UNIVERSITETET I STAVANGER

MASTERGRADSSTUDIUM I
RISIKOSTYRING OG SIKKERHETSLEDELSE

MASTEROPPGAVE

SEMESTER:
Høst 2018

FORFATTER:
Angélique Colle

VEILEDER:
Jon Selvik

TITTEL PÅ MASTEROPPGAVE:

I hvilken grad benyttes risiko- og trusselvurderinger aktivt i arbeid med informasjonssikkerhet, og spesifikt som input til hendelseshåndtering ved tilsiktede angrep?

EMNEORD/STIKKORD:
Risiko, trusselanalyse, IT-sikkerhet, informasjonssikkerhet, risikoanalyse

SIDETALL: 84 (inkl. forside og alle vedlegg)

STAVANGER …22.10.18…….
DATO/ÅR

Forord

Det er ønskelig å rette en takk til informantene, som har tatt seg tid til å bidra med sin innsikt og kompetanse.

Videre er det ønskelig å takke veileder Jon Selvik for gode råd, samt min familie som har utvist tålmodighet i denne prosessen.

Sammendrag

Bakgrunn

Bakgrunnen for denne oppgaven var interesse for ondsinnede angrep på informasjonssikkerhetssiden. De siste årene har det vært en økende rapportering av ondsinnede angrep på informasjonsinfrastruktur. Og det er her særlig inn mot sektorer som drifter og forvalter kritisk infrastruktur. Det var et ønske om å se på mulige synergier mellom strategisk og operativt/utøvende IT-sikkerhetsarbeid, all den tid det gjøres en del analyser på strategisk side, som burde være nyttig også utover det rent formelle som følger av krav til risikoanalyser.

Formål

Formålet med prosjektet er å se på organisering av informasjonssikkerhetsarbeid blant aktører som forvalter kritisk infrastruktur og/eller informasjon, herunder med fokus på sikring mot tilsiktede angrep. I dette ligger angrep som er nøye planlagt, og hvor informasjonsteknologi enten er et middel eller et våpen. Det er her fokusert på sikring mot tilsiktede angrep, og hvordan dette håndteres i risikovurderinger.

Teori valgt i denne oppgaven er først og fremst teori rundt risiko, risikoanalyser, trusselanalyser og beredskap. Fokuset er tilsiktede angrep og IT-sikkerhet.

Metode

I oppgaven er det valgt å benytte kvalitativ metode. Det ble gjennomført intervjuer av et utvalg informanter fra ulike virksomheter som kan sorteres under sektorer som alle drifter og forvalter kritisk infrastruktur.

Funn

Selv om det gjennomføres et høyt antall risikoanalyser av nye og endrede systemer, er det noen svakheter i måten disse gjøres på. Dette medfører vanskeligheter med å kunne gjenbruke deler av disse vurderingene inn mot overvåkning og hendelseshåndtering.

Konklusjon

Konklusjonen på denne oppgaven gir ikke noen form for oppskrift eller et entydig svar. Den viser imidlertid at det er noen svakheter i metode for gjennomføring av risikovurderinger innen IT-sikkerhet, herunder særlig på trusselanalysesiden, som vanskeliggjør gjenbruk av en del av materialet inn mot overvåkning og hendelseshåndtering.

Innholdsfortegnelse

1. Innledning

1.1 Bakgrunn

Det er en økende digitalisering i samfunnet, og vi legger fra oss, eller blir avkrevd, mer og mer informasjon. I følge Lysneutvalget (NOU 2015:13) er digitaliseringen en driver for økonomiske vekst og innovasjon. Samtidig har den forenklet individets hverdag. Informasjonsinfrastruktur er komplekst, gjennomgripende og under stadig utvidelse. En slik utvidelse sees gjerne på et applikasjonsnivå, der forventninger om økt funksjonalitet og innovasjon medfører en rask endringstakt. Mange virksomheter sitter da med stor gjeld i form av applikasjoner og infrastruktur som er gammel, samtidig med at de skal følge opp med stadig nye og forbedrede løsninger for å dekke forventninger, ønsker og behov fra både kunder, ansatte og myndigheter. Det er mange og sammensatte grunner til at det ikke alltid er lett å bytte ut eldre og mindre sikker infrastruktur, eksempelvis som følge av at kritisk utstyr er avhengig av den (NOU 2015:13).

Teknologi skaper ikke bare nye muligheter, men i følge Lysneutvalget også nye sårbarheter (NOU 2015:13). Internett sørger for at man er sårbare, der viktige tjenester er avhengig av forholdsvis få og ofte eksponerte komponenter. Tjenester er tilgjengelige fra hele verden, også for ondsinnede aktører. I følge Lysneutvalget (NOU 2015:13) medfører rask utvikling i trusselbildet at teknologi man tidligere regnet for å holde et høyt sikkerhetsnivå, nå kanskje er usikkert.

Sikkerhet både rundt infrastrukturen og dataene vi utveksler er i en slik setting svært viktig. For avhengighet mellom systemer og utveksling av informasjon er økende, og det fulle bildet av hvilke løsninger som er avhengige av hva, og hvordan all informasjon vi sender fra oss sikres, er vanskelig å få den fulle oversikt over.

1.2 Problemstilling

Oppgavens problemstilling er formulert som følgende:

I hvilken grad benyttes risiko- og trusselvurderinger aktivt i arbeid med informasjonssikkerhet, og spesifikt som input til hendelseshåndtering ved tilsiktede angrep?

For å kunne besvare problemstillingen, er det formulert tre forskningsspørsmål:

1. Hvordan gjennomføres det strategiske arbeidet med sikkerhet, herunder risiko- og trusselvurderinger?

2. Hva trengs som input i arbeidet med overvåkning og hendelseshåndtering av tilsiktede angrep?

3. På hvilken måte er det tilrettelagt for samhandling på tvers av strategisk og operativt sikkerhetsarbeid?

1.3 Kontekst

Det har vært et økende fokus på IT-sikkerhet de siste årene, etter en rekke hendelser som har medført skade på, og tap av, verdier. En del av disse hendelsene har vært resultat av tilsiktede angrep, hvorav noen av disse har vært spesifikt rettet mot enten en sektor eller en virksomhet. Eksempler på dette er angrepet på Helse Sør-Øst på nyåret i 2018. Andre angrep har rammet bredere, mindre spesifikt, som WannaCry og NotPetya våren 2017, som blant annet rammet offentlige og private virksomheter i Europa, herunder det britiske helsevesenet.

Tradisjonelt har man målt informasjonssikkerhet etter sikkerhetsprinsippene konfidensialitet, integritet og tilgjengelighet. Forholdet mellom de tre er ikke alltid likt fordelt, ei heller bestandig. Prinsippene må veies opp mot hverandre og formålet med den nye eller endrede løsningen.

