Universitetet i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering: Master i Samfunnssikkerhet	Vårsemesteret, 2021 Åpen
Forfatter: Sanna Blakkestad	
Fagansvarlig: Henrik Kvadsheim Veileder: Henrik Kvadsheim	
Tittel på masteroppgaven: Bevissthet rundt cybersikkerhet i kommunal sektor - En kvalitativ studie av hvordan ulike former for opplæring og trening påvirker ansattes bevissthet rundt cybersikkerhet. Engelsk tittel: Awareness of cybersecurity in the municipal sector – A qualitative study of how various forms of education and training affect employee´s awareness of cybersecurity.	
Studiepoeng: 30	
Emneord: Cybersikkerhet, bevissthet, situasjonsbevissthet, læring, kunnskap, kompetanse, opplæring, kommunal sektor, sikkerhetskultur, un-rocked boat.	Sidetall: 60 + vedlegg/annet: 74 Stavanger, 13.07.2021

Bevissthet rundt cybersikkerhet i kommunal sektor

En kvalitativ studie av hvordan ulike former for opplæring og trening påvirker ansattes bevissthet rundt cybersikkerhet.

Masterstudium i Samfunnssikkerhet

Universitetet i Stavanger

Vår 2021

Sanna Blakkestad

FORORD

Denne oppgaven markerer slutten på min toårige masterstudie i Samfunnssikkerhet ved Universitetet i Stavanger. Det har vært to utfordrende og ikke minst lærerike år. Spesielt siste semester og masteroppgaven har vært krevende, men også utrolig spennende.

Jeg vil rette en stor takk til alle som har bidratt til at denne oppgaven ble til. Takk til min veileder, Henrik Kvadsheim, for gode diskusjoner og veiledning gjennom hele løpet. Takk til alle informanter som stilte til intervju, delte kunnskap og bidro med spennende innsikt i oppgavens tematikk.

Sanna Blakkestad
Stavanger, 13.07.2021

SAMMENDRAG

Norge er et av verdens mest digitaliserte land. Den digitale utviklingen har skutt fart de siste tiårene, noe som ikke bare medfører nye muligheter og gevinster, men også nye utfordringer og sårbarheter. Denne studien ønsker å belyse hvordan kommunesektoren håndterer denne utviklingen ved å studere deres opplæring og trening med hensyn til cybersikkerhet. Formålet med studien er videre å fokusere på hvordan kommunens bruk av opplæring og trening påvirker de ansattes bevissthet rundt cybersikkerhet, samt hvilke utfordringer som hemmer dette arbeidet. På bakgrunn av dette er følgende problemstilling lagt til grunn:

«Hvordan jobber kommunesektoren med opplæring og trening innenfor cybersikkerhet, hvilke utfordringer hemmer dette arbeidet - og hvilke implikasjoner har det for de ansattes bevissthet rundt cybersikkerhet?»

For å besvare problemstillingen har kommunens interne, skriftlige dokumenter blitt analysert. Det er også utført dybdeintervjuer med fem ansatte i ulike tjenesteområder i kommunen som jobber med cybersikkerhet på daglig basis. Gjennom intervjuene har de delt sin erfaring og kunnskap om opplæringen og treningen som gjennomføres i kommunens ulike tjenesteområder. Resultatene fra dokumentanalysen og intervjuene vil diskuteres i lys av teori om kunnskap, kompetanse, læring, bevisstgjøring, situasjonsbevissthet, sikkerhetskultur og «un-rocked boat». Disse brukes for å belyse hvilke implikasjoner kommunens arbeid med opplæring og trening har for de ansattes bevissthet rundt cybersikkerhet. Utfordringer som hemmer dette arbeidet, vil også diskuteres i lys av «un-rocked boat» teorien.

Studien avdekker at kommunen benytter seg av flere ulike tiltak for opplæring og trening. Disse tiltakene inkluderer sikkerhetsreglement, taushetserklæring, kurs, tester, nyhetssaker og diskusjon. Samtidig er det mangel på tilpasning av opplærings- og treningsopplegg for ulike ansatte med forskjellige behov, og for ulike avdelinger med forskjellige problemstillinger, grunnet mangel på ressurser. Resultatet av studien viser likevel til at de ovennevnte tiltakene er effektive for å øke de ansattes bevissthet. Studien konkluderer også med at de tiltakene som krever størst grad av aktiv deltakelse, og som dermed er mest effektive for å øke bevissthet, gjennomføres svært sjelden. Det kan derfor settes spørsmål ved hvor varig effekten av disse tiltakene er, ettersom cybersikkerhet er et område med rask teknologisk utvikling som krever kontinuerlig opplæring og trening for å opprettholde de ansattes bevissthet rundt cybersikkerhet.

Innholdsfortegnelse

Figuroversikt

Tabelloversikt

1 Innledning

1.1 Bakgrunn

De siste tiårene har vi sett store teknologiske endringer i samfunnet. Med den økte digitaliseringen kommer nye muligheter og gevinster, men også nye sårbarheter og utfordringer (NOU, 2015:13, s. 43). Innen året 2020 estimerte EU-kommisjonen at 90 prosent av jobbene innenfor EU ville kreve digitale ferdigheter. De fleste i dag har en viss forståelse for hvordan en sikrer informasjon i papirbaserte, manuelle prosesser, men den økte digitaliseringen av lagring av informasjon har ført til en fremmedgjøring som krever opplæring og forståelse i større grad enn tidligere (NOU, 2015:13, s. 43). I den nye digitale hverdagen øker kommunenes avhengighet av informasjons- og kommunikasjonsteknologi (IKT) for produksjon og leveranse av kommunale tjenester, samtidig øker også de digitale truslene og sårbarhetene både i omfang og alvorlighetsgrad. NorSIS utførte i 2017 en utredning av kommuners håndtering av informasjonssikkerhet, og resultatet av den viste til at det er et stort behov for å styrke kompetanse på dette området (Gjøvikregionen, u.å.).

I dag krever nesten enhver jobb en form for teknologiske ferdigheter, både i det daglige arbeidet samt for å beskytte seg mot cyberkriminelle aktører. Dette har ført til et krav om mer kompetanse rundt forsvarlig bruk av IKT-systemer og ulike cyberangrepsmetoder en må være bevisst på. De profesjonelle, kriminelle aktørene blir også stadig flinkere på å pakke inn truslene slik at de ser mer pålitelige ut. Bevissthet og sikkerhetsforståelse blant ansatte er derfor stadig viktigere for å klare å plukke opp forsøk på cyberangrep for å forhindre å bli offer for blant annet phishing-mail[1]. Dette krever opplæring og trening på et nivå som passer alle ansatte, ikke bare de med spesialkompetanse innenfor IT (NSR, 2020, s. 78).

«Mennesket er det svakeste leddet» er et kjent ordtak og beskriver hvor viktig det er å sikre den menneskelige delen av organisasjonen, ikke bare den tekniske, når det kommer til den overordnede cybersikkerheten. Det er dokumentert at manglende ledelsesforankring, menneskelige feilhandlinger og manglende bevissthet er årsaken til uønskede IKT-hendelser (NOU, 2015:13, s. 53). Fra mørketallsundersøkelsen (2020, s. 6) fremkommer det også at blant de som utsettes for sikkerhetsbrudd mener halvparten at det skyldes menneskelig feil, og hele 39 prosent anser mangel på sikkerhetsbevissthet blant de ansatte som det største

[1] Se underkapittel 2.5 for beskrivelse av begrepet

problemet. For å kunne opptre sikkert i en stadig mer digitalisert hverdag er det derfor en forutsetning at ansatte i virksomheter har grunnleggende ferdigheter om hvordan en bruker IKT-systemer på en forsvarlig måte (NOU, 2015:13, s. 44).

Denne oppgaven vil fokusere særlig på begrepet bevissthet og hvordan en kan oppnå bevissthet rundt cybertrusler i kommunesektoren. Med bevissthet menes menneskets evne til å oppleve, registrere og sanse hva som foregår i ens omgivelser (Hansen, 2020). Opp imot cybertrusler vil det si å være i stand til å eksempelvis gjenkjenne en phishing-mail eller oppdage om noe virker mistenkelig i løpet av arbeidsdagen. Dette kan være krevende å opprettholde til enhver tid samtidig med andre krevende arbeidsoppgaver. Informasjonssikkerhet eller cybersikkerhet er tidligere noe en har assosiert med IT-avdelingen, men i dag interagerer nesten alle ansatte i organisasjonen med IT-systemer på en eller annen måte. Dette krever bevissthet, kompetanse og ferdigheter om en vil unngå uheldige og uønskede hendelser. For å utvikle disse ferdighetene og den nødvendige kompetansen kreves det tilrettelagt opplæring og trening for de ansatte.

1.1.1 Avgrensning

Oppgaven undersøker hvilke implikasjoner den aktuelle kommunens arbeid med opplæring og trening har for de ansattes bevissthet rundt cybersikkerhet. Studien avgrenses dermed kun til å se på kommunesektoren. Denne sektoren ble valgt grunnet en hypotese om at offentlig sektor har et større krav til åpenhet og tilgjengelighet enn privat sektor, samt en mangel på digital kompetanse (SSB, 2019). Videre valgte jeg å fokusere på én stor kommune i Norge slik at jeg kunne gå dypere inn i kommunen, dens ulike avdelinger, og hvordan de jobber med cybersikkerhet og opplæring for å få et godt overblikk på tvers av tjenesteområder.

Ettersom oppgaven omhandler de ansattes *bevissthet* rundt cybersikkerhet og cybertrusler, fokuseres det ikke på de tekniske tiltakene eller aspektene ved cybersikkerhet. Oppgaven vil kun konsentrere seg om den menneskelige faktoren. Jeg vil heller ikke forsøke å måle dagens trusselbevissthet rundt cybersikkerhet eller å måle effekten ulike opplærings- og treningsopplegg har på de ansattes bevissthet. Oppgaven vil heller sannsynliggjøre hvordan de ansattes bevissthet påvirkes gjennom de ulike opplærings- og treningstiltakene kommunen kjører i dag, ved hjelp av oppgavens teoretiske rammeverk.

1.2 Faglig relevans

Norge er et av verdens mest digitaliserte land, og koronapandemien har bidratt til å forsterke dette i enda større grad. Som følge av pandemien antas det at den digitale utviklingen er fremskyndet med tre år i samfunnet som helhet. Denne utviklingen er positiv, men kommer ikke uten risiko og sårbarheter som må håndteres. Det er derfor enda viktigere at vi nå sørger for at ansatte i virksomheter utvikler kompetanse og bevissthet rundt cybersikkerhet ettersom trusselbildet er i konstant endring (NSR, 2020, s. 4).

Denne økte kompleksiteten i det digitale domenet fører med seg utfordringer både på lokalt og regionalt nivå. Håndteringen av de store endringene i trusselbildet og dets kompleksitet er særlig utfordrende for kommunesektoren som består av mange små enheter som har ansvar for viktige systemer og tjenester i samfunnet. Spesielt ettersom det i kommunesektoren er mangel på kompetanse innenfor cybersikkerhet, samtidig som kommunene har veldig mange ansatte med svært ulik bakgrunn, kunnskap og erfaring (NOU 2015:13, s. 250). Utfordringen med å nå ut til alle ansatte og øke deres bevissthet rundt cybersikkerhet tilstrekkelig kan derfor være særlig stor i denne sektoren.

1.3 Tidligere forskning

I dette kapittelet redegjøres det for tidligere forskning som har relevans for oppgavens tematikk. Cybersecurity Insiders utførte i 2018 en kartlegging av virksomheters syn på «insider threats». Dette fordi de mener at alt for mange assosierer «insider threats» med en ondsinnet aktør, men i realiteten er ansatte som uten hensikt utfører en feilhandling den største årsaken til uønskede cyberhendelser. Rapporten viser til at virksomheter er like bekymret for tilsiktede dataangrep som uaktsomme, utilsiktete handlinger fra ansatte. Det fremkommer også av rapporten at for tredje år på rad oppgis mangel på trening og ekspertise som den største barrieren for å bedre risikostyring av «insider threats». Rapporten konkluderer blant annet med at forebygging gjennom økt bevissthet er det viktigste fokusområdet for å forsvare seg mot at ansatte utfører feilhandlinger som kan øke risikoen for uønskede cyberhendelser (Cybersecurity Insiders, 2008).

Choi, Kim, Goo & Whitmore (2008) skriver i sin artikkel «Knowing is doing» om hvordan informasjonssystemer har penetrert alle aspekter ved dagens virksomheter, og hvordan dette krever sikring i større grad enn tidligere. De vektlegger bevissthet mot cybertrusler som den

første barrieren mot uønskede cyberhendelser og mener det er den viktigste faktoren for suksess i å beskytte virksomhetens informasjonssystemer. For å øke bevisstheten mot cybertrusler nevnes følgende tiltak: utvikle prosedyrer og retningslinjer, sørge for at de ansatte er oppmerksomme på gjeldende prosedyrer og retningslinjer, samt viktigheten av trening og opplæring. Denne artikkelen la føring for oppgavens fokus på trening og opplæring, samt interne skriftlige dokumenter som sentrale faktorer for økt bevissthet.

I artikkelen «Organizational security culture: embedding security awareness, education and training» skrevet av Furnell & Clarke vektlegges bevissthet og forståelse for å oppnå god sikringskultur. Selv om bevissthet, trening og kunnskap er bevist å være i korrelasjon med nivået av sikkerhet i en virksomhet mener de at mange organisasjoner ikke benytter seg av disse tiltakene i stor nok grad. Ved å benytte disse tiltakene mener de at en vil kunne oppnå en kollektiv bevissthet hvor alle ansatte forstår sin rolle, samt viktigheten av denne for virksomhetens helhetlige sikringsnivå. Implementering av trening og tiltak for å øke de ansattes kunnskap om cybersikkerhet og cybertrusler vektlegges her som sentral for det overordnede nivået av cybersikkerhet i en virksomhet (Furnell & Clarke, 2005).

Marta Kruke skrev i 2017 en masteroppgave med fokus på ansattes kollektive bevissthet og hvordan det kan påvirke barrierer som skal forhindre uønsket innsyn i sensitiv informasjon. Oppgaven konkluderte med at kollektiv bevissthet blant virksomhetens ansatte er avgjørende for å kunne opprettholde både myke, harde og forebyggende barrierers funksjon. Det poengteres også at de ansatte må ha kjennskap til verdier som skal beskyttes, samt oppdatert kjennskap til trusselbildet som foreligger for å kunne oppnå en kollektiv bevissthet i virksomheten. Dette arbeidet er med på å illustrere viktigheten av bevissthet blant ansatte i virksomheter for å opprettholde cybersikkerheten til enhver tid, og var med på å forme min oppgave gjennom et ønske om å se hvordan dette kan gjøres gjennom opplæring og trening (Kruke, 2017).

I et felt med rask digital innovasjon og stadig endrende trusselbilde er det viktig å kontinuerlig opprettholde de ansattes bevissthet overfor cybertrusler for å sikre et forsvarlig cybersikkerhetsnivå. Dette arbeidet er utfordrende, og denne oppgaven vil bidra til å belyse hvordan ulike former for opplæring- og treningsopplegg påvirker ansattes bevissthet rundt cybersikkerhet.

1.4 Problemstilling og forskningsspørsmål

Basert på delkapitlene ovenfor er problemstillingen formulert som følger:

«Hvordan jobber kommunesektoren med opplæring og trening innenfor cybersikkerhet, hvilke utfordringer hemmer dette arbeidet - og hvilke implikasjoner har det for de ansattes bevissthet rundt cybersikkerhet?»

For å kunne besvare problemstillingen er følgende forskningsspørsmål utarbeidet:

FS1: *«Hva blir vektlagt i opplærings- og treningsopplegget i kommunen, og hvilke utfordringer hemmer dette arbeidet?»*

FS2: *«Hvordan tilrettelegges det for aktiv deltakelse i opplærings- og treningsopplegg i kommunen, og hvilke implikasjoner har det for de ansattes bevissthet?»*

1.5 Oppgavens struktur

I innledende del av oppgaven redegjøres det for valg av tema, tidligere forskning, problemstilling og forskningsspørsmål, samt avgrensning av oppgaven.

Kapittel 2 redegjør for oppgavens kontekst og vil gjennomgå kommunens ansvarsområder og arbeid, lovverk som er relevante for kommunesektorens arbeid med cybersikkerhet, skillet mellom begrepene informasjonssikkerhet, IKT-sikkerhet og cybersikkerhet, samt de største cybertruslene samfunnet og derigjennom kommunene står overfor i dag.

Kapittel 3 presenterer oppgavens teoretiske rammeverk. I kapittel 4 utdypes de metodiske valgene som er gjort gjennom oppgavens løp. Avslutningsvis diskuteres etiske betraktninger, samt oppgavens styrker og svakheter.

I kapittel 5 presenteres oppgavens empiriske funn, som videre diskuteres i lys av det teoretiske rammeverket i kapittel 6.

Avslutningsvis oppsummeres oppgavens hovedfunn som gir svar på studiens problemstilling i kapittel 7.

2 Kontekst

I dette kapittelet presenteres kommunens ansvarsområder og deres arbeid for å gi leseren et innblikk i ansvaret kommunesektoren har for opprettholdelsen og driften av kritiske infrastrukturer og samfunnsviktige funksjoner. Kapittelet gjennomgår også noen sentrale lover kommunene er underlagt som illustrerer hva de er pålagt å gjøre i forhold til cybersikkerhetsarbeidet. Det presenteres også noen sentrale begreper for oppgaven som informasjonssikkerhet, IKT-sikkerhet, cybersikkerhet og bevissthet for å klargjøre hvordan de brukes i denne studien. Avslutningsvis redegjøres det for de største cybertruslene kommunene står overfor i dag.

2.1 Kommunens ansvarsområder og arbeid

Kommunesektoren har et generelt og grunnleggende ansvar for å ivareta befolkningens trygghet og sikkerhet innenfor sitt geografiske område. Både kommuner og fylkeskommuner er underlagt kommunal beredskapsplikt og har derigjennom et pålagt ansvar for å gjennomføre helhetlige risiko- og sårbarhetsanalyser og gjennom disse kartlegge, systematisere og vurdere risikoen for uønskede hendelser som kan inntreffe i kommunen, samt hvilke konsekvenser disse kan medbringe (NorSIS, 2017, s. 25). Fylkeskommuner og kommuner er ikke en del av den hierarkisk oppbygde statsforvaltningen, de er selvstendige forvaltningsnivåer. Det betyr at de har selvstendig ansvar for innbyggerne sine når det kommer til å løse oppgaver, yte tjenester, drive samfunnsutvikling og utøve myndighet. Kommunen må også selv gjennomføre gode utviklings- og digitaliseringstiltak innenfor sine ansvarsområder. Det vil være kritisk for den kommunale sektoren dersom deres registre, systemer, tjenester eller nettet som eies av staten stopper å fungere eller går fullstendig ned (NorSIS, 2017, s. 24).

I Norge i dag er de fleste kritiske infrastrukturer og samfunnsviktige funksjoner digitalisert, noe som medfører nye sårbarheter. Denne digitaliseringen fører til at flere samfunnsområder er gjensidig avhengige og risikobildet øker derfor i kompleksitet. En forutsetning for et trygt og sikkert samfunn er derfor at de digitale systemene som stadig inkorporeres i samfunnsviktige funksjoner er sikre og pålitelige (NorSIS, 2017, s. 21-22). Digitaliseringsstrategien har derfor satt opp følgende mål for kommuner og fylkeskommuner for å ivareta sikkerheten når det kommer til informasjonssikkerhet, personvern og dokumentasjonsforvaltning:

1. Kommunal sektor skal ivareta informasjonssikkerhet og personvern på alle områder
2. Kommunal sektor skal sikre at riktig informasjon er tilgjengelig for rett person
3. Kommunal sektor skal sørge for innebygd personvern i nye løsninger
4. Kommunal sektor skal ha styringssystem for informasjonssikkerhet
5. Kommunal sektor skal dele informasjon om sikkerhetshendelser de har vært utsatt for
6. Kommunal sektor skal ha helhetlig dokumentasjons- og arkivforvaltning

NOU 2015:13 Digital sårbarhet – Sikkert samfunn trekker også frem følgende problemstilling: «*Digitalisering av samfunnet har skapt avhengigheter og sårbarheter som går på tvers av sektorer, ansvar og landegrenser. Digital sårbarhet og IKT-sikkerhet blir i økende grad sett på som noe som omhandler beskyttelse av velstandssamfunnet i sin helhet, ikke bare som et teknologispørsmål»* (NorSIS, 2017, s. 21-22).

Dette er relevant for den kommunale sektoren ettersom det er kommunen som har ansvar for at dens innbyggere får grunnleggende velferdsgoder som skolegang, sosialhjelp, barnevern, legehjelp og sykehjem. Alle innbyggerne i Norge bor i en kommune, og vi benytter oss av de tjenestene den tilbyr gjennom hele livet (Ung.no, 2021).

2.2 Lovverk og krav

2.2.1 Kommunal beredskapsplikt

Forskriften skal sikre at kommunen ivaretar befolkningens sikkerhet og trygghet. Kommunen er gjennom forskriften pålagt å jobbe systematisk og helhetlig med samfunnssikkerhetsarbeid på tvers av kommunale sektorer for å redusere risiko for tap av liv eller skade på helse, miljø og materielle verdier (Forskrift om kommunal beredskapsplikt, 2011, § 1).

Det systematiske og helhetlige arbeidet med samfunnssikkerhet innebærer blant annet gjennomføring av en helhetlig risiko- og sårbarhetsanalyse. På bakgrunn av denne skal kommunen videre utarbeide mål, strategier, prioriteringer og plan for oppfølging av samfunnssikkerhets og beredskapsarbeidet. Det skal også utarbeides en spesifikk beredskapsplan, med utgangspunkt i risiko- og sårbarhetsanalysen, som skal bidra til å forberede kommunen på å håndtere uønskede hendelser (Forskrift om kommunal beredskapsplikt, 2011, § 2, §3 og §4).

2.2.2 Sikkerhetsloven

Sikkerhetsloven gjelder blant annet for statlige, fylkeskommunale og kommunale organer (Sikkerhetsloven, 2019, § 1-2). Etter den nye sikkerhetsloven trådte i kraft i januar 2019 er fortsatt offentlig forvaltning hoved virkeområde, men lovens virkeområde utvides i takt med dagens risiko- og trusselbilde (Deloitte, 2018). Formålet med loven er «*a) å trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser, b) å forebygge, avdekke og motvirke sikkerhetstruende virksomhet, og c) at sikkerhetstiltak gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn»* (Sikkerhetsloven, 2019, § 1-1).

Loven innebærer blant annet at virksomhetens forebyggende sikkerhetsarbeid skal være en del av virksomhetens styringssystem, samt at virksomheten til enhver tid skal sikre at ansatte, leverandører og oppdragstakere har tilstrekkelig risiko- og sikkerhetsforståelse (Sikkerhetsloven, 2019, § 4-1). Loven setter også krav til beskyttelse av skjermingsverdig informasjon. Dette innebærer at virksomheten selv skal sørge for et forsvarlig sikkerhetsnivå for slik informasjon slik at de ikke blir kjent for uvedkomne, ikke går tapt eller blir endret og at den er tilgjengelig ved tjenstlig behov (Sikkerhetsloven, 2019, § 5-2). Dette er bare noen av de områdene loven omfatter, og for å kunne imøtekomme disse kreves det systematisk og helhetlig beredskaps- og samfunnssikkerhetsarbeid. Et slikt arbeid krever en kombinasjon av menneskelige, elektroniske, fysiske og organisatoriske tiltak.

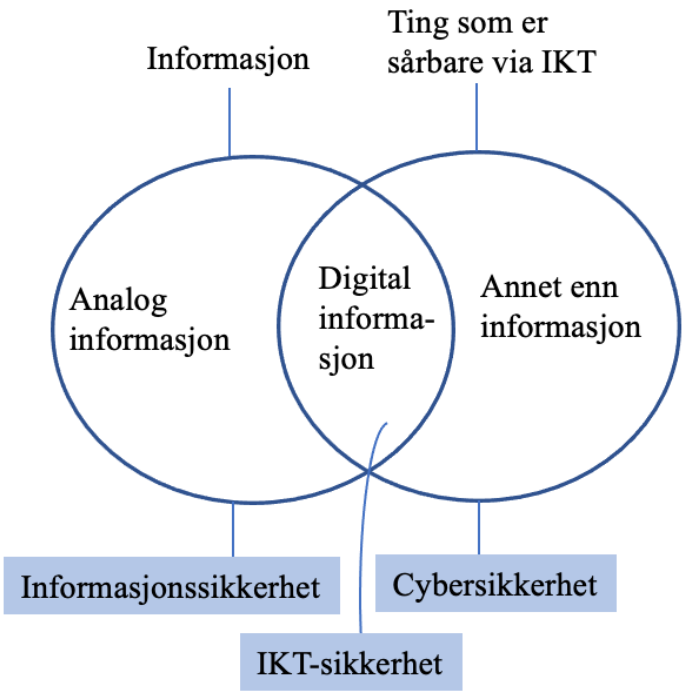
2.2.3 NIS-direktivet og KommuneCSIRT

EU innførte NIS-direktivet i 2016 som pålegger medlemmer av EU og EØS å sikre et samordnet nivå for landets IKT-sikkerhet. Dette skal gjennomføres ved å «*lage en strategi for sikkerhetsarbeidet, etablere en IKT-sikkerhetsberedskapsenhet (CSIRT) og pålegge operatører og leverandører av samfunnsviktige tjenester IKT-sikkerhetskrav og varslingsplikt ved alvorlige IKT-sikkerhetshendelser*» (Justis- og beredskapsdepartementet, 2016). I tråd med denne anbefalingen ble det etablert en KommuneCSIRT som trådte i kraft 1. januar 2020. En slik KommuneCSIRT skal bidra til at kommunene er robuste og evner å forebygge og håndtere nåværende og fremtidige IKT-trusler (NorSIS, 2017, s. 14).

2.3 Informasjonssikkerhet, IKT-sikkerhet og Cybersikkerhet

Det benyttes ulike begreper når en snakker om digital sikkerhet, som informasjonssikkerhet, IKT-sikkerhet og cybersikkerhet. Begrepene brukes i mange tilfeller om hverandre, men jeg vil her forsøke å redegjøre for de ulike begrepene. Informasjonssikkerhet handler om sikring av informasjon, både den som lagres digitalt og den som lagres analogt. IKT-sikkerhet innebærer beskyttelse av informasjons- og kommunikasjonsteknologi (IKT), det vil si maskinvare og programvare (NVE, 2017, s. 15). Det er særlig tre sikkerhetsmål som er kjent i ivaretakelsen av IKT-sikkerhet. Disse er konfidensialitet, tilgjengelighet og integritet (NOU 2015:13, s. 34). Konfidensialitet innebærer å sikre at uvedkomne ikke får tilgang til informasjon, og at det kun er de som har autorisert tilgang til informasjonen får se den. Konfidensialiteten til informasjonen er svært viktig å opprettholde ettersom brudd på konfidensialitet nærmest er umulig å gjenopprette i det digitale domenet. Tilgjengelighet innebærer at tjenester og informasjon skal være tilgjengelig ved behov (NOU 2015:13, s. 34). Integritet innebærer at informasjonen er pålitelig, samt at tjenester og systemer fungerer som tiltenkt. Det innebærer også at ingen uvedkomne skal kunne endre informasjonen. Disse målene kommer også med noen utfordringer ettersom de kan være motsigende. Dersom sensitiv informasjon skal ha høy konfidensialitet og deles med færrest mulig, vil den bli mindre tilgjengelig. Dersom informasjonen har høy grad av tilgjengelighet vil informasjonen lettere kunne komme på avveie eller bli endret av uvedkomne, og integriteten svekkes (NOU 2015:13, s. 35). Det å finne en balanse mellom disse noe motsigende sikkerhetsmålene kan derfor være svært utfordrende, og krever overveielse og prioritering.

Når en derimot snakker om cybersikkerhet viser det til alt cyberdomenet består av, både datasystem og kommunikasjonsinfrastruktur, samt lagring og formidling av informasjon. Begrepet cybersikkerhet handler derfor om å beskytte alt som er sårbart på bakgrunn av at det er koplet opp mot eller avhengig av informasjons- og kommunikasjonsteknologi. God IKT-sikkerhet alene tilsvarer likevel ikke god cybersikkerhet. Cybersikkerhet handler også om «ikke-digitale» sikringstiltak som for eksempel prosedyrer, konsekvensreduserende tiltak, økt kompetanse og bevisstgjøring (NVE, 2017, s. 15). I denne oppgaven benyttes hovedsakelig begrepet cybersikkerhet, men ettersom noen av informantene benytter informasjonssikkerhet i sitt ordforråd brukes disse to tidvis om hverandre. Figuren nedenfor illustrerer likhetene og ulikhetene mellom disse begrepene:



Figur 1: Sammenhengen mellom begrepene Informasjonssikkerhet, IKT-sikkerhet og Cybersikkerhet (tilpasset fra NVE, 2017, s. 15)

2.4 Bevissthet

I dette delkapittelet vil jeg redegjøre for begrepet bevissthet i relasjon til dets bruk i denne studien. Bevissthet er et fenomen det ikke foreligger en entydig forståelse av. Det er et begrep som brukes i flere ulike sammenhenger, ofte med en uklar betydning. Tougas presenterer fenomenet bevissthet som tre samtidige intensjonelle prosesser som omhandler å forvente fremtiden, oppfatte nåtiden og huske fortiden (Tougas, 2012, s. x). Å være bevisst vil si at en kan oppfatte situasjonen en befinner seg i, og vurdere hvilke utfall en handling kan føre til ved hjelp av tidligere erfaringer. Bevissthet kan relateres til situasjonsforståelse eller situasjonsbevissthet og defineres av Endsley (2000, s. 3) som *«the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future*». Situasjonsbevissthet handler om det å være oppmerksom eller årvåken på det som foregår rundt en, forstå hva informasjonen en innhenter betyr, og forutse hvilken betydning den har i nær fremtid.

Weick & Sutcliffe (2007, s. 12) omtaler også begrepet årvåkenhet i relasjon til tilnærmingen om høyt pålitelige organisasjoner. De mener at en godt utviklet situasjonsbevissthet kan bidra til at en kontinuerlig gjør små justeringer i arbeidet sitt som videre gjør at en kan forhindre

akkumulering av feil. På denne måten vil en kontinuerlig være bevisst på arbeidet en gjør, og oppdage feil eller avvik tidlig slik at de kan justeres før en uønsket hendelse inntreffer. Siponen (2000, s. 31) introduserer også begrepet bevissthet innenfor en cybersikkerhetstilnærming og presenterer følgende forklaring for begrepet: «*a state where users in an organization are aware of - ideally committed to - their security mission (often expressed in end-user security guidelines)».* Ifølge Siponen refererer cybersikkerhetsbevissthet til hvilken grad de ansatte forstår viktigheten av organisasjonens sikkerhetspolicyer, regler og retningslinjer, samt hvilken grad de arbeider i samsvar med disse policyene, reglene og retningslinjene (Siponen, 2000, s. 31).

De ansattes bevissthet i denne studien relateres så til deres bevissthet rundt trygg og sikker bruk av IT-systemer, deres bevissthet rundt cybertrusler som kan ramme bedriften, bevissthet om hvordan de skal håndtere en situasjon der de møter på en potensiell cybertrussel, samt bevissthet om hva de skal gjøre dersom de mistenker et avvik eller en uønsket hendelse som kan true organisasjonens cybersikkerhet.

2.5 Cybertrusler

Et cyberangrep er en ekstern trussel som forsøker å skade, forstyrre eller overbelaste et datasystem. Vanlige konsekvenser av cyberangrep er at datasystemer slutter å virke eller ikke fungerer som tiltenkt. Dersom det forekommer avbrudd i daglig drift, kan det igjen føre til økonomisk tap. Videre kan cyberangrep føre til tap av informasjon eller kundedata, noe som kan få alvorlige konsekvenser for bedriftens omdømme og brukernes tillit (NHO, 2018). Under presenteres det som ifølge NorSIS (2020) er noen av de største digitale truslene i samfunnet som kommunene utsettes for og må forholde seg til i sitt arbeid med opplæring og trening av de ansatte.

Phishing

Phishing er en av de aller største kjernetruslene mot privatpersoner og virksomheter. Phishingangrep tilrettelegger også for at en kan utføre en rekke andre former for digital kriminalitet. Typisk kontaktes offeret gjennom e-post, hvor avsender fremstår som en pålitelig virksomhet. I disse e-postene spilles det ofte på fristelse, frykt eller tillit for å få mottaker til å klikke på en link eller et vedlegg lagt ved i e-posten (NorSIS, 2020, s. 21).

Løsepengevirus

Løsepengevirus er et virus som krypterer innholdet på offerets datamaskin, og krever penger for å frigjøre det. Det er en type skadevare som typisk spres via vedlegg eller linker i e-post, Microsoft Office-filer eller infiserte nettsider (NorSIS, 2020, s. 18).

Svindelforsøk

I næringslivet er de mest vanlige svindelsformene direktørsvindel og fakturasvindel. Ved direktørsvindel sendes det en e-post til for eksempel en økonomiarbeider fra en sjef eller direktør i virksomheten, og det bes om en større overføring til et gitt kontonummer eller betaling av en falsk faktura. Ved fakturasvindel sendes det ut faktura for reelle tjenester eller produkter mottatt av virksomheten, men kontonummeret er endret. Et slikt angrep forekommer ofte etter en lengre periode med sosial manipulering slik at fakturaen fremstår som reell (NorSIS, 2020, s. 22-23).

ID-tyveri

ID-bevis, tilgang til et system eller en konto stjeles og benyttes av andre som utgir seg for å være deg. Dette kan blant annet forekomme når en person trykker på en link i en phishing-mail, og oppgir brukernavn og passord (NorSIS, 2020, s. 19).

Verdikjedeangrep

NorSIS (2020, s. 27) ser en økende trend ved at kriminelle ikke angriper sine mål direkte, men heller går igjennom det svakeste leddet og jobber seg opp til hovedmålet derfra. Dette kan være usikrede enheter, underleverandører eller en kunde med adgang til virksomhetsmålet.

Kontohacking

Ved et slikt angrep tar hackeren over en persons eller virksomhetens konto. Brukernavn og passord kan ha blitt gjort tilgjengelig ved et tidligere datainnbrudd eller kan ha blitt oppgitt som følge av en phishing e-mail. Et slikt angrep kan få konsekvenser for virksomhetens kunder, og kan føre til tap av omdømme (NorSIS, 2020, s. 24).

Datainnbrudd

Uvedkomne bryter seg inn i datasystemet med formål om å stjele forretningshemmeligheter, personopplysninger eller kundelister. Hackerne kommer seg inn i systemet ved å utnytte dets sårbarheter eller ved at noen i virksomheten utilsiktet laster ned skadelig programvare som gir hackeren tilgang til datasystemet (NorSIS, 20202, s. 25).

Menneskelig feil

Ifølge Mørketallsundersøkelsen i 2018 er menneskelig feil årsaken til mer enn halvparten av sikkerhetsbruddene i norske virksomheter. Ettersom antall digitale enheter øker blir systemer stadig mer uoversiktlige og komplekse. Faren for at noen gjør en feil øker da i takt med systemets kompleksitet. Det kreves derfor stadig mer kunnskap og bevissthet for å redusere risikoen for at cybertrusler skal ramme egen virksomhet (NorSIS, 2020, s. 25).

3 TEORI

I dette kapittelet vil oppgavens teoretiske rammeverk presenteres. Kapittelet starter med å utdype begrepene kunnskap, kompetanse og læring, samt hvordan en lærer og tilegner seg kunnskap og kompetanse. Det vil så redegjøres for bevisstgjøring og hva som kreves for å sikre bevissthet i organisasjoner. Dernest presenteres Endsleys (2000) teori om situasjonsbevissthet. Til slutt forklares sikkerhetskultur som begrep og teori, samt teorien «un-rocked boat».

3.1 Kunnskap, kompetanse og læring

3.1.1 Fra kunnskap til kompetanse

Filstad skiller mellom begrepene kunnskap og kompetanse. Kunnskap er et resultat av erfaringer, tolkninger og meninger. En benytter denne kunnskapen gjennom refleksjoner, interaksjoner og sosiale kontekster som gjør at en er i stand til å danne en forventning om hvordan en situasjon kan utspille seg. Kunnskap er både en individuell, sosial og kulturell prosess hvor en tilegner seg kunnskap gjennom å lære, for så å videreutvikle den ved hjelp av deltakelse og praksis. Kunnskapen blir først til kompetanse når en anvender den i praksis. I organisasjoner vil kunnskap og læringsprosesser derfor først og fremst få verdi når de ansatte finner måter å anvende kunnskapen gjennom aktiv deltakelse og trening, de vil derigjennom utvikle kompetanse om det de har lært (Filstad, 2016, s. 124).

Kompetanse kan defineres som «*de samlede kunnskaper, ferdigheter, evner og holdninger som gjør det mulig å utføre aktuelle oppgaver i tråd med krav og mål»* (Lai, 2013, s. 46). For å forstå denne definisjonen må det spesifiseres hva som menes med kunnskap, ferdigheter, evner og holdninger. Begrepet kunnskap beskriver hva en kan om et bestemt tema, mens ferdigheter omhandler hvor flinke vi er til å utføre bestemte arbeidsoppgaver. En kan for eksempel ha kunnskap om hvordan en skal utføre en arbeidsoppgave uten å ha ferdighetene til å utføre den i praksis. Når vi snakker om evner tenker vi ofte på noe som er medfødt, og noe som vi er ekstra flinke til. Men evnene våre er påvirkelige, og vi kan med trening bli bedre på noe. Å inneha de rette holdningene er helt sentralt for kvaliteten på arbeid som gjøres. Det hjelper ikke å ha gode kunnskaper om cybersikkerhet dersom holdningen til å ivareta cybersikkerheten ikke er til stede (Olsen, 2016, s. 240-241). En god strategi for kompetanseutvikling burde derfor ta hensyn til og omfatte disse fire elementene, alt etter hvilke kompetansebehov som identifiseres. Det hjelper for eksempel ikke å introdusere

kunnskap dersom det egentlig er behov for å øve på hvordan denne kunnskapen kan omsettes i praksis. Dersom en innehar kunnskapen, men mangler ferdigheter til å utføre den i praksis kreves det muligheter til å trene slik at en kan utvikle kompetanse (Olsen, 2016, s. 241).

Gjennom kompetanseutvikling videreutvikler eller lærer vi oss ny kunnskap og nye ferdigheter (Olsen, 2016, s. 238). Cybersikkerhet er et område som er i konstant endring, den teknologiske utviklingen går fort og kriminelle utøvere utvikler stadig nye metoder for angrep. Livslang læring er et begrep som har fått en sentral plass i EU´s politikk om utdanning og kompetanseutvikling. Begrepet reflekterer viktigheten av å konstant være faglig oppdatert og utvikle sin kompetanse i møte med teknologiske, markedsmessige og samfunnsmessige endringer (Olsen, 2016, s. 239). Dette krever at virksomheter og medarbeider sørger for å drive kompetanseutvikling i samme tempo som disse endringene. Slik kompetanseutvikling forutsetter læring. For å forstå kompetanse må vi derfor også se på hvordan vi lærer.

3.1.2 Læring

Virksomheter påvirkes av utvikling og endringer innad i organisasjonen, i tillegg til eksterne forhold. Disse endringene kan være relatert til kunders og brukeres behov og forventninger til sikkerhet, utvikling og muligheter innenfor teknologi, til ny informasjon eller til nye ledere med nye visjoner og strategier (Filstad, 2010, s. 177). Når utvikling og endring forekommer i virksomheten krever det også utvikling og endring blant medarbeiderne i denne virksomheten, ofte i form av læring. Læring kan defineres som *«tilegnelse av ny eller endret kompetanse – i form av kunnskaper, ferdigheter eller holdninger – som gir relativt varige endringer i en persons atferdspotensial»* (Lai, 2013, s. 119). Ser en på arbeidsplassen som et læringsmiljø vil en først og fremst se arbeidsplassen som en formell organisasjon hvor ledelsesstruktur, organisering, produksjonsform og teknologi blir viktig. Men innenfor disse formelle strukturene vil også den uformelle læringen som oppstår i sosial interaksjon mellom kollegaer for å løse arbeidsoppgaver i praktisk arbeid være av stor betydning (Filstad, 2010, s. 177).

I en studie utført av Filstad i 2012 kommer det frem at praktisk utøvelse av arbeidsoppgaver er av størst betydning når det kommer til læring. Det fremkommer også av studien at de viktigste formene for læring i praksis er kommunikasjon og mulighet for å praktisere med kollegaer, i tillegg vurderes kurs og trening som meget effektive læringsarenaer på arbeidsplassen. Ved å benytte seg av disse elementene kan arbeidsplassen sørge for utvikling

av kompetanse gjennom praktisk anvendelse av kunnskap en har tilegnet seg (Filstad, 2016, s. 177). Det vil derfor være gunstig å implementere kompetanseutviklingstiltak som gir de ansatte mulighet til å teste ut det de har lært gjennom praktiske oppgaver eller gjennom diskusjon med medarbeidere (Olsen, 2016, s. 245). Læring handler altså ikke bare om individuell kunnskapstilegnelse, det krever også interaksjon og aktiv deltakelse (Olsen, 2016, s. 246).

Filstad trekker også frem den tause kunnskapen når vi snakker om læring. Taus kunnskap er *«den kunnskapen som ikke kan forklares med ord og dermed ikke kan utrykkes eksplisitt»* (Filstad, 2016, s. 114). Å ha kunnskap og å være kompetent krever at en har en form for taus kunnskap i kombinasjon med eksplisitt kunnskap, disse er to sider av en persons totale kompetanse. Eksplisitt kunnskap defineres som «*den kunnskapen som kan uttrykkes gjennom språket ved hjelp av språkets formuleringer av ord, tall og symboler»* (Filstad, 2016, s. 114). En kan skille mellom disse to formene for kunnskap ved å si at den eksplisitte kunnskapen er den en kan sette ord på, nemlig den teoretiske kunnskapen, mens taus kunnskap er den praktiske kunnskapen som kreves på arbeidsplassen. Disse to formene for kunnskap krever ulike læringsarenaer. Eksplisitt kunnskap kan digitaliseres, for eksempel på intranettet, gjennom regler, skriftlig dokumentasjon og strategidokumenter. Taus kunnskap på den andre siden er forankret i praksis, det vil si gjennom selve utførelsen av en handling og den konkrete konteksten og situasjonen den utføres i. Den tause kunnskapen formidles derfor gjerne gjennom kroppsspråk, handling, å praktisere sammen og anvende andre ikke-språklige kommunikasjonsformer. Vi er ikke i stand til å kommunisere den tause kunnskapen som er forbundet med en handling ettersom en må ta hensyn til ulike kontekster og situasjoner en kan møte på arbeidsplassen (Filstad, 2016, s. 115).

Det mest optimale for læring er derfor en kombinasjon av å forklare eksplisitt og samtidig være i en situasjon som gir mulighet for praktisk utførelse av en handling. Et eksempel på dette kan illustreres dersom en skal følge en oppskrift når en lager mat. Personen som har laget oppskriften har gjort kunnskapen sin eksplisitt gjennom å forklare fremgangsmåte og mengde av hver ingrediens. Men den tause kunnskapen vil blant annet være å kjenne om deigen har riktig konsistens, eller å smake til om det er riktig mengde krydder, som er egenskaper som utvikles gjennom erfaring (Filstad, 2016, s. 115). Den tause kunnskapen kan derfor sies å være *«læring gjennom handling ved at personen må gjøre det selv»* (Filstad, 2016, s. 116).

Når en ser på arbeidsplassen som en læringsarena for praktiske erfaringer er det også to ulike forhold som påvirker læring hos de ansatte. Disse to forholdene er hvordan arbeidsplassen tilrettelegger for læringsmuligheter for de ansatte, og i hvilken grad de ansatte velger å benytte seg av læringsmulighetene de blir tilbudt. Her oppstår en gjensidig avhengighet mellom nøkkelelementene i deltakende trening, opplæring og erfaring (Billett, 2004, s. 109).

3.2 Bevisstgjøring

De ansattes kunnskap og bevissthet er en av de viktigste forutsetningene for å etablere og opprettholde et akseptabelt nivå av cybersikkerhet i en virksomhet. Mangel på slik kunnskap og bevissthet er som regel den største trusselen mot cybersikkerheten (Daler, Gulbrandsen, Høie & Sjølstad, 2019, s. 213). Det er derfor sentralt for virksomhetens cybersikkerhet å gi alle deres ansatte opplæring som motiverer dem til å ha fokus på sikkerhet. Slik opplæring vil tilrettelegge for at de ansatte blir bevisste på virksomhetens regler og prosedyrer, samt at de utvikler de nødvendige ferdighetene til å handle i tråd med dem (Daler et al., 2019, s. 213). En slik sikkerhetsopplæring bør omfatte:

- Informasjon om hvorfor sikkerhet er nødvendig
- Innføring i regler og retningslinjer som skal følges
- Metoder som viser hvordan sikkerhetskontroller skal utføres
- Rutiner som viser hvordan de enkelte applikasjoner skal forvaltes sikkerhetsmessig korrekt
- Innføring i rutiner for rapportering og sikkerhetsbrudd (Daler et al., 2019, s. 213-214)

Regler, instrukser og rutiner som implementeres i forbindelse med sikkerhetskrav kan fort bli oppfattet av de ansatte som tungvinte, unødvendige eller overdrevne. Det er derfor viktig at disse kravene står i rimelig forhold til det som skal beskyttes og at de ansatte forstår hvorfor og hvordan de skal benytte disse sikkerhetskravene (Daler et al., 2019, s. 214). Et sentralt opplærings- og holdningsskapende program bør ta sikte på å fremme motivasjon og holdninger, kunnskap og bevissthet, aksept og forståelse av tiltak, risikoforståelse og ansvar for kvalitet og sikkerhet i eget arbeid. En forutsetning for at dette arbeidet skal bli vellykket er blant annet at dette programmet må bygge på et enkelt og forståelig grunnlag, slik at alle ansatte i ulike deler av bedriften forstår hva det innebærer (Daler et al., 2019, s. 214).

3.3 Situasjonsbevissthet

Fokuset på situasjonsbevissthet har økt med den raske utviklingen av teknologiske løsninger som skaper større avstand mellom mennesker og de systemene de opererer (Flin, O´Connor & Crichton, 2008, s. 17). De raske teknologiske endringene virksomhetene utsettes for krever også at de ansattes situasjonsbevissthet kontinuerlig må endres i takt med den teknologiske utviklingen for å ikke bli utdatert og mangelfull (Endsley, 2000, s. 4). Situasjonsbevissthet kan forklares som «å vite hva som foregår rundt en», og tilsvarer en operatørs forståelse av en situasjon som vil danne grunnlaget for videre beslutningstaking, og fungerer som det første steget i beslutningsprosessen. Den vanligste definisjonen av begrepet presenterer situasjonsbevissthet som *«persepsjonen av elementene i miljøet rundt en ..., å forstå deres betydning og å være i stand til å forutse hvordan situasjonen vil kunne utvikle seg»* (Flin et al., 2008, s. 17; Endsley, 2000, s. 1-2). For ansatte i virksomheter vil dette være av stor betydning for cybersikkerheten, blant annet når det kommer til å gjenkjenne phishing-mail. En må være i stand til å oppfatte signaler, forstå risikoen disse kan presentere og forutse hva som kan forekomme dersom for eksempel en link trykkes på. En vil ut ifra denne prosessen beslutte hvordan en handler videre. En kan altså dele situasjonsbevissthet inn i tre prosesser: (1) samle informasjon, (2) tolke denne informasjonen og (3) forutse fremtidige virkninger (Flin et al., 2008, s. 17).

Oppfattelse av signaler

Det første nivået handler om persepsjon og oppfattelse av riktige og viktige signaler, og er fundamentalt for å forme et riktig bilde av en situasjon (Endsley, 2000, s. 3; Saus & Johnsen, 2016, s. 228). Informasjonsutvelgelse handler om hvordan en legger vekt på en type informasjon, men kan se bort i fra en annen. For de ansatte i kommunen kan dette for eksempel være gjenkjennelse av elementer i en mail som tyder på at den ikke er pålitelig. Her er det særlig to faktorer som spiller inn, nemlig evne og motivasjon. Ens evne til informasjonsbehandling forutsetter at en har fysisk tilgang på informasjonen, tid til behandling av informasjonen og at det er et begrenset antall distraherende faktorer til stede. Motivasjonen avhenger av personlige interesser, verdier og bevissthet. For de som arbeider med kommunikasjon er det derfor viktig å ha oversikt over disse egenskapene for å kunne tilpasse kommunikasjonsstrategiene til de ansattes grad av evne og motivasjon (Njå, Sommer, Rake & Braut, 2020, s. 94-95). Kommunikasjonen om trusler må tas ned på et nivå som gjør

den effektiv for mottakeren, og derigjennom øker mottakerens evne og motivasjon til informasjonsutvelgelse som reflekterer omverdenen.

Forståelse

Det andre nivået er knyttet til forståelse av situasjonen gjennom å integrere informasjonen en har hentet inn i det første nivået (Saus & Johnsen, 2016, s. 228). Når en har hentet inn signaler må en kombinere, tolke og lagre informasjonen. Her gir en mening til signalene en har oppfattet og vurderer deres relevans opp mot målet en jobber mot (Endsley, 2000, s. 3). På den måten vil en få et helhetlig bilde av omgivelsene og sammenligne det opp mot oppsatte planer og mål (Saus & Johnsen, 2016, s. 228).

Mulighet til å forutse

På det tredje og høyeste nivået av situasjonsbevissthet vil en være i stand til å forutse. Dette nivået bygger på de to foregående nivåene og dreier seg om å forutse fremtidig utvikling av situasjonen. Kommer en til dette tredje nivået vil en oppnå den dypeste formen for forståelse for situasjonen, og dermed den dypeste formen for situasjonsbevissthet (Endsley, 2000, s. 4; Saus & Johnsen, 2016, s. 228).

3.4 Sikkerhetskultur

For å få et helhetlig bilde av de ansattes bevissthet mot cybertrusler er det sentralt å se på de medvirkende faktorene som kan fremme eller hemme denne bevisstheten. En studie utført av Parsons et al. (2015, s. 125) påpeker en korrelasjon mellom bevissthet rundt cybersikkerhet og sikkerhetskultur. Personer som jobber i virksomheter med god sikkerhetskultur viste seg å være mer sannsynlig å inneha kunnskap, holdninger og atferd i samsvar med virksomhetens retningslinjer og prosedyrer for cybersikkerhet. Det er interessant å se på hvordan kommunen jobber med opplæring og trening for å skape bevissthet, ettersom ansattes atferd og holdninger i stor grad påvirkes av virksomhetens sikkerhetskultur. En god sikkerhetskultur kjennetegnes blant annet av at individer i virksomheten er bevisste på de potensielle risikoene og egnede preventive tiltakene virksomheten opererer med, samt at de tar ansvar for å opprettholde og forbedre sikkerheten i informasjonssystemene de benytter (OECD, 2002, s. 8). James Reason benytter følgende definisjon på sikkerhetskultur i sin bok *Managing the risks of organizational accidents*:

«The safety culture of an organization is the product of individual and group values, attitudes, competencies, and patterns of behaviour that determine the commitment to, and the style and proficiency of, an organizations health and safety programmes. Organizations with a positive safety culture are characterized by communications founded on mutual trust, by shared perceptions of the importance of safety and by confidence in the efficacy of preventive measures" (1997, s. 194).

Reason støtter denne definisjonen, men har sitt eget nøkkelprinsipp for sikkerhetskultur som omhandler en informert kultur. Hovedelementene i en slik informert kultur er en rapporterende, rettferdig, fleksibel og lærende kultur. I denne tilnærmingen er en informert kultur et synonym for sikkerhetskultur. Reason trekker først frem viktigheten av en rapporterende kultur hvor de ansatte rapporterer avvik eller feilhandlinger. Dette tilrettelegges av organisasjonens grad av rettferdig kultur, som vil si at de ansatte har tillit til organisasjonen på en slik måte at de ikke er redde for sanksjoner og straff dersom de rapporterer et avvik. Dette kan gjøres blant annet ved at organisasjonen oppfordrer til, gjerne også belønner rapportering av sikkerhetshendelser. En fleksibel kultur involverer tilretteleggelse for å skifte fra et top-down hierarki til en flatere hierarkisk modell ved en krise, slik at de som står nærmest krisen får makt til å ta beslutninger angående dens håndtering. Med en lærende kultur menes en organisasjons ønske og kompetanse til å implementere viktige sikkerhetstiltak når deres behov indikeres (Reason, 1997, s. 195). Under vil jeg utdype nærmere de tre type kulturene som synes mest relevante for denne oppgavens hensikt, nemlig en rapporterende kultur, en rettferdig kultur og en lærende kultur. Den fleksible kulturen utelates her ettersom jeg ikke studerer hvordan organisasjonen organiserer seg ved eventuelle ulykker og uønskede hendelser.

En rapporterende kultur

Å få folk til å rapportere kritiske hendelser eller nesten-ulykker er ikke lett å få til, spesielt når det innebærer at de selv må oppgi sine egne feil. Selv når det ikke handler om egne feil er det ikke alle som forstår verdien av å rapportere saker de finner mistenksomme eller bekymringsverdige. Dette gjelder særlig dersom de ansatte ikke har tro på ledelsen benytter seg av og handler på bakgrunn av denne informasjonen. De ansatte kan også gjerne være redde for at de selv eller kollegaene sine kan få negative konsekvenser av rapporten. I tillegg er det et par andre elementer som hindrer folk i å rapportere avvik, som for eksempel det

ekstra arbeidet det krever, et naturlig ønske om å glemme at hendelsen inntraff, frykt for straff eller mangel på tillit (Reason, 1997, s. 196).

En rettferdig kultur

Den rettferdige kulturen bygger på noe av det samme som tilrettelegger for en rapporterende kultur. Reason refererer til en rettferdig kultur som en atmosfære av tillit, hvor folk oppfordres til å gi sikkerhetsrelevant informasjon, gjerne også medfølger belønning for slik atferd. Samtidig skal det skilles mellom akseptabel og uakseptabel oppførsel. En skal ikke straffe alle feilhandlinger, men det kreves sanksjoner i noen tilfeller hvor folk opptrer uansvarlig på arbeidsplassen. Det er fortsatt mulig å gi sanksjoner, men de ansatte skal få et klart skille mellom hva som er greit og ikke (Reason, 1997, s. 205).

En lærende kultur

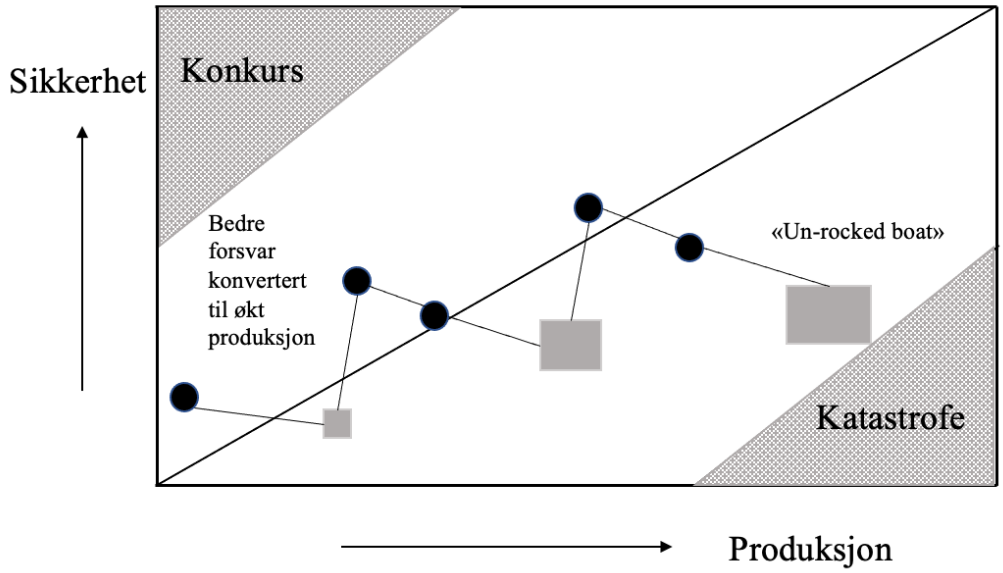
Til slutt kommer vi inn på den lærende kulturen. Læring avhenger av et godt informasjonsgrunnlag, at en har tilstrekkelig kompetanse til å handle basert på denne informasjonen, og at en har vilje til å iverksette endringer når det er behov for det. Dette betyr at læring har funnet sted dersom den informasjonen beslutningstakerne har fått omsettes til faktisk handling som medfører forbedringer (Kongsvik, 2013, s. 116).

Reason vektlegger også viktigheten av å ikke glemme å være redd for de mange truslene som kan penetrere systemene en benytter for opprettholdelsen av en god sikkerhetskultur. Ved fravær av uønskede hendelser mener Reason at det er viktig å informere om ulykker og nesten-ulykker som har rammet andre organisasjoner, for å opprettholde respekten for og det proaktive arbeidet mot truslene som kan ramme organisasjonen (Reason, 1997, s. 195). Denne tankegangen utdypes nærmere i delkapittelet under.

3.5 Un-rocked boat

Produksjon og sikkerhet er prosesser nærmest alle organisasjoner må veie opp mot hverandre i dag. Alle organisasjoner som produserer et produkt, som for eksempel helsetilbud, transport, finansiell hjelp eller andre tjenester, kan potensielt utsette folk for fare. Produksjon av produkt og tjenester krever derfor former for sikkerhetstiltak som beskytter mennesker mot disse potensielle farene. I en ideell verden vil nivået av sikkerhetstiltak være tilsvarende farenivået produksjonen av tjenester og produkter introduserer, også kalt paritetssonen. Jo mer

omfattende produksjonen av tjenester og produkter er, jo større er risikoeksponeringen og dermed behovet for tilsvarende beskyttelse (Reason, 1997, s. 3). Forholdet mellom slik produksjon og beskyttelse illustreres i figuren under:



Figur 2: "Un-rocked boat" (tilpasset fra Reason, 1997, s. 5)

Denne modellen viser til to ekstreme ytterpunkter hvor den ene er konkurs og den andre er katastrofe. Ettersom sikkerhetstiltak krever ressurser fra produksjonen, som mennesker, penger og materiell vil et for stort fokus på sikkerhet kunne ende i organisasjonens konkurs. På den andre siden, om en fokuserer i for stor grad på produksjon, og ser bort i fra sikkerhetstiltak for potensielle farer, vil det kunne ende i en katastrofal hendelse. Hovedfokuset til modellen er hvordan mange organisasjoner navigerer seg mellom disse to ytterpunktene gjennom organisasjonens levetid. Ettersom en trenger ressurser fra produksjonen til å implementere sikkerhetstiltak er det ofte produksjonen som vil ha prioritet gjennom en organisasjons levetid. Størstedelen av menneskene som jobber i organisasjoner har også ferdigheter som går på produksjon heller enn sikkerhet, noe som vil legge til rette for større fokus på produksjonsdelen i organisasjonen. Produksjon er i tillegg enklere å måle ved hjelp av tall og statistikk, mens god sikkerhet ofte indikeres av fravær av uønskede hendelser (Reason, 1997, s. 4). Det er også lett å glemme å være varsom for hendelser som skjer sjelden, spesielt når sikkerheten konkurrerer med organisasjonens profitt og vekst (Reason, 1997, s. 6).

En ser derfor en tendens til at organisasjoner kun har stort fokus på beskyttende tiltak kort tid etter en nesten-ulykke eller ved en uønsket hendelse. Over tid, uten uønskede hendelser, vil en kunne få en tankegang om at sikkerheten er god nok, og som resultat vil sikkerheten gradvis avta igjen for å sikre større avkastning fra produksjonen. I figuren over illustreres dette forholdet ved hjelp av sorte prikker og grå firkanter. De sorte prikkene viser til et høyt fokus på sikkerhet, men etter hvert som organisasjonen ikke opplever noen sikkerhetshendelser avtar sikkerheten gradvis, inntil en nesten-ulykke inntreffer (grå firkant). Etter slike nesten-ulykker eller uønskede hendelser strammes sikkerheten inn igjen, før den gradvis avtar til fordel for organisasjonens produksjon helt til en ny, mer alvorlig hendelse inntreffer (Reason, 1997, s. 6).

3.6 Analytiske implikasjoner

Teorien som er presentert i dette kapittelet vil bidra til å svare på forskningsspørsmålene og problemstillingen. Det er redegjort for teori om kunnskap, kompetanse, læring, bevisstgjøring, situasjonsbevissthet, sikkerhetskultur og «un-rocked boat». Teori om kunnskap og kompetanse, læring, bevisstgjøring, sikkerhetskultur og «un-rocked boat» har bidratt til å forme forskningsspørsmål 1. Teoriene vil benyttes for å belyse hvilke implikasjoner kommunens bruk av opplæring og trening har for de ansattes bevissthet, teorien om «un-rocked boat» vil bidra til å sannsynliggjøre hvorfor kommunen møter på utfordringer i cybersikkerhetsarbeidet sitt. Teori om læring, bevisstgjøring og situasjonsbevissthet har også bidratt til å forme forskningsspørsmål 2 om påvirkningen aktiv deltakelse i opplæring og trening har på de ansattes bevissthet. De vil benyttes for å belyse hvilke implikasjoner kommunens tilretteleggelse for aktiv deltakelse har på de ansattes bevissthet mot cybersikkerhet.

4. Forskningsmetode

I dette kapittelet vil studiens forskningsmetode presenteres, samt begrunnelse for de metodiske valgene som er gjort i løpet av oppgaven. Det vil redegjøres for datainnsamling, utvalg av informanter, samt hvordan det er arbeidet for å sikre forskningens kvalitet. Avslutningsvis presenteres de etiske refleksjonene som har oppstått gjennom oppgavens løp, og det redegjøres for styrker og svakheter ved studien.

4.1 Studiens formål og forskningsdesign

Bakgrunnen for studien var et ønske om å få innsikt i hvordan ulike former for læring og trening, samt utforming av prosedyrer og retningslinjer påvirker ansattes bevissthet rundt cybersikkerhet i en virksomhet. Kommunal sektor ble valgt ettersom de arbeider med store mengder sensitiv data, samt en hypotese om at de har et større krav til tilgjengelig informasjon og åpenhet som et offentlig organ, i tillegg til at det tidligere har blitt påpekt en mangel på kompetanse innenfor cybersikkerhet i kommunesektoren. Jeg valgte å studere én stor kommune i Norge for så å se nærmere på dens ulike tjenesteområder for å få et overordnet bilde av arbeidet med opplæring og trening i hele kommunen. Dette dannet grunnlaget for oppgavens problemstilling og tilhørende forskningsspørsmål. Underveis i prosessen har både problemstillingen og forskningsspørsmålene blitt endret og justert. Studien preges derfor av et eksplorativt design. En eksplorerende studie ble valgt på bakgrunn av fleksibiliteten det gir til å utvikle og presisere problemstillingen etter hvert som jeg fikk mer innsikt i oppgavens tematikk (Thagaard, 2013, s. 16).

I denne oppgaven så jeg det videre som mest hensiktsmessig å benytte et abduktivt forskningsdesign, som beskriver et samspill mellom en induktiv og en deduktiv tilnærming (Thagaard, 2013, s. 201). Gjennom en induktiv tilnærming forsøker en å komme frem til en empirisk generalisering, mens en deduktiv tilnærming tar utgangspunkt i en hypotese, for så å teste denne hypotesens logiske validitet. En abduktiv tilnærming derimot tar utgangspunkt i å tolke et fenomen innenfor et teoretisk rammeverk, og en vil på den måten komme frem til en av flere mulige forklaringer på et fenomen avhengig av hvilket teoretisk rammeverk en velger (Dey, 2004, s. 91). Ifølge Blaikie & Priest er forskningsdesign prosessen som kopler sammen forskningsspørsmål, empiriske data og forskningens konklusjon. Det er altså en plan for hvordan en går fra en problemstilling som forsøkes besvart til å kunne besvare denne problemstillingen (Blaikie & Priest, 2019, s. 33). En abduktiv tilnærmingen ble så valgt

ettersom jeg ønsket å forklare fenomenet «bevissthet rundt cybersikkerhet i kommunesektoren» gjennom å benytte et teoretisk rammeverk, for å komme frem til en mulig forklaring på hvordan ulike opplæring- og treningsopplegg påvirker ansattes bevissthet rundt cybersikkerhet i kommunesektoren.

4.2 Kvalitativ forskningsmetode

I denne oppgaven valgte jeg å benytte meg av en kvalitativ forskningsmetode for å få innsikt i og skape forståelse for oppgavens tema. Jeg valgte å ta utgangspunkt i én stor kommune i Norge, og ønsket å få innsikt i hvordan de jobber med opplæring og trening innenfor cybersikkerhet i de ulike tjenesteområdene. Først ønsket jeg å få innsikt i dokumenter som beskrev hvordan de jobber med dette, for så å snakke med de som står ansvarlige for cybersikkerheten i hver avdeling. Etter mange mail frem og tilbake med ulike ansatte i kommunen som var relevante for oppgavens problemstilling ble det klart at det var stor begrensning på skriftlig datamateriale. Grunnet begrenset tilgang på interne dokumenter, ble det satt mest fokus på dybdeintervjuer med cybersikkerhetsansvarlige i avdelingen. Gjennom samtaler med intervjuobjekter om deres kunnskap og erfaringer har jeg samlet inn data for å øke forståelsen for oppgavens problemstilling. Det skilles mellom to ulike forskningsmetoder i samfunnsvitenskapelig forskningsmetode, kvalitativ og kvantitativ metode. Det som skiller de ulike metodene, er hvordan en samler inn datamateriale. Kvantitativ metode vektlegger utbredelse og antall, og baserer seg vanligvis på tall og statistikk, mens kvalitativ metode søker å gå mer i dybden og er preget av større fleksibilitet (Thagaard, 2013, s. 17). Både den kvalitative forskningsmetoden og den abduktive tilnærmingen som ble valgt i oppgaven gav rom for fleksibilitet, og derigjennom justering av problemstilling og teoretisk rammeverk, ettersom jeg fikk mer innsikt i oppgavens tema og utfordringene knyttet til temaet.

4.3 Datainnsamling

Kvalitativ metode gir mulighet for å studere dokumenter og gjennomføre intervjuer. I denne oppgaven benyttes både dokumentanalyse og semi-strukturerte intervju. Intervjuene preger oppgaven i størst grad ettersom det var her jeg fikk størst mengde informasjon som var formålstjenlig for oppgavens problemstilling.

4.3.1 Dokumentanalyse

I starten av forskningsprosjektet ønsket jeg å samle inn dokumenter fra informantene jeg henvendte meg til før jeg startet intervjuprosessen. De skriftlige dokumentene som ble etterspurt var dokumenter som beskriver hvordan kommunen jobber med bevisstgjøring av de ansatte som blant annet prosedyrer, policyer, retningslinjer og planverk. Dette for å få et mer helhetlig bilde av deres arbeid med opplæring og trening av sine ansatte når det kom til å skape bevissthet overfor cybertrusler. Men ettersom det kun var én av informantene som hadde slike dokumenter som ble etterspurt, måtte oppgavens problemstilling endres litt ut ifra denne nye informasjonen. Her var det eksplorative designet fordelsaktiv ettersom det gav fleksibilitet til å endre prosjektet etter informasjonen fra datainnsamlingen var innhentet (Thagaard, 2013, s. 60). Dokumentene som er tatt i bruk i oppgaven inkluderer nyhetssaker som omhandler plan for opplæring, generell informasjon om cybersikkerhet og ulike angrepsmetoder, sikkerhetsregler kommunen arbeider etter, samt taushetserklæringen alle ansatte må skrive under på. Sikkerhetsreglementet og taushetserklæringen var det eneste jeg fikk innsikt i av kommunens retningslinjer og prosedyrer. Resterende dokumenter var nyhetssaker som omhandlet cybersikkerhet som kommunen sender ut til de ansatte over intranettet med informasjon som synes viktig for dem å ha kjennskap til.

4.3.2 Intervjusituasjon og intervjuguide

Det ble gjennomført fem dybdeintervjuer med personer ansvarlig for cybersikkerhet i ulike avdelinger i kommunen. Dette gav mulighet til å få innsikt i problemstillinger og utfordringer innenfor ulike tjenesteområder, i tillegg til hvordan de ulike tjenesteområdene arbeidet med opplæring og trening. Før første intervju ble gjennomført utviklet jeg en semi-strukturert intervjuguide som fungerte veiledende i intervjusituasjonen. Det semi-strukturerte intervjuet gav mulighet for en fleksibilitet som oppgaven dro nytte av ettersom jeg kunne stille oppfølgingsspørsmål eller få mer utdypende svar om nødvendig. En slikt delvis strukturert tilnærming preges av at temaene forskeren ønsker svar på er bestemt på forhånd, men rekkefølgen av temaene kan tilpasses intervjupersonens fortelling (Thagaard, 2013, s. 98).

Intervjuguiden består av cirka 20 spørsmål (se vedlegg I). Ettersom det ble utført flere intervju ble den endret litt underveis. Dette da noen informanter gav ny innsikt i temaet og tok opp nye temaer som ble vurdert som interessante for problemstillingen. Jeg fjernet derfor fortløpende spørsmål som ble vurdert som overflødige, og la til spørsmål som var relevante for problemstillingen. For å skape dynamikk i intervjuet ble intervjuguiden delt opp i ulike

temaer og strukturert som en dialog mellom intervjuperson og forsker, noe som gav mulighet for refleksjoner og innspill utover spørsmålene som var inkludert i intervjuguiden. Intervjuguiden bestod også av noen åpne spørsmål hvor intervjupersonene tok opp forholdvis ulike tema som var relevante for deres tjenesteområde og avdeling. Dette gav et bredt spekter av ulike svar og viste til hva de ulike intervjupersonene vektla.

Intervjuene ble gjennomført over teams, og varte mellom 30 og 65 minutter. Alle intervjuene ble tatt opp med en ekstern lydopptaker, med intervjupersonenes samtykke. Dette var svært formålstjenlig ettersom jeg kunne fokusere helt og fullt på intervjupersonen istedenfor å være avhengig av å notere underveis i intervjuet. Det gav meg også mulighet til å høre igjennom intervjuene i etterkant og derigjennom bli bevisst på min egen opptreden i intervjuene, og forbedre meg på eventuelle svakheter. Å gjennomføre lydopptak under intervjuene gjorde også at jeg kunne kvalitetssikre sitat som ble brukt, slik at det ikke ble preget av min egen oppfattelse under eventuell notering. Etter at datamaterialet var ferdig bearbeidet, ble lydopptaket slettet for å beskytte informantenes anonymitet. For å forsikre meg om at intervjupersonene var fullstendig klar over hva det innebar å delta i studien sendte jeg også ut informasjonsskriv og samtykkeerklæring i forkant av intervjuene (se vedlegg II). Her ble det gitt informasjon om hva studien handlet om, hva deltakelse i studien innebar, hva informasjonen de oppga ville brukes til, hvem som ville få innsikt i denne informasjonen, samt at de ville bli anonymisert i oppgaven.

4.3.2.1 Valg av intervjuobjekter

Jeg startet med å kontakte en aktuell kommune og fikk satt opp et virtuelt møte med en som jobbet med IT-sikkerhet i kommunens IT-avdeling. I dette møtet gjennomgikk vi oppgavens tematikk, og basert på det fikk jeg kontaktinformasjon til ulike IT-ansvarlige i ulike avdelinger i organisasjonen som vi anså som hensiktsmessige for oppgaven. Min kontaktperson i kommunen sendte også ut mail til disse IT-ansvarlige i kommunen med informasjon om oppgaven, og at de ville bli kontaktet av meg i løpet av kort tid. På denne måten fikk jeg kontakt med personer som hadde kvalifikasjoner som var strategiske i forhold til oppgavens problemstilling og teoretiske perspektiv (Thagaard, 2013, s. 60).

Jeg startet altså med en kartlegging av ulike personer i kommunen som jobbet med og hadde erfaring med cybersikkerhet, og som hadde et ansvar for dette innenfor sin avdeling. Ikke alle de jeg kontaktet i første omgang hadde mulighet til eller ønske om å delta i studien. Utvalget

av informanter preges derfor av en kombinasjon av tilgjengelighetsutvalg og et strategisk utvalg. Det vil si at deltakerne i studien presenterte egenskaper som var relevante for problemstillingen, men fremgangsmåten for å velge ut deltakere basertes på at de var tilgjengelige til å delta (Thagaard, 2013, s. 61). Bruken av tilgjengelighetsutvalg syntes særlig nødvendig ettersom koronapandemien preget noen tjenesteområder særlig hardt. Flere av deltakerne som ble kontaktet hadde derfor ikke tid til å delta i studien, men kunne likevel være behjelpelige med å foreslå andre mulige informanter med forholdsvis like kvalifikasjoner.

I tabellen under presenteres informantene som benyttes i oppgaven. Tabellen gir informasjon om informantenes stillingstittel, og hvor mange år de har jobbet med cybersikkerhet for å illustrere deres erfaring.

Informant	**Stillingstittel**	**Antall år innen IT-arbeid**
Informant A	Seksjonssjef for IT-systemforvaltning	<10 år
Informant B	Sikkerhetsrådgiver på IT-avdeling	>10 år
Informant C	Pedagogisk IKT-rådgiver	<10 år
Informant D	IT-rådgiver	<10 år
Informant E	IT-rådgiver	<10 år

Tabell 1: Oversikt over informanter

4.4 Kvalitetskriterier

I delkapitlene under vil det redegjøres for oppgavens kvalitetsmessige styrker og svakheter. Dette vil gjøres gjennom å benytte begrepene reliabilitet, validitet og overførbarhet. Jeg vil så gjennomgå hvordan jeg har gått frem for å sikre at studien til enhver tid har vært etisk forsvarlig. Avslutningsvis vil det redegjøres for oppgavens styrker og svakheter i lys av forskningsmetoden som er valgt.

4.4.1 Reliabilitet

Reliabilitet handler om påliteligheten av studien, og hvorvidt en annen forsker som benytter samme metode ville kommet frem til samme resultat (Thagaard, 2013, s. 202). For å sikre oppgavens reliabilitet ble det tatt lydopptak under intervjuene. Dette ble gjort for å slippe å ta notater underveid slik at jeg kunne fokusere fullt og helt på intervjupersonen og deres reaksjoner. Dette bidro til en bedre flyt i intervjuet ettersom jeg kunne gi min fulle oppmerksomhet til intervjupersonen (Thagaard, 2013, s. 112).

Lydopptak under intervjuer ble særlig viktig ettersom alle intervjuene måtte tas over Teams grunnet koronasituasjonen. Når en ikke gjennomfører intervju ansikt til ansikt kan en miste verdifull interaksjon mellom forsker og intervjuperson, dette forsøkte jeg å unngå i størst mulig grad ved å fokusere kun på selve intervjuet. Etter hvert intervju ble lydopptaket så transkribert. Dette gav også mulighet til å kunne kvalitetssikre alle sitat ved å få de nedskrevet ordrett fra lydfilen. På denne måten utelukker en at ens egne fortolkninger kan påvirke oppgaven, og en skaper data som er mer uavhengige av forskerens oppfatninger enn ved bruk av notater (Thagaard, 2013, s. 203).

Det redegjøres også for det teoretiske rammeverket som legger grunnlaget for tolkningene som er gjort, forskningsstrategien som brukes, fremgangsmåte for innsamling av data og metodiske valg som er gjort i løpet av studien. Dette bidrar til å styrke oppgavens reliabilitet da det gir leseren innsikt i hvordan forskningsprosessen har foregått og hvordan jeg som forsker har kommet frem til oppgavens konklusjon (Thagaard, 2013, s. 202).

4.4.2 Validitet

Validitet handler om gyldighet av tolkning av data, og hvorvidt resultatene av studien gjenspeiler virkeligheten som studeres (Thagaard, 2013, s. 204). For å sikre studiens validitet ble alle intervjupersoner, samt kommunen de arbeider i anonymisert. Dette ble vurdert som viktig ettersom oppgaven undersøker en sensitiv tematikk, og gjennom å anonymisere kan intervjupersonene bli mer velvillige til å snakke åpent om tematikken. Anonymisering av intervjupersonene kan også føre til større tillit til forskeren om at informasjonen som kommer frem gjennom intervjuet vil bli vurdert gjennomgående slik at en ikke videreformidler eventuell sensitiv informasjon (Thagaard, 2013, s. 29). Gjennom å skape en slik tillit og åpenhet mellom forsker og intervjuperson kan det argumenteres for at resultatene av studien gjenspeiler virkeligheten som studeres i større grad.

Valget om å benytte lydopptak under intervjuet ble også viktig for å styrke oppgavens validitet. Ved å transkribere lydopptakene ordrett kunne jeg sikre korrekt gjengivelse av informantenes utsagn, og unngå påvirkning av mine egne fortolkninger. Det var også samsvar mellom studiens og informantenes forståelse av sentrale begreper som bevissthet og cybersikkerhet, som igjen styrker validiteten ved at det er enighet rundt den operasjonelle definisjonen av begrepene (Grønmo, 2016, s. 253).

4.4.3 Overførbarhet

Studiens overførbarhet vurderes i forhold til om studien kan være relevant i en større sammenheng (Thagaard, 2013, s. 211). Denne studien er en liten studie, avgrenset til én kommune. Med dette følger også visse begrensninger som påvirker studiens overførbarhet. Det er 356 kommuner i Norge av ulike størrelser og areal. Det kan tenkes at studien kan være overførbar til en viss grad til kommuner på lik størrelse med den aktuelle kommunen i studien. Men for kommuner som er større og mindre en denne kommunen følger det gjerne også mer eller mindre ressurser til slikt opplærings- og treningsmateriell. Likevel virket informantene å ha god innsikt i hvordan ulike kommuner arbeider med cybersikkerhet, og uttalte at det er store likheter i dette arbeidet i dag.

4.4.4 Etiske refleksjoner

Under forskningsprosessen er et det essensielt å ivareta deltakernes integritet og sikre at deltakerne ikke på noen måte tar skade av å delta i forskningen (Thagaard, 2013, s. 119). Dette etiske prinsippet har vært ledende for forskningsprosessen og de valg som er tatt i forhold til informantene. Før intervjuprosessen startet ble prosjektet meldt til NSD for å sikre at alle data bearbeides og lagres trygt. Etter NSD´s godkjenning av prosjektet har konfidensialitet vært etterstrebet. Av denne grunn valgte jeg å anonymisere informantene på en slik måte at deres identitet ikke kan gjenkjennes i oppgaven.

Jeg har også vært bevisst på hvordan jeg har behandlet og lagret informasjonen som kom frem gjennom intervjuene. Lydopptaket av intervjuene ble lagret på en egen båndopptaker, og ble transkribert etter hvert intervju slik at lydopptakene kunne slettes fortløpende. Det ble også sendt ut samtykkeskjema i forkant av hvert intervju for å sikre at alle informantene var klar over hva deltakelse i studien innebar for dem, samt hvordan informasjonen de gav fra seg ville bli behandlet slik at de kunne gi et informert samtykke til å delta i studien.

4.5 Metodiske styrker og svakheter

Ulike metoder for datainnsamling gir ulike måter å belyse et tema på. Den kvalitative forskningsmetoden i kombinasjon med en abduktiv tilnærming anses som en styrke i oppgaven ettersom det gav mulighet til et dypere dykk i temaet enn en kvantitativ metode ville gjort. En abduktiv tilnærming tilrettela også for veksling mellom teori og empiri ettersom jeg fikk mer innsikt i tematikken. Det anses også som en styrke at det ble benyttet en semi-strukturert tilnærming under intervjuene ettersom det tilrettela for å følge informantenes fortelling, og gav mulighet til å utdype temaene de tok opp som ikke var inkludert i intervjuguiden på forhånd. En semi-strukturert intervjusituasjon kan også bidra til å skape større tillit mellom intervjuperson og forsker da intervjupersonen kan føle seg mer i kontroll når en strukturerer temaene etter det de selv tar opp. På denne måten kan intervjupersonen være mer avslappet og åpen under intervjuet, dette anses som en styrke for oppgavens problemstilling (Thagaard, 2013, s. 97).

En faktor som kan ha preget svarene intervjupersonene gav under intervjuet er at de var klar over oppgavens tematikk på forhånd. Dette anses både som en styrke og en svakhet. At de visste hva intervjuet dreiet seg om, og fikk muligheten til å se over intervjuguiden på forhånd

kan ha vært en styrke ettersom de fikk litt tid til å reflektere og tenke over sine meninger før intervjuet. På den andre siden kan det gjøre at intervjupersonen ubevisst legger mer vekt på oppgavens tematikk enn det som er realiteten. Likevel opplevde jeg at intervjupersonene var veldig åpne og ærlige på hva som blir og ikke blir gjort i dag, samt hva de kunne gjort bedre.

Grunnet koronasituasjonen var det flere av de med sikkerhetsbakgrunn som jobbet innen cybersikkerhet som også hadde fått ansvar for å jobbe med smittesituasjonen i kommunen. Noen avdelinger var generelt hardere rammet av koronasituasjonen og hadde derfor ikke tid å avse til å delta i studien. Jeg fikk dermed færre intervjuer enn ønsket, og dette sees som en klar svakhet ved oppgaven. Likevel opplevde jeg en metning under datainnsamlingen da det fremkom lite ny informasjon under de siste intervjuene. Det at samtlige intervjupersoners utsagn bekreftet hverandre sees derfor som en styrke, særlig med tanke på at jeg kun fikk gjennomført fem intervjuer. Der det var tid mellom intervjuene valgte jeg å høre igjennom og transkribere hvert intervju før det neste, på denne måten dro jeg læring fra intervjusituasjonen og kunne forbedre mine prestasjoner i forhold til hvordan jeg stilte spørsmål for å få bedre flyt i samtalen.

Den innledende tanken ved oppgaven var som sagt å benytte kommunens interne, skriftlige dokumenter i første omgang, for så å supplere med intervjuer. Da det kun var en av informantene som oppgav at de hadde slike skriftlige dokumenter ble dokumentanalysen svært begrenset. Dette anses som en svakhet i oppgaven. Jeg måtte derfor fokusere på intervjuene i større grad. Det jeg fikk av informasjon fra kommunen gav likevel en innsikt i oppgavens tematikk, og et bedre grunnlag for intervjuguiden da jeg hadde noe informasjon å basere denne på.

5. Empiri

I dette kapittelet vil jeg presentere oppgavens funn gjort gjennom intervjuer og dokumentstudier som beskrevet i kapittel 4. Disse funnene bidrar til å svare på oppgavens problemstilling:

«Hvordan jobber kommunesektoren med opplæring og trening innenfor cybersikkerhet, hvilke utfordringer hemmer dette arbeidet - og hvilke implikasjoner har det for de ansattes bevissthet rundt cybersikkerhet?»

Kapitlene under er strukturert etter forskningsspørsmålene. Kapittel 5.1 vil omhandle hvilke tiltak kommunen gjennomfører for opplæring og trening for sine ansatte, samt hvilke utfordringer kommunen opplever i arbeidet med opplæring og trening. Jeg velger også her å inkludere informantenes forståelse av begrepene «cybersikkerhet» og «bevissthet» ettersom de setter rammene for oppgavens problemformulering. Til slutt vil jeg presentere kommunens tilretteleggelse for aktiv deltakelse i trenings- og opplæringsopplegg. Det må likevel påpekes at noen av funnene glir over i hverandre og vil nevnes både i 5.1 og 5.2.

5.1 Hva blir vektlagt i opplærings- og treningsopplegg i kommunen?

5.1.1 Skriftlige dokumenter

I starten av arbeidet med dette masterprosjektet etterspurte jeg skriftlige dokumenter av samtlige informanter fra de ulike avdelingene. De skriftlige dokumentene som ble etterspurt var, som nevnt tidligere, dokumenter som beskriver hvordan kommunen jobber med bevisstgjøring av de ansatte som blant annet prosedyrer, policyer, retningslinjer og planverk. Av de fem informantene som valgte å delta i studien var det kun én informant jeg fikk tilsendt dokumenter av (Informant A). De som ikke sendte noen skriftlige dokumenter, oppga følgende årsaker:

- Forholdsvis nyansatt og har ikke oversikt over skriftlige dokumenter, så det var for tidkrevende (Informant C)
- Har ikke dokumentasjon knyttet til cybersikkerhet på sitt nivå i avdelingen (Informant B og D)
- Har ingen dokumenter å sende (Informant E)

Under vil jeg gjennomgå det jeg fikk tilsendt av skriftlige dokumenter av informant A. Noe av det som fremkommer i disse dokumentene er likevel ting som gjelder for hele kommunen og som derfor også er relevant for de informantene som ikke sendte skriftlig dokumentasjon.

Det første dokumentet inneholder informasjon som sendes ut til alle ledere med informasjon om opplæringsplaner som er relevante for deres ansatte. Det informeres om hvilke typer kompetanse det er vurdert et behov for på bakgrunn av saker som er meldt inn til IT-avdelingen, samt hvor en finner disse opplæringsplanene. Jeg fikk også tilsendt et dokument tiltenkt ledere med en egen kompetanseplan for dem. Her poengteres også viktigheten av at planene blir gjennomført med bakgrunn i at lederne må ha kjennskap til det tekniske utstyret som benyttes, og sørge for at de ansatte har nok kunnskap til forsvarlig håndtering av systemene kommunen har valgt å bruke. I opplærings- og kompetanseplanene som gjaldt ledere og ansatte informeres det om at ikke alle kurs nødvendigvis er relevant for hver enkelt, og at de selv markerer det som ikke er relevant for dem.

Vedlagt lå det også med eksempler på nyhetssaker som blir lagt ut på intranettet for alle ansatte i hele kommunen. Her informeres det blant annet om å være varsom når en åpner vedlegg fra e-poster, forsvarlig bruk og håndtering av passord, forsvarlig forvaltning av pin-koder og brukernavn, og sikkerhetsreglementet som er gjeldende i kommunen. Det ligger også ved kontaktinformasjon til IT Support med en oppfordring om å ta kontakt dersom det er noe en er usikker på eller det er noe som virker mistenksomt. Et nytt tiltak kommunen også har startet med som ble kommunisert via nyhetssak på intranettet, er å melde avvik direkte på avdelingen eller personene det gjelder. Tidligere ble avvik meldt til IT-avdelingen. Dette er et tiltak som er startet for å forsøke å hindre alvorlige sikkerhetsbrister og skape bedre kultur for cybersikkerhet. Dette ble innført ettersom kommunen erfarte at årsaken til brudd ofte er at ansatte ikke er klar over at de bryter retningslinjene.

Jeg fikk også tilsendt taushetserklæring og sikkerhetsreglement som alle ansatte må skrive under på før de inntrer i sin stilling i kommunen. Her informeres det om de ansattes ansvar for å hindre uvedkommende innsyn i sensitive personopplysninger, samt enkle tiltak som skal overholdes på arbeidsplassen. Eksempler på slike tiltak som nevnes i sikkerhetsreglementet er at en henter utskrifter umiddelbart, at en ikke låner ut brukernavn og passord, og at en plasserer skjermen sin på en slik måte at uvedkommende ikke kan se hva som står. Skriver en

under på denne bekrefter en også at en har gjort seg kjent med de retningslinjer som gjelder for behandling av personopplysninger.

5.1.2 Informantenes forståelse av «cybersikkerhet»

Informantene presenterer forholdsvis lik forståelse av begrepet cybersikkerhet. Informant A forklarer at cybersikkerhet består av to ulike komponenter. På den ene siden har man den tekniske sikkerheten som består av IT-arkitekturen som skal sikre en for eventuelle angrep. På den andre siden har en det menneskelige, hvor en må sørge for at de ansatte har nok kompetanse til å bruke systemene riktig, og ikke handler på en måte som øker risikoen for uønskede hendelser. Informant B presenterer også en lik forståelse av cybersikkerheten som illustrert i utdraget under:

«Når en snakker om cybersikkerhet snakker man om hele spekteret. Ikke bare IT-systemene, men menneskene bak systemene, teknologien og prosessene. Så på mange måter bør en ikke fokusere på å jobbe med IT-lenger, men å jobbe med cybersikkerhet og se på hele spennet hvor menneskene er en ekstremt viktig del».

Når de ble spurt om hva de forstår med cybersikkerhet trekker flere informanter (C, D) frem viktigheten av de tre nøkkelbegrepene innenfor IKT-sikkerhet, konfidensialitet, integritet og tilgjengelighet. Informant C mener at konfidensialiteten innebærer at informasjonen kommunen lagrer og bearbeider skal være konfidensiell i alle ledd med tanke på korrespondanse, og hvor ulik informasjon kan lagres. Integriteten går på at all informasjon skal være korrekt og at en sikrer at ingen får tilgang til å endre informasjonen i kommunens systemer. Tilgjengelighet trekkes frem som det mest utfordrende fordi det krever en balanse mellom de to andre nøkkelbegrepene, konfidensialitet og integritet. Dersom en skal sikre de to førstnevnte kan det resultere i at en gjør informasjon utilgjengelig i større grad. Samtlige informanter hadde forholdsvis lik forståelse for begrepet cybersikkerhet, som D nevner er de i kommunen opptatt av å benytte seg av nasjonalt veiledningsmateriale når det kommer til cybersikkerhet, prosjektmetodeverk og gjennomføring av tiltak nettopp fordi:

«vi skal ikke sette oss ned å tenke kloke tanker selv når flinke folk har gjort det før oss, så det er litt bevisst».

5.1.3 Informantenes forståelse av begrepet «bevissthet»

Når det kommer til begrepet bevissthet presenterer informantene også her forholdsvis lik forståelse. Informant A starter med å forklare bevissthet som at en:

«faktisk får med deg det som blir sagt, at en har tygget igjennom det en blir fortalt og at du kan det teoretiske. At en kan ta og manifestere det, og at en kan se det i praksis, bruke det i praksis og gjøre det til en del av hverdagen».

Informant A legger også vekt på at bevissthet handler om å implementere cybersikkerhet inn i hverdagsarbeidet, og at *«en ikke bare kan dra det frem av skuffen innimellom».* Det nevnes også at bevissthet handler om å være på vakt mot ting som kan oppleves mistenksomt på arbeidsplassen. For eksempel om ting oppleves for godt til å være sant, så er det som regel det. Informant C mener derfor at bevissthet er det motsatte av å være ukritisk.

Oppmerksomhet er også et ord som kom opp i sammenheng med bevissthet. Det å være oppmerksom i arbeidet sitt, samt å være klar over sin rolle eller sitt ansvar på arbeidsplassen. Det nevnes også at bevissthet handler om å vite at handlingen en utfører kan få konsekvenser for hele virksomheten. For eksempel om en får en phishing-mail legger kommunen vekt på å informere om konsekvenser som kan forekomme om en ikke er oppmerksom, og derfor klikker på en link. Dersom en er klar over risikoen ulike handlinger kan medføre vil en være mer bevisst (Informant D). Informant E svarer følgende på betydningen av de ansattes bevissthet mot cybertrusler:

«Bare sånn ut av mitt hode, så tenker jo at det har en veldig stor betydning, kanskje en avgjørende betydning for det vil kunne avgjøre om en på en måte er oppmerksom på eller fanger opp om en for eksempel får en type phishing-mail. Om man fanger opp eller stiller spørsmålstegn ved de små avvikene som kanskje er, eller at en ser at noen driver og snoker rundt eller viser interesse for noe som de ikke burde vist interesse for. At en er rett og slett litt sånn årvåken og kombinert med kunnskap slik at en vet hva en skal være årvåken på.»

5.1.4 Kommunens tiltak for opplæring og trening

Av intervjuene fremkommer det at kommunen kjører en forholdsvis overordnet strategi for opplæring og trening med noen avdelingsinterne ulikheter. Hele kommunen benytter blant annet en del kurs gjennom KS (kommunesektorens organisasjon) for ledere og ansatte. KS har

en egen plattform som heter KS læring som består av mange kurs som er relevante for kommunene og dens ansatte. Her deles kurs fra ulike kommuner, både i Norge og Skandinavia slik at kursmateriale til enhver tid er mest mulig oppdatert. Opplæringsmaterialet i kommunen består av åtte e-læringsmoduler med ulike kurs som blant annet inkluderer informasjonssikkerhet, personvern, bruk av mobile enheter, informasjon om ulike angrepsmetoder og lagring av informasjon. Dette er kurs som alle de ansatte er pålagt å gjennomgå én gang. Kursene består av informasjonsvideoer, samt noen spørsmål som skal besvares både i løpet av kurset, samt på slutten. Jeg fikk muligheten til å gjennomføre et slikt kurs og så da at kurset startet med en egenvurdering av ens kunnskap før kurset, for så en ny vurdering etter kurset. Dette fordi det er ønskelig å se om kurset gir ekstra påfyll av kunnskap og dermed en økt bevissthet og trygghet om kursets tematikk. Disse kursene er lagt opp slik at den som står ansvarlig for de ansattes gjennomføring på hver avdeling har oversikt over hvem som har fullført og ikke. På denne måten kan de ta direkte kontakt med dem som ikke har fullført, oppfordre dem til å ta kurset, og sikrer dermed at alle ansatte har gjennomført alle kurs.

Flere av informantene på de ulike avdelingene opplyste også om at de benyttet nyhetssaker for å nå ut til sine ansatte (Informant A, B, E). I disse opplyses det blant annet om hendelser som har skjedd i andre virksomheter, nye angrepsmetoder eller typer angrep som er spesielt relevante, hvor en finner opplæringsplaner, hvilke opplæringskurs som bør tas, samt hvem en kan kontakte om en lurer på noe. Her har også de ansatte mulighet til å påvirke hva det skrives nyhetssaker om. Som informant A legger vekt på er det de som jobber ute i avdelingene og benytter disse systemene som ser best hva som «rører seg». Det vektlegges derfor å få feedback fra dem om hva som anses som viktig å informere alle ansatte i ulike avdelinger om. Et tiltak kommunen benytter for å tilrettelegge for å få slik feedback er rapportering av avvik. Dette regnes ikke som en del av opplæringen, men benyttes som en form for trening. De ansatte blir oppfordret til å rapportere avvik dersom de oppdager noe som virker mistenkelig eller som vekker bekymring. Kommunen har også tidvis innført belønning for rapportering av avvik for å forsøke å sette terskelen for at de ansatte rapporterer inn avvik lavest mulig. De ansatte oppfordres til å gi tilbakemelding på alt fra små til store avvik, slik at denne informasjonen kan deles med andre ansatte som kan dra nytte av den. På denne måten sikrer de at nyhetssakene som deles har relevans for de ansatte i sitt daglige arbeid med cybersikkerhet.

Det vektlegges både i nyhetssakene og i den generelle informasjonen som deles å konkretisere det slik at det får en praktisk nytteverdi for de ansatte. På denne måten ønsker de at de ansatte skal forstå at *«dette er noe som angår meg»* (Informant E). Det forsøkes derfor å kommunisere informasjonen på en hensiktsmessig måte, med størst mulig forenkling av begreper som kan være for abstrakte for den vanlige ansatte.

Kommunen gjennomfører også en øvelse eller test hvert år som bestilles inn fra en ekstern aktør. Siste test som ble gjennomført var en penetrasjonstest i form av en phishing-mail. På denne måten kan de teste hvor godt opplæringen og treningen fungerer i praksis. Informant A illustrerer fordelene med å gjennomføre slike tester i utdraget under:

«Vi bestiller årlig noen utenifra til å gjøre et angrep. For eksempel, sist var det en penetreringstest. Da avdekket vi at de tjenestene vi bruker for å oppdage det fungerte, også merket vi også noen svakheter, og de tar vi jo tak i med en gang. Det er jo derfor vi jevnlig har sånne tester for å se hvor svakhetene er, for verden endrer seg jo hele veien, teknologien endrer seg kjapt, så derfor må vi ha litt hjelp til å sjekke hvor svakhetene våre er slik at vi kan gjøre noe med dem».

Informant A og B nevner også at det ble innført et nytt arbeidsmål om god sikkerhetskultur det siste året. Dette inkluderer å jobbe med kommunikasjon og diskusjon med de ansatte om det som angår cybersikkerhet. Å forbedre sikkerhetskulturen er noe som har vært spesielt i fokus i 2020 og 2021, men dette er noe som kommunen ser er viktig og som de vil fortsette å jobbe med. Den største utfordringen flere av avdelingene opplever når det kommer til sikkerhetskulturen i dag er at cybersikkerhet anses som IT-avdelingens ansvar. Dette er en holdning som forsøkes endret gjennom økt bevissthet, som utdraget under illustrerer:

«Bevisstheten i dag ligger i at det er IT-avdelingen som tar seg av sikkerhet. Det er jo litt misforstått for alle ansatte skal jo ivareta IT-sikkerheten, tilbake til det jeg har sagt hele tiden. Man tror at IT-sikkerhet det er noe som har med IT-avdelingen å gjøre, da tar de og sikrer oss. Hva skal jeg gjøre, nei ingenting, jeg trenger ikke å gjøre noe, hvis det går galt så er det ikke min feil uansett. Og det er en litt dårlig holdning å ha når en snakker om IT-sikkerhet. Sikkerheten igjen er ikke sterkere enn det svakeste leddet (...) det er lett å si at IT-avdelingen jobber med informasjonssikkerhet. Men det er ikke nok, hele virksomheten må

jobbe med informasjonssikkerhet. Så dette handler jo om å skape en sikkerhetskultur og skape et sikkerhetsengasjement.» (Informant B)

Når det kommer til dette med sikkerhetskultur og bevisstgjøring trekker flere av informantene (A, B, E) frem repetisjon som en sentral faktor. De mener at opplæringen ikke bare kan være en engangsgreie eller noe en kjører innimellom, men at de små dryppene i hverdagen kan være vel så viktig for det holdningsskapende og bevisstgjørende arbeidet i kommunen. Når informant B ble spurt om hvilke elementer de fokuserte på for å sikre størst mulig utbytte for de ansattes kompetanseutvikling kom følgende uttalelse:

«Repetisjon, repetisjon, repetisjon, repetisjon, det er også veldig viktig at en varierer spørsmålene og varierer opplegget. Gjør det spennende og interessant. Belønne de som får det til og repetere jevnlig for å holde det friskt i minnet, det tror jeg er veldig viktig.»

Jevnlig repetisjon av opplæringsmaterialer og små drypp med informasjon i hverdagen trekkes også frem grunnet den raske teknologiske utviklingen. Det krever konstant modernisering for å holde seg oppdatert på samfunnets trusselbilde til enhver tid. Flere informanter var åpne om at de gjerne skulle gjort mer, men med de ressursene de har i dag er det ikke mulig.

5.1.5 Kommunens kommunikasjon av cybersikkerhet

I løpet av intervjuene fremkom det også elementer som vektlegges når det kommer til kommunikasjon rundt cybersikkerhet. Trygghet er et ord som flere informanter (A, B) nevnte når vi snakket om opplæring, trening og arbeidet med cybersikkerhet. Informant A nevner viktigheten av at alle skal føle seg trygge i sin rolle og på sitt ansvar på arbeidsplassen. Dette anses som essensielt ettersom frykt, usikkerhet og tvil kan drepe engasjementet til de ansatte når det kommer til cybersikkerhet. De er derfor opptatt av å kommunisere cybersikkerhet ved å legge vekt på at IT-avdelingen er dere for å hjelpe dem, ikke for å straffe dem, og på denne måten tilrettelegge og senke terskelen for at de ansatte tar kontakt om det er noe de er usikre på. Informant B nevnte også viktigheten av at de ansatte skal føle at de har et trygt sted å henvende seg til om det er noe de trenger hjelp til eller om de har en bekymring.

Informant A nevner også at de er opptatt av måten de kommuniserer gjennomføring av kurs ved å forsøke å gi de ansatte mer eierskap over opplæringsarbeidet. De er oppmerksomme på å ikke gjøre det til en plikt som påføres dem ovenfra, men å bruke inkluderende språkbruk som illustrert i følgende utdrag:

«Jeg prøver å bruke kursene som noe vi har sammen sånn at de skal få litt mer eierskap til opplæringsplanen. For jeg tror ikke mye på pekefinger. Jeg tror mye mer på at hvis vi snakker sammen og prøver å snakke på et språk vi forstår hverandre på, så er det mye lettere å få med seg de andre til å skjønne viktigheten av det og faktisk gjøre noe med det. Vi må spille på lag tenker jeg.»

Dette korrelerer med informant D sine uttalelser om hvordan en kan kommunisere cybersikkerhet på en måte som motiverer de ansatte. Informant D mener at cybersikkerhet og sikkerhet generelt fort kan få et litt negativt fokus hvor en får beskjed om alt en ikke skal gjøre, og hvor skummelt og farlig det kan være. Dette kan gjøre det vanskelig å få folk med på laget, da påført frykt kan minske de ansattes engasjement og motivasjon rundt cybersikkerhetsarbeidet. Informantene mener derfor at en bør gi cybersikkerhet et mer positivt fokus og legge mer vekt på hvordan en som ansatt kan bidra til å gjøre sikkerheten bedre. Selv om fryktbasert kommunikasjon frarådes nevnes kommunikasjon om potensielle konsekvenser av ulike handlinger av flere informanter som en motiverende faktor for at de ansatte skal engasjere seg i cybersikkerhetsarbeidet (Informant A, C, D, E). Dette fordi det skaper en forståelse, blant annet for hvorfor en gjennomfører ulike tiltak, hvorfor en skal være oppmerksom på cybertrusler og hvorfor en skal gjennomføre ulike kurs. Kommunen jobber med generell informasjon av konsekvenser av ulike feilhandlinger og cybertrusler en kan møte på i arbeidshverdagen, samt kommunikasjon av relevante konsekvenser andre virksomheter utsettes for i Norge. Et eksempel på dette var når kommunen forsøkte å implementere tofaktorautentisering i 2020. De møtte da på motstand fra noen ansatte grunnet at noen ting ble mindre tilgjengelig og mer tungvint. Etter at Stortinget ble angrepet på epost ble det derimot større støtte i organisasjonen for å implementere tofaktorautentisering, og det ble gjennomslagskraft for å gjennomføre det uten mye motstand. Det å bruke relevante eksempler og forklare mulige konsekvenser av å ikke implementere sikkerhetstiltak øker de ansattes velvilje til å være med på endringen selv om det kan gjøre informasjon mindre tilgjengelig. Informant D illustrerer dette i følgende utdrag:

«Det at de ansatte forstår relevansen de har i sikkerhetsarbeidet tror jeg kan ha ganske masse å si. Det kan ha stor betydning det at de ansatte er klar over konsekvensene av å ikke innføre sikkerhetstiltak. Å fortelle hva konsekvensene kan være og kunne være åpen synes jeg er det viktigste når du jobber med dette arbeidet. Da får de ansatte forståelse for hvorfor vi gjør det vi gjør og blir mer motivert til å godta endringene».

Informant A trekker også inn det å være åpen med sine ansatte om ulike konsekvenser av uønskede handlinger. Informanten mener at måten en kommuniserer disse konsekvensene på kan ha stor betydning for de ansattes bevissthet. Det skal nødvendigvis ikke være en skremselspropaganda som tvinger folk til å være oppmerksomme, så det er viktig å tenke over hvordan en legger det frem. Informant A legger vekt på at en ikke bare skal fokusere på alt en ikke skal gjøre, og hvor farlig det kan være, men at de ansatte blir mer motivert av å høre hva en skal gjøre og hvordan:

«Jeg tror det kan være lurt å ha et litt mer positivt fokus enn bare pekefinger da, og sette de ansatte i stand til å få nok kunnskap om eller nok kompetanse om hvordan de skal handle riktig da, ikke bare hvordan de ikke skal gjøre. Det verste er når ting går litt over hodet på folk, da gir en jo litt opp av og til og tenker at det er ikke noe jeg trenger å bry meg om, for jeg skjønner ikke hva de snakker om uansett. Så jeg tenker at det å jekke ned, og bruke språk som alle skjønner, dette med klart språk er viktig».

Språkbruk er også et viktig punkt som kom opp igjennom intervjuene. Som informanten ovenfor nevner er klart språkbruk viktig i kommunikasjon med de ansatte. De har erfart i kommunen at ulike avdelinger kan ha sin egen språkkultur og sitt eget fagspråk. Det er en stor organisasjon med et stort spekter av ulike mennesker med ulik bakgrunn. Dersom en skal nå gjennom til alle må en bruke et språk som alle forstår. Hvordan kommunen jobber for å sikre klart språkbruk i kommunikasjonen som går ut til de ansatte kommer jeg tilbake til i delkapittel 5.2.1.

5.1.6 Kommunens utfordringer med cybersikkerhetsarbeidet

Gjennom intervjuene ble jeg også presentert for noen sentrale utfordringer kommunen møter på i sitt cybersikkerhetsarbeid. Et element som samtlige informanter nevnte som en stor utfordring var det å tilpasse opplærings- og treningsopplegget til ulike ansatte. I dag jobber de med et overordnet opplegg som er beregnet på dem som kan minst. Som informant A uttaler har de veldig mange ulike typer mennesker i kommunen, og det er utfordrende å inkludere alle i en generalisert opplæringsplan. De har blant annet lærere, helsepersonell, ingeniører, resepsjonister og økonomer, det er ulike mennesker med ulike behov som krever ulik opplæring. Informantene oppgir at de gjerne skulle tilpasset skriftlig dokumentasjon og opplæringsmateriell i større grad, men at det krever mye arbeid, noe de ikke har ressurser til å gjennomføre i dag. Når alle de ulike avdelingene gjennomfører samme opplæringsmateriell vil det da si at de selv står ansvarlige for å oversette det til sin spesifikke avdeling og dens behov. Informant C uttaler illustrerer dette i følgende utdrag:

«Det er slik at alle nyansatte må gå igjennom en opplæringsplan knyttet til blant annet IT-sikkerhet og gjennomføre et sånn lite kurs i personvern og datasikkerhet. Der kommer det jo frem prosedyrer og retningslinjer og den slags, men jeg ser at utfordringen nok er at dette er en ting som gjelder for alle ansatte også er det veldig forskjellig hvordan dette ser ut om en jobber innen helse, eller om en jobber innen skole eller kommunikasjon eller hva en jobber med. Og jeg tror nok at utfordringen blir i stor grad å oversette det til den jobben du gjør, sånn at du forstår at, dette kan jeg faktisk lagre i google drive eller dette må jeg lagre i arkivsystemet vårt.»

Hvor en for eksempel skal lagre ulik informasjon med ulik grad av sensitivitet i de ulike avdelingene kan derfor bli en risikovurdering som den enkelte ansatte må vurdere selv. Ideelt sett, med tid og ressurser, ser informantene at tilpasset opplæring til de ulike tjenesteområdene hadde vært positivt for den helhetlige cybersikkerheten i kommunen. På den måten kunne det blitt kjørt opplæringsmateriell med fokus på problemstillinger som er relevant for avdelingen og som er tilpasset deres hverdag (Informant B, C, D). Som nevnt tidligere ser kommunen at dersom en klarer å gjøre opplæringsmateriellet relevant og nært knyttet de ansattes hverdag drar de ansatte mer nytte av det og kan enklere implementere det i sitt hverdagsarbeid. Cybersikkerhet er jo også noe en tradisjonelt sett har snakket om i tekniske fora, og det består av et begrepsapparat som ikke er tilgjengelig for folk flest. Det å

forenkle og allmenngjøre denne kunnskapen til enhver ansatt er et utfordrende arbeid som fortsatt jobbes med i kommunen (Informant E).

En annen utfordring informantene oppgir at de møter på i arbeidet med cybersikkerhet, som en stor organisasjon, er å få til en overordnet koordinering mellom de ulike tjenesteområdene. Hver avdeling jobber litt hver for seg, og det er krevende å samordne og koordinere tiltakene godt nok. Faren ved dette er at det kan utgjøre en trussel når en i økende grad digitaliserer tjenester. Manglende koordinering og samarbeid i digitaliseringen kan føre til at data blir tilgjengelig for uvedkomne (Informant D). Et overordnet, helthetlig arbeid med cybersikkerhet krever koordinering på tvers av tjenesteområdene, noe som vil være ekstremt ressurskrevende. Informant E savner en mer overordnet og systematisk tilnærming til opplæring og kommunikasjon av den digitale sikkerheten i kommunen, og mener dette kunne styrket den helhetlige cybersikkerheten. Å koordinere cybersikkerheten på tvers av tjenesteområdene i kommunen anses også som utfordrende ettersom hvert tjenesteområde står overfor ulike problemstillinger og har ulike behov. Informant A trekker frem den vanskelige avveiningen mellom service og sikkerhet. Denne vil være ulik for ulike tjenesteområder, for eksempel sitter avdelingen helse og velferd på mye sensitiv informasjon og må derfor prioritere personvern i stor grad. For andre tjenesteområder vil det gjerne være andre faktorer som må prioriteres i større grad. Det jobbes derfor fortsatt forholdsvis fragmentert med cybersikkerhet i kommunen, og det vil være vanskelig å koordinere dette arbeidet når en opererer med ulike avdelinger som tilbyr ulike tjenester. Informant D oppgir også at kommunen ønsker å dele data, og operere med åpne datakilder som kan komme innbyggerne og næringslivet til gode. Men at det også her må gjøres avveininger mellom konfidensialitet, integritet og tilgjengelighet.

Informant D nevner også at det kan utgjøre en risiko dersom en går en lengre periode uten uønskede sikkerhetshendelser, og at det da kan dannes en tankegang i øverste ledelse om at de har full kontroll på sikkerheten. Men som informanten også nevner skal det bare en alvorlig sikkerhetshendelse til før det verdensbildet raser sammen.

5.2 Hvordan tilrettelegges det for aktiv deltakelse i opplærings- og treningsopplegg i kommunen?

5.2.1 Kommunens bruk av diskusjon i opplæring og trening

Under intervjuene ble diskusjon nevnt som et positivt tiltak for aktiv deltakelse i opplæring og trening. En utfordring som er nevnt tidligere i oppgaven er dette med å benytte forståelig språk når en snakker om cybersikkerhet. Samt å kommunisere hva som er relevant for den enkelte ansatte og det aktuelle tjenesteområde, og på den måten gjøre det relevant og forståelig for alle. Som informant C sier så er kommunen en sammensatt organisasjon med flere 1000 ansatte, og det kan være vanskelig å nå ut til alle:

«Det er en utfordring med å skape bevissthet rundt digital sikkerhet i virksomhetene når vår virksomhet er en virksomhet som har så mange ulike avdelinger. Vi er ikke en bedrift som produserer et produkt og har strømlinjeformet at alle jobber med det samme. En kommune er jo ganske sammensatt kan du si».

For å motvirke at folk ikke forstår informasjon som legges ut, og for å legge til rette for alle ansatte beskriver informant A hvordan de benytter kommentarfelt i alle nyhetssaker som blir lagt ut. Dette gjøres fordi de har erfart at innenfor cybersikkerhet så kan visse begreper bli for abstrakte for den vanlige ansatte. Dersom de ikke forstår hva som blir informert om så er det fort gjort å se bort ifra det. Ved å benytte kommentarfelt under nyhetssaker på intranettet tilrettelegges det for at de ansatte kan si ifra om det er noe de ikke forstår eller om det er noe de er usikre på. På denne måten kan språket og teksten justeres slik at alle forstår hva det gjelder og hvordan de skal bruke det. Dette er en måte kommunen tilrettelegger for aktiv deltakelse i cybersikkerhetsarbeidet.

Under kommentarfeltet i nyhetssaker som publiseres på intranettet observerer informantene også at de ansatte både gir tilbakemeldinger og diskuterer seg imellom. Denne plattformen som åpner for diskusjon anses som positiv i arbeidet med å skape bevissthet rundt cybertrusler blant de ansatte. Et eksempel fra informant A illustrer dette:

«Når det skulle innføres tofaktorautentisering ble det mye diskusjon, og jeg tenker at diskusjon er bra. Når du har kommentarfeltet åpent, da får du kanskje noen sure kommentarer også er det noen som svarer på en skikkelig måte og sier at dette er ikke for å gjøre livet vanskelig, det er faktisk på grunn av sikkerhetshensyn. Så jeg tenker at det er en

sunn diskusjon å ha. Det er helt supert at en ansatt på sykehjem kan være med i diskusjonen på lik linje med oss fra IT. Da ble det bevissthet også for hvorfor vi gjorde det».

Diskusjon trekkes altså frem som en fin form for aktiv deltakelse for de ansatte. I tillegg til at det skaper bevissthet for cybersikkerhet gir det også variasjon fra de typiske e-læringskursene. Informant D som er med på å utarbeide et nytt informasjonssikkerhetsstyringssystem mener at diskusjon er positivt både på grunn av variasjonen det gir, samt at en får en annen form for samspill og dynamikk mellom de ansatte. Diskusjonsøvelser er derfor noe som skal innføres i større grad i dette nye informasjonssikkerhetsstyringssystemet slik at de ansatte blir aktivisert og utfordret i større grad.

5.2.2 Kommunens bruk av praktisk utførelse i opplæring og trening

Informantene ble også spurt om de har noen form for opplæring og trening som tilrettelegger for aktiv deltakelse i form av praktisk utførelse. Da var det to elementer som fremkom av intervjuene, nemlig quiz som skal besvares i løpet av kursene de gjennomfører og årlige bestilte øvelser fra en ekstern aktør.

Under disse kursene som utføres gjennom opplæringen må de ansatte gjennomføre en quiz. Dette skjer i samsvar med videoer som presenteres i løpet av kurset, hvor den ansatte så må svare på noen enkle spørsmål om hva de har lært, eller en type vurdering av egen kunnskap både før og etter kurset. Informant C svarer følgende på spørsmål om hvordan de tilrettelegger for aktiv deltakelse i opplæringen:

«Da drar jeg jo frem disse opplæringsplanene da som krever at en responderer, altså at det ikke bare er informasjon, men at det er noe som krever respons. Det vi har nå er en video med en quiz i etterkant, det er jo gjerne det vi har av trening som krever aktiv deltakelse tenker jeg.»

Informant D trekker også frem at når en gjennomgår disse kursene så må en også aktivt trykke seg videre til neste side, i tillegg til å trykke på et alternativ her og der. På denne måten forsøker de å gjøre kursene mest mulig interaktive slik at en holder oppmerksomheten til de ansatte gjennom hele kurset.

Det bestilles også årlig inn en ekstern aktør til å gjennomføre en øvelse i kommunen. Dette gjelder for alle tjenesteområdene og alle ansatte. Gjennom slike tester får de ansatte testet sin

kunnskap og sine ferdigheter i praksis. I 2020 ble det gjennomført en penetreringstest ved bruk av en phishing-mail for å teste hvordan de ansatte responderte på dette, og hvorvidt det ble oppdaget. Gjennom slike tester får de derfor testet de ansatte sine ferdigheter, samt at kommunen ser hvor svakhetene er og kan gjøre noe med dem. Disse behovene som identifiseres blir da implementert i større grad i opplæringen, og forhåpentligvis gjør det de ansatte bedre rustet til å håndtere cybertrusler i fremtiden.

6 Diskusjon

I dette kapittelet vil de empiriske funnene redegjort for i kapittel 5, drøftes opp mot oppgavens teoretiske rammeverk presentert i kapittel 3. Kapitlene under er inndelt etter forskningsspørsmålene. Først tar jeg for meg FS1: *«Hva blir vektlagt i opplærings- og treningsopplegget i kommunen, og hvilke utfordringer hemmer dette arbeidet?»,* for så å gjennomgå FS2: *«Hvordan tilrettelegges det for aktiv deltakelse i opplærings- og treningsopplegg i kommunen, og hvilke implikasjoner har det for de ansattes bevissthet?».*

6.1 Hvilken betydning har kommunens vektlegging av opplæring og trening for de ansattes bevissthet rundt cybersikkerhet?

I dette delkapittelet vil jeg redegjøre for kommunens bruk av skriftlige dokumenter, informantenes forståelse av begrepene cybersikkerhet og bevissthet, bevisstgjøringstiltak de benytter, deres kommunikasjon av cybersikkerhet og hvilke implikasjoner disse elementene har for de ansattes bevissthet rundt cybersikkerhet. Avslutningsvis vil det drøftes rundt elementer som hemmer dette arbeidet.

6.1.1 Hvordan påvirker de skriftlige dokumentene som omhandler cybersikkerhet de ansattes bevissthet mot cybertrusler?

De ansattes kunnskap og bevissthet er en av de viktigste forutsetningene for å etablere og opprettholde et akseptabelt nivå av informasjonssikkerhet i en virksomhet. Mangel på slik kunnskap og bevissthet er som regel den største trusselen mot informasjonssikkerheten (Daler, Gulbrandsen, Høie & Sjølstad, 2019, s. 213). Ifølge Daler et al., (2019) er innføring i regler og retningslinjer, samt kjennskap til rutiner for hvordan en skal forvalte IT-systemene sikkerhetsmessig korrekt, en viktig del av de ansattes opplæring rundt cybersikkerhet. For å sikre at de ansatte har kjennskap til disse tingene sender kommunen ut sikkerhetsreglement og taushetserklæring til de ansatte. Den enkelte ansatte skal sette seg inn i disse dokumentene og skrive under på at de har gjort seg kjent med informasjonen før de inntrer i sin stilling i kommunen. Dette er et godt tiltak for å sikre at alle ansatte har kjennskap til regler og retningslinjer, men som informant A, B og E nevner er repetisjon et viktig element i bevisstgjøringen av de ansatte. At en kun har krav om underskrift når en inntrer i stillingen sin kan derfor føre til at bevisstheten svekkes over tid. Dette argumentet støttes av informant A sitt utsagn om at brudd på cybersikkerheten ofte skyldes at de ansatte ikke er klar over at de bryter kommunens retningslinjer.

Nyhetssaker er også et element flere informanter benytter seg av for å spre informasjon til de ansatte. Her informeres det blant annet om cybersikkerhetsbrudd i andre kommuner og hvilke konsekvenser det fikk for dem. Som flere informanter trekker frem, er de ansattes forståelse for potensielle konsekvenser av brudd på cybersikkerheten en sentral faktor for deres motivasjon for å opprettholde god cybersikkerhet. Informant D trekker frem at de ansatte er mer bevisste dersom de er klar over risikoen og konsekvensene ulike handlinger kan medføre for organisasjonen. Dette samsvarer med Daler et al. (2019) sin teori om bevisstgjøring, hvor informasjon om hvorfor sikkerhet er nødvendig er en viktig motivasjonsfaktor for de ansatte, fordi de da forstår hvorfor det for eksempel innføres nye sikkerhetstiltak. Det blir bevissthet for hvorfor de må følge retningslinjer og prosedyrer, eller hvorfor endringer implementeres. Informant A nevnte et eksempel på viktigheten av slik forståelse for konsekvenser når de forsøkte å implementere tofaktorautentisering i kommunen i 2020. Som nevnt i 5.2.1 var det innledningsvis mye motstand fra de ansatte grunnet at ting ble mer tungvint, og informasjon ble mindre tilgjengelig. Men etter angrepet på Stortinget ble det lagt ut en nyhetssak om hendelsen, de ansatte forsto da hvorfor tiltaket ble innført og det ble større gjennomslagskraft for gjennomføringen. Dette eksempelet illustrerer hvordan informasjon om sikkerhet og økt forståelse for hvorfor sikkerhetstiltak implementeres, øker de ansattes vilje og motivasjon til å etterfølge sikkerhetstiltak. De får økt bevissthet for cybersikkerheten i virksomheten og forstår derigjennom hvorfor slike sikkerhetstiltak er nødvendige (Daler, 2019).

6.1.2 Informantenes forståelse av begrepene cybersikkerhet og bevissthet

Da informantene ble spurt om deres forståelse av begrepene cybersikkerhet og bevissthet presenterte de alle forholdvis lik forståelse for begrepene. Deres forståelse for cybersikkerhet handlet om det helhetlige bildet som inkluderer både den tekniske sikkerheten, og det som går på det menneskelige. Når det kommer til det menneskelige var det stort fokus på kompetanse til å bruke IT-systemene på en sikker og forsvarlig måte, samt å ikke handle på en måte som øker risikoen for sikkerhetshendelser.

Informantene presenterte også en forholdsvis samsvart forståelse for bevissthet som begrep. De nevnte viktige ord og setninger som «å være på vakt», «det motsatte av å være ukritisk», oppmerksomhet og årvåkenhet. Samtlige informanter mente også at de ansattes bevissthet var viktig i kommunens arbeid med cybersikkerhet. Som informant A nevner er det viktig å implementere bevissthet i hverdagsarbeidet med cybersikkerhet, og at en er oppmerksom på

ens rolle og ansvar på arbeidsplassen. Informantene nevnte at det var mangel på koordinering i opplæringen og treningen innenfor cybersikkerhet i kommunen. At de har en lik forståelse for disse grunnleggende begrepene legger derimot et godt utgangspunkt for et godt, helhetlig arbeid med cybersikkerhet og bevisstgjøring.

6.1.3 Hvordan påvirker kommunens tiltak for opplæring og trening de ansattes bevissthet mot cybersikkerhet?

Gjennom de skriftlige dokumentene som nevnes ovenfor får de ansatte kunnskap om kommunens sikkerhetsreglement, og korrekt og sikker bruk av IT-systemene. Kunnskap er et resultat av erfaringer, tolkninger og meninger. Når en benytter denne tilegnede kunnskapen gjennom refleksjon, interaksjon og sosiale kontekster kan en få evnen til å danne en forventning om hvordan ulik respons på ulike situasjoner resulterer i ulike utfall. Om en så videreutvikler denne kunnskapen gjennom deltakelse og anvendelse i praksis vil de ansatte kunne utvikle kompetanse om det de har lært (Filstad, 2016, s. 124). Under vil jeg gjennomgå elementene kommunen benytter både for å videreutvikle de ansattes eksisterende kunnskap, samt hvordan de tilrettelegger for aktiv deltakelse og trening i praksis for å utvikle kompetanse og bevissthet rundt cybersikkerhet.

Det som vektlegges i størst grad av samtlige informanter når de ble spurt om hvordan de kjører opplæring innenfor cybersikkerhet for de ansatte er kursing. Kommunen benytter som sagt en plattform som heter KS læring, hvor de har satt sammen et opplæringsmateriell som består av åtte e-læringsmoduler. Disse omhandler viktige temaer innenfor cybersikkerhet som personvern, forsvarlig bruk av mobile enheter, informasjon om ulike angrepsmetoder, forsvarlig lagring av informasjon og generell cybersikkerhet. Dette er kurs som gjennomgås én gang i løpet av de ansattes arbeidstid i kommunen. Filstad (2016) nevner kurs som et meget viktig element for læring på arbeidsplassen. Når det kommer til læring på arbeidsplassen legges det også vekt på å tilrettelegge for å praktisere kunnskapen en har tilegnet seg i praksis, samt viktigheten av interaksjon og aktiv deltakelse (Olsen, 2016, s. 246). Informant D forteller at de forsøker å benytte seg av kurs som er interaktive. Kursene inneholder derfor en eller flere spørsmål som må besvares både før, under og etter gjennomført kurs. En må også aktivt klikke seg videre mellom hver side, på denne måten forsøker kommunen å holde de ansattes oppmerksomhet gjennom hele kurset og sørge for å aktivisere dem underveis. Men som informant C nevner er det begrenset hvor aktivisert en kan bli når en sitter foran PC-skjermen. Slike interaktive kurs med videoer og spørsmål er

likevel et godt tiltak, og vil kunne bedre de ansattes bevissthet gjennom økt kunnskap og forbedrede ferdigheter til å håndtere situasjoner med potensielle forsøk på angrep. Men selv om kursene er interaktive gir de ikke mulighet for praktisk utførelse i en simulert reell situasjon. Fra en studie utført av Filstad i 2012 fremkommer det at praktisk utførelse av oppgaver er av størst betydning for læring i organisasjoner. Disse kursene vil nok kunne øke de ansattes kunnskap i stor grad, men hvorvidt det øker deres kompetanse, og derigjennom forståelse og bevissthet for cybersikkerhet kommer jeg tilbake til i delkapittel 6.2.2.

Slike kurs som benyttes i opplæring og trening rundt cybersikkerhet har også en svakhet ved at de kun uttrykker eksplisitt kunnskap. Eksplisitt kunnskap er *«den kunnskapen som kan uttrykkes gjennom språket»* (Filstad, 2016, s. 114). De ansatte kan utvikle taus kunnskap når de gjennomgår dette kurset ved å vurdere den informasjonen de har fått gjennom videoene og svare på spørsmål, men en får likevel ikke inkludert alle typer handlinger og situasjoner en kan måtte håndtere i løpet av arbeidshverdagen. Taus kunnskap er spesifikk i den forstand at en må ta hensyn til ulike kontekster og situasjoner, og dette er vanskelig å få til gjennom standardiserte kurs som skal være relevante for hele kommunen (Filstad, 2016, s. 115). Særlig ettersom kommunen opererer med mange ulike tjenesteområder hvor de ansatte har ulike arbeidshverdager og oppgaver. Den beste formen for læring er som nevnt i teorikapittelet en kombinasjon av å forklare eksplisitt, og samtidig være i en situasjon som gir mulighet for praktisk utførelse av en handling (Filstad, 2016, s. 115). Dette oppnår en til en viss grad gjennom benyttelse av slike kurs, men en vil kunne tilrettelegge for større gevinst for de ansattes bevissthet gjennom å benytte aktiv deltakelse og praktisk utførelse i større grad.

Bruk av slik aktiv deltakelse og praktisk utførelse benyttes i kommunen gjennom årlige tester og øvelser. Den siste testen som ble gjennomført var en penetrasjonstest som ble bestilt gjennom en ekstern aktør. Her ble det sendt ut falske phishing-mail som tilrettela for at de ansatte fikk prøve seg i en reell situasjon, i kontekst av deres arbeidshverdag. På denne måten får de testet de ansattes situasjonsforståelse i praksis, og sikre at de er i stand til å oppfatte signaler, forstå signalenes betydning og er i stand til å forutse mulig fremtidig utvikling av situasjonen (Endsley, 2000, s. 3). Gjennom slike praktiske tester får kommunen god oversikt over hvilke aspekter ved de ansattes bevissthet som gjerne er mangelfulle. Disse svakhetene kan så adresseres i større grad i fremtidige kurs og nyhetssaker. Informant A nevnte at de i kommunen var svært opptatt av å lære etter slike tester, og deretter videreutvikle og forbedre opplærings- og treningsopplegget. Slik endring og forbedring viser til kommunens lærende

kultur. Etter testene eller øvelsene innhenter de informasjon, handler basert på denne informasjonen, og viser derfor vilje til å implementere endringer når det identifiseres behov for det (Kongsvik, 2013, s. 116). En god lærende kultur er en sentral indikator på en god helhetlig sikkerhetskultur. Parsons et al. (2015), identifiserte en korrelasjon mellom sikkerhetskultur og bevissthet rundt cybersikkerhet, hvor personer som jobber i en virksomhet med god sikkerhetskultur også viste seg å inneha kunnskap, holdninger og atferd som samsvarte med virksomhetens prosedyrer og retningslinjer. At kommunen viser en god lærende kultur kan derfor sannsynliggjøre at de gjennom bruk av slike tester forbedrer opplærings- og treningsopplegget, og over tid også de ansattes bevissthet rundt cybersikkerhet.

Et annet tiltak kommunen vektlegger er feedback og rapportering av avvik fra de ansatte. En rapporterende kultur er en viktig del av å ha en god sikkerhetskultur i en organisasjon. Dette kan være utfordrende å få til ettersom folk flest sjelden ønsker å innrømme dersom de har gjort feil selv. Dersom de ikke har tro på at ledelsen benytter seg av informasjonen, og handler på bakgrunn av den, kan det også hindre folk i å rapportere avvik eller ting som virker mistenksomt (Reason, 1997, s. 205). Å være oppmerksom på og oppdage avvik krever også bevissthet. For å få folk til å rapportere kritiske hendelser, nesten-ulykker eller ting de oppfatter som urovekkende er det viktig å skape tillit mellom ledere og ansatte. I kommunen jobber de aktivt med å oppfordre de ansatte til å rapportere avvik, samt å gi feedback om saker de observerer i arbeidshverdagen. Som informant A nevner er det de som jobber ute i avdelingene som står nærmest truslene og farene som kan ramme kommunen. Å lytte til de ansatte er derfor et element som oppleves særdeles viktig for informant A. De sørger også for å skrive nyhetssaker på bakgrunn av den feedbacken og rapporteringen de får fra de ansatte, på denne måten ser de ansatte at tiden de bruker på å rapportere hendelser har betydning for ledelsen. Informant B nevner også at de tidvis har gjennomført belønninger for å oppfordre til rapportering. Dette kan være med på å fjerne frykten for straff ved at de opplever at rapportering anses som et positivt gode for kommunen. Informant B la også vekt på at de ansatte ikke mislykkes dersom de gjør en feilhandling, så lenge det rapporteres inn viser det til bevissthet rundt cybersikkerheten, og det er alltid en suksess når de gir slike tilbakemeldinger. En slik holdning vil bidra til å skape tillit i organisasjonen, det bidrar også til åpenhet mellom de ansatte og ledelsen, og vil derfor kunne styrke den rettferdige kulturen i virksomheten. God rapporterende, rettferdig og lærende kultur tilrettelegger for diskusjon, åpenhet og læring og vil videre legge et godt grunnlag for de ansattes forståelse, holdninger

og kompetanse til å overholde prosedyrer og retningslinjer. De vil videre bli bevisste på potensielle risikoer ved cybertrusler og egnede preventive tiltak for å opprettholde og forbedre cybersikkerheten i kommunen (OECD, 2002).

6.1.4 Hvilke implikasjoner har kommunens kommunikasjon av cybersikkerhet for de ansattes bevissthet?

Hvordan en kommuniserer cybersikkerhet og cybertrusler kan påvirke de ansattes bevissthet rundt disse tingene. Informantene (A, B) nevner at de ønsker at de ansatte skal føle seg trygge på jobb, både i sin rolle og på sitt ansvar for cybersikkerheten. De fokuserer derfor på å vektlegge at IT-avdelingen er der som en støtte for de ansatte, ikke for å ta dem dersom de utfører feilhandlinger. På denne måten opplever de at det senker terskelen for at de ansatte tar kontakt om det er noe de er usikre på. Frykt, usikkerhet og tvil kan drepe de ansattes engasjement når det gjelder å ivareta og utvikle sin kompetanse innenfor cybersikkerhet. Som Billett (2004) nevner er det to forhold som påvirker læring på arbeidsplassen. Både hvordan organisasjonen tilrettelegger for de ansattes læring, og hvorvidt de ansatte benytter seg av disse læringsmulighetene. Det er to forhold som er gjensidig avhengige for å sikre kontinuerlig læring (Billett, 2004, s. 109). Kommunens fokus på trygghet kan øke de ansattes engasjement og motivasjon for cybersikkerhetsarbeidet, og sørge for at de benytter seg av læringsmulighetene de blir tilbudt. Denne tryggheten vil også kunne tilrettelegge for to-veis kommunikasjon ved at de ansatte tør å henvende seg til IT-avdelingen dersom de lurer på noe i forhold til cybersikkerhetsarbeidet. Slike henvendelser krever tillit. Dersom en frykter straff for å innrømme feilhandlinger eller avvik vil en unngå å oppgi dette til ledelsen.

Informant A var også bevisst på sin kommunikasjon i form av at kursene ikke skulle føles som noe som ble pålagt dem av ledelsen. De benytter heller kursene som *«noe vi har sammen»,* slik at de ansatte får mer eierskap over sin egen opplæring og trening. Som informant A nevner er det også viktig å kjenne sitt publikum, både i forhold til hvordan informasjon kommuniseres, samt hvor den kommuniseres. De ansattes motivasjon til å trene på bevissthet avhenger av personlige interesser, verdier og eksisterende bevissthet for cybertrusler. For de som arbeider med å kommunisere budskap ut til sine ansatte er det derfor viktig å ha oversikt over disse egenskapene for å kunne tilpasse kommunikasjonsstrategiene til den enkelte ansattes evner og motivasjon (Njå et al., 2020, s. 94). Informant A var veldig bevisst på dette, og oppga at de av den grunn benyttet åpne kommentarfelt på alle nyhetssaker

som legges ut på intranettet. Det tilrettelegger for at de ansatte på en rask og enkel måte kan gi beskjed dersom det er noe de ikke forstår i informasjonen som legges ut. Informantene nevner også at de i kommunen er veldig bevisst på språkbruken de benytter i nyhetssaker som gjelder alle ansatte. Samtlige informanter nevnte at når en kommuniserer cybersikkerhet så kan begrepene en bruker fort bli litt for abstrakte for den «vanlige» ansatte. De forsøker derfor i størst mulig grad å benytte språk som er forståelig for alle ansatte. For at informasjonen som kommer frem i nyhetssakene skal være effektiv for mottakeren må den tas ned på et allment nivå (Njå et al., 2020, s. 95). Det anses også som sentralt for læring og økt bevissthet blant de ansatte at informasjonen i nyhetssakene konkretiseres og gjøres så relevant som mulig, slik at de ansatte forstår at *«dette er noe som angår meg».*

Ved å benytte et inkluderende språkbruk motiverer det de ansatte til å arbeide forsvarlig og sette seg inn i regler og retningslinjer. Informant B nevner også at de forsøker å gi cybersikkerhet et mer positivt fokus, istedenfor å fortelle hvor farlig det er, tilnærmer de seg de ansatte ved å legge vekt på hvordan de kan bidra. Informant D forteller at ved å benytte språk som de ansatte forstår sikrer de at de ansatte har tilstrekkelig kunnskap og kompetanse for hvordan de skal handle i ulike situasjoner. Hvis en kun legger vekt på alt en ikke skal gjøre kan en risikere at de ansatte ikke har kunnskapen og ferdighetene til å faktisk handle riktig i ulike situasjoner. Å benytte inkluderende språkbruk og gi cybersikkerhet et positivt fokus kan bidra blant annet til den rapporterende kulturen ved at de ansatte får mer eierskap til sitt ansvar. Ved at det fokuseres på at cybersikkerhet og kursene er noe «vi har sammen» istedenfor pekefinger-tilnærming kan det bidra til at folk lettere rapporterer avvik eller nesten-hendelser. Dette fordi det bygges større tillit mellom de ansatte og ledelsen, og de blir mer bevisste på hvordan de selv bidrar til god cybersikkerhet i kommunen.

Flere informanter (A, C, D, E) mente også at åpen kommunikasjon av mulige konsekvenser av brudd på retningslinjer er en viktig faktor for de ansattes bevissthet. Forståelse for potensielt utfall av avvik kan fungere som en motiverende faktor og øke de ansattes engasjement for cybersikkerhet. Dette korrelerer med Daler et al., (2019) sin teori om bevisstgjøring, hvor informasjon om hvorfor sikkerhet er nødvendig for de ansattes motivasjon til å kontinuerlig opprettholde sikkerheten. Nyhetssakene på intranettet benyttes blant annet til å informere om uønskede hendelser i lignende organisasjoner, samt hvilke konsekvenser hendelsene medførte. Kommunen erfarte at slik informasjon kan gjøre de ansatte mer medgjørlige til implementering av nye sikkerhetstiltak. Eksempelet nevnt

tidligere om innføring av tofaktorautentisering illustrerer virkningen av slik kommunikasjon. Slike endringer i de ansattes holdning tyder på en god lærende kultur i kommunen. Læring avhenger av et godt informasjonsgrunnlag, at en har kompetanse til å handle basert på denne informasjonen og at en har vilje til å iverksette endring når det er behov for det (Kongsvik, 2013, s. 116). I denne situasjonen ser vi at ledelsen i kommunen viste god bevissthet ved å beslutte å implementere tofaktorautentisering, når behovet for tiltaket ble informert godt til de ansatte viste også de vilje til å iverksette endring for å styrke cybersikkerheten.

6.1.5 Hvilke utfordringer møter kommunen på i arbeidet med bevisstgjøring rundt cybersikkerhet?

Kommunen møter på ulike utfordringer i opplærings- og treningsopplegget de kjører for å øke de ansattes bevissthet mot cybersikkerhet. Flere informanter nevnte at de ser at de gjerne skulle tilpasset opplærings- og treningsopplegget i større grad enn de gjør i dag. De kjører i dag et opplegg som er forholdsvis overordnet og generalisert. Kommunen opererer med ulike tjenesteområder som står overfor ulike problemstillinger, som krever ulik grad av konfidensialitet og som har ansatte med ulike behov. Som nevnt tidligere har de sett en positiv virkning på de ansattes bevissthet når de går ut med nyhetssaker som er konkrete og relevante for de ansatte. Å sikre en større relevans i kursene for de ulike ansatte, samt å adressere ulike behov i kursene nevnes også som et element som kunne gjort kursene mer effektive. Men grunnet mangel på ressurser er dette ikke mulig å gjennomføre i dag.

Selv om kommunen benytter et overordnet opplegg for opplæring gjennom sine kurs nevner informantene at de savner et helhetlig, systematisk og koordinert arbeid med cybersikkerhet i kommunen. Det jobbes i dag forholdsvis fragmentert med cybersikkerhet, og de opplever en mangel på koordinering mellom de ulike tjenesteområdene. Dette er samtidig utfordrende å gjennomføre ettersom kommunen leverer flere ulike tjenester som krever ulik tilnærming og avveining mellom blant annet produksjon og sikkerhet. Eksempelvis jobber noen tjenesteområder, som helse og velferd, med større grad av personvernverdig informasjon enn andre. Kommunen som helhet ønsker å dele data og operere med åpne datakilder som kan komme innbyggerne og næringslivet til gode, men avveiningen mellom konfidensialitet, integritet og tilgjengelighet blir her viktig.

Informant B nevner også at når en har fravær av uønskede hendelser kan det oppstå en tanke om at «*dette har vi kontroll på*». Fokuset og prioriteringen av sikkerhet, her cybersikkerhet,

kan da avta litt og det settes ikke av ressurser til for eksempel koordinering av cybersikkerhetsarbeidet eller tilpasning av opplærings- og treningsopplegg. Dette korrelerer med Reasons teori om «un-rocked boat». Jo lenger tid det går fra en uønsket hendelse eller en nesten hendelse, jo mer eroderer sikkerheten. Det krever ofte en uønsket hendelse for at sikkerheten skal prioriteres. Dette skyldes ofte at jo mer ressurser en bruker på sikkerhet, jo mindre har en tilgjengelig for produksjonen (Reason, 1997, s. 4). Det må likevel være en god balanse mellom fordelingen av ressurser til sikkerhet og produksjon, fullt fokus på den ene eller den andre er ikke bærekraftig for en organisasjon. Basert på Reasons teori om «un-rocked boat» kan der derfor tenkes at det ikke prioriteres ressurser til tiltakene som skal til for å håndtere disse utfordringene ettersom de ikke har opplevd noen uønskede hendelser i kommunen som illustrerer et klart behov for deres implementering. Det oppstår heller en tankegang om at sikkerheten er god nok som den er, og ressursene prioriteres til å sikre større avkastning fra produksjonen (Reason, 1997, 4).

6.2 Hvilke implikasjoner har kommunens tilretteleggelse av aktiv deltakelse for de ansattes bevissthet rundt cybersikkerhet?

I delkapitlene under vil jeg diskutere kommunens bruk av diskusjonsbasert opplæring og praktisk utførelse, og dets implikasjoner for de ansattes bevissthet i lys av oppgavens teoretiske rammeverk.

6.2.1 Hvordan påvirker diskusjonsbasert opplæring de ansatte bevissthet?

Gjennom intervjuene kom det frem at kommunen benytter et begrenset antall tiltak for aktiv deltakelse i opplærings- og treningsopplegget i kommunen. En form for aktiv deltakelse informantene oppgir å benytte seg av er diskusjon. Kommunen består av et stort antall mennesker med ulik bakgrunn, erfaring og forståelse for cybersikkerhet, og tiltaket ble implementert grunnet et ønske om økt interaksjon mellom alle ansatte på tvers av tjenesteområder. For å sørge for at alle de ansatte mottar informasjonen i nyhetssaker, og forstår hvordan den påvirker dem i sin arbeidshverdag forteller informant A at de alltid har åpent kommentarfelt under nyhetssakene. Kommentarfeltet tilrettelegger for diskusjon blant de ansatte, hvor ansatte på tvers av ulike tjenesteområder kan interagere med hverandre. Den positive effekten av en slik plattform har blitt synliggjort ved flere tilfeller av implementering av nye sikkerhetstiltak i kommunen. I følge Filstad (2016) er kommunikasjon en av de viktigste og mest virkningsfulle formene for læring i praksis. Kommentarfeltene under

nyhetssakene tilrettelegger for kommunikasjon og diskusjon mellom ulike ansatte fra ulike tjenesteområder, hvor de kan lære av hverandre og hverandres erfaringer. Eksempelet nevnt i 6.1.1 om innføring av tofaktorautentisering viser hvordan denne kommunikasjonen mellom de ansatte fremmet kunnskap, holdninger og bevissthet, som videre førte til økt aksept og forståelse for tiltaket som skulle implementeres (Daler et al., 2019, s. 214). På denne måten kan de ansatte interagere med hverandre og dra læring av hverandre gjennom deling av kunnskap som fostrer økt forståelse og bevissthet. Informant D som jobber med utarbeiding av nytt informasjonssikkerhetsstyringssystem trekker også frem at slik diskusjon er virkningsfullt for de ansattes bevissthet ettersom det gir en variasjon fra de typiske e-læringskursene, samt at en blir aktivisert på en annen måte. Det tilrettelegger for en ny type samspill og dynamikk mellom de ansatte som en ikke får gjennom kurs. Diskusjonsøvelser er derfor noe de jobber med å implementere i større grad i det nye informasjonssikkerhetsstyringssystemet.

6.2.2 Hvilke implikasjoner har praktisk utførelse for de ansattes bevissthet?

Da informantene ble spurt om de hadde noen form for praktisk utførelse i opplærings- og treningsopplegget de kjørte ble det nevnt to ulike elementer. Det første var at de benytter seg av kurs som er mest mulig interaktive. Kursene inkluderer spørsmål som må besvares og vurderinger som må gjøres, i tillegg til at en fysisk må klikke seg videre til neste side slik at det krever noe fra den ansatte som gjennomfører det. Informantene mente at praktisk utførelse var en viktig del av opplæringen, og at de gjerne skulle benyttet seg av en slik tilnærming i større grad. Men grunnet mangel på tid og ressurser lar ikke dette seg gjennomføre. Det ble også nevnt at kommunen som helhet bestiller en ekstern aktør til å gjennomføre en øvelse eller test hvert år. Siste test som ble gjennomført var en penetreringstest hvor det ble sendt ut en falsk phishing-mail til alle ansatte. Det blir da klart hvor god kompetanse og bevissthet de ansatte har knyttet til potensielle cybertrusler. Slike interaktive kurs og tester som krever aktiv deltakelse og praktisk utførelse tilrettelegger for utvikling av kompetanse og økt bevissthet for de ansatte. Ved å få mulighet til å teste kunnskapen de ansatte har tilegnet seg i praksis får de også mulighet til å utvikle og forbedre sin situasjonsbevissthet. Tester som den kommunen utførte i 2020 i form av en falsk phishing-mail tilrettelegger for at de ansatte får øvd seg på å oppfatte signaler, forstå signalenes betydning, forutse mulige utfall av situasjonen og beslutte hvordan de skal handle (Endsley, 2000, s. 3).

Gjennom denne spesifikke penetrasjonstesten fikk de ansatte øvet og videreutviklet sine evner i form av å gjenkjenne elementer i en mail som tilsier at den er upålitelig. Evnen til å gjennomføre dette i praksis forutsetter kunnskap. Kursene informantene oppgir å benytte er en av elementene som setter de ansatte i stand til å oppfatte signaler på eksempelvis en phishing-mail. Etter at de ansatte har innhentet informasjon om situasjonen, må denne informasjonen kombineres og tolkes, på den måten gir en mening til de signalene en har oppfattet. Til slutt vil en vurdere fremtidig utvikling av situasjonen, og beslutte hvordan en skal håndtere situasjonen på en måte som overholder virksomhetens prosedyrer og retningslinjer (Endsley, 2000, s. 3). Etter at denne penetreringstesten ble gjennomført i kommunen erfarte de at de ansatte håndterte situasjonen riktig og rapporterte avviket til ledelsen. Dette viser til at de ansatte har god situasjonsbevissthet og at de, når det kommer til phishing-mail, har oppnådd den dypeste formen for forståelse og bevissthet.

Praktisk utførelse og aktiv deltakelse tilrettelegger for at kunnskap videreutvikles til kompetanse. Ved at de ansatte får anvende den kunnskapen de har tilegnet seg gjennom tester og øvelser vil de også utvikle ferdighetene til utføre denne kunnskapen i praksis om de møter på en faktisk cybertrussel de må håndtere (Olsen, 2016, s. 241). Selv om slike kurs og tester er effektive for å utvikle de ansattes bevissthet, kan det settes spørsmål ved hvor vedvarende denne bevisstheten er ettersom disse tiltakene gjennomføres sjelden. Kursene de ansatte gjennomfører, blir kun gjennomført én gang i løpet av deres arbeidstid i kommunen. Testene på den andre siden gjennomføres årlig. Ettersom cybersikkerhet er et område som er i konstant endring, kreves det kontinuerlig læring for å opprettholde bevisstheten tilstrekkelig. De ansatte kunne derfor gjerne fått enda større grad av bevissthet ved å gjennomføre disse kursene mer enn én gang i løpet av sin arbeidstid i kommunen.

7 Konklusjon

Formålet med denne oppgaven har vært å studere kommunens opplærings- og treningsopplegg, og hvilke implikasjoner det har for de ansattes bevissthet rundt cybersikkerhet. Dette kapittelet vil besvare oppgavens problemstilling:

Hvordan jobber kommunesektoren med opplæring og trening innenfor cybersikkerhet, hvilke utfordringer hemmer dette arbeidet - og hvilke implikasjoner har det for de ansattes bevissthet rundt cybertrusler?

For å besvare problemstillingen ble det utarbeidet to forskningsspørsmål som gjennom oppgaven er presentert og diskutert. Forskningsspørsmål 1 belyser hvordan kommunen jobber med opplæring og trening innenfor cybersikkerhet, samt hvilke utfordringer som hemmer dette arbeidet. Det fremkommer i drøftingen av FS1 at kommunen benytter seg av skriftlige dokumenter som gir de ansatte kunnskap om hvilke retningslinjer de må forholde seg til og hvordan de skal gjøre dette. Det sendes også ut nyhetssaker som forklarer viktigheten av å opprettholde cybersikkerheten, eksempler på cybertrusler som rammer andre virksomheter, samt hvilke konsekvenser disse uønskede hendelsene medfører. Gjennom informasjon om potensielle cybertrusler og konsekvenser får de ansatte bevissthet rundt viktigheten av cybersikkerhet, og motivasjon til å overholde retningslinjene. Kommunen opplever likevel at den største grunnen til at det forekommer brudd på cybersikkerheten skyldes at de ansatte ikke er klar over at de bryter retningslinjene. Tiltak som kursing, tester og feedback benyttes for å forsøke å øke de ansattes bevissthet i større grad. Slike kurs og tester krever større grad av aktiv deltakelse, og vil derfor også bidra til å utvikle kompetanse ettersom de ansatte her får anvendt kunnskapen de har tilegnet seg i praksis. Testene og kursene tilrettelegger også for en kombinasjon av eksplisitt og taus kunnskap, som er den mest optimale formen for læring. Disse tiltakene vil derfor kunne bidra til å videreutvikle de ansattes bevissthet i enda større grad enn kun den eksplisitte kunnskapen de ansatte får gjennom retningslinjer og nyhetssaker.

Informantene nevnte også noen utfordringer i arbeidet med å øke bevisstheten rundt cybersikkerhet. Ettersom kommunen er en stor virksomhet, består den av mange ulike mennesker med ulik bakgrunn og erfaring. I tillegg leverer de mange tjenester, og de ulike

tjenesteområdene står overfor ulike problemstillinger, og har ulike behov for å opprettholde god cybersikkerhet. I lys av dette kan det settes spørsmål ved hvor virkningsfullt et overordnet, generalisert opplærings- og treningsopplegg er. Et mer spesifikt og tilpasset opplegg er derimot noe informantene oppgir at det ikke er tilstrekkelig med ressurser til å implementere. Å sette av flere ressurser til å styrke cybersikkerheten vil kreve ressurser fra andre områder, som produksjon av tjenester, og vil generere kostnader. Informant B kommenterer dette og mener at en mulig forklaring på årsaken til dette er at de enda ikke har opplevd en alvorlig uønsket hendelse knyttet til cybersikkerhet, og at det da kan oppstå en tanke i ledelsen om at cybersikkerheten er god nok.

Forskningsspørsmål 2 viser at kommunen tilrettelegger for aktiv deltakelse til en viss grad. Når det kommer til opplæring og trening som krever aktiv deltakelse benytter kommunen diskusjon, kurs, og praktiske tester. Det tilrettelegges for diskusjon ved å ha åpne kommentarfelt under nyhetssakene som legges ut, hvor alle ansatte på tvers av tjenesteområder kan komme med bidrag. Gjennom slik diskusjon kan de interagere med hverandre og dra læring av hverandre, og på den måten fremme kunnskap, holdninger og bevissthet. Kursene forsøkes også å gjøres mest mulig interaktive ved å benytte quizer som skal besvares underveis, på denne måten er de ansatte nødt til å anvende kunnskapen de har til å vurdere de ulike spørsmålene. Kommunen bestiller også inn en test eller øvelse fra en ekstern aktør hvert år. På denne måten får de ansatte testet sine evner i praksis, i en simulert reell situasjon. Ved å kjøre slike tester oppdager kommunen hvilke kompetansebehov som eksisterer, samt at de ansatte får øvet sin situasjonsbevissthet. Slik øving vil hjelpe dem å oppfatte viktige signaler som kjennetegner cybertrusler, for så å kombinere og tolke disse signalene. Til slutt vil de da være i stand til å forutse fremtidig utvikling av situasjonen de står overfor og oppnår den dypeste former for bevissthet. Slik diskusjon, kursing og øving vil tilrettelegge for utvikling av kompetanse og økt bevissthet ved at de ansatte får brukt kunnskapen de har tilegnet seg i praksis.

Basert på det ovennevnte konkluderer studien med at tiltakene kommunen benytter for opplæring og trening er virkningsfulle og effektive for de ansattes bevissthet rundt cybersikkerhet. De kunne likevel muligens vært enda mer virkningsfulle, og i større grad opprettholdt de ansattes bevissthet over tid, dersom de gjennomføres mer kontinuerlig, og om de tilpasses til ulike tjenesteområders behov i større grad. Kursene som blir vektlagt i størst grad av samtlige informanter gjennomføres kun én gang i løpet av de ansattes arbeidstid i

kommunen. Ettersom cybersikkerhet er et område med rask teknologisk endring, vil større grad av vedlikehold av bevisstheten være gunstig for kommunens helhetlige cybersikkerhet.

7.1 Forslag til videre forskning

Gjennom studiens løp har det dukket opp flere elementer som hadde vært interessante å belyse ytterligere. Det hadde for det første vært interessant å undersøke oppgavens problemstilling fra de ansattes perspektiv, og deres opplevelse av opplæringen og treningen de gjennomfører. Hvorvidt den oppleves tilstrekkelig, og hvilke elementer de opplever som særlig virkningsfulle for sin bevissthet rundt cybersikkerhet.

En av informantene nevnte også en interessant problemstilling for store virksomheter som kommunen, som problematiserte hvor en skal ansette IT-personell for å sikre koordinert arbeid med cybersikkerhet og bevisstgjøring. Ettersom de er en stor virksomhet med flere ulike tjenesteområder var det utfordrende å vite hvor IT-personellet skulle plasseres for å etablere et systematisk, helhetlig arbeid med cybersikkerhet på tvers av tjenesteområdene.

I forhold til studiens omfang ble utvalget av informanter begrenset til én kommune for å kunne gå i dybden på tematikken jeg ønsket å studere. Det hadde videre vært interessant å se hvorvidt de samme resultatene oppstår dersom en undersøker et større utvalg.

Referanser

Billett, S. (2004). Learning through work – Workplace participatory practices. I H. Rainbird, A. Fuller & A. Munro (Red.), *Workplace Learning in Context* (s. 109-125). London: Routledge

Blaikie, N. & Priest, J. (2019). *Designing social research* (3. utg.). Cambridge: Polity Press

Choi, N., Kim, D., Goo, J. & Whitmore, A. (2008). Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action. *Information Management and Computer Security, 16*(5), 484-501. https://www.emerald.com/insight/content/doi/10.1108/09685220810920558/full/html

Cybersecurity Insiders. (2018). *Insider threaths.* Hentet fra https://crowdresearchpartners.com/wp-content/uploads/2017/07/Insider-Threat-Report-2018.pdf

Daler, T., Gulbrandsen, R., Høie, T. A. & Sjølstad, T. (2019). *Håndbok i datasikkerhet – informasjonsteknologi og risikostyring* (4. utg.). Bergen: Fagbokforlaget

Deloitte. (2018). Ny sikkerhetslov og NIS-direktivet. Hentet fra https://www2.deloitte.com/no/no/pages/legal/articles/sikkerhetslov-januar-2019.html

Dey, I. (2004). Grounded theory. I C. Seale, G. Gobo, J. F. Gubrium & D. Silverman (Red.), *Qualitative Research Practice* (s. 80-93). London: Sage Publications

Endsley, M. R. (2000). Theoretical Underpinnings of Situation Awareness: A Critical Review. I M. R. Endsley & D. J. Garland (Red.), *Situation Awareness Analysis and Measurement* (s. 3-32). New York: CRC Press.

Filstad, C. (2010). *Organisasjonslæring – fra kunnskap til kompetanse*. Bergen: Fagbokforlaget

Filstad, C. (2016). *Organisasjonslæring – fra kunnskap til kompetanse* (2. utg.). Bergen: Fagbokforlaget

Flin, R., O´Connor, P. & Crichton, M. (2008). *Safety at the sharp end*. Farnham: Ashgate Publishing Limited

Forskrift om kommunal beredskapsplikt. (2011). Forskrift om kommunal beredskapsplikt (FOR-2011-08-22-894). Hentet fra https://lovdata.no/dokument/SF/forskrift/2011-08-22-894

Furnell, S. & Clarke, N. (2005). *Organizational Security Culture: Embedding Security Awareness, Education and Training.* Hentet fra http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.678.9294&rep=rep1&type=pdf

Gjøvikregionen. (u.å.). Ny satsing på cybersikkerhet. Hentet 29.01.2020 fra http://www.gjovikregionen.no/blog/aktuelt/ny-satsing-pa-cybersikkerhet/

Grønmo, S. (2016). *Samfunnsvitenskapelige metoder* (2. utg.). Bergen: Fagbokforlaget

Hansen, M. K. (2020, 5. mars). Bevissthet. Hentet fra https://snl.no/bevissthet

Justis- og beredskapsdepartementet. (2016, 16. desember). NIS-direktivet. Hentet fra https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2014/sep/nis-direktivet/id2483374/

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

Kruke, M. (2017). *Beskyttelse av sensitiv informasjon: en studie av norske nettselskapers beskyttelse av sensitiv informasjon* (Masteroppgave). UiT Norge arktiske universitet, Tromsø.

Lai, L. (2013). *Strategisk kompetanseledelse* (3.utg). Bergen: Fagbokforlaget

NHO. (2018, 30. april). Hva er et cyberangrep? Hentet fra https://arbinn.nho.no/Medlemsfordeler/medlemsfordeler-nho/nho-forsikring2/sporsmal-og-svar/hva-er-et-cyberangrep/

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

NorSIS. (2017). *Utredning av kommunal sektors felles behov for et kompetansesenter for håndtering av IKT-hendelser (KommuneCSIRT).* Hentet fra https://norsis.no/wp-content/uploads/2018/05/Utredning-Kommune-CSIRT.pdf

NorSIS. (2020). *Trusler og trender 2019-2020.* Hentet fra https://norsis.no/trusler-og-trender-2019-2020/

NOU 2015:13. (2015). *Digital sårbarhet – sikkert samfunn – beskytte enkeltmennesker og samfunn i en digitalisert verden.* Oslo: Justis- og beredskapsdepartementet.

NSR. (2020). *Mørketallsundersøkelsen 2020*. Hentet fra https://www.nsr-org.no/produkter-og-tjenester/publikasjoner/morketallsundersokelsen

NVE. (2017). *Regulering av IKT-sikkerhet.* (26/ 2017). Hentet fra http://publikasjoner.nve.no/rapport/2017/rapport2017_26.pdf

OECD. (2002). *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.* Hentet fra https://www.oecd.org/sti/ieconomy/15582260.pdf

Olsen, T. H. (2016). Kompetanseutvikling. I A. Mikkelsen & T. Laudal (Red.), *Strategisk HRM 2: HMS, etikk og internasjonale perspektiver* (2. utg., s. 238-276). Oslo: Cappelen Damm

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R. & Jerram, C. (2015). The Influence of Organizational Information Security Culture on Information

Security Decision Making. *Journal of Cognitive Engineering and Decision Making 9*(2), 117-129. https://doi.org/10.1177/1555343415575152

Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Farnham: Ashgate Publishing Limited.

Saus, E.-R. & Johnsen, B. H. (2016). Menneskelig svikt og feilhandlinger. I J. Eid & B. H. Johnsen (Red.), *Operativ psykologi* (2. utg., s. 216-231). Bergen: Fagbokforlaget

Sikkerhetsloven. (2019). Lov om nasjonal sikkerhet (LOV-2018-06-01-24). Hentet fra https://lovdata.no/dokument/NL/lov/2018-06-01-24

Siponen, M. T. (2000). Conceptual foundation for organizational information security awareness. *Information Management and Computer Security, 8*(1), 31-41. https://doi.org/10.1108/09685220010371394

SSB. (2019, 11. Juni). Digitalisering i kommunene. Hentet fra https://www.ssb.no/teknologi-og-innovasjon/artikler-og-publikasjoner/digitalisering-i-kommunene

Thagaard, T. (2013). *Systematisk og innlevelse: En innføring i kvalitativ metode* (4. utg.). Bergen: Fagbokforlaget.

Tougas, C. (2012). *The phenomena of awareness: Husserl, Cantor, Jung.* Oxfordshire: Taylor & Francis group.

Ung.no. (2021, 29. januar). Kommunens oppgaver. Hentet fra https://www.ung.no/demokrati-og-valg/653_Kommunens_oppgaver.html

Weick, K. E. & Sutcliffe, K. M. (2007). *Managing the Unexpected: Resilient Performance in an Age of Uncertainty.* San Francisco: Jossey-Bass.

Vedlegg I: Intervjuguide

Bakgrunn

1. Hva er din stillingstittel?
2. Hvor lenge har du jobbet med cybersikkerhet?
3. Hva er din rolle og ditt ansvar?

Digital sikkerhet

4. Hva forstår du med cybersikkerhet?
5. Hva anser du som de største truslene mot cybersikkerheten i din bedrift?
6. Har dere opplevd uønskede hendelser relatert til cyberangrep?
    a. Hvis ja: hvilke typer angrep?
    b. Hvis ja: hva bidro til at hendelsen inntraff i din oppfattelse?
    c. Hvis nei: hva har bidratt til at dere ikke har blitt utsatt for en uønsket hendelse?
7. Hvordan jobber dere for å kommunisere viktigheten av god digital sikkerhet og motivere de ansatte til å opprettholde dette?
8. Har dere prosedyrer, retningslinjer og instruksjoner som beskriver hva dere forventer av de ansattes oppførsel når det kommer til cybersikkerhet?
9. Ut ifra din erfaring, føler du at cybersikkerhet kan bli for abstrakt og komplisert for de ansatte?

Bevissthet

10. Hva forstår du med bevissthet?
11. Hvilken betydning mener du bevissthet hos de ansatte har når det kommer til den digitale sikkerheten i kommunen?
12. Hvordan foregår opplæring og bevisstgjøring blant de ansatte når det gjelder digitale sikkerhetsutfordringer?
13. Involverer dere de ansatte på noen måte i cybersikkerhetsarbeidet?
14. Hva gjør dere av konkrete tiltak for å skape bevisstheten rundt cybertrusler? (eks. plakater, work-shops, foredrag, e-læring?)
    a. Hvis nei: hva forhindrer disse tiltakene?

15. Har dere noen form for trening som krever aktiv deltakelse fra de ansatte? (eks. simulering av phishing angrep, praktiske oppgaver, diskusjon)
16. Hvilke elementer har dere fokus på i opplæring og trening for å sikre størst mulig utbytte for kompetanseutviklingen?
17. Hva anser du som den største utfordringen med å skape bevissthet rundt digital sikkerhet i virksomheten?
18. Ut ifra din erfaring, hva er det viktigste som bør gjøres for å styrke ansattes bevissthet i forhold til cybertrusler og forsvarlig bruk av IT-systemer?
19. Har du noen tanker om tiltak som ikke er iverksatt, men som kunne styrket riktig bruk av informasjonssystemene?

Avsluttende

20. Er det noe ekstra du vil tilføye?
21. Er det greit at jeg sender oppfølgingsspørsmål på mail om det er nødvendig?

Vedlegg II: Samtykkeskjema

Samtykkeskjema

Formål

I forbindelse med min masteroppgave i Samfunnssikkerhet skal jeg gjennomføre intervjuer i ulike avdelinger i din kommune. Oppgaven omhandler trusselbevissthet i kommunal sektor, og hvordan opplærings- og treningsopplegg påvirker de ansattes bevissthet rundt cybersikkerhet.

Hva innebærer det for deg å delta?

Dersom du velger å stille til intervju vil intervjuet ta for seg ulike spørsmål knyttet til problemstillingen. Det er mulighet for å se gjennom intervjuguiden før intervjuet dersom det er ønskelig. Intervjuet vil vare i ca. 30-45 minutter.

Konfidensialitet etterstrebes, og alle informanter vil anonymiseres ved hjelp av en kode. På denne måten sikrer jeg at opplysningene blir behandlet anonymt. Dersom det er ønskelig vil du også få mulighet til å godkjenne tekst og sitat som brukes i oppgaven før den leveres.

For å kunne gjengi pålitelige data og kvalitetssikre dine uttalelser er det ønskelig å benytte taleopptak under intervjuet. Dette for å unngå distraksjon ved å måtte ta notater, samt for å kunne delta aktivt i samtalen. Opptaket vil da kun lyttes til av meg i etterkant av intervjuet, og slettes så snart det er transkribert.

Det er frivillig å delta

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine opplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke ønsker å delta, eller senere velger å trekke deg.

Ved å signere denne erklæringen godtar du at opplysninger som gis under intervjuet kan benyttes videre i oppgaven.

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *«Bevissthet rundt cybersikkerhet i kommunal sektor»*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☐ å delta i intervju
- ☐ at opplysningene som er oppgitt under intervju kan benyttes videre i oppgaven

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

(Signert av prosjektdeltaker, dato)