Bacheloroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Vilde Nylund Johnsen
Karianne Kjønås
Thea Erbe Thomassen

Åpenhetens dilemma

Bacheloroppgave i IT-drift og informasjonssikkerhet
Veileder: Erjon Zoto

Mai 2021

NTNU
Kunnskap for en bedre verden

Vilde Nylund Johnsen
Karianne Kjønås
Thea Erbe Thomassen

Åpenhetens dilemma

Bacheloroppgave i IT-drift og informasjonssikkerhet
Veileder: Erjon Zoto
Mai 2021

Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for informasjonssikkerhet og kommunikasjonsteknologi

NTNU
Norwegian University of
Science and Technology

Sammendrag

Tittel:	Åpenhetens dilemma
Dato:	20.05.2021
Deltakere:	Vilde Nylund Johnsen Karianne Kjønås Thea Erbe Thomassen
Veileder:	Erjon Zoto, universitetslektor, Institutt for informasjonssikkerhet og kommunikasjonsteknologi
Oppdragsgiver:	Roar Thon, Nasjonal sikkerhetsmyndighet (NSM)
Nøkkelord:	Informasjonssikkerhet, Media, NSM, Dataangrep, Intervju
Antall sider:	61
Antall vedlegg:	4
Tilgjengelighet:	Åpen

Sammendrag: Åpenhetens dilemma innen IT sikkerhet handler om at deling av informasjon og erfaringer er viktig for å beskytte landet mot trusler, samtidig som deling kan avsløre sårbarheter og svakheter hos virksomhetene som deler informasjonen. Denne oppgaven tar i bruk intervjuer for å få svar på spørsmål knyttet til rutiner og erfaringer relatert til IT-sikkerhet, og kan brukes til å identifisere faktorene som påvirker virksomheter i valget om åpenhet overfor både Nasjonal sikkerhetsmyndighet (NSM) og offentligheten. Undersøkelsen viser at virksomhetene sin opplevelse av relevans og ønske om å hjelpe andre er de største faktorene som påvirker deling til både NSM og media. Deling overfor NSM gjøres også mye fordi virksomhetene ønsker å få hjelp til å håndtere hendelsene. Lovverk går igjen som årsak til at virksomheter har delt en hendelse, men også ikke delt. Ulike sektorer påvirkes ulikt av sitt lovverk. Vurderingen rundt å gå ut med informasjon om en hendelse påvirkes også av hvordan virksomheter tror det vil påvirke offentlighetens syn på virksomheten.

Abstract

Title:	Åpenhetens dilemma
Date:	20.05.2021
Authors:	Vilde Nylund Johnsen Karianne Kjønås Thea Erbe Thomassen
Supervisor:	Erjon Zoto, universitetslektor, Institutt for informasjonssikkerhet og kommunikasjonsteknologi
Employer:	Roar Thon, Nasjonal sikkerhetsmyndighet (NSM)
Keywords:	Information security, Media, NSM, Hacking
Pages:	61
Attachments:	4
Availability:	Open

Abstract: The dilemma of openness within the information technology security community is about sharing information and experiences to protect the country against threats, whilst being considerate of the weaknesses that can be exposed for the companies who choose to share information. This thesis uses interviews to find out which routines and experiences different companies have with IT security, and use the information to identify the factors that affect organizations in the choice of being open towards both Nasjonal sikkerhetsmyndlighet (NSM) and the public. The research revealed that how relevant the companies perceive the incident, and their desire to help others, are the factors that affect sharing an incident with NSM and the media the most. Openness towards NSM is also affected by the level of help the companies need to handle the situation. Laws are repeatedly listed as the reason for organizations sharing an incident, but also when they do not share it. Different sectors are affected differently by various laws and regulations. The choice of sharing information is also influenced by how organizations believe the incident will affect the public's opinion of the company.

Forord

Utviklingen i det digitale trusselbildet fører til økende og skjerpede krav til informasjonssikkerhet. Kravene treffer den enkelte virksomhet som ansvarlig for behandling av informasjon og digitale systemer og tjenester. Samtidig som digitaliseringen åpner for nye muligheter så øker også risikoen for sårbarheter og sikkerhetsbrudd. De digitale løsningene skal fungere med både interne og eksterne brukere og ulike aktører har ulike roller som krever tilgang på tvers av behandlingsansvar. Sikkerhetsnivået avhenger i stadig større grad av samarbeid og dialog på tvers av virksomheter og respektive tredjeparter for å kunne beskytte seg selv og hverandre. Jo mer vi har lært om informasjonssikkerhet, jo mer har dette skapt interesse hos oss.

Denne bacheloroppgaven tar utgangspunkt i Nasjonal Sikkerhetsmyndighet (NSM) sin rapport "Risiko 2020" og deres observasjoner og vurderinger rundt dilemmaet mellom krav til konfidensialitet og hemmelighold av sikringstiltak og sikkerhetsbrudd og behovet for åpenhet og deling av erfaringer og kompetanse mellom aktørene.

Oppgaven har gitt oss muligheter for å bli kjent med ulike aktører i et utvalg av virksomheter som selv har erfaringer med dilemmaet. Det har vært spennende og lærerikt å intervjue disse aktørene og se nærmere på deres valg og prioriteringer for å kunne konkludere med en hypotese om hva som ligger til grunn for vurderinger og valg de gjør.

Tusen takk til Roar Thon og NSM for oppdraget og veiledning av oppgaven.
Takk til vår veileder Erjon Zoto for veiledning gjennom arbeidet.
Takk til Tom Røise og Erik Hjelmås for gjennomlesing og tilbakemeldinger.
Takk til Gaute Bjørklund Wangen for verdifull veiledning.

Og til slutt en spesiell takk til sikkerhetsledere og ansatte ved virksomhetene som er intervjuet for deres imøtekommenhet, deling og engasjement for oss og vår oppgave. Vi ser frem til å dele resultatene fra dette samarbeidet med dere og andre interessenter i bransjen.

Innhold

Figurer

Akronymer

AAR After Action Review. 36

CERT Computer Emergency Response Team. 11, 37, 38

GDPR General Data Protection Regulation. 36

IKT Informasjons- og kommunikasjonsteknologi. 7

ISMS Information Security Management System. 29

ISO International Organization for Standardization. 15, 29

IT Informasjonsteknologi. iii

ITIL Information Technology Infrastructure Library. 11, 29

MAPP Microsoft Active Protections Program. 11

NCSC Nasjonalt Cybersikkerhetssenter. 30, 37, 38, 47

NDA Non-Disclosure Agreement. 11

NHO Næringslivets Hovedorganisasjon. 20, 26

NIST National Institute of Standards and Technology. 9, 25, 27, 29, 48

NSM Nasjonal sikkerhetsmyndlighet. iii, iv, 2, 4, 6, 13, 18, 24, 25, 28, 29, 31, 32, 39–43, 46, 47, 49, 55, 56

NTNU Norges teknisk-naturvitenskapelige universitet. 4, 5, 22, 62

NVE Norges vassdrag- og energidirektorat. 13, 20, 33

SCADA Supervisory Control And Data Acquisition. 27

TLP Traffic Light Protocol. 11, 28, 31

Kapittel 1

Introduksjon

1.1 Bakgrunn og Formål

Ulike sikkerhetshendelser rammer norske virksomheter i større grad nå enn tidligere [1]. I den anledning er det stor variasjon i hvilke virksomheter som ønsker å være åpne eller ikke rundt disse hendelsene. Dette rammer både små og store virksomheter over hele landet. I 2020 ble både Stortinget og Østre Toten kommune utsatt for omfattende dataangrep. Dette er bare to av mange sikkerhetshendelser som har oppstått i 2020. Stortinget opplevde et datainnbrudd i deres e-postsystemer som rammet den viktigste demokratiske institusjonen i Norge. Østre Toten kommune opplevde et dataangrep mot deres datasystem hvor all data ble kryptert og sikkerhetskopier slettet. I disse to hendelsene har det vært forskjeller i hvordan virksomhetene har valgt å dele og vært åpen om situasjonen. [2, 3]

Formålet med denne oppgaven er å få belyst hvilke faktorer som danner beslutningsgrunnlaget for valgene norske virksomheter tar når de vurderer deling og åpenhet knyttet til en sikkerhetshendelse. Det skal undersøkes hva virksomhetene legger vekt på og tenker når de velger å dele eller ikke dele, og hvem som tar valget om å dele. Gjennom oppgaven skal det forsøkes å finne likheter og forskjeller, og se om funnene kan brukes til å få virksomheter til å dele mer.

1.2 Problemområde

Hvordan de ulike virksomhetene håndterer den økende graden av sikkerhetshendelser kan variere basert på hvilke rammeverk de benytter seg av, hvilke rutiner som er på plass og hvilke lovverk de er underlagt. Et omdiskutert tema som denne oppgaven skal ta for seg er om virksomheter velger å ikke dele sikkerhetshendelser grunnet frykt for at dette kan føre til tap av omdømme [4, 5].

Mørketallsundersøkelsen tar opp sikkerhetshendelser og håndtering av disse på

ledelsesnivå. Her blir det spesifisert at ledelsen har både kjennskap til og er involvert i de ulike sikkerhetshendelsene. Hos 69% av virksomhetene blir ledelsen trukket inn som en del av følgende etter hendelsen. Om involveringen av ledelsen påvirker om virksomheten deler mer er ikke diskutert. [4]

Den årlige innbyggerundersøkelsen fra Forsvaret viser at den generelle befolkningen også under en pandemi har sikkerhetshendelser som sin største frykt når det kommer til nasjonal sikkerhet. Undersøkelsen avdekket for første gang i 2017 at nordmenn opplevde sikkerhetshendelser som den største trusselen mot nasjonal sikkerhet, og trusselen har toppet listen siden. [6, 7]

I det samme tidsrommet har det oppstått flere større sikkerhetshendelser virksomheter ikke har kunnet skjule blant annet grunnet deres omfang, og at kunder ikke får tilgang til tjenesten(e) virksomheten leverer [2, 3, 8, 9]. Dette har også ført til at det i det små har blitt mer åpenhet rundt sikkerhetshendelser [10]. Likevel er det vanskelig å si om dette har en sammenheng eller ikke, da det ikke er nok forskning på temaet.

1.3 Problemstilling

Oppgaven skal ta for seg denne problemstillingen:

> *"Hvilke faktorer påvirker virksomheter sitt valg om åpenhet?"*

1.3.1 Hypotese

Oppgaven baserer seg på to hypoteser.

> Hypotese 1:
> *virksomheter ønsker ikke å dele sikkerhetshendelser med media av frykt for tap av omdømme hos offentligheten, som kan føre til økonomisk tap gjennom tap av kunder.*
>
> Hypotese 2:
> *virksomheter som ikke involverer ledelsen i håndtering av hendelser er mindre åpne om sikkerhetshendelser enn der ledelsen er involvert.*

1.3.2 Forskningsspørsmål

Denne oppgaven skal forsøke å svare på følgende forskningsspørsmål:

- Hvilke faktorer er med på å påvirke virksomheter sitt valg om åpenhet overfor NSM og andre virksomheter for lærdom og videreutvikling?
- Hvilke faktorer er med på å påvirke virksomheter sitt valg om åpenhet for media?

- Hvilke faktorer er med på å påvirke valget om åpenhet i ulike sektorer?
- På hvilket ledelsesnivå blir sikkerhetshendelser håndtert, i praksis, i virksomhetene?

1.4 Prosjektmål

Målet for denne oppgaven er å identifisere og diskutere punktene som er beskrevet, for å kunne dannet ett godt grunnlag til å svare på oppgavens problemstilling.

- Få en klar formening om hva virksomheter legger i ordet "åpenhet" rundt sikkerhetshendelser.
- Hvilke regulatoriske rammeverk rundt sikkerhetshendelser og tvungen åpenhet eksisterer.
- Hvilke behov for hemmelighold eller konfidensialitet rundt sikkerhetshendelser har de ulike virksomhetene, og hvordan fungerer det i praksis.
- Hvilke behov og muligheter for åpenhet om digitale sårbarheter og hendelser har virksomheter.
- Identifisere hva virksomhetene selv ser på som fordeler og ulemper ved åpenhet og deling av sikkerhetshendelser.

1.5 Avgrensning

Oppgaven skal vurdere hvordan man kan tilrettelegge for åpenhet og samarbeid om digitale sårbarheter og sikkerhetshendelser ved å se på noen utvalgte fagforum og møteplasser etablert for å tilrettelegge for samarbeid og deling:

- Digitale varslingssystemer og responsfunksjoner.
- Samarbeidsmiljø for forebyggende sikkerhet.
- Fagforum og uformelle/uregulerte møteplasser.

Oppgaven avgrenser til åpenhet mellom virksomheter i Norge og vurderer ikke problemstillinger knyttet til interne tilganskontrollregimer.

1.6 Målgruppe

Oppgaven sin målgruppe er norske virksomheter, IT-sikkerhetsansatte, forskere og studenter som er interessert i informasjonssikkerhet. En stor andel norske virksomheter er små og mellomstore, og oppgaven skal derfor fokusere på virksomheter i forskjellige størrelser, ikke bare store. Virksomhetene er også fordelt på flere sektorer for å videre tilrettelegge for relevans på tvers av sektor. Dette vil gi et resultat som er mer representativt for målgruppen. [11]

1.7 Oppgavebeskrivelse

Nasjonal sikkerhetsmyndlighet (NSM) er en fagmyndighet for forebyggende sikkerhet. NSM gir blant annet råd om og fører tilsyn med sikring av informasjon, informasjonssystemer, objekter og infrastruktur av nasjonal betydning. Videre er NSM nasjonalt fagmiljø for digital sikkerhet og har på nasjonalt nivå et ansvar for å oppdage, varsle og koordinere håndtering av alvorlige digitale angrep. [12]

I rapporten "Risiko 2020" vurderer NSM risikoen for at samfunnet skal rammes av tilsiktede handlinger som direkte eller indirekte kan skade viktige samfunnsinteresser. Rapporten tar blant annet opp dilemmaet åpenhet versus hemmelighold: "Åpenhet, deling av informasjon og erfaring, og samarbeid på tvers av ansvarsområder er stadig viktigere for å beskytte seg mot truslene. Samtidig kan denne åpenheten avsløre svakheter og sårbarheter hos hverandre. Hvor er den beste balansen mellom åpenhet og hemmelighold?". [12]

Stadig flere norske virksomheter opplever sikkerhetshendelser [1]. Mange deler informasjon om hendelsen innen sin sektor, andre deler informasjonen bredere. Flere står frem i offentlighetens lys med sin hendelse og andre velger å holde hendelsen skjult. Nasjonal sikkerhetsmyndighet ønsker å få økt kunnskap om hva som kan bidra til økt deling og åpenhet rundt sikkerhetshendelser.

Oppgaven skal se nærmere på åpenhetens dilemmaet og undersøke ulike kriterier for å balansere verdien av åpenhet, deling, og samarbeid mot risikoen for hendelser og skade. Gjennom deling av informasjon legger virksomheten også til rette for å selv kunne motta bistand til håndtering av hendelsen. Deling av informasjon om hendelser tilrettelegger for læring og bedre forebygging, både i egen virksomhet og hos andre.

1.8 Prosjektgruppens bakgrunn

Gruppen går tredje og siste året på bachelor i IT-drift og informasjonssikkerhet ved Norges teknisk-naturvitenskapelige universitet (NTNU). Gjennom studiet har gruppemedlemmene tilegnet seg kunnskap innen flere fagområder, hvor risikostyring, prosjektplanlegging, tjenesteforvaltning, hendelseshåndtering og generell informasjonssikkerhet er direkte relevant for denne oppgaven. Oppgaven krever direkte forståelse for disse fagområdene, både for å lage relevante spørsmål og for å forstå svarene og kunne diskutere med intervjuobjektene.

1.9 Rammer

Rapporten er skrevet på norsk ettersom publikum og alle intervjuobjektene er norske, og kulturforskjeller gjør at resultatet ikke nødvendigvis er relevant for virksomheter i andre land. I tillegg kan språklige nyanser spille en aktiv rolle i forståelsen av innholdet.

Rapporten vil bli skrevet i ShareLatex. På grunn av smittesituasjonen i landet blir intervjuene gjennomført digitalt over Microsoft Teams. Til analysen er programvaren NVivo benyttet med en lisens fra NTNU som er gyldig frem til 31.12.2021. Prosjektet skal være ferdig og leveres 20.05.2021.

1.10 Arbeidsmetode

Prosjektperioden deles inn i to hovedfaser. Først er det fokus på teori og utarbeidelse av intervjuguiden. Når dette er ferdig begynner gjennomføringen av selve intervjuene og analysen av svarene. Arbeidet foregår sekvensielt, hvor den første delen må være fullført før neste kan påbegynnes. Innenfor hver hovedseksjon foregår hendelsene parallelt, da analysen av et intervju kan foregå samtidig som intervjuene gjennomføres.

1.11 Rapportstruktur

I kapittel 2 beskrives alle teorier som trekkes frem i intervjuspørsmålene og legger grunnlaget for det faglige innholdet i oppgaven. I kapittel 3 beskrives de ulike metodene som er tatt i bruk i løpet av prosjektet for å gjennomføre intervjuene og analysere resultatet. Intervjuspørsmålene beskrives i kapittel 4, delt inn i kategorier med tilhørende beskrivelse av teorier og hensikter som er gjeldende i hver kategori. Selve analysen er beskrevet i kapittel 5, hvor dataen som er samlet inn gjennom intervjuene oppsummeres og illustreres ved bruk av figurer.

Resultatene diskuteres i kapittel 6 ved å svare på spørsmål knyttet til hensikter beskrevet i intervjuguiden, og refleksjoner gruppen har gjort seg gjennom intervjuprosessen. Her beskrives også begrensinger, erfaringer og kritikk til oppgaven, i tillegg til foreslått videre arbeid. Til slutt kommer konklusjonen i kapittel 7, hvor forskningspørsmålene og problemstillingen blir besvart på, og hypotesene konkludert.

Kapittel 2

Teori

2.1 Introduksjon

Teorikapittelet består av flere seksjoner, hvor hver del detaljert beskriver en type teori som er relevant for oppgaven. Rapporten baserer seg på en stor mengde teori for å kunne analysere om innsamlet data samsvarer med eksisterende teorier. Definisjoner er tydelig beskrevet for å forsikre en felles forståelse av begrepene. Dette er viktig for å hindre at ulike begrepsdefinisjoner lager misforståelser som kan påvirke resultatet i oppgaven. Dette gjelder også lovverk og hvilke virksomheter som er underlagt hvilke lover og regler, og om disse lovene er til hinder for åpenhet og deling av ulike sikkerhetshendelser.

Mange virksomheter benytter seg av rammeverk som spesifiserer og setter krav til virksomheten og deres samarbeid med andre. Virksomheter som ikke tar i bruk rammeverk kan gi andre svar og gjøre ting på en annen måte, noe som kan ha betydning for oppgaven. Også artikler og rapporter utgjør en relevans for oppgaven grunnet erfaring og konkrete tall på ulik data.

2.2 Definisjoner

Klare definisjoner er nødvendig for å oppnå riktig forståelse i rapporten. Definisjonene av åpen informasjon og en trussel er hentet fra NSM. Definisjonen av en sikkerhetshendelse er hentet fra Nettvett da NSM sin definisjon baserer seg på kritisk infrastruktur. Definisjonen fra NSM kan være relevant for enkelte virksomheter, men mange virksomheter har ikke kritisk infrastruktur eller sikkerhetshendelser tilknyttet kritisk infrastruktur. Dermed blir Nettvett sin definisjon mer relevant for denne oppgaven.

> Åpen informasjon
> *Åpen informasjon er informasjon som ved lovlig fremgangsmåte er tilgjengelig for alle som ønsker å finne den. Verdien av enkeltbiter av åpen informasjon trenger ikke isolert sett å være stor* [13].

Sikkerhetshendelse
En sikkerhetshendelse er en aktivitet eller situasjon som har forårsaket skade på eller truer personell, informasjon eller andre verdier [14].

Informasjons- og kommunikasjonsteknologi (IKT) sikkerhetshendelse
Tilsiktede uønskede hendelser eller trusler om slike hendelser i det digitale rom som er rettet mot kritisk infrastruktur og /eller kritiske samfunnsfunksjoner [13].

Trussel
Mulig uønsket handling som kan gi en negativ konsekvens [13].

Ledelse
Menneskene som har ansvar for beslutninger og resultater i virksomheter [15].

2.3 Lovverk

Flere lover setter tydelige krav til ledelsens ansvar ovenfor informasjonssikkerhet og IKT-hendelser. Leder sitt ansvar kan ikke delegeres, men leder kan delegere oppgaver i virksomheten og tilordne myndighet til å fatte beslutninger. Dette gir muligheter for at bemyndigede personer kan beslutte hemmelighold eller utlevering innenfor sitt myndighetsområde, men øverste leder har likevel det overordnede ansvaret. Hvilke lovverk som skal tas i bruk avhenger av hvilken informasjon virksomheten behandler og hvilke hendelser som inntreffer.

Sikkerhetsloven skal forebygge, avdekke og motvirke sikkerhetstruende virksomhet [16]. Sikkerhetsloven gjelder for statlige, fylkeskommunale og kommunale foretak, i tillegg til leverandører, som behandler sikkerhetsgradert informasjon eller råder over og behandler systemer som har kritisk betydning for grunnleggende nasjonale funksjoner [16, 17]:

§ 4-1: Sikkerhetsstyring.
Virksomhetens leder har ansvaret for det forebyggende sikkerhetsarbeidet. Dette skal være en del av virksomhetens styringssystem hvorav sikkerhetstilstanden i virksomheten skal regelmessig kontrolleres. Virksomheten skal også sørge for at ansatte, leverandører og oppdragstakere har tilstrekkelig risiko- og sikkerhetsforståelse.

§ 4-2: Vurdering av risiko.
Virksomheten skal regelmessig gjennomføre vurdering av risiko.

§ 4-3: Plikt til å gjennomføre sikkerhetstiltak og øvelser.
Virksomheten skal gjennomføre de forebyggende sikkerhetstiltakene som må til

> *for å gi et forsvarlig sikkerhetsnivå og redusere risikoen knyttet til sikkerhetstruende virksomhet*.

> § 4-4: Krav til dokumentasjon.
> *Virksomheten skal dokumentere vurderingen av risiko og de gjennomførte og planlagte sikkerhetstiltakene*.

> § 4-5: Varslingsplikt.
> *Virksomheten skal varsle sikkerhetsmyndigheten og andre tilsynsmyndigheter*.

> § 8-9: Autorisasjon.
> *Virksomhetens leder er autorisasjonsansvarlig og har ansvaret for sikkerhetsmessig ledelse og kontroll av autoriserte personer*.

Sikkerhetsloven gjelder for statlige, fylkeskommunale og kommunale foretak som behandler[18]:

> § 8-11: Varslingsplikt om forhold som kan påvirke sikkerhetsmessig skikkethet.
> *En klarert og autorisert person skal umiddelbart varsle den autorisasjonsansvarlige om forhold som kan være av betydning for om personen er sikkerhetsmessig skikket*.

> § 8-12: Utlevering av informasjon til Politiets sikkerhetstjeneste.

Sikkerhetsloven trådte i kraft 01.01.2019.

Personopplysningsloven gjelder ved behandling av personopplysninger som utføres i forbindelse med aktivitetene ved virksomheten til den behandlingsansvarlige. Loven gir generelle bestemmelser om behandling av personopplysninger.

Relevant er kapittel IV:

> Artikkel 24: Den behandlingsansvarliges ansvar [19].

> Artikkel 33: Melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten [20].

Se presiseringer og unntak:

> § 4: Geografisk virkeområde.
> *Loven og personvernforordningen gjelder for behandling av personopplysninger som utføres i forbindelse med aktivitetene ved virksomheten til en behandlingsansvarlig eller en databehandler i Norge, uavhengig av om behandlingen finner sted i EØS eller ikke* [21].

Personopplysningsloven trådte i kraft 20.07.2018.

Det er mange lover som regulerer virksomhetens ansvar ved behandling av informasjon om fysiske personer. Felles er at det er øverste leder som er ansvarlig for at lovens krav etterleves. Lovene beskriver virksomhetenes ansvar for å vurdere risiko, gjennomføre forebyggende tiltak og internkontroll og varsle myndigheter og berørte ved sikkerhetsbrudd og avvik.

2.4 Rammeverk

NIST Guide to Cyber Threat Information Sharing [22]

Rammeverket er skrevet av National Institute of Standards and Technology (NIST) og gir retningslinjer for etablering og deltagelse i relasjoner for deling av trusler og annen informasjon relatert til IKT-sikkerhet. Den beskriver fordeler og utfordringer med deling, viktigheten av tillit, og spesifikke datahåndteringshensyn.

Det er mange fordeler knyttet til deling av informasjon og etablering av relasjoner for deling, men det er også noen utfordringer. Kollektiv økning av kunnskap og ferdigheter er en fordel, da deling av informasjon i et nettverk lar hver organisasjon lære mer om trusler og sikkerhet. En annen fordel er at virksomhetene lærer mer om sikkerhetsmiljøet og trusselbildet, som kan gjøre de mer forberedt på å håndtere hendelser. Samlingen av små biter informasjon i nettverket kan avsløre mønstre og gi dypere forståelse for angrepsmetoder, som også kan hjelpe virksomhetene med å respondere raskere på hendelser. Jo mer virksomhetene lærer om angrepsmetoden og trusselaktører, jo bedre forberedt blir de på angrep. Deling gir derfor virksomheter mulighet til et mer fleksibelt forsvar som er forberedt på mange forskjellige situasjoner.

En stor utfordring med deling er at det krever mye arbeid å etablere tillit mellom partene. Det krever også mye ressurser å sette opp automatiserte systemer for mottakelse og behandling av delt informasjon, som er nødvendig for å fullt kunne utnytte all informasjonen som deles. Det er også sterkt anbefalt at virksomheter etablerer retningslinjer, rutiner og kontrollmekanismer for deling for å unngå at sensitiv informasjon havner på avveie, da dette kan gi store konsekvenser for virksomheten både økonomisk og i forhold til omdømme. Ønsker virksomheten tilgang til klassifisert informasjon krever det ressurser å opprettholde klarering for kontinuerlig tilgang til informasjonen. I tillegg krever faste delingsavtaler visse verktøy og infrastruktur for å prosessere store mengder data, som kan være vanskelig for virksomheter med mindre infrastruktur som overveldes av så store datamengder.

En del av arbeidet med å etablere relasjoner er å fastsette målsettinger. Disse beskriver ønsket utfall ved deling i forhold til virksomhetens forretningsprosesser og sikkerhetspolicyer. Målsettingene brukes i det videre arbeidet med å bestemme omfanget av virksomhetens innsats i delingsarbeid, utvelgelse av nettverk for deling, og for å gi støtte til aktiviteter knyttet til deling.

Før virksomheten går i gang med å dele informasjon bør det settes opp et regelverk for deling. Dette skal være med på å kontrollere spredningen av informasjonen og hindre formidling av sensitiv informasjon som kan gi store konsekvenser om det havner på avveie. Reglene bør beskrive hvem det kan deles med og under hvilke omstendigheter, krav for tilbaketrekning og sensurering av informasjon, og om sitering er lov. Det anbefales også å utrede og dele ut retningslinjer for mottakere av informasjon som beskriver hvordan informasjonen skal håndteres.

Microsoft framework for information sharing [23]

"A framework for cybersecurity information sharing and risk reduction" er et rammeverk fra Microsoft for deling av IT-sikkerhetsinformasjon og reduksjon av risiko. Som en del av arbeidet knyttet til et økende fokus på deling, opprettet Microsoft et program for å gi virksomheter tidlig tilgang til sårbarhetsinformasjon. Gjennom dette arbeidet oppdaget de at kontinuerlig deling krever arbeid og klare definisjoner og mål. Rammeverket ble utviklet for å belyse problemstillingen og hjelpe virksomheter med delingsprosessen. [24]

Det finnes mange typer IT-sikkerhetsinformasjon som kan deles. Microsoft har delt disse inn i hendelser, trusler, sårbarheter, tiltak, situasjonsdata, beste praksis, og strategiske analyser. Informasjon om hendelser beskriver forsøkte og vellykkede angrep, som hva slags data som er tapt, teknikker som er brukt, og mål og konsekvens for angrepet. Trusler beskriver mulige uønskede handlinger som kan gi negative konsekvenser. Sårbarheter er svakheter i programvare, hardware og business prosesser som kan utnyttes, og tiltak er metoder for å begrense disse og/eller hindre trusler. Situasjonsdata beskriver nylige hendelser og trusler, og gir virksomheter et bedre grunnlag for å respondere på hendelser. Beste praksis er informasjon om gunstige gjøremåter og metoder, og strategiske analyser beskriver trender og forventet utfall virksomheter analyserer for å forberede seg på fremtidige risikoer. De ulike typene informasjon har ulike bruksområder, men alle bidrar til økt kunnskap om sikkerhet for virksomheter.

Figur 2.1 viser hvordan de ulike typene informasjon henger sammen. Beste praksis danner grunnlaget for informasjon. Videre kommer trusler, sårbarheter, hendelser og tiltak, som sammen danner et godt grunnlag for utformingen av situasjonsdata. På toppen kommer strategisk analyse, som ofte er basert på varierende perspektiver fra hendelser og annen IT-sikkerhetsinformasjon. [23]

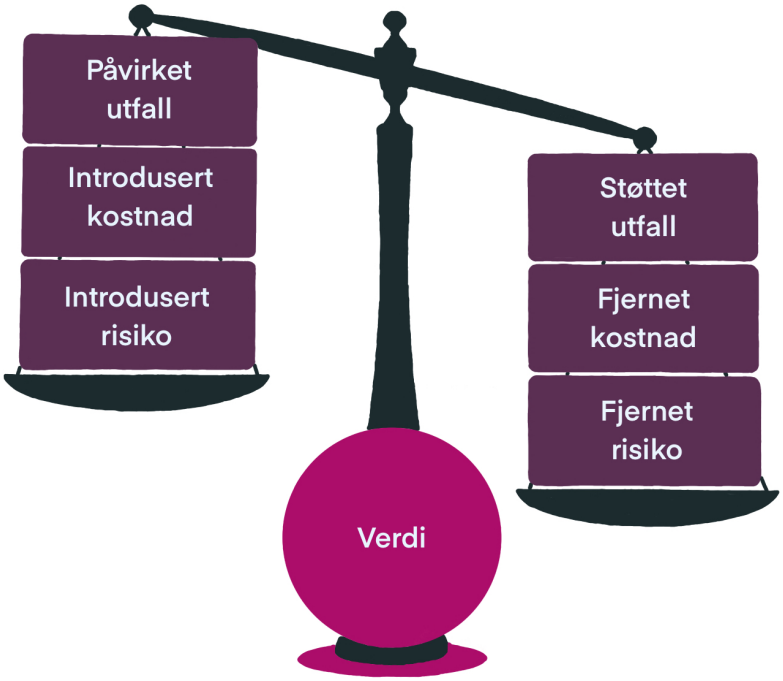
Figur 2.1: Microsoft pyramide over informasjonsstyper [23]

Virksomheter har flere valg når det kommer til metode for deling av IT sikkerhetsinformasjon. De mest brukte metodene er formell utveksling, sikkerhetsklareringsbasert, tillitsbasert og episodisk deling. Formell utveksling skjer ofte gjennom en avtale og kombineres gjerne med en kontrakt, som en Non-Disclosure Agreement (NDA), eller gjennom et medlemskap slik som Microsoft Active Protections Program (MAPP) og Computer Emergency Response Team (CERT). Sikkerhetsklareringsbasert deling er en mer målrettet type formell utveksling som brukes mye mellom etterretningstjenester. Tillitsbasert deling skjer i grupper med likesinnede, ofte under og etter en sikkerhetshendelse. Traffic Light Protocol (TLP) brukes mye til denne metoden for deling der man ikke alltid har klart definerte regler for deling med de andre virksomhetene. TLP er et system for klassifisering av informasjon, hvor informasjonen får tildelt fargen rød, rav, grønn eller hvit, som avgjør hva mottakeren av informasjonen får lov til å gjøre med den og om de får lov å dele den videre [25]. Episodisk deling vil si at virksomhetene deler når noe skjer, som under og etter en hendelse, og de deler ofte fordi de trenger hjelp eller ønsker å advare andre virksomheter om en ny trussel.

ITIL rammeverk

Information Technology Infrastructure Library (ITIL) er et rammeverk for levering av effektive IT/digitale løsninger. Det er utviklet med målet om å hjelpe virksomheter oppnå verdi. ITIL hjelper virksomheter med å innføre tjenesteleveransesystemer og et felles språk for å nå kundenes behov. [26]

For å oppnå verdi må risikoen og kostnadene være lavere enn det positive utkomme som er resultat av handlingen. Figur 2.2 illustrerer forholdet mellom utkomme, risiko, kostnad og verdi. Kostnadene og risikoene som blir introdusert med handlingen, for eksempel å dele informasjon, må veie mindre enn kostnadene og risikoen som trekkes fra virksomheten når de har etablert en delingsrelasjon. Det må også være færre utkomme som blir påvirket enn det man får ut av relasjonen. Alle tre trenger ikke være mindre, men den totale vekten av kostnad, risiko og påvirket resultat må være lavere enn de positive sidene for å skape verdi. [27]



Figur 2.2: Vekt for måling av oppnådd verdi [27]

2.5 Artikler og rapporter

Mørketallsundersøkelsen

Næringslivets Sikkerhetsråd kom i 2020 ut med den 12. mørsketallsundersøkelsen. Undesøkelsen brukes til å kartlegge IT-bransjen og undersøke omfanget av datakriminalitet, sikkerhetshendelser og sikkerhetsbevissthet hos norske virksomheter. Mørketallsundersøkelsen gjennomføres annenhvert år, og i undersøkelsen fra 2020 var det 1601 virksomheter som deltok. [4, 28]

Mørketallsundersøkelsen har fokus på å synliggjøre hva som gjøres og hvordan virksomheter oppfatter sikkerhetshendelser. I 2020 ble det blant annet avdekket at årsaken til at sikkerhetshendelser ble oppdaget var tilfeldigheter i halvparten av tilfellene, og rutiner i de resterende tilfellende. For virksomhetene som var utsatt for en sikkerhetshendelse er det 69% som involverer ledelsen og 38% som rapporterer hendelsen inn til styret. Undersøkelsen viser også at kun 41% av virksomhetene drifter IT internt. Disse tallene gir en indikasjon på hva som kan forventes av svar fra intervjuobjektene, og gir føring på oppgavens hypotese [4].

Risiko 2020 Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet har utgitt sin årlige risikorapport, Risiko 2020. Rapporten tar for seg blant annet sårbarheter i et digitalt samfunn hvorav åpenhetens dilemma blir diskutert. NSM beskriver videre hvordan åpen informasjon kan misbrukes til blant annet å planlegge uønsket aktivitet og kriminalitet mot enkeltpersoner og virksomheter. Åpen informasjon er informasjon som ved lovlig fremgangsmåte er tilgjengelig for alle som ønsker å finne den. Mengden åpen informasjon og muligheten til å sammenstille informasjon digitalt innebærer en betydelig risiko for at trusselaktører får innsikt i forhold som er ønsket at skjermes eller burde skjermes. [12]

Teknisk Ukeblad Maritim

Artikkelen "Holder dataangrep hemmelig: – Skip er blitt smittet med virus, og har måttet slepes til dokk" beskriver et problem i maritim sektor der flere blir utsatt for hackerangrep. Når hackerne først får tilgang til et system er det lett å få tilgang til flere systemer. Elisabet Haugsbø i DNV GL beskriver to årsaker til store mørketall innen cybersikkerhet; at virksomheter ikke er klar over at de har blitt utsatt for dataangrep, og at de er redde for å dele informasjon om angrep av frykt for tap av omdømme og økt eksponering. [5]

2.6 Teori innhentet under intervju

Noen av spørsmålene i intervjuguiden dekker regelverk og forskrifter virksomhetene er underlagt som kan påvirke deres valg om åpenhet. Enkelte regelverk er spesielle for enkelte sektorer, som for eksempel beredskapsforskriften til Norges vassdrag- og energidirektorat (NVE) for kraftsektoren. Her beskrives regelverk, forskrifter, standarder og rammeverk som ulike virksomheter er underlagt og benytter seg av, men som ikke er en del av intervjuguiden. Disse ble samlet inn gjennom svarene på ulike intervjuspørsmål.

2.6.1 Lovverk

Kraftberedskapsforskriften gjelder forebygging, håndtering og begrensning av virkningene av ekstraordinære situasjoner som kan skade eller hindre produksjon, omforming, overføring, omsetning og fordeling av elektrisk energi eller fjernvarme [29]. Kraftberedskapsforskriften gjelder for kraftforsyningens beredskapsorganisasjonsenheter (KBO-enhet).

Kraftberedskapsforskriften trådte i kraft 01.01.2013.

Offentleglova inneholder bestemmelser om retten til å få se (innsyn) i dokumenter i offentlig forvaltning. Hovedregelen er at alle kan kreve innsyn i saksdokumenter, journaler og andre lignende registre. Loven inneholder også bestemmelser om hva som regnes som dokument og når et dokument blir offentlig [30]. Offentlighetsloven gjelder i utgangspunktet for «den virksomhet som drives av forvaltningsorganer», jf § 1 [31].

Offentlighetsloven trådte i kraft 01.01.2009.

Arkivloven gir overordnede og grunnleggende regler om arkiv, særlig om arkiv i offentlig forvaltning. Bestemmelsene i arkivloven skal sikre en helhetlig samfunnsdokumentasjon. Formålet er å ta vare på arkiv som inneholder rettighetsdokumentasjon eller har verdi for forskning, kultur og forvaltning. Virkeområdet for arkivloven er alle offentlige organer unntatt Stortinget og dets organer (§ 5) [32].

Arkivloven trådte i kraft 01.01.1999.

Anskaffelsesloven inneholder flere bestemmelser som pålegger offentlige innkjøpere å ta hensyn til miljø, arbeidsforhold og sosiale forhold ved gjennomføringen av sine anskaffelser. Plikten gjelder statlige, fylkes-kommunale og kommunale myndigheter og offentligrettslige organer [33].

Anskaffelsesloven trådte i kraft 01.01.2017.

Der det som anskaffes er knyttet til utøvelsen av en forsyningsaktivitet, det vil si aktiviteter som har til formål å utøve forsyning som nærmere angitt i §§ 1-3 til 1-9, vil anskaffelsen være underlagt forsyningsforskriften. Forskriften gjelder for statlige, fylkeskommunale og kommunale myndigheter, offentligrettslige organer og sammenslutninger med en eller flere slike oppdragsgivere. I tillegg gjelder forsyningsforskriften for offentlige foretak og andre virksomheter som utøver forsyningsaktivitet på grunnlag av enerett eller særrett [34].

Forsyningsforskriften trådte i kraft 01.01.2017.

2.6.2 Standarder og rammeverk

International Organization for Standardization 27001

International Organization for Standardization (ISO) er en internasjonal standardiseringsorganisasjon som har utviklet standarder for forskjellige sektorer. ISO 27001 er en internasjonal standard som er utarbeidet for å stille krav til etablering, implementering, vedlikehold og kontinuerlig forbedring av et ledelsessystem for informasjonssikkerhet. Det er mange fordeler ved å benytte seg av ISO 27001. Først og fremst kan et ledelsessystem for informasjonssikkerhet bevare konfidensialitet, integritet og tilgjengelighet til informasjon ved å benytte en risikostyringsprosess. Videre kan bruken av rammeverket gi tillit hos interessenter gjennom tilstrekkelig håndtering av risikoer. [35]

Grunnprinsipper for IKT-sikkerhet

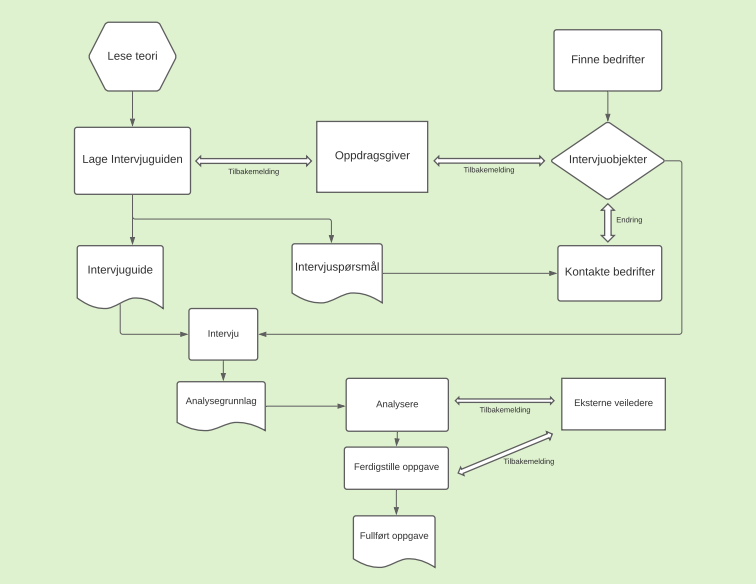
NSMs grunnprinsipper for IKT-sikkerhet definerer et sett med prinsipper og underliggende tiltak for å beskytte informasjonssystemer (maskinvare, programvare og tilknyttet infrastruktur), data og tjenestene de tilbyr mot uautorisert tilgang, skade eller misbruk. Fordelen ved å benytte seg av NSMs grunnprinsipper for IKT-sikkerhet er at bruken skal bidra til å heve sikkerhetskompetanse og sikkerhetsnivået i norske virksomheter. Disse er relevante for alle norske virksomheter, både i offentlig og privat sektor. [36]

Kapittel 3

Metode

3.1 Introduksjon

Metoden er en beskrivelse av hva som er gjort og alle valg som er tatt i løpet av oppgaven. Det første metodevalget omhandler kvalitativ eller kvantitativ analyse. Videre beskrives valgene tatt rundt oppbygningen av intervjuguiden, før utvelgelsen og rekrutteringen av intervjuobjekter beskrives. Til slutt omtales gjennomføringen av intervjuene og deretter analysen. Figur 3.1 viser stegene som er tatt i denne prosessen. Flytdiagrammet følger definerte byggestandarder, med unntak av at prosesser er rektangler med runde hjørner, og eksterne bidragsytere representeres gjennom rektangler med rette hjørner [37].



Figur 3.1: Aktiviteter i metode

3.2 Datainnsamlingsmetode

For å avgjøre metoden for datainnsamling må man se på forskningsspørsmålene definert under problemstillingen 1.3. Disse spørsmålene ser på årsaker og rutiner, og åpner opp for bruk av både tallfestet data samtidig som man går i dybden på et smalt fagfelt. Det er altså nødvendig å tallfeste deler av dataen, men store deler av datainnsamlingen krever mer detaljerte svar.

Kvantitativ metode baserer seg på å samle inn og tallfeste data, og kan derfor passe til deler av oppgaven. Likevel passer ikke kvantitativ metode for å samle inn alt av dataen som er nødvendig, og innsamlingen kan ikke alene gjennomføres med denne metoden. Kvalitativ metode går ut på å få dyp kunnskap på et smalere felt, og gjennomføres ofte ved intervjuer eller observasjoner. Siden forskningspørsmålene dekker et smalt fagområde i dybden, passer denne metoden bedre. Slik kan detaljerte svar samles inn, samtidig som man også kan hente inn data som kan tallfestes i intervjuene. Intervju er en undersøkelsesmetode som passer bra til oppgavens formål, og er derfor den valgte metoden. [38]

3.3 Intervjuguide

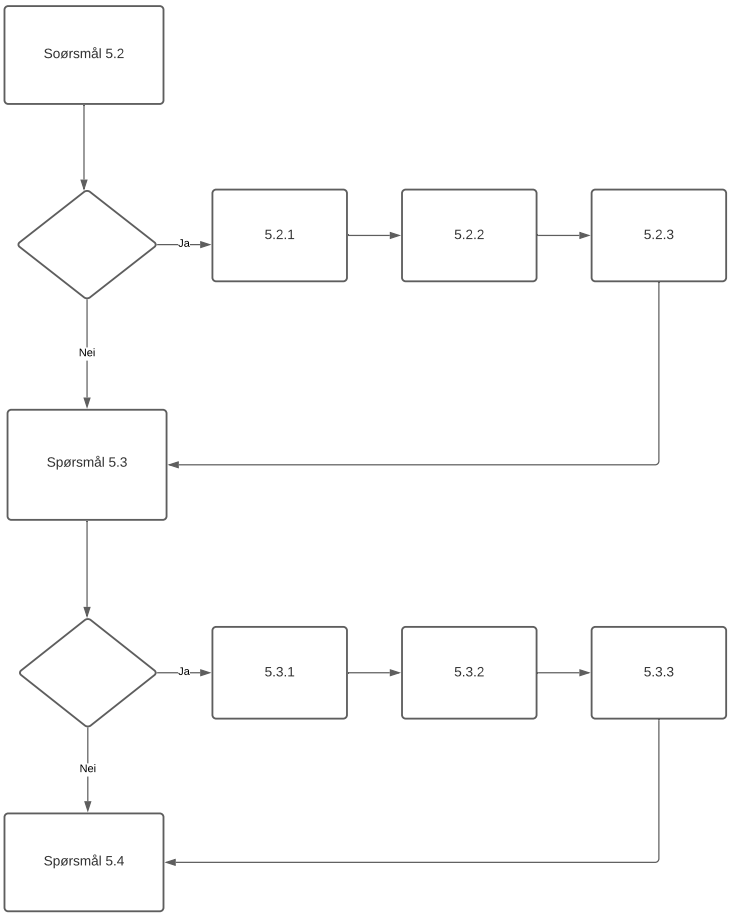
Intervjuguiden er en sentral del av oppgaven, og danner grunnlaget for intervjuene, og senere analysen, som skal gjennomføres. Hvert spørsmål er knyttet til teori og hensikt. Teorien er med for å gi analysen et faglig grunnlag, og gjøre konklusjoner mer reelle. Hensikten gir retningslinjer for analysen og beskriver sammenligningspunkter det er viktig å legge vekt på i analysen.

Lesing av teori er en viktig og lang prosess. Et bredt søk knyttet til hendelser i media, rammeverk og regelverk ble gjennomført. Det finnes mye teori knyttet til hendelseshåndtering og IT-sikkerhet generelt, men veldig lite på deling av IT-sikkerhetsinformasjon spesifikt. Teorien ble valgt utifra relevans og pålitelighet. Alle mulige spørsmål ble notert ned og koblet til teori, og deretter kategorisert. Hensikten med hvert spørsmål ble definert, og en del spørsmål ble eliminert på grunn av manglende hensikt.

Intervjuguiden er delt opp i fem kategorier. Først kommer spørsmålene om strategiske valg og kommunikasjonsstrategier hos virksomhetene. Deretter kommer spørsmål om regelverk, og videre følger spørsmål om rutiner og prosesser hos virksomhetene. Deretter er det spørsmål om virksomhetenes ressurser og kompetanse, før det avsluttes med spørsmål om erfaringer og evalueringer.

Intervjuguiden er delvis bygget opp som en slags trestruktur. Det finnes en stamme med spørsmål som alle virksomheter vil bli stilt, men også grener med spørsmål som bare stilles hvis de har svart ja eller nei på visse spørsmål. Figur 3.2 viser

forgreningen for to av spørsmålene. Dette er gjort for å hindre at virksomheter blir stilt spørsmål som ikke er relevante til deres situasjon og opplevelser.



Figur 3.2: Struktur på forgrening av spørsmål

Det er to definisjonsspørsmål som stilles for å sikre enighet om hva en sikkerhetshendelse er og hva åpen informasjon er. Disse skal i utgangspunktet hentes fra NSM, men siden deres definisjon på en IKT-sikkerhetshendelse relaterer til kritisk infrastruktur, og det ikke er relevant for alle virksomheter, ble en annen definisjon benyttet. Begge definisjonene er beskrevet i kapittel 2. I ettertid har NSM endret definisjonen på en IKT-sikkerhetshendelse [13].

Styrkene ved oppbygningen av intervjuguiden ligger i teorien og hensikten. Som

tidligere beskrevet lager disse grunnlaget for en mer troverdig konklusjon og en analyse med flere klart definerte sammenligningspunkter. I tillegg er hensikten en hjelp til å luke ut mindre relevante spørsmål slik at man bare sitter igjen med det mest nødvendige. Ulempene med en slik oppbygning er at relevante spørsmål kan bli kuttet fordi man ikke finner relevant teori. Teorien er heller ikke alltid relevant for alle virksomhetene, spesielt lovverk som ikke gjelder alle.

3.4 Intervjuobjekter

Valget av intervjuobjekter har stor betydning for resultatet av oppgaven fordi ulike virksomheter har ulike rutiner og strategier. Det må avgjøres om alle intervjuobjektene skal tilhøre samme sektor, eller om det skal plukkes ut et gitt antall virksomheter fra flere forskjellige sektoter.

Fordelen med å kun intervjue en sektor er at virksomhetene har kunnskap og erfaring innen samme fagområde, og er ofte underlagt det samme regelverket. Den negative siden er at det blir en mindre representativ undersøkelse, og eventuelle konklusjoner vil ikke nødvendigvis gjelde for andre sektorer. Fordelen med å intervjue virksomheter fra forskjellige sektorer er at man får et mer representativt utvalg av norske virksomheter, og man får sett eventuelle forskjeller på tvers av sektorene. Ulempen er at det kan bli vanskeligere å trekke eventuelle konklusjoner om de ulike sektorene. Siden det er færre virksomheter per sektor blir grunnlaget for analysen mindre.

Valget av intervjuobjekter falt på flere sektorer for å gjøre oppgaven mer relevant for flere virksomheter. For å motvirke de negative sidene ved dette ble det satt en begrensning på fire sektorer. For hver sektor skal det helst hentes inn minst fem virksomheter, slik at man får et analysegrunnlag. Sektorene som vurderes er hentet fra Norsk Industri og regjeringen sine nettsider [39, 40].

Valg av sektor har en betydning fordi ulike spørsmål kan slå ulikt ut i de forskjellige sektorene. Finans- og helsesektor ble fort valgt bort grunnet tvungen åpenhet gjennom strenge lovverk. Hensikten med analysen er å identifisere faktorer for frivillig deling, og en stor mengde virksomheter som ikke har et valg knyttet til deling er derfor mindre ønskelig. De foreslåtte sektorene ble derfor kommuner, offentlig eid, telekom, kraft/energi, maritim og konsulent. Telekom ble kuttet da eventuelle dataangrep hos virksomheter i sektoren antas å være meget synlige for kunder, som gjør valget om åpenhet mindre frivillig. Konsulentbedrifter ble kuttet fordi det antas at disse ofte er mer modne innen sikkerhet og derfor er mindre representative for norske virksomheter. I tillegg må flere av virksomhetene ta hensyn til deres kunder sine ønsker om deling, så vel som virksomheten sine egne.

Virksomhetene ble plukket ut basert på spesifikke kvalifikasjoner. Sider som Norsk

Industri, Norges vassdrag- og energidirektorat (NVE) og Regjeringen.no ble søkt for å finne lister over virksomheter i de ulike sektorene, i tillegg til de virksomhetene gruppen hadde kjenneskap til [39–41]. Definisjon for størrelsen på virksomheter er hentet fra Næringslivets Hovedorganisasjon (NHO), der små virksomheter har 1-20 ansatte, mellomstore virksomheter har 21-100 ansatte og store virksomheter har over 100 [42]. Enkelte offentlige virksomheter ble kuttet fordi de er så store at det i flere tilfeller ikke er felles rutiner for hele virksomheten, men heller individuell gjennomførelse i ulike seksjoner. I utvelgelsen ble det også gjort et søk etter virksomheter som hadde gått ut i media med sikkerhetshendelser for å sikre at data om valg rundt deling av media ble samlet inn under intervjuene.

3.5 Rekruttering

De utvalgte virksomhetene, cirka 40 i første omgang, fikk alle tilsendt en mail med informasjon og invitasjon til intervju. Intervjuobjektene som svarte positivt ble sendt intervjuspørsmålene og et databehandlingsskjema. I dokumentet med intervjuspørsmålene virksomhetene fikk tilsendt, var hensikten fjernet helt, samt deler av teorien. Dette ble fjernet fordi virksomhetene ikke trenger å vite hensikten for å kunne svare på spørsmålene, og fordi mye av teorien heller ikke er nødvendig for å forstå og kunne svare på spørsmålet. Det er heller ikke heldig å presentere virksomheter med lovverk de er underlagt, men kanskje ikke følger, da dette kan gjøre at de er tilbakeholdende i besvarelsen sin.

Databehandlingsskjemaet er et dokument som beskriver hva informasjonen fra intervjuene skal brukes til, og hvordan det skal behandles. Dokumentet signeres av begge parter, og skal gi virksomhetene en forsikring på at dataen kun brukes til det den er ment for. Intervjuobjektene skal også krysse av for om de ønsker anonymitet eller ikke, og undertegnede plikter til å ikke bryte med dette ønsket. Dokumentet er lagt som vedlegg C.

De utvalgte virksomhetene ble kontaktet i uke 7, rett før deler av landet hadde vinterferie. Fordi vinterferien var fordelt på uke 8 og 9 var det likevel flere virksomheter som svarte raskt. Oppfølgingsmail ble sendt ut hvis virksomhetene ikke svarte innen to uker. I maritim sektor var det kun en bedrift som svarte, og manglende muligheter for å kontakte spesifikke personer gjorde at denne sektoren ble erstattet med transportsektoren. Da disse ble kontaktet ganske sent i prosessen, ble det gjennomført intervju med kun tre virksomheter i sektoren.

Det var varierende svar i de andre sektorene også, og det ble vanskelig å nå fem intervjuobjekter for alle sektorene. Det var kun i kraft- og kommunesektoren dette ble nådd, og dette kan ha sammenheng med at gruppen hadde kontaktinformasjon til IT ansatte i flere av virksomhetene, i tillegg til at kontaktinformasjonen til kommunedirektører var lett tilgjengelig på Internett. Det var en tydelig fordel å

kontakte personer direkte for å delta i undersøkelsen.

3.6 Gjennomføring av intervju

I forkant av første intervju gjennomførte gruppen et 'testintervju' på hverandre for øve på gjennomføring og oppdage eventuelle feil/mangler. Det ble ikke gjennomført et testintervju med en bedrift da det var for få intervjuobjekter til at et sett med svar kunne legges vekk. Rettelser på spørsmålene ble heller gjennomført underveis, og bruken av intervju gjorde det mulig å sikre at intervjuobjektet svarte på riktig spørsmål.

Det ble satt av 1 time og 30 minutter til hvert intervju, men flere ble kortet ned til en time da dette passet bedre for flere av intervjuobjektene. De aller fleste intervjuene ble fullført innen en time. Det ene intervjuet måtte gjennomføres på 25 minutter, og noen av de mer repetitive spørsmålene, i tillegg til de der man kunne finne svaret på nett, ble kuttet for å holde tidsfristen. Enkelte av intervjuspørsmålene ligner mye, og det legges her vekt på nyansen mellom de. I tilfeller der virksomheten gjennom tidligere spørsmål har svart på andre spørsmål, forsøker intervjueren å stille disse mer bekreftene, slik at man er helt sikre på å ha forstått intervjuobjektet.

I tidsplanen for oppgaven var det satt av litt over en og en halv måned. Dette ble kuttet ned med en uke for å få bedre tid til å gjennomføre analysen. På grunn av påskeferien ble det fem uker å gjennomføre intervjuene på, og det måtte derfor gjennomføres fire intervjuer i uken for å nå ønsket antall intervjuobjekter. Intervjuene fordelte seg mer ujevnt, med opptil fem intervjuer noen uker, og ned til ett intervju andre uker. Totalt ble det gjennomført 19 intervjuer.

3.7 Gjennomføring av analyse

Koding av innsamlet data kan gjennomføres på flere måter. Første alternativ er å manuelt kode svarene i Microsoft Excel ved å trekke ut essensen av hvert svar og føre dette inn i et skjema. En ulempe ved dette er at det tar lang tid, og ekstra kommentarer til spørsmålene blir ikke med. Det andre alternativet er å bruke et verktøy for analyse av kvalitative undersøkelser. I denne oppgaven ble NVivo benyttet [43]. Fordelen er at man kan gjennomføre søk i dataene, for eksempel etter hva kommunene svarte på et gitt sprøsmål. Fordelen med verktøyet er at det gjør analyseringen og kodingen av datagrunnlaget enklere. Samtidig krever det tid å sette seg inn i bruk og muligheter. Det er også viktig å sjekke om verktøyet sin databehandling og personvernerklæring er i tråd med satte krav for den innsamlede dataen.

NVivo ble valgt fordi gruppen anså dette som best for å få frem detaljer og nyanser i analysen. NVivo ble valgt over andre lignende verktøy fordi NTNU tilbyr en lisens til programmet for sine studenter. Programmet tilfredstiller også satte krav for behandling av data [44, 45]. Funksjonalitetene ble benyttet etter beste evne basert på informasjon hentet inn fra programmet sine hjemmesider og tilgjengelige videoer.

NVivo er en litt mer komplisert programvare, som krever at man setter seg inn i det, men den gir til gjengjeld mange muligheter. Referat fra hvert intervju ble lastet opp som en egen fil. Det ble laget en kode per spørsmål, og hvert svar ble koblet til den korresponderende koden. Deretter ble det laget en klasse av hver fil, og disse ble klassifisert som intervjuobjekter. For hvert intervjuobjekt ble det satt to attributter, sektor og størrelse. 'Matrix Coding Query' ble benyttet for å søke etter svar. Der kan man sette hvilken verdi en gitt attributt skal ha, og hvilke kode(r) man ønsker å søke etter. Dermed kan man for eksempel gjennomføre et søk på hva virksomhetene i kraftsektoren svarte på spørsmålet om øvelser på sikkerhetshendelser.

Grafer brukes i oppgaven for å illustrere enkelte svar på en mer oversiktlig måte enn med tekst, og for å vise både helhetsbilder og forskjeller mellom sektorene. Microsoft Excel benyttes da dette er et program gruppen har erfaring med og som har verktøy for å produsere grafer. For å lage en figur som viser hvor mange virksomheter i hver sektor som har hatt en hendelse, ble det laget en tabell med sektorene beskrevet i kolonnene, og svaralternativene på hver sin rad. Tabellen ble markert, og Microsoft Excel sin diagramfunksjon ble benyttet. Dataetiketter ble deretter lagt til på figurene. Figur 3.3 viser hvordan tabellen kan se ut.

	A	B	C	D	E	F
1						
2						
3	Svar alternativer	Kraft	Offentlig	Kommune	Transport	
4	Ja	5	3	4	3	
5	Nei	2	1	1	0	
6						
7						
8						

Figur 3.3: Eksempel fra Microsoft Excel

Kapittel 4

Intervjuguide

4.1 Introduksjon

Datainnsamling er den delen med anvendbar data som er blitt benyttet for å kunne analysere data og deretter gjøre det mulig å evaluere utfall. I denne prosessen har det vært fokus på å samle inn relevante data og målrettede variabler. Datainnsamlingen har foregått gjennom intervju via Teams.

4.2 Intervjuguide

Intervjuguiden i sin helhet ligger i vedlegg B. Den består av fem kategorier hvor hver kategori tar for seg ulike felt for å danne et helhetlig bilde av hver enkelt bedrift. Spørsmålene er sentrert rundt rutiner og rammeverk, erfaringer og virksomheten sine holdninger rundt deling av sikkerhetshendelser. Spørsmålene dekker et ganske lite faglig område, men er til gjengjeld meget detaljert på de ovennevnte punktene.

Kategori 1: Strategiske valg og kommunikasjonsstrategi

Kategorien strategiske valg og kommunikasjonsstrategi handler om hva virksomheter gjør på forhånd av sikkerhetshendelser. Det legges vekt på rutiner og rammeverk og hva virksomheten skal gjøre i ulike situasjoner, samt hva de er villige til å gjøre. I tillegg går spørsmålene inn på hvor mye virksomheten samarbeider med andre, både i og utenfor sektoren sin. I denne kategorien er det også spørsmål med rammeverk som teorigrunnlag, for å kartlegge bruken av rammeverk og en mulig effekt av dette. Disse rammeverkene er beskrevet i kapittel 2. Det første spørsmålet i kategorien er et definisjonsspørsmål relatert til hva en IKT-sikkerhetshendelse er, som stilles på dette tidspunktet for å ha oversikt over hvilken definisjon virksomheten benytter senere til spørsmålene som dekker deling av sikkerhetshendelser.

Hensikten med spørsmålene i denne kategorien går mye ut på å analysere hvordan ulike ting som er på plass før en hendelse oppstår, er med på å påvirke valget om å dele, som konkurranse, regler, hvem som skal dele og bruk av rammeverk. I tillegg analyseres det om virksomheter er mer villige til å dele enkelte typer informasjon over andre. I kategorien stilles det derfor spørsmål om virksomheten samarbeider om sikkerhet med andre i samme sektor, om virksomheten har et rammeverk for håndtering og rapportering av hendelser, og hvilke typer informasjon virksomhetene er villige til å dele med NSM.

Kategori 2: Regelverk

Regelverk er en kategori som undersøker hvilke lover og regler som påvirker virksomheter sitt valg om åpenhet. Kategorien har også et definisjonspørsmål for åpen informasjon, som er definert og beskrevet i kapittel 2 under 2.2. Hensikten med spørsmålene i regelverk kategorien er å skille mellom frivillig og ufrivillig deling, for å identifisere situasjonene der tvungen deling er årsaken til at virksomheter deler.

Spørsmålene som stilles i denne kategorien er hvilke lovverk hindrer virksomheten i å dele sikkerhetshendelser, og hvilke lovverk forplikter virksomheten til å rapportere om sikkerhetshendelser. Teorien som brukes til spørsmålene er lovverk, hvor sikkerhetsloven og personopplysningsloven var beskrevet på forhånd. Hvilke lovverk som påvirker vil variere en del mellom virksomheter og sektorer, men personopplysningsloven gjelder alle. Relevante lovverk er beskrevet i teorikapittelet under 2.3.

Kategori 3: Rutiner og prosesser

Kategorien for rutiner og prosesser dekker hvilke etablerte rutiner som eksisterer hos den enkelte virksomheten, og om disse faktisk følges. Dette er rutiner knyttet til deling, håndtering og øvelser. Teorien koblet til spørsmålene er igjen lovverk, da spesielt sikkerhetsloven har en del krav knyttet til rutiner. Ikke alle virksomheter er dekket av sikkerhetsloven, så dette er mer ment som et eksempel. Gjennom spørsmålene vil andre lovverk som påvirker innføringen av rutiner avdekkes. Spørsmålene skal også avdekke om rutiner og prosesser blant virksomhetene har innvirkning på håndtering av sikkerhetshendelser og rapportering av disse.

Hensikten med de ulike spørsmålene varierer. Spørsmålene knyttet til øvelser ser på modenhet og om dette øker sannsynligheten for at virksomhetene deler hendelser. Spørsmålene om hvem som skal ta valget om å dele en sikkerhetshendelse, og hvem som skal håndtere en hendelse, har til hensikt å avklare om det er enklere for virksomheter å dele hvis disse håndteringsrutinene er på plass før en hendelse

inntreffer. Spørsmålene om rutinene faktisk følges stilles for å passe på at analysen har grunnlag i hva som faktisk skjer i virksomheten, ikke bare det som skal gjøres.

Kategori 4: Ressurser og kompetanse

Spørsmålene knyttet til ressurser og kompetanse skal gi innsyn til hver enkelt bedrift sin faglige kompetanse og posisjon. Teorien til disse spørsmålene dekker enten lovverk som krever enkelte typer kompetanse, og mørketallsundersøkelsen som har påstander knyttet til tjenesteutsetting av IT-avdelingen og samarbeid med CERTer.

Hensikten med spørsmålene er å se på sammenligningspunkter i forhold til modenhet, og for å se om økt ressurser innen IT fører til mer deling. Det blir forespurt om virksomhetene har egen IT-avdeling, eget personell med kompetanse innen sikkerhet og hendelseshåndtering, og om virksomhetene er medlem av en type CERT, CSIRT eller lignende.

Kategori 5: Erfaringer og evalueringer

Siste kategori tar for seg hvilke erfaringer og evalueringer virksomhetene har opplevd og gjennomført. Dette er kategorien med flest spørsmål, men ikke alle virksomhetene vil bli stilt alle spørsmålene. Virksomheter som ikke har hatt en stor eller mellomstor sikkerhetshendelse blir ikke stilt noen av spørsmålene i denne kategorien. Teorien knyttet til spørsmålene omfatter rammeverk som beskriver potensielle positive og negative konsekvenser ved å dele, i tillegg til NSM sin oppfatning til deling, og mørketallsundersøkelsen. Fordelene og ulempene med deling er beskrevet under NIST rammeverket i kapittel 2.

Hensikten med spørsmålene er å identifisere hvilke virksomheter som har delt med hvem, hvorfor og eventuelle positive eller negative konsekvenser de har opplevd som kan påvirke videre deling av sikkerhetshendelser. Virksomhetene blir spurt om de har delt med NSM og andre beredskapsorganisasjoner, media eller ingen. For alle positive svar følges det opp med spørsmål om hvorfor de delte, mulige konsekvenser, og om disse konsekvensene har påvirket videre deling. Det siste spørsmålet dekker årsaker til sikkerhetshendelsene virksomhetene har hatt.

Kapittel 5

Analyse

5.1 Aktørene

Analysen oppsummerer hva de ulike virksomhetene har svart, både som en helhet, og en sammenligning av de ulike sektorene. Det er totalt fire sektorer som er analysert. Kraftsektoren omfatter både kraftprodusenter og nettselskaper, og det er intervjuet totalt syv virksomheter i denne sektoren. Seks av syv virksomheter har over 100 ansatte, og defineres derfor som store virksomheter av NHO [42]. Den siste virksomheten, Rakkestad Energi AS, er et lite nettselskap. Størrelsen på de store virksomhetene varierer mye, med noen som har et par hundre ansatte og andre som har flere tusen.

	Stor	**Mellomstor**	**Liten**	**Sum**
Kraft	6	0	1	7
Offentlig	2	2	0	4
Kommune	5	0	0	5
Transport	3	0	0	3
Sum	16	2	1	19

Tabell 5.1: Frekvenstabell

I den offentlige sektoren er det intervjuet fire virksomheter. To av de er store virksomheter, og de to andre er mellomstore, altså har de mellom 20-100 ansatte. Av de fire er det tre som har valgt å ikke være anonyme. Posten er den store virksomheten, og jobber med post og logistikk i Norge. Enova SF er en mellomstor bedrift som jobber med å gi økonomisk støtte til virksomheter og enkeltpersoner som ønsker å bruke eller utvikle klimavennlige teknologier for å hjelpe Norge på veien mot et lavutslippssamfunn [46]. Avfall Sør er den andre mellomstore virksomheten, og håndterer avfall i Kristiansand og Vennesla kommune [47]. I starten av 2020 ble virksomheten utsatt for et stort dataangrep [48].

Kommunesektoren er i oppgaven representert gjennom fem geografisk distribuerte kommuner. Ansatte i en kommune dekker også lærere, helsearbeidere og flere andre viktige roller i kommunene, og alle fem defineres dermed som store virksomheter. Kommunene som har valgt å ikke være anonyme er Harstad, Bodø, Kristiansund og Oslo. Harstad ligger i Troms og Finnmark, Bodø ligger i Nordland og Kristiansund ligger i Møre og Romsdal fylke.

I transportsektoren var det tre virksomheter som stilte til intervju. Alle tre virksomhetene har over 100 ansatte, og regnes derfor som store virksomheter. Likevel er det stor variasjon i antall ansatte, hvor en har rett over 100, mens de to andre har flere tusen ansatte. Alle tre virksomhetene ønsket å være anonyme i denne undersøkelsen.

5.2 Kategori 1: Strategiske valg og kommunikasjonsstrategi

5.2.1 Helhetsanalyse

Definisjonen på en sikkerhetshendelse, beskrevet i kapittel 2, er virksomhetene generelt sett enige med. Halvparten av virksomhetene har ikke en egen definisjon, men de tenker likevel at denne kan passe. Av de som har egne definisjoner nevnes det at den er lignende. En bedrift i kraftsektoren trekker frem at Supervisory Control And Data Acquisition (SCADA) systemer kunne blitt inkludert, men at definisjonen ellers er grei. En annen bedrift inkluderer situasjoner som ikke forårsaker skade i sin definisjon. To av kommunene trekker også frem konfidensialitet, integritet og tilgjengelighet.

Alle virksomhetene har et rammeverk de benytter seg av. Det er derimot noen ulikheter mellom bedriftrene i hvilket rammeverk de tar i bruk og hva det baserer seg på. ISO27001, NIST, og NSMs grunnprinsipper er de som i all hovedsak blir trukket frem og som virksomhetene bygger sine rammeverk på. Figur 5.1 viser de ulike standardene og rammeverkene som nevnes. Her er det en virksomhet som har nevnt alle fire rammeverkene, og tre andre som også har nevt ISO27001.

Figur 5.1: Spørsmål: Har bedriften/organisasjonen et rammeverk for håndtering og rapportering av sikkerhetshendelser?

Det er variasjon blant virksomhetene om hvem som påtar seg avgjørelsen om åpenhet om en sikkerhetshendelse. 13 svarer at denne avgjørelsen blir tatt i toppledelsen, der flere oppgir spesifikke roller som administrerende direktør og/eller konsernsjef. Også kriseledelsen blir nevnt som ansvarlig for åpenhet om en hendelse. Det var en bedrift som svarte at avgjørelsen om åpenhet blir gjort av personen som er nært tilknyttet hendelsen.

Ingen av intervjuobjektene har gjennomført en formell risikovurdering på å dele informasjon med andre virksomheter. Det vanligste er å enten gjøre det muntlig, eller foreta en vurdering fra case til case. Fire virksomheter har fastslått at verdien av å dele uansett vil stå over eventuelle risikoer. Regler for deling er det flere som har, først og fremst er TLP i bruk hos de ulike CERTene. Hos de offentlige virksomhetene og kommunene er det andre regler som spiller inn og som må tas hensyn til.

Over halvparten av virksomhetene har ingen nedskrevne mål for deling, men felles for nesten alle virksomhetene er deres kultur for deling. Virksomhetene har et ønske om å være til hjelp for andre, samt motta hjelp da informasjonsdeling skal være gjensidig. Virksomhetene uttrykker at deling på tvers er med på å øke kunnskapen og er en hjelpsom læring til fordel for alle. Av alle intervjuobjektene er det kun to som bare deler når de må.

Ingen av virksomhetene deler informasjon med NSM og media som de ikke har lov til. Personopplysninger, samarbeidsavtaler, bransjespesifikke begrensninger, og børssensitiv informasjon er informasjon som ikke vil bli delt. I tillegg vil informasjon som anses som irrelevant for NSM og andre beredskapsorganisasjoner holdes internt.

Alle virksomhetene legger vekt på lavterskel for deling med NSM. Informasjon som omhandler metoder og konsekvenser, teknisk informasjon, informasjon om hendelsen og sårbarheter, er eksempler på informasjon som deles med NSM. Informasjon om en pågående hendelse eller en endt hendelse som har påvirket virksomhetene sine kunder, er informasjon som alle virksomhetene er villige til å dele med media. Også informasjon som er lovpålagt og av offentlig interesse vil bli delt.

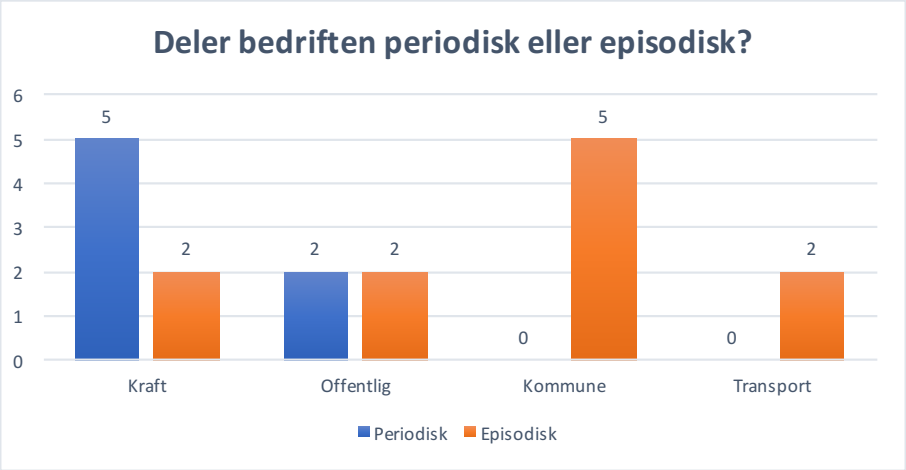
5.2.2 Sektorspesifikk analyse

Virksomhetene i kraftsektoren benytter seg av rammeverk som bygger på blant annet ITIL, NIST, ISO, og NSMs Grunnprinsipper. I offentlig sektor benytter alle seg av rammeverk, og to spesifikt ISO27001 rammeverket. Også i kommunesektoren blir det benyttet rammeverk, men ingen spesifikke er nevnt. Alle virksomhetene i transportsektoren benytter seg av rammeverk og her trekker en frem at deres Information Security Management System (ISMS) er basert på ISO27001.

I kraftsektoren er det noe variasjon i hvem som tar avgjørelsen om å være åpen om en sikkerhetshendelse. Dette foregår som regel i toppledelsen, men konsernsjef blir ikke nødvendigvis involvert. Svaret varierer ut fra virksomheten sin størrelse og om toppledelsen befinner seg på nivå en eller nivå to. En av virksomhetene innenfor kraftsektoren har ingen formell retningslinje på dette, og avgjørelsen blir tatt av den ansatte som er ansvarlig for hendelsen etter rådføring fra kommunikasjonsavdelingen.

Tre av fire virksomheter i offentlig sektor svarer at avgjørelsen tas i toppledelsen. Den siste virksomheten lar konserndirektør ta avgjørelsen. Blant kommunene vil avgjørelsen bli tatt av enten kommunedirektør eller toppledelsen hos fire av fem. Beslutningen tas av kriseledelsen i den siste kommunen. I transportsektoren blir valget om åpenhet rundt en sikkerhetshendelse bestemt hos toppledelsen. En av virksomhetene spesifiserer at denne avgjørelsen vil bli tatt av administrerende direktør.

Det er variasjon blant sektorene i forhold til deling av informasjon periodisk eller episodisk, slik figur 5.2 viser. Både i kommune- og transportsektoren deler alle kun episodisk, mens det i både kraft og offentlig sektor er mer fordelt mellom periodisk og episodisk deling. I den offentlige sektoren fordeler dette seg slik at de store virksomhetene er de som deler periodisk.



Figur 5.2: Spørsmål: Deler dere informasjon periodisk, gjennom for eksempel en formell avtale, eller gjøres det heller en vurdering når en hendelse først inntreffer?

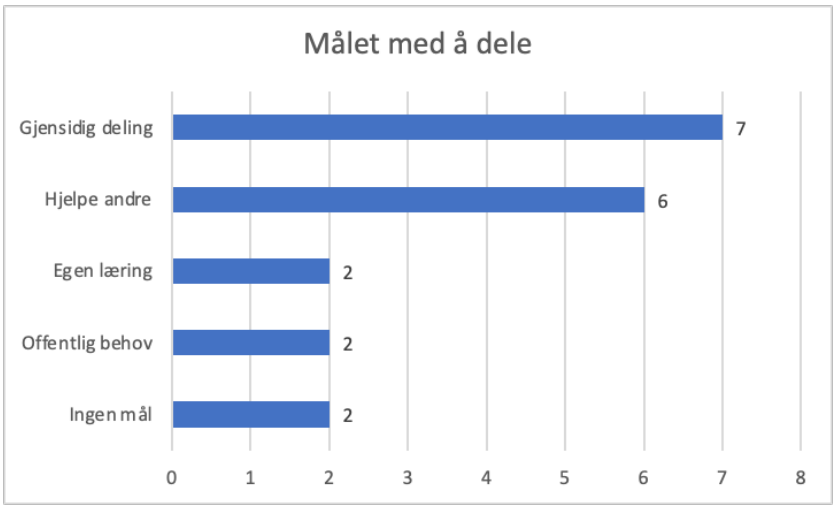
15 av 19 virksomheter samarbeider om sikkerhet med andre virksomheter i samme sektor. Kraftsektoren har KraftCERT, som legger et godt grunnlag for samarbeid, og alle virksomhetene i sektoren er med her. Kommunesektoren har tilsvarende i KommuneCSIRT, men ikke alle er med i denne. Likevel samarbeider alle kommunene med andre kommuner i nærområdet om sikkerhet. Hverken offentlig sektor eller transportsektoren har et etablert samarbeidsorgan, men tre av virksomhetene har dannet egne forum for samarbeid, og har kontakt med andre sikkerhetsansvarlige. Det har vært snakk om et felles samarbeid i transportsektoren, men dette ble ikke gjennomført da virksomhetene har så forskjellige systemer og arbeidsoppgaver. De anbefales heller å være med i NCSC.

Holdningene knyttet til å samarbeide og dele med konkurrenter er ganske like på tvers av sektorene. Halvparten av alle virksomhetene har ikke konkurranse, inkludert kommunesektoren hvor ingen har konkurrenter. Alle som har konkurrenter er klare på at de fortsatt deler. I kraftsektoren skjer mye av delingen gjennom KraftCERT, hvor både konkurrenter og ikke konkurrenter deltar, og det er ingen av intervjuobjektene som ønsker å skille mellom disse i arbeidet for bedre sikkerhet. Virksomheter i alle sektorene trekker frem at sikkerhet ikke er et av de punktene man konkurrerer om, og det er mye bedre for sektoren og samfunnet at alle blir bedre på sikkerhet.

Risikovurdering knyttet til deling av informasjon tas i kraftsektoren vanligvis enten gjennom dialog eller fra sak til sak. Dette gjøres også mye i offentlig sektor. I kommunesektoren er det mindre vurdering, og to forteller at de har en kultur på at man skal dele med andre kommuner. I transportsektoren har alle virksomhetene gjort vurderinger, enten risikovurdering på informasjonsdeling eller verdivurdering av informasjonen de har, men ikke deling av IKT-hendelser spesifikt.

TLP er det mest brukte systemet for å sette krav og regler til deling av informasjon med andre virksomheter hos intervjuobjektene. I kraftsektoren er det tre som nevner dette spesifikt, og det trekkes frem at dette benyttes av KraftCERT. Også i de andre sektorene nevnes TLP hos de som er med i forskjellige CERTer. I både offentlig- og kommunesektor påvirker offentlighetsloven virksomhetene på deling, siden mye av informasjonen skal være offentlig tilgjengelig. I transportsektoren er det en som har definert egne regler, og en som tar det når muligheten for å dele oppstår.

Kraftsektoren uttrykker tydelig at deres mål for deling er å være til hjelp for andre virksomheter, og bidra til gjensidig utveksling, som kan føre til økt stabilitet i sektoren. Både kommune- og offentlig sektor svarer at deling skal være til hjelp for deres egen del og andres, ved at informasjonen de deler hjelper andre, samtidig som virksomheten kan motta hjelp. I transportsektoren er det kun en bedrift som har gjensidig utveksling som sitt mål, mens de andre deler til fordel for offentligheten. Figur 5.3 viser hvor mange som har nevnt hver av de ulike målene.



Figur 5.3: Spørsmål: Har bedriften noen satte mål for hva dere ønsker å oppnå med å dele?

Kraftsensitiv og børssensitiv informasjon er informasjon som kraftsektoren ikke vil dele med hverken NSM, andre beredskapsorganisasjoner, eller media. Informasjon som anses som urelevant blir heller ikke delt. To av virksomhetene i offentlig sektor har samarbeidsavtaler med leverandører og kunder, og informasjon som omhandler problemer hos disse deles ikke. I kommunesektoren blir ikke informasjon holdt tilbake grunnet offentlighetsloven. I transportsektoren er det kun enkeltpersoner sine feiltrinn som ikke gir direkte konsekvenser for virksomheten, som ikke deles.

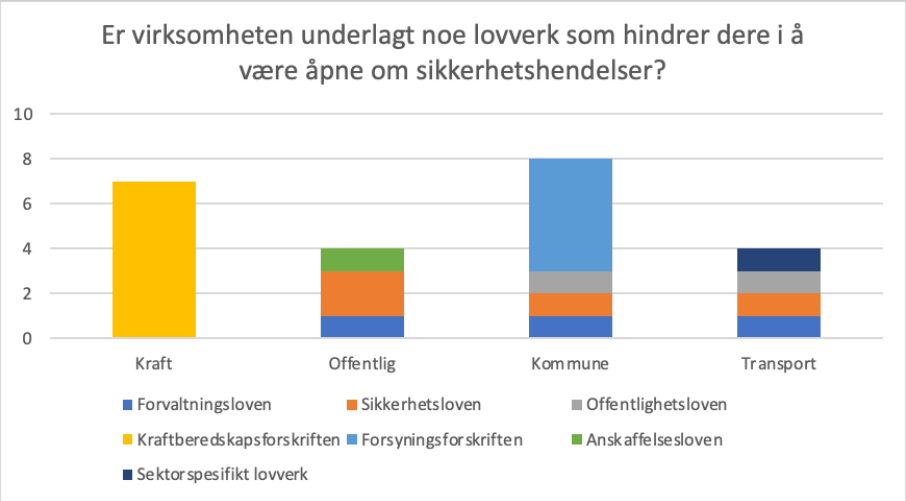
Virksomhetene i kraftsektoren deler først og fremst informasjon med samarbeidspartnerene i KraftCERT. Utover dette vil virksomhetene dele informasjon med NSM der det er relevant. Det oppleves som meget verdifullt å dele informasjon med NSM i den offentlige sektoren. Til NSM blir det delt informasjon om hendelser, metoder, og mye annet. Også kommunesektoren og transportsektoren deler alle typer informasjon med NSM.

Informasjon om både pågående og avsluttede hendelser som påvirker kunder vil kraftsektoren dele med media. Fire virksomheter har svart at de ser til måten Hydro håndterete sin hendelse som en rettesnor for nivået av deling de bør legge seg på [49]. Informasjon som omhandler en sikkerhetshendelse hos virksomheter i offentlig sektor vil bli delt med media, men her blir det lagt vekt på forsiktighet rundt forklaringen for å motvirke feiltolkning av media. Blant kommunene er det å dele med media ikke nødvendigvis en prioritet for alle når en sikkerhetshendelse inntreffer. I transportsektoren vil alle sikkerhetshendelser som påvirker kunder bli delt, og media brukes som en informasjonskilde for kundene.

5.3 Kategori 2: Regelverk

I forhold til definisjonen om åpen informasjon, som er beskrevet i kapittel 2, har virksomhetene litt mer varierte oppfatninger. En del synes denne kan anvendes, spesielt første del av definisjonen. Noen oppfatter delen om sammensetning av informasjon som litt uklar, men også her er det flere som bruker en egen definisjon. En bedrift trakk fram situasjonen der informasjon blir tilgjengelig uten at den nødvendigvis er åpen, på grunn av feil knyttet til begrensning av tilgjengelighet. Det er også påpekt at denne kan være litt for teoretisk for offentlig sektor da det meste av informasjon skal være offentlig der, speseilt for de virksomhetene som er underlagt offentlighetsloven.

Virksomhetene er underlagt flere lovverk som både stiller krav til tilbakeholdelse av informasjon, samt deling og rapportering. Felles for alle er personvernloven, som stiller krav til rapportering av hendelser. Flere virksomheter er også underlagt sikkerhetsloven som påvirker deling i begge retninger. Kraftberedskapsforskriften er svært sentral for kraftsektoren, og setter mange føringer til hva virksomheten kan og ikke kan dele. Anskaffelsesloven kan i ulike situasjoner stå til hinder for deling av informasjon i offentlig sektor. Figur 5.4 viser hvilke lovverk som hindrer virksomhetene i å dele en hendelse. Dette er basert på hva virksomhetene har svart, så det kan være flere som er underlagt lovverk som de ikke har nevnt her.



Figur 5.4: Spørsmål: Er bedriften/organisasjonen underlagt noe lovverk som hindrer dere i å være åpne om sikkerhetshendelser?

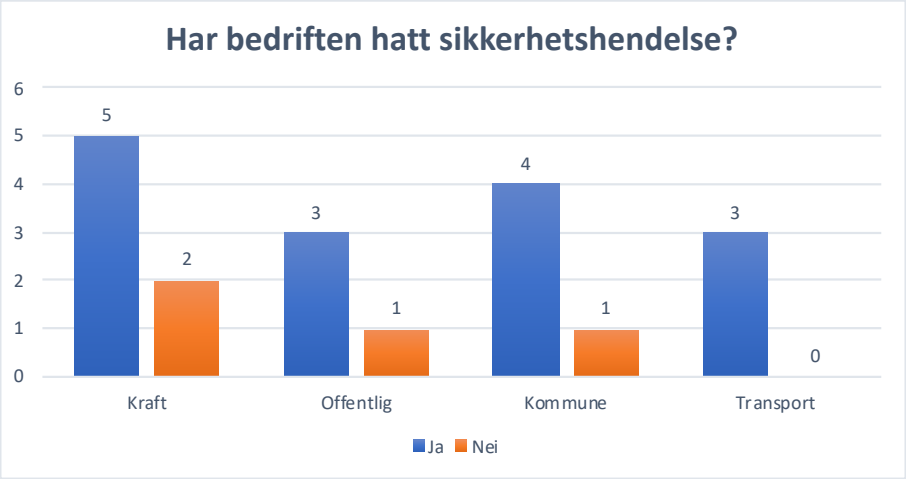
På den andre siden stiller arkivloven og offentlighetsloven krav til rapportering av sikkerhetshendelser. I kommunesektoren hindrer forsyningsforskriften deling av informasjon om hendelser som omhandler vannforsyningen i kommunen. Offentlighetsloven og forvaltningsloven stiller krav til rapportering og deling av sikkerhetshendelser i sektoren. Forvaltningsloven og lovverk spesifikt til enkelte fagfelt er lovverk som påvirker hvor mye informasjon virksomhetene i transportsektoren kan dele. Samtidig stiller både offentlighetsloven og personvernloven krav til rapportering og deling av sikkerhetshendelser, med mindre det skal unntas offentligheten.

At et lovverk krever rapportering av en hendelse betyr ikke nødvendigvis at hendelsen må deles med offentligheten. Hendelser som må rapporteres til NVE gjennom kraftberedskapsforskiften kan omhandle kraftsensitiv informasjon som gjør at virksomheten ikke får lov til å dele hendelsen. Samtidig vil offentlighetsloven tvinge deling med offentligheten når en hendelse rapporteres.

5.4 Kategori 3: Rutiner og prosesser

5.4.1 Helhetsanalyse

Totalt av alle virksomhetene som er intervjuet har 15 hatt minst en middels eller stor sikkerhetshendelse. Det er ikke satt en tidsbegrensing på når hendelsen inntraff. Ingen av sektorene har ikke hatt en hendelse, og som figur 5.5 viser, har de som ikke har hatt hendelse fordelt seg på kraft-, offentlig- og kommunesektoren.

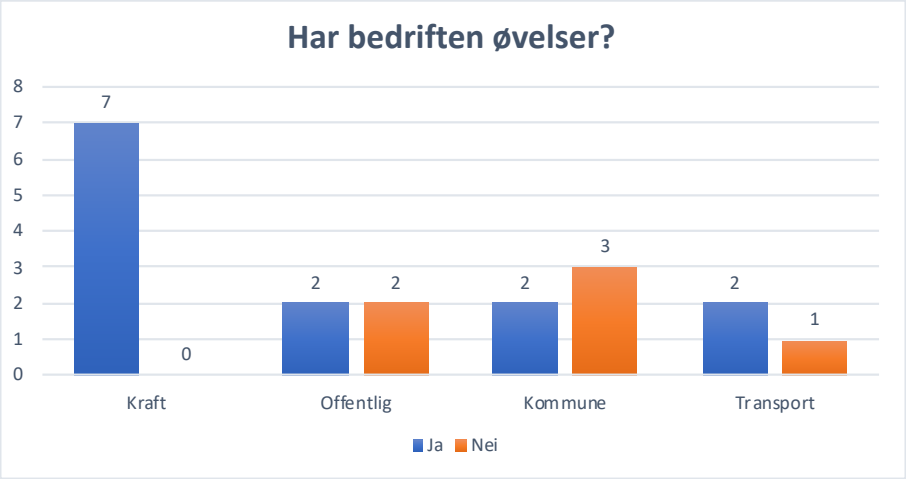


Figur 5.5: Spørsmål: Har bedriften hatt en sikkerhetshendelse?

Alle intervjuobjektene har etablerte rutiner for håndtering av en hendelse. Innholdet varierer meget, men det går mye i avvik- eller beredskapssystemer. Virksomhetene har ofte en beredskapsplan hvor ulike nivåer av beredskap er definert, da ulike hendelser skal hånderes på forskjellige nivåer. Alle virksomhetene er også klare på at disse rutinene faktisk følges. En har opplevd at rutinene for store sikkerhetshendelser ikke har vært gode nok når en slik hendelse har inntruffet, og har derfor endret rutinene i ettertid.

Felles for alle virksomhetene er at håndteringen av de større hendelsene skal gjøres hos en form for ledelse. Det er en del som tar det helt opp til toppledelsen i virksomheten. Virksomhetene som setter beredskap eller krisestab lar ofte beredskaps- eller kriseleder ta hovedansvaret for delegering av oppgaver og rapportering. Tre virksomheter lar de som sitter med hendelsen, ofte IT-ledelsen, håndtere den. Alle er tydelige på at hendelsene faktisk håndteres på det satte nivået i beredskapsplanen.

Ikke alle har øvelser på IT-sikkerhetshendelser. Figur 5.6 viser at totalt 13 av virksomhetene har øvelser på IT-sikkerhet spesifikt, mens seks virksomheter ikke har det. Det er ikke slik at disse seks ikke øver i det hele tatt, flere av de øver ofte på andre scenarioer mer knyttet til fysisk sikkerhet. Virksomhetene med IT-sikkerhetsøvelser har også andre type øvelser.



Figur 5.6: Spørsmål: Har dere øvelser knyttet til å respondere på sikkerhetshendelser som en del av håndteringsrutinene deres?

Hyppigheten av øvelsene varierer meget, halvparten har en eller to ganger årlig, mens tre virksomheter har annenhvert eller hvert tredje år. Den vanligste typen er skrivebordsøvelser, men et par har også strategisk eller teknisk øvelse. To av virksomhetene gjennomfører øvelser ved bruk av rollespill slik at de ansatte får prøvd seg i en reell situasjon. Her trekkes spesielt Hydro inn, da to virksomheter har utført øvelser basert på den store Hydro hendelsen [49].

Erfaringene rundt øvelsene er varierende. Fem virksomheter syns det er vanskelig å si noe konkret, men noen oppfatninger går igjen. Bevisstgjøringsarbeid og innføring av rapporteringssystem har hatt større påvirkning enn øvelser på rapportering av sikkerhetshendelser. En tredjedel opplever at øvelser har endret seg etter hendelser, fordi man fort ser hva som ikke fungerer, og dermed hva man må øve mer på. Også andre virksomheter sine hendelser brukes som inspirasjon for øvelser for å gjøre de mer motiverende og relevante.

5.4.2 Sektorspesifikk analyse

I kraftsektoren er det i hovedsak beredskapsleder som har ansvaret for å håndtere en stor hendelse, og hvis ikke virksomheten har en slik rolle er det ledelsen sitt ansvar. Både offentlig- og transportsektor følger samme opplegg, men der er det kriseledelse i stedet for beredskapsleder. Det er større variasjon blant kommunene, der en har toppledelsen, en bruker kriseledelse og de resterende gir ansvaret til IT-ledelsen. Alle virksomhetene informerer at hendelsene blir håndtert på det satte ledelsesnivået.

Kraftsektoren er pålagt å ha øvelser gjennom kraftberedskapsforskriften, og alle

intervjuobjektene i denne sektoren følger dette kravet med øvelser en til to ganger i året. I de andre sektorene er det mer variasjon, med cirka halvparten som har øvelser i hver sektor. I den offentlige sektoren øves det også en til to ganger årlig. Både kommune- og transportsektoren har virksomheter som øver annenhvert år, men det er også en bedrift i transportsektoren som øver på sikkerhetshendelser tre ganger årlig.

I transportsektoren har begge virksomhetene som har øvelser fokus på å involvere toppledelsen i øvelsene, og gjennomfører både skrivebordsøvelser og tekniske øvelser. Skrivebordsøvelser brukes også flittig i kommune- og kraftsektoren, med to kraft virksomheter som også har strategisk eller operativt nivå. I den offentlige sektoren brukes også skrivebordsøvelser, men de legger vekt på øving på kriseledelse og hos krisestaben. De har også scenariobaserte øvelser med spillstab for de virkelig store hendelsene hvor større deler av virksomheten trekkes inn.

Det er en generell oppfatning om at det ikke er øvelser som fører til økt rapportering av sikkerhetshendelser, men heller andre ting. I kraftsektoren pekes bevisstgjøringsarbeid og etablering av rapporteringssystem som årsakene til økt rapportering. Transportsektoren er enige med innføring av rapporteringssystem, og erfarer i tillegg at GDPR har ført til økt rapportering. I den offentlige sektoren påpeker Posten at de som deltar på øvelser ofte er de som allerede har høy bevissthet på sikkerhet.

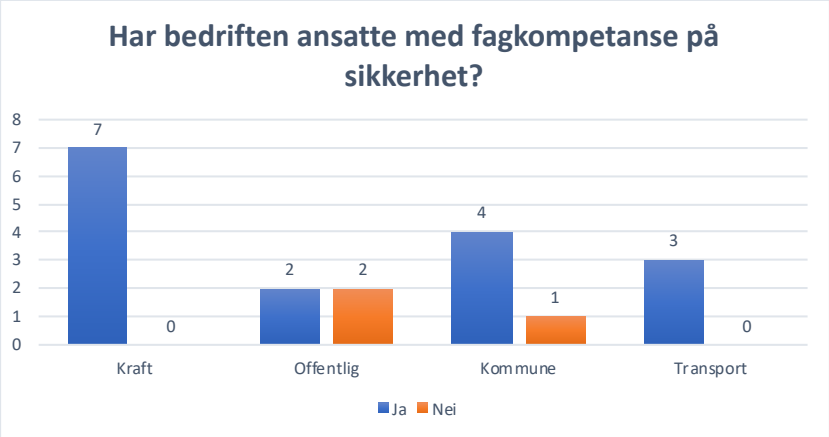
Det er mer variasjon i erfaringene knyttet til endring av øvelser etter hendelser. Her er transportsektoren særlig positiv, og bruker både egne hendelser og andres som grunnlag for endringer av øvelsene. Underveis i en hendelse ser man fort hva som ikke fungerer, og da må dette øves på. Bruken av andre virksomheter sine hendelser som grunnlag gjør øvelsene mer motiverende og de ansatte får øvd på et relevant trusselbilde. Kraftsektoren deler denne oppfatningen, og tilpasser øvelsene etter det de ser virksomheten trenger å øve på. Også offentlig sektor gjør dette, og bruker After Action Review (AAR) til å finne ut hva som må forbedres. AAR er en metode for analysering av et gjennomført arbeid, og handler om å identifisere styrker, svakheter og områder som kan forbedres hos de ansatte [50]. Kommunene har ikke hatt den type store hendelser som har påvirket noe særlig.

5.5 Kategori 4: Ressurser og kompetanse

5.5.1 Helhetsanalyse

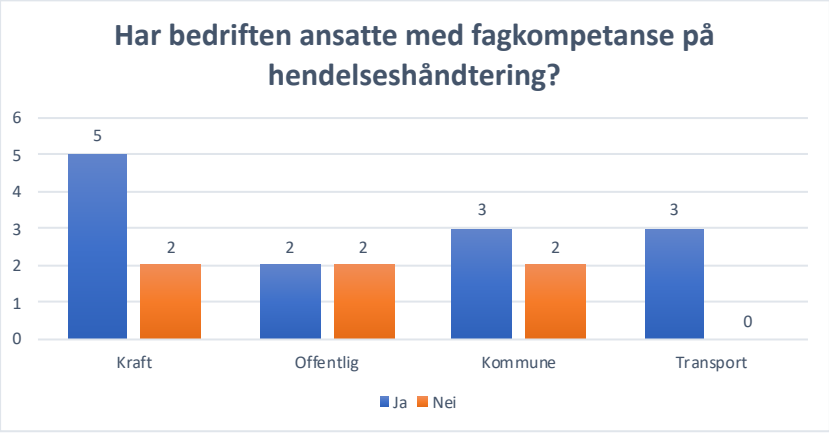
16 av 19 virksomheter har en egen IT-avdeling. Størrelsen på avdelingen varierer veldig, med noen som bare har et par ansatte, som først og fremst stiller krav til leverandører og avgjør hvilke tjenester virksomheten trenger å sette ut, og andre har over 300 ansatte på IT. Også blant de store varierer størrelsen kraftig, med alt fra åtte eller tolv til de største på 200-300. Figur 5.7 viser at 16 virksomheter også

har minst en ansatt med kompetanse innen sikkerhet. Kun tre virksomheter har ikke egne folk med denne kompetansen.



Figur 5.7: Spørsmål: Har bedriften fagpersonell med kompetanse innen sikkerhet?

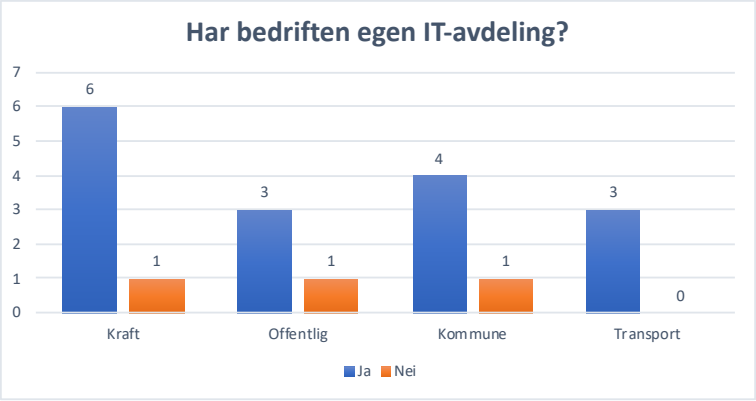
To tredeler har egne ansatte med kompetanse innen hendelseshåndtering, slik figur 5.8 viser. Av de seks som ikke har dette spesifikt, svarer de at de har ansatte med erfaring innen beredskap og krisehåndtering av fysiske hendelser, eller at de ønsker å sende ansatte på kurs. Ikke alle virksomhetene er med i en type CERT eller CSIRT heller. De som nevnes er KraftCERT, NCSC, KommuneCSIRT og HelseCERT. Det er totalt 13 som er med i en av disse fire, og seks som ikke er det.



Figur 5.8: Spørsmål: Har bedriften fagpersonell med kompetanse innen hendelseshåndtering?

5.5.2 Sektorspesifikk analyse

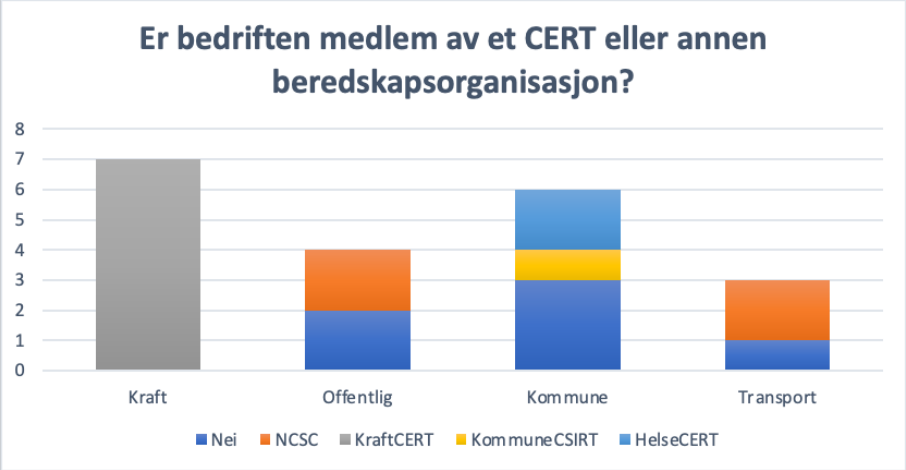
Fordelingen av virksomhetene med egen IT-avdeling er ganske jevn, og fremstilles i figur 5.9. I kraftsektoren har alle dette, untatt Rakkestad Energi, som er en liten bedrift. I den offentlige sektoren er det kun den mellomstore virksomheten Avfall Sør som ikke har en egen IT-avdeling. Oslo kommune som en helhet har en IT-avdeling, men den seksjonen som ble intervjuet har ikke det. Ellers har alle de andre kommunene egen IT-avdeling, og det har også alle virksomhetene i transportsektoren.



Figur 5.9: Spørsmål: Har bedriften egen IT-avdeling?

Både i kraft- og transportsektoren har alle virksomhetene ansatte med kompetanse innen sikkerhet. I den offentlige sektoren er det to av fire, og det er de to mellomstore virksomhetene som ikke har denne kompetansen. En av kommunene har heller ikke dette. De samme virksomhetene i den offentlige sektoren og kommunen har ikke egne ansatte med kompetanse på hendelseshåndtering heller. Alle virksomhetene i transportsektoren har denne kompetansen, mens i kraftsektoren er det to som ikke har det, slik figur 5.7 illustrerer.

Alle virksomhetene i kraftsektoren er medlem i KraftCERT. I den offentlige sektoren er det to virksomheter som er medlem av NCSC, og to som ikke er med i et CERT. To kommuner er med i HelseCERT, og en av de har planer om å bli med i KommuneCSIRT. Planer om dette har også en annen kommune, og den siste kommunen var ikke helt sikker. Transportsektoren har ikke et eget CERT, og to av virksomhetene er derfor heller med i NCSC. Hvor mange som er en del av hver av disse vises i figur 5.10.

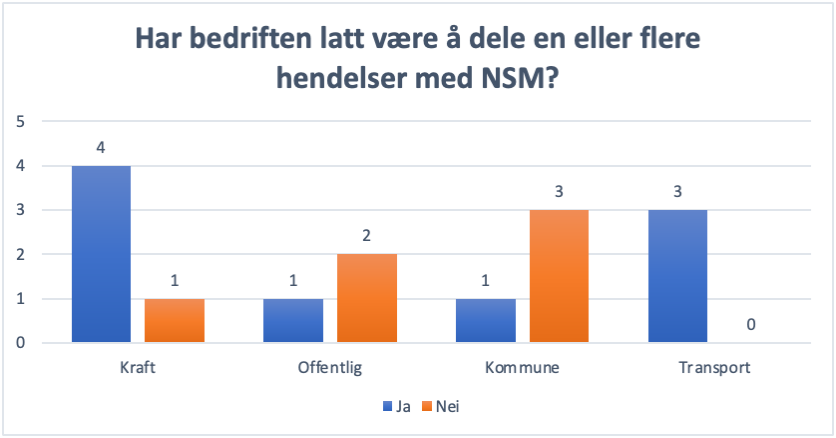


Figur 5.10: Spørsmål: Er bedriften medlem av et CERT, SektorCert, CSIRT eller andre organer for samarbeid innen sikkerhet?

5.6 Kategori 5: Erfaringer og evalueringer

5.6.1 Helhetsanalyse

Av alle virksomhetene som har hatt en stor eller mellomstor sikkerhetshendelse, er det ti stykker som har valgt å ikke dele minst en av hendelsene med NSM, og seks som har valgt å dele alle. Fordelingen av disse på tvers av sektor vises i figur 5.11. Her er det bare 15 virksomheter totalt, da kun 15 har hatt en stor eller mellomstor hendelse. De som ikke har delt har svart at de enten ikke så på det som relevant informasjon å dele med NSM, eller at det ikke var et etablert samarbeid og det ble derfor ikke med i vurderingen rundt deling av sikkerhetshendelser.



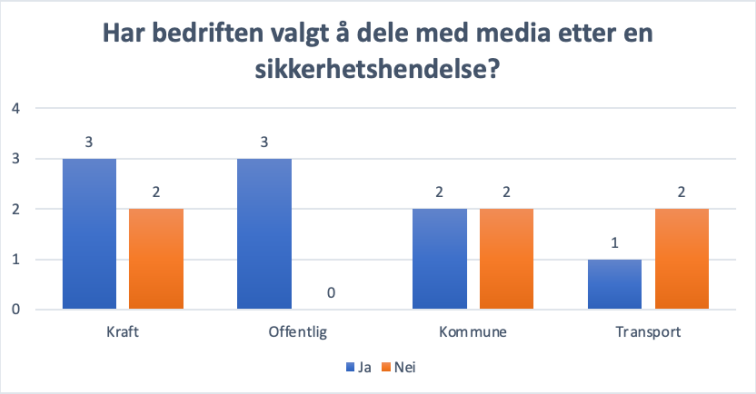
Figur 5.11: Spørsmål: Er det en eller flere hendelser dere har valgt å ikke dele med NSM, NCSC og andre beredskapsorganisasjoner, og heller ikke media?

I ettertid kan ingen virksomheter rapportere om opplevd positiv eller negativ konsekvens rundt det å ha delt eller ikke ha delt med NSM. Virksomhetene som har delt opplever at delingen har gått som forventet uten noen videre konsekvens, men de håper at informasjonen var til hjelpe for andre. De som ikke har delt har generelt lite å kommentere da det er vanskelig å måle konsekvens av å ikke dele. Det skal nevnes at en bedrift som ikke delte opplever at de nok har gått glipp av en mulighet til å få hjelp, uten at de kan utdype videre om hva denne hjelpen skulle vært.

Erfaringene til virksomhetene har ikke videre påvirket dem til å dele mer eller mindre med NSM i ettertid. Siden det ikke er opplevd noen positive eller negative konsekvenser av hverken det å dele eller å ikke dele, har det ikke vært en endring i adferd.

Det er totalt ti virksomheter som har valgt å dele minst en hendelse med NSM eller en annen beredskapsorganisasjon. Virksomhetene valgt å dele med disse for å informere bransjen og hjelpe andre virksomheter beskytte seg for samme type angrep. I tillegg er det mange virksomheter som kontakter NSM om en hendelse for å få hjelp, både teknisk og med håndteringen. Disse hendelsene er ikke delt videre til media, og dette er ofte fordi det ikke oppleves som relevant, eller fordi hendelsen avslører tekniske detaljer og sårbarheter som kan hemme virksomheten om det ble gjort offentlig.

Igjen er det ingen som har gjort noen målinger på konsekvenser, både positive og negative. Likevel opplever flere av virksomhetene det som positivt å dele med NSM og andre beredskapsorganisasjoner fordi de får den hjelpen de trenger, og fordi de opplever at det hjelper andre virksomheter. Ingen har noe konkret eksempel på at de positive konsekvensene har ført til mer deling, men virksomhetene opplever det som motiverende å støtte fellesskapet, og det støtter opp om tanken at å dele var den riktige avgjørelsen.



Figur 5.12: Spørsmål: Er det en eller flere hendelser dere har valgt å dele med media?

Av de 15 virksomhetene er det ni stykker som har vært ute i media om minst en hendelse, og seks som ikke har vært det. Figur 5.12 viser fordelingen på tvers av sektorene. Virksomhetene går oftest ut fordi hendelsen påvirker kundene, og da er det viktig at disse blir informert. Det er også flere som går ut i situasjoner der de vet media uansett kommer til å finne ut av det, og de ønsker å ha kontroll over narrativet.

Virksomhetene opplever å få mange positive tilbakemeldinger, men det har en negativ side også. Flere er misfornøyde med måten media presenterer hendelsen, og opplever at media ikke forstår situasjonen. Erfaringene er at media stiller feil spørsmål, og forklarer hendelser på feil måte, slik at hvertfall to virksomheter har måtte gått ut i ettertid å rette opp i utsagn fra media. Disse erfaringene har ikke hindret virksomhetene i å dele hendelser ved senere anledninger, men flere velger å være litt mer nøysomme i mediahåndteringen.

Figur 5.13: Spørsmål: Er det en eller flere hendelser dere har valgt å dele med media der dere ikke har delt med NSM, NCSC eller andre beredskapsorganisasjoner først?

Det er kun en bedrift som har valgt å dele en hendelse med media uten å først kontakte NSM eller en annen beredskapsorganisasjon, som figur 5.13 viser. Dette var en stor bedrift i kraftsektoren, og de opplevde positiv respons, i tillegg til at de fikk belyst temaet, som var deres mål med delingen. Det er ikke satte rutiner for hvem som skal avgjøre om å gå ut i media i denne virksomheten, så erfaringene var ikke med på å påvirke videre deling.

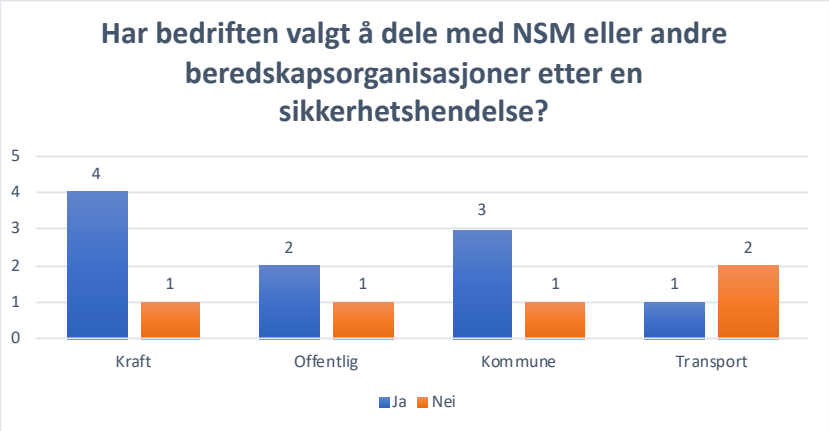
Figur 5.14: Spørsmål: Hva anser dere som årsaken(e) til hendelsen(e) dere har hatt?

De to mest nevnte årsakene til en sikkerhetshendelse hos intervjuobjektene er menneskelig feil og feil hos tredjepart. Andre årsaker som trekkes frem er knyttet til uforutsette og motiverte trusler, gamle systemer, manglende sikkerhet og manglende oversikt, for å nevne noen. Det er kun de to første som nevnes av flere enn to virksomheter. Figur 5.14 viser en full oversikt over alle nevnte årsaker. Her har virksomhetene svart fritt uten å bli gitt alternativer på årsaker.

5.6.2 Sektorspesifikk analyse

På spørsmålet om hvem som erfaringsmessig tar avgjørelsen om virksomheten skal dele informasjon om en hendelse eller ikke, svarer alle untatt en at det gjennomføres slik rutinene tilsier. Det er altså kun en bedrift hvor dette er tilfeldig utifra hvem som håndterer hendelsen.

Figur 5.15 viser fordelingen av virksomhetene som har delt minst en hendelse med NSM. Det er ikke en sektor som skiller seg noe særlig ut på dette punktet, hvor kun en til to stykker per sektor ikke deler. I alle sektorene legges det vekt på at en av årsakene til å dele er at man kan få hjelp. I transportsektoren ble kun dette nevnt, mens de andre sektorene også trekker frem at deling gjøres for å hjelpe bransjen og andre virksomheter, både ved bevisstgjøring på trusselbildet og ved å advare og gi tiltak mot en spesifikk trussel. Det trekkes også frem at hendelsen ikke deles videre til media fordi det ikke oppleves som relevant.



Figur 5.15: Spørsmål: Er det en eller flere hendelser dere har valgt å ikke dele med media som dere delte med NSM, NCSC eller andre beredskapsorganisasjoner?

Tre av fire sektorer svarer at hovedårsaken til deling med NSM er for å hjelpe andre. Mye av informasjonen som ikke oppleves som relevant for media deles likevel med NSM, da det er ulikt hva som kan være interessant for disse, og de kan gå inn på mer tekniske detaljer som man helst ikke vil ha ut i media. Transportsektoren skiller seg ut ved å kun legge fokus på at de deler for å få hjelp. Kraftsektor nevner også dette, men har ikke like stort fokus på å få hjelp, men mer samholdet og læringsutvekslingen som kommer med deling.

Samtlige virksomheter har hatt en positiv opplevelse ved å dele med NSM. Transportsektoren ble betrygget over at hendelsen var over. Offentlig sektor har ingen målinger, men velger å anta at det har en stor verdi å dele. Kommunesektoren presiserer at det var godt å få hjelp når det skjedde sikkerhetshendelser og kraftsektoren hadde positive opplevelser rundt det å få og gi hjelp med hendelsene. Kraftsektoren anser det som viktig å fortsette med deling, og blir motivert av å støtte oppunder felleskapet. De andre sektorene har ikke opplevd noe som har fått de til å endre deres ståsted knyttet til deling.

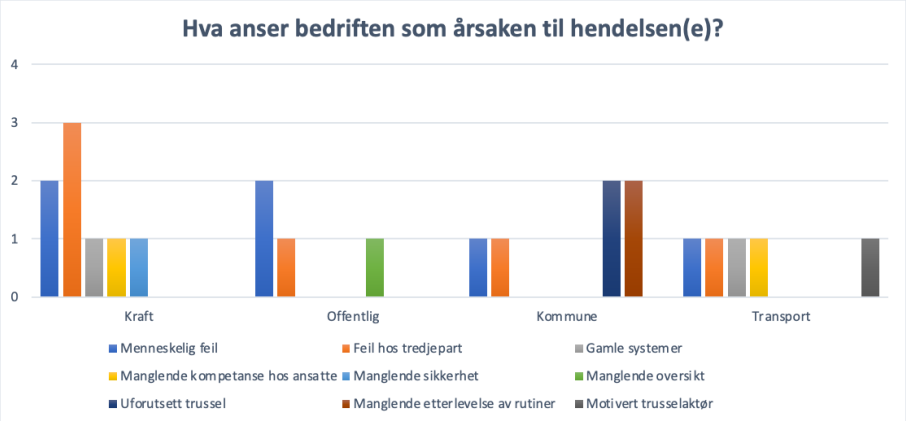
Figur 5.12 illustrerer fordelingen av virksomheter som har delt en eller flere sikkerhetshendelser med media. Dette fordeler seg ganske jevnt i hver sektor, hvor cirka halvparten har valgt å dele en hendelse i hver sektor. Unntaket er offentlig sektor, hvor alle tre som har opplevd minst en stor eller mellomstor sikkerhetshendelser har valgt å dele den med media.

Samtlige svarer at de har delt med media for å informere kunder og brukere om hva som har skjedd, hvordan det påvirker de og hvor lenge de antar at hendelsen vil påvirke normal drift. Kraftsektoren og offentlig sektor presiserer at de også deler for å få kontroll på hvordan media formidler hendelsen. De har liten tillit

til at media håndterer saken på en god måte og vil derfor selv gå ut med korrekt informasjon. Kommunesektoren opplever det som naturlig å gå ut i media om hendelser, og som et offentlig organ føler de seg forpliktet til det. Transportsektoren viser til at media kan plukke opp politianmeldelser, og dette kan derfor være en årsak til at hendelser er delt med media. Disse virksomhetene legger også vekt på et ønske om å ha kontroll over narrativet.

Å dele åpent med offentligheten oppleves ikke som direkte negativt. Kraftsektoren har ingen målinger, men har motatt gode tilbakemeldinger og utelukkende positiv respons på deres åpenhet. Offentlig sektor er mer delt, hvor to av virksomhetene opplever positiv respons, mens den siste syns det er negativt med måten media graver etter informasjon som ikke kan bli gitt ut. Kommunesektoren har ikke erfart noen negative konsekvenser når media har plukket opp saker hos dem. Transportsektoren opplever at rask kommunikasjon knyttet til hendelseshåndtering er viktig for å gjøre kundene mer tålmodige. De negative konsekvensene ved deling slår ut når media kommer med feilforklaringer eller feil opplysninger knyttet til saken.

Erfaringen fra å dele med media har ikke påvirket sektorene til å endre mening i forhold til viktigheten av deling. Virksomhetene i kraftsektoren meddeler at de vil fortsette å dele. Offentlig sektor erkjenner at det er fint å få bekreftelse på at sikkerhetshendelser blir håndtert på en god måte, men vil være mer bevisst på ordvalget i fremtiden. Kommunesektoren opplever det som vanskelig å uttale seg da de ikke egentlig har opplevd noen konsekvenser ved å dele. Transportsektoren ser på det som positivt at de er blitt flinkere på å gå ut med informasjon før media begynner å rapportere om hendelsen.



Figur 5.16: Spørsmål: Hva anser dere som årsaken(e) til hendelsen(e) dere har hatt?

Figur 5.16 viser årsaker til sikkerhetshendelser fordelt på sektorene. Manglende oversikt, motiverte trusselaktører og manglende sikkerhet er årsaker som kun

går igjen en gang. Uforutsett trussel og manglende etterlevelse av rutiner er bare nevnt i kommunesektoren, men til gjengjeld er hver av disse årsakene nevnt av to kommuner. Gamle systemer og manglende kompetanse hos ansatte er felles for både kraft- og transportsektoren. Årsakene som er felles for alle sektorer er menneskelig feil og feil hos tredjepart.

Kapittel 6

Diskusjon

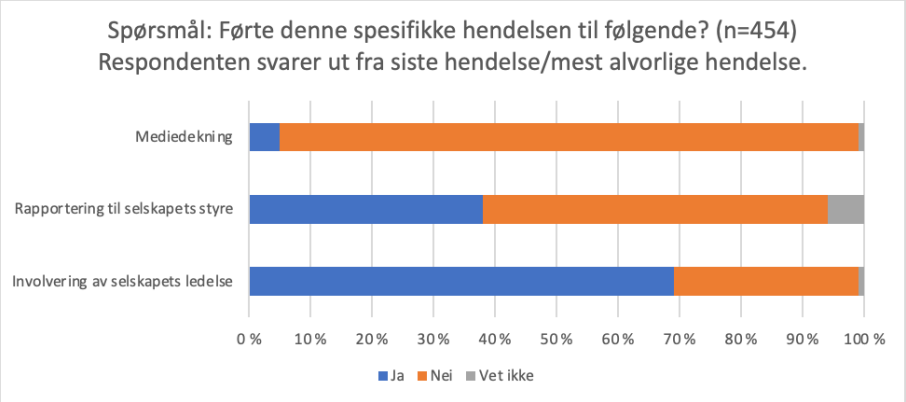
6.1 Introduksjon

I diskusjonen blir hensikten med de ulike spørsmålene trukket inn og besvart for å trekke linjer og se på sammenhenger mellom ulike faktorer. I tillegg beskrives refleksjoner rundt funnene som ikke er direkte knyttet til hensikten. Til slutt omtales begrensinger, erfaringer og videre arbeid som kan gjennomføres.

6.2 Resultater

Av de virksomhetene som har hatt sikkerhetshendelser, involverer alle utenom to virksomheter ledelsen i avgjørelsen om å skulle dele eller ikke. Samtidig involveres ledelsen eller krisestab i rapportering og håndtering av store hendelser hos alle virksomheter utenom et par kommuner, hvor det er IT-ledelsen som håndterer hendelsen. Dette vil si at alle virksomhetene som har hatt en stor hendelse har involvert ledelsen gjennom enten håndtering eller valget om deling, eller ved begge som de fleste virksomhetene gjør. Også de to virksomhetene som ikke har delt en hendelse med verken NSM, andre beredskapsorganisasjoner eller media, har involvert ledelsen.

Resultatene fra denne undersøkelsen og resultatene i mørketallsundersøkelsen er ulike. I mørketallsundersøkelsen er det kun 69% av virksomhetene som involverer ledelsen som følge av en hendelse og 38% rapporterer til styret, mens det i denne undersøkelsen er 19 av 19 som involverer ledelsen. Figur 6.1 viser de tre følgene etter en hendelse som er mest relevante til denne undersøkelsen. Forskjellen kan begrunnes både i det ulike totale antallet intervjuobjekter, der det var 454 virksomheter som svarte på spørsmålet i mørketallsundersøkelsen og 19 i denne, og med at mørketallsundersøkelsen har større spenn i størrelsen på virksomhetene som er intervjuet. [4]

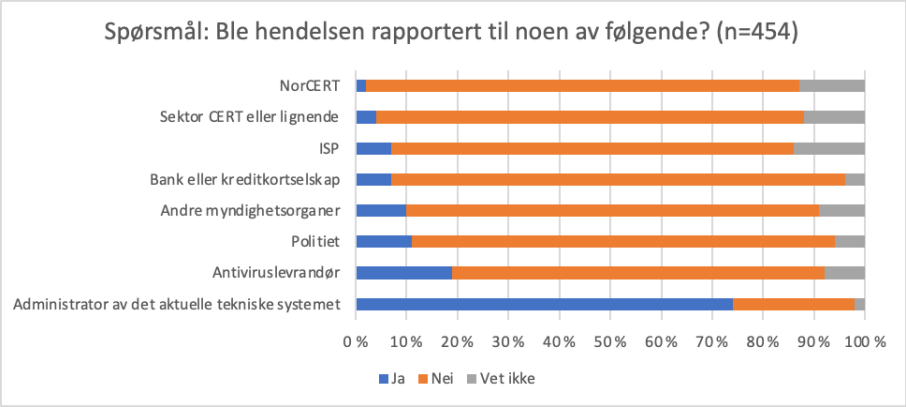


Figur 6.1: Fra mørketallsundersøkelsen: Førte denne spesifikke hendelsen til følgende?

Figur 6.1 viser også i hvor mange prosent av tilfellene der mediadekning ble en følge av hendelsen. I mørketallsundersøkelsen involveres media i 5% av tilfellene, noe som er svært forskjellige fra 9 av 15 som er tallene i denne undersøkelsen. Den største årsaken til dette er at i utvelgelsen av intervjuobjektene ble det i denne undersøkelsen lett spesifikt etter virksomheter som har gått ut i media om en hendelse, mens mørketallundersøkelsen ikke har plukket ut slike virksomheter. Her har undersøkelsene forskjellig fokus, og tallene kan derfor ikke sammenlignes.

Som figur 5.2 viser deler de fleste av virksomhetene episodisk, men dette varierer stort mellom sektorene. I kraftsektoren er det kun to av syv som bare deler episodisk, og i offentlig sektor deler halvparten periodisk. Det mest interessante her er at i den offentlig sektoren er det de store virksomhetene som deler periodisk, og de mellomstore som deler episodisk. Samtidig er det to store virksomheter i kraftsektoren som bare deler episodisk. Resultatene viser ingen klar sammenheng mellom periodisk deling og økt deling med NSM eller media, da to av virksomhetene som deler episodisk har delt med minst en av disse, og andre virksomheter som deler periodisk har latt være å dele. [4]

I mørketallsundersøkelsen er bare 4% av virksomhetene medlem av en form for sektorCERT, mens 2% rapporterer til NCSC [4]. Figur 6.2 viser hvor de ulike virksomhetene i mørketallsundersøkelsen rapporterte hendelsen. Intervjuobjektene i denne undersøkelsen fordeler seg ikke på samme måte, slik figur 5.10 viser. Her kan man se at 68% er medlem av at samarbeidsorgan, hvor 52% er medlem av en form for sektorCERT og 21% er medlem av NCSC. De som er medlem av et samarbeidsorgan har oftere kontakt med disse, noe som fører til hyppigere deling med samarbeidsorganet dersom en hendelse inntreffer. Det kan tolkes ut ifra tallene at dersom virksomheten er medlem i et samarbeidsorgan, vil de oftere dele med disse. Likevel er det ingen tegn til at dette påvirker delingen med media.



Figur 6.2: Fra mørketallsundersøkelsen: Ble hendelsen rapportert til noen av følgende?

Intervjuene viser at virksomheter som har konkurranse fortsatt ser på sikkerhetssamarbeid som viktig, og sikkerhet er ikke et av punktene de ønsker å konkurrere på. Sunn konkurranse baserer seg på å levere en tjeneste eller et produkt som er bedre enn konkurrentene, ikke det å holde tilbake viktig sikkerhetsinformasjon som kan gå utover kunder. Dersom det er uoppdagede sikkerhetshull er det ikke snakk om "hvis" man blir utsatt, men heller "når", og da vil alle virksomhetene tjene på at dette blir oppdaget og varslet om så fort som mulig. Virksomheter og andre intervjuobjekter som ikke er i konkurranse har kommentert at sikkerhet er noe alle burde samarbeide om uavhengig av konkurranse. Det er mange som prøver å finne sikkerhetshull, og angriperene trenger bare å ha rett en gang, mens virksomhetene og andre må ha rett hele tiden.

Det er veldig varierende om virksomhetene har satte regler for deling eller ikke innad i sin virksomhet. Virksomhetene som har etablerte regler for deling, slik NIST rammeverket anbefaler at de å ha, deler konsekvent. Virksomhetene som ikke har regler deler de også, men i denne undersøkelsen er det mer deling blant virksomhetene som har satte regler, enn hos de uten. Det er ikke nødvendigvis en sammenheng her, for eksempel kan bruken av rammeverk som setter tydelige retningslinjer på hvordan virksomheten skal håndtere og rapportere en sikkerhetshendelse, også påvirke deling. Virksomhetene sine holdninger til deling har også mye å si, men det kan forsatt være en sammenheng mellom bruk av regler og deling.

Det er en felles kultur blant de fleste virksomhetene om å ha fokus på deling. Flertallet informerer om hvor nyttig deling er for virksomheten i forbindelse med økt kunnskap og lærdom. For noen virksomheter har det å dele med andre vært helt essensielt for å utvikle kompetansen og bli bedre på sikkerhet. Delingen har også gitt virksomheter muligheten til å oppdatere og sikre systemene sine mot et pågående angrep hos en annen virksomhet, for å hindre at de også selv blir utsatt,

slik som med Microsoft Exchange og Citrix sårbarhetene [51, 52].

Det er ikke mye informasjon virksomhetene ikke er villige å dele med NSM eller andre beredskapsorganisasjoner. Også de som ikke har en formell avtale med NSM er åpne for å dele med de. Grensen går i hovedsak på deling med media, hvor de fleste kun er villige til å dele informasjon om hendelser. Informasjonstyper som hvertfall ikke skal ut i det offentlige er sårbarheter og tiltak, da disse kan utnyttes av trusselaktører. Virksomhetene er også forsiktige med å dele informasjon om systemene de bruker, da trusselaktører i fremtiden kan lete etter sårbarheter i de spesifikke systemene. Hvor mange detaljer om en hendelse som deles varierer fra virksomhet til virksomhet, og noen er mer villige til å dele enn andre.

Undersøkelsen finner ingen konkret sammenheng mellom innføring av øvelser og økt åpenhet om sikkerhetshendelser. Det øvelser har ført til er økt kompetanse på hendelseshåndtering hos de ansatte, og forbedring av rutiner som ikke har vært ideelle. Forbedringen av rutiner gjør at virksomhetene står bedre stilt til å håndtere faktiske hendesler, som kan positivt påvirke deling da virksomheten kan legge vekt på god håndtering. Dermed kan øvelser være med på å påvirke åpenhet om sikkerhetshendelser.

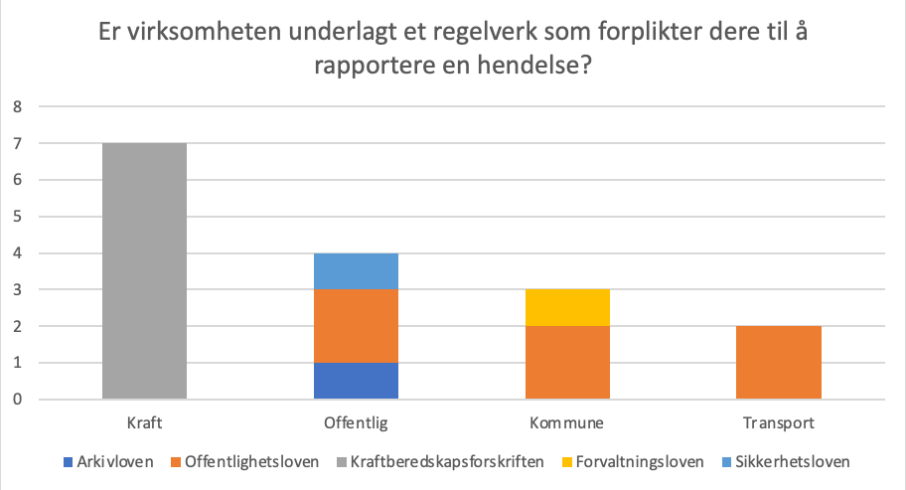
De fleste virksomhetene har ansatte med kompetanse innenfor sikkerhet og hendelseshåndtering, men ikke alle. De små og mellomstore virksomhetene har lite egen kompetanse på sikkerhet og hendelseshåndtering, men det er ingen tegn til at dette fører til mindre deling. To av disse har ikke hatt en hendelse, mens Avfall Sør har vært ute i media med sin. En mulig konsekvens av økt kompetanse og tilgang på ressurser er en større forståelse av hva slags informasjon som burde offentliggjøres og ikke, men det er ingen konkrete eksempler på dette her.

Faktorene som påvirker virksomheter sitt valg om åpenhet er meget like på tvers av alle virksomhetene. Når virksomhetene velger å ikke dele en hendelse med NSM eller andre samarbeidsorganer er dette fordi de ikke anser hendelsen som relevant. Dette er også den største årsaken for å ikke dele hendelser med media. Det er litt flere hensyn å ta før virksomheter deler med media, for eksempel er det situasjoner der virksomheter ikke deler en hendelse fordi det avslører sårbarheter i systemene til virksomheten.

Det er mer variasjon i faktorene som positivt påvirker valget om deling. Først og fremst ønsker virksomhetene å informere og hjelpe andre virksomheter slik at alle er forberedt på trusselen og kan sikre sine egne systemer, i tillegg til å sjekke om de selv er under angrep. Virksomhetene deler også for å få hjelp fra NSM eller andre beredskapsorganisasjoner. Det er vanskelig å stå i en stor hendelse, og mange virksomheter er ikke forberedt eller har ikke ressursene til å kunne beskytte seg mot angrep på den størrelsen.

Det er flere faktorer som må vurderes når en virksomhet tenker å dele med media. Hvis hendelsen påvirker kunder er det stor sannsynlighet for at de velger å gå ut. Det finnes også en del lovverk som gjør at virksomhetene ikke har noe valg i å dele hendelsen eller ikke. Dette betyr ikke nødvendigvis at det holdes en pressekonferanse, flere publiserer informasjonen som en pressemelding på sine nettsider, og så er det opp til media om den plukkes opp eller ikke. Oslo kommune sin hendelse i forbindelse med Microsoft Exchange sårbarheten ble plukket opp av media fordi deres rapportering av hendelsen var tilgjengelig for offentligheten [51, 53].

I samme periode var det en annen virksomhet i offentlig sektor som la ut en pressemelding om en annen hendelse, som ikke ble plukket opp av media. Årsaken til dette kan ha vært fordi media var opptatt med hackingen av Stortinget , eller at de bare ikke fikk det med seg [54]. Det er også noen virksomheter som velger å dele hendelser for å belyse problemet og fortelle offentligheten mer om hva som faktisk skjer i sikkerhetsverden. Figur 6.3 viser hvilke lovverk som forplikter virksomhetene til å rapportere en hendelse, utenom personvernloven fordi alle er dekket av denne. Igjen vises bare lovverk virksomhetene selv har nevnt, og ikke alle de nødvendigvis er underlagt

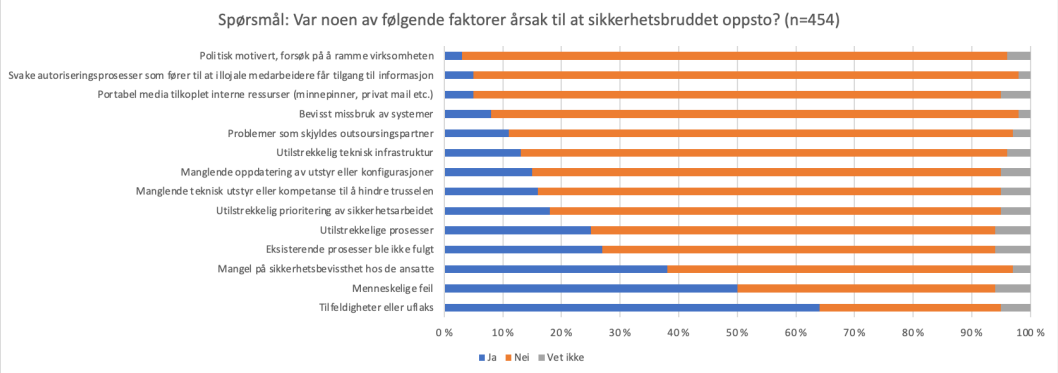


Figur 6.3: Spørsmål: Er bedriften underlagt et regelverk som forplikter bedriften/organisasjonen til å rapportere en hendelse?

Den største negative konsekvensen en virksomhet har opplevd er at media presenterer hendelsen feil, og at virksomheten i ettertid må ut og rette opp informasjon som ikke er korrekt. Dette har likevel ikke ført til at virksomheter lar være å dele hendelser i ettertid. Virksomhetene oppgir at de er mer forsiktige med hva slags informasjon og detaljer de deler offentlig, men de velger fortsatt å dele.

De to vanligste årsakene til at en sikkerhetshendelse oppstår hos intervjuobjektene

er menneskelig feil og feil hos tredjepartsleverandør, se figur 5.14. Andre årsaker gjelder også, men de har mindre hyppighet, og det er maks to virksomheter som har nevnt samme årsak. Både menneskelig feil og feil hos tredjepart går igjen hos alle sektorene, og det er minst en virksomhet i hver sektor som har nevnt en av disse.
Også mørketallsundersøkelsen trekker frem disse som årsaker for sikkerhetshendelser, men der kommer feil hos tredjepartsleverandør lengre ned, slik figur 6.4 viser. Siden undersøkelsen gjennomført i denne oppgaven dekker mange færre virksomheter, kan den høye frekvensen av årsaken være en tilfeldig konsentrasjon av mange virksomheter som har blitt påvirket av de kjente feilene hos tredjepartsleverandører [51, 52, 55]. At menneskelig feil er den vanligste årsaken er nok ikke en tilfeldighet, da den også er den nest mest nevnte årsaken i mørketallsundersøkelsen 2020. [4]



Figur 6.4: Fra mørketallsundersøkelsen: Var noen av følgende faktorer årsak til at sikkerhetsbruddet oppsto?

Alle virksomhetene som ble intervjuet bruker rammeverk for rapportering og håndtering av sikkerhetshendelser. Det er derfor vanskelig å finne sammenhenger mellom bruk av rammeverk og åpenhet om sikkerhetshendelser. Det samme gjelder for bruk av etablerte rutiner, og diskusjon rundt disse punktene blir derfor utelatt i denne undersøkelsen. Alle virksomhetene oppgir også at de etablerte rutinene følges i alle situasjoner, og undersøkelsen mangler derfor datagrunnlag til å analysere situasjoner der rutiner ikke overholdes.

6.3 Refleksjoner

Flere virksomheter føler et ansvar overfor andre i å være åpne om sikkerhetshendelser. Ansvarsfølelsen har ofte sitt grunnlag i deres posisjon og tilgang på ressurser. Flere av de mindre virksomhetene, og de som bare har et par hundre ansatte, har opplevd å få mer støtte og ressurser til arbeidet med sikkerhet etter

at andre har stått frem og vært åpen om en hendelse. Både de store og de små virksomhetene bruker andre sine hendelser til øvelser og lærdom også. Altså er det en tydelig fordel for andre virksomheter når en virksomhet velger å dele en hendelse med offentligheten.

Alle virksomhetene utenom en samarbeider om sikkerhet. Samarbeidet foregår både innad i en sektor og på tvers av de. Virksomhetene uttrykker et ønske om å bygge en kultur i virksomheten for samarbeid om sikkerhet både med konkurrenter og ikke konkurrenter. Mange legger vekt på viktigheten av samarbeid for å øke egen og nasjonens sikkerhet og motstandskraft, i møtet med et stadig utviklende trusselbilde.

Et problem som ble tatt opp av flere virksomheter under intervjuene er medias manglende kunnskap og forståelse for informasjonssikkerhet. Det var flere som trakk frem mediahåndteringen av den nyeste hendelsen på stortinget, hvor de hadde reagert på enkelte av spørsmålene som ble stilt [54]. De trekker spesielt frem at det ble spurt om det er flaut å bli hacket en gang til. For mange i sikkerhetsbransjen oppleves dette som urelevant og bidrar til å skape misforståelser rundt situasjonen. Media har en viktig rolle, og de skal stille de spørsmålene befolkningen lurer på, men ønsket er at journalistene har kunnskap om teknologi og sikkerhet på lik linje som sports- eller kulturjournalister har på sine fagområder. Da kan media fortsatt opprettholde rollen sin som formidler til befolkningen, men man kan potensielt unngå spørsmålene som skaper misforståelser og feiltolkninger av situasjonen.

6.4 Erfaringer knyttet til prosess

Prosessen med å skrive bacheloroppgaven har for det meste gått etter planen. Vedlegg D viser Gantt diagrammet som er en oversikt over planlagte frister og tidsrammer. Kun en av tidsfristene er ikke overholdt. Dette er fristen for å definere grupperingen av intervjuobjekter, som tok lenger tid å avklare enn først antatt. Den eneste konsekvensen dette kan ha medført er at rekruttering av virksomheter kanskje kunne begynt en uke tidligere. Intervjuprosessen startet til riktig tid og avsluttet innen gitt tidsfrist, som ble justert ned slik det er forklart i kapittel 3. Det ble likevel foretatt et intervju etter fristen, fordi virksomheten hadde blitt kontaktet sent i prosessen og tilhører transportsektoren der det var mangel på intervjuobjekter.

Videre har analyse av datainnsamlingen foregått som planlagt. Analysen har foregått underveis i gjennomførelsen av intervju samt i ettertid for å analysere de siste intervjuene. Arbeidet med analysen avsluttet cirka en uke før fristen. Ferdigstillingen av oppgaven ble startet og fullført før de satte tidspunktene. Første fullstendige gjennomlesing var ferdig til 03.05, slik at veiledere fikk en uke på å

lese gjennom oppgaven og gi tilbakemelding. Kun generering av forside og selve innleveringen sto igjen til 18.05. Gruppen opplever at oppgaven var godt planlagt og at det var lett å følge tidsplanen. Den største utfordringen var mangel på tid til å gjennomføre intervjuene, men å sette av mer tid ville gitt for liten tid til å gjennomføre analysen.

6.5 Begrensninger

Underveis i arbeidet dukket det opp punkter som kunne forbedres og burde gjennomføres på en annen måte. De største begrensningene i denne oppgaven er knyttet til intervjuobjektene. Først og fremst ble ikke målet på fem virksomheter per sektor nådd. Dette er noe som burde vært tilstede for en bedre analyse. I tillegg ble fordelingen av størrelsen på virksomheter veldig skjev, og analysen på tvers av størrelse kunne derfor ikke gjennomføres. Her kunne mer tid blitt brukt på å kontakte virksomheter, blant annet å ringe i stede for kun å sende e-post, slik at virksomhetene fikk enda tydeligere forklart hvorfor de var ønsket som intervjuobjekt.

Et annet problemområde er inndelingen i offentlig sektor. Innenfor den offentlige sektoren finnes det mange sektorer, men ikke alle disse er veldig store, slik som post og logistikk, og avfall. Disse sektorene er ikke store nok til å kunne brukes som egen sektor, men virksomhetene kan likevel ha verdifull input. Disse ble derfor samlet under ett i denne undersøkelsen, men det fører til at analysen ikke blir like representativ for sektoren. I tillegg finnes det offentlig eide virksomheter i de andre sektorene som er inkludert i denne undersøkelsen, noe som også kan være med på å påvirke resultatet.

I kapittel 3, beskrives det at enkelte store offentlige virksomheter ble kuttet fordi styringen var delt, og at ikke hele virksomheten hadde de samme rutinene. Det viste seg underveis at Oslo kommune også faller innenfor dette, så svarene fra det intervjuet er ikke nødvendigvis representativt for kommunen som en helhet.

Til slutt bør det også nevnes at spørsmålene burde vært mer spesifikke på når de refererer til sikkerhet og hendelseshåndtering generelt, og når de relaterer spesifikt til IT-sikkerhet og håndtering av IT-sikkerhetshendelser. Fordi datainnsamlingen ble gjort gjennom intervju og ikke spørreundersøkelse kunne disse forskjellene spesifiseres underveis, men det kan være situasjoner hvor forskjellen ikke ble presisert, og dette kan ha en innvirkning på resultatet.

6.6 Videre arbeid

Dette er et fagområde med rom for mye mer forskning og analyser, og det er mye videre arbeid som kan gjennomføres. Virksomhetene selv har foreslått at det kan gjøres en lignende undersøkelse på sikkerhetskultur og holdninger hos leverandørene, siden disse ofte er involvert i virksomhetene sine hendelser. Det ble også foreslått å gjøre en undersøkelse av mediehusene på samme tema, for å se deres nivå og holdninger og få innblikk i situasjonen fra deres side.

Det er også store muligheter for å gjennomføre analysen med fokus på størrelser i stede for sektorer, hvor det rekrutteres større antall virksomheter fra de ulike størrelsene. Et område som skulle diskuteres i denne oppgaven var konsekvenser av å dele sikkerhetshendelser med media i forhold til aksjekursen, men det viser seg at forskningen som de fleste refererer til har endret konklusjonen sin. Det bør derfor gjennomføres flere analyser som undersøker dette spesifikt, eventuelt vente til mer forskning publiseres på dette temaet for å diskutere dette nærmere. [56, 57]

Kapittel 7

Konklusjon

Den første hypotesen oppgaven tar for seg handler om at virksomhetene ikke deler informasjon om sikkerhetshendelser av frykt for tap av omdømme. Resultatet av denne undersøkelsen inneholder ingen informasjon som bekrefter denne hypotesen, kanskje tvert imot. Virksomhetene er redde for tap av omdømme, men ikke på grunn av hendelsen i seg selv. Problemene virksomhetene har tilknyttet dette er situasjoner der media uttaler seg feil om hendelser. Det er ingen som har nevnt frykt for tap av omdømme som en direkte årsak til at de ikke har delt en hendelse. Dermed kan hypotesen verken bekreftes eller avkreftes, men ingen av intervjuobjektene i denne undersøkelsen opplever dette som veldig treffende.

Den andre hypotesen og det siste forskningspørsmålet spør om det er en sammenheng mellom åpenhet om sikkerhetshendelser og om ledelsen er involvert i håndteringen av de. Basert på funnene i denne undersøkelsen er det lite sammenheng. Her blir ledelsen inkludert i håndteringen av store hendelser og/eller i avgjørelsen om åpenhet hos samtlige virksomheter. Om dette resultatet er representativt for norske virksomheter er usikkert, i mørketallsundersøkelsen inkluderer 69% av 454 virksomheter ledelsen, men der er det ikke gjort en analyse på sammenhengen med åpenhet om hendelser. Det kan forsatt være en sammenheng, men en større undersøkelse må gjennomføres for å kunne si noe sikkert.

Det første forskningsspørsmålet dekker hvilke faktorer som er med på å påvirke virksomheter sitt valg om åpenhet til offentligheten. Oppfatning av relevans står sentralt, fordi hva virksomheten anser som relevant eller ikke er med på å avgjøre hva som vil bli delt med media. Hvordan hendelsen påvirker kunden, og om den avslører sensitiv informasjon om virksomheten, er også viktige faktorer. Lovverk spiller en sentral rolle fordi flere lovverk både står til hinder for åpenhet, og stiller krav til rapportering av hendelser. Til slutt trekkes det frem at virksomheter deler hendelser med media for å informere og hjelpe andre virksomheter.

Det andre forskningsspørsmålet dekker hvilke faktorer som er med på å påvirke deling av informasjon med NSM. Her står ønsket om å dele for å hjelpe andre virk-

somheter sterkt. De større virksomhetene påtar seg et naturlig ansvar for deling, som bidrar til økt kunnskap og tilgang på ressurser for de mindre virksomhetene. I tillegg kan NSM og andre beredskapsorganisasjoner bidra med hjelp og støtte til håndtering av hendelser, noe som motiverer virksomheter til å dele med disse.

Det tredje forskningsspørsmålet spør om hvilke faktorer som varierer mellom sektorene. Den eneste faktoren som påvirker valget om åpenhet som varier mellom sektorene er lovverk. I offentlig- og kommunesektoren er det offentlighetsloven som stiller flest krav til deling av hendelser. Kraftberedskapsforskriften stiller både krav til hemmelighold og rapportering av hendelser i kraftsektoren. Disse lovverkene holder ofte tilbake informasjon som kan avsløre sårbarheter hos virksomhetene, som er en av hovedårsakene til at åpenhet er et dilemma. Flertallet av virksomhetene har et tydelig ønske om å være åpen og dele på tvers av virksomheter og/eller sektor, men opplever at det ikke alltid er like lett å dele.

Det altså flere faktorer som påvirker virksomheter i valget om åpenhet. Hva som påvirker deling med NSM, og hva som påvirker deling med media varierer. Faktorene med mest betydning i denne undersøkelsen er hva virksomhetene anser som relevant, ønsket om å hjelpe andre virksomheter, behovet for hjelp, og lovverk.

Bibliografi

[1] Norsk Senter for Informasjonssikring - NorSIS. (mai 2020). «Cyberangrepsforsøk mot norske virksomheter økte kraftig i april.» Sist sjekket: 31.01.21, adresse: https://norsis.no/cyberangrepsforsok-mot-norske-virksomheter-okte-kraftig-i-april/.

[2] Utenriksdepartementet, *Datainnbruddet i Stortinget*. adresse: https://www.regjeringen.no/no/aktuelt/pm_inbrudd/id2770135/.

[3] H. A. Solbakken. (). «Sensitiv pasientinformasjon kan være på avveie etter dataangrep,» adresse: https://www.nrk.no/innlandet/ostre-toten-kommune-angrepet-av-hackere-_-pasientinformasjon-og-helsedata-kan-vaere-pa-avveie-1.15321398.

[4] Næringslivets sikkerhetsråd, «Mørketallsundersøkelsen 2020,» 2020.

[5] A. B. Jensen. (jan. 2019). «"Holder dataangrep hemmelig: – Skip er blitt smittet med virus, og har måttet slepes til dokk".» Hentet: 15.02.21, adresse: https://www.tu.no/artikler/dnv-gl-svaert-uheldig-at-ikke-flere-selskaper-er-apne-om-dataangrep/456148?key=eW9RCGdp.

[6] Forsvaret. (2017). «Forsvarets innbyggerundersøkelse 2017.»

[7] Forsvaret, «Forsvarets innbyggerundersøkelse 2020,» 2020.

[8] F. S. Nilsen og E. Bøe. (des. 2020). «Hurtigruten utsatt for omfattende dataangrep.» Sist sjekket: 31.01.21, adresse: https://e24.no/naeringsliv/i/BlrBVv/hurtigruten-utsatt-for-omfattende-dataangrep.

[9] M. B. Røise. (des. 2020). «Hackere tok ned vinmonopolet.» Sist sjekket: 31.01.21, adresse: https://www.digi.no/artikler/hackerne-tok-ned-vinmonopolet-no-i-dag-har-de-varslet-et-mye-verre-angrep/504268?key=SEmLthuY.

[10] J. Birkeland. (nov. 2020). «Mer åpenhet rundt cybertrusler.» Sist sjekket: 31.01.21, adresse: https://www.cw.no/artikkel/sikkerhet/mer-apenhet-rundt-cybertrusler.

[11] N. Hovedorganisasjon. (sep. 2020). «Små og mellomstore bedrifter.» Sist sjekket: 03.02.21, adresse: https://www.nho.no/tema/sma-og-mellomstore-bedrifter/artikler/sma-og-mellomstore-bedrifter-smb/.

[12] Nasjonal Sikkerhetsmyndighet, «Risiko 2020,» apr. 2020.

[13] NSM. (jan. 2020). «Begrepsliste til bruk for rammeverk for ha ndtering av IKT-sikkerhetshendelser.» Hentet: 20.01.21 og 24.02.21, adresse: https://nsm.no/getfile.php/133863-1593022742/Demo/Dokumenter/vedlegg-4---begrepsliste.pdf.

[14] Nettvett. (sep. 2019). «Hendelseshåndtering.» Hentet: 24.02.21, adresse: https://nettvett.no/hendelseshandtering/.

[15] I. Sagberg. (apr. 2021). «Ledelse.» Hentet: 12.05.21, adresse: https://snl.no/ledelse.

[16] NSM. (jan. 2020). «Sikkerhetsloven og forskrifter.» Hensikt: 10.02.21, adresse: https://nsm.no/regelverk-og-hjelp/sikkerhetsloven-og-forskrifter/.

[17] Lovdata. (jan. 2020). «Lov om nasjonal sikkerhet (Sikkerhetsloven).» Hentet: 10.02.21, adresse: https://lovdata.no/dokument/NL/lov/2018-06-01-24?q=sikkerhetsloven.

[18] Lovdata. (jan. 2020). «Lov om nasjonal sikkerhet (Sikkerhetsloven).» Hentet: 10.02.21, adresse: https://lovdata.no/dokument/NL/lov/2018-06-01-24?q=sikkerhetsloven.

[19] Lovdata. (jul. 2018). «Lov om behandling av personopplysninger (Personopplysningsloven).» Hentet: 10.02.21, adresse: https://lovdata.no/dokument/NL/lov/2018-06-15-38/KAPITTEL_gdpr-4-2#KAPITTEL_gdpr-4-2.

[20] Lovdata. (jul. 2018). «Lov om behandling av personopplysninger (Personopplysningsloven).» Hentet: 10.02.21, adresse: https://lovdata.no/dokument/NL/lov/2018-06-15-38/KAPITTEL_gdpr-4-2#KAPITTEL_gdpr-4-2.

[21] Lovdata. (jul. 2018). «Lov om behandling av personopplysninger (Personopplysningsloven).» Hentet: 10.02.21, adresse: https://lovdata.no/dokument/NL/lov/2018-06-15-38/KAPITTEL_2#KAPITTEL_2.

[22] C. Johnson, L. Badger, D. Waltermire, J. Snyder og C. Skorupka, «Guide to Cyber Threat Information Sharing,» *NIST Special Publication*, årg. 800-150, 2016. DOI: http://dx.doi.org/10.6028/NIST.SP.800-150.

[23] C. Goodwin og J. P. Nicholas, «A framework for cybersecurity information sharing and risk reduction,» 2015.

[24] Microsoft Security. (jan. 2015). «Putting Information Sharing into Context.» Hentet: 16.02.21, adresse: https://www.microsoft.com/security/blog/2015/01/27/putting-information-sharing-into-context/.

[25] Cybersecurity and Infrastructure Security Agency. (). «Traffic Light Protocol (TLP) Definitions and Usage.» Hentet: 26.04.21, adresse: https://www.cisa.gov/tlp.

[26] AXELOS. (). «What is ITIL®?» Hentet: 16.02.21, adresse: https://www.axelos.com/best-practice-solutions/itil/what-is-itil.

[27] AXELOS, *ITIL Foundation*, 4th Edition. The Stationary Office (TSO), 2019.

[28] N. sikkerhetsråd. (). «Publikasjoner.» Hentet: 12.05.21, adresse: https://www.nsr-org.no/produkter-og-tjenester/publikasjoner/morketallsundersokelsen.

[29] Lovdata. (jan. 2013). «Forskrift om sikkerhet og beredskap i kraftforsyningen (Kraftberedskapsforskriften).» Hentet: 16.03.21, adresse: https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157?q=beredskapsforskriften#KAPITTEL_1.

[30] Lovdata. (jan. 2009). «Lov om rett til innsyn i dokument i offentleg verksemd (Offentleglova).» Hentet: 16.03.21, adresse: https://lovdata.no/dokument/NL/lov/2006-05-19-16?q=offentlighetsloven.

[31] Regjeringen. (jan. 1997). «St.meld. nr. 32 (1997-98).» Hentet: 03.05.21, adresse: https://www.regjeringen.no/no/dokumenter/stmeld-nr-32-1997-98-/id191621/?ch=4.

[32] Arkivverket. (2020). «Arkivloven.» Hentet: 03.05.21, adresse: https://www.arkivverket.no/forvaltning-og-utvikling/regelverk-og-standarder/lover-og-forskrifter-for-arkiv/arkivloven.

[33] Regjeringen. (2017). «Nytt anskaffelsesregelverk.» Hentet: 04.05.21, adresse: https://www.regjeringen.no/no/tema/naringsliv/konkurransepolitikk/offentlige-anskaffelser-/forste-kolonne/nytt-anskaffelsesregelverk/id2518659/.

[34] Regjeringen. (2018). «Virkeområde for forsyningsforskriften.» Hentet: 04.05.21, adresse: https://www.regjeringen.no/no/tema/naringsliv/konkurransepolitikk/offentlige-anskaffelser-/andre-kolonne/virkeomrade-for-forsyningsforskriften/id2598956/.

[35] Standard Norge. (2021). «NS-EN ISO/IEC 27001 Ledelsessystemer for informasjonssikkerhet - Krav.» Hentet: 12.05.21, adresse: https://www.standard.no/fagomrader/ikt/it-sikkerhet/isoiec-27001/.

[36] Nasjonal Sikkerhetsmyndighet. (aug. 202). «Grunnprinsipper for IKT-sikkerhet.» Hentet: 12.05.21, adresse: https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/grunnprinsipper-ikt.

[37] Lucidchart. (). «Flowchart Symbols and Notation.» Henter: 25.04.21, adresse: https://www.lucidchart.com/pages/flowchart-symbols-meaning-explained.

[38] G. Andersen. (jan. 2019). «Valg av forskningsmetode.» Hentet: 19.04.21, adresse: https://ndla.no/nb/subject:19/topic:1:195989/topic:1:195829/resource:1:56937?filters=urn:filter:f3d2143b-66e3-428c-89ca-72c1abc659ea.

[39] Norsk Industri. (). «Bransjer i Norsk Industri.» Hensikt: 24.02.21, adresse: https://www.norskindustri.no/bransjer/.

[40] Regjeringen.no. (2020). «Hva staten eier.» Hentet: 24.02.21, adresse: https://www.regjeringen.no/no/tema/naringsliv/statlig-eierskap/selskaper---ny/id2604524/.

[41] NVE. (jan. 2021). «Eierskap i norsk vann- og vindkraft.» Hentet: 24.02.21, adresse: https://www.nve.no/energiforsyning/kraftmarkedsdata-og-analyser/eierskap-i-norsk-vann-og-vindkraft/?ref=mainmenu.

[42] NHO. (). «Fakta om små og mellomstore bedrifter (SMB).» Hentet: 24.02.21, adresse: https://www.nho.no/tema/sma-og-mellomstore-bedrifter/artikler/sma-og-mellomstore-bedrifter-smb/.

[43] K. L. Vik. (aug. 2020). «NVivo.» Hentet: 13.05.21, adresse: https://innsida.ntnu.no/wiki/-/wiki/Norsk/NVivo.

[44] QSR International. (2021). «QSR International Global Data Privacy Policy.» Hentet: 06.04.21, adresse: https://www.qsrinternational.com/privacy-policy.

[45] NVIVO. (). «Data security and privacy.» Hentet: 06.04.21, adresse: https://help.mynvivo.com/nvtranscription/Content/NVT_data_security.htm.

[46] Enova. (). «Om Enova.» Hentet: 03.05.21, adresse: https://www.enova.no/om-enova/.

[47] Avfall sør. (). «Våre innsamlingsordninger.» Hentet: 03.05.21, adresse: https://avfallsor.no/henting-av-avfall/vare-ordninger/.

[48] J. E. Heftøy. (jan. 2020). «Dessverre en naturlig konsekvens.» Hentet: 03.05.21, adresse: https://avfallsbransjen.no/2020/01/31/10103/.

[49] Digi. (2019). «Hydro er fortsatt ikke friskmeldt etter dataangrepet i mars.» Hentet: 12.05.21, adresse: https://www.digi.no/artikler/hydro-er-fortsatt-ikke-friskmeldt-etter-dataangrepet-i-mars/464771.

[50] S. Salem-Schatz, D. Ordin og B. Mittman. (2010). «Guide to the After Action Review.» Hentet: 13.05.21, adresse: https://www.cebma.org/wp-content/uploads/Guide-to-the-after_action_review.pdf.

[51] M. B. Jørgenrud. (2021). «Titusener utsatt for angrep mot kritisk Exchange-sårbarhet. NSM ser angrep også mot servere i Norge.» Hentet: 22.04.21, adresse: https://www.digi.no/artikler/titusener-utsatt-for-angrep-mot-kritisk-exchange-sarbarhet-nsm-ser-angrep-ogsa-mot-servere-i-norge/507638.

[52] M. B. Jørgenrud. (jan. 2020). «Angripere skanner nettet etter sårbare Citrix-servere.» Hentet: 22.04.21, adresse: https://www.digi.no/artikler/angripere-skanner-nettet-etter-sarbare-citrix-servere/482600.

[53] NRK. (2021). «Oslo rådhus utsatt for dataangrep.» Hentet: 22.04.21, adresse: https://www.nrk.no/osloogviken/oslo-radhus-utsatt-for-dataangrep-1.15428162.

[54] E. Alnes, K. Skårdalsmo, M. Gundersen, L. Tomter og J. K. Thommessen. (2021). «Stortinget er utsett for dataangrep – data skal vere henta ut.» Hentet: 22.04.21, adresse: https://www.nrk.no/norge/stortinget-utsett-for-nytt-dataangrep-1.15411279.

[55] Nasjonal sikkerhetsmyndighet. (2020). «Sårbarhet i SolarWinds Orion.» Hentet: 22.04.21, adresse: https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/varsler-fra-ncsc/sarbarhet-i-solarwinds-orion.

[56] P. Bischoff. (nov. 2019). «How data breaches affect stock market share prices.» Hentet: 05.05.21, adresse: https://web.archive.org/web/20191123205642/https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/.

[57] P. Bischoff. (feb. 2021). «How data breaches affect stock market share prices.» Hentet: 05.05.21, adresse: https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/.

Vedlegg A

Prosjektavtale

Prosjektavtale med NTNU og oppdragsgiver.

NTNU

Vår dato Vår referanse

Norges teknisk-naturvitenskapelige universitet

Prosjektavtale

mellom NTNU Fakultet for informasjonsteknologi og elektroteknikk (IE) på Gjøvik (utdanningsinstitusjon), og

_____

_____ (oppdragsgiver), og

_____

_____

_____ (student(er))

Avtalen angir avtalepartenes plikter vedrørende gjennomføring av prosjektet og rettigheter til anvendelse av de resultater som prosjektet frembringer:

1. Studenten(e) skal gjennomføre prosjektet i perioden fra _____ til_____ .

   Studentene skal i denne perioden følge en oppsatt fremdriftsplan der NTNU IE på Gjøvik yter veiledning. Oppdragsgiver yter avtalt prosjektbistand til fastsatte tider. Oppdragsgiver stiller til rådighet kunnskap og materiale som er nødvendig for å få gjennomført prosjektet. Det forutsettes at de gitte problemstillinger det arbeides med er aktuelle og på et nivå tilpasset studentenes faglige kunnskaper. Oppdragsgiver plikter på forespørsel fra NTNU å gi en vurdering av prosjektet vederlagsfritt.

2. Kostnadene ved gjennomføringen av prosjektet dekkes på følgende måte:
   - Oppdragsgiver dekker selv gjennomføring av prosjektet når det gjelder f.eks. materiell, telefon/fax, reiser og nødvendig overnatting på steder langt fra NTNU på Gjøvik. Studentene dekker utgifter for ferdigstillelse av prosjektmateriell.
   - Eiendomsretten til eventuell prototyp tilfaller den som har betalt komponenter og materiell mv. som er brukt til prototypen. Dersom det er nødvendig med større og/eller spesielle investeringer for å få gjennomført prosjektet, må det gjøres en egen avtale mellom partene om eventuell kostnadsfordeling og eiendomsrett.

3. NTNU IE på Gjøvik står ikke som garantist for at det oppdragsgiver har bestilt fungerer etter hensikten, ei heller at prosjektet blir fullført. Prosjektet må anses som en eksamensrelatert oppgave som blir bedømt av intern og ekstern sensor. Likevel er det en forpliktelse for utøverne av prosjektet å fullføre dette til avtalte spesifikasjoner, funksjonsnivå og tider.

4. Alle bacheloroppgaver som ikke er klausulert og hvor forfatteren(e) har gitt sitt samtykke til publisering, kan gjøres tilgjengelig via NTNUs institusjonelle arkiv hvis de har skriftlig karakter A, B eller C.

Tilgjengeliggjøring i det åpne arkivet forutsetter avtale om delvis overdragelse av opphavsrett, se «avtale om publisering» (jfr Lov om opphavsrett). Oppdragsgiver og veileder godtar slik offentliggjøring når de signerer denne prosjektavtalen, og må evt. gi skriftlig melding til studenter og instituttleder/fagenhetsleder om de i løpet av prosjektet endrer syn på slik offentliggjøring.

Den totale besvarelsen med tegninger, modeller og apparatur så vel som programlisting, kildekode mv. som inngår som del av eller vedlegg til besvarelsen, kan vederlagsfritt benyttes til undervisnings- og forskningsformål. Besvarelsen, eller vedlegg til den, må ikke nyttes av NTNU til andre formål, og ikke overlates til utenforstående uten etter avtale med de øvrige parter i denne avtalen. Dette gjelder også firmaer hvor ansatte ved NTNU og/eller studenter har interesser.

5. Besvarelsens spesifikasjoner og resultat kan anvendes i oppdragsgivers egen virksomhet. Gjør studenten(e) i sin besvarelse, eller under arbeidet med den, en patentbar oppfinnelse, gjelder i forholdet mellom oppdragsgiver og student(er) bestemmelsene i Lov om retten til oppfinnelser av 17. april 1970, §§ 4-10.

6. Ut over den offentliggjøring som er nevnt i punkt 4 har studenten(e) ikke rett til å publisere sin besvarelse, det være seg helt eller delvis eller som del i annet arbeide, uten samtykke fra oppdragsgiver. Tilsvarende samtykke må foreligge i forholdet mellom student(er) og faglærer/veileder for det materialet som faglærer/veileder stiller til disposisjon.

7. Studenten(e) leverer oppgavebesvarelsen med vedlegg (pdf) i NTNUs elektroniske eksamenssystem. I tillegg leveres ett eksemplar til oppdragsgiver.

8. Denne avtalen utferdiges med ett eksemplar til hver av partene. På vegne av NTNU, IE er det instituttleder/faggruppeleder som godkjenner avtalen.

9. I det enkelte tilfelle kan det inngås egen avtale mellom oppdragsgiver, student(er) og NTNU som regulerer nærmere forhold vedrørende bl.a. eiendomsrett, videre bruk, konfidensialitet, kostnadsdekning og økonomisk utnyttelse av resultatene. Dersom oppdragsgiver og student(er) ønsker en videre eller ny avtale med oppdragsgiver, skjer dette uten NTNU som partner.

10. Når NTNU også opptrer som oppdragsgiver, trer NTNU inn i kontrakten både som utdanningsinstitusjon og som oppdragsgiver.

11. Eventuell uenighet vedrørende forståelse av denne avtale løses ved forhandlinger avtalepartene imellom. Dersom det ikke oppnås enighet, er partene enige om at tvisten løses av voldgift, etter bestemmelsene i tvistemålsloven av 13.8.1915 nr. 6, kapittel 32.

12. Deltakende personer ved prosjektgjennomføringen:

NTNUs veileder (navn): _____

Oppdragsgivers kontaktperson (navn): _____

Student(er) (signatur): _____ dato _____

_____ dato _____

_____ dato _____

_____ dato _____

Oppdragsgiver (signatur):_____ dato _____

Signert avtale leveres digitalt i Blackboard, rom for bacheloroppgaven.
Godkjennes digitalt av instituttleder/faggruppeleder.

Om papirversjon med signatur er ønskelig, må papirversjon leveres til instituttet i tillegg.
Plass for evt sign:

Instituttleder/faggruppeleder (signatur): _____ dato _____

Vedlegg B

Intervjuguide

Den komplette intervjuguiden med alle spørsmål, teori og hensikt.

Kategori 1: Strategiske valg/kommunikasjonsstrategi

1.1	**Teori**: IKT-sikkerhetshendelse: «Tilsiktede uønskede hendelser eller trusler om slike hendelser i det digitale rom som er rettet mot kritisk infrastruktur og /eller kritiske samfunnsfunksjoner» (NSM, 2017:3). Definisjon fra nettvett: "En sikkerhetshendelse er en aktivitet eller situasjon som har forårsaket skade på eller truer personell, informasjon eller andre verdier." **Spørsmål**: Dette er NorSIS sin definisjon av en sikkerhetshendelse. Er dette en passende definisjon for deres bedrift, eller definerer dere det på en annen måte? **Hensikt**: Hensikten med spørsmålet er å kartlegge de ulike definisjonene som benyttes og avgjøre om det er en felles enighet om hva en sikkerhetshendelse er.

1.2	**Teori**: Se sikkerhetsloven, kap 4 § 4-1: sikkerhetsstyring. Virksomhetens leder har ansvar for det forebyggende sikkerhetsarbeidet. Se også sikkerhetsloven, kap 4 § 4-4: krav til dokumentasjon. Virksomheten skal dokumentere vurderingen av risiko og de gjennomførte og planlagte sikkerhetstiltakene. 7 av 10 bedrifter har et rammeverk og/eller et styringssystem for informasjonssikkerhet (se mørketallsrapporten). Rapportering til datatilsynet → se personopplysningssikkerhetsloven, artikkel 33: Melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten. Ved brudd på personopplysningssikkerheten skal den behandlingsansvarlige uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til det, melde bruddet til vedkommende tilsynsmyndighet i samsvar med artikkel 55, med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter. Dersom bruddet ikke meldes til tilsynsmyndigheten innen 72 timer, skal årsakene til forsinkelsen oppgis. **Spørsmål**: Har bedriften/organisasjonen et rammeverk for håndtering og rapportering av sikkerhetshendelser? **Hensikt**: Hensikten med spørsmålet er å se om bruk av rammeverk har noe å si for deling, blant annet se på om de som bruker rammeverk deler mer.

1.3	**Teori**: Referer til spesifikke bedrifter i media knyttet til deling av hendelser. **Spørsmål**: Hvem skal avgjøre om bedriften er åpne om hendelser eller ikke? På hvilket ledelsesnivå er vedkommende? **Hensikt**: Hensikten med spørsmålet er å se om hvilket nivå denne avgjørelsen tas på har en påvirkning på om man deler.

1.4	**Teori**: Microsoft har et rammeverk for deling av cybersikkerhetsinformasjon, der de beskriver de fire vanligste måtene å dele informasjon på. Formelt: Gjennom avtalte kanaler eller kontrakter. I forhold der man har en NDA eller annen type kontrakt, gjennom medlemskap i ulike organer som MAPP og nasjonale eller sektor CERT Sikkerhetsklareringsbasert: En mer spesifisert versjon av et formelt samarbeid, typisk brukt av etteretningstjenester for å dele klassifisert informasjon Tillitsbasert: Gjennom grupper med likesinnede bedrifter. Deler oftere når det skjer noe, ikke periodisk. Bruker ofte TLP systemet for klassifisering av informasjonen Episodisk (ad hoc): Deler når det oppstår nye situasjoner man ikke har vært borti før, ofte fordi man trenger hjelp eller ønsker å advare andre bedrifter om en ny trussel **Spørsmål**: Deler dere informasjon periodisk, gjennom for eksempel en formell avtale, eller gjøres det heller en vurdering når en hendelse først inntreffer? **Hensikt**: Hensikten med spørsmålet er å se på om bedrifter er mer åpne for å dele informasjon om hendelser om de allerede deler annen informasjon periodisk.

1.4.1	**Teori**: Se 1.4 **Spørsmål**: Samarbeider bedriften om sikkerhet med andre innenfor samme sektor? **Hensikt**: Hensikten med spørsmålet er å analysere sikkerhetskulturen innenfor de ulike sektorene

1.4.2	**Teori**: Se 1.4 **Spørsmål**: Har bedriften gjort et bevisst valg om å dele/ikke dele med konkurrenter? **Hensikt**: Hensikten med spørsmålet er å analysere om konkurranse har en negativ effekt på utbyggingen av en god sikkerhetskultur innenfor en sektor

1.5	**Teori**: ITIL rammeverket legger vekt på verdien en bedrift får ut av det de gjennomfører. Er risikoen og kostnaden større enn verdien av utkomme er det ikke lønnsomt for bedriften å gjennomføre handlingen. **Spørsmål**: Har bedriften gjennomført en risikovurdering i forhold til å dele informasjon med andre bedrifter? Isåfall, hva er de største risikoene ved å dele? **Hensikt**: Hensikten med spørsmålet er å finne ut hva som får bedrifter til å ikke dele og se om det er noe NSM kan gjøre for å redusere noen av de nevnte risikoene

1.6	**Teori**: NIST Guide to Cyber Threat Information Sharing oppfordrer bedrifter å etablere regler for informasjonsdeling, og mener dette vil kunne hjelpe å kontrollere spredning av informasjonen og hindre negative konsekvenser. **Spørsmål**: Har dere noen regler for deling? Hvis ja, hva er de? **Hensikt**: Hensikten med spørsmålet er å vurdere om innføring av regler har gjort det lettere for bedrifter å dele eller om de har delt mer fordi de har satte regler.

1.7	**Teori**: NIST Guide to Cyber Threat Information Sharing anbefaler bedrifter å sette mål og ønsket utfall for deling for å hjelpe organisasjonen finne ut om hvordan deling bør foregå i forhold til hva og med hvem. **Spørsmål**: Har bedriften noen satte mål for hva dere ønsker å oppnå med å dele? **Hensikt**: Hensikten med spørsmålet er å se på hva bedrifter ønsker å få ut av å dele og se om NSM kan bruke svarene i sitt arbeid med å få flere til å dele.

1.8	**Teori**: I Microsoft sitt rammeverk for deling av cybersikkerhetsinformasjon beskriver de disse typene informasjon man kan dele: Hendelser: Informasjon om forsøkte og vellykkede angrep, som hva slags data som er tapt, teknikker som er brukt og mål og konsekvens for angrepet Trusler: Mulig uønsket handling som kan gi en negativ konsekvens (fra NSM sin begrepsliste) Sårbarheter: Sårbarheter i programvare, hardware og business prosesser som kan utnyttes Tiltak: Metoder for å begrense sårbarhetene og/eller hindre trusler, slik at konsekvens og/eller sannsynlighet for en risiko reduseres Situasjonsdata: Informasjon om nylige hendelser og trusler som gir bedrifter et bedre grunnlag for å respondere på hendelser Beste praksis: Informasjon om gunstige gjøremåter og metoder, som anbefalte sikkerhetskontroller og når patching bør foregå Strategiske analyser: Beregninger av trender og forventede utfall bedrifter gjør for å forberede seg på fremtidige risikoer **Spørsmål**: Hva slags type informasjon ville dere ikke delt med NSM, National Cyber Security Centre (NCSC) og andre beredskapsorganisasjoner, eller media? **Hensikt**: Hensikten med spørsmålet er å se om bedrifter er mindre villige til å dele enkelte typer informasjon.

1.9	**Teori**: Se 1.8 **Spørsmål**: Hva slags type informasjon ville dere delt med NSM, NCSC og andre beredskapsorganisasjoner, og ikke media? **Hensikt**: Hensikten med spørsmålet er å se om bedrifter er mer villige til å dele enkelte typer informasjon med NSM som de ikke er villige til å dele med media.

1.10	**Teori**: Se 1.8 **Spørsmål**: Hva slags type informasjon ville dere delt til media? **Hensikt**: Hensikten med spørsmålet er å se om bedrifter er mer villige til å dele enkelte typer informasjon med media.

Kategori 2: Regelverk

2.1	**Teori**: Åpen informasjon er informasjon som ved lovlig fremgangsmåte er tilgjengelig for alle som ønsker å finne den. Verdien av enkeltbiter av åpen informasjon trenger ikke isolert sett å være stor. **Spørsmål**: Dette er NSM sin definisjon på åpen informasjon. Er dette en passende definisjon for deres bedrift, eller definerer dere det på en annen måte? **Hensikt**: Hensikten med spørsmålet er å kartlegge de ulike definisjonene som benyttes og avgjøre om det er en felles enighet om hva åpenhet er.

2.2	**Teori**: Se personopplysninsgssikkerhetssloven, artikkel 33: melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten. Se politiregisterloven, kap 5 § 19: Generelt om utlevering av opplysninger. Se politiregisterloven, kap 6 § 23: Omfanget av taushetsplikten. Se pasientjournalloven kap 3 § 15: Taushetsplikt. Se helseregisterloven kap 2 § 16: Plikt til å innrapportere data til statistikk. Se helseregisterloven kap 3 § 1: Taushetsplikt. **Spørsmål**: Er bedriften/organisasjonen underlagt noe lovverk som hindrer dere i å være åpne om sikkerhetshendelser? **Hensikt**: Hensikten med spørsmålet er å identifisere lovverk som påvirker valget om åpenhet for å separere frivillig og tvungen deling.

2.3	**Teori**: Dersom bedriften/organisasjonen er underlagt sikkerhetsloven, se kapittel 4, § 4-5: varslingsplikt. **Spørsmål**: Er bedriften underlagt et regelverk som forplikter bedriften/organisasjonen til å rapportere en hendelse? **Hensikt**: Hensikten med spørsmålet er å identifisere lovverk som påvirker valget om åpenhet for å separere frivillig og tvungen deling.

Kategori 3: Rutiner og prosesser

3.1	**Teori**: Refererer tilbake til definisjonen på en sikkerhetshendelse som er: En sikkerhetshendelse er en aktivitet eller situasjon som har forårsaket skade på eller truer personell, informasjon eller andre verdier. **Spørsmål**: Har bedriften hatt en sikkerhetshendelse? **Hensikt:** Hensikten med spørsmålet er å identifisere hvor mange av intervjuobjektene som har hatt en sikkerhetshendelse.

3.2	**Teori**: Se sikkerhetsloven, kap 4 § 4-1: sikkerhetsstyring. Virksomhetens leder har ansvar for det forebyggende sikkerhetsarbeidet. Se også sikkerhetsloven, kap 4 § 4-4: krav til dokumentasjon. Virksomheten skal dokumentere vurderingen av risiko og de gjennomførte og planlagte sikkerhetstiltakene. 7 av 10 bedrifter har et rammeverk og/eller et styringssystem for informasjonssikkerhet (se mørketallsrapporten). Rapportering til datatilsynet → se personopplysningssikkerhetsloven, artikkel 33: Melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten. Ved brudd på personopplysningssikkerheten skal den behandlingsansvarlige uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til det, melde bruddet til vedkommende tilsynsmyndighet i samsvar med artikkel 55, med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter. Dersom bruddet ikke meldes til tilsynsmyndigheten innen 72 timer, skal årsakene til forsinkelsen oppgis. **Spørsmål**: Har bedriften/organisasjonen rutiner for håndtering og rapportering av sikkerhetshendelser? Med håndtering mener vi her hvem som delegerer oppgaver og har ansvar for å følge opp i etterkant og kanskje rapportere lengre opp i systemet. **Hensikt**: Hensikten med spørsmålet er å se om etablerte rutiner for hendelseshåndtering er en påvirkende faktor i bedrifters valg om å være åpne.

3.2.1	**Teori**: Se 3.2 **Spørsmål**: Følger dere faktisk disse rutinene når en sikkerhetshendelse oppstår? **Hensikt**: Hensikten med spørsmålet er å oppdage situasjoner der bedrifter ikke følger rutiner og om det kan være med å påvirke valget rundt åpenhet.

3.2.2	**Teori**: Se sikkerhetsloven kap 4, § 4-1: sikkerhetsstyring: Virksomhetens leder har ansvaret for det forebyggende sikkerhetsarbeidet. Forebyggende sikkerhetsarbeid skal være en del av virksomhetens styringssystem. Sikkerhetstilstanden i virksomheten skal regelmessig kontrolleres. Virksomheten skal sørge for at ansatte, leverandører og oppdragstakere har tilstrekkelig risiko- og sikkerhetsforståelse. For leverandører til sikkerhetsgraderte anskaffelser gjelder kapittel 9. **Spørsmål**: På hvilket ledelsesnivå blir sikkerhetshendelser håndtert i bedriften/organisasjonen? **Hensikt**: Hensikten med spørsmålet er å identifisere hvilke ledelsesnivå som involveres i de ulike bedriftene og om det er en sammenheng mellom involvert ledelsesnivå og valg om åpenhet.

3.2.3	**Teori:** Se 3.2.2 **Spørsmål**: Blir sikkerhetshendelser faktisk håndtert på dette ledelsesnivået? **Hensikt:** Hensikten med spørsmålet er å oppdage situasjoner der bedrifter ikke følger rutiner og om det kan være med å påvirke valget rundt åpenhet.

3.2.4	**Teori:** Se 3.2.2 **Spørsmål**: Hva er årsaken til at sikkerhetshendelser ikke blir håndtert slik rutinen tilsier? **Hensikt:** Hensikten med spørsmålet er å oppdage situasjoner der bedrifter ikke følger rutiner og analysere hvorfor.

3.2.5	**Teori:** Se 3.2 **Spørsmål**: Hvem er det som håndterer hendelsene, og på hvilke ledelsesnivå er vedkommende? **Hensikt:** Hensikten med spørsmålet er å se på hvem som håndterer hendelser hos bedrifter som ikke har satte rutiner for dette på forhånd.

3.3	**Teori**: Se sikkerhetsloven kap 4, § 4-3: plikt til å gjennomføre sikkerhetstiltak og øvelser. **Spørsmål**: Har dere øvelser knyttet til å respondere på sikkerhetshendelser som en del av håndteringsrutinene deres? **Hensikt**: Hensikten med spørsmålet er å analysere modenheten til bedriftene og se om mer omfattende håndteringsrutiner påvirker deling.

3.3.1	**Teori**: Se sikkerhetsloven kap 4, § 4-3: plikt til å gjennomføre sikkerhetstiltak og øvelser. Virksomheten skal regelmessig gjennomføre øvelser for å vurdere effekten av iverksatte sikkerhetstiltak. **Spørsmål**: Hvor ofte har dere øvelser knyttet til sikkerhetshendelser, og hvordan er de lagt opp? **Hensikt**: Hensikten med spørsmålet er å analysere modenheten til bedriftene og se om mer omfattende håndteringsrutiner påvirker deling.

3.3.2	**Teori:** Se sikkerhetsloven kap 4, § 4-3: plikt til å gjennomføre sikkerhetstiltak og øvelser, § 4-4: krav til dokumentasjon, (§ 4-5: varslingsplikt?) Hvis ja på 3.3: **Spørsmål**: Har innføringen av rutiner for trening på håndtering av sikkerhetshendelser hatt noen innvirkning på antall rapporterte sikkerhetshendelser? **Hensikt:** Hensikten med spørsmålet er å analysere modenheten til bedriftene og se om mer omfattende håndteringsrutiner påvirker deling.

3.3.3	**Teori:** Se punkt 3.3.1 Hvis ja på 3.3: **Spørsmål**: Har øvelser rundt sikkerhetshendelser endret seg etter dere har vært gjennom en hendelse? eks hyppighet, gjennomføring… **Hensikt:** Hensikten med spørsmålet er å analysere modenheten til bedriftene og se om mer omfattende håndteringsrutiner påvirker deling.

Kategori 4: Ressurser og kompetanse

4.1	**Teori**: Mørketallsundersøkelsen I følge mørketallsundersøkelsen er det 21 prosent av virksomhetene har fullt ut outsourcet it-driften og videre er det 31 prosent som delvis outsourcer. **Spørsmål**: Har bedriften egen IT-avdeling? **Hensikt**: Hensikten med spørsmålet er å identifisere sammenligningspunkter mellom bedriftene i forhold til modenhet og analysere hvordan dette kan påvirke åpenhet.

4.2	**Teori**: Se sikkerhetsloven, sikkerhetsloven krever et forsvarlig sikkerhetsnivå → indirekte kan man da si at kompetanse innen sikkerhet er nødvendig for å oppfylle ulike regulatoriske intensjoner. Det krever kompetanse å løse slike krav, og "beskytte mot uautorisert utlevering" vil kreve kompetent hendelseshåndtering for å unngå at konfidensiell informasjon kommer på avveie og misbrukes. Også ulike krav til internkontroll, eks i økonomiregelverk, eks internkontrollforskriften vil kunne forankre krav til kompetanse for å treffe nødvendige tiltak og rutiner ved sikkerhetsbrudd. **Spørsmål**: Har bedriften fagpesonell med kompetanse innen sikkerhet? **Hensikt**: Hensikten med spørsmålet er å identifisere sammenligningspunkter mellom bedriftene i forhold til modenhet og analysere hvordan dette kan påvirke åpenhet.

4.3	**Teori**: Se sikkerhetsloven, sikkerhetsloven krever et forsvarlig sikkerhetsnivå → indirekte kan man da si at kompetanse innen sikkerhet er nødvendig for å oppfylle ulike regulatoriske intensjoner. Det krever kompetanse å løse slike krav, og "beskytte mot uautorisert utlevering" vil kreve kompetent hendelseshåndtering for å unngå at konfidensiell informasjon kommer på avveie og misbrukes. Også ulike krav til internkontroll, eks i økonomiregelverk, eks internkontrollforskriften vil kunne forankre krav til kompetanse for å treffe nødvendige tiltak og rutiner ved sikkerhetsbrudd. **Spørsmål**: Har bedriften fagpersonell med kompetanse innen hendelseshåndtering? **Hensikt**: Hensikten med spørsmålet er å identifisere sammenligningspunkter mellom bedriftene i forhold til modenhet og analysere hvordan dette kan påvirke åpenhet.

4.4	**Teori**: Mørketallsundersøkelsen 2020 beskriver at offentlige bedrifter deler mer til sektor CERT enn andre. **Spørsmål**: Er bedriften medlem av et CERT, SektorCert, CSIRT eller andre organer for samarbeid innen sikkerhet? **Hensikt**: Hensikten med spørsmålet er å identifisere sammenligningspunkter mellom bedriftene i forhold til modenhet og analysere hvordan dette kan påvirke åpenhet.

Kategori 5: Erfaringer og evalueringer

5.1	**Teori:** Referer til spesifikke bedrifter i media knyttet til deling av hendelser. **Spørsmål**: Erfaringsmessig, hvem tar valget om å være åpne eller ikke om en hendelse, og på hvilke ledelsesnivå er vedkommende? **Hensikt:** Hensikten med spørsmålet er å avgjøre hvem som faktisk tar valget om å være åpne eller ikke i de ulike bedriftene for å analysere om dette er med å påvirke beslutningen.

5.2	**Teori**: NIST Guide to Cyber Information Sharing beskriver utfordringer med å dele. Utfordringene går ut på at det krever tillit å dele informasjon med andre bedrifter, og at det kan ta tid å bygge opp et samarbeid over en plattform med automatiserte varslingsmekanismer. Det er fare for at sensitiv informasjon kan komme på avveie, og det kan være problematisk å dele informasjon som er klassifisert. I tillegg kan bedriften har regelverk/rutiner som gjør deling vanskelig, og plattformer som ikke tillater anonym deling kan gjøre at færre ønsker å dele. **Spørsmål**: Er det en eller flere hendelser dere har valgt å ikke dele med NSM, NCSC og andre beredskapsorganisasjoner, og heller ikke media? **Hensikt**: Hensikten med spørsmålet er å identifisere hvem som har hatt sikkerhetshendelser uten å dele.

5.2.1	**Teori**: Se 5.2 Hvis ja på 5.2: **Spørsmål**: Hvorfor delte dere ikke denne hendelsen? (Til oss: Har frykt for omdømme vært en faktor?) **Hensikt**: Hensikten med spørsmålet er å finne ut av årsakene til at bedrifter ikke deler noe om dette.

5.2.2	**Teori**: NIST Guide to Cyber Threat Information Sharing beskriver utfordringer med å dele. Utfordringene går ut på at det krever tillit å dele informasjon med andre bedrifter, og at det kan ta tid å bygge opp et samarbeid over en plattform med automatiserte varslingsmekanismer. Det er fare for at sensitiv informasjon kan komme på avveie, og det kan være problematisk å dele informasjon som er klassifisert. I tillegg kan bedriften har regelverk/rutiner som gjør deling vanskelig, og plattformer som ikke tillater anonym deling kan gjøre at færre ønsker å dele. Hvis ja på 5.2: **Spørsmål**: Har bedriften opplevd noen negative eller positive konsekvenser ved å ikke dele med NSM, NCSC og andre beredskapsorganisasjoner, og heller ikke media?

	Hensikt: Hensikten med spørsmålet er å finne ut om bedrifter har fått opplevd noe positivt eller negativt ved å ikke dele, og om det har hatt noen påvirkning for videre deling.

5.2.3	**Teori**: Se 5.2.2 Hvis ja på 5.2: **Spørsmål**: Har disse erfaringene i ettertid påvirket deres valg om deling av sikkerhetshendelser? **Hensikt**: Hensikten med spørsmålet er å finne ut om bedrifter har fått opplevd noe positivt eller negativt ved å ikke dele, og om det har hatt noen påvirkning for videre deling.

5.3	**Teori**: I NSM sin risikorapport 2020 oppfordrer de til å dele informasjon som kan være til nytte for andre. **Spørsmål**: Er det en eller flere hendelser dere har valgt å ikke dele med media som dere delte med NSM, NCSC eller andre beredskapsorganisasjoner? **Hensikt**: Hensikten med spørsmålet er å identifisere hvem som har hatt sikkerhetshendelser som de har delt med NSM.

5.3.1	**Teori**: Se 5.3 Hvis ja på 5.3: **Spørsmål**: Hvorfor delte dere med NSM, NCSC eller andre beredskapsorganisasjoner? **Hensikt**: Hensikten med spørsmålet er å finne ut av årsakene til at bedrifter deler med NSM.

5.3.2	**Teori**: NIST Guide to Cyber Threat Information Sharing beskriver fordeler og utfordringer med å dele informasjon. Fordelene kan være at flere får økt kunnskap og ferdigheter, at bevisstheten rundt sikkerhetshendelser og trusler økes, flere bedrifter kan få en bedre evne til å forstå og utnytte informasjon, og man kan bygge et mer fleksibelt forsvar. Utfordringene går ut på at det krever tillit å dele informasjon med andre bedrifter, og at det kan ta tid å bygge opp et samarbeid over en plattform med automatiserte varslingsmekanismer. Det er fare for at sensitiv informasjon kan komme på avveie, og det kan være problematisk å dele informasjon som er klassifisert. I tillegg kan bedriften har regelverk/rutiner som gjør deling vanskelig, og plattformer som ikke tillater anonym deling kan gjøre at færre ønsker å dele. Hvis ja på 5.3: **Spørsmål**: Har bedriften opplevd noen negative eller positive konsekvenser ved å dele med NSM, NCSC og andre beredskapsorganisasjoner? **Hensikt**: Hensikten med spørsmålet er å finne ut om bedrifter har fått opplevd noe positivt eller negativt ved å dele med NSM, og om det har hatt noen påvirkning for videre deling.

5.3.3	**Teori**: Se 5.3.2 Hvis ja på 5.3: **Spørsmål**: Har disse erfaringene i ettertid påvirket deres valg om deling av sikkerhetshendelser? **Hensikt**: Hensikten med spørsmålet er å finne ut om bedrifter har fått opplevd noe positivt eller negativt ved å dele med NSM, og om det har hatt noen påvirkning for videre deling.

5.4	**Teori**: Referer til spesifikk bedrift som har mediahendelse. **Spørsmål**: Er det en eller flere hendelser dere har valgt å dele med media? **Hensikt**: Hensikten med spørsmålet er å identifisere hvilke bedrifter som deler med media.

5.4.1	**Teori**: Se 5.4 Hvis ja på 5.4: **Spørsmål**: Hvorfor delte dere denne hendelsen med media? **Hensikt**: Hensikten med spørsmålet er å identifisere årsakene til at bedrifter deler med media.

5.4.2	**Teori**: Se 5.4 Hvis ja på 5.4: **Spørsmål**: Har bedriften opplevd noen negative eller positive konsekvenser ved å dele med media? **Hensikt**: Hensikten med spørsmålet er å finne ut om bedrifter har fått opplevd noe positivt eller negativt ved å dele med media, og om det har hatt noen påvirkning for videre deling.

5.4.3	**Teori**: Se 5.4 Hvis ja på 5.4: **Spørsmål**: Har disse erfaringene i ettertid påvirket deres valg om deling av sikkerhetshendelser? **Hensikt**: Hensikten med spørsmålet er å finne ut om bedrifter har fått opplevd noe positivt

	eller negativt ved å dele med media, og om det har hatt noen påvirkning for videre deling.

5.5	**Teori**: Referer til spesifikk bedrift som har mediahendelse **Spørsmål**: Er det en eller flere hendelser dere har valgt å dele med media der dere ikke har delt med NSM, NCSC eller andre beredskapsorganisasjoner først? **Hensikt**: Hensikten med spørsmålet er å identifisere hvilke bedrifter som deler med media, og se i hvilke situasjoner NSM er med på denne avgjørelsen og ikke.

5.5.1	**Teori**: Se 5.5 Hvis ja på 5.5: **Spørsmål**: Hvorfor delte dere ikke denne hendelsen NSM, NCSC eller andre beredskapsorganisasjoner først? **Hensikt**: Hensikten med spørsmålet er å identifisere årsakene til at bedrifter deler med media, og se om kommunikasjon med NSM påvirker dette valget på noen måte.

5.5.2	**Teori**: Se 5.5 Hvis ja på 5.5: **Spørsmål**: Har bedriften opplevd noen negative eller positive konsekvenser ved å ikke dele med NSM, NCSC eller andre beredskapsorganisasjoner først? **Hensikt**: Hensikten med spørsmålet er å finne ut om bedrifter har fått opplevd noe positivt eller negativt ved å dele med media, om det har hatt noen påvirkning for videre deling, og om NSM sin innblanding påvirker dette.

5.5.3	**Teori**: Se 5.5 Hvis ja på 5.5: **Spørsmål**: Har disse erfaringene i ettertid påvirket deres valg om deling av sikkerhetshendelser? **Hensikt**: Hensikten med spørsmålet er å finne ut om bedrifter har fått opplevd noe positivt eller negativt ved å dele med media, om det har hatt noen påvirkning for videre deling, og om NSM sin innblanding påvirker dette.

5.6	**Teori**: Mørketallsundersøkelsen 2020 har spurt bedrifter hva som var årsaken til sikkerhetsbruddet. De vanligste årsakene var uflaks eller tilfeldigheter, menneskelige feil og mangel på sikkerhetsbevissthet blant de ansatte. **Spørsmål**: Hva anser dere som årsaken(e) til hendelsen(e) dere har hatt? **Hensikt**: Hensikten med spørsmålet er å identifisere årsakene til sikkerhetshendelser og se hvordan årsaken er med på å påvirke deling av de ulike hendelsene.

Vedlegg C

Databehandlingsskjema

Databehandlingsskjemaet som ble sendt ut til alle intervjuobjekter for signering i forkant av intervju.

Med dette dokumentet bekrefter vi, Karianne Kjønås, Thea Erbe Thomassen og Vilde Nylund Johnsen at all innsamling av data til bacheloroppgaven “Åpenhetens dilemma” vil holdes internt, og når data er ferdigbehandlet vil det slettes. Innleveringsfristen for bacheloroppgaven er den 20. Mai, og databehandlingen vil ansees som ferdig innen da.

Svar på intervjuspørsmålene trekkes inn i analysen, men transkripsjon av intervjuet vil ikke publiseres i eller utenfor oppgaven.

I det tilfellet at intervjuobjektet ønsker å være anonyme vil fremdeles størrelse på bedriften og sektor bedriften tilhører beskrives, men all annen informasjon vil anonymiseres.

Det ønskes at bedriften selv, i dette dokumentet velger om de ønsker å være anonym eller ei, og anerkjenner at dokumentet er lest og godkjent.

Jeg bekrefter at vår bedrift ønsker å være anonym [ ]
Jeg bekrefter at vår bedrift ikke ønsker å være anonym [ ]

Jeg bekrefter at dokumentet er lest og godkjent [ ]

Dato: _____

Bedrift: _____

Representant for bedrift: _____

Signatur: _____

Dato: _____

Karianne Kjønås: _____

Thea Erbe Thomassen: _____

Vilde Nylund Johnsen: _____

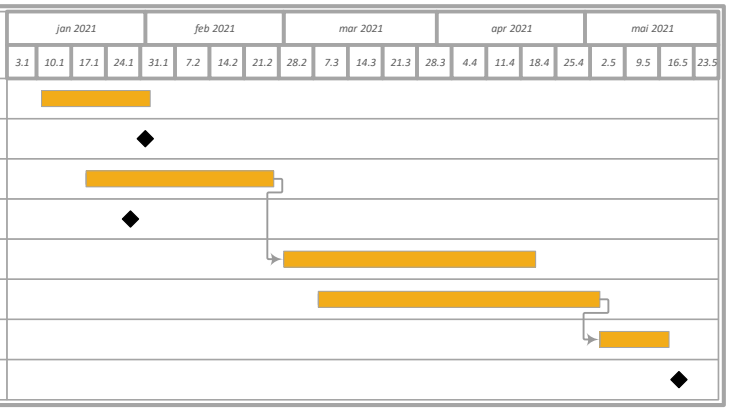
Vedlegg D

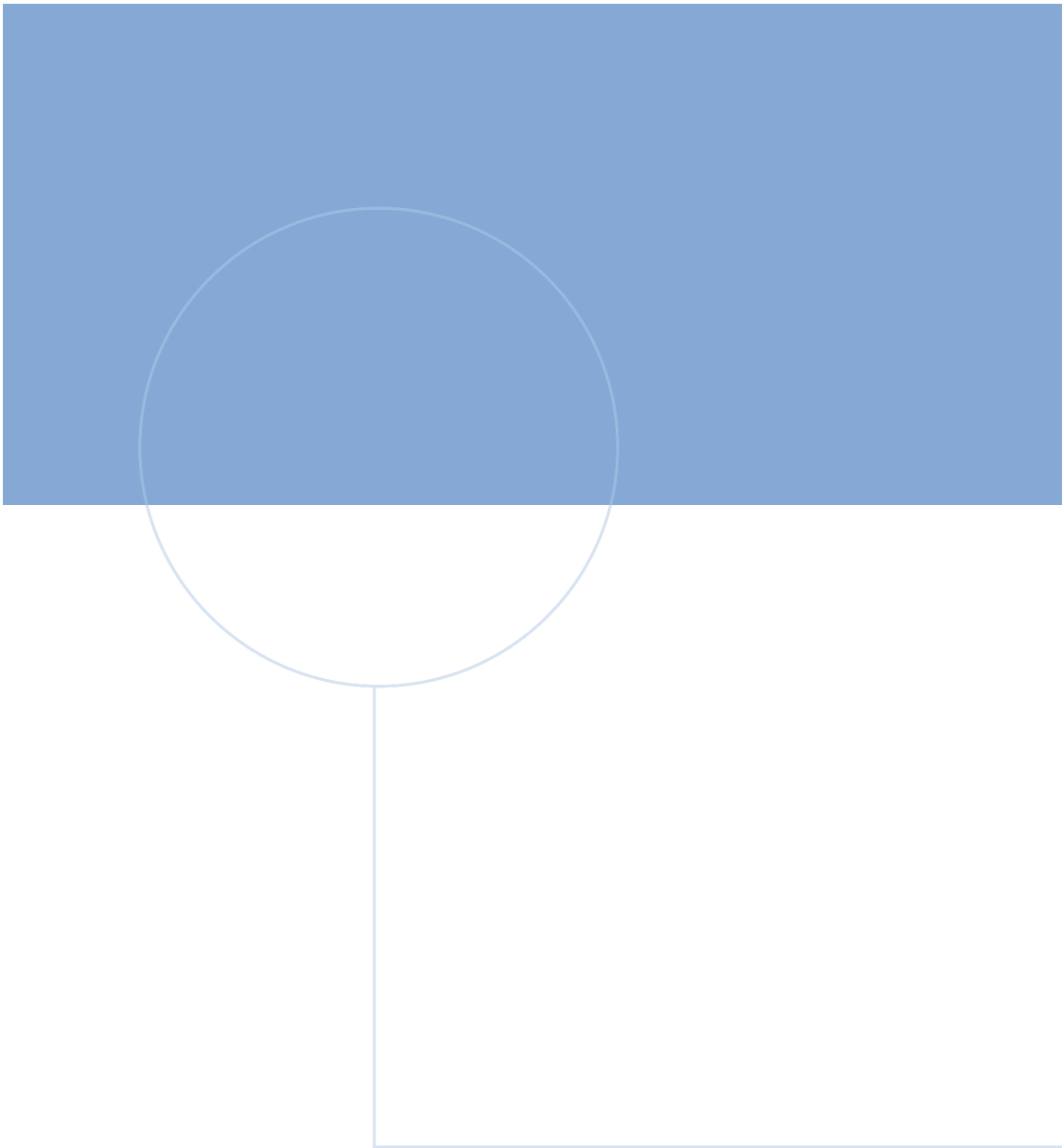
Ganttdiagram

Ganttdiagram for bacheloroppgaven

Gantt diagram

ID	Oppgavenavn	Start	Ferdig	Varighet
1	Prosjektplan	11.01.2021	01.02.2021	16d
2	Prosjektavtale	01.02.2021	01.02.2021	0d
3	Intervjuguide	20.01.2021	26.02.2021	28d
4	Definere intervjuobjektgruppering	29.01.2021	29.01.2021	0d
5	Intervju	01.03.2021	20.04.2021	37d
6	Intervjuanalyse	08.03.2021	03.05.2021	41d
7	Ferdigstilling av oppgave	04.05.2021	17.05.2021	10d
8	Innleveringsfrist	20.05.2021	20.05.2021	0d





NTNU

Kunnskap for en bedre verden