Det gjennomføres et høyt antall risikoanalyser innen IT, herunder i forbindelse med implementeringer, oppgraderinger og endringer i applikasjoner og infrastruktur. Prosessuelt sett inneholder risikoanalysene også trusselanalyser. Trusselanalyser og –informasjon er viktig i arbeid med overvåkning og håndtering av tilsiktede, uønskede hendelser. Men det er usikkert om det faktisk gjennomføres reelle trusselanalyser i forbindelse med risikoanalysene, og videre om risiko- og trusselanalysene benyttes aktivt i arbeidet med overvåkning og hendelseshåndtering, slik at man drar nytte av en form for dokumentasjon og vurdering som uansett skal gjøres.

1.4 Avgrensinger i oppgaven

I denne oppgaven er fokuset å se på hvordan det arbeides med IT-sikkerhet inn mot tilsiktede angrep. Spesifikt innebærer det å se på om risiko- og trusselvurderinger, med særlig vekt på risiko- og trusselanalyser, brukes i arbeidet med overvåkning og hendelseshåndtering av tilsiktede angrep hos et utvalg virksomheter. Virksomhetene er valgt ut fordi de alle forvalter og drifter kritisk infrastruktur. Det er imidlertid ikke fokusert på den kritiske infrastrukturen eller dataene virksomhetene forvalter, eller virksomhetenes forhold til sikkerhetsloven, i oppgaven. Men fordi de aktuelle virksomhetene har befatning med kritisk infrastruktur, stilles det også høyere krav med hensyn til sikker drift og forvaltning, samt at det er rimelig å anta at tilsiktede angrep som kan ramme virksomhetenes informasjonsinfrastruktur er en nærliggende tanke og vil ha forholdsvis høyt fokus i virksomhetene.

Fordi det var ønskelig å skaffe til veie informasjon om hva en virksomhet gjør innenfor IT-sikkerhet, og eventuelt hvorfor man gjør det, eller ofte vel så interessant hvorfor de eventuelt ikke gjør det, ble det gjennomført dybdeintervjuer med syv IT-sikkerhetsressurser fra et utvalg virksomheter. Ressursene tilhører alle én av de tre sektorene helse, forsvar/justis og finans. Utgangspunktet var å se hva som gjøres, eller som nevnt hva som ikke gjøres, på tvers av sektorene. Altså har utgangspunktet ikke vært å spesifikt se på forskjellene mellom de ulike sektorene.

Et utvalg av ulike teorier er valgt ut for å belyse problemstillingen, innen for ulike temaer som eksempelvis sårbarhet, trusselanalyse, risikoanalyse og –styring og beredskap, da det overordnet sett er informasjonssikkerhet som er tema, og det var ønskelig å se helhetlig på problemstillingen. Det foreligger mye teori rundt risikovurderinger generelt, hvorav dermed også risikoanalyser og risikostyring. Samtidig er det begrenset med teori rundt risiko- og trusselanalyser innenfor IT. Dette til tross for at det er aspekter ved IT som kan være med på å komplisere bildet man forsøker risikovurdere. Og der det foreligger teori, tar har fokuset ofte vært på tilgjengelighetssiden, selv om integritet og konfidensialitet også inngår i de tre prinsippene innen IT-sikkerhet.

1.5 Oppbygning og struktur på oppgaven

Oppgaven er inndelt i følgende seks deler:

Den første delen av oppgaven er innledningen, hvor bakgrunn for valg av oppgavens tema

presenteres. Videre presenteres oppgavens problemstilling, samt forskningsspørsmålene som er brukt. Deretter redegjøres det for kontekst, samt hvilke avgrensinger som er gjort, og hvorfor. Til sist presenteres oppgavens oppbygning.

Oppgavens andre del er teorikapittelet, hvor det vil redegjøres for relevante begreper og teorier innenfor temaene for oppgaven. I store trekk gjelder det begrepene og temaene sikkerhet, beredskap, sårbarheter, risiko, risikovurdering – og analyse, risikostyring og trusselanalyser. Det redegjøres for sikkerhet generelt og sikring spesielt, i tillegg til de tre prinsippene IT-sikkerhet tradisjonelt tufter på, i tillegg til kort om sikkerhetsorganisering. Beredskap presenteres generelt, men også inn mot hendelseshåndtering hvor dette er relevant for IT-sikkerhet. Sårbarhetsbegrepet redegjøres for både i lys av samfunnssikkerhetsdefinisjonen og IT-definisjonen. Deretter presenteres en gjennomgang av risiko og hva dette er, samt risikovurdering og –analyse hvor de ulike delene av disse presenteres. Risikostyring presenteres med hensyn til formål og suksessfaktorer. Avslutningsvis redegjøres det for trusselanalyser, med fokus på sikring.

I den tredje delen av oppgaven redegjøres det for de metodevalg som er tatt, herunder hvilke styrker og svakheter det medfører. Det redegjøres videre for bakgrunn valg av informanter, intervjuform og datainnsamling, diskusjon rundt validiteten og etiske problemstillinger.

Oppgavens fjerde del er presentasjon av de empiriske funnene fra intervjuer gjennomført med informanter fra ulike sektorer. De empiriske dataene vil presenteres ved bruk av de tre forskningsspørsmålene.

Oppgavens femte del er drøfting av empirien opp mot teorien. I dette ligger en gjennomgang av forskningsspørsmålene med basis i empirien fra intervjuene, og det teoretiske grunnlaget. Drøftingen vil videre søke å besvare forskningsspørsmålene.

I den sjette og siste delen av oppgaven vil en sammenfatning av funnene presenteres, sammen med en konklusjon og forslag til videre forskning.

1.6 Begrepsbruk

Det er nødvendig med noen begrepsavklaringer da enkelte ord benyttes om hverandre, og andre er det lagt en bestemt definisjon rundt.

CERT: Computer Emergency Respons Team

IRT: Incident Response Team

IT-sikkerhet går under mange navn. Noen ganger er det en bakenforliggende årsak til det, hvor man ønsker å snevre inn begrepsbruken. Imidlertid vil denne oppgaven, grunnet ulik teori og informanter benytte disse begrepene om hverandre: IT-sikkerhet informasjonssikkerhet, IKT-sikkerhet og cybersikkerhet.

Kritisk infrastruktur: Her legges Sårbarhetsutvalgets definisjon til grunn, altså systemer som, dersom de ikke fungerer, vil ha en sterk negativ effekt på samfunnet (NOU 2000:24)

Operativ og utøvende, som er synonymer i denne oppgaven. Betegnelsene benyttes for å skille de som sitter med mer tekniske IT-sikkerhetsoppgaver kontra de som arbeider med de strategiske oppgavene.

Risikovurderinger: Risikoanalyse + risikoevaluering (Aven et. al 2010). Det er her nødvendig å poengtere at risikovurdering, risikoanalyse og RoS brukes om hverandre inne IT-sikkerhet.

Tilsiktede angrep: Med dette menes bevisste, ondsinnede handlinger. Man kan her også granulere ytterligere til spesifiserte og uspesifiserte angrep, hvor sistnevnte eksempelvis kan være virusangrep hvor handlingen er tilsiktet, men det er noe mer tilfeldig hvordan det rammer.

2. Teori

Innledningsvis er det ønskelig å redegjøre for noen grunnleggende begreper innen informasjonssikkerhet, for deretter å presentere noen sentrale teorier rundt risikovurderinger og trusselanalyser. Kapittelet er inndelt etter tema, og teori vil presenteres i følgende rekkefølge:

1. Sikkerhet
2. Beredskap
3. Sårbarheter
4. Risiko
5. Risikoanalyse og -vurdering
6. Risikostyring
7. Trusselanalyser

Det første delkapittelet er en redegjørelse av sikkerhet generelt, og sikring med fokus på IT-sikkerhet spesielt. De tre sikkerhetsmålene man tradisjonelt vurderer IT-sikkerhet mot, vil presenteres. Disse er henholdsvis konfidensialitet, integritet og tilgjengelighet. Her vil det hovedsakelig basere seg på Lysneutvalget NOU 2015:13. I tillegg vil sikkerhetsorganisering på IT-siden presenteres med utgangspunkt i NSMs veileder i sikkerhetsstyring (2015), Engan et al. (2016) og Jore (2017)

I det andre delkapittelet er det ønskelig å redegjøre for beredskap. Alvorlige IT-sikkerhetshendelser fordrer beredskap og vil derfor bli berørt all den tid tilsiktede angrep kan medføre alvorlige kriser som igjen vil fordre planlegging og øvelser i forkant, samt planer. I tillegg faller hendelseshåndtering under dette delkapittelet. Det tas det utgangspunkt i Aven et al (2010), Aven et al., (2008), Perry og Lindell (2003), Engen et. al (2016) og NSM (2015).

I det tredje delkapittelet er det ønskelig å beskrive sårbarheter generelt, og inn mot IKT-sikkerhet spesielt. Dette fordi sårbarheter innen IKT-sikkerhet ofte defineres på en litt annen måte enn den tradisjonelle definisjonen for sårbarheter. Delkapittelet tar for seg sårbarhetsbegrepene som benyttes av Rausand og Utne (2014), Sårbarhetsutvalget (NOU 2000:24) og Lysneutvalget (NOU 2015:13).

Det fjerde delkapittelet er en gjennomgang av et lite utvalg av teorier rundt risiko, og hva som ligger i dette. I dette kapittelet er det hovedsakelig Aven (2015), Aven et. al (2010), Engen et. al (2016) og Rausand og Utne (2014) det tas utgangspunkt i, og hvordan de beskriver risiko.

I det femte delkapittelet omhandler risikoanalyser og -analyser. Det tas her sikte på å beskrive risikoanalyser og –vurderinger generelt, samt inn mot IT-sikkerhetssiden. I dette delkapittelet tas det hovedsakelig utgangspunkt i Aven et. al (2010), Rausand og Utne (2014), Refsdal et. al (2015), Busmunrud et. al (2015) og NSMs Håndbok i Risikovurdering for sikring (2016), samt Lysneutvalget (NOU 2015:13).

I delkapittel seks tar for seg risikostyring. Det vil også redegjøres for NSMs sikkerhetsstyringsbegrep (NSM 2015). herunder også sikkerhetsstyring. Aven (2015), Rausand og Utne (2014).

Trusselanalyser et viet et eget delkapittel, delkapittel syv, da dette gjør seg særlig gjeldende når man skal forholde seg til tilsiktede angrep på IT-sikkerhetssiden. Det tas her utgangspunkt i NSM (2016), Aven et. al (2010), Refsdal et. al (2015) og Rausand og Utne (2014).

2.1 Sikkerhet

2.1.1 Safety og security

Jore & Egeli (2015) henviser til at flere over tid har skilt mellom safety og security ved at safety beskriver beskyttelse fra utilsiktede hendelser, herunder eksempelvis ulykker, mens security er beskyttelse mot tilsiktede handlinger som terror. Dette innebærer at det er hensikten bak hendelsen som avgjør om den defineres som sikkerhet eller sikring, all den tid sikkerhet er utilsiktet mens sikring er tilsiktede.

2.1.2 De tre pilarene innen informasjonssikkerhet

IKT-sikkerhet handler i følge Lysneutvalget (NOU 2015:13) om ”*å beskytte IKT og informasjonen i informasjonssystemene mot uønskede hendelser*” (NOU 2015:13, s. 34). Ofte måles dette mot noen sikkerhetsmål, hvorav de tre mest kjente er konfidensialitet, integritet og tilgjengelighet, ofte kalt CIA etter engelsk *Confidentiality*, *Integrity* og *Availability*. I disse begrepene ligger dog flere aspekter som også er viktige i et informasjonssikkerhetsperspektiv,

men som overordnet kan sies å falle under ett av de tre overordnede begrepene. Det redegjøres for disse sikkerhetsmålene under.

2.1.2.1 Konfidensialitet

Konfidensialitet i et informasjonssikkerhetsperspektiv, innebærer at informasjon kun er tilgjengelig for de som er autorisert til å se informasjonen. I dette ligger at informasjon ikke skal komme uvedkommende i hende. I IKT-sfæren vil brudd på konfidensialitetsprinsippet kunne være uopprettelig (NOU 2015:13, s. 34). Et eksempel på et konfidensialitetsbrudd vil kunne være at uvedkommende får tilgang til elektroniske pasientjournaler, og i verste fall sprer disse.

2.1.2.2 Integritet

Å sikre integriteten til data i et informasjonssikkerhetsperspektiv, refererer til at man skal kunne stole på at "*informasjonen skal være korrekt og gyldig*" (NOU 2015:13, s.35). Brudd på prinsippet om integritet kan eksempelvis være at en uautorisert aktør endrer på kontonummer i et lønnssystem, slik at en virksomhets HR-avdeling uforvarende utbetaler lønn til feil person. De har stolt på at kontoinformasjonen har vært korrekt i lønnssystemet.

2.1.2.3 Tilgjengelighet

Tilgjengelighet i et informasjonssikkerhetsperspektiv innebærer at autoriserte ressurser skal kunne stole på at de har tilgang til den informasjon de trenger, når de trenger den. Tilgjengelighet kan sees på flere nivåer. Det er den tekniske tilgjengeligheten, som innebærer at systemet er oppe, og brukerens perspektiv, som innebærer at vedkommende får tilgang til informasjon når det trengs. I tilgjengelighetsprinsippet er det sistnevnte som er viktigst, da det er fullt mulig for en løsning å være teknisk sett opp, men likevel utilgjengelig for de autoriserte brukerne. Et eksempel på manglende tilgjengelighet er når for mange brukere forsøker å konsumere en tjeneste samtidig, slik at noen brukere ikke når gjennom, eller når gjennom først en stund senere. Tjenesten oppleves derfor som utilgjengelig for dem.

2.1.2.4 Avveininger

I tillegg til de tre sikkerhetsprinsippene konfidensialitet, integritet og tilgjengelighet, finnes det også noen andre viktige sikkerhetsprinsipper som til dels kan sies å omfattes av de tre overordnede prinsippene, men som likevel er verdt å nevne. Disse er *ikke-fornekting*,

autentisitet og *sporbarhet*. I følge Lysne-utvalget (NOU 2015:13, s. 35) er ikke-fornekting, av engelske non-repudiation, at "*en digital handling ikke skal kunne benektes i etterkant*". Autentisitet er et begrep nært beslektet med *ikke-fornekting*, og refererer til "*å sikre opphavet til informasjonen*" (NOU 2015:13, s. 35).

De tre sikkerhetsprinsippene vil ikke alltid være like viktige. Avhengig av situasjon, organisasjon, data og verdier, vil graden av de ulike prinsippene måtte veies opp mot hverandre, all den tid de noen ganger vil stå i direkte motsetning til hverandre. Lysneutvalget (NOU 2015:13) trekker frem "*Need to share*" som motstykke til den tradisjonelle "*Need to know*" (NOU 2015:13, s. 35), hvor konfidensialitetsprinsippet utfordres av tilgjengelighetsprinsippet. Omstendigheter rundt vil i mange tilfeller ha innvirkning på hvilket sikkerhetsprinsipp som står sterkest i gitte situasjoner og i visse sektorer. Eksempelvis vil konfidensialitet rundt helseinformasjon for den enkelte oppfattes på en annen måte enn konfidensialitet rundt økonomi, samtidig som at integriteten til helseopplysningene vil være prekære i forbindelse med situasjoner som krever bruk av dataene, som en operasjon. I akutte situasjoner vil kanskje tilgjengelighet veie tyngst for en pasient. Hvordan de tre prinsippene veies opp mot hverandre vil derfor også variere fra virksomhet til virksomhet, alt etter både hva slags informasjon virksomheten forvalter, og situasjonen rundt. Det må derfor gjøres avveininger rundt hvordan man veier de ulike sikkerhetsprinsippene opp mot hverandre.

2.1.4 Sikkerhetsorganisering - IT

Sikkerhetsarbeid på IT-siden innebærer både strategiske og utøvende oppgaver. Det er virksomheten selv som må vurdere hvordan det er ønskelig å organisere sikkerhetsarbeidet. Blant annet kan de operative/utøvende driftsoppgavene og de strategiske sikkerhetsfunksjonene organiseres ulike steder i organisasjonen. Imidlertid er det viktig at de strategiske og utøvende funksjonene samarbeider, slik at de er i stand til å gjennomføre de nødvendige aktivitetene (NSM 2015).

2.1.4.1 Strategiske sikkerhetsfunksjoner

Strategisk sikkerhetsarbeid er ofte kontrollerende, rådgivende og koordinerende. Både sikkerhetsleder og informasjonssikkerhetsleder er tradisjonelt strategiske sikkerhetsroller, i tillegg til eventuelt kryptosikkerhetsleder (NSM 2015). Avhengig av virksomheten, kan disse funksjonene både være samlet eller spredt flere steder i organisasjonen.

I større virksomheter kan funksjonene dekkes av en stab. Men ”*det kan fort medføre for stor avstand mellom disse rollene*” dersom sikkerhetsleder og informasjonssikkerhetsleder er organisert i ulike enheter, eksempelvis ved at informasjonssikkerhetsleder er lagt under IKT (NSM 2015, s. 32). Sikkerhetsleder skal forvalte styringssystemet for sikkerhet, informasjonssikkerhetsleder forvalter styringssystem for informasjonssikkerhet, ISMS. Sikkerhets- og informasjonssikkerhetsleder har koordinerende, rådgivende og styrende oppgaver, som blant annet kan inneholde revisjoner, fasilitere risikovurderinger, jobbe med veiledning og kompetansebygging, planlegge øvelser, følge opp tiltak og rapportere til ledelsen (NSM 2015).

2.1.4.2 Utøvende sikkerhetsfunksjoner

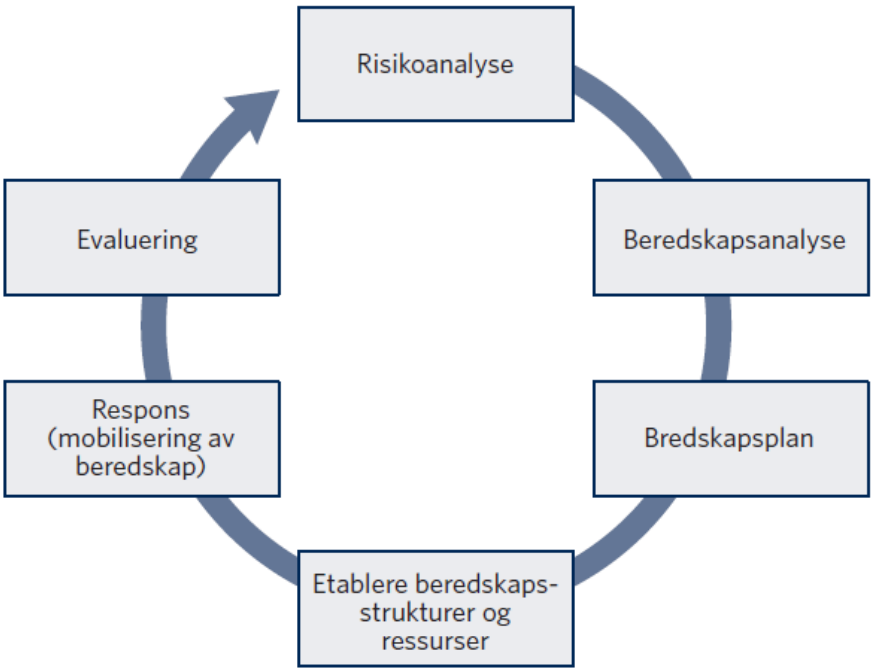
I følge NSM (2015) er det, innenfor IT-sikkerhet, behov for ressurser som har en mer teknisk og operativ IT-sikkerhetskompetanse. Disse er ofte organisert under IKT-funksjonen (NSM 2015, s. 48), men må rapportere, og arbeide tett med, sikkerhetsstaben (NSM 2015, s. 33). Dette kan innebære blant annet å ha oversikt over IT-infrastruktur, herunder eksempelvis nettverk. Ha endringskontroll, herunder også logg, deteksjon, etablere IDS[1]-er i nettverket for å overvåke og inspisere trafikken, samt motta, agere og koordinere trusselinformasjon, samt skanne virksomhetens infrastruktur for sårbarheter og jobbe med å redusere disse. I større virksomheter kan det også være en CERT[2]-funksjon, som blant annet skal varsle og håndtere angrep.

2.2 Beredskap

2.2.1 Beredskap – faser og aktiviteter i beredskapen

I følge Engen et. al (2016) er formålet med beredskap ”*å forutse mulige trusler og utfordringer slik at de kan håndteres på en effektiv måte, for så å etablere ressurser og utstyr for å håndtere disse*” (Engen et al. 2016, s. 280), og videre hevdes det at beredskapsarbeid er forberedelser til håndtering av de kriser man ikke kan forebygge. I dette ligger flere aktiviteter fordelt på faser, som til sammen bidrar til en god beredskap. Disse fasene er henholdsvis inndelt i risikoanalyser, beredskapsanalyser, beredskapsplan, øvelser.

[1] Intrusion Detection System
[2] Computer Emergency Response Team



Figur 2 - Faser i beredskapsarbeid (Engen et al. 2016).

2.2.2 Risiko- og beredskapsanalyser

En risikoanalyse er et viktig element i et helhetlig arbeid med sikkerhet, både som selvstendig dokumentasjon, som et ledd i beslutningsprosesser og som innspill til en rekke andre tilstøtende prosesser, som eksempelvis beredskapsplanlegging. ”*Hensikten med analysene er å finne frem til best mulige løsninger og tiltak sett i forhold til de mål en har satt seg*” (Aven et al., 2008, s. 16). For å avdekke hvilke trusler eller farer man må forholde seg til, gjennomføres derfor risikoanalyser, som er viktig input til beredskapsplanlegg (Perry & Lindell 2003). En beredskapsanalyse skal legge rammer for de hendelsene man ønsker å etablere beredskap for, i tillegg til å gi et bilde av dimensjoneringen man må ta høyde for. Dimensjoneringen, og herunder også ressursbehovene, skal kartlegges. I denne prosessen kan det være relevant å både se på interne ressurser, men også å skaffe til veie oversikt over eksterne ressurser (Engen et al. 2016).

2.2.3 Skillet mellom planlegging og plan

Perry og Lindell (2003) ser på forholdet mellom tre komponenter innen beredskapsplanlegging som de anser for å være kritiske: planlegging, øvelse og skriftlige planer (Perry & Lindell 2003). Selv om de i dette arbeidet i stor grad retter seg blant annet mot offentlige og private aktører i formelle, frivillige eller politiske organisasjoner, og tar for

seg beredskapsplanlegging hovedsakelig relatert til natur- og teknologikatastrofer samt terror, og herunder arbeid mellom de relevante aktører, anses deres teorier likevel relevante for organisasjoner som enten isolert sett, eller i samarbeid med andre aktører, etablerer beredskapsprosesser med dertil tilhørende planlegging, øvelser og formelle dokumenter. De fremhever viktigheten av det å ikke blande sammen planlegging med en skriftlig plan (Perry & Lindell 2003, s. 338). I dette tilfellet er det snakk om skillet mellom beredskaps*planleggingen* og selve beredskaps*planen*, eller "*prosess versus produkt*" (Engen et al. 2016, s. 291).

Bakgrunnen for dette, hevder Perry & Lindell (2003), er at planlegging er en mer eller mindre evigvarende (jurisdiksjonell) prosess, mens planen, herunder forstått som den skriftlige planen, kun er et øyeblikksbilde av prosessen som helhet. Av dette følger at de skriftlige planene ikke kan isoleres fra beredskapsprosessens øvrige komponenter, men heller være en integrert del av det totale beredskapsarbeidet. Dette støttes av Engen et. al (2016), som poengterer at planleggingsprosessen skal ende i et planverk ved behovsavklaringer, deltagelse, strategier både for beredskapsprosess og –produkt, samt justeringer enten som følge av endringer i forutsetningene eller som følge av erfaringer hentet fra praktiske øvelser eller faktiske hendelser. Eksempelvis er blant annet trusler, ressurser og omgivelser dynamiske, og de endrer seg med tiden. Dette må reflekteres i beredskapsplaner, slik at man ikke etablere beredskap for gårsdagens trusler (Engen et al. 2016).

2.2.4 Beredskapsplanlegging

Beredskapsplanlegging kan forstås og implementeres som en prosess (Perry & Lindell 2003). I dette ligger blant annet muligheter for utvikling og vedlikehold av individuelle prestasjoner og gruppeprestasjoner som er opparbeidet ved bruk av trening, øvelser og tilbakemeldinger. I dette ligger også mulighetene for å gå tilbake til de ulike delene eller fasene av planleggingsarbeidet, for så å se på om det er noe som forhindrer eller obstruerer evnen til å oppnå et mål. De hevder videre at den uformelle kommunikasjonen mellom aktører under en øvelse i seg selv har en verdi: Å bli kjent med hverandre, ikke minst å kjenne hverandres behov og måter å agere på, og å i praksis samarbeide om å løse et problem skaper et miljø for gjensidig forståelse, og er følgelig fruktbart for et samarbeid (Perry & Lindell 2003).

Engen et al. (2016) fremhever at en beredskapsplanlegging, hvis den skal anses for effektiv, skal "*oppmuntre til hensiktsmessig krisehåndtering*" (Engen et al. 2016, s. 289), men at det

ikke nødvendigvis er synonymt med rask respons i kriser. I dette ligger at man skal unngå impulsive handlinger fordi man ikke tar seg tid til å påse at det bildet man har av en situasjon faktisk medfører korrekthet (Engen et al. 2016). Videre bør planleggingsprosessen legge opp til fleksibilitet, heller enn detaljstyring, da behovene i en krise kan være skiftende. Et høyt detaljnivå i en beredskapsplan medfører at den raskt blir utdatert, og fordrer dermed stadige oppdateringer (Engen et al. 2016 og Perry & Lindell 2003). Det er videre viktig med kjennskap til hvilke menneskelige reaksjoner som er sannsynlig eller ikke, slik at man reduserer faren for feil ressursbruk (Engen et el. 2016).

2.2.5 Beredskapsplan

Beredskapsplanen er den fysiske dokumentasjonen på den beredskapen man etablerer. I dette ligger de rent praktiske stegene, ressursene og utstyret som omfattes i beredskapen. Den skal sikre de viktigste verdiene i en organisasjon, herunder først og fremst liv og helse, men også andre verdier en organisasjon forvalter. For at beredskapsplanen skal være hensiktsmessig, må det være gjort en prioritering av verdier på forhånd, og en kartlegging av ressursbehov. Med bakgrunn i risiko- og beredskapsanalysene skal det i beredskapsplanen fremkomme oversikt over blant annet hvem som har ansvaret for hva, hvem som skal kontaktes når, hvem som kan beslutte, hvor og når dette skal skje etc. I følge Engen et al. (2016) skal beredskapsplanen ”*sikre at responsen i en krise er planlagt, forutsigbar, effektiv og koordinert*” (Engen et al. 2016, s. 286), og har listet opp noen punkter som de mener kjennetegner en god beredskapsplan, herunder kortfattet, forståelig, skal kunne brukes under stor usikkerhet, forholde seg til tidspress, skal løpende evalueres og oppdateres og skal skape beredskapsbevissthet.

Beredskapsplanen er et levende dokument. Endringer i trusselbilde, verdier, ressurssituasjon og –behov, samt en rekke andre områder, vil kunne påvirke beredskapsplanen, og følgelig vil den ikke kunne defineres som ferdig. Videre er det formålstjenlig med en helhetlig tilnærming til beredskapsplanleggingen slik at man kan holde beredskapsplanen på et mest mulig generisk nivå. Eksempelvis kan en beredskapsplan ha en todelt operativ del der den ene er generisk og ”bred”, mens en annen del i større grad tar for seg mer definerte og spesifikke hendelser og hvordan disse skal håndteres. Det ligger en fare i at man etablere beredskapsplaner som ikke kan brukes fordi de er praktisk gjennomførbare, såkalte ”fantasidokumenter” eller en symbolsk beredskap (Engen et al. 2016). Det er i tillegg svært

viktig at beredskapsplanen er kompatibel med andre aktører og organisasjoners planer i grenseflatene mellom de ulike beredskapsplanene (Engen et al. 2016).

2.2.6 Øvelser

Å øve på hendelser og kriser gir viktig input til evaluering av beredskapen. Gjentatte øvelser i å håndtere hendelser vil over tid kunne styrke en organisasjons evne til å sette sammen er fungerende beredskap (Perry & Lindell 2003). Dersom det under en øvelse ikke avdekkes noen problemer, mener Perry & Lindell (2003) at det er grunn til å anta at scenariet det er øvd på enten er for enkelt eller at evalueringen i ettertid er for dårlig (Perry & Lindell 2003). Utover dette er øvelser en mulighet for å opprette kontakt med andre aktører og organisasjoner man ellers ikke jobber tett på (Engen et al. 2016). Det er altså antatt at det er et positivt tegn å avdekke konflikter, manglende koordiner og andre problemer i denne delen av beredskapsarbeidet.

NSM (2015) trekker frem eksempler på tre typer øvelser, herunder skrivebordøvelser hvor man gjennomfører teoretisk øvelse med begrenset omfang. I dette ligger blant annet å ta utgangspunkt i noen scenarier, og gå gjennom beredskapsplanen med hensyn på disse. En slik øvelse er gjerne begrenset til enkelte funksjoner. Den andre typen øvelse er spilløvelser, der man benytter en dreiebok, og alle som har definerte roller i beredskapsplanen skal delta. En tredje type øvelse er feltøvelser, hvor man får en realistisk gjennomgang beredskapsplanen. Disse er spesielt nyttige i scenarier hvor koordinering av andre parter er nødvendig, eksempelvis nødetater. Forskjellen på spill- og feltøvelser er at tiltak skal iverksettes i feltøvelsene.

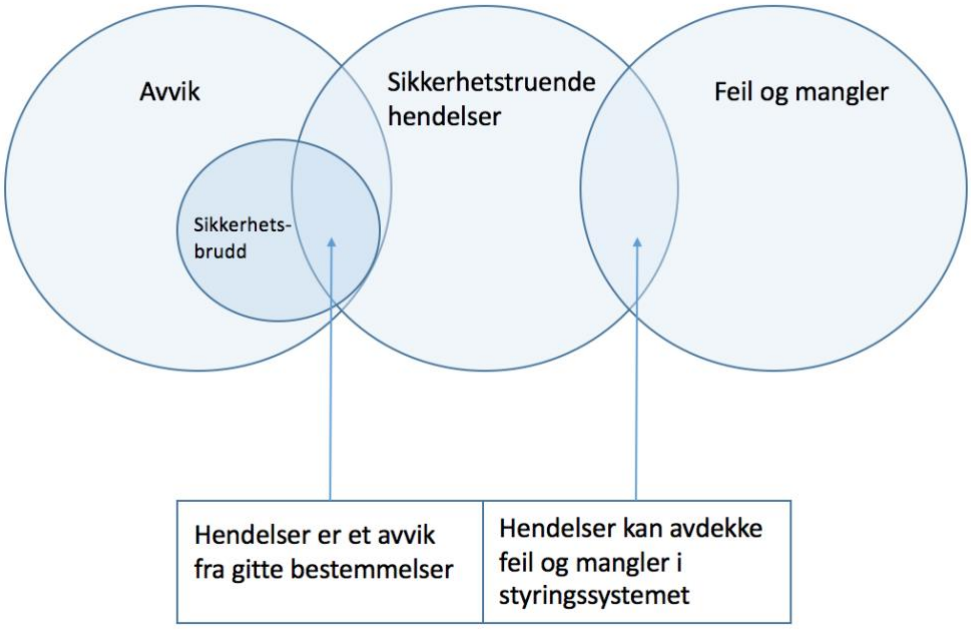
2.2.7 Beredskapsprinsipper

I Norge foreligger det fire prinsipper som samfunnssikkerhets- og beredskapsarbeidet er organisert etter (Engen et. al 2016). Disse er henholdsvis ansvarsprinsippet, likhetsprinsippet, nærhetsprinsippet og samvirkeprinsippet. Ansvarsprinsippet innebærer at det er den som har det daglige ansvaret for et område, som også har ansvar for tjenesten under en krise eller katastrofe, samt planlegging og forberedelser. Likhetsprinsippet betyr at organiseringen både til daglig og under krise skal være mest mulig lik. Nærhetsprinsippet tar utgangspunkt i at den med best forutsetninger for å forstå en situasjon, ofte er den som er nærmest krisen. Det er derfor et prinsipp at håndteringen av kriser skal foregå på lavest mulig nivå. Med

samvirkeprinsippet påligger det virksomheten, eventuelt myndigheten eller etaten, et selvstendig ansvar for å påse at best mulig samarbeid med andre relevante aktører i forbindelse med beredskapsarbeidet, herunder også forebygging og krisehåndtering (Engen et. al 2016).

2.2.8 Hendelseshåndtering

Dersom pålagte krav, enten til eller av virksomheten, ikke er fulgt, oppstår et avvik eller en hendelse som har det til felles av det kan skade eller true verdier (NSM 2015).
I følge NSM (2015) skjer korrigering av avvik på to nivåer, henholdsvis at avviket korrigeres og at man finner årsakene til at avviket oppsto for å hindre at tilsvarende avvik skjer på nytt. NSM deler hendelser og avvik inn i tre kategorier, henholdsvis feil og mangler, avvik og sikkerhetstruende hendelser. De tre relaterer seg til styringssystemet for sikkerhet.



Figur 1 - Forholdet mellom de ulike hendelses- og avvikskategoriene, etter NSM (2015, s. 24)

Feil og mangler relaterer seg til forhold som ikke er regulert i interne retningslinjer. Avvik er derimot brudd krav eller føringer, og kan ha ulik alvorlighetsgrad. Sikkerhetstruende hendelser er alvorlige hendelser som kan innebære, for IT-sikkerhetssiden, tap av informasjonssikkerhetsprinsippene konfidensialitet, integritet og tilgjengelighet av varierende grad. Disse kan blant annet komme av systematiske feil i den forebyggende sikkerheten eller ikke være fanget opp av risikovurderinger og tiltak (NSM 2015, s. 24). Videre skal avvik og

hendelser, for å redusere risiko og hindre gjentagelse, registreres, rapporteres og håndteres internt i virksomheten (NSM 2015).

2.3 Sårbarheter

I følge Sårbarhetsutvalget, er en sårbarhet ”(…) *et uttrykk for de problemer et system vil få med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet. Sårbarhet er knyttet opp til mulig tap av verdi.”* (NOU 2000:24: 18). Dette innebærer ikke en definisjon av hvorvidt hendelsen er tilsiktet eller ikke, men snarere et uttrykk for symptomer.

En utbredt definisjon av sårbarhet innen IT-sikkerhet, av det engelske *vulnerability*, er imidlertid en feil eller svakhet i et system eller prosessene rundt. Disse feilene eller manglene kan medføre at IT-sikkerheten kan utsettes for en trussel eller en fare. En slik sårbarhet eller svakhet kan videre utnyttes av en trusselagent (Rausand og Utne. 2014, s. 27). NSM benytter samme definisjon i sin årlige rapport om IKT-risikobilde, hvor de skisserer sårbarhetskartlegging som mulig forarbeid til eventuelle senere operasjoner, hvor de vil kunne utnytte sårbarheter for å komme seg videre inn i en virksomhets infrastruktur (NSM 2018, s. 10).

Sårbarhet som begrep har derfor en noen avvikende betydning innen informasjonssikkerhet kontra den generelle forståelsen av begrepet innen sikkerhet. Og hvor sårbarheter innen IT-sikkerhet relaterer seg mer til en svakhet ved et system som tilrettelegger for en uønsket hendelse mer enn en svakhet som kan oppstå som følge av en uønsket hendelse.

I følge Lysneutvalget kan digitale sårbarheter deles i to kategorier (NOU 2015:13, s. 31):

1. *Sårbarheter som er kjent og akseptert fordi det blir vurdert at kostnadene ved de aktuelle tiltakene ikke står i forhold til skadepotensialet, trusselen eller verdien.*
2. *Sårbarheter som ikke blir gjenstand for tiltak fordi sårbarheten enten er ukjent, feilvurdert, ikke forstått eller mangelfullt kommunisert.*

Lysneutvalget peker videre på at for digitale sårbarheter, er det de sårbarheter som faller under punkt to, som utgjør et særlig problem (NOU 2015:13, s. 31).

Programvare er særlig utsatt for aktører som søker etter sårbarheter (NOU 2015:13, s. 39). Programvare er en del av omtrent alt vi omgir oss med, fra mobiltelefoner, biler, strømmålere og datamaskiner. Derfor utgjør dette en viktig sårbarhet innenfor IT. Ved utvikling av programvare er det først og fremst funksjonalitet som er driveren. Dette medfører ofte et ønske om å spare tid, og dermed er det ikke uvanlig å gjenbruke kodesnutter for vanlige funksjoner. En slik gjenbruk innebærer dog også at svakheter i koden spres til ny programvare (NOU 2015:13).

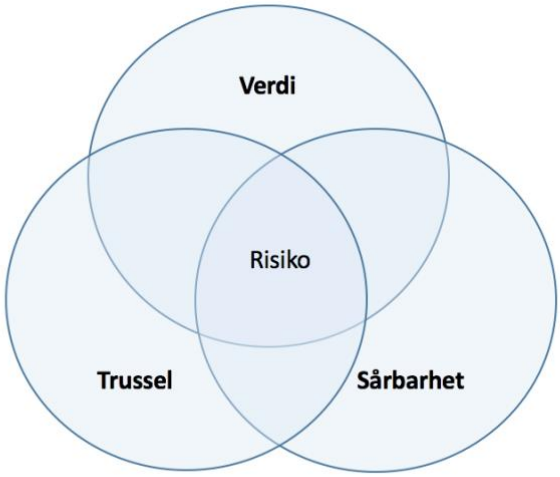
NSM (2016) deler sårbarheter inn i tre kategorier, henholdsvis de organisatoriske sårbarhetene som går på styring, de menneskelige sårbarhetene og de teknologiske sårbarhetene, hvorav også IT inngår. Det stilles videre opp eksempler på sårbarheter som går på IT, hvor blant annet manglende oppgradering av program- og maskinvare og manglende herding av applikasjoner nevnes som eksempler (NSM 2016, s. 20).

2.4 Risiko

I følge Refsdal et. al (2015) refererer risiko til en rekke konsepter som til sammen utgjør en risiko. I dette ligger kombinasjonen av hendelser som kan inntreffe, sannsynligheten for at hendelsene inntreffer, konsekvensene av de eventuelle hendelsene, og hvilke verdier de eventuelle hendelsene kan få konsekvenser for. Dette innebærer at selv om en hendelse vil kunne være noe negativt, er det omstendighetene, herunder også verdien, som avgjør om en hendelse er negativ eller ikke (Refstad et al., 2015, s. 10-11).
Lyseutvalget viser, i NOU 2015:13 til NS 5814:2008 (108) og NS 5832:2014 for å beskrive risiko som henholdsvis:
"(...) en kombinasjon av sannsynligheten for og konsekvensen av en uønsket hendelse" (NOU 2015:13, s. 32)
Og
"*(...) forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen*" (NOU 2015:13, s. 32)

Førstnevnte benyttes gjerne i forbindelse med utilsiktede angrep, mens sistnevnte benyttes ved tilsiktede angrep, der man må ta høyde for at det finnes aktører som bevisst går inn for å skade, og som har den nødvendige kapasiteten og viljen til å gjennomføre. En slik aktør vil ha evne og mulighet til å opptre smidig, og vil kunne justere taktikk i møte med endringer i det

forestående offerets sikkerhetstiltak etter hvert som trusselsituasjonen endrer seg (NOU 2015:13, s. 32).
I følge NSM (2016) er det, i risikovurderinger hvor man har fokus på tilsiktede uønskede handlinger, ofte en fordel å se på risiko som en funksjon av verdi, trussel og sårbarhet.



Figur 2 - Trefaktormodell etter NSM (2016, s. 9)

Ettersom man ikke med sikkerhet kan vite hva som kommer til å skje i fremtiden, ei heller hvilke konsekvenser disse eventuelle hendelsene kan få, har man en usikkerhet både rundt hva som kan skje og hvilke konsekvenser det kan medføre (Aven et. al, 2010).

Rausand og Utne. (2014) påpeker at risiko viser til eventuelle fremtidige hendelser, og at mulige fremtidige hendelser nødvendigvis vil være forbundet med usikkerhet. Normalt vil man ikke kunne være sikker på hvorvidt en uønsket hendelse vil inntreffe eller ikke, og derav benyttes sannsynlighet for å anslå hvorvidt en uønsket hendelse vil inntreffe eller ikke, og frekvens for å anslå hvor ofte den uønskede hendelsen eventuelt vil inntreffe (Rausand og Utne 2014, s. 22).

Avens definisjon av risiko tar høyde for usikkerheten i risiko, i det han definerer risiko som ”*kombinasjonen av konsekvensene C av en aktiviteten og tilhørende usikkerhet U*” (Aven 2015, s. 60). Usikkerheten reflekterer her usikkerheten rundt hva konsekvensen vil bli, all den tid denne er fremtidig, og vil ofte kunne uttrykkes i sannsynlighet (Aven 2015).
Engen et al (2016) viser til Aven og Renn (2010), som hevder at sannsynligheten i seg selv ikke er nok til å uttrykke usikkerheten.

Engen et al (2010) viser til Renn (2008), som, etter å ha klassifisert risikoer, skiller ytterligere mellom fire ulike risikoer. Disse er henholdsvis lineære risikoer, komplekse risikoer, tvetydige risikoer og usikre risikoer. De lineære risikoene peker på forholdsvis kjente hendelser og situasjoner hvor man har tilgjengelig en del data. De komplekse risikoene viser til kompliserte årsak-virkningssammenhenger, der det er vanskelig å knytte årsak og effekt av en hendelse sammen. Tvetydige risikoer "viser til hvordan vi tenker om, mener om og vurderer de risikoene vi står overfor" (Engen et. al 2016, s. 85). De usikre risikoene er vanskeligheter med å forutse hendelser og konsekvenser. Disse er ofte knyttet til usikkerhet. I tillegg vil graden av usikkerhet variere, som kan spenne fra blant annet det vi vet at vi ikke vet til det vi ikke vet at vi ikke vet. Sistnevnte, det vi ikke vet at vi ikke vet, omtales noen ganger som *svarte svaner* (Engen et al, 2016). Svarte svaner er en metafor for hendelser som oppstår svært sjelden, kommer veldig overraskende på, og som kan ha svært vidstrakte eller alvorlige konsekvenser (Refsdal et. al, 2015).

2.5 Risikoanalyse og –vurdering

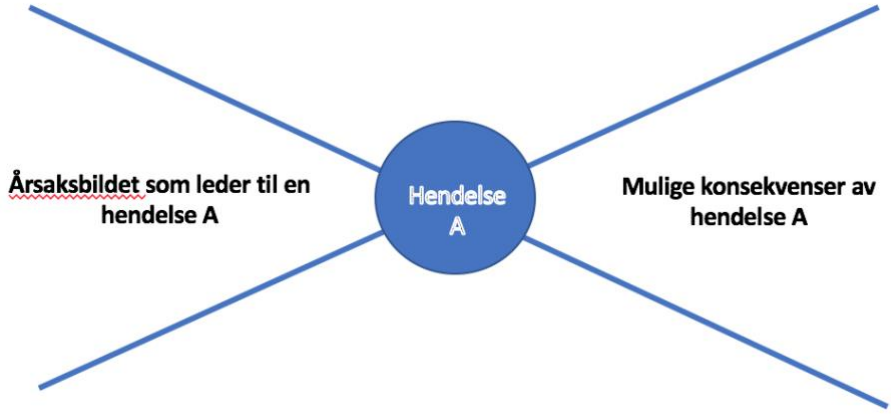
2.5.1 Risikoanalysen og de forberedende stegene

I følge Aven et. al (2010) har risikoanalyser "*som mål å kartlegge og beskrive risiko*" (Aven et. al, 2010, s.13), der risiko er mulige, fremtidige hendelser, og dermed har en iboende usikkerhet ved seg. Risikoanalyser kan gjennomføres på ulike måter, og det finnes en rekke metoder for å kartlegge og beskrive risiko. I følge Aven et. al (2010) er formålet som i stor grad er førende for hvilken metode som egner seg best, og vil være mest hensiktsmessig å benytte seg av, for gjennomføring av en risikoanalyse. Videre pekes det på en overordnet kategorisering av tre risikoanalysemetoder: forenklet risikoanalyse, standard risikoanalyse og modellbasert risikoanalyse (Aven et. al, 2010). Den forenklede risikoanalysen har en kvalitativ fremgangsmåte, standard risikoanalyse kan være både kvalitativ og kvantitativ, mens modellbaserte risikoanalyser som regel er kvantitative og benytter gjerne teknikker som eksempelvis feiltreanalyse. Kvantitative risikoanalyser spenner fra små standardanalyser med predefinerte skalaer til store og komplekse analyser hvor en rekke beregninger gjennomføres. følge Refsdal et. al (2015) fungerer kvantitative risikoanalyser best på et mer fingranulert og teknisk nivå inne IT-sikkerhet.

I følge Aven (2010) kan en risikoanalyse benyttes for å etablere et risikobilde. I dette ligger identifiserte forhold som kan påvirke risikobildet og tiltakenes effekt på risiko. Imidlertid gjennomføres risikoanalyser ofte fordi det stilles som krav (Aven 2010, s. 16), herunder som følge av lovverk eller andre interne eller eksterne krav. Imidlertid bør motivasjonen med en risikoanalyse være å skaffe til veie et godt beslutningsunderlag (Aven 2010).

En risikoanalyseprosess kan deles inn i flere trinn etter hvilke aktiviteter som skal gjøres. Målsettingen ved analysen, samt kompleksiteten i det man analysere, avgjør om alle eller bare noen av trinnene sal være med, samt hvilke rekkefølge de bør komme i (Refsdal et. al, 2014): *Etablere målsetting og rammebetingelser* for risikoanalysen, hvor man innhenter bakgrunnsinformasjon, formelle rammebetingelser, risikoakseptkriterier og interessenter. Neste steg er *systembeskrