Sikkerhet på hybridkontor – den nye normalen?

Prosjektoppgave i SAM500 Infrastruktur og sårbarhet

Våren 2022

Figurliste

Tabelliste

Innholdsfortegnelse

1.0 Hybridkontor – den nye normalen?

Den sosiale nedstengningen under pandemien innebar en lang periode med hjemmekontor i det norske arbeidslivet. Arbeidsgivere ble tvunget til å tenke nytt, og til å endre hverdagen for sine ansatte. Den nye hverdagen innebar blant annet høy grad av digitaliserte løsninger og fleksibilitet. Da samfunnet åpnet opp igjen var det en del private og offentlige bedrifter, og virksomheter som fortsatte å benytte seg av hjemmekontor, i kombinasjon med fysisk oppmøte på arbeidsplassen. Denne type hybrid løsning viser en ny trend i arbeidslivet, og kan beskrives som et skifte i arbeidslivets organisering.

Hybridkontoret gir store muligheter, men kan også føre med seg risikoer og sårbarheter. De teknologiske systemene og den kritiske infrastrukturen som samfunnet er helt avhengig av, blir kontinuerlig overført til det digitale domenet (Engen, Gould, Kruke, Lindøe, Olsen og Olsen, 2021, s. 243). Flere virksomheter og kommuner har de siste årene blitt utsatt for dataangrep i ulikt omfang. Noen av faktorene som har bidratt til denne utviklingen er økende bruk av skytjenester, fjerntilgangsløsninger og hjemmekontor (NSM, 2021, s. 14). En hybrid løsning av hjemmekontor og fysisk oppmøte, har tidligere ikke vært en utbredt arbeidsform. Det vil kunne bety at bedrifter og ansatte ikke nødvendigvis har gode nok erfaringer med å opprettholde forsvarlig IKT-sikkerhet på hjemmekontor. Store mengder dokumenter ligger lagret digitalt, og det gir muligheter for aktører med tilsiktede og ondsinnede hensikter å få tilgang til og å utnytte systemet (NSM, 2021, s. 7). Dataangrepet mot Østre Toten kommune i 2021 er et eksempel som viser hvordan en kommune kan bli satt ut av spill på svært kort tid. Kommunene leverer og vedlikeholder kritisk infrastruktur. Ved et omfattende dataangrep kan kommuner derimot risikere å miste sin evne til å tilby innbyggerne kritiske samfunnsfunksjoner. Samfunnet er i dag bygget på digitaliserte systemer, og nye løsninger i arbeidslivet er viktig for velferds- og samfunnsutviklingen. Digitaliserte systemer vil alltid være tilknyttet sårbarheter, samtidig som den raske utviklingen kan føre til et utvidet og mer komplekst sårbarhetsbilde (Engen m.fl., 2021). Dermed er det viktig å problematisere og stille spørsmålstegn ved potensielle konsekvenser hybridkontor har på IKT-systemet i kommuner.

1.1 Formål og problemstilling

Formålet i denne oppgaven er å sammenligne to kommuner for å undersøke hvilke konsekvenser hybridkontor har for risiko og sårbarhet i IKT-systemet, og hvordan dette håndteres. Problemstillingen vil sette søkelys på organisatoriske løsninger i kommunene.

Undersøkelser rundt dette temaet vil videre være samfunnsmessig relevant for å forebygge og forhindre forekomsten av ytterligere risikoer og sårbarheter i IKT-systemet på hybridkontor. Basert på formålet med oppgaven er følgende problemstilling utarbeidet:

Hvilke konsekvenser har hybridkontor for risiko og sårbarhet i IKT-systemer i kommunene, og hvordan jobber de for å håndtere dette?

For å besvare problemstillingen er det formulert følgende forskningsspørsmål:

FS1: *Hvilke tekniske utfordringer opplever kommunene knyttet til risiko og sårbarhet i IKT-systemer på hybridkontor, og hvordan blir dette ivaretatt gjennom sikkerhetsmessige tiltak?*

FS2: *Hvordan definerer kommunene god digital sikkerhetskultur, og hvordan sikrer de at de ansatte opprettholder god digital sikkerhetskultur på hybridkontor?*

2.0 Teori

I dette kapittelet vil de teoretiske perspektivene oppgaven bygger på bli redegjort for. Perspektivene legger grunnlaget for analysen som gjennomføres ved hjelp av innhentet datamateriale fra to kommuner. Kapittelet vil redegjøre for teori knyttet til IKT-sikkerhet som kritisk infrastruktur, modell for sikkerhetsstyring, risiko- og sårbarhetsdimensjoner i digitale systemer, og digital sikkerhetskultur.

2.1 IKT-sikkerhet som kritisk infrastruktur

IKT-sikkerhet som kritisk infrastruktur er oppgavens basisteori, og legger grunnlaget for resten av teorikapitlet. Kritisk infrastruktur defineres av myndighetene som «de anlegg og systemer som er nødvendige for å opprettholde samfunnets kritiske funksjoner, som igjen dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse» (Njå et al., 2020, s.140). Direktoratet for samfunnssikkerhet og beredskap (DSB) har utviklet en skisse som viser hvordan man vurderer hva som er kritiske samfunnsfunksjoner og kritisk infrastruktur.

Figur 1: Vurdering av kritisk infrastruktur og kritiske samfunnsfunksjoner (Njå m.fl., 2020, s.141).

Samfunnsviktige funksjoner er kategorisert i styringsevne og suverenitet, befolkningens sikkerhet og samfunnets funksjonalitet (DSB, 2016; Njå m.fl., 2020). Befolkningens sikkerhet er «funksjoner som har en direkte betydning for samfunnets evne til å ivareta befolkningens grunnleggende sikkerhet» (Njå m.fl., 2020, s. 143), og IKT-sikkerhet i sivil sektor er underlagt denne kategorien. IKT-sikkerhet i sivil sektor «omfatter sikkerhet for samfunnskritisk informasjon lagret i sivile databaser, samt for systemer, funksjoner og tjenester som databaser og registre er avhengig av i forbindelse med oppdatering av og/eller tilgjengeliggjøring av informasjonen» (DSB, 2016, s. 63).

For å ivareta IKT-sikkerheten, så må man ivareta delfunksjonene *sikring av registre, arkiver mv., personvern og hendelseshåndtering* i IKT-systemer. Beskrivelse av delsystemene vises i tabell 1.

Tabell 1: Oversikt over den kritiske samfunnsfunksjonen IKT-sikkerhet (DSB, 2016, ss. 14-15).

Samfunnskritisk funksjon	**Navn**	**Funksjonsevne**
IKT-sikkerhet i sivil sektor	Sikre registre, arkiver mv.	Evne til å opprettholde tilstrekkelig tilgjengelighet, integritet og konfidensialitet i databaser, systemer, registre og arkiver som er nødvendige for å ivareta kritiske samfunnsfunksjoner og/eller personers og virksomheters rettigheter
	Personvern	Evne til å sikre konfidensialitet og integritet i registre og arkiver som inneholder taushetsbelagte personopplysninger
	Hendelses-håndtering i informasjons- og kommunikasjons-systemer	Evne til å avdekke informasjonssikkerhetshendelser, begrense skade og raskt gjenopprette normal drift i registre og systemer med kritisk samfunnsfunksjon og/eller som inneholder taushetsbelagte personopplysninger

2.1.1 NSM sine grunnprinsipper for IKT-sikkerhet

For å håndtere utfordringene tilknyttet IKT-sikkerhet, har Nasjonal Sikkerhetsmyndighet (NSM) etablert fire grunnprinsipper som fungerer som universelt normgrunnlag og retningslinjer for det forebyggende arbeidet med IKT-sikkerhet. Målet er å kunne kjenne til og håndtere sårbarheter før en angriper utnytter disse i et dataangrep (NVE, 2021, s. 19). Ved å legge prinsippene til grunn vil man ha rutiner og personell for å skape oversikt og administrere sårbarhetene. NSM sine grunnprinsipper vil bli brukt som et vurderingsgrunnlag for hvordan kommunene arbeider med IKT-sikkerhet på hybridkontor, samt for å underbygge kommunene sine tiltak.

1. *Identifisere og kartlegge*

Identifisering og kartlegging er grunnleggende for all sikkerhetsstyring, risikostyring og forvaltning av IKT (NVE, 2021, s. 33). Det handler om å opparbeide og få en forståelse av virksomhetens styringsstrukturer, tjenester, IKT-systemer, brukere og leveranser (NSM, 2020, s. 6). Kartlegging av enheter og programvare er viktig for å få en oversikt og forståelse over IKT-infrastrukturen i virksomheten, men også for å kjenne til sårbarheter i programvarer (NVE, 2021, s. 26). Bevissthet rundt sikkerhetsutfordringer, sårbarheter og vurdering av kompenserende tiltak er sentralt for sikkerhet- og risikostyring i kommunene.

2. *Beskytte og opprettholde*

Beskytte og opprettholde handler om å ivareta en forsvarlig sikring av IKT og opprettholdelsen av den sikre tilstanden både over tid og ved endringer (NVE, 2021, s. 25). Etablering av sikker tilstand innebærer tiltak som vil kunne motstå eller begrense skadene fra dataangrep (NSM, 2020, s. 6). I praksis vil dette bety at virksomheten må konfigurere og tilpasse datamaskiner og programvare slik at ønsket sikkerhet i virksomheten oppnås og tilfredsstiller behovet gitt av arbeidsoppgaver (NVE, 2021, s. 27). Etablering av rutiner for rapportering og innføring av sikkerhetskonfigurasjonen på enheter, programvarer og tjenester er viktig for å hindre at angripere utnytter disse.

3. *Oppdage*

Dette prinsippet innebærer å ha løsninger for å oppdage og fjerne sårbarheter og sikkerhetstruende hendelser. Det kan gjennomføres ved hjelp av analyser og innsamling av sikkerhetsrelevant data, som for eksempel sårbarhetskartlegging og overvåking av IKT-systemet (NSM, 2020, s. 6). Samtidig handler det om å oppdage avvik fra ønsket sikker tilstand

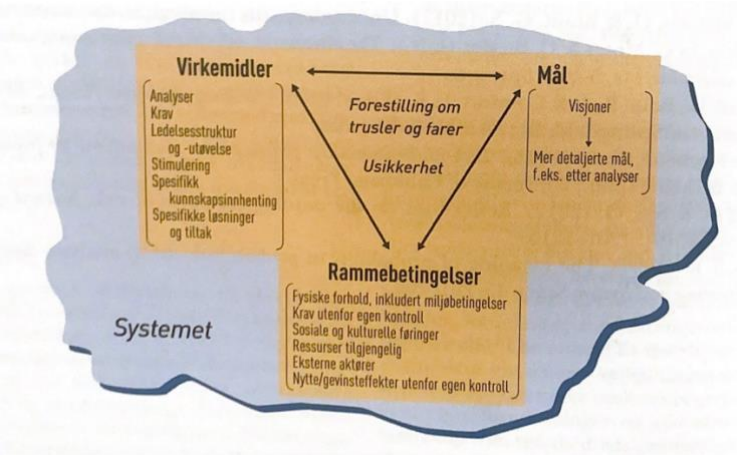
gjennom analyser av sikkerhetsovervåking. Kombinasjonen av manglende tilstrekkelig sikkerhetsovervåking og mangelfulle sikkerhetsanalyser, gjør det enkelt for angripere å skjule handlinger og aktiviteter i virksomhetens informasjonssystemer (NVE, 2021, s. 28).

4. *Håndtere og gjenopprette*

Det siste prinsippet handler om å håndtere de sikkerhetstruende hendelsene effektivt, rette feil og gjenopprette funksjonaliteten til systemene (NVE, 2021, s. 25). Virksomheten bør innføre aktiviteter for å håndtere hendelser som en prosess, som inkluderer forberedelse, vurdering, kontrollering og håndtering av hendelser, gjenoppretting av normaltilstand, og deretter forbedring av sikkerheten basert på erfaringer fra håndteringen (NSM, 2020, s. 7). En rolle- og ansvarsoversikt koplet til virksomhetens beredskapsplan er hensiktsmessig, og en god plan for håndtering av dataangrep er forutsatt at flere av grunnprinsippene ligger til grunn.

2.2 Modell for sikkerhetsstyring

Njå m.fl. (2020) presenterer en modell for sikkerhetsstyring av samfunnet. Sikkerhetsstyring kan defineres som «alle tiltak som iverksettes for å oppnå, opprettholde og videreutvikle et sikkerhetsnivå i overensstemmelse med definerte mål» (Njå m.fl., 2020, s. 65). Denne modellen er delt inn i tre elementer; mål, virkemidler og rammebetingelser. Elementene henger nøye sammen og påvirker hverandre. Mål (visjoner) handler om hva organisasjonen eller virksomheten ønsker å oppnå, og kommuner er avhengig av å ha visjoner med arbeidet sitt. Virkemidler (tiltak) brukes for å komme frem til målet, og det må skje innenfor visse rammebetingelser. Det finnes mange forskjellige virkemidler, og de blir vanligvis gruppert innenfor krav, ledelsesstrukturer og -utøvelse, stimuleringer, spesifikk kunnskapsinnhenting, og spesifikke løsninger og tiltak. Rammebetingelser kan for eksempel være sosiale eller kulturelle føringer, tilgjengelige ressurser eller eksterne aktører (Njå m.fl., 2020). For norske kommuner er lover og forskrifter en del av rammebetingelsene, og de mest relevante for IKT-sikkerhet er forskrift om informasjonssikkerhet, sikerhetsloven, og personopplysningsloven.



Figur 2: Modell for sikkerhetsstyring (Njå m.fl., 2020, s. 64).

Modell for sikkerhetsstyring er spesielt relevant for denne oppgaven fordi kommuner er avhengig av å styre IKT-sikkerheten på hybridkontor til å være på et tolererbart nivå. Ettersom hybridkontor har blitt en permanent løsning for mange kommuner, er dette noe som må settes søkelys på. Det er ulike virkemidler som kan være aktuelle for å oppnå sikkerhetsmål, og generelt har kommuner ulike sikkerhetsmål fordi de har ulike forutsetninger og betingelser. Det gjelder med tanke på blant annet befolkningsstørrelse, ulikt areal, og ulikt antall ansatte som benytter hybridkontor. I denne oppgaven blir to kommuner sammenlignet, og de har relativt sett de samme forutsetningene og rammebetingelsene. Ved å ta utgangspunkt i at de har liknende mål for IKT-sikkerhet på hybridkontor, er det spesielt interessant å vurdere forskjeller i hvilke virkemidler som benyttes i arbeidet.

2.3 Risiko – og sårbarhetsdimensjoner i digitale systemer

Systemer med høy risiko for uhell og ulykker defineres av Charles Perrow (1999, s. 4) som systemer med tette koplinger og høy kompleksitet. Perrow argumenterer for at desto tettere koplinger og høyere grad av kompleksitet, jo større vil risikoen være for systemulykker (Engen m.fl., 2021, s. 162). Et eksempel på et slikt komplekst system er kommunenes IKT-system. Nye hybride kontorløsninger kan bidra til å øke kompleksiteten, og det kan videre gi økt sårbarhet og potensielle konsekvenser for det som har verdi for oss mennesker. For eksempel sensitiv informasjon som kommer på avveie.

I dagens samfunn er komplekse systemer beskrevet som allestedsnærværende (Perrow, 1999; Renn, Lucas, Haas & Jaeger, 2019). De kombinerer både menneskelige og digitale komponenter, og blir også omtalt som systemiske risikoer (Wolf & Serpanos, 2018, s. 17). Det

forventes at disse systemene dekker både *safety*- og *security*-aspekter (Wolf & Serpanos, 2018, s. 17), men det har vist seg å være svært krevende. I denne oppgaven vil de engelske begrepene *safety* og *security* brukes for å beskrive ulike aspekter ved det norske begrepet *sikkerhet.* Begrepene brukes ofte om hverandre i akademia, ettersom de har flere likheter og felles bruksområder (Jore, 2019, s. 160). Likevel har de to begrepene noen forskjeller som gjør det nødvendig å separere dem.

Safety viser til risikoen og usikkerheten knyttet til ikke-planlagte handlinger og hendelser som uhell, ulykker, naturkatastrofer osv. (Engen m.fl., 2021, s. 101). I denne oppgaven vil sikkerhet knyttet til safety-begrepet sette søkelys på interne uhell og uintensjonell svikt i de digitale systemene til kommunene. Jore (2019) definerer *security* som «den faktiske eller oppfattede evnen til å forberede seg for, tilpasse seg, stå imot og komme seg etter farer og kriser skapt av menneskers tilsiktede og ondsinnede handlinger, som for eksempel sabotasje, organisert kriminalitet eller hacking» (Jore, 2019, s. 169). Ifølge Jore (2019) er hovedskillet mellom begrepene safety og security den ondsinnede intensjonaliteten ved en handling. I denne oppgaven vil sikkerhet knyttet til security-begrepet peke på eksterne angrep på IKT-systemet i kommunene.

Som oftest klarer ikke systemer å møte de forventningene som stilles til sikkerhet, men Wolf og Serpanos (2018) skriver at ved å anvende ny teknologi og teknikker kan det gjøre systemene sikrere både innen safety og security (Wolf & Serpanos, 2018, s. 17). På denne måten blir det tydelig at teori knyttet til safety og security gjør seg gjeldende for denne oppgaven. På hybridkontoret kan det oppstå trusler både innenfra (safety) og utenfra (security), og det er dermed nyttig å se sikkerhetsaspektet i IKT-systemet fra de to forskjellige perspektiver.

2.4 Digital sikkerhetskultur

Alle organisasjoner og virksomheter har en organisasjonskultur. På mange måter er organisasjonskulturen essensen av selve organisasjonen, og en overordnet beskrivelse av hvordan organisasjonen fungerer i praksis med tanke på verdier som ligger til grunn for arbeidet. Underlagt den overordnede organisasjonskulturen finnes begrepet sikkerhetskultur. Alle virksomheter har en form for sikkerhetskultur, men den kan være av ulik grad avhengig av organisasjonstype. Reason (1997) peker også på sikkerhetskultur som noe underlagt den generelle organisasjonskulturen, men som et sosialt fenomen som oppstår og utvikles under

læring og erfaring, informasjonsdeling og utvikling av normer, og verdier innad i organisasjonen.

I vår tid ser vi at økt grad av digitalisering i arbeidslivet krever økt oppmerksomhet på sikkerhetskultur i virksomheter og organisasjoner. Som en videreføring av sikkerhetskulturen, har det med årene blitt naturlig å skille mellom generell sikkerhetskultur og digital sikkerhetskultur (cybersikkerhetskultur). Det finnes flere ulike definisjoner på hva cyber-sikkerhetskultur innebærer. Heretter omtales det som digital sikkerhetskultur. NorSIS har derimot i sin rapport The Norwegian Cyber Security Culture (2016) laget en felles samlebetegnelse for de viktigste nøkkelpunktene:

> *(...) digital sikkerhetskultur omfatter all sikkerhet som handler om beskyttelse av eiendeler fra de ulike truslene som utgjøres av visse iboende sårbarheter, og cybersikkerhet handler følgelig om å beskytte informasjonsmidlene. Cybersikkerhetskultur er altså holdningene, antakelsene, troene, verdiene og kunnskapen som folk bruker i sin interaksjon med informasjonsmidlene. Dermed består cybersikkerhetskultur av atferd og et sett med ideer og holdninger* (Malmedal & Røislien, 2016, s. 28).

Å ha en felles sikkerhetsforståelse vil kunne skape en mer enstemmig kultur hvor disse verdiene legger grunnlag for effektiv og sikker planlegging, utførelse og analyser av arbeidet. Faktorene er med på å definere om det eksisterer en «god» eller «dårlig» sikkerhetskultur.

Ifølge Reason (1997, s. 195) finnes det noen grunnleggende forutsetninger for at sikkerhetskulturen i en virksomhet skal være «god». Her trekkes begrepet *informerende kultur* frem som en viktig faktor. I korte trekk handler informerende kultur om fire komponenter som må være til stede for å oppnå en nyttig informerende kultur: rapporterende kultur, rettferdighetskultur, fleksibel kultur, og lærende kultur. Rapporterende kultur innebærer å skape tillitsbånd og trygge rammer for at uheldige eller kritikkverdige forhold kan rapporteres til øvre hold, samtidig som det skal være enkelt og forståelig. Tillit er i denne sammenheng et viktig aspekt, og skal være gjensidig fordelaktig for partene. Rettferdighetskultur handler om rettferdighet i virksomheten, og kan oppleves subjektivt. Likevel er det et viktig grunnelement for å skape trygge rammer, samt en forståelse av hvordan saker håndteres innad i organisasjonen. Reason (1997) peker særlig på at bevisst utførte eller usikre handlinger krever oppfølging og korrigering, mens det å gi straff for ubevisste og uvitende handlinger verken er nyttig for opprettholdelse av kulturen eller særlig hensiktsmessig. Det å ha en konsekvent

holdning og rutiner rundt dette vil støtte opp under følelsen av at det finnes en rettferdighetskultur blant organisasjonens ansatte.

Fleksibel kultur handler om en virksomhets evne og villighet til å omstille seg i en uvanlig situasjon som krever en annen form for håndtering forskjellig fra det daglige arbeidet. Dette er situasjoner som innebærer stor risiko, ulykker, angrep, eller hvor det er viktig å kunne gjøre tilpasninger raskt og arbeide ut fra gitt scenario. Det krever samarbeid, kommunikasjon og læring på tvers av hierarkisk fordeling. Fleksibel kultur er gjerne sett i sammenheng med high reliability organizations (HRO), hvor komplekse og tett koplete systemer til tross for høy grad av kompleksitet, i liten grad opplever store ulykker eller hendelser med store organisatoriske konsekvenser (Engen m.fl., 2021). Det fjerde og siste komponenten er lærende kultur. Lærende kultur er hovedsakelig evnen til å trekke ut lærdom fra hendelser, implementere disse i fremtidig sikkerhetsarbeid, og å benytte kunnskapen til å etablere målrettet opplæring og utbedring av atferd i organisasjonen.

De nevnte komponentene kan overføres direkte til digital sikkerhetskultur, hvor det er viktig med både rapportering, oppfølging, tillit, fleksibilitet og ikke minst læring. I forbindelse med hybridkontor er det å opprettholde en felles risiko- og sikkerhetsforståelse, på tross av individuelle forståelser og holdninger til sikkerhet, særdeles viktig. Ved å ta i bruk digital sikkerhetskultur som teori vil det være mulig å belyse og diskutere funnene i oppgaven knyttet til det menneskelige aspektet ved hybridkontor.

3.0 Metode

Oppgaven er blitt gjennomført som en kvalitativ undersøkelse. Primærkilden er semistrukturerte intervjuer gjennomført med to forskjellige kommuner. Det er gjennomført en komparativ studie som sammenligner konsekvenser hybridkontor har for risiko og sårbarheter i IKT-systemet i to kommuner. I tillegg vil oppgaven se på hvordan kommunene jobber for å håndtere konsekvensene.

3.1 Utvalg og rekruttering

For å komme i kontakt med informanter benyttet vi et tilgjengelighetsutvalg. Det blir beskrevet som et strategisk utvalg av tilgjengelige deltakere som representerer egenskaper som er

relevant for oppgaven (Thagaard, 2018). Denne oppgaven baseres på kommuner fordi de har ansvar for å ivareta og drifte kritisk infrastruktur og kritiske samfunnsfunksjoner. I kommune 1 ble informantene valgt ut gjennom snøballmetoden (Blaikie & Priest, 2019). Først ble beredskapssjefen kontaktet, som igjen satte oss i kontakt med andre som var mer relevante for å besvare oppgavens problemstilling og forskningsspørsmål. I kommune 2 ble informanten, som ble ansett som mest relevant, kontaktet direkte.

Tabell 22: Beskrivelse av informantutvalget

Kommune	**Stilling**
Kommune 1	Sikkerhetsrådgiver IKT-sikkerhet
Kommune 1	Rådgiver informasjonssikkerhet
Kommune 2	Avdelingsleder for IKT-drift og brukerservice

Tabell 3 viser informasjon om de forskjellige kommune. På bakgrunn av at det i denne oppgaven var ønskelig å sammenligne to kommuner, så ble det vurdert som viktig at det eksisterte noen likheter mellom de utvalgte. I dette tilfelle ble likheten antall innbyggere i kommunene.

Tabell 33: Beskrivelse av kommunene størrelse og innbyggertall

Kommune	**Størrelse**	**Innbyggertall**
Kommune 1	Omtrent 150 km^2	Under 60 000
Kommune 2	Omtrent 450 km^2	Under 60 000

3.2 Reliabilitet og validitet

3.2.1 Reliabilitet

Oppgaven består av to semistrukturerte intervjuer. Ved å basere seg på flere kilder vil det øke studiens relabilitet. Ettersom det i denne oppgaven kun er benyttet intervju, kan dette derimot svekke studiens reliabilitet. Det kan likevel argumenteres for at de utvalgte informantene styrker studiens pålitelighet. Da denne studien omhandler IKT-sikkerhet på hybridkontor hos norske kommuner, ønsket vi kontakt med informanter som jobber med IKT-sikkerhet i kommuner. På bakgrunn av informantenes kunnskap og erfaringer ble det gitt innsikt i hvordan hybridkontor kan ha konsekvenser for risiko og sårbarhet i IKT-systemet spesifikt hos kommunene.

For å besvare oppgavens problemstilling ble det ansett som hensiktsmessig å intervjue et fåtall kunnskapsrike og relevante informanter fra hver kommune. Det har gitt god innsikt i hvordan de to kommunene opererer, men samtidig kan det også argumenters for å begrense eller utelukke andre perspektiver på IKT-sikkerhet på hybridkontor. Kommunene virket å ha relativt lik forståelse knyttet til risiko og sårbarheter IKT-systemet, og det styrker oppgavens reliabilitet.

Intervjuerne hadde ingen tilknytning til kommunene som ble intervjuet, og hadde derfor ikke forutinntatte vurderinger om kommunene eller informantene. Videre har prosessen med å innhente data blitt redegjort for, i tillegg til hvordan informantene har blitt rekruttert. Det gir andre et grunnlag for å vurdere kvaliteten på dette prosjektet (Thagaard, 2018). Ved å være åpne om styrker og svakheter knyttet til oppgavens datainnsamling, gjennomgått data og datakildene som er brukt, kan det argumenteres for at studien har en viss grad av etterprøvbarhet. Disse poengene kan bidra til å styrke oppgavens relabilitet. Samtidig er det valgt å ekskludere navnet på kommunene på grunn av personvernhensyn, og det gjør det vanskelig å etterprøve studien.

3.2.2 Intern validitet

Kildens evne til å gi riktig informasjon er viktig for å vurdere den interne validiteten (Jacobsen, 2005). Intervjuobjektene besitter kunnskap som gjør de til noen av de fremste i sin kommune på IKT-sikkerhet. Det ble gjort skriftlige notater underveis i intervjuene, og informantene fikk mulighet til å gjennomgå dataene i etterkant før de ble benyttet som analysemateriale. Da fikk informantene mulighet til å endre eller bekrefte vår forståelse av intervjuet, og det er styrkende for den interne validiteten. På en annen side er det kun valgt å benytte intervju som datainnsamlingsmetode. Det har konsekvenser for muligheten til å kontrollere data fra kommunene sine intervjuene, med data fra andre innsamlingsmetoder. Den interne validiteten blir svekket av denne avgjørelsen.

3.2.3 Ekstern validitet

Studien er et resultat av datainnhenting fra tre informanter fra to forskjellige kommuner. Resultatene viser at norske kommuner står ovenfor de samme eksterne truslene, og den menneskelige aktøren vil mest sannsynlig ha de samme utfordringene når det kommer til IKT-sikkerhet. De innhentede dataene viser at tross kommunenes ulike innfallsvinkel, likevel gir visse indikasjoner på et felles grunnlag og likhet i sikkerhetsarbeid i norske kommuner. I hvilken grad resultatene er overførbare er ikke undersøkt nærmere.

4.0 Empiri og diskusjon

I dette kapitlet vil det redegjøres for oppgavens funn fra intervjuene med kommune 1 og 2, og funnene vil bli drøftet i sammenheng med teorikapitlet. Det vil bidra til å besvare oppgavens problemstilling: *Hvilke konsekvenser har hybridkontor for risiko og sårbarhet i IKT-systemer i kommunene, og hvordan jobber de for å håndtere dette?*

4.1 Omfanget av hybridkontor

Både kommune 1 og kommune 2 har utstrakt bruk av hybridkontor. Informanten fra kommune 2 konstaterer at hybridkontor har kommet for å bli. En undersøkelse gjennomført i regi av kommunen i etterkant av pandemien viste et stort ønske blant kommunens ansatte om å fortsatt ha mulighet for hjemmekontor én til to dager i uka. I kommune 1 var løsningen med hybridkontor allerede godt implementert i forkant av pandemien, og statistikk viser i etterkant at ¼ fortsatt benytter hybridkontor. Da pandemien traff kommune 2, beskrev informantene bruk av hjemme- og hybridkontor som en «eksplosjon». Kommunen gikk fra å ha 200-300 brukere av hjemme- og hybridkontor, til totalt sett 2000 brukere.

4.2 FS1: Hovedfunn – kommune 1

Informantene forteller at kommune 1 hadde mye tilrettelagt allerede før koronapandemien inntraff og den økte bruken av hjemmekontor ble en realitet. De hadde blant annet gjennomført personvern- og konsekvensvurderinger (Personopplysningsloven, 2018), og grunnleggende lisenser og utstyr var etablert. Likevel opplevde kommune 1 flere tekniske utfordringer i overgangen til hjemmekontor, og etter hvert hybridkontoret. Informantene forteller at selv om lisenser og utstyr i utgangspunktet var etablert før pandemien, måtte de tekniske systemene oppdateres og tilpasses en større brukergruppe. Et av de tekniske systemene som måtte oppdateres var føringer for hvilke oppgaver som kunne utføres på hjemmekontor, og det ble styrt av den såkalte hjemmekontorløsningen. Det vil si at systemer og tjenester blir styrt ut ifra tjenstlige behov. Oppdatering og tilpasning beskriver informantene som en tidkrevende, men nødvendig jobb.

Det er særlig tre utfordringer som blir nevnt i forbindelse med hjemmekontor; svake passord, hjemmerutere, og svindelforsøk gjennom e-poster. Kommune 1 uttrykker at hjemmerutere er utfordrende å ha kontroll over, og informantene påpeker at det per i dag ikke eksisterer en

velfungerende teknisk løsning på dette problemet. Det eksisterer kun interne bevisstgjørings-kampanjer for ansatte, men det omhandler i større grad organisatoriske tiltak som blir diskutert i neste delkapittel. Hjemmerutere er dermed å anse som en utfordring for styringen av IKT-sikkerhet på hybridkontor. Ved innføring av hybridkontor som en del av normalsituasjonen, var det dermed behov for flere tiltak som måtte iverksettes av kommunen for å løse de sikkerhetsmessige utfordringene.

Informantene vektlegger spesielt to tekniske tiltak; bruk av totrinnsverifisering og utvidelse av passordlengde. I tillegg påpekes barrierer og filtre i kommunenes systemer som sentrale. Svindel gjennom e-post har økt ved bruk av hybridkontor, og personer med ondsinnede hensikter utnytter sårbarhetene i kommune 1 sine systemer. Kommune 1 har barrierer og filtre som allerede stopper flere millioner e-poster i måneden, men avsender bytter domener til enhver tid og dermed stanses ikke samtlige av e-postene. Informantene påpeker at de alltid ligger på etterskudd på dette området, og at det er en stor utfordring at angripere stadig finner nye måter å infiltrere og forsøke å skade IKT-systemet. Samtidig er dette med på å gjøre at kommune 1 alltid må holde seg oppdatert på den digitale utviklingen.

Avslutningsvis forteller informantene om en sikkerhetssituasjon som kontinuerlig er i endring. Tidligere var trusselen i større grad mot teknologi enn mot mennesker, men det har skjedd en endring. Informantene nevner den pågående sikkerhetspolitiske situasjonen i Europa, og viktigheten av å holde seg oppdatert på hva som skjer i systemene til kommunen. Kommune 1 får varsler dersom ansatte får unormal aktivitet på sine PCer, og anser det som et helt nødvendig tiltak for at det ikke skal skje et større dataangrep.

4.3 FS1: Hovedfunn - kommune 2

Kommune 2 opplever også flere tekniske utfordringer tilknyttet risiko og sårbarhet på hybridkontoret, og kommunen viser til ulike løsninger tatt i bruk for å ivareta sikkerheten i systemene. Den største utfordringen for kommune 2 er spesielt knyttet til et økt antall angrep utenfra, og at denne typen angrep blir mer og mer avansert. Her nevnes for eksempel DDOS-angrep (tjenestenektangrep), hvor angriperen sperrer brukere ute av en nettressurs ved å «oversvømme» nettstedet med en enorm mengde trafikk (Netsecurity, u.å.). På denne måten har ikke serveren kapasitet til å håndtere flere forespørsler, og brukere som skal ha tilgang blir hindret fra dette. Det kan videre få konsekvenser for den daglige driften i kommunen.

Informanten poengterer at de er usikre på om kommunen er godt nok rustet mot morgendagens angrep, og sier at dette er noe de aldri sikkert kan vite.

Tekniske tiltak som er iverksatt av kommunen er totrinnsverifisering, lange passord, og bruk av VPN-løsninger. Videre gir kommunen ut egne PCer til de ansatte, som blir brukt både på kontoret og på hjemmekontoret. Dette er viktig, ettersom de ansattes trådløse hjemmenettverk er utsatt for angrep og krever sikring i økende grad. PCene er utstyrt på en måte som gjør at ansatte må koble et adgangskort til PCen for å få tilgang til kommunens digitale infrastruktur. Disse tiltakene hadde kommunen allerede innført før pandemiens utbrudd, og de bidrar i større grad til å beskytte kommunens infrastruktur. Hvis et dataangrep likevel skulle skje, har kommune 2 gått til innkjøp av en IRT-tjeneste (Incident Response Team). Informanten forklarer at dette er en tjeneste som tilbys av et kompetansemiljø, for eksempel et konsulenthus, som kan bistå i en situasjon der et system svikter eller er under digitalt angrep. Informanten sier at kommunen ikke har denne kompetansen selv og kjøper derfor denne tjenesten for å øke beredskapen.

I kommune 2 er det gjennomført ROS-analyser for de tekniske tiltakene kommunen tar i bruk, for eksempel Office 365, VPN osv. Dette er løsninger som benyttes når det gis tilgang til kommunes infrastruktur utenfor kommunens nettverk. Det er imidlertid ikke utført en egen ROS-analyse på konseptet hybridkontor, og hvordan de ansatte forholder seg til eget og eksternt nettverk. Et annet sikkerhetsmessig tiltak som retter seg mer mot de organisatoriske løsningene kommunen har valgt å ta i bruk, er å opprette en stilling dedikert direkte til informasjonssikkerhet. Denne personen påpeker hva IKT-avdelingen burde og ikke burde gjøre i gitte scenarioer. Informanten mener det er nyttig å ha en pådriver som kan se situasjonen fra ulike perspektiver, og at det var positivt for sikkerhetsstyringen at kommuneledelsen så nødvendigheten av en slik stilling.

Informanten uttrykker videre at kommune 2 har iverksatt de tekniske tiltakene og barrierene de kan per i dag. Samtidig legger informanten til at oppmerksomheten mot sikring av de digitale systemene har økt den siste tiden. Det ses spesielt i sammenheng med erfaringer andre kommuner har hatt med dataangrep, og hvilke konsekvenser et angrep kan ha for infrastrukturen i en kommune (ref. angrepet på Østre Toten kommune). I tillegg har den pågående sikkerhetspolitiske situasjonen i Europa påvirkning. Informanten sier at i etterkant av slike erfaringer, ble de forskjellige sikkerhetsløsningene knyttet til hybridkontoret gjennomgått og jobbet ytterligere med. Selv om informanten fortalte en del om tekniske

utfordringer og løsninger, så mener informanten at det menneskelige aspektet utgjør den største utfordringen for sikkerhetsstyringen i dag.

4.4 Forskningsspørsmål 1

4.4.1 Et komplekst IKT-system – nye farer og trusler knyttet til security og safety

Tankegangen til Perrow (1999) kan ses i sammenheng med kommunenes IKT-system som stadig blir mer tettkoblet og komplekse. Feil eller svikt i én del av det digitale systemet vil raskt kunne forplante seg, som igjen kan få store konsekvenser for verdier i samfunnet. Kommunene står stadig overfor nye trusler og farer. IKT-systemene til kommunene drifter kritiske infrastrukturer og samfunnsfunksjoner, noe som betyr at et angrep på systemet vil være en påkjenning på kommunens evne til å opprettholde forsvarlig drift (Njå m.fl., 2020). Kommunene har digitalisert sitt arbeid i takt med den teknologiske utviklingen, og store deler av viktig informasjon og infrastruktur ligger nå lagret på digitale plattformer. Kommunene står således ovenfor utfordringer som er knyttet til security-relaterte trusler (Jore, 2019). I tråd med NSM (2020) sine grunnprinsipper, er det derfor viktig at kommunene evner å *oppdage* trusler og avvik fra ønsket sikker tilstand i IKT-systemet tidlig nok for å avverge kritiske hendelser.

Ifølge NSM (2020) er det viktig at kommunene evner å *beskytte og opprettholde* IKT-systemet i ønsket tilstand. Kommune 1 oppdaterer systemene jevnlig, noe som krever mye tid og ressurser, men som også er helt nødvendig for at de skal klare å beskytte og opprettholde. Hybridkontoret skaper utfordringer for kommune 1 sin evne til å beskytte og opprettholde IKT-sikkerhet ved at hjemmerutere tas i bruk. Det er vanskelig for kommunen å ha kontroll over de private hjemmeruterene, noe som kan øke risikoen og sårbarheten for security-hendelser dersom de ansatte ikke er bevisste på sikkerheten på eget nettverk og egen PC. Det viser at systemet blir enda mer komplekst når kommunens digitale system møter det private systemet. Dette er fordi man står ovenfor to systemer som er gjensidig avhengig av hverandre for at hybridkontoret skal fungere optimalt. Denne sammenslåingen understreker hvordan Perrow (1999) beskriver at risikoen for uønskede hendelser øker dersom systemet blir mer komplekst. Kommunene poengterer også at sikkerhetssituasjonen er i rask og kontinuerlig endring. Tidligere var trusselen i større grad rettet mot det teknologiske systemet, mens i dag ser kommunene at trusselbildet er blitt endret til å ha fokus mot offeret. Dette er safety-relaterte utfordringer, som krever at kommunene har iverksatt virkemidler for å kunne beskytte seg.

Kommune 1 og kommune 2 har ulik tilnærming for å vurdere hvilke virkemidler som anses hensiktsmessig for sikkerhetsstyring på hybridkontor (Njå m.fl., 2020). På den ene siden vektlegger kommune 1 i stor grad det menneskelige aspektet, med bevisstgjøring og økt kunnskap omkring digital sikkerhet hos de ansatte. Bevissthet rundt sikkerhetsutfordringer og sårbarheter er én av flere faktorer som er sentralt for sikkerhetsstyringen i kommunen (NSM, 2020). På den andre siden setter kommune 2 i større grad søkelys på det helhetlige tekniske systemet og utfordringer knyttet til stadig mer avanserte, ondsinnede og intensjonelle dataangrep. Foreløpig har ikke angrepene klart å gjøre store skader på det digitale systemet. Dette trenger ikke nødvendigvis å være spesielt knyttet til nye utfordringer med hybridkontor, men kan generelt være en konsekvens av den digitale utviklingen. På bakgrunn av dette ser man at både det menneskelige aspektet og det tekniske systemet i samhandling er viktig for å håndtere sikkerhetsrelaterte utfordringer.

4.4.2 Et optimistisk syn på det digitale systemet

Begge kommunene er bevisst på at digitale systemer er sårbare, men de har likevel høy tillit til at sine egne digitale systemer tåler påkjenningene de potensielt blir påført ved angrep. Hybridkontor har hovedsakelig begrensninger på bakgrunn av arbeidsoppgaver som krever fysisk tilstedeværelse, som for eksempel helsevesenet, heller enn på bakgrunn av svakheter i systemet. På tross av kommunenes komplekse digitale infrastruktur, gir kommunene uttrykk for å være fremtidsrettet, forberedt og utrustet for eventuelle uforutsette uønskede hendelser. På bakgrunn av dette kan det tolkes som at kommunene har et perspektiv som ligner Wolf og Serpanos (2018) sitt syn på at bruk av ny teknologi og teknikker, som hybridkontor, gjør systemene sikrere. I noe kontrast finnes Perrows perspektiv som uttrykker at hybridkontor som ny teknologi kan gi et større og mer uoversiktlig system som kan ha et stort katastrofe-potensial.

Kommune 2 uttrykker at de har gjort det de kan av sikkerhetstiltak for å styrke den tekniske delen av det digitale systemet. Et slikt optimistisk syn, basert på Wolf og Serpanos (2018) og HRO (Engen m.fl., 2021) sitt perspektiv, forsøker å synliggjøre at ved å innføre gode organisatoriske tilrettelegginger og skape en god sikkerhetskultur, kan hybridkontoret være hensiktsmessig. Å ha et utelukkende optimistisk perspektiv kan samtidig være med på å undergrave kommunenes forståelse av kompleksiteten og usikkerheten i det digitale systemet. Dette understrekes av kommune 1 som sier at til tross for barrierer og filtre for å stanse svindel og angrep, så ser de likevel at avsenderen bytter domener og angrepsmetoder. Dette gjør at ikke

alt fanges opp i kommunens systemer. Å ha gode systemer som kan fange opp og stanse angrep, kan være som et sikkerhetsmål som kommunene har for IKT-systemet (Njå m.fl., 2020). Med den raske teknologiske utviklingen er risikobildet i en kontinuerlig dynamisk prosess, og det er noe kommunene må ta i betraktning til enhver tid. Dette er i tråd med Perrow (1999) sitt mer pessimistiske perspektiv om at det alltid foreligger systemiske risikoer i digitale systemer, som betyr at svikt eller feil i systemet lett kan oppstå og gi alvorlige konsekvenser. For kommunene understreker dette også viktigheten av å finne en balanse mellom disse to ulike perspektivene knyttet til hvordan de ser på det digitale systemet. En sammenligning av kommune 1 og kommune 2 viser at de er samkjørte i hva de anser som de største tekniske utfordringene på hybridkontoret, og hva som kreves for å håndtere disse på best mulig måte.

4.4.3 Økende behov for flere tiltak

Det kommer frem i intervjuene at verken kommune 1 eller kommune 2 har foretatt ROS-analyser direkte tilknyttet hybridkontor. Ettersom hybridkontor kan sees som en viktig bidragsyter til en mer kompleks digital hverdag, vil sikringen av digitale systemer kreve en kontinuerlig og opphøyet grad av beskyttelse. I henhold til NSM (2020) sitt første grunnprinsipp er *identifisering og kartlegging* grunnleggende for sikkerhetsstyringen av IKT-systemet for å få en oversikt og forståelse av systemet. Et steg i riktig retning vil da være å gjennomføre ROS-analyser slik at det kan etableres et system som kan *oppdage* sårbarhetene og risikoene hybridkontoret kan medføre. I forbindelse med hvordan Perrow (1999) omtaler komplekse (digitale) systemer, kan det derimot stilles spørsmålstegn ved om ROS-analyser, totrinnsverifisering og lange passord vil være tilfredsstillende nok hvis den raske digitale utviklingen tas i betraktning.

Basert på utfordringene beskrevet ovenfor, ser kommune 1 og kommune 2 behov for flere tiltak for å styre IKT-sikkerhet på hybridkontor. Selv om kommune 1 og kommune 2 har de samme rammebetingelsene, har kommunene ulik oppfatning om hvilke virkemidler som skal benyttes for å styre IKT-sikkerhet. Kommune 1 tar i bruk noe de kaller *hjemmekontorløsningen*, som består av en del tekniske innretninger som VPN, tilgangsstyring gjennom authenticator-apper og styring av hvilke enheter som er tilknyttet systemet. Det har vist seg aktuelt og nødvendig, ettersom kommune 1 tillater at både private og eksterne PCer kobler seg på kommunens IKT-system. Kommune 2 tillater på sin side ikke dette, men krever at deres ansatte bruker interne PCer som eies av kommunen. Likevel benytter de seg av VPN på hjemmekontor. På denne måten synliggjøres ulike tilnærminger til styring og tilgangskontroll i de to kommunene, og ulike måter å forhindre safety- og security-hendelser på hybridkontor (Jore, 2019; Njå m.fl.,

2020). Kommune 2 påpeker at de i forbindelse med uønskede hendelser har gått til innkjøp av en IRT-tjeneste for å håndtere og gjenopprette IKT-systemer i etterkant av tilsiktede dataangrep. Dette kan kobles til NSM sitt grunnprinsipp for *håndtering og gjenoppretting* (NSM, 2020). Informanten forteller at kommune 2 ikke har kapasitet til å gjenopprette funksjonaliteten til IKT-systemene på egenhånd, og benytter seg dermed av en ekstern aktør for å gjenopprette til normaltilstand. Kommune 1 har på sin side flere ressurser og økt kapasitet direkte rettet mot dataangrep. Kommune 1 har et eget IT-sikkerhets team, hvor flere ansatte i ulike roller har ansvar for IKT-sikkerhet og gjenoppretting av normalsituasjon etter eventuelle hendelser.

4.4.4. Rammebetingelser og virkemidler for å beskytte og opprettholde IKT-sikkerhet

For å ivareta en forsvarlig sikring av det digitale systemet i kommunene, og for å opprettholde en sikker tilstand både over tid og ved ulike endringer, har kommunene valgt noen ulike tiltak. Det stemmer overens med NSM (2020) sitt andre grunnprinsipp om å etablere tiltak som kan *beskytte og opprettholde* IKT-systemet. For å iverksette hensiktsmessige tiltak for IKT-systemet, så må kommunene ta rammebetingelser i betraktning. Generelt er kommuner regulert av flere rammebetingelser, og lover og forskrifter er en del av dette (Njå m.fl., 2020). Flere lover og forskrifter kan kobles mot IKT-sikkerhet i sivil sektor (se DSB, 2016, s. 63). I henhold til sikkerhetsloven skal virksomheten regelmessig gjennomføre vurdering av risiko. Denne vurderingen skal danne et videre grunnlag for iverksetting av tiltak (Sikkerhetsloven, 2018, §4-2). Tiltak for styring av IKT-sikkerhet er for eksempel spesifikke, tekniske tiltak som totrinnsverifisering og innføring av lange passord. Dette er grunnleggende tiltak kommunene har rettet oppmerksomhet mot i lang tid, og som har en god effekt for styring av IKT-systemer (NSM, 2019). Disse tiltakene gjør seg også gjeldende i bruken av hybridkontor.

Det er tydelig at de to kommunene har forskjellige perspektiver på hvordan man skal forholde seg til tiltak. På den ene siden setter kommune 1 søkelys på en mer kontinuerlig prosess for utbedring av de tekniske utfordringene, og påpeker at man alltid vil ligge på etterskudd i arbeidet. På en annen side fremstår det som at kommune 2 har en mer defensiv holdning til teknisk sikring av IKT-systemer. Informanten fra kommune 2 sier at kommunen har gjennomført de tekniske tiltakene som kommunen anser som nødvendige for å *beskytte og opprettholde* deres IKT-systemer på en forsvarlig måte (NSM, 2020), og at de største utfordringene i dag ligger i det menneskelige aspektet. Kommune 2 påpeker at det dermed må settes søkelys på det menneskelige og organisatoriske tiltak i større grad enn på tekniske tiltak. Informanten knytter usikkerhet til om kommune 2 er godt nok rustet mot morgendagens

angrep. Det kan fremstå som paradoksalt, ettersom mer komplekse dataangrep og en mer kompleks arbeidshverdag med hybridkontor, vil kunne kreve kontinuerlig oppdatering og forbedring av barrierer.

Begge kommunene nevner flere av de samme risikoene og sårbarhetene i IKT-systemene tilknyttet bruk av hybridkontor. Med bakgrunn i uttalelsene fra kommune 1 og kommune 2, er det tydelig at det eksisterer ulike synspunkter på om IKT-sikkerheten på hybridkontor skal jobbes med kontinuerlig eller periodevis, basert på eksempelvis sikkerhetssituasjonen i Europa. Ulike sikkerhetsmessige tiltak vektlegges, selv om det overordnede målet hos begge kommunene er å sikre sitt IKT-system slik at de kan fortsette å drifte sin kommune. Sikkerhetsmessige tiltak varierer fra mer komplekse tiltak som å gå til innkjøp av eksterne tjenester som kommune 2 har gjort, til enklere tiltak som å kreve lange passord. Det poengteres likevel fra begge kommunene at det menneskelige aspektet er den viktigste barrieren for å beskytte mot angrep på IKT-systemet på hybridkontoret. Samtidig kommer ikke kommunene unna at det menneskelige aspektet også kan være en sårbarhet for IKT-systemet.

4.5 FS2: Hovedfunn - kommune 1

Kommune 1 mener god digital sikkerhetskultur i stor grad handler om bevisstgjøring og kommunikasjon. Det handler ikke kun om selve innholdet i kommunikasjonen, men også *hvordan* informasjonen kommuniseres til ansatte i kommunen. Bevisstgjøring er også en av de største utfordringene. Informantene sier at hvis de ansatte vet *hva* de skal gjøre, *hvordan* og *hvorfor* de burde gjøre det, blir de ansatte den beste sikkerhetsressursen kommunen har mot indre og ytre trusler. Dette krever derimot klare retningslinjer og tydelig kommunikasjon fra sikkerhetsavdelingen i kommunen.

På bakgrunn av denne tankegangen er det iverksatt flere tiltak i hensikt å sikre at de ansatte opprettholder god digital sikkerhetskultur i kommunen. Dette inkluderer bevisstgjørings-kampanjer knyttet til personvern, informasjonssikkerhet og generell IT-sikkerhet. Det har videre blitt gjennomført flere kampanjer internt med særlig fokus på passord, og da spesielt passordlengde. Det har vist seg å være svært utfordrende å innføre en passord-policy med 8-9000 ansatte, og informantene ser at det fortsatt er rom for forbedring på dette området. Videre er det også behov for forbedring når det gjelder sikring mot svindel-e-post, og de ansattes bevisstgjørelse rundt denne problematikken. Ifølge informantene stopper de flere millioner e-poster bare i løpet av én måned, noe som tilsier at svindel på e-post er svært vanlig. Bare nylig

forteller informanten om to ansatte som responderte på svindel-e-post, og det kun kort tid etter at sikkerhetsavdelingen i kommunen hadde sendt ut informasjon om at man måtte være kritisk og bevisst på svindel gjennom e-post. Andre faktorer som også bidrar til å bygge sikkerhetskultur, er å ha allierte og/eller ambassadører for å nå ut til alle ansatte, samt involvering av ledelsen i kommunen. Kommune 1 poengterer imidlertid at det har vært utfordrende å få ledelsen til å forstå viktigheten av god digital sikkerhetskultur, og at bevisstgjøring av ledelsen kontinuerlig må arbeides med.

Kommune 1 anser digital sikkerhetskultur som en stor utfordring for IKT-sikkerhet på hybridkontor. Da informantene blir spurt om innsatsen som legges ned for å sikre god sikkerhetskultur blant de ansatte, svarer de at veien dit fortsatt er lang. Å forandre allerede iboende holdninger og verdier hos mennesker er vanskelig. Arbeidet med dette er noe man aldri blir ferdig med, fordi det er en kontinuerlig prosess som må opprettholdes og forbedres. Det ble i denne sammenheng poengtert at pandemien og bruk av hybridkontor har vært en kickstart for bevisstgjøringen av digital sikkerhetskultur, og hvordan denne kan opparbeides til å bli bedre.

4.6 FS2: Hovedfunn - kommune 2

Kommune 2 mener det er flere faktorer som er med på å definere en god digital sikkerhetskultur. For det første er det nødvendig med opplæring i de verktøyene man har tilgjengelig. For det andre er gode rutiner og opplæring i atferd på digitale plattformer viktig for IKT-sikkerhet. For det tredje vil aktiv jobbing med å melde avvik og riktig håndtering av informasjonssikkerhetstiltak bidra til å bedre sikkerhetskulturen. Informanten nevner at det har vært dårlig kultur for dette før, men ser nå at antall avvik som meldes inn er høyere enn tidligere. Informanten sier det ikke nødvendigvis skyldes at det er flere avvik enn tidligere, men håper det er på grunn av en bevisstgjøring om hvor viktig det er å melde ifra for å kunne bearbeide feil og mangler i de tekniske barrierene.

For kommune 2 er det i tillegg viktig at ledere og mellomledere i organisasjonen implementerer prinsipper fra sikkerhetskultur i sitt arbeid, slik at de ansatte i hver avdeling kan bli mer bevisst. Ifølge informanten har det etter hvert blitt flere og flere ledere som uttrykker viktigheten av sikkerhetskultur. Derfor har det i det siste også blitt enklere å få bevilget penger til nødvendige sikkerhetstiltak, enn det informanten har opplevd tidligere. Informanten ser dette i

sammenheng med truslene som følge av en ustabil sikkerhetssituasjon i Europa, og poengterer at bevisstgjøring og nye sikkerhetstiltak er noen av de viktigste barrierene mot angrep utenfra.

Arbeid med god sikkerhetskultur anses som en viktig barriere for å redusere sjansen for menneskelig svikt. For å opparbeide dette har kommunen flere holdningskampanjer og kurs knyttet til risiko og sårbarheter ved hybridkontoret. Det inkluderer for eksempel et IT-sikkerhetskurs samtlige ansatte skal gjennomføre. Kurset består av opplæring i håndtering av trusler, hva ansatte kan bli utsatt for av svindelforsøk, og gode råd om hvordan man bør oppføre seg på digitale plattformer. Ansatte som jobber med personvern og sikkerhet i kommunen har i tillegg hatt egne årlige kurs. Kursene skal i utgangspunktet være obligatoriske, men enkelte ansatte skylder på dårlig tid og gjennomfører derfor ikke kursene. Videre nevner informanten at det blir sendt ut kampanjer som opplyser hvordan de ansatte skal sikre trådløst nettverk ved bruk av hjemmekontor. Kampanjene inneholder også informasjon om opprettelse av lange passord. Dette er for øvrig tiltak som er blitt innført etter pandemiens utbrudd. I tillegg til kampanjer og kurs finnes et IKT-reglement alle nyansatte skal følge, og det er ledernes ansvar å påse at reglementet blir opprettholdt. Slike tiltak fører blant annet til bedre oversikt for den ansatte over kommunens ulike tjenester, og hva som gjelder av reglement på de forskjellige avdelingene.

Informanten eksemplifiserer med svindel på e-post for å understreke viktigheten av god digital sikkerhetskultur. En utfordring som stadig gjentas i kommunen er at ansatte trykker på utrygge lenker, åpner infiserte vedlegg eller oppgir informasjon i svindelsammenheng på e-poster. Kommunen har ikke opplevd alvorlige dataangrep, men det har vært enkelte tilfeller der noen PCer har blitt infisert som resultat av dette. Svindel på e-post har derimot ikke utgjort en trussel mot det sentrale overordnede systemet i kommunen, fordi det allerede foreligger gode tekniske barrierer knyttet til slike svindelforsøk. Samtidig vil noen svindel-e-post og infisert materiale unngå barrierene, og ifølge informanten vil god digital sikkerhetskultur derfor kunne bidra til å oppdage og rapportere svindel-e-post.

4.7 Forskningsspørsmål 2

4.7.1 Ulike tilnærminger til digital sikkerhetskultur

Digital sikkerhetskultur er et begrep kommunene er godt kjent med, og begge uttrykker at det omhandler bevisstgjøring blant de ansatte. Kommunene har likevel til dels ulike tilnærminger til oppbygging av digital sikkerhetskultur. Digital sikkerhetskultur ble definert i teorikapitlet

(Malmedal & Røislien, 2016, s. 28), og det vil i dette delkapittelet diskuteres om kommunenes tanker og holdninger rundt sikkerhetskultur samsvarer med definisjonen.

Kommune 1 sin beskrivelse av begrepet handler i stor grad om bevisstgjøring av og kommunikasjon med ansatte. Ifølge kommunen er ansatte ideelt sett den beste sikkerhets-ressursen kommunen har mot både indre og ytre trusler, så lenge de ansatte vet *hva* de skal gjøre, *hvordan* de skal gjøre det og *hvorfor* de burde gjøre det. Dette er i tråd med definisjonen til Malmedal & Røislien (2016) som vektlegger utvikling av blant annet holdninger og kunnskap for å oppnå en god digital sikkerhetskultur. Med andre ord er den digitale sikkerhetskulturen avhengig av god kommunikasjon for å sikre bevisstgjøring og økt kunnskap hos de ansatte. Kommunikasjonen krever derfor tydelige holdningskampanjer og retningslinjer fra sikkerhetsavdelingen i kommunen, med hensikt å skape en felles forståelse og felles praksis. Reason (1997) trekker dette frem som viktige tiltak for å danne en felles forståelse på arbeidsplassen. Det kan føre til bevissthet, riktig atferd og gode interne verdier som vil sikre at utviklingen av IKT-sikkerheten blir en fremtidsrettet prosess.

Det at kommune 1 legger vekt på kommunikasjon, kan tyde på at de har en lærende kultur (Reason, 1997). Å lære av egne og andres erfaringer rundt digital sikkerhet er viktig for å forstå egne sårbarheter. Det kan indirekte føre til en organisatorisk fleksibilitet, som vil bidra til å øke evnen og villigheten til å omstille seg, både etter og i forkant av en uønsket hendelse. I stor grad innebærer det å holde seg oppdatert på nye teknologiske løsninger, og legge til rette for at systemene vil tåle ulike påkjenninger.

I likhet med definisjonen (Malmedal & Røislien, 2016) vektlegger kommune 2 betydningen av adferd tilknyttet digital sikkerhetskultur. Gode rutiner og opplæring i atferd på digitale plattformer er noe som trekkes særlig frem. Gjennom opplæring vil man kunne bidra til å øke kunnskapsnivået om trusler og sårbarheter i forbindelse med hybridkontor. På bakgrunn av hvordan kommune 2 definerer og praktiserer digital sikkerhetskultur, har kommunen således en tilnærming som ligner HRO, som innebærer at god sikkerhetskultur kan være med på å redusere sannsynligheten for uønskede hendelser (Engen m.fl., 2021). Kommune 2 ønsker i tillegg at det skal være kultur for å melde inn avvik. Det kan knyttes til Reason (1997) sin beskrivelse av en rapporterende kultur som en forutsetning for god sikkerhetskultur. Ved å ha gode og trygge rammer for rapportering av avvik, vil det resultere i økt grad av tillit mellom ansatte og ledelsen. Samtidig gir det muligheter til å stanse og/eller begrense uønsket aktivitet

i systemene tidlig i forløpet. Reason (1997) peker også på dette som et av de viktigste grunnprinsippene for å opprettholde god digital sikkerhetskultur.

Til tross for at kommunene har ulike tilnærminger til god digital sikkerhetskultur, er de tydelig bevisst på å bygge digital sikkerhetskultur på tvers av hele organisasjonen. Felles for kommunene er ønsket om at alle ledere og mellomledere må være bevisste på konseptet. Slik digital sikkerhetskultur blir beskrevet av Malmedal & Røislien (2016), så handler det blant annet om holdninger mennesker har i møte med digitale systemer. På sikt vil en felles forståelse av sikkerhet derfor være avgjørende for at organisasjonen klarer å utvikle en god digital sikkerhetskultur. Basert på det som har blitt diskutert, kan det tolkes at kommunenes holdninger og tanker rundt digital sikkerhetskultur samsvarer overordnet med definisjonen (Malmedal & Røislien, 2016), til tross for at de har forskjellig innfallsvinkler på konseptet.

4.7.2 Digital sikkerhetskultur som barriere

Et eksempel på en situasjon som utfordrer den digitale sikkerhetskulturen på hybridkontor er som nevnt svindelforsøk på e-post. Det er særlig krevende for kommunene at ansatte trykker på lenker eller oppgir informasjon gjennom svindel-e-post. For å minimere muligheten for mennesker til å være den sårbare komponenten i IKT-systemer på hybridkontor, er sikkerhetskultur helt grunnleggende. Samtidig er det essensielt at sikkerhetskulturen på det fysiske kontoret overføres og opprettholdes på hjemmekontor. Det kan også ses i lys av NSM sine grunnprinsipper for det forebyggende arbeidet med IKT-sikkerhet (NSM, 2020).

For det første kan god digital sikkerhetskultur bidra til å *beskytte og opprettholde* forsvarlig sikring av IKT over tid (NSM, 2020). Kommuner kan etablere rutiner og bevissthet overfor de ansatte, og tilpasse datamaskiner og programvare på hybridkontor slik at det er enkelt for hver ansatt å opprettholde rutiner og oppmerksomhet rundt sikkerhet. Tilstrekkelig forfølging av dette prinsippet kan for eksempel ha stor effekt på utfordringene kommune 1 og kommune 2 påpeker med svindelforsøk av ansatte gjennom e-poster. For det andre kan god digital sikkerhetskultur bidra til å *oppdage* og fjerne sårbarheter (NSM, 2020). Ved at kommunene både setter større søkelys på sårbarhetsvurderinger rundt IKT-sikkerhet på hybridkontor, samt har en kultur for å melde ifra om avvik i systemet, gjør at de ansatte får mer kunnskap og blir mer bevisst på IKT-sikkerhet. God sikkerhetskultur er avgjørende for at NSM sine grunnprinsipper skal bli gjennomført på en god måte. Dersom dette mangler, kan prosessen fra å identifisere til å gjenopprette være utfordrende og preget av manglende sammenheng og kontroll.

4.7.3 Bevisstgjøring, kommunikasjon og ledelse

I en prosess hvor arbeidshverdagen blir todelt, slik som ved hybridkontoret, kan det argumenteres for at kommunenes systemer blir mer komplekse og krever høyere grad av bevissthet. Med utgangspunkt i hvordan Perrow (1999) beskriver komplekse systemer, kan det diskuteres om det faktisk er mulig å oppnå tilstrekkelig kunnskap. Kommunene opplevde et økt antall digitale angrep utenfra etter pandemiens utbrudd, og ble gjort oppmerksomme på at deres ansatte ikke hadde tilstrekkelige ferdigheter og kunnskap i møte med slike trusler. Mangel på ferdigheter og kunnskap kan anses som en utfordring for sikkerhetsstyring av IKT-sikkerhet (Njå m.fl., 2020). Kommune 2 sier derfor at bevisstgjørelse kan være den viktigste barrieren en kommune har mot digitale trusler. Dette samsvarer med kommune 1 sitt utsagn om at det er de ansatte som er den beste sikkerhetsressursen kommunen har mot både indre og ytre trusler. Dette avhenger igjen av at de vet hva de skal gjøre, hvordan de skal gjøre det og hvorfor de burde gjøre det. Kommunene prøver å oppnå bevisstgjøring gjennom virkemidler som kampanjer, kurs for de ansatte, eller opplæring i de tekniske verktøyene brukt på hybridkontoret. Dette omtaler Njå m.fl. (2020) som organisatoriske tiltak for styring av IKT-sikkerhet. Det krever klare og tydelige retningslinjer og kommunikasjon fra sikkerhetsavdelingen i kommunen, noe kommunene setter søkelys på å opprettholde og utvikle.

Kommunene sier at ledelsen har et stort ansvar for organisering og styring av digital sikkerhetskultur. Det er viktig at ledelsen ser god digital sikkerhetskultur som et sentralt virkemiddel for IKT-sikkerhet på hybridkontor. Som illustrert i teorikapitlet presenterer Njå m.fl. (2020) "ledelsesstruktur- og -utøvelse" som en av flere virkemidler knyttet til sikkerhetsstyring. Ansatte i ulike avdelinger vil bli mer bevisst på å opprettholde god sikkerhetskultur, dersom ledelsen på en tydelig måte kommuniserer hvorfor god digital sikkerhetskultur er viktig. I NSM sitt første grunnprinsipp, som omhandler *identifisering og kartlegging,* er det helt essensielt med en forståelse av ledelsesprioriteringer for sikkerhetsstyringen i virksomheten (NSM, 2020). Med andre ord er ledelsens atferd, holdninger og handlinger i forbindelse med sikkerhet i IKT-infrastrukturen viktig for utvikling og opprettholdelse av et velfungerende system. En lik forståelse og innsats på tvers av ledere vil også føre til bedre oversikt og kontroll over systemet, og gi bedre grunnlag for innføring av nødvendige sikkerhetstiltak underveis.

Det presiseres fra både kommune 1 og kommune 2 at utviklingen av en god digital sikkerhetskultur er en kontinuerlig prosess. Kommune 1 forteller at de har en lang vei å gå, og at kommunen til enhver tid har et ansvar for å være bevisst på å utvikle den digitale

sikkerhetskulturen. Det er for å hindre mennesket som en sårbarhet i størst mulig grad, og heller utvikle mennesket til å være en barriere for uønskede hendelser i IKT-systemet på hybridkontor. En god digital sikkerhetskultur kan anses som et ideelt mål for kommunene, og arbeidet med å utvikle god digital sikkerhetskultur mener kommunene er det viktigste virkemiddel for å etablere en tolererbar IKT-sikkerhet på hybridkontor (Njå m.fl., 2020).

5.0 Konklusjon

Hybridkontor er et relativt nytt konsept som har utviklet seg etter utbredt bruk av hjemmekontor under koronapandemien. Det innebærer at kommunene fortsetter å tilby en kombinasjon av hjemmekontor med fysisk oppmøte på arbeidsplassen. Det har blitt *den nye normalen* for mange ansatte i kommunene. Oppgavens formål har vært å besvare problemstillingen: *Hvilke konsekvenser har hybridkontor for risiko og sårbarhet i IKT-systemer i kommunene, og hvordan jobber de for å håndtere dette?*

Kommunene opplever flere utfordringer med styring av IKT-sikkerhet på hybridkontor, som igjen kan ha konsekvenser for risiko og sårbarhet i IKT-systemene. De tekniske utfordringene er særlig svake passord, bruk av private hjemmerutere, og svindel-e-poster. For å håndtere utfordringene har kommunene iverksatt flere tiltak. Det inkluderer jevnlig oppdatering av de tekniske systemene, totrinnsverifisering, innføring av lange passord og VPN. Utbedringer av disse tiltakene kan bidra til en bedre sikkerhetsstyring av IKT-systemet på hybridkontor. Likevel er det vanskelig å få gjennomslag for hvert tiltak, og ikke alle tiltak blir gjennomført av alle ansatte i tilstrekkelig grad. Sikkerhetsstyring, og innføring eller utbedring av eksisterende tekniske tiltak, er en kontinuerlig prosess for kommunene. Samtidig er det utfordrende å forutse nye angrep og være godt nok forberedt for hvert enkelt tilfelle.

Til tross for kommunene sine tekniske utfordringer og virkemidler, ble den menneskelige faktoren trukket frem som den største utfordringen for IKT-sikkerhet på hybridkontor. Et virkemiddel som både kommune 1 og kommune 2 vektlegger, er bedring av sikkerhets-kulturen. Kommune 1 trekker frem bevissthet og kommunikasjon om viktige elementer av begrepet god digital sikkerhetskultur, mens kommune 2 trekker frem adferd, gode rutiner og opplæring. Felles for kommunene er viktigheten av ledelsens involvering i arbeidet. En god digital sikkerhetskultur er fundamentet for at flere av de tekniske tiltakene skal fungere optimalt. På hybridkontor er god digital sikkerhetskultur svært viktig fordi de ansatte i større grad blir ansvarliggjort for å begrense mulighet til svikt i IKT-systemene, og for å danne en

felles forståelse som vil virke veiledende og styrke følelsen av en felles forståelse for verdier og holdninger på arbeidsplassen.

Hybridkontor kan med andre ord ha store konsekvenser for risiko og sårbarhet i IKT-systemer i kommunene, dersom kommunene ikke evner å iverksette funksjonelle tekniske tiltak eller å styrke den digitale sikkerhetskulturen. Hvis kommunene derimot evner å oppnå dette, så vil det kunne skape mindre risiko og sårbarhet for IKT-systemene på hybridkontor. Samtidig vil det fjerne usikkerhet både for kommunens ansatte og for kommunen som innehaver av kritiske samfunnsfunksjoner. Selv om de tekniske tiltakene ble nevnt som et viktig element i sikkerhetsarbeidet, var kontinuerlig bevisstgjøring for å styrke den digitale sikkerhetskulturen ansett som det viktigste tiltaket for IKT-sikkerhet på hybridkontor.

Referanseliste

Blaikie, N. & Priest, J. (2019). *Designing social research: the logic of anticipation* (3rd edition.). Polity Press.

Direktoratet for samfunnssikkerhet og beredskap [DSB]. (2016). *Samfunnets kritiske funksjoner: Hvilken funksjonsevne må samfunnet opprettholde til enhver tid?* Versjon 1.0. https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-2_januar.pdf

Engen, O.A.H., Gould, K.A.P., Kruke, B.I., Lindøe, P.H., Olsen, K.H. & Olsen, O.E. (2021). *Perspektiver på samfunnssikkerhet* (2. utg.). Cappelen Damm Akademisk.

Jacobsen, D. I. (2005). *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode* (2.utg.). Høyskoleforlaget.

Jore, S. (2019). The conceptual and Scientific Demarcation of Security in Contrast to Safety. *European Journal for Security Research, (1)*4, s. 157-174.

Malmedal, B., Røislien, H. E., (2016). *The Norwegian Cyber Security Culture*. NorSIS, Norge. https://norsis.no/wp-content/uploads/2016/09/The-Norwegian-Cybersecurity-culture-web.pdf

Nasjonal sikkerhetsmyndighet (NSM). (2019). *Råd og anbefalinger om passord.* Hentet fra https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/rad-og-anbefalinger-om-passord

Nasjonal sikkerhetsmyndighet [NSM]. (2020). *NSMs grunnprinsipper for IKT-sikkerhet* (versjon 2.0). https://nsm.no/getfile.php/133735-1592917067/Filer/Dokumenter/Veiledere/nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf

Nasjonal sikkerhetsmyndighet [NSM]. (2021). *Risiko 2021 – helhetlig sikring mot sammensatte trusler*. https://nsm.no/getfile.php/136419-1616673370/Filer/Dokumenter/Rapporter/NSM_Risiko_2021_web_enkeltside_1203.pdf

NetSecurity. (u.å). *Hva er Ddos-angrep?* https://www.netsecurity.no/begrepsordliste/ddos-angrep?utm_term=&utm_campaign=DSA+%7C+Alle+sider&utm_source=adwords&utm_medium=ppc&hsa_acc=3943857293&hsa_cam=6520817474&hsa_grp=78981225995&hsa_ad=383630224947&hsa_src=g&hsa_tgt=dsa-

19959388920&hsa_kw=&hsa_mt=&hsa_net=adwords&hsa_ver=3&gclid=Cj0KCQjw06OTBhC_ARIsAAU1yOW4X7rvFBqrFhTL2qhKR4XS_6Dmez4GBqQVanaxrld1fjoF7iVRaXYaAlnSEALw_wcB

Norges vassdrags- og energidirektorat [NVE]. (2021). *IKT-sikkerhetstilstanden i kraftforsyningen i 2021*. Ekstern rapport (nr. 19/2021).

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

Perrow, C. (1999). *Normal accidents: living with high-risk technologies.* Princeton University Press: Princeton.

Personopplysningsloven. (2018). *Lov om behandling av personopplysninger.* (LOV-2018-06-15-38). Lovdata. https://lovdata.no/dokument/NL/lov/2018-06-15-38

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

Sikkerhetsloven. (2018). *Lov om nasjonal sikkerhet*. (LOV-2018-06-01-24). Lovdata. https://lovdata.no/lov/2018-06-01-24

Renn, O., Lucas, K., Haas, A. & Jaeger, C. (2019). Things are different today: The challenge of global systemic risks, *Journal of Risk Reseach, 22*(4): 401-415.

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

Wolf, M and Serpanos, D. (2018). Safety and Security in Cyber-Physical Systems and Internet-of-Things Systems. *Proceedings of the IEEE, 106*(1). Doi: 10.1109/JPROC.2017.2781198