von Solms (2006) beskriver hvordan styringen av informasjon bør foregå ved hjelp av en modell. I styringen blir det strategiske nivået forstått som det viktigste i forhold til hvilke mål organisasjonen har. Det er styret som er ansvarlige for sikkerheten og det er deres ansvar å kommunisere hvor viktig det er med beskyttelse av informasjonen i organisasjonen. I tillegg på det strategiske inkludere hvordan IT har en rolle og hvordan IT sin strategi passer organisasjonens strategi (von Solms & von Solms, 2006).

Kankanhalli, Teo, Tan & Wei (2003) har gjennomført en studie angående informasjonssikkerhet, det ser ut til toppledelsens støtte er positivt relatert til forebyggende innsats i informasjonssikkerhet i organisasjonen. Funn i studien tyder på at toppledelsens støtte ofte resulterer i riktig fordeling av ressurser, som gjør det blir lettere å satse på viktig forebyggende programvarer innenfor informasjonssikkerhet. Ettersom det er en tydelig positiv effekt på det forebyggende informasjonssikkerhets-arbeidet med ledelsesforankring, hevder Kankanhalli et al., (2003) at organisasjoner med svak ledelsesforankring kan forsøke å tilføre dette i arbeidet med informasjonssikkerhet (Kankanhalli, Teo, Tan & Wei, 2003, s. 151). Thong, Yap og Raman (1996) mener det er viktig med toppledelsens støtte for å påvirke effektiviteten av informasjonssikkerhet, i tillegg kan toppledelsen gi ressursene som trengs for

prosjekter for å forbedre informasjonssikkerheten (Thong, Yap & Raman, 1996). Hagen (2009) henvist i Skotnes (2015) definerer informasjonssikkerhet som hovedsak et ledelsesansvar. Videre formidles det at informasjonssikkerhet bør være i alle ledelsesprosesser (Hagen, 2009, referert i Skotnes, 2015). Knapp, Franklin Morris, Marshall og Byrd (2009) forteller i sin studie at hvis ikke informasjonssikkerhet blir styrt av ledelsen kan føre til dårligere utvikling av sikkerhet og det kan føre til redusert organisasjonssikkerhet, det viser også til at uten toppledelsens støtte virker ikke alle sikkerhetstiltak viktige, med mindre ledelse synes de er viktige (Knapp, Franklin Morris, Marshall & Byrd, 2009).

I casestudien til Armenia et al., (2019) presenteres det som viktig at sikkerhet forankres i ledelsen. Det gjelder spesielt når det handler om å identifisere farer, er fokuset fra toppledelse viktig for å forstå miljøet organisasjonen handler innenfor. Toppledelsen skal også definere det som er prioritet for organisasjonens oppdrag og styring av cybersikkerhet. Det som inngår i styring er policyer, prosedyrer og prosesser og må være forstått av ledelsen for at det skal kunne styres (Armenia et al., 2019). Digdir (2022) beskriver hvordan det er virksomhetens leder som skal etablere styring og kontroll i virksomheten. I tillegg blir det nevnt at en leder i en virksomhet har en rolle som innebærer at nødvendige etableringsaktiviteter blir utført i arbeidet med informasjonssikkerhet, og følge opp rutiner og se at tiltak som er implementert fungerer (Digitaliseringsdirektoratet, 2022). I artikkelen til Young og Poon (2013) som omhandler prosjekter, viser det tydelig at ledelsesforankring er betydelig viktig for et prosjekts suksess. Det viser til at ledelsesforankring av prosjekter er viktigere for suksess enn tradisjonell praksis (Young & Poon, 2013).

3.9 Kultur i organisasjoner

Reason's (1997) teori handler om hvordan organisasjoner kan administrere eller regulere risikoer ved utfordrende teknologi. I teorien blir det prøvd å identifisere generelle prinsipper og verktøy som er anvendelige for alle organisasjoner som står overfor farer av en eller annen art (Reason, 1997). Blant samfunnsvitere er det uenighet om kultur er noe en organisasjon 'har' eller om det er noe organisasjonen 'er' (Reason, 1997, s. 192). Det førstnevnte perspektivet baserer seg på at det er ledelsens makt som kan føre til endring av kultur gjennom tiltak og praksis, mens det sistnevnte ser på kultur som noe som kommer ut av organisasjonens verdier, overbevisninger og ideologier (Reason, 1997, s. 192-194) Kultur vil bli brukt som en terminologi forståelse for temaer som blir brukt videre i oppgaven.

For å forklare sikkerhetskultur, starter Reason (1997) med å forklare begrepet organisatorisk kultur, for å forstå hvordan det får plass i en sikkerhetskultur og hvordan den kan bygges. En organisatorisk kultur ifølge Reason (1997): «Delte verdier (hva som er viktig) og tro (hvordan ting fungerer) som samhandler med en organisasjons strukturer og kontrollsystemer for å produsere atferdsnormer (måten vi gjør ting på her)» (Reason, 1997, s. 192). Ifølge Bellot (2011) viser tidligere forskning at det ikke er en felles definisjon på en organisatorisk kultur. Organisatorisk kultur er sosialt konstruert, og det oppstår når mennesker samhandler (Bellot, 2011, s. 36)

3.10 Sikkerhetskultur

Ifølge Reason (1997) er sikkerhetskultur noe som kan utvikles sosialt ved å identifisere ulike deler som er viktige for en fungerende helhet (Reason, 1997, s. 191-192). I Reason's (1997) teori blir det beskrevet hvordan en sikkerhetskultur ikke er noe som oppstår tilfeldig etter en katastrofal ulykke, men det oppstår gradvis. Å lage en sikkerhetskultur er en prosess med kollektiv læring og det består ikke av en enhet, men en rekke samkjørte elementer, som forbedrer sikkerheten (Reason, 1997, s. 191, 192). Reasons (1997) teori hevder at det er fire kritiske delkomponenter av en sikkerhetskultur. Disse er; en rapporteringskultur, en rettferdig kultur, en fleksibel kultur og en læringskultur. De skal sammen utgjøre en informert kultur som tilsvarende er en sikkerhetskultur, med formål om å begrense organisatoriske ulykker (Reason, 1997, s. 195). For at det skal kunne skje, er det viktig å lage et sikkerhetsinformasjonssystem som samler inn og analyserer hendelser som kan bli til en ulykke. I tillegg er det viktig å kommunisere informasjon om sikkerhet og regelmessige kontroller av viktige systemer (Reason, 1997, s. 194-196). Det er avgjørende at de som drifter eller bestemmer over systemene har kunnskap om menneskelige, tekniske og miljømessige faktorer som kan ha betydning for sikkerheten som helhet (Reason, 1997, s. 194-196). Reasons definisjon på sikkerhetskultur vil bli brukt videre i oppgaven:

> Sikkerhetskulturen i en organisasjon er et produkt av individuelle og gruppeverdier, holdninger, kompetanser og atferdsmønstre som bestemmer forpliktelsen til, og ferdigheten til, en organisasjons helse- og sikkerhetsprogrammer. Organisasjoner med en positiv sikkerhetskultur er preget av kommunikasjon basert på gjensidig tillit, felles oppfatninger om hvor viktig sikkerhet er, og av tillit til effektiviteten av forebyggende tiltak (Reason, 1997, s. 194).

I en ideell sikkerhetskultur fortsettes det å drive organisasjonen mot målet om maksimal sikkerhetsledelse uavhengig av lederens personlighet eller aktuelle utfordringer for organisasjonen (Reason, 1997, s. 195). Hollnagel (2014) beskriver hvordan en god sikkerhetskultur kan føre til bedre sikkerhet i organisasjonen (Hollnagel, 2014, s. 87). Choudry, Fang og Mohamed (2007) oppdaget at en positiv sikkerhetskultur innebærer fem deler. Først beskrives det hvordan ledelsens forpliktelse er viktig for sikkerhetskulturen. Det at ledelsen bryr seg om ansatte, at det er gjensidig tillit og troverdighet mellom dem og kontinuerlig overvåking av systemer og korrigerende atferd. Videre beskrives det hvor viktig det er å arbeide mot å forbedre arbeidsstedet til enhver tid (Choudhry, Fang & Mohamed, 2007, s. 1005). På bakgrunn av studiens kontekst, vil denne teorien bli brukt videre for å diskutere «cybersikkerhetskulturen» i kommunene.

3.10.1 Rapporteringskultur

Videre hevder Reason (1997) at en rapporteringskultur avhenger av at hvert sikkerhetsinformasjonssystem har villig deltakelse fra ansatte til å rapportere om brudd på sikkerheten, altså menneskene som er i direkte kontakt med farer. I et organisasjonsklima er mennesker forberedt på å rapportere feil og nesten-ulykker (Reason, 1997, s. 195-197). Det betyr at om en hendelse oppstår, som f.eks. det blir klikket på en lenke på PC-en uten med vilje, skal dette rapporteres til sikkerhetsansvarlige. I tillegg vil en organisasjon med effektiv rapporteringskultur ha oversikt over hvordan de håndterer skyld og straff (Reason, 1997, s. 195-197).

3.10.2 Fleksibel kultur

I en fleksibel kultur handler det om at organisasjonen kan skifte fra hierarkisk styring under en krise til en flatere struktur, der kontrollen overføres til individer som er eksperter på temaet, og deretter tilbake til hierarkisk styring når en nødsituasjon er over (Reason, 1997, s. 195). Dette er en vesentlig tilpasningsevne for en kriseforberedt organisasjon og avhenger av gjensidig respekt mellom ansatte (Reason, 1997, s. 195). Gjensidig respekt handler om at man i dette tilfellet har respekt for arbeiderne sine ferdigheter, erfaringer og evner (Reason, 1997, s. 195). En fleksibel kultur betyr også å ha en kultur som er i stand til å effektivt tilpasse seg krav som endrer seg (Reason, 1997, s. 214).

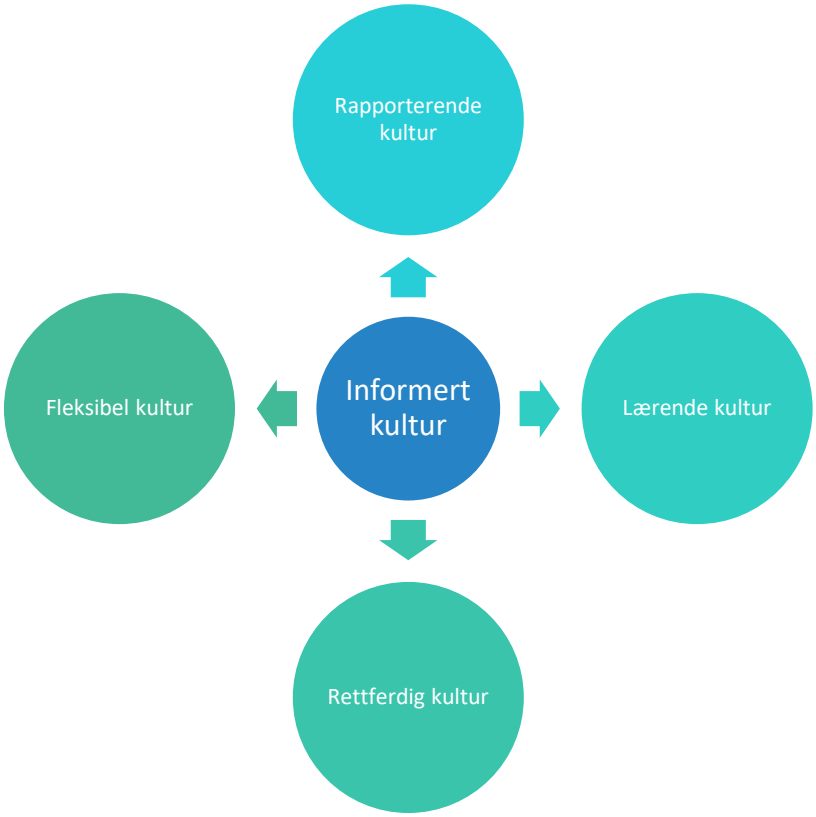
3.10.3 Rettferdig kultur

Ifølge Reason (1997) er en rettferdig kultur vanskelig å oppnå. I en organisasjon er der det likevel er en tro på at rettferdighet vil skje innenfor rimelighetens grenser. Det finnes noen

prinsipper i en rettferdig kultur. Disse er prinsippene om akseptable og uakseptable handlinger (Reason, 1997, s. 205). Prinsippene innebærer at man ikke skal straffe alle feil eller handlinger som ikke har vært utført etter sikkerhetsprinsipper. Dette skal gjelde uansett hvor alvorlig faren viser seg å være. Det er heller ikke riktig at man ikke skal gi sanksjoner til handlinger som kan føre til ulykker (Reason, 1997, s. 204-206). For organisasjoner er det en utfordring å skille mellom «dårlig oppførsel» og usikre hendelser. Det er likevel i flere tilfeller ikke hensiktsmessig å tilskrive noen skyld. Dermed er det en forutsetning for en rettferdig kultur å kunne skille mellom akseptable og uakseptable handlinger (Reason, 1997, s. 204-206). Det betyr likevel ikke at alle handlinger som er ikke akseptable skal straffes, for det kan føre til at ansatte i organisasjonen ikke ønsker eller våger å si ifra om avvik. Derfor finnes det ulike tiltak som eksempelvis anonymisering i rapporter der det meldes om avvik som er blitt utført (Reason, 1997, s. 205). Hollnagel (2014) beskriver også hvordan en rettferdig kultur handler om hvordan det er viktig med tillit i organisasjonen, slik at ansatte blir belønnet for å rapportere sikkerhetsrelatert informasjon.

3.10.4 Læringskultur

Læringskultur er den viktigste kulturen organisasjonen bør ha for å få en god sikkerhetskultur. Det skal være vilje og kompetanse til å trekke de riktige konklusjonene fra sikkerhetsinformasjonssystemet, og vilje til å gjennomføre store reformer når behovet oppstår (Reason, 1997, s. 195). Nedenfor i figur 8 vises det hvordan de fire ulike kulturene til sammen utgjør en informert kultur som er en sikkerhetskultur.



Figur 8: Sikkerhetskultur (Reason, 1997).

3.11 Oppsummering av teorikapittelet

Denne studien tar for seg hvordan kommuner arbeider med cybersikkerhet og om hendelser fører til endring. De ulike teoriene som har blitt presentert er et rammeverk for hva som skal brukes for å diskutere med empirien som blir samlet inn. Først har det blitt fremvist forskning på temaet for å vise hva lignende studier er kommet frem til og for å se om det er likhet eller ulikhet i forhold til empirien.

Etterfølgende blir det presentert teori om begrepet cybersikkerhet og hvordan det oppfattes ulikt. Her blir det presentert ulike definisjoner og forståelser, men definisjonen til Von Solms og Van Niekerk er det som blitt brukt som begrep videre i oppgaven. Denne definisjonen handler om å sikre funksjoner i cyberrommet, som gjelder både individer, organisasjoner eller nasjoner. I tillegg blir det fremvist hvordan begrepet skiller seg fra lignende begreper som IKT-sikkerhet og informasjonssikkerhet. Det blir også beskrevet litt om hva som er viktig i arbeidet med cybersikkerhet.

Sårbarheter blir presentert som følge av at det er en terminologiforståelse for oppgavens temaer. Her har det blitt presentert en definisjon på sårbarheter i teknologi av Rausand og Utne som handler om hvordan et system vil få problemer når det oppstår en uønsket hendelse

for å gjenoppta etter en prosess. Det blir også vist frem ulike tekniske, organisatoriske og menneskelige sårbarheter for å vise eksempler. Dette gir et grunnlag for det som diskuteres videre i oppgaven.

Det blir presentert ulike perspektiver på risiko. Disse perspektivene hjelper oss å forstå fenomenet risiko, og hva som legges i begrepet når det er snakk om risiko og hvordan fenomenet påvirker kommunens arbeid med cybersikkerhet. Aven presenterer ulike sider ved perspektivet der hovedtemaene usikkerhet og alvorlighet om hendelser og konsekvenser. Risikopersepsjon er ulike måter å se på risiko. I teorien har det blitt presentert ulike måter man forstår risiko på.

Etterfølgende ble risikostyring fremvist. Risikostyring handler å identifisere risikoen en organisasjon står ovenfor, for å deretter følge en prosess for å redusere eller kontrollere risiko. Det vil også bli presentert forsiktighetsprinsippet og føre-var-prinsippet. Dette er presentert for å forstå hvordan risikostyring av cybersikkerhet er i kommunene.

I teorien om beredskap fortelles det av Rausand og Utne hvordan man når alvorlige situasjoner eller hendelser oppstår bør ha beredskap for å være forberedt. Videre blir det presentert beredskapsprosessen som består av flere faser av Engen et al. Det vil dermed bli relevant videre i oppgaven for å se om det er likheter med kommunens arbeid med beredskap i forhold til cybersikkerhet.

Teorien om ledelsesforankring handler om at det ofte i prosesser ved sikkerhet eller generelt temaer som kommer opp bør ledelsesforankres for at det skal prioriteres i hele organisasjonen.

Teorien om kultur av Reason har blitt vist frem som en terminologiforståelse som brukes videre i oppgaven for å forklare en sikkerhetskultur.

Til sist i teorikapittelet har det blitt beskrevet teori om sikkerhetskultur. Hovedsakelig fra perspektivet til Reason (1997) hvor han beskriver fire ulike kulturer som til sammen utgjør en informert kultur, tilsvarende en sikkerhetskultur.

4.0 Metode

I denne studien har jeg valgt å se på arbeidet med cybersikkerhet i norske kommuner, og om angrepet på Østre Toten har ført til endringer. Jeg bestemte meg for å bruke en fortolkende studie hvilket er en kvalitativ metode. Det vil i dette kapittelet bli redegjort for valgene jeg har tatt underveis. Forskningsprosessen som er blitt utført i denne studien vil bli fremvist fra start til slutt. I tillegg beskrives valgene som ble gjort og hvorfor disse ble tatt. Til slutt fremstilles svakheter og styrker med valgt metode og studiens kvalitet.

4.1 Valg av metode

Formålet med studien er å se på hvordan arbeidet med cybersikkerhet i norske kommuner utføres, og om angrepet på Østre Toten har ført til endringer. Studien pågikk fra september 2021 til mai 2022. For å kunne fordype meg i temaet og forstå hvordan kommuner arbeidet med cybersikkerhet, valgte jeg kvalitativ metode. Ettersom jeg ønsket å gå i dybden på temaet om arbeidet med cybersikkerhet i kommunene, er kvalitativ metode egnet for dette (Tjora, 2017, s. 28). Innenfor den kvalitative metoden ble det utført dybdeintervjuer. Ved å utføre dybdeintervju får man informantenes tanker, erfaringer og opplevelser, som kan bidra med å gi forståelse av arbeidet med cybersikkerhet i kommunen. Dette mener jeg vil hjelpe å få en mer forståelse for hvordan tilstanden har vært i kommuner før angrepet på Østre Toten, hvordan det har ført til endringer og hvorfor forholdene er som de er i kommunene. Metoden ble valgt på bakgrunn av problemstillingen som er egnet for å gå i dybden på fenomenet.

I denne studien har jeg tilrettelagt for å få en forståelse av kommunens arbeid med cybersikkerhet, og om det på bakgrunn av angrepet på Østre Toten har blitt en endring i kommunene. Denne metoden vil bli brukt som et hjelpemiddel for å forstå hvordan virkeligheten til informantene er og hvordan de opplever arbeidet med cybersikkerhet i kommunene (Jacobsen, 2015, s. 21).

4.2 Kvalitative dybdeintervjuer

Årsaken til at kvalitative dybdeintervjuer ble valgt som metode var for å finne ut av hvordan de som drifter det tekniske for kommunen opplever arbeidet med cybersikkerhet. For å finne ut hvordan kommunene arbeidet med cybersikkerhet var det viktig at informantene kunne snakke i en relativt fri samtale. Hensikten med intervjuene var å gå innom noen spesifikke tema som jeg lagte på forhånd i intervjuguiden (Tjora, 2017, s. 113). Dybdeintervju ble valgt for å få kjennskap til informantenes virkelighet, og å forstå hvordan de opplever arbeidet med

cybersikkerhet i kommunene, ettersom det er noe de arbeider med daglig (Tjora, 2017, s. 114).

Intervjuene varte mellom 45- 90 minutter, og ble gjennomført via Teams. Intervjuguiden besto av åpne temaer med stikkord som kunne brukes for å få mer innsikt hvis informantene skulle stå fast, eller hvis jeg som forsker gikk tom for oppfølgingsspørsmål. Intervjuguide er en oversikt over hvilke temaer vi skal innom i løpet av intervjuet (Jacobsen, 2015, s. 150). Ved å velge semistrukturerte dybdeintervju kunne informantene gå i dybden om temaer som jeg ikke hadde nevnt tidligere, men hadde likevel en liste over temaer som skulle tas opp. Semistrukturert betyr at intervjuet har en halvfast struktur (Tjora, 2017, s. 264). Årsaken til valget var for å finne ut om det fantes noen underliggende temaer som forelå i kommunens arbeid med cybersikkerhet som en utforskende undersøkelse. Intervjuguiden hjalp meg likevel til å komme innom de samme temaene med de ulike informantene, for at det skulle kunne være rammer rundt det som skulle diskuteres i forhold til oppgavens problemstilling. Samtidig sikrer dette at vi kom inn på de viktige temaene som jeg ønsket å belyse (Jacobsen, 2015, s. 150). Derimot vil en negativ konsekvens kunne bli at noe av det informantene snakker om ikke er sammenlignbart, ettersom det muligens kun forekommer i en av kommunene.

4.3 Utvalg og presentasjon av informanter

Som følge av at denne studien er kvalitativ, ble det valgt informanter som kan uttale seg reflektert om det temaet jeg studerer (Tjora, 2017, s. 130). Dermed ble det valgt et strategisk utvalg basert på informanter med visse egenskaper for denne studien. Informantene som ble valgt var personer som var egnet til å snakke om temaet cybersikkerhet, og har kunnskap om prosessene og kunnskap om emnet. Utvalget besto dermed av informanter som arbeider med informasjonssikkerhet, en form for leder i IKT-avdeling eller IKT- leder. Informantene arbeider for drift av IKT-avdelingen til kommunen, enten det var innad i kommunen eller «outsourcet». Disse informantene ble strategisk utvalgt fordi de kan noe om hvordan kommunene arbeider med cybersikkerhet, og kan derfor uttale seg om temaene (Thagaard, 2018, s. 54; Tjora, 2017, s. 130).

Rekruttering av informanter ble gjort via snøballmetoden og tilgjengelighetsutvalg. Det var på bakgrunn av at jeg fikk et navn av veilederen min som kunne hjelpe meg med å finne flere informanter. Snøballmetoden handler om å starte med kontakter en har, for å så få tips til nye informanter (Tjora, 2017, s. 135). Ved å velge denne rekrutteringsprosessen står man ovenfor

noen etiske retningslinjer fordi de informantene som blir gitt informasjon om, ikke har samtykket til at informasjonen om dem blir delt med forsker (Thagaard, 2018, s. 57). På bakgrunn av de opplysningene som kom frem fra andre informanter er det likevel grunner til at denne informasjonen var mulig å finne ut av ved å bruke kommunene sine nettsider. Under kapittelet om etiske refleksjoner vil det bli diskutert mer grundig.

I utvalget ønsket jeg å få variasjon med tanke på geografi og størrelse på kommunene, derfor prøvde jeg å finne informanter fra flere steder i Norge. Ettersom jeg brukte rekruttering hovedsakelig fra snøballmetoden var de fleste av intervjuobjektene fra Øst i Norge. Heldigvis ble det etter hvert som oppgaven skred frem, tilgjengeliggjort objekter fra andre steder i landet som Midt-Norge og noen fra Nord-Norge. Etter hvert fikk jeg også informanter fra Sør-Norge, og til slutt Vest-Norge.

Noe som er viktig å tenke på ved utvalgets størrelse er tid og ressurser (Thagaard, 2018, s. 59). I utgangspunktet hadde jeg planlagt å intervjue opp mot 15 informanter for å få forståelse for fenomenet. Da intervjuene ble gjennomført merket jeg likevel at jeg havnet på det som heter et «metningspunkt». Det betyr at informasjonen som kommer frem blant informantene synes ikke å gi mer informasjon om temaet som jeg ikke hadde hørt gjennom de andre intervjuene (Thagaard, 2018, s. 59). Dette merket jeg underveis i perioden jeg intervjuet og stoppet etter 10 informanter. Informantene kom innom de fleste sakene, uten at jeg trengte å spørre om alle temaene jeg hadde i intervjuguiden, noe som førte til en relativ fri samtale hvor jeg i flere tilfeller kun trengte å stille oppfølgingsspørsmål. Nedenfor i tabell 2 viser det en oversikt over informantene, hvor de var fra i Norge og om de arbeidet innen ekstern eller intern IKT-avdeling.

Informant	**Intern vs. Ekstern**
1	Nord-Norge, intern
2	Midt-Norge, intern
3	Midt-Norge intern
4	Midt-Norge, intern
5	Midt-Norge, ekstern
6	Vest, ekstern
7	Vest, ekstern
8	Sør, internt
9	Vest, internt

10	Vest, intern

Tabell 2: Oversikt over informanter

4.4 Forberedelser og gjennomføring av intervjuer

Forberedelsene gikk ut på å undersøke feltet som handlet om cybersikkerhet og kommuner. Det var for å kunne forstå hva som var gjort tidligere på området. Dermed fant jeg relevant forskning som fikk meg til å tenke videre på interessante tema, og kom frem til en interessant problemstilling. Deretter gikk jeg i gang med planlegging av intervjuguide og hvilke temaer som skulle med. I utformingen av intervjuguide benyttet jeg meg av å se på tidligere intervjuguider som var laget innenfor samme tema for å få inspirasjon. Dette ga meg en veldig strukturert intervjuguide først, men ettersom jeg ønsket at informantene skulle få muligheten til å snakke om temaer jeg ikke hadde nevnt, ville en semistrukturert intervjuguide passe bedre. På bakgrunn av dette laget jeg en semistrukturert intervjuguide, hvor jeg benyttet meg av temaer som jeg ville gjennomgå i intervjuene. I tillegg laget jeg stikkord som kunne hjelpe meg og informantene med å komme dypere inn i disse temaene hvis det skulle stoppe opp.

Etter dette gikk jeg i gang med å få tak i informanter. Først og fremst prøvde jeg å kontakte noen via e-post, og fikk en del svar i starten. Med tiden viste det seg at flere ikke svarte på e-postene jeg hadde sendt, og som følge av tid og ressurser så jeg meg nødt til å ringe rundt til informanter. Jeg fikk først en liste med navn via bekjente. Derimot viste det seg at kun tre av individene som sto på listen hadde mulighet til å stille opp på intervju. Blant dem som ikke kunne delta var det noen som ikke hadde tid, ikke svarte på e-posten jeg sendte eller svarte i senere tid da jeg allerede var begynt å analysere det jeg hadde. Jeg så derfor ikke behov for flere informanter også på bakgrunn av at jeg følte jeg hadde nådd et «metningspunkt» som tidligere nevnt. For å få flere informanter sjekket jeg ulike nettsider til ulike kommuner for å se om det lå noen stillingstitler, navn og nummer ute, som jeg kunne kontakte.

De fleste av personene jeg ringte til tok telefonen, men det var også noen få som ikke svarte. Fremdeles hadde ikke alle informantene jeg ringte mulighet til å stille på intervjuet. Årsaken til at flere informanter ikke hadde tid til å stille på intervju var en travel hverdag, noe flere begrunnet med Covid-19 pandemien. Da informantene hadde takket ja, sendte jeg dem informasjonsskriv som jeg hadde laget på forhånd. I informasjonsskrivet sto litt mer om detaljene, og samtykkeskjema. I tillegg ble det presentert litt om hva intervjuene skulle handle om, hvilke rettigheter de hadde og at de kunne trekke seg når som helst om det skulle være ønskelig. Jeg foreslo for informantene at de kunne velge mellom Zoom og Microsoft Teams,

men alle intervjuene ble gjennomført over Microsoft Teams. I forkant av intervjuene ble jeg enig med informantene om tidspunkt, og kunne derfor sende en innkalling på Teams noen dager i forveien. Informantene godtok møteinnkallingen jeg sendte dem på e-post og dermed var tidspunkt avtalt. Intervjuene foregikk for det meste på tomannshånd, men ettersom to av informantene hadde ønske om å ta med en informant til, ble det i to av tilfellene intervjuet to om gangen. Denne formen for intervju går under fokusgruppeintervju (Jacobsen, 2015, s. 159). Ved å ha fokusgruppe kan det få frem hvordan individene har erfart arbeidet med cybersikkerhet i kommunene og hjelpe å utvikle ny kunnskap (Jacobsen, 2015, s. 159, 160). I starten av intervjuene spurte jeg informantene om jeg kunne ta opptak av intervjuene på Teams. Alle informantene godtok opptak, noe som førte til at jeg ikke trengte å skrive veldig mye notater underveis og kunne fokusere på deltakeren for å få en god samtale. I tillegg hjalp det meg senere i transkriberingen for å få frem hva som ble sagt ordrett (Jacobsen, 2015, s. 153).

4.5 Kvalitativ Analyse

Metoden som har blitt brukt i denne studien er fenomenologisk og med tanke på jeg ønsket å få en forståelse i hvordan informantenes opplevelser, benyttet jeg meg av innholdsanalyse. I forskningen forsøkte jeg å forstå meningen i det som ble sagt, og hva det kunne bety for arbeidet med cybersikkerhet i kommunen (Johannessen, Christoffersen & Tufte, 2016, s. 169-171). Innholdsanalysen ble først gjennomført i selve transkriberingen for å holde meg nært stoffet. Det ble benyttet fargekoder som rød, gul og grønn, der rød ble brukt for det som viste seg å være mest relevant for problemstillingen, deretter gul for litt mindre relevant og grønn for det som viste seg å ikke være relevant. Innholdsanalyse ble brukt for å kunne redusere det som ble sagt i intervjuene til færre, men mer meningsfylte kategorier (Jacobsen, 2015, s. 207). Etter jeg hadde benyttet fargekoder for å analysere det som var relevant for problemstillingen, startet jeg å sette koder på disse. Å kode betyr å sette merkelapper eller navn på utsnitt av teksten (Johannessen et al., 2016, s. 171). Koding ble brukt som et verktøy for å organisere meningen av det som ble sagt av informantene (Johannessen et al., 2016, s. 171). Jeg kodet som følge av metoden «In-Vivo» som betyr at jeg brukte ord eller korte setninger fra informantenes eget språk (Miles, Huberman & Saldaña, 2020, s. 65). Hensikten til det var fordi det kunne hjelpe meg å forstå meningen i det som ble sagt og ivareta det spesifikke innholdet (Tjora, 2017, s. 197). Deretter samlet jeg kodene i ulike kategorier. Kategoriene dannet videre ulike temaer, som er gjennomgående og handlet om det samme (Jacobsen, 2015, s. 207).

4.6 Studiens kvalitet

Studiens kvalitet baserer seg på om forskningen er troverdig eller ikke (Thagaard, 2018, s. 181). For å vise at denne studien er troverdig har jeg vært åpen om hele forskningsprosessen fra start til slutt. Dette er for å vise hvordan jeg har kommet frem til resultatene, og for at andre kan vurdere denne prosessen (Thagaard, 2018, s. 181). Det er derfor viktig å ha åpenhet i hele forskningsprosessen. Frem til nå har jeg forklart hvordan jeg har gjennomført forskningsprosessen, valg av metode, analyse og utvalg av informanter. Det vil nå videre bli presentert i hvilken grad studien er troverdig eller ikke. Det vil bli basert på reflektering av studiens gyldighet, pålitelighet, overførbarhet og etiske refleksjoner. Jeg vil også gå innom styrker og svakheter ved valg av denne metoden.

4.7 Styrker og svakheter ved valgt metode

Jacobsen (2015) beskriver hvordan kravet til kvalitative studier handler om forskerens evne til å kunne reflektere rundt samspillet mellom forskningen og de resultatene man presenterer. Refleksivitet er et begrep som innebærer at forskeren prøver å utnytte sin kunnskap om hva som kan skje i for eksempel selve intervjusituasjonen, og forklare hvordan situasjonen preges av at det forskes på (Jacobsen, 2015, s. 246). I denne delen vil det bli presentert hvordan forskningen har ført til de resultatene som jeg har presentert, i tillegg vil jeg forsøke å avdekke og forklare hvordan situasjonen kan ha blitt preget av at den forskes på. I denne forskningsprosessen kan det være en svakhet å bruke strategisk utvelgelse, sett i sammenheng med at informantene hadde ulike stillingstitler og de jobbet enten som driftsorganisasjon for kommunen, eller innad i kommunene. Informantene kan ha ulike virkeligheter i arbeidet med cybersikkerhet, ettersom de har ulike oppgaver. Samtidig vil det kunne føre til at man får et bredere perspektiv, fordi cybersikkerhet omfatter store områder og det vil kunne hjelpe oss å få et mer helhetlig perspektiv på hvordan kommuner arbeider med cybersikkerhet og om angrepet på Østre Toten har ført til endringer. Det vil også kunne bidra til å få ulike perspektiver på temaet. På en annen side vil det å velge strategisk ha ført til at jeg har fått snakket med informanter som kan uttale seg om temaet, noe som er en styrke ved valgt metode.

En annen mulig svakhet med strategisk utvelgelse kan være at jeg kun valgte informanter som kan omtale seg om cybersikkerhet. Cybersikkerhet omfatter hele kommunen, og dermed burde det muligens blitt valgt informanter fra ulike sektorer, som toppledelsen eller beredskapsavdelingen. Det er fordi det var store temaer som ble gjennomgått i intervjuene, og informanter fra ulike sektorer kunne bidratt med å få et helhetlig bilde på cybersikkerhet. På

en annen side er arbeidet med cybersikkerhet komplekst og i flere tilfeller bør IT-avdelingen være involvert i alle prosessene. Derfor vil det være en styrke å bruke strategisk utvalg.

Det vil i tillegg kunne være en styrke å bruke fenomenologisk metode, ettersom det ved intervjusituasjonen alltid er en mulighet for at informantene ikke er åpne nok som følge av lojalitet til sin arbeidsplass eller situasjonen. I så tilfelle vil en fortolkende studie kunne bidra til at man kan forstå mer virkeligheten av og hva det informantene har sagt faktisk betyr.

4.8 Pålitelighet

Pålitelighet eller det som kalles reliabilitet handler om undersøkelsen har skapt de resultatene jeg har kommet frem til (Jacobsen, 2015, s. 241). Pålitelighet vil være med på å vise om de resultatene jeg er kommet frem til er troverdige (Thagaard, 2018, s. 181). For å vise om denne studien er pålitelig er det viktig å diskutere hvordan undersøkelsesopplegget, datainnsamlingen og analysen jeg har utført kan påvirke resultatet (Jacobsen, 2015, s. 241). I undersøkelsen benyttet jeg meg av semistrukturerte dybdeintervju. Ettersom jeg valgte dybdeintervju, vil jeg som forsker kunne ha en intervjueffekt. Dersom tilfellet er at jeg har hatt en intervjuereffekt på informantene, kan det påvirke fenomenet som undersøkes og det er noe som bør diskuteres (Jacobsen, 2015, s. 241, 242).

Jeg har tidligere i metode-kapittelet fremvist metoden og analysen jeg har brukt, for at andre skal kunne kritisk vurdere forskningsprosessen og det at prosjektet er utført på en pålitelig og tillitsvekkende måte. Dette kan vise at forskningen er pålitelig (Thagaard, 2018, s. 187). Likevel vil det i denne metoden ikke være mulig å komme tilbake til samme resultat ved bruk av den samme metoden som jeg har brukt fordi teknologi og samfunnet er stadig i endring, og det kan føre til at holdninger om cybersikkerhet stadig er i endring på grunn av paradigmeskifte (Thagaard, 2018, s. 187-188).

Intervjuene ble gjennomført via Teams. Dette var på grunnlag av at jeg ikke hadde nok ressurser, Covid-19 pandemien og at det virket gunstig for alle parter. Informantene fikk valget om å velge mellom dataprogrammet Teams og Zoom, men alle valgte Teams. Ifølge Jacobsen (2015) er hvor intervjusituasjonen foregår viktig, og kan ha innspill på hva informanten svarer (Jacobsen, 2015, s. 152). I den hensikt vil det å intervjue via Teams føre til at den som blir intervjuet muligens føler seg mer tilpass og dermed mer åpen om synspunktene fordi informantene kunne velge stedet de ble intervjuet på. På en annen side kan det ha ført til at informantene har vært mer påpasselige på hva de fortalte som følge av at de kunne ha vært redde for noen avlyttet og som ikke skulle avlytte samtalen. Dog var temaene

etter min mening ikke sensitive og dermed trenger det likevel ikke å ha vært et problem. I intervjusituasjonen forsøkte jeg å være nysgjerrig, men også åpen og ærlig for å skape tillit til informantene. I tillegg prøvde jeg også å ha et kritisk og åpent blikk på det som ble sagt i intervjuene. Informantene var anonyme i hele forskningsprosjektet, noe som muligens kan ha ført til åpenhet, ettersom det ikke kan gå utover deres kommune eller dem som individer i etterkant av forskningsprosjektet. Jeg opplevde ikke at jeg som forsker hadde påvirkning på hva informantene svarte. Årsaken til det var at jeg lot informantene snakke om det de ville, og trengte kun å nevne temaer før de begynte å beskrive sine perspektiver, som gjorde at opplevelsen min var at de visste hva de snakket om.

På denne måten kunne informantene snakke fritt om hvordan de arbeider med cybersikkerhet, og jeg fikk mulighet til å kunne stille oppfølgingsspørsmål. Det vil likevel være vanskelig å vite hvilken effekt jeg egentlig hadde på deltakerne, ettersom intervjuet gikk over teams og konsekvenser av det kan være en ikke får med seg kroppsspråket på samme måte som man kunne gjort i en tilsvarende situasjon der en møtes. På en annen side opplevde jeg at begreper ble tolket forskjellig, som kan være en av baksidene med å benytte meg av semistrukturerte intervjuer. Når dette skjedde, forsøkte jeg å stille oppfølgingsspørsmål for å få dem mer inn på tema. Jeg opplevde at informantene fortalte deres sannhet og at jeg som intervjuer ikke påvirket svarene.

4.9 Gyldighet

Gyldighet, troverdighet eller det man kaller validitet handler om de tolkninger jeg som forsker kommer frem til (Thagaard, 2018, s. 189). Gyldighet knyttes til om svarene som blir funnet frem til, er svar på det spørsmålet jeg forsøkte å stille under forskningsprosessen (Tjora, 2017, s. 232). Det vil si; om mine fremgangsmåter og funn virkelig reflektert over virkeligheten på en riktig måte (Johannessen et al., 2016, s. 230). Ettersom dette studiet er fortolkende, så kan dette være komplisert (Tjora, 2017, s. 232). Årsaken til at det kan være komplisert å få frem virkeligheten er fordi jeg i denne studien har tolket hva det informantene sier kan bety for arbeidet med cybersikkerhet og endringer etterfulgt av angrepet på Østre Toten. Likevel tolket jeg basert på konkret det informantene har sagt i intervjuene, som viser at studien reflekterer virkeligheten til informantene. I denne studien valgte jeg at informantene skulle være anonyme. Anonymitet innebærer at opplysningene som kommer frem, ikke kan spores tilbake til informantene (Jacobsen, 2015, s. 50). Hensikten til jeg valgte å ha informantene anonyme var at de kan føle at de kan snakke åpent om den virkeligheten som er, uten at informasjonen vil kunne spores tilbake til informantene. Dette kan bidra til åpenhet mellom informant og

intervjuer, fordi det ikke vil kunne spores tilbake til informantene om de forteller noe de føler kan svekke synet man har på kommunen som organisasjon.

Intervjuene ble gjennomført over Teams og det ble tatt opptak av intervjuene. Ettersom det ble tatt opptak og transkribert som følge, kan det være preget av det de faktisk sier, og ikke min tolkning av hva de sier. Det var veldig viktig for meg å være nøyaktig i forskningsprosessen å få frem presis det de mente, og transkriberingen av opptakene kan ha hjulpet med nettopp det. Samtidig som en fortolkende studie handler om meningen bak det informantene forteller i intervjuene (Johannessen et al., 2016, s. 169)

4.10 Overførbarhet

I kvalitativ forskning handler det om å utvikle en forståelse av fenomenet vi studerer (Thagaard, 2018, s. 193). Ekstern gyldighet av forskning handler om i hvilken grad funnene fra en undersøkelse kan generaliseres til andre enn dem man faktisk har undersøkt (Jacobsen, 2015, s. 237). Ettersom det er en kvalitativ studie kan ikke denne studien generaliseres, dette er på grunn av at verden stadig er i endring hvor holdninger og kunnskap endres. Det kan likevel være grunn til å tro at funnene er gyldige i andre kommuner, ettersom kommuner i Norge er organisert likt. På en annen side vil man aldri kunne vite om det er gyldig i andre kommuner, før man sjekker. Med andre ord vil det kunne vise seg å være nyttig for flere kommuner å vurdere om de funnene som er gjort i denne undersøkelsen samsvarer med andre kommuner.

4.11 Etiske refleksjoner

Når det planlegges og gjennomføres prosjekter, er det noen retningslinjer som ligger til grunn. Disse retningslinjene handler om å ha respekt for menneskers privatliv, deres anonymitet og rett til å delta eller ikke delta i prosjektet (Thagaard, 2018, s. 60). I prosjektfasen ble det meldt inn til Norsk senter for forskningsdata (NSD) detaljer om prosjektet og hvordan dette skulle gjennomføres. Hensikten med dette var å vise åpenhet om utfordringer og hvordan de arbeider med cybersikkerhet i kommunene. Derfor var det viktig for studien at informantene skulle være anonyme og at det var etisk korrekt. NSD godkjente prosjektet mitt, i samsvar med at informantene skulle anonymiseres og det at opplysningene om deltakerne skulle behandles konfidensielt. Ifølge forvaltningsloven er all informasjon som kan tilbakeføres til enkeltpersoner taushetsbelagt (Johannessen et al., 2016, s. 90). Siden jeg hadde informasjon om informantene, valgte jeg derfor å beholde informantene anonyme.

I forkant av intervjuene sendte jeg et informasjonsskriv der det sto opplysninger om hva studien skulle handle om, og at informantene skulle være anonyme. I tillegg fikk informantene beskjed om at de når som helst kunne velge å ikke delta i prosjektet. Etter at jeg hadde transkribert intervjuene ble disse anonymisert der jeg lagret det. I etterkant av intervjuene og transkriberingen lot jeg de informantene som ønsket det få lov til å lese gjennom transkriberingen, for at de skulle kunne kommentere om det var noe jeg hadde misforstått eller om de ikke ville delta likevel.

Ved å velge deltagere basert på snøballmetoden, er det noen etiske problemer (Thagaard, 2018, s. 57). Når jeg gikk i gang med å velge informanter fikk jeg først noen navn av bekjente som jeg kunne kontakte for å få informanter. Dette betyr at det har blitt delt informasjon om informantene uten at de selv har samtykket (Thagaard, 2018, s. 56-57). På en side kan dette ha vært etisk ukorrekt fordi individene ikke har ønsket at jeg skal få den informasjonen. På en annen side er det grunner til å tro at det er etisk korrekt, ettersom informasjonen jeg fikk ligger ofte på kommuner sine nettsider.

5.0 Empiri

I denne delen vil det bli fremvist empirien som jeg har samlet inn. Empirien vil presenteres i sammenheng med temaene jeg utviklet i analysen av det som kom frem i intervjuene, derav vil jeg påpeke at noen av funnene glir over i hverandre og nevnes i flere deler. I empirien vil det legges frem det som senere skal diskuteres i forhold til forskningsspørsmålene og teorien. Noen av temaene fra intervjuguiden er ekskludert ettersom jeg fokuserer på temaene som fremsto i analysen. I noen av sitatene vil det ikke bli tatt med hele setninger, ettersom det ikke er relevant for denne oppgaven. Det vil først bli gjennomgått temaet som handler om cybersikkerhet og ledelse før vs. etter angrepet på Østre Toten, deretter beredskap, øvelser, gjenoppretting og planer. I tillegg belyses empirien som handler om sårbarheter, IKT-avdelingens plassering, sikkerhetskultur og IKT-kompetanse, risikoforståelse i kommunen og sikkerhetsarbeidet. Eksempelvis fremheves det de ulike informantene har sagt for å understreke temaene og måten de er sammenlignet på. Til slutt vil det være en oppsummering av funnene.

5.1 Ledelse og Cybersikkerhet

5.1.1 Ledelsesforankring før vs. etter angrep

Angrepet på Østre Toten har vist seg å være viktig for flere av kommunene, ettersom flere beskriver endring av eller hos ledelsen i kommunene (Informant nr. 1, 4, 5, 6, 7, 8, 9 og 10). Den ene kommunen forteller åpent om en hendelse der de ble angrepet, noe som førte til endringer i ledelsen. Informant nr.1 forteller:

> «Så vi har god støtte fra ledelsen, men det har jo noen årsaker og det har det jo fordi vi har konkret vært i en virussituasjon som tvang dem til dette» (Informant nr. 1).

Utover dette kommer det frem i intervjuene at flere av informantene mente at det tidligere handlet om oppetid for ledelsen. Det formidles at det har vært vanskelige valg for ledere, som står ovenfor det å skulle velge en nødvendig sykepleier eller om de skal betale mer for sikkerhet (Informant nr. 4, 5). Informant nr. 4 sier:

> «Men som sagt den skvisen som kommunen sitter i, som å velge mellom sykepleier og lærer og antivirus på elevmaskiner f.eks. det, den er reell» (Informant nr. 4).

Flere av informantene forteller hvordan Østre Toten har ført til en oppvåkning for ledere når det kommer til hvor viktig det er med søkelys på cybersikkerhet. Blant annet fortelles det om hvilke økonomiske konsekvenser det fikk for Østre Toten kommune. Dette var den direkte årsak til at ledelsen forsto at noe måtte gjøres (Informant nr. 4). Informant nr.6 forklarer

hvordan angrepet på Østre Toten har ført til endringer i kommunen, hvor ansatte fra IKT-avdeling har blitt inkludert i styremøter. I likhet med informant nr. 4 var det et «wake-up call» for daværende styreleder. Ledelsen viser nå derfor mye mer interesse enn før forteller informant nr. 6.

Informantene nr. 1, 4, 5, 7, 8, 9 og 10 forteller tydelig at det har vært et oppsving i fokus på cybersikkerhet etterfulgt av angrepet på Østre Toten. Det blir tydeligere bevisstgjøring i toppledelsen, de får flere ressurser, samtidig som det blir mer søkelys på sikkerhetsarbeidet. Informantene forteller at det tidligere var lite fokus på cybersikkerhet, på forskjellige grunnlag. Noen forsto IKT-avdeling som en leverandør og der det var strengere med økonomien. Informant nr.8 forteller:

> «En ting er jo det jeg nevnte med at det har nok blitt sett på veldig mye som en teknisk greie som leverandøren vår ordner opp i. Det er noe de kan. Vi har ikke tekniske ressurser i vår kommune til å jobbe med det og vi har ikke egen drift, egne brannmurer, egne IT-løsninger. Det er det de som driver med, da blir det jo at det er de som har ansvar for det.»

> «(…) var det greit, da kunne en driftsorganisasjon komme inn og hjelpe til, da ville de høre om det. Så det er sånn, du er så avhengig av de hendelsene for at kommunen skal kunne prioritere opp imot sikkerhet. Så det å gå ut og fortelle om en trussel som kan komme, det har liksom nesten ikke noe for seg, fordi de tror ikke det kommer til å skje. Før det smeller da» (Informant nr. 5)

I samsvar med dette nevner også informant nr. 3, nr.6 og nr.10 hvordan ledelsen legger ansvaret for cybersikkerhet over til IKT-avdeling. Årsaken til det er fordi ledelsen ikke har kunnskap eller forståelse for tiltak som må gjøres. Ledelse er ikke klar over risikoen eller bevisste på konsekvensene av et cyberangrep (Informant nr. 3 og 5). Det nevnes også blant flere av informantene at det nå arbeides med å få økt kunnskap og forståelse hos øverste ledelse. (Informant nr. 1 og 5). Informant nr.3 forteller at den overordnede lederen har ikke kompetanse og setter dermed full tillit til IKT-leder i kommunen:

> «Leder har vel egentlig. Uten at vi har snakket om det, full tillit til hva jeg gjør. Jeg har jo ikke tydelige definerte myndigheter per dags dato» (Informant nr. 3).

Informant nr. 3 forteller videre hvordan ledelsen likevel ikke er godt nok bevisste på konsekvensene av dataangrep. Ledelsen har litt forståelse, men velger likevel å ikke prioritere

for eksempel beredskapsplan i forhold til cybersikkerhet. Informant nr. 6 forteller også hvordan ledelsen etter angrepet på Østre Toten snur seg mot IKT-avdeling for hjelp. Også informant nr. 10 forteller hvordan kommunedirektøren kaster ballen over til IKT-avdeling og derved gir ansvaret for cybersikkerhet over til IKT-leder. Når det kommer til å forstå cybersikkerhet, forteller nr.6 at:

> «Sett ifra et sikkerhetsperspektiv så kan man jo stille spørsmål til om de faktisk forstår konsekvenser av å ha så gammel infrastruktur kjørende da. Vi har også en del av skylden for at det ikke har blitt, at erstatning ikke har kommet på luften tidligere. Men de er bevisste rundt det, men forståelsen kan man kanskje stille spørsmål ved» (Informant nr. 6).

I sammenheng med dette forteller informant nr. 8 at ledelsen snakker om at cybersikkerhet er viktig og at de jobber litt med det. Dog er cybersikkerhet likevel så komplisert at de har ikke mulighet til å forstå eller forholde seg til det. Informant nr.9 hevder også at en tror det ikke kan forventes at ledelsen over informant nr.9 har dybdekunnskap i det som går på cyberkriminalitet og cybersikkerhet. Videre i intervjuene viser det seg at flere har engasjerte ledere, av de som er kommunedirektører på nåværende tidspunkt (Informant nr.2, 7, 9, 10). De forteller hvordan ledelsen er engasjert, de får fokus fra ledelsen og skjønner at ting må endres og gjøres. Informant nr. 10 forteller:

> «Men han rådmannen som vi har nå, han er fast tilsatt nå. Han er ekstremt opptatt av sikkerhet og relevante løsninger. Han har veldig tillit til meg og mine folk som fagpersoner» (Informant nr. 10).

> «Så det må jeg si at han har fokus og han, han ordner penger til oss så vi får gjort det vi ønsker å gjøre. og han forventer at vi leverer det vi får penger til, og det gjør vi også. Hele tiden» (Informant nr. 10).

I samsvar med dette forteller også informant nr.7 som nevnt tidligere at det har blitt gjort endringer etter Østre Toten sitt angrep for å få mer cybersikkerhet på plass. Det blir også nevnt hvordan ledelsen er med på at det skal gjøres endringer, og det er fullt mulig å forankre flere sikkerhetsutfordringer opp i ledelsen (Informant nr. 2 og 7). Informantene forteller:

> «(…) så har dette løftet seg betraktelig nå siden mars i år der dette fokuset har blitt helt voldsomt i forhold til både tiltakene vi har gjort, men også fokuset i fra politikerne våre, og ifra administrativ leder, så jeg har veldig tillit til det fokuset og den støtten så

vi har rundt dette og det viser de tiltakene vi måtte gjøre ganske kjapt etterpå» (informant nr.1).

«Så er det jo opp til linjeledere når det kommer til prioriteringer og budsjetteringer og de praktiske tingene, men de støtter det». (Informant nr. 2).

5.2 Beredskap

5.2.1 Øvelser

I intervjuene spurte jeg blant annet om informantene har øvelser i kommunene i forhold til cybersikkerhet. Øvelser på cybersikkerhet viser seg å være ganske nytt tema eller ikke eksisterende blant informantene. Henholdsvis kommenterer både informant nr. 1, 3, 8, 9 og 10 at de ikke har hatt konkrete øvelser som gjelder cybersikkerhet, men at de har kjørt «Phising-mail», informasjon til ansatte om cybersikkerhet og lignende. Informant nr. 3 svarte:

«Vi har aldri hatt noen definerte øvelser nei. Tanken har heller aldri slått meg» (Informant nr. 3).

Det viser seg likevel at flere av informantene planlegger å ha øvelse snarest eller i løpet av førstkommende år. Noen har også nylig hatt øvelser (Informant nr. 2, 4, 5, 6, 7, 9 og 10). Informant nr. 2 er veldig klar på at de ikke har drevet med øvelser, og hvordan dette er noe de kunne blitt bedre på. Tankene som er blant ansatte i kommunen er at de ikke trenger å øve fordi de tar det som det kommer, som fører til ulike bilder på hva man faktisk gjør når en står ovenfor et angrep. Informant nr. 2 forteller blant annet hvorfor de ikke har øvd tidligere, og hvordan dette er en utfordring.

«Fordi at det er fjernt. Det er så veldig mange ting som man ikke rekker i hverdagen, som man blir målt på. Man føler jo på at man ikke har folk nok til å få nesten gitt mat til dem som skal ha mat» (Informant nr. 2).

«Men grunnen til at det ikke blir trenet så mye på er nok rett og slett fordi at det er ikke så mye kultur for det, det er det ene. Og det andre er at man er opptatt av de tingene som man skal levere tjenestene på.» (Informant nr. 2).

Informant nr. 4 forteller også hvordan det å øve på cybersikkerhetshendelser er ganske nytt i kommune-Norge. Det nevnes at kommuner har vært gode på øvelser knyttet til HMS, brann, naturkatastrofer og lignende. Kommuner har vært forskånet for virkeligheten når det gjelder cybersikkerhet i stor grad. Informant nr. 4 forteller:

> «Cyber som på en måte er litt sånn sabotasje og noen som ikke vil deg vel. Og der har kommunen tenkt at alle er glade i kommunen. Vi har ikke noe av verdi, type den ting. Jeg tror det er et fåtall av kommunale virksomheter som faktisk har kjørt øvelser knyttet til Cybersikkerhet» (Informant nr. 4).

Informant nr. 4 sier at de skal for første gang ha øvelser, noe som de tok opp høsten 2021. I tillegg beskriver informant 4 hvordan de har planlagt å ha øvelser hvert år, hvor det er et kommunalt tema, og hvor kanskje krisen starter i kommunene. Tidligere har det vært øvelser, men da av teknisk art og ikke hvor en har øvelser på hele trusselbildet innenfor cybersikkerhet. En interessant side av det å ha øvelse kommer frem da informant 4 forteller:

> «Og det er jo klart at i løpet av den øvelsen så identifiserer man en del ting som vi må gjøre og som kommunen må gjøre og som man må ta stilling til litt på en annen måte» (Informant nr. 4).

En av kommunene gjennomførte nylig en øvelse på cybersikkerhet. Her kom det frem flere avvik som krevde oppfølging i form av tiltak for å hindre avvik (Informant nr. 6). Det var ting som ble oppdaget som man må ta stilling til på en annen måte, som også krevde flere ressurser. Informanten hevder også at det virket som det var flere i kommunen som da fikk økt forståelse. Det kan blant flere nevnes kommunedirektøren, beredskapsansvarlige og ledere for kommunale foretak. Øvelsene fikk de ansatte i kommunen til å innse hvor avhengige de faktisk er av datasystemene sine. Det var en øyeåpner at de skal basere seg på penn og papir den dagen det virkelig slår til (Informant nr. 6).

5.2.2 Gjenoppretting

Gjennom intervjuene kommer det frem at helse er gode på gjenoppretting, og å jobbe uten digitale systemer (Informant nr. 1, 8, 9 og 10). Helse har manuelle rutiner hvor de blant annet skriver ut medisiner og lignende på papir. De er derfor vant til manuelle prosedyrer fordi det handler om liv eller død, forteller informant nr. 1. Informant nr. 10 forteller:

> «Hvis et A-system går ned eller hvis vi får et fiberbrudd da og et b-system går ned så har vi helt klare rutiner på hvordan vi skal få det opp og gå. Og at vi varsler og får i gang manuelle rutiner» (Informant nr. 10).

Det er tanker på hvordan man skal gjenopprette viktige systemer, men ingen tydelig plan på det, nevner informant nr. 2. Informant nr.8 forteller litt om planer på gjenoppretting:

> «Hvis alt nettet går ned både fiber og mobilnett og sånt i et område så har vi større problemer. Vi har ikke fullverdige rutiner der alt skrives ut og ligger i «backup» alltid, for å si det sånn. Det har vi ikke. Men hvis alt nettet er nede samtidig så har vi nok større problemer enn at ikke vi kan lese eposten vår direkte. Da har vi, da er det et eller annet stor naturkatastrofe eller et eller annet som har skjedd» (Informant nr. 8).

5.2.3 Planer og IKT-trusselbilde

Informantene ble spurt om hvordan cybersikkerhet er iverksatt i beredskapsplanene og hvordan cybersikkerhet er et tema. Informantene nr. 1, 3, 6 og 7 forteller at planene de har ikke inkluderer cybersikkerhet eller IKT. Nr.1 hevder likevel på tross av at cybersikkerhet ikke var inkludert i planene, reagerte de ganske bra med den vanlige beredskapsplanen under et cyberangrep kommunen opplevde.

Videre formidler informant nr.1 at grunnen til de ikke har hatt disse beredskapsplanene på plass før er fordi det ikke har vært forankret noen plass, eller vært et tema. Derimot forteller informant nr. 1 at de hadde tydelige planer med kopi av harddisken, noe som førte til at de klarte seg ganske bra under angrepet. Nr.2 forteller derimot at de har en beredskapsplan som innebærer IKT-sikkerhet, men de har ikke hatt tydelig plan på hvordan å gjenopprette etter angrep. Informant nr. 3 fastslår at de har prøvd å få til beredskapsplan som inneholder IKT-trusselbilde, men på grunn av manglende ressurser har det falt fra som tema. Informant nr. 8 mener at IKT avdelingen som drifter for kommunen har planer og rutiner med tanke på beredskapsplanene, men at det er noe som IKT-leder innad i kommunen ikke har kjennskap til. Informant nr.10 sier kommunene de drifter for har cybersikkerhet som tema i beredskapsplanene sine. Felles for flere av kommunene var at de jobber mot å bedre beredskap i kommune. Hvilket betyr at de jobber med implementeringen av IKT-trusselbilde, nyere og bedre planer, og øvelser som innebærer digitale trusler (Informant nr. 1, 4, 5, 6, 7 og 9). Informant nr. 7 hevder:

> «Nei det er vel bare vi jobber i den samme sikkerhetsgjennomgangen så er vi på punktet som gjelder beredskapsarbeidet nå, så vi er, vi har en del og gjøre der og det holder vi på med og, vi har så vidt kommet i gang der, vi kommer til å ha litt mer ekstra fokus, tenke på dataangrep og den delen da» (Informant nr. 7).

> «Til sommeren, når vi tar sommerferie i 2022 så skal vi ha politiske godkjente beredskapsplaner og en overordnet plan over alt dette som ligger godkjent» (Informant nr. 1).

> «For det er jo ikke snakk om, om vi blir angrepet, vi blir angrepet hundrevis av ganger hver uke, så det er jo litt sånn, men når er det angrepet lykkes? Og da må type beredskap være på plass» (Informant nr. 4.)

Når det kommer til fokus på IKT-trusselbilde, har fokuset kun vært blant de som drifter IKT-sikkerhet for kommunen. Dette er en tjeneste kommunen har kjøpt, og dermed faller fokuset litt vekk fra kommunen hevder informant nr. 1. Fokuset på trusselbilde har levd i IKT-avdelingen tidligere, men det har aldri kommet noe lenger opp i organisasjonen eller vært noe tema på ledermøter. Det kan ha gjort at topplederne kanskje ikke har tenkt veldig mye på trusselbildet forteller informanten. I likhet med det hevder også informant nr. 2 at det er kun IKT-avdelingen som i det hele tatt er opptatt av det som kalles trussel-aktører.

Informant nr. 2 opplever at man risiko vurderer, uten å tenke på hva som skjer hvis alt nett er nede. Det blir hevdet av informant nr. 2:

> «Får ikke med meg resten til å gjøre det ferdig noe som heter lokal trusselvurdering. Og det har vi gjort. Det er et dokument vi har for å kommunisere og for å bruke understøtte av andre risikovurderinger. Fordi det er jo helt umulig å risiko-vurdere noe som helst hvis man ikke kjenner trusselbildet egentlig og det trusselbildet som er kjent» (Informant nr. 2)

Når det kommer til planarbeid erkjenner informant nr.1 at det er utrolig hvordan en kommune som deres kan gå så mange år uten at dette var et fokus. Det hevdes at årsaken til at det kan skje er at planarbeid tar mye tid. Det er noe som ikke kommer fort på plass, fordi det er et innviklet hierarki med flere titalls systemer, både store og små. Det er viktig at dette implementeres i fagenhetene, og at alle drar i samme retning for å sy sammen planene og at de blir jobbet med over tid (Informant nr. 1).

5.3 Organisatoriske sårbarheter

Et tema som kom opp blant flere av informantene var at cybersikkerhet var utfordrende på grunn av måten kommunen er organisert. Informantene som enten jobbet som driftsorganisasjon for kommunen eller som jobbet for IKT-avdeling i kommunen, påpekte hvordan plasseringen av IKT avdelingen hadde påvirkning på cybersikkerheten. Det blir spesifikt nevnt i noen av tilfellene hvordan organisasjonen har en IKT-avdeling som blir sett på som adskilt fra kommunen og hvordan dette samarbeidet er en utfordring (Informant nr. 6, 7 og 8). De forklarer med et eksempel på hvordan arbeidet med cybersikkerhet blir en utfordring, da de som IKT-avdeling skal kun ha ansvaret for det tekniske, mens kultur

innenfor cybersikkerhet er opp til resten av organisasjonen. Blant annet kan ikke de som driftsorganisasjon bestemme om det skal gjøres opplæring for ansatte obligatorisk, fordi dette er opp til kommunene selv. Det fortelles også at de som drifter for kommunene ikke alltid kommer så lett igjennom for å få aksept for å foreta seg noe:

> «(…) at de er der, men likevel så får vi ikke alltid aksept for det som kanskje ja, når vi ønsker å foreta oss noe for å fjerne sårbarheter og sånn så er det kanskje ikke, det henger kanskje ikke alltid så godt sammen som vi skulle ønske da» (Informant nr. 7).

Motsatt forteller informant nr. 9 og 10 at de som intern IKT avdeling får mer handlingsrom:

> «Vi er mer fleksible, vi har veldig mye mer handlingsrom for å gjøre ting» (Informant nr. 10).

Informantene trekker frem utfordringer i arbeidet med tilgang og kontroll av systemer (Informant nr. 8, 9 og 10). Det trekkes frem at det er utrolig mange ansatte og det er vanskelig å styre hvem som skal ha tilgang og kontroll på hva. Informant nr. 8 ønsker at flere roller skal være like på tvers av de ulike kommuner:

> «(…) holde vedlike, derfor ønsker de at roller og sånn skal være lik på tvers av kommuner sånn at det er mulig å holde oversikten over hvilke tilganger de forskjellige rollene har» (informant nr. 8).

> «Det vil si at du kan beholde brukeren din i fagprogrammet, og det vil si at du har litt dårlig kontroll på om de har tilgang etter at de har sluttet eller ikke sluttet» (Informant nr. 9).

Informant nr. 10 forteller hvordan de nylig har endret systemene sånn at den datoen ansatte slutter, slettes hele brukeren deres for å sikre at de ikke har videre tilgang på systemer som de ikke skal ha tilgang på. Det blir mye diskutert om hvor komplisert sammensatt en kommune er, organisatorisk. Informantene forteller hvor komplisert det er å lage planer, da det er flere forskjellige sektorer som skal være med og mange ansatte som skal inkluderes i disse planene (Informant nr. 7, 8). Det finnes flere ulike systemer som fører til at det blir vanskelig å ha kontroll og oversikt.

> «Det kommer litt forskjellig gang eller litt spesiell flyt på forskjellige områder der. Det er litt sånn det er organisert. Og føler det også har en del innvirkning på cybersikkerhetsbiten da, det med alle de faktorene rundt her» (Informant nr. 8).

Det er også vanskelig å gjennomføre cybersikkerhet ute i sektorene på grunn av at kompetansen er lav, og kunnskapen er veldig ulik (Informant nr. 4, 5, 7, 8). Informantene beskriver også at det er en utfordring å få leverandører av IKT-systemer til å forholde seg til cybersikkerhet på en god måte. Samarbeidet blir vanskelig, fordi for en leverandør handler det om at de skal levere systemer som fungerer og er sikre, men leverandøren informerer ikke om tilstanden rundt cybersikkerhet og hvordan de jobber med dette. Kommunikasjonen mellom sikkerhet og hva som gjøres innenfor dette området er komplisert, og kommunen og IKT-avdelingen fremstår som to separate organisasjoner. Dermed blir kommunene nødt til å stille høyere krav til leverandørene hevdes det av en informant. Informant nr. 3 sier:

> «Vi får jo heller ikke tilbakemeldinger om at sikkerhetsarbeidet som gjøres hos leverandørene våre, vi må jo i relevante anledninger prøve å spørre litt» (Informant nr. 3).

Hovedoppfatningen jeg satt igjen med etter intervjuene var at IT-avdelingen var litt adskilt fra kommunen, dermed blir det ikke samarbeid i cybersikkerhetsarbeidet med resten av kommunen. De overlater cybersikkerhet til IT-avdelingen og ansvaret blir deres. En kommune nevnte at ansatte i utgangspunktet ikke spør IT-avdelingen om sikkerhet (Informant nr. 4).

> «Og dessverre så er vel tilstanden i kommune- Norge at de spør ikke IKT-avdeling om sikkerhet sånn i utgangspunktet. Så vi har tvunget oss litt inn» (Informant nr. 4).

Informant nr. 2 forteller om hvordan de nylig har gjort en internkontroll på vann og avløp. Driftskontrollsystemene har de stålkontroll på, men når det ble spurt hva de hadde gjort med risikovurderinger opp mot de sårbarhetene som var i datasystemene, fikk informant nr. 2 en kopi av en epost fra 2018 hvor IKT- driftssjef hadde vært på befaring hos dem for å se hvor serveren var plassert og så hadde de en dialog om dette. Kommentaren var at risikovurderinger er noe IKT-avdeling skal ta seg av. Deretter var de ferdige med internkontrollen. Det fører dermed til at de som arbeider med vann og avløp ikke bruker ressurser på cybersikkerhet da de tenker at IKT-avdeling har kontroll. Informanten forteller at IKT-avdeling kan risikovurdere og at de kan lage antivirus program på serveren på vannverket og holde denne oppdatert samt sørge for at kommunikasjon ikke går rett ut på internett. Det er uansett utfordringer på cybersikkerhet som avdelingen likevel ikke håndterer (Informant nr. 2).

Andre utfordringer i kommunens arbeid med cybersikkerhet handlet om ressurser. Informantene forteller hvordan kommunene har anstrengt økonomi og hvordan dette fører til utfordringer i arbeidet med cybersikkerhet (nr. 2, 3, 4, 6, 9 og 10). Informant nr. 5 sier:

> «(…), men det er jo litt sånn i kommune Norge, det er penger som rår. Og det er mange hatter på enkeltpersoner» (Informant nr.5).

Informantene beskriver hvordan det var enklere å få mer tilgang på ressurser og økonomiske bidrag til å drive med forbedringer på cybersikkerhet etter angrepet på Østre Toten (Informant nr. 1, 2, 3 og 4). Informant nr. 2 forteller også hvordan IKT avdelingen ikke får penger til systemer som er lovpålagt og sørger for oversikt. Informant nr. 3 forteller om hvorfor de ikke har beredskapsplan som innebærer cybersikkerhet som tema:

> «Så dette dreier seg egentlig om ressurser, om å ha penger og tid til å sette seg ned med de tingene her og vi har veldig flinke folk her hos oss som kunne laget de her rapportene, men det dreier seg faktisk om tiden vår» (Informant nr.3).

5.4 IKT-avdelingens plassering

Et tema som var interessant som flere av informantene kommer innpå er hvor IKT/IT-avdelingen bør plasseres og hvilke fordeler eller ulemper det er å ha IKT-avdeling internt i kommunen eller som en ekstern avdeling som drifter for kommunen. Informant nr. 1 som IKT-leder i sin kommune forklarer:

> «Men det er utrolig effektivt at jeg sitter og hører på hva skolesjefen, helse og sosial sjefene har som utfordringer, det blir en status for få det helhetlige blikket av organisasjonen vår» (Informant nr. 1).

> «Fordi vi ser at i den prosessen vi har nå og, er informasjon, kommunikasjon og ikt en strategisk greie som må etableres så høyt opp som mulig» (Informant nr. 1).

Selv om informant 1 mente at det fra strategisk smart å ha IKT-avdeling så høyt opp som mulig i organisasjonen, var det likevel grunner til å ikke ha all kompetansen innad i kommunen. Årsaken til dette er at det hevdes at en får bedre kompetanse ved å ha IKT-avdelinger i fagmiljøer. De får da et utstrakt samarbeid og deler erfaringer med driftsorganisasjoner eksternt. I tillegg til dette mente informant nr. 1: skal man ha kompetansen innad, er det veldig viktig å ha folk som kan det og som jobber hele tiden for å utvikle seg innenfor IKT-arbeidet. Videre formidler informanten hvordan det å ha IKT-avdeling strategisk plassert i kommunen, hjelper dem å ha tett kontakt med politisk ledelse og

ikke minst en oversiktlig organisasjon der de får raskt på plass de kritiske ressursene de trenger for å kunne ta det et hakk videre. Informant nr. 6 forteller også hvordan kommunen har endret på organiseringen etter angrepet på Østre Toten. IKT leder har nå blitt invitert med i styremøter sammen med toppledelsen, noe som ikke var forholdet før:

> «(…) har jo vært med inn i styremøtet flere ganger og orientert for en tiltaksplan met antall punkt som skal utbedres» (Informant nr. 6).

På den andre siden forteller informantene nr. 8, 9 og 10 om hvordan de mener det er flere forhold som viser til at det er viktig å ha kunnskapen internt. De mener derfor at det har flere fordeler å ha en intern avdeling enn å ha den eksternt. Nr. 8 forteller:

> «Hadde vi hatt mer ressurser lokalt, hadde vi satt nærmere, og da ville jo kommunedirektøren vært kanskje mer informert om hva som skjer på dette området, enn det er nå når det er noen eksterne som driver på med den tekniske biten av det. Men det er vanskelig å ha det internt fordi man får ikke tak i nok gode fagfolk. Det ville kanskje blitt tatt bedre hånd om, nå er det bare noe som gjøres i tillegg til alt annet» (Informant nr. 8).

> «Det må jo være nærhet til brukerne og bestiller-kompetanse. Når vi for mange år siden så var jo dette med «outsourcing» veldig hipt og ja, alle erfaringene i fra den tiden når det skjedde var jo at når de dro ut hele IKT- avdelingen så mistet de noe fordi de hadde ikke igjen bestiller-kompetansen tilbake i kommunen, så det er jo den hvis vi skulle ha gjort det så måtte vi allikevel satt med mennesker internt» (Informant nr. 9).

5.5 Sikkerhetskultur og IKT-kompetanse

Flere av informantene opplyste om hvordan ansatte som jobber i kommunen ikke har kunnskap når det kommer til cybersikkerhet (nr. 3, 5, 6, 7, 8 og 9). Utfordringer er at det er vanskelig å drive med opplæring av ansatte. Årsaken til det er fordi det er veldig ulik bakgrunn og kunnskap blant ansatte. For dem handler det om drift og helt andre arbeidsoppgaver enn cybersikkerhet. Det spiller også inn at ansatte ikke får avsatt tid til å lære mer om cybersikkerhet da de har for mange oppgaver og ikke prioriterer det. Det fremkommer likevel da de fleste har hørt om angrepet på Østre Toten så blir flere og flere mer bevisste rundt temaet.

Informantene formidler videre opplæring som en viktig del i tiden fremover for de ansatte (nr. 2, 4, 5, 6, 7, 8, 9 og 10). For ansatte i kommunen til informant nr. 6 er det lagt ut egne

læringsplattformer der det legges ut ofte stilte spørsmål og typiske sikkerhetsspørsmål, men at det er avhengig av at ansatte kjenner til denne plattformen og faktisk benytter seg av den. Det er likevel tilrettelagt for at ansatte skal kunne finne frem på egenhånd. Informant nr. 6 og 7 forteller også hvordan opplæring har blitt obligatorisk i kommunene. Derimot forteller informant nr. 8 at det har blitt forsøkt å sette et kompetansekrav for de ansatte, men at det ikke har fått gjennomslag da det viste seg å være for vanskelig å kreve av ansatte. Informant nr. 2 forteller hvordan de bruker mye tid på opplæring blant ansatte. De har nå kjørt ulike tester der de blant annet ikke får fullført testen hvis de ikke har svart riktig, noe som fører til økt kunnskap blant ansatte. Informant nr. 4 forteller hvordan de jobber for å gjøre ansatte mer sikkerhetsbevisste:

> «(…) hvor vi har begynt å snakke verdikjeder helt fra, holdt på å si vernepleieren ute i helse og helt inn i datasenteret opp i skyløsningen og hvordan man skal ivareta de enkelte ledd, få verdivurdert opplysninger, slette sensitivitet og så har vi fått veldig mye drahjelp fra andre organisasjoner og Østre Toten saken. Da har de plutselig skjønt at dette er litt mer alvorlig enn de trodde» (Informant nr. 4).

Videre formidler informant nr. 5 og nr. 3 hvordan ansatte og ledere ikke har kunnskap til hva som bør gjøres i forhold til sikkerhetsarbeidet, og at det mangler en forståelse på risikoen:

> «De er ikke klar over at dette her er en risiko. De har ikke forhold til personopplysninger i det hele tatt. De vet ikke når de bryter loven da. Så den kompetansen på bakke, på grunnivå, den er ikke til stede, så det er en stor jobb å få den kunnskapen opp i kommunene. Og da hjelper det nesten ikke å snakke på overordna nivå, det store truslene, regjeringen og sånne ting, fordi de ser ikke dette i sin hverdag da» (Informant nr. 5).

> «Hvis jeg går inn der om kvelden så vet jeg at pc-en står i stor grad ulåst, innlogget i fagsystemer og klare for å misbrukes» (Informant nr. 3).

Flere av informantene nevner hvordan bevisstheten rundt temaet har blitt mye større etter angrepet på Østre Toten, og hvordan flere viser interesse for cybersikkerhet (Informant nr. 2, 8 og 9). I motsetning til flere av de andre informantene mener informant nr. 2: «at de har i gjennomsnittet modne ansatte». Det blir også snakket om at fokuset og forståelsen er mye mer til stedet nå i det offentlige en tidligere. Informant 1 beskriver at det er de ansatte som kanskje har gjort den største utviklingen, de har tatt utviklingen av digitalisering hurtig i forhold til cybersikkerhet. De har også noen ansatte som har mer fokus og forståelse enn andre

(Informant 1). Informant nr. 1 forteller også om at: «det er mye mer modenhet nå i det offentlige når det kommer til det digitale, i forhold til tidligere på grunn av den unge alderen og forståelsen for IKT». Det fortelles om hvordan de ansatte nå har en helt annen holdning til cybersikkerhet og at forstår mer om hvordan en skal forholde seg til det. Informanten hevder at dette kan ha noe med generasjonsskifte å gjøre (Informant nr. 1).

Videre snakkes det om sikkerhetskultur, da forteller tre av informantene hvordan det er fokus på rapportering av avvik. Informant nr. 7 forteller at kommunene de drifter for har egne sikkerhetsansvarlige som opererer med de rettighetene å melde inn avvik til datatilsynet. Det blir også fortalt hvordan kommunen får en rapport fra datatilsynet på det som har skjedd, hvis det har vært en alvorlig hendelse (Informant nr. 8).

> «Ja et målebarometer er jo avviksmeldinger og så kan du si hvor mye avvik vi får inn, så det er jo en kultur-greie, det å få registrert avvik for å se hvordan ting ikke fungerer/fungerer. Så var det jo det jeg va innpå som er en stor utfordring. Det å få kontroll på overvåkning og kontroll på dataflyten» (Informant nr. 2).

5.6 Risikoforståelse i kommunene

Før angrepet på Østre Toten var det veldig mange ulike forståelser av cybersikkerhet blant både ledere og ansatte. Informantene forteller hvordan de før har tenkt at «det skjer ikke oss», informant nr. 3 sier:

> «Det var jo litt sånn vekkelsen min da med IKT-sikkerhet og at det der kan skje med oss også, vi er ingen til å sitte å tro og være så naive at hvem skal bry seg om vår lille kommune». (Informant nr. 3.)

> «Fordi vi har jo faktisk hatt et spark i rumpa, mot andre som har sittet og tenkt at dette skjer ikke oss, hvordan har de tenkt» (Informant nr. 1).

> «Det er det jo sånn vi er bygd sånn, at sånne ting skjer ikke her hos oss, det skjer jo ikke meg» (Informant nr. 1).

Da jeg spurte informantene om det har vært endringer i fokus fra kommunen, bekrefter flere av informantene at tidligere har det handlet om opptid for kommunene (Informant nr. 2, 4, 5, 6, 7, 8, 9). På bakgrunn av dette forteller informantene at sikkerhet ikke har blitt prioritert. Informant nr.1 forteller:

> «Ledelsen oppe, skjønte ikke rollen til IKT og til det faget rett og slett. Jeg tror det er så enkelt som det» (Informant nr. 1).

> «Før dette her så var fokuset på IKT sikkerheten lav og hvert fall, jeg kan ikke snakke for han tidligere kollegaen min, men kan snakke for meg selv og jeg må jo si at jeg har vært naiv i når det gjelder IKT sikkerheten til kommunen, jeg har tenkt at på grunn av at vi «outsourcer» alt så er alt ivaretatt, det er sikkert» (Informant nr.3).

> «Men de leverandørene der er jo heller ikke. Fordi at det her er jo systemer som er tenkt skal bare stå og levere hele tiden, og ja det er klart at å legge inn en oppdatering der så kanskje du forstyrrer leveransen, du kan oppleve nedetid, og det har vært tungt for dem og svelge, men samtidig så ligger det jo, man kan jo ta null kontroll som dagbladet kjørte for noen år siden hvor de kunne la pumpestasjoner osv. bare med å skanne hva som ligger eksponert på internett» (Informant nr.5).

Informantene forteller også i forhold til beredskap hvorfor de ikke har hatt planarbeidet på plass tidligere:

> «(…) og det har vi gjort på en lurere måte i ettertid, så hvorfor vi ikke hadde planarbeidet på plass det var nok at i før jeg kom inn her så har aldri dette vært en type tema» (Informant nr. 1).

Når det kommer til øvelser og hvor mye man skal investere i cybersikkerhet sier informant nr. 2:

> «Si det er 150 kommuner og har skjedd en gang de siste årene så katastrofalt som det skjedde med Østre Toten. 1 av 150 på 20 år. Sannsynligheten er, man begynner å regne på det da, for at det skal treffe oss. Også tar man liksom og ser litt sånn retrospektiv på det og finner ut at ja, hvis vi klarer å halvere risikoen med å investere en halv million, og nei det er ikke verdt det, da tar vi den risikoen» (Informant nr. 2)

En annen interessant ting som informant nr. 1 nevnte var:

> «Jeg tror ikke at vår kommune eller noen kommuner kommer til å komme i sånn utpressings situasjon slik som politikerne våre er redde for. De tro vi vil måtte betale 50 millioner kroner til Russland» (Informant nr. 1).

Det blir også snakket om at informantene mener det er tilfeldigheter som gjør at kommunene blir angrepet eller ikke. Informant nr. 2 hevder:

> «Det er jo det store, det er jo helt tilfeldig om det treffer deg eller ikke. Og det blir vel sånn som en sa i gamle dager at er ikke det at alarm på bilen sikrer deg mot innbrudd i

bilen, men hvis du har alarm og ikke bilen ved siden av så er det den man bryter seg inn i. Det er liksom. Men angriper eller går til verks der det lykkes lett da» (Informant nr. 2)

5.7 Læringssted for kommunene

Funn som kom frem i intervjuene på hvorfor kommunene blant annet ikke hadde beredskapsplaner var at informantene ønsket hjelp fra sentrale myndigheter og offentlige instanser. Informantene forteller hvordan interesseorganisasjoner eller sentrale myndigheter burde kommet på banen med mer verktøy, tydeligere informasjon om hva som krevdes innenfor cybersikkerhet i kommunene (Informant nr. 1, 3, 4 og 5). Informantene nevner hvordan Kommunesektoren (KS) er en av de som har kommet på banen etter angrepet på Østre Toten med flere tiltak enn før som kan gjøres for at kommunene er mer forberedt på cyberangrep. Informant nr. 1 forteller hvordan de ber om hjelp for å få verktøy til å lage beredskapsplaner:

> «(…) og det vi egentlig gjør i kommunene også oppi dette her er at vi ber om hjelp, vi ber til KS til hjelp om dette. Vi trenger å få noen verktøy rundt dette for å lage disse tingene her» (Informant nr. 1).

> «(…) og da er jo vann og avløp helt essensielt, og kommune har en stor del av det. Og da er det litt sånn at ikke kommunaldepartementet går ut og sier det her er en del av kritisk infrastruktur i Norge og dette har ekstra krav for beskyttelse i forhold til sikkerhetsloven og sånn det er en artig greie» (Informant nr.5).

Å finne et kompetansesenter for kommuner, noen som kan ta litt ansvar og hjelpe norske kommuner å forstå trusselbildet og ha mer kompetanse rundt dette nevner informant nr. 2. Informanten nevner også hvordan det kan være lurt å samordne tiltak som bør gjøres. Informant nr. 4 forholder seg til at departementer, utdanningsforbund og staten burde kommet tidligere på banen med å stille krav til både leverandører og de som drifter for kommunen. Hadde disse kommet på banen tidligere kunne det vært lettere å drive på med cybersikkerhet for kommuner.

> «Og derfor mener jeg at stat og på en måte departement og disse direktoratene, de må på en måte, departement og disse direktoratene de må på banen, mye sterkere» (Informant nr. 4).

Når det kommer til dette med samarbeid, nevner også noen av informantene hvordan spesielt KS er kommet på banen i ettertid (Informant nr. 1, 9, 10). Informant nr. 10 beskriver hvordan de er med på samarbeidsfora som f.eks. KS har veldig mye, de utvikler nye konsepter, grupperinger der flere går sammen fordi de har samme utfordringene enten de er store eller små. Informant nr. 9 forteller:

> «Og så har vi jo fått mer dybdekunnskap om det etter hvert gjennom nasjonal sikkerhetsmyndighet, gjennom organisasjoner, jeg tror jeg har fått det meste der gjennom de forskjellige seminarene og webinarene» (Informant nr. 9).

5.8 Oppsummering av empiriske funn

Hovedfunnene i denne empirien var i forhold til toppledelsen og cybersikkerhet at det var en tydelig endring hos toppledelsen etter angrepet på Østre Toten. Flertallet av informantene rapporterte om oppsving i fokus basert på det. Videre var det tydelig blant tre av kommunene hvordan ansvaret fremdeles blir lagt over til IKT-avdeling. Fire av informantene forteller hvordan de har tydelig engasjerte ledere etterfulgt av angrepet på Østre Toten.

I forhold til temaet beredskap forteller flere av informantene at de ikke har hatt øvelser. Derimot forteller hele sju av ti informanter at de har planlagt å ha øvelser gjeldende cybersikkerhet. Når det kommer til gjenoppretting hevder noen av informantene at helse er gode på å arbeide uten digitale systemer og er gode på gjenoppretting. Fire av informantene forteller hvordan beredskapsplaner ikke inkluderer cybersikkerhet eller IKT sikkerhet, eller IKT-trusselbilde. Flere av informantene forteller hvordan de jobber med å forbedre beredskapsplanene, blant annet å inkludere IKT-trusselbilde.

Når det kommer til sårbarheter, forteller informantene om organisatoriske sårbarheter. Ifølge informantene er IKT-avdelingen sett på som separat fra kommunen, spesielt når de som drifter for kommunen er eksterne. Motsatt forteller de som arbeider i intern drift for kommunen at de får mer handlingsrom og dermed har lettere for å fjerne sårbarheter.

Det hevdes at kommunen er en komplisert organisasjon og at dette fører til at det er vanskelig med tilgang og kontroll av alle ansatte, og det er komplisert å lage planer når så mange ulike sektorer skal med. Kommunene hadde problemer med å få nok ressurser til å drive med cybersikkerhet før angrepet på Østre Toten, men i ettertid har dette vært enklere.

IKT-plassering er et tema som dukker opp blant flere av informantene. Flere nevner hvordan det er fordeler å ha IKT-avdeling internt i kommunen, mens noen få kommenterer hvordan

det kan være fordeler å ha den eksternt for å få bedre kompetanse. Empiriske funn i forhold til sikkerhetskultur i kommunene fremhevet at det var stor enighet om at det er vanskelig for ansatte å ha kompetanse og komplisert å drive med opplæring. Det siste empiriske funnet handlet om hvordan fire kommuner ønsker mer hjelp fra sentrale myndigheter og noen av informantene forteller hvordan KS er startet med å hjelpe kommunene i arbeidet med cybersikkerhet.

6.0 Diskusjon

Dette kapittelet vil diskutere empirien i lys av teorien. Fremstillingen av diskusjonen er basert på forskningsspørsmålene som er laget for å komme frem til svaret på problemstillingen. Her vil temaene fra empirien bli diskutert i lys av flere teorier, ettersom flere av teoriene er bindende. Empirien vil også komme frem i flere deler av diskusjonen for å kunne besvare forskningsspørsmålene. Diskusjonen bygger på denne problemstillingen:

«Hvordan er arbeidet med cybersikkerhet i norske kommuner, og har angrepet på Østre Toten ført til endringer?»

Forskningsspørsmål:

1. Hvordan påvirker ledelsesforankring arbeidet med cybersikkerhet?
2. Hvordan ligger risikostyring til grunn for arbeidet med cybersikkerhet i kommunene?
3. Hvordan er sikkerhetskultur integrert i arbeidet med cybersikkerhet?

6.1 Ledelsesforankring før angrepet på Østre Toten

Informantene fortalte hvordan ledelsen fokuserte på oppetid og ikke prioriterte arbeidet med cybersikkerhet før angrepet på Østre Toten. Dersom tilfellet er at cybersikkerhet ikke var ledelsesforankret i kommunene før angrepet på Østre Toten, kan det ha sammenheng med hvorfor cybersikkerhet ble nedprioritert. På en annen side kan det bety at oppetid handler om at de faktisk prioriterer cybersikkerhet, fordi de forstår at brudd på cybersikkerheten kan føre til nedetid for kommunen. Ifølge studien til Uchendu (2021) er støtte fra toppledelsen viktig for å prioritere sikkerhet. Hvis toppledelsen ikke selv prioriterer arbeidet med cybersikkerhet, kan det virke som om hele organisasjonen ikke trenger å prioritere det, og dermed påvirkes arbeidet med cybersikkerhet. Dette kan føre til at ansatte tenker det samme og dermed blir ikke forebyggende arbeid med cybersikkerhet prioritert. Informantene forteller at det før angrepet på Østre Toten var vanskelig for toppledelsen i kommunene å skulle velge mellom en sykepleier eller virusbeskyttelse på PC'er på bakgrunn av ressurser, og det virker dermed som topplederne ikke har forstått betydningen av cybersikkerhet. I lys av at toppledelsen før angrepet på Østre Toten ikke har forstått at cybersikkerhet er viktig, (for det kan gå ut over dem som trenger en sykepleier eller de som trenger en lærer), kan det se ut til at cybersikkerhet ikke har vært ledelsesforankret i kommunene før angrepet på Østre Toten.

Ifølge Aven og Renn (2010) er forståelsen av risiko når individer selv vurderer risiko basert på tidligere hendelser som vil si erfaringen de har med risikosituasjonen. Et relevant punkt her kan være at toppledelsen i kommunene ikke har forstått risikoen av å ikke ha cybersikkerhet

eller hvor viktig det er med ledelsesforankring. En mulig forklaring kan være at toppledelsen vurderer risikoen som følge av at kommuner tidligere ikke har opplevd noe lignende det som skjedde med Østre Toten. Dermed virker ikke cyberangrep som en risiko for kommunene. Sannsynligheten vurderes som liten for en uønsket hendelse som cyberangrep og derfor har de ikke innført ikke forebyggende tiltak. Blant annet fortelles det om hvordan kommunene tidligere har tenkt: «det skjer ikke oss», når det gjelder cyberangrep. Det vil blant annet kunne bety at de ikke ser på cybersikkerhet som en risiko fordi de enten tenker at sannsynligheten for hendelsen er liten, eller at alvorlighetsgraden av et cyberangrep ikke er stor (Pritchard, 2015, s. 7).

En annen mulig forklaring kan være at topplederne i kommunene før angrepet på Østre Toten har forstått sannsynligheten av hvor ofte et cyberangrep kan forekomme, men de har ikke forstått hvor mye skade konsekvensene av et cyberangrep kan påføre organisasjonen. Perspektivet om risiko til Aven og Renn (2010) viser til at sannsynlighet og konsekvenser er med i beregninger som gjøres for å se hvor stor risikoen er. I motsetning til dette perspektivet kan det se ut til at kommunene muligens ikke har tatt med konsekvensene i en risikovurdering, som følge av at toppledelsen ikke har forstått risikoen. Dersom toppledelsen ser på risikoen for brudd på cybersikkerhet som liten, kan det se ut til at arbeidet med cybersikkerhet ikke var ledelsesforankret før angrepet på Østre Toten. Det kan ha påvirket arbeidet med cybersikkerhet, at toppledelsen ikke har forstått at brudd på cybersikkerheten utgjorde en trussel mot kommunene.

6.2 Ledelsesforankring etter angrepet på Østre Toten

Von Solms og Von Solms (2006) mener det er styret i organisasjonen som er ansvarlige for sikkerheten. Blant flere av informantene fortelles det om at toppledelsen overlater ansvaret for cybersikkerhet til IKT-avdelingen for arbeidet med cybersikkerhet etter angrepet på Østre Toten. Dersom tilfellet er at IKT-avdelingen er ansvarlige for cybersikkerhet, kan det også bety at cybersikkerhet ikke er ledelsesforankret, ettersom de fraskriver seg ansvaret. Hvis IKT-avdelingen har ansvaret, må de også ha myndighet til å gjøre noe med det. Det er toppledelsen som skal delegere beslutningsmyndighet, og dermed har ansvaret (Jacobsen, 2009, s. 85). På en annen side kan det bety at toppledelsen fremdeles ser seg som ansvarlige fordi de kan skaffe ressursene. Studien til Thong et al., (1996) viser til at det er toppledelsen som kan gi ressurser som behøves for å forbedre sikkerheten. Dermed kan toppledelsen gi ressurser til IKT-avdelingen som har teknisk kunnskap om temaet. En annen mulig forklaring til at toppledelsen henvender seg til IKT-avdelingen kan være at de ønsker forsvarlig

cybersikkerhet i kommunene. Informantene forteller videre at toppledelsen ikke har nok kunnskap om risikoen de står ovenfor med cyberangrep, og det kan virke som at de ønsker å forstå risikoen ved å ikke ha forsvarlig cybersikkerhet. Samtidig som en leder kanskje ikke har den tekniske kompetansen, bør de likevel forstå at cybersikkerhet angår hele organisasjonen. Marvell (2015) beskriver hvor viktig det er for organisasjoner å ha hele bildet på cybersikkerhet i organisasjonen, for å forstå hvilke trusler organisasjonen står ovenfor og hvilke trusler som aksepteres (Marvell, 2015, s. 26). Når en leder får forståelse kan det øke kunnskapen rundt cybersikkerhet og det kan bidra til at alle de ulike sektorene forstår hvilke tiltak som må gjøres for å redusere sårbarheter. I tillegg vil det også kunne bidra til at toppledelsen tilfører ressurser til alle sektorene. Ettersom det kommer frem i intervjuene at de ønsker hjelp fra IKT-avdeling, kan det virke som om de ikke helt forstår hvor ansvaret for arbeidet med cybersikkerhet ligger.

Videre vises det til endring i toppledelsens prioritet av arbeidet med cybersikkerhet i kommunene etter angrepet på Østre Toten. I likhet med tidligere studier kan det se ut til at når sikkerhet forankres i toppledelsen, er det et positivt utslag på sikkerhetsarbeidet i organisasjonen (Kankanhalli et al., 2003). Ifølge flere informanter har de fått flere ressurser, beredskap og planer etter angrepet på Østre Toten. Dersom arbeidet med cybersikkerhet er forankret i toppledelsen, kan det virke som at effekten blir endringer tilhørende cybersikkerhet. På en annen side kan toppledelsens forandring i fokus føre til endringer i selve styringen av cybersikkerhet. Blant annet kan det bli tilført mer ressurser i arbeidet med opplæring av cybersikkerhet til ansatte, noe som kan føre til mer kunnskap om hvilke cybertrusler man står ovenfor og dermed større oversikt over trusselbildet. Uten dette vil det være vanskelig for kommunen å redusere sårbarheter, fordi de vet ikke hvilke angrep de står ovenfor eller hva som kan skje. Dersom cybersikkerhet er blitt ledelsesforankret etter angrepet på Østre Toten, vil det kunne bety at det har ført til atferdsendringer i organisasjonen. I forlengelse av dette kan det se ut til at toppledelsen har forstått risikoen ved å ikke ha forsvarlig cybersikkerhet, og dermed tilført ressurser til forebygging og beredskap. I samsvar med studien til Thong et al., (1996) kan toppledelsens støtte gi ressurser som behøves for å forbedre arbeidet i kommunene.

Et eksempel på dette er når informantene forteller at det er enklere å få ressurser nå enn før. I tillegg er ansatte fra IKT-avdelingen blitt invitert til styremøter sammen med toppledelsen for å formidle risikoen slik at styret får oversikt over risikoene de står ovenfor i de ulike sektorene. Det kan tyde på at ledelsesforankring bidrar til endring i organisasjonen, og

dermed endring i arbeidet med cybersikkerhet. Kommunene iverksetter dermed tiltak for å forbedre cybersikkerheten. En annen mulig forklaring kan være at når arbeidet med cybersikkerhet er ledelsesforankret, kan det bety at ansatte også forstår hvor viktig det er å f.eks. logge ut av PC'en før de går hjem om kvelden eller ikke trykker på en link i en epost som virker mistenkelig.

Sju av ti informanter forteller hvordan toppledelsen etter angrepet på Østre Toten har oppsving i fokus. Selv om informantene forteller om at toppledelsen har mer fokus på cybersikkerhet, kan det være andre årsaker til at arbeidet med cybersikkerhet har fått tilført mer ressurser. På den ene siden kan det være at informantene antar at de har fått tilført mer ressurser etter angrepet på Østre Toten. Men allikevel kan det være andre grunner som informantene ikke forstår, og det kan jo også tenkes at ressursene har vært like hele tiden. En annen mulig forklaring kan være at informantene har forstått hvor viktig det er med cybersikkerhet og dermed startet å prioritere det i IKT-avdelingen. På en annen side er det flere grunner til å tro at ledelsesforankring er årsaken til endring i arbeidet med cybersikkerhet, som følge av at det er toppledelsen som har mulighet til å prioritere cybersikkerhet som ansvarlige for arbeidet.

6.3 Risikostyring av cybersikkerhet

I den første fasen av beredskap handler det om å ha nøyaktig kunnskap om trusselen (Perry & Lindell, 2003). I intervjuene kommer det frem at flere av informantene ikke har hatt IKT-trusselbilde i beredskapsplanene. Det kan virke som kommunene tidligere har godtatt risikoen for å bli utsatt for et cyberangrep. Et eksempel på dette er når den ene informanten forteller om at de har akseptert risikoen fordi det koster for mye med forebyggende arbeid. I likhet med studien til Choodakowska et. Al (2022) der det viste til mangel på økonomiske ressurser i arbeidet med cybersikkerhet i kommunene. Det kan se ut til at kommunene ikke har forstått risikoen, hvor stor sannsynligheten er, eller hvor store økonomiske tap brudd på cybersikkerheten kan før til. Endring av risikoforståelsen ifølge informantene var da toppledelsen forstod hvordan dette påvirket økonomien i Østre Toten. Det ser ikke ut til at kommunene har tatt innover seg Engen et al. (2016) sin teori om beredskap og hvor viktig det er å være forberedt på alvorlige hendelser (Engen et al., 2016, s. 280-286). Men etter angrepet på Østre Toten, har de identifisert truslene de står ovenfor. Det kan bety at de ikke har gjort forebyggende arbeid tidligere, men har endret det etter et alvorlig angrep mot en lignende organisasjon. Dette kommer frem når kommunene forteller om planer om å opprette

aktiviteter i beredskapsplanene som inneholder å gjennomføre IKT-trusselbilde mot kommunene, men at det ennå ikke er gjennomført.

På en annen side kan det være at de har identifisert risikoen av cyberangrep, men på bakgrunn av kommunens forståelse av risiko har det blitt forstått som en akseptert risiko. Engen et al. (2016) beskriver hvordan enhver virksomhet har akseptkriterier for risikoer. Det betyr at det er noen kriterier som skal til for at de kan akseptere risikoen (Engen et al., 2016, s. 284). Samtidig fortelles det i intervjuene at flere av kommunene har planer om å implementere IKT-trusselbilde som kan bety at kommuners oppfattelse av risiko har endret seg etter angrepet på Østre Toten og dermed har akseptkriterier mulig endret seg. I lys av angrepet kan det se ut til at konsekvensene som kan ramme en kommune er store hvis de skulle bli utsatt for cyberangrep. Det er mulig at risikoforståelsen har endret seg basert på opplevd risiko. I likhet med studien til Slovic et al. (2005) betyr det at individer definerer risiko etter egen målestokk (Slovic et al., 2005). Dersom kommunene vurderer risiko etter tidligere erfaringer, vil de ikke kunne forutse, forstå eller analysere risikoer i samfunnet før de allerede har skjedd. Det vil derfor være vanskelig for kommunene å lage gode risikoanalyser fordi de ikke har nøyaktig kunnskap om trusselen (Perry & Lindell, 2003). Årsaken til at kommunene har vurdert risiko slik kan være at de ikke har kommunisert nok om temaet. På en annen side kan det bety at kommunene har håndtert risiko subjektivt, og ikke etter statistikk basert på lignende tidligere hendelser (Vatnelid, 2018, s. 19). Dersom flere i kommunene forstår risiko subjektivt, betyr det ikke at det ville betydd noe for dem at flere andre organisasjoner har opplevd cyberangrep. Hvis kommunene hadde fått statistikk over hyppigheten av cyberangrep, er det likevel ikke sikkert at de hadde tatt innover seg risikoen dersom de forstår risikoen subjektivt. Kommunene vil dermed ikke forstå trusselbildet de stå ovenfor, som igjen kan føre til dårlig risikostyring for de ikke forstår hvilke tiltak som må gjøres for å være forberedt eller klar til å gjenopprette etter et cyberangrep.

I den andre fasen av beredskap bør det bli gitt en ramme for hendelser som det trengs beredskap for. I tredje fase vil det bli dokumentert hva som behøves i form av f.eks. utstyr og planer for hva som skal gjøres (Engen et al., 2016, s. 284-286). Funn i denne studien viser at flere av kommunene ikke har laget beredskap i forbindelse med cybersikkerhet. I likhet med studien til Wirtz og Weyerer (2017) kan det se ut til at kommunene før angrepet på Østre Toten også hadde manglende beredskapstiltak og de må forbedre dette for å være forberedt på cybersikkerhet (Wirtz & Weyerer, 2017). En annen mulig forklaring kan være at kommunen ikke har disse planene fordi de ikke har gjennomført en risikoanalyse som tar for seg

cybersikkerhet. Dersom kommunene ikke har cybersikkerhet i planene, kan det bety at de ikke har kartlagt risikoen som uforsvarlig cybersikkerhet medfører. Kan de ikke styre risikoen med tiltak for å redusere sårbarheter eller forberede seg på cyberangrep, kan det føre til nedetid i kritisk infrastruktur fordi de vet ikke hvilke sårbarheter de bør redusere. Et annet relevant punkt er at informantene forteller at helsesektoren er god på gjenoppretting om det skulle skje noe. Det viser til at kommunene har utført tiltak som gjenoppretting for å være forberedt dersom kommunene skulle oppleve nedetid. Ettersom informantene forteller at planene ikke har vært forankret eller at de ikke har hatt nok ressurser til å utføre dem, kan det bety at toppledelsen ikke har støttet konsekvent cybersikkerhetsarbeidet.

Den siste delen av en beredskapsprosess er å gjennomføre øvelser for å kunne innføre tiltak på hvilke svakheter og sårbarheter som finnes i systemene, og forbedre beredskapsplanen (Engen et al., 2016, s. 284-286). I intervjuene vises det til at flere av informantene ikke har hatt øvelser når det gjelder cybersikkerhet før angrepet på Østre Toten. Det faktum at flertallet av informantene i kommunene svarte at de ikke hadde hatt øvelser relatert til cybersikkerhet, kan vise til at det har vært manglende risikostyring av cybersikkerhet før angrepet på Østre Toten. Blant annet kan det bety at kommunene ikke forsto viktigheten av å øve. En informant forteller at de ikke øver fordi det ikke er kultur for det. Det fortelles også at årsaken til at kommunene ikke øver er at flere ansatte i kommunen tenker at de tar det som det kommer. Poenget med øvelser er å oppdage hvilke tiltak kommunene kan gjøre for å redusere sannsynlighetene og konsekvensene av cyberangrep, eller hvordan de kan forberede seg på dette. Presentert av Engen (2016) handler siste fase i beredskapsarbeidet om å lære av virkelige hendelser og trekke lærdom av det man trener og øver på (Engen et al., 2016, s. 286). Organisasjoner benytter seg av beredskapsprosesser for å være forberedt på ulykker, eller for å motstå disse. En veldig viktig del i arbeidet med cybersikkerhet er å redusere sårbarhetene (Galinec et al., 2017). Såfremt kommunene ikke øver i forbindelse med cybersikkerhet, kan det bety de ikke finner noen måte å redusere sårbarhetene fordi det kan føre til at de ikke forstår hva de er. Hensikten med en øvelse er evaluering av beredskapen som er etablert (Engen et al., 2016, s. 280). Samtidig forteller flere informanter hvordan de etter angrepet på Østre Toten i nærmeste fremtid har en plan om å korrigere beredskapsplanene og ta med cybersikkerhet som et tema, eller har nylig hatt øvelser. På en side betyr dette at kommunene har forstått viktigheten av å øve på cybersikkerhet og hvordan det vil hjelpe dem å oppdage sårbarheter som kan reduseres. Øvelser vil dermed også bidra som tiltak for å redusere risikoen for cyberangrep. I likhet med studien til Knuth et al., (2014)

kan det virke som kommunene forstår risiko basert på opplevelse av risiko, ettersom kommunene har startet med øvelser som gjelder cybersikkerhet etter angrepet på Østre Toten. Selv om kommunene muligens ikke selv har opplevd angrep, har de ha fått en opplevelse av hvilke konsekvenser andre kommuner har opplevd når de ble utsatt for et cyberangrep. En annen mulig årsak til at kommunene har startet med øvelser etter angrepet på Østre Toten kan være som følge av at risikostyringen av toppledelsen har blitt bedre. Ifølge Aven krever en suksessfull risikostyring ledelsesforankring (Aven, 2008a).

Videre formidles det årsaker til at risikostyringen av cybersikkerhet er komplisert i kommunene på grunn av organiseringen. Ettersom det forstås som en utfordring, kan det se ut som om organiseringen ikke er tatt med i betraktning i en risikoanalyse. Det kan hende at kommunene tidligere har syntes det har vært for komplisert å innføre organiseringen til kommunene som en del av risikoen. En annen side kan være at de ikke har forstått risikoen ved å ikke innføre organiseringen til kommunen som en del av risikoanalysen. I likhet med tidligere studier er risikoforståelse avhengig av om man har opplevd lignende type farer før (Knuth et al., 2014). En annen mulig forklaring kan være at det virker som kommunene har tolket risikoen med cybersikkerhet basert på egen forståelse av risikoen. Et eksempel på det kan være den ene informanten som forteller om vannverk som ikke ønsket nedetid, og derfor ikke ville oppdatere systemene. Det kan bety at ansatte i vannverket forstår risikoen med cyberangrep basert på sin egen dømmekraft av risikoen (Slovic et al., 2005). Derimot hvis vannverket forstår hvor viktig det er med cybersikkerhet for å ikke oppleve nedetid ville nok opplevelsen av risiko vært annerledes. Mulig ville det vært lettere for vannverket å ha nedetid i noen timer for å oppdatere systemene i motsetning til lengre tid som et cyberangrep kan føre til. En annen mulig forklaring kan være at kommunene ikke har tatt for seg forsiktighetsprinsippet i møte med cyberangrep. Det kan bety at når de har analysert risikoen med organiseringen av kommunene, burde forsiktighet være herskende prinsipp, der det bør bli utført tiltak for å redusere konsekvenser som man ikke vet noe om (Aven, 2006, 2008a, 2015). Ettersom man ikke kan vite hvor store konsekvensene kan bli som følge av et cyberangrep, bør det likevel utføres med forsiktighet i arbeidet i kommunene. Det betyr at kommunene må utføre tiltak for å være forberedt, selv om de ikke vet hvor store konsekvensene er. På bakgrunn av at kommunene ikke har tatt med organiseringen i risikoanalysen, kan det bety at risikostyringen av cybersikkerhet ikke har vært der i utgangspunktet. En annen mulig forklaring er at informantene forteller hvordan de har startet med adgangskontroll av IKT-systemene som gjør at blant annet ansatte som slutter å arbeide i

kommunene ikke lenger får administrasjonsrettigheter. Det kan bety at kommunene har forstått hvor viktig det er å redusere sårbarheter for at det ikke skal være like lett å angripe kommunene (Galinec et al., 2017, s. 284, 285).

En annen utfordring som kommer frem i kommunene er hvordan IKT-avdelingens plassering har betydning for arbeidet med cybersikkerhet. Men er det virkelig slik at kommunens plassering faktisk har påvirkning på arbeidet med cybersikkerhet? Eller kan det også bety at risikostyringen av arbeidet med cybersikkerhet ikke er god nok? En mulig forklaring kan være at ansatte og toppledelsen i kommunene ikke har hatt god nok kunnskap om cybersikkerhet. Dersom det er sistnevnte, vil tilfellet være organisatoriske sårbarheter som manglende krav til sikkerhetskompetanse (Rausand & Utne, 2022, s. 404). Det vil ha betydning for kommunen for arbeidet med cybersikkerhet, fordi de mangler sikkerhetstiltak, som for eksempel overvåkning av risikoen cybersikkerhet medfører. Hvis det ikke er nok kunnskap i hele organisasjonen om cybersikkerhet, kan årsaken være at risikostyringen av cybersikkerhet i kommunene ikke har vært god nok fordi de har ikke redusert sårbarhetene.

Samtidig forteller en informant om hvordan endring av IKT-plasseringen har påvirket risikostyringen av cybersikkerhet i kommunen. Der har en ansatt innenfor IKT-avdelingen blitt plassert strategisk i hierarkiet og fått oversikt over hele organisasjonen. Det var et tiltak som ble gjort etter angrepet på Østre Toten og det kan ha ført til at kommunene har gjort tiltak for å styre risikoen. Ifølge Aven er prosesser og strategier viktige for å kunne kartlegge og styre risikoen (Aven, 2015, s. 13, 14). En annen mulig forklaring kan være at toppledelsen i de ulike kommunene etter angrepet på Østre Toten har forstått hvor viktig det er med kunnskap om cybersikkerhet i alle sektorene. Derav vil plasseringen av IKT-avdelingen kunne føre til at det blir mer oversikt over sårbarheter i organisasjonen. Et eksempel på det er når informantene forteller hvordan ansatte i innkjøpsavdelingen ikke har sikkerhetskompetanse. En oversikt vil muligens bidra til at ansatte som har sikkerhetskompetanse og forstår risikoen ved innkjøp av nye PC-er på skolen kan bidra med sin kompetanse.

Videre når det kommer til utvikling av beredskapsplaner og øvelser gjeldende cybersikkerhet forteller flere informanter at de ønsker hjelp fra sentrale myndigheter eller lignende. Det virker som om ansatte i kommunen ikke har innsikt i risikoforhold gjeldende cybersikkerhet, og vet ikke hva som trengs i arbeidet med cybersikkerhet ettersom de fraskriver seg ansvaret. I arbeidet med risikostyring er innsikt i risikoforhold viktig for å kunne styre risikoen (Aven,

2015, s. 13). Dersom tilfellet er at kommunene selv ikke har innsikt i risikoforholdene, vil det kunne bety at risikostyringen i kommunene når det kommer til cybersikkerhet ikke er god nok. En annen mulig forklaring kan være at kommunene ikke har redusert organisatoriske sårbarheter, ettersom de har hatt mangelfulle beredskapsplaner og manglende øvelser. Som følge av at noen av informantene ønsker hjelp til utvikling av beredskapsverktøy og lignende i arbeidet med cybersikkerhet, kan det virke som om kommunene i likhet med studien til Cheng og Groysberg (2019) ikke har prosesser og den ekspertisen som behøves for å henvende seg til cyberangrep (Cheng & Groysberg, 2019, s. 39-46).

6.4 Sikkerhetskultur

I en sikkerhetskultur er det felles oppfatninger om hvor viktig sikkerhet er og atferdsmønstre som bestemmer forpliktelsen til sikkerheten (Reason, 1997, s. 194). Informantene forteller at de ulike sektorene i kommunene oppfatter cybersikkerhet på forskjellige måter. Dette kan tyde på at ansatte i kommunen ikke har delte måter å tenke eller handle på for hvordan de arbeider med cybersikkerhet, og at ansatte i kommunen har lav kompetanse om cybersikkerhet. I lys av at kompetansen ute i sektorene er for lave, kan det også føre til at de ikke følger sikkerhetsrutiner. Med utgangspunkt i den lave kompetansen om cybersikkerhet er de ansatte ute i sektorene muligvis uforstående til viktigheten av sikkerhetsrutiner. Årsaken kan være at kommunen ikke har hatt god nok kommunikasjon med ansatte om hvor viktig det er å for eksempel logge ut av PCen, som den ene informanten forteller ikke er blitt gjennomført i den ene avdelingen i kommunen. Å glemme å logge ut av PC-en kan ha store konsekvenser og er en fysisk sårbarhet når det gjelder tekniske systemer (Rausand & Utne, 2022, s. 404).

I likhet med tidligere studier kommer det frem at for å bygge en god cybersikkerhetskultur er det viktig med toppledelsens støtte (Uchendu et al., 2021). På en side kan det være toppledelsen som ikke har kommunisert godt nok hvor viktig det er å lære opp ansatte på grunn-nivå til å kunne forstå viktigheten av å logge av Pcen. En viktig del i en sikkerhetskultur er å kommunisere informasjon om sikkerhet (Reason, 1997, s. 194-196). På en annen side kan det hende at kommunene har hatt mangelfulle rutiner når det kommer til å logge av PCen, i likhet med studien til Ruud (2011), hvor det også var mangelfulle sikkerhetsrutiner. Ruuds masteroppgave presenterer hvordan det er manglende sikkerhetsrutiner når det kommer til personopplysninger, som i likhet med denne studien kan vise til at det muligens generelt har vært mangelfulle sikkerhetsrutiner (Ruud, 2011). Årsaken til at ansatte ikke har lært dette, kan være at de ikke har opplevd et cyberangrep før. Det kan i

likhet med tidligere studier bety at de baserer risiko på bakgrunn av subjektiv forståelse (Slovic et al., 2005). I henhold til dette vil det likevel være viktig med en felles forståelse av viktigheten av cybersikkerhet, noe det ikke ser ut til at de har i kommunene. Som følge av at ansatte har veldig ulik kompetanse har ansatte ulike atferdsmønstre i situasjonene.

En annen årsak til at det ikke er felles oppfatninger om hvor viktig sikkerhet er i kommunene, er at formålet for de ansatte er å utføre oppgavene sine med daglige gjøremål. For en sykepleier handler det om å gi riktig medisin til dem som skulle trenge det, og for sykepleierne virker det ikke like viktig å huske å logge ut før de drar, i forhold til hvor viktig det er å gi medisin. En annen informant forteller hvordan det blant ansatte som drifter vann og avløp hadde vanskelig for å stenge ned vannverket for å oppdatere systemene. Årsaken til at ansatte har ulike syn på risiko kan bunne ut i at de har ulike meninger om hvor elementær cybersikkerhet er. Det fortelles hvordan cybersikkerhet blir forstått som en teknisk del, og noe som leverandøren ordner opp i. Det kan vise til at toppledelsen ikke har kjennskap til risikosituasjonen og i likhet med Knuth et al. (2014) ser på risiko basert på erfaringen de har med den type eller lignende risiko. En annen mulig forklaring kan være at toppledelsen i kommunene ikke har definert hva som er prioritet i organisasjonen (Armenia et al., 2019). Hvis toppledelsen ikke har kommunisert måter å tenke på om cybersikkerhet, kan det i så tilfelle påvirke måten ansatte tenker på, og for dem vil daglige oppgaver virke viktigere. Informant nr. 2 nevner i intervjuene; Årsaken til at kommunene ikke har cybersikkerhetsrelaterte øvelser er fordi det hverken er kultur for det, eller at kommunene er mer opptatt av det de skal levere tjenester på.

6.4.1 Læringskultur

I en læringskultur skal det være vilje og kompetanse til å trekke de riktige konklusjonene fra sikkerhetsinformasjonssystemet, og til å gjennomføre store reformer når behovet oppstår (Reason, 1997, s. 195). Dette viser til at kommunene etter angrepet på Østre Toten har gjort tiltak for å bedre cybersikkerheten fordi angrepet fikk dem til å forstå risikoen. Halvparten av kommunene beskriver endringer i arbeidet med sikkerhet, hvor blant annet prioriteringer er annerledes. Dette kan vise til at kommunene har forstått at det er viktig å gjøre store endringer. Samtidig fortelles det blant annet om at arbeidet er komplisert som følge av organisasjonen og at flere ønsker hjelp fra sentrale myndigheter. Dermed virker det som om kommunene muligens har endret læringskulturen blant ansatte, men at det er for komplisert og at de dermed trenger hjelp til arbeidet. Likevel kan det bety at kommunene gjør endringer som følge av at de ser behov for å ha bedre cybersikkerhet.

6.4.2 Rapporterende kultur

I en rapporterende kultur vil de menneskene som er i direkte kontakt med farer rapportere feil og nesten-ulykker (Reason, 1997, s. 195-197). Tre av informantene forteller hvordan de på ulike måter har noen som melder inn avvik i tekniske komponenter, hvilket bidrar til en rapporteringskultur. Men svakheten som ikke nevnes her, er at de innmeldte avvikene er av en teknisk natur og ikke nødvendigvis noe som støtter nok opp i forholdet om en rapporteringskultur. Det at informantene ikke nevner rapporterte avvik på hendelser der ansatte har utøvd dårlig dømmekraft (f.eks. klikket på lenker eller lastet opp vedlegg fra ukjente avsendere), viser at det kan tenkes at en rapporteringskultur ikke er oppnådd i forhold til et mulig ønsket mål. For at en skal få til en rapporteringskultur som bidrar til en sikkerhetskultur, kan det være viktig at ansatte rapporterer på alle trusler mot organisasjonen, ikke bare tekniske. Ettersom cybersikkerhet er mer enn bare det tekniske, vil det dermed ikke være en rapporteringskultur som tar med seg alle elementene innenfor cybersikkerhet. Dersom de ansatte i hele organisasjonen har en rapporteringskultur ville det kunne bety at toppledelsen får kjennskap til avvik fra hele organisasjonen.

Ifølge Reason (1997) vil villig deltakelse fra alle ansatte om å rapportere brudd på sikkerheten bidra til en rapporteringskultur. På en annen side fortelles det om hvordan kunnskap ute i sektoren er lav og at det er ikke bevissthet rundt cybersikkerhet. Det kan bety at når ansatte da opplever et cyberangrep ikke rapporterer det, fordi de ikke har kunnskap og ikke vet at de faktisk har stått ovenfor et cyberangrep. I tillegg forteller noen av informantene om hvordan ansatte har blitt mer bevisste etter angrepet på Østre Toten, som kan ha ført til at neste gang de åpner en epost som ikke virker troverdig forstår at dette skal rapporteres til toppledelsen. Det kan hende de ansatte gjerne tidligere har tenkt at det har ikke har noen hensikt å rapportere da de fjerner eposten. Men organisasjonen har behov for en oversikt over mye hendelser som skjer og hvor de kommer fra slik at de kan sette inn tiltak eller redusere sårbarheter for å hindre angrep. Ifølge Galinec et al. (2017) er det viktig å redusere sårbarheter i arbeidet med cybersikkerhet. Det vil alltid være noen ansatte som ikke er like gode til å oppdage trusler og derfor er det viktig at de ansatte får best mulig beskyttelse. På en annen side kan det være at kommunene ikke ønsker en rapporteringskultur fordi det også kan være en bakside. Baksiden kan være at ansatte begynner å bli angivende, som kan føre til dårlig kultur generelt. Ettersom kommunene ikke rapporterer om flere enn tekniske avvik, kan det virke som om at de ikke arbeider med dette temaet blant ansatte. I lys av lav sikkerhetskompetanse blant ansatte kan det se ut som om det ikke har blitt kommunisert hvor

viktig det er med rapportering av hendelser med avvik. Kommunikasjon om hvor viktig sikkerhet er, er en del av en sikkerhetskultur (Reason, 1997, s. 194-196). Ma et al. (2021) mener at ledelsesforankring er den viktigste funksjonen for praksisen i organisasjonsmiljøet. Dersom tilfelle er at toppledelsen ikke har kommunisert hvor viktig rapportering er i arbeidet med cybersikkerhet kan det også påvirke praksisen, og ansatte vil dermed ikke forstå hvorfor det er nødvendig å rapportere avvik. På en annen side kan det være at ansatte i IKT-avdelingen ikke har kommunisert hvor viktig det er å rapportere hendelser. Selv om lederen har det overordnede ansvaret kan det virke som toppledelsen har gitt ansvaret til IKT-avdelingen, som kan være årsaken til at det ikke har blitt arbeidet med en rapporterende kultur i kommunene. Et annet relevant punkt er at noen av informantene forteller hvordan ansatte er veldig modne når det kommer til cybersikkerhet. Det kan bety at de har forstått hvor viktig det er med cybersikkerhet og at de har fokus på å rapportere avvik og generelle rutiner. Informantene forklarer ikke hva de legger i «en moden ansatt». Det kan hende at ansatte forstår at de ikke skal klikke på en epost, men betyr det at de vet at de skal rapportere om slike hendelser? Basert på det informantene sa, kan det virke som om de har en rapporterende kultur når det kommer til tekniske tiltak, mens de arbeider med å få ansatte til å forstå viktigheten av sikkerhetsrapportering og derav kompetanseheving samt økt forståelse.

6.4.3 Fleksibel kultur

En fleksibel kultur innebærer det å skifte modus fra hierarkisk struktur til en flatere struktur der det er oppgaveeksperter på stedet, og tilbake til vanlig modus igjen (Reason, 1997, s. 195). I intervjuene fortelles det om at ledere ofte overlater cybersikkerhetsrelaterte problemer til IKT-avdelingen. I lys av at toppledelsen gir cybersikkerhetsrelaterte problemer til IKT-avdeling kan det se ut til at de i kommunene har forstått at for å ha en sikkerhetskultur i kommunen, bør det foreligge en fleksibel kultur. På den ene siden kan det virke som kommunene hele tiden har en flatere struktur, siden det i flere tilfeller fortelles av informantene at det er IKT-avdelingen som skal ta seg av arbeidet med cybersikkerhet. Hvis tilfellet er at toppledelsen fraskriver seg ansvaret fullstendig med cybersikkerhet, kan det tyde på at kommunene har problemer med å ha en fleksibel kultur. På en annen side forteller informantene at de i flere tilfeller har engasjerte ledere i toppledelsen som gir ressurser til arbeidet med cybersikkerhet. Dette kan vise til at kulturen er fleksibel i den grad hvor den øverste lederen har ansvaret, men delegerer arbeidet med cybersikkerhet til de som er eksperter på stedet. Gjensidig tillit handler om at man har respekt for ansattes kompetanse og motsatt (Reason, 1997, s. 195). Det kan vise hvordan kommunene på nåværende tidspunkt

satser mot en god cybersikkerhetskultur og ressursene blir fordelt korrekt i likhet med studien til Uchendu et al (2021). Dette kan indikere at arbeidet med å ha en fleksibel sikkerhetskultur er forstått av toppledelsen, noe som kan føre til at det er en tilstedeværende fleksibel kultur etter angrepet på Østre Toten.

6.4.4 Rettferdig kultur

En rettferdig kultur innebærer å sette en grense for hva som er akseptabel eller uakseptabel grense for handlinger som kan føre til organisatoriske cybersikkerhetsbrudd (Reason, 1997, s. 204-206). I intervjuene forteller noen av informantene at det tidligere har blitt prøvd å kreve et visst nivå sikkerhetskompetanse av ansatte, men at det ble tatt bort fordi det var for vanskelig å etterleve. Dersom kommunene ikke setter grenser, kan det dannes en uønsket kultur der brudd og avvik ikke blir rapportert. Ved at kommunene viser med adferd hva som er akseptabelt ved enten å straffe eller premiere handlinger, vil det også etter en stund dannes en ønsket og rettferdig kultur (Reason, 1997, s. 204-206). Det er likevel ikke slik at man kan straffe alle uakseptable handlinger, fordi det kan føre til at ansatte ikke tør å si ifra hva som hendt (Reason, 1997, s. 204-206). Det som kan trekkes ut av dette er at det ikke er en grense på hvilke handlinger som er tillatt og ikke. En slik mangel på grenser i en organisasjon kan føre til at ansatte ikke har nok fokus på prioritering av forebyggende tiltak som de burde. Dersom tilfellet er at kommunene ikke har grenser for akseptable og uakseptable handlinger, vil det også kunne påvirke holdningene i organisasjonen. Det kan bety holdninger blant ansatte og ledere, som for eksempel kan være at ansatte ikke forstår at man skal være konsekvente med å logge ut av PC-en for sikkerhet, fordi de forstår ikke konsekvensene. Dersom handlingene ikke får konsekvenser kan det føre til at de fortsetter slik de alltid har gjort. Det er likevel viktig med tillit i organisasjonen, slik at ansatte skal bli belønnet for å rapportere sikkerhetsrelatert informasjon (Hollnagel, 2014, s. 87). En annen mulig forklaring kan være at ansatte ikke har fått nok opplæring i sikkerhetsrutiner. I likhet med studien til Ruud (2011) viser det at ansatte i kommunene ikke hadde fått nok opplæring i forhold til systemene.

Informantene forteller derimot at det er en utfordring å skulle drive med opplæring av ansatte i kommunen fordi det er mange ulike sektorer. Det å nå over alle sektorer, og å få til den samme forståelsen over et så stort område, gir mange utfordringer. Det er vanligvis ikke nok å gjennomføre en gang, det er noe som bør følges opp jevnlig da det stadig er endring i utfordringer samt nye mennesker som kommer inn i organisasjonen. På en annen side er det også en utfordring at IKT-avdelingen blir forstått som adskilt fra kommunene, og i noen

tilfeller fortelles det at kommunen har ansvaret for sikkerhetskultur, mens IKT-avdelingen som er ekstern er ansvarlige for det tekniske. Dette kan bety at siden det ikke er IKT-avdelingen som er ansvarlige for sikkerhetskulturen, er vanskelig å kommunisere hva som er akseptable og ikke akseptable handlinger. Informantene forteller at de ikke har kontroll på hva som blir gjort av ansatte og at de heller ikke har myndighet til å bestemme over kommunene når IKT-avdelingen er eksterne. Toppledelsens forpliktelse er avgjørende for en god sikkerhetskultur (Choudhry et al., 2007). Det er dermed viktig at toppledelsen i arbeidet med cybersikkerhet kommuniserer hva som er akseptable og uakseptable handlinger.

7.0 Konklusjon

Formålet med denne studien er å se på hvordan kommuner arbeider med cybersikkerhet og om det har ført til endringer i kommunene etter cyberangrepet på Østre Toten i januar 2021. Det vil være hensiktsmessig for å se om kommunenes arbeid med cybersikkerhet er forsvarlig og muligens forstå hvilke utfordringer kommuner står ovenfor. Gjennom en kvalitativ forskningsmetode, innholdsanalyse, teori og diskusjon har studien fokusert på arbeidet med cybersikkerhet i norske kommuner for å kunne svare på oppgavens problemstilling som er:

«Hvordan er arbeidet med cybersikkerhet i norske kommuner, og har angrepet på Østre Toten ført til endringer?»

For å svare på denne problemstillingen har det blitt utformet 3 forskningsspørsmål som har blitt diskutert gjennom oppgaven. Det første forskningsspørsmålet er:

- **Hvordan påvirker ledelsesforankring arbeidet med cybersikkerhet?**

Funnene viser til at det kan virke som om det har vært en svak ledelsesforankring av arbeidet med cybersikkerhet før angrepet på Østre Toten. Årsakene til dette er blant annet at det for toppledelsen i kommunene har vært prioritert andre ting. Eksempler på dette er oppetid eller at de ansatte ikke har hatt nok ressurser. Det kan virke som om toppledelsen i kommunene ikke har hatt nok fokus på cybersikkerhet fordi de blant annet ikke har forstått risikoen ved uforsvarlig cybersikkerhet, og at det har vært holdninger som «det skjer ikke oss». Funnene kan også vise til at toppledelsen etter angrepet på Østre Toten har prioritert cybersikkerhet i større grad. De har forstått hvor stor risikoen kan være, og dermed tilført flere ressurser til arbeidet med cybersikkerhet. I tillegg vil funn som viser til at toppledelsen snur seg mot IKT-avdeling for hjelp kunne bety at toppledelsen forstår risikoen. Funnene viser også til endringer av plassering av IKT-leder og at IKT-ledere er invitert inn i styremøter. Dette kan bety at arbeidet med cybersikkerhet har blitt mer forsvarlig etter angrepet på Østre Toten. Tilhørende virker det som om ledelsesforankring påvirker arbeidet med cybersikkerhet, som følge av at det blir fortalt at det er blitt tilført mer ressurser og økt forståelse av toppledelsen i etterkant av angrepet på Østre Toten.

- **Forskningsspørsmål 2: Hvordan ligger risikostyring til grunn for arbeidet med cybersikkerhet i kommunene?**

Funnene tilsier at risikostyringen av cybersikkerhet i kommunene kan ha vært svak, spesielt før angrepet på Østre Toten. I kommunene er det tydelig at det ikke har vært implementert

beredskap for hendelser som cyberangrep. Det fremvises at risikooppfattelsen har påvirket ansattes arbeid med å styre risikoen, ettersom flere kommuner ikke har forstått hvor viktig det er å øve på cybersikkerhet for å oppdage sårbarheter og dermed være forberedt. Det fremkommer av funnene at de fleste av kommunene ikke har hatt øvelser før angrepet på Østre Toten. Samtidig kan det tilsynelatende virke som om de fleste kommunene har gjort endringer i arbeidet med risikostyringen av cybersikkerhet. Det kan vises gjennom at flere kommuner har planer om å implementere cybersikkerhet i beredskapsplanene, ha øvelser, implementere IKT-trusselbilde eller nylig har hatt øvelser.

Det kommer også frem at det har blitt tilført mer ressurser i arbeidet med risikostyringen, noe som kan vise til endringer i kommunenes arbeid med cybersikkerhet. Risikostyringen har ikke tatt høyde for måten kommunene er organisert på, ettersom flere av informantene forteller at det er komplisert å drive med cybersikkerhet i mange ulike sektorer. Det kan virke som om kommunene har utfordringer med å få tak i riktig ekspertise for å drive med forsvarlig risikostyring, ettersom at flere av informantene ønsker hjelp i arbeidet med cybersikkerhet. Risikostyringen i kommunene kan virke svak fordi de ikke har ikke har utført prosesser for å redusere sårbarheten på mer enn det tekniske. Ettersom kommunene arbeider med forbedring av arbeidet med cybersikkerhet kan det se ut som risikoforståelsen har endret seg og dermed risikostyringen blitt forbedret. Derved ligger risikostyringen til grunn for arbeidet med cybersikkerhet.

- **Forskningsspørsmål 3: Hvordan er sikkerhetskultur integrert i arbeidet med cybersikkerhet?**

Funnene viser at arbeidet med sikkerhetskulturen i kommunene er komplisert. Årsaken er blant annet at det er flere ulike sektorer med forskjellig kunnskap som gjør opplæring av ansatte vanskelig. For kommunene virker det utfordrende å ha en god sikkerhetskultur når det kommer til cybersikkerhet. Interessant funn er at det tilsynelatende kan virke som om ansatte i kommunene påvirkes av risikoforståelse fordi det handler mer om daglige gjøremål. Sikkerhetskulturen i kommunene kan vise til at det ikke har vært nok kunnskap. Likevel kan det virke som om kommunene har lærende kulturer, ettersom de fleste forteller om endringer i beredskap etter angrepet på Østre Toten. Det viser at kommunene er villige til å lære og at de arbeider med endring når de ser behovet. Funnene i denne studien viser også til at det muligens ikke er en tilstedeværende rapporteringskultur, ettersom ansatte har lav kunnskap og at det som følge av dette er vanskelig å rapportere. Når det kommer til rettferdig kultur virker

det som om toppledelsen i kommunene ikke har gått ut med akseptable og ikke akseptable handlinger, noe som kan ha ført til at de ikke har arbeidet med å ha en rettferdig kultur når det gjelder cybersikkerhet. Toppledelsen har tilført flere ressurser etter angrepet på Østre Toten, men de trenger likevel kompetansen til ansatte i IKT-avdelingen. Det viser at kommunene har en tilstedeværende fleksibel kultur. Det virker som toppledelsen har forstått hvor viktig det er med ressurser til IKT-avdelingen for å ha forsvarlig cybersikkerhetskultur i kommunene. Sikkerhetskulturen i forhold til cybersikkerhet virker dermed mangelfull gjeldende cybersikkerhet, og arbeidet er komplisert som følge av kommunenes organisering.

Dette hjelper meg med å svare på problemstillingen som er:

«Hvordan er arbeidet med cybersikkerhet i norske kommuner, og har angrepet på Østre Toten ført til endringer?»

Arbeidet med cybersikkerhet i kommunene er komplisert på bakgrunn av at det er flere ulike sektorer og risikoforståelsen har vært «det skjer ikke oss». Et viktig funn som virker gjennomgående i denne studien er at ledelsesforankring påvirker arbeidet med cybersikkerhet. Dette kommer av at det samtidig som det beskrives om endringer i toppledelsen, også er endringer i flere forbyggende aktiviteter i arbeidet med cybersikkerhet. I tillegg kan det se ut som risikoforståelsen har påvirket kommunenes arbeid med cybersikkerhet, av den grunn at risikostyringen tilsynelatende har endret seg etter angrepet på Østre Toten. Arbeidet med sikkerhetskultur gjeldende cybersikkerhet er likevel komplisert, men det arbeides stadig mot forbedring. Dernest kan det virke som om arbeidet med cybersikkerhet i kommunene er utfordrende og mangelfullt, men at angrepet på Østre Toten kan ha ført til endringer.

7. 1 Veien videre

Videre interessant forskning kunne være å gå i dybden av de ulike temaene og se om slike hendelser som Østre Toten fører til atferdsendring i arbeidet med cybersikkerhet over tid, og om det har vært konkrete tiltak basert på arbeidet med cybersikkerhet.

En annen forskning som kunne være relevant å se på er hvordan arbeidet med cybersikkerhet er i kommunene med et annet utvalg av informanter. Utvalget kunne bestått av informanter fra ulike sektorer, som skole, vann og avløp, toppledelsen og de som arbeider med beredskap i kommunene. Ved sammenheng fra flere sektorer ville det vært mulig å få et større bilde på hvordan arbeidet med cybersikkerhet er i kommunene, og man får flere perspektiver.

Litteraturliste

Armenia, S., Ferreira Franco, E., Nonino, F., Spagnoli, E. & Medaglia, C. M. (2019). Towards the Definition of a Dynamic and Systemic Assessment for Cybersecurity Risks. *Systems research and behavioral science, 36*(4), 404-423. https://doi.org/10.1002/sres.2556

Aven, T. (2006). On the Precautionary Principle, in the Context of Different Perspectives on Risk. *Risk management (Leicestershire, England), 8*(3), 192-205. https://doi.org/10.1057/palgrave.rm.8250010

Aven, T. (2008a). *Risk Analysis: Assessing Uncertainties Beyond Expected Values and Probabilities* (1. utg.). New York: New York: John Wiley & Sons, Incorporated.

Aven, T. (2008b). A semi-quantitative approach to risk analysis, as an alternative to QRAs. *Reliability engineering & system safety, 93*(6), 790-797. https://doi.org/10.1016/j.ress.2007.03.025

Aven, T. (2011). On Some Recent Definitions and Analysis Frameworks for Risk, Vulnerability, and Resilience. *Risk Anal, 31*(4), 515-522. https://doi.org/10.1111/j.1539-6924.2010.01528.x

Aven, T. (2015). *Risikostyring : grunnleggende prinsipper og ideer* (2. utg. utg.). Oslo: Universitetsforl.

Aven, T. & Renn, O. (2010). *Risk Management and Governance: Concepts, Guidelines and Applications*. Berlin, Heidelberg: Berlin, Heidelberg: Springer Berlin Heidelberg.

Aven, T. & Renn, O. (2012). On the Risk Management and Risk Governance of Petroleum Operations in the Barents Sea Area. *Risk Anal, 32*(9), 1561-1575. https://doi.org/10.1111/j.1539-6924.2011.01777.x

Bellot, J. (2011). Defining and Assessing Organizational Culture. *Nurs Forum, 46*(1), 29-37. https://doi.org/10.1111/j.1744-6198.2010.00207.x

Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia economics and finance, 28*, 24-31. https://doi.org/10.1016/S2212-5671(15)01077-1

Branch, J. (2021). What's in a Name? Metaphors and Cybersecurity. *Int Org, 75*(1), 39-70. https://doi.org/10.1017/S002081832000051X

Chapman, T. A. & Reithel, B. J. (2021). Perceptions of Cybersecurity Readiness among Workgroup IT Managers. *The Journal of computer information systems, 61*(5), 438-449. https://doi.org/10.1080/08874417.2019.1703224

Chase, R. E. (2015). *Security leader insights for risk management : lessons and strategies from leading security professionals*. Amsterdam, Netherlands: Elsevier.

Cheng, J. Y.-J. & Groysberg, B. (2019). Cybersecurity: The Insights You Need from Harvard Business Review. I *HBR Insights Series* (s. 176). La Vergne: La Vergne: Harvard Business Review Press.

Choodakowska, A., Kandula, S. & Przybylska, J. (2022). Cybersecurity in the Local Government Sector in Poland: More Work Needs to be Done. *Lex localis-journal of local self-government, 20*(1), 161-192. https://doi.org/10.4335/20.1.161-192(2022)

Choudhry, R. M., Fang, D. & Mohamed, S. (2007). The nature of safety culture: A survey of the state-of-the-art. *Safety science, 45*(10), 993-1012. https://doi.org/10.1016/j.ssci.2006.09.003

Craigen, D., Diakun-Thibault, N. & Purse, R. (2014). Defining Cybersecurity. *Technology innovation management review, 4*(10), 13-21. https://doi.org/10.22215/timreview/835

Crichton, D. (2002). UK and Global Insurance Responses to Flood Hazard. *Water international, 27*(1), 119-131. https://doi.org/10.1080/02508060208686984

Crichton, D. (2008). Role of Insurance in Reducing Flood Risk. *Geneva papers on risk and insurance. Issues and practice, 33*(1), 117-132. https://doi.org/10.1057/palgrave.gpp.2510151

Departementene. (2019). *Nasjonal strategi for digital sikkerhet*. Hentet fra https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/nasjonal-strategi-for-digital-sikkerhet.pdf

Digitaliseringsdirektoratet. (2022). *Ledelsens styring og oppfølging*. Hentet fra https://www.digdir.no/informasjonssikkerhet/ledelsens-styring-og-oppfolging/3044

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

Galinec, D., Možnik, D. & Guberina, B. (2017). Cybersecurity and cyber defence: national level strategic approach. *Automatika, 58*(3), 273-286. https://doi.org/10.1080/00051144.2017.1407022

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W. & Spiegel, J. (2012). The Law of Cyber-Attack. *California law review, 100*(4), 817-885.

Helsetilsynet. (2020). *Hvordan er sykehusene forberedt på IKT-bortfall?* (3). Hentet fra https://www.helsetilsynet.no/globalassets/opplastinger/publikasjoner/rapporter2020/helsetilsynetrapport3_2020.pdf

Hollnagel, E. (2014). *Safety-I and safety-II: the past and future of safety management* (1. utg.). Farnham: Farnham: Ashgate Publishing Ltd.

Hovik, S. & Inger Marie, S. (2004). Kommunal organisering 2004. I: Oslo: Norsk institutt for by- og regionforskning.

Jacobsen, D. I. (2009). *Perspektiver på kommune-Norge : en innføring i kommunalkunnskap*. Bergen: Fagbokforl.

Jacobsen, D. I. (2015). *Hvordan gjennomføre undersøkelser? : innføring i samfunnsvitenskapelig metode* (3. utg. utg.). Oslo: Cappelen Damm akademisk.

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

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y. & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International journal of information management*, *23*(2), 139-154. https://doi.org/10.1016/S0268-4012(02)00105-6

Kessel, D. & Røsrud, K. (2021, 08.02.2021). Østre Toten har vært uten datasystemer en måned etter hacking. Hentet fra https://www.nrk.no/innlandet/kan-ta-et-halvt-ar-for-ostre-toten-a-rette-opp-dataangrep-1.15364106

Knapp, K. J., Franklin Morris, R., Marshall, T. E. & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & security*, *28*(7), 493-508. https://doi.org/10.1016/j.cose.2009.07.001

Knuth, D., Kehl, D., Hulse, L. & Schmidt, S. (2014). Risk Perception, Experience, and Objective Risk: A Cross-National Study with European Emergency Survivors. *Risk analysis*, *34*(7), 1286-1298. https://doi.org/10.1111/risa.12157

Kommune-CSIRT. (2020). *Digitalt situasjonsbilde* (01). Hentet fra https://kommunecsirt-no.offcenit.com/Digitalt-situasjonsbilde-K-CSIRT-no.1-2020-final.pdf?mtime=20210119141525&focal=none

KPMG. (2018). Stadig flere norske virksomheter usettes for cyberangrep: 7 av 10 skylder på tilfheldigheter og uflaks. Hentet 06.04.2022 fra https://kommunikasjon.ntb.no/pressemelding/stadig-flere-norske-virksomheter-utsettes-for-cyberangrep-7-av-10-skylder-pa-tilfeldigheter-og-uflaks?publisherId=16282382&releaseId=17853618

KPMG. (2021). *IKT-sikkerhet i Østre Toten kommune forut for angrepet 9.januar 2021* (1). Hentet fra https://www.ototen.no/_f/p1/i5689ceb7-72b4-44d0-970c-a5c4828047e5/offentlig-versjon.pdf

Langø, H.-I. & Sandvik, K. B. (2013). Cyberspace og sikkerhet. *Internasjonal politikk, 71*(2), 221-228. https://doi.org/10.18261/ISSN1891-1757-2013-02-05

Lewallen, J. (2021). Emerging technologies and problem definition uncertainty: The case of cybersecurity. *Regulation & governance, 15*(4), 1035-1052. https://doi.org/10.1111/rego.12341

Ma, Y., Liu, Y., Appolloni, A. & Liu, J. (2021). Does green public procurement encourage firm's environmental certification practice? The mediation role of top management support. *Corporate social-responsibility and environmental management, 28*(3), 1002-1017. https://doi.org/10.1002/csr.2101

Marvell, S. (2015). Real-Time Cyber Security Risk Management. *ITNow, 57*(4), 26-27. https://doi.org/10.1093/itnow/bwv097

Mehiriz, K. & Gosselin, P. (2016). Municipalities' preparedness for weather hazards and response to weather warnings. *PLoS One, 11*(9), e0163390-e0163390. https://doi.org/10.1371/journal.pone.0163390

Miles, M. B., Huberman, A. M. & Saldaña, J. (2020). *Qualitative data analysis : a methods sourcebook* (Fourth edition. utg.). Los Angeles, Calif: SAGE.

Nasjonal Sikkerhetsmyndighet. (2022). *Risiko 2022*. Hentet fra https://nsm.no/getfile.php/137798-1644424185/Filer/Dokumenter/Rapporter/NSM_rapport_final_online_enekeltsider.pdf

Njå, O., Sommer, M., Rake, E. L. & Braut, G. S. (2020). *Samfunnssikkerhet : analyse, styring og evaluering*. Oslo: Universitetsforlaget.

NorSIS. (2021). *Trusler og trender 2021*. Hentet fra https://norsis.no/wp-content/uploads/2021/03/NorSIS_Trusler_Trender_2021_Digital.pdf

NOU 2000: 24. (2000). *Et sårbart samfunn*. Hentet fra https://www.regjeringen.no/contentassets/1c557161b3884335b4f9b89bbd32b27e/no/pdfa/nou200020000024000dddpdfa.pdf

NOU 2015: 13. (2015). *Digital sårbarhet- sikkert samfunn*. Hentet fra https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf

NVE. (2017). *Regulering av IKT-sikkerhet*. Hentet fra https://publikasjoner.nve.no/rapport/2017/rapport2017_26.pdf

Perry, R. W. & Lindell, M. K. (2003). Preparedness for Emergency Response: Guidelines for the Emergency Planning Process. *Disasters, 27*(4), 336-350. https://doi.org/10.1111/j.0361-3666.2003.00237.x

Pidgeon, N. (1998). Risk assessment, risk values and the social science programme: why we do need risk perception research. *Reliability engineering & system safety, 59*(1), 5-15. https://doi.org/10.1016/S0951-8320(97)00114-2

Politiets Sikkerhetstjeneste. (2022). *Nasjonal trusselvurdering 2022*. Hentet fra https://www.pst.no/alle-artikler/trusselvurderinger/ntv-2022/

Pritchard, C. L. (2015). *Risk management : concepts and guidance* (Fifth edition. utg.). Boca Raton: CRC Press, Taylor & Francis Group.

Rausand, M. & Utne, I. B. (2022). *Risikoanalyse : teori og metoder* (2. utgave. utg.). Bergen: Fagbokforlaget.

Reason, J. (1997). *Managing the Risks of Organizational Accidents* (1. utg.)Taylor & Francis.

Ruud, J.-K. (2011). *Hva skjer med journalen min? Hvilke faktorer er det som bidrar til, eller hindrer en sikker behandling av sensitive opplysninger i kommunen?* (Masteroppgave, Universitetet i Stavanger). University of Stavanger, Norway. Hentet fra https://uis.brage.unit.no/uis-xmlui/bitstream/handle/11250/184592/Hva%20skjer%20med%20journalen%20min%2c%20masteroppgave%20Jan-K%c3%a5re%20Ruud.pdf?sequence=1&isAllowed=y

Sjoberg, L. (2000). Factors in risk perception. *Risk Anal, 20*(1), 1-11. https://doi.org/10.1111/0272-4332.00001

Skotnes, R. Ø. (2015). Management commitment and awareness creation - ICT safety and security in electric power supply network companies. *Information and computer security, 23*(3), 302-316. https://doi.org/10.1108/ICS-02-2014-0017

Slovic, P. (1987). Perception of risk, 280-285. https://doi.org/info:doi/

Slovic, P., Fischhoff, B. & Lichtenstein, S. (2005). Facts and fears: understanding perceived risk (1979). *Policy and practice in health and safety, 3*(2), 65.

Thagaard, T. (2018). *Systematikk og innlevelse : en innføring i kvalitative metoder* (5. utg. utg.). Bergen: Fagbokforl.

Thong, J. Y. L., Yap, C.-S. & Raman, K. S. (1996). Top Management Support, External Expertise and Information Systems Implementation in Small Businesses. *Information systems research, 7*(2), 248-267. https://doi.org/10.1287/isre.7.2.248

Tjora, A. H. (2017). *Kvalitative forskningsmetoder i praksis* (3. utg. utg.). Oslo: Gyldendal akademisk.

Uchendu, B., Nurse, J. R. C., Bada, M. & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & security, 109*, 102387. https://doi.org/10.1016/j.cose.2021.102387

Vatnelid, I. L. (2018). *Risiko : en innføring i god praksis*. Oslo: Gyldendal.

von Solms, R. & van Niekerk, J. (2013). From information security to cyber security. *Computers & security, 38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

von Solms, R. & von Solms, S. H. (2006). Information Security Governance: A model based on the Direct–Control Cycle. *Computers & security, 25*(6), 408-412. https://doi.org/10.1016/j.cose.2006.07.005

Wirtz, B. W. & Weyerer, J. C. (2017). Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats. *International journal of public administration, 40*(13), 1085-1100. https://doi.org/10.1080/01900692.2016.1242614

World Economic Forum. (2022). *The Global Risks Report 2022* (17th edition). Hentet fra https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

Young, R. & Poon, S. (2013). Top management support—almost always necessary and sometimes sufficient for success: Findings from a fuzzy set analysis. *International journal of project management, 31*(7), 943-957. https://doi.org/10.1016/j.ijproman.2012.11.013

Oversikt over vedlegg

-Vedlegg A: Intervjuguide

-Vedlegg B: Informasjonsskriv

-Vedlegg C: Godkjenning fra NSD

Vedlegg A: Intervjuguide

Intervjuguide

Først og fremst, samtykker du til at jeg tar opp dette intervjuet?

Del 1. Uformell Prat

Bakgrunn

Hvor lenge har du jobbet? Hva jobber du som? Hva er din stillingstittel?

1. **Digitalisering**

Hvordan jobber dere med digitaliseringen?

I hvilken grad er det opplæring for ansatte? Med/uten systemer.

Hvordan ville dere jobbet uten disse systemene?

2. **Ledelse og cybersikkerhet**

Hvordan jobber ledelsen med cybersikkerhet?

Fortelle litt om ledelsens arbeid med cybersikkerhet? (Prioritet, engasjerte, ansvar)

Og hvordan har dette endret seg etter angrepet? (Østre Toten, ledelsestrender, endringer?)

3. **Beredskap**

Gjennomgang? Hvordan er det lagt opp til å håndtere cyberangrep?

Hvordan forbereder dere på cyberangrep/cybertrusler? Nevn litt om beredskap. (Øvelser, IKT-trusselbildet, Gjenoppretting)

Varslingssystemer, Informasjonsflyt

Kan du forklare beredskap før og etter angrep Østre Toten? (endringer, tiltak)

Hvordan jobber dere reaktivt eller proaktivt med cybersikkerhet?

Øvelser?

4. **Sikkerhetskultur**

-Ansatte kompetanse? Utfordringer? Øke bevissthet? Før vs. Etter Østre Toten.

5. **Sårbarheter**

Etter din mening; hva er den største sårbarheten?

Organisatorisk: risikovurderinger? Ofte? Hva innebærer den?

Hva er de organisatoriske sårbarhetene?

Menneskelige: hvordan tar dere høyde for menneskelige sårbarheter?

Teknologiske: Kontroll av tilgang til systemer?

6. **Fremtiden**

Hvordan arbeider dere for å være forberedt? (Ny teknologi, tiltak)

Noe mer du vil tilføye?

7. **Ekstramateriale**

Kjenner dere til angrepene på Østre Toten kommune?

Hvordan kommuniserte de dette? (Rapporter, media)

Hva mener du vi kan lære av situasjonene til Østre Toten?

Vedlegg B: Informasjonsskriv

Deltakelse i forskningsprosjektet «Cybersikkerhet i norske kommuner»

Dette er et spørsmål til deg om å delta i et masterprosjekt hvor formålet er å undersøke de organisatoriske forutsetningene for cybersikkerhet i kommunen. Jeg er i denne sammenheng opptatt av om kommuner arbeider med cybersikkerhet, og hvilke utfordringer de står ovenfor. I dette skrivet blir det gitt informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Denne studien tar for seg den foreløpige problemstillingen: «Hvordan er arbeidet med cybersikkerhet i norske kommuner?» Med denne problemstillingen vil jeg undersøke hvordan kommuner arbeider med cybersikkerhet og muligens hvilke utfordringer de står ovenfor.

I dette prosjektet er formålet å få innblikk i hvordan det står til med cybersikkerheten i kommuner i Norge i dag. Dette vil innebære for kommunen å få en oversikt over trusselbildet og hvordan de ulike lederne arbeider med sikkerheten. Jeg skal undersøke hvor motstandsdyktige de er og hvordan de jobber med beredskapsplan tilhørende cybersikkerhet.

Hvem er ansvarlig for forskningsprosjektet?

Forskningsprosjektet er laget ved Nord Universitet, og Nord Universitet er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?

Jeg kontakter deg fordi du er ansatt hos kommunen eller arbeider innenfor drift av kommunens IT-systemer.

Hva innebærer det for deg å delta?

- Hvis du godtar invitasjonen om å delta i prosjektet vil du bli intervjuet av meg Nina Danielsen.
- Intervjuet gjennomføres over zoom eller teams, med mindre noe annet avtales.
- Intervjuet vil sannsynlig ta minst 60 minutter.

- Intervjuet blir tatt opp med en opptaker og transkriberes i en helhet. Spørsmålene som vil bli stilt handler om digitalisering, ledelse, beredskap, sikkerhetskultur, sårbarheter og fremtiden.
  Jeg er innforstått med at informasjon rundt kommunens arbeid med cybersikkerhet kan være konfidensiell informasjon om samfunnskritisk infrastruktur, og at det derfor kan være visse begrensninger i hvilken grad informanter kan gi informasjon om dette temaet.

Dine rettigheter

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

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

Det er frivillig å delta

Det er frivillig om en velger å delta i prosjektet eller ei. Velger en å delta, kan man når som helst trekke samtykke tilbake uten at det er nødvendig å gi en begrunnelse for dette. Opplysninger om deg som informant vil bli anonymisert og det vil ikke ha negative konsekvenser for deg om du ikke vil delta eller senere velger å trekke deg.

-Jeg vil bare bruke opplysningene om deg til formålene jeg har fortalt om i dette skrivet. Jeg behandler opplysningene konfidensielt og i samsvar med personregelverket.

-Ditt personvern- hvordan dine opplysninger blir oppbevart og brukt

- Det er kun jeg, Nina Louise Danielsen og min veileder, Harald Fardal, ved Nord Universitet, som har tilgang på opplysningene om deg.

-Jeg vil ta opptak av intervjuet, men det vil bli slettet ved prosjektslutt.

-Navnet og kontaktopplysningene dine vil jeg erstatte med en kode som lagres på egne navneliste adskilt fra øvrige data.

-Konfidensialitet opprettholdes ved at datamaterialet krypteres for at informasjonen ikke skal kunne leses av uvedkommende.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?

Prosjektet vil etter planen avsluttes den 18.mai 2022. Ved prosjektslutt vil alle personopplysninger, opptak og transkripsjoner slettes.

Hvordan kan du finne ut mer?

Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:

Meg; Nina Louise Danielsen, på e-post: ninalouisedan@hotmail.com
eller telefon: 47419434

Min veileder, Harald Fardal: Dsb. E-post: Harald.Fardal@dsb.no eller telefon: +47 90 60 65 86

Vårt personvernombud: Toril Irene Kringen. Epost: personvernombud@nord.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 telefon: 53211500

Med vennlig hilsen

Nina Louise Danielsen
Student, Nord Universitet

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet «Hvordan er arbeidet med cybersikkerhet i norske kommuner?», og har fått anledning til å stille spørsmål. Jeg samtykker til å delta i intervju og til at mine opplysninger behandles frem til prosjektet er avsluttet i mai 2022.

(Signert av prosjektdeltaker, dato)

Vedlegg C: Godkjenning fra NSD

NSD NORSK SENTER FOR FORSKNINGSDATA

Vurdering

Referansenummer

308665

Prosjekttittel

Hvordan er mindre kommuner i Norge forberedt på cyberangrep

Behandlingsansvarlig institusjon

Nord Universitet / Fakultet for samfunnsvitenskap / Velferd og sosiale relasjoner

Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)

Harald Fardal, Harald.Fardal@dsb.no, tlf: +4733412523

Type prosjekt

Studentprosjekt, masterstudium

Kontaktinformasjon, student

Nina Louise Danielsen, ninalouisedan@hotmail.com, tlf: 47419434

Prosjektperiode

20.10.2021 - 17.05.2022

Vurdering (1)

15.12.2021 - Vurdert

Det er vår vurdering at behandlingen av personopplysninger i prosjektet vil være i samsvar med personvernlovgivningen så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjemaet med vedlegg 15.12.21, samt i meldingsdialogen mellom innmelder og NSD. Behandlingen kan starte.

TYPE OPPLYSNINGER OG VARIGHET
Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til 17.05.2022.

LOVLIG GRUNNLAG
Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres, og som den registrerte kan trekke tilbake. Lovlig grunnlag for behandlingen vil dermed være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a.

PERSONVERNPRINSIPPER

NSD vurderer at den planlagte behandlingen av personopplysninger vil følge prinsippene i personvernforordningen om:

• lovlighet, rettferdighet og åpenhet (art. 5.1 a), ved at de registrerte får tilfredsstillende informasjon om og samtykker til behandlingen
• formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke viderebehandles til nye uforenlige formål
• dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet
• lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet

DE REGISTRERTES RETTIGHETER
NSD vurderer at informasjonen om behandlingen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13.

Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18) og dataportabilitet (art. 20).

Vi minner om at hvis en registrert tar kontakt om sine rettigheter, har behandlingsansvarlig institusjon plikt til å svare innen en måned.

FØLG DIN INSTITUSJONS RETNINGSLINJER
NSD legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32).

Ved bruk av databehandler (spørreskjemaleverandør, skylagring eller videosamtale) må behandlingen oppfylle kravene til bruk av databehandler, jf. art 28 og 29. Bruk leverandører som din institusjon har avtale med.

For å forsikre dere om at kravene oppfylles, må dere følge interne retningslinjer og eventuelt rådføre dere med behandlingsansvarlig institusjon.

MELD VESENTLIGE ENDRINGER
Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til NSD ved å oppdatere meldeskjemaet. Før du melder inn en endring, oppfordrer vi deg til å lese om hvilke type endringer det er nødvendig å melde: https://www.nsd.no/personverntjenester/fylle-ut-meldeskjema-for-personopplysninger/melde-endringer-i-meldeskjema Du må vente på svar fra NSD før endringen gjennomføres.

OPPFØLGING AV PROSJEKTET
NSD vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Kontaktperson hos NSD: Sturla Herfindal

Lykke til med prosjektet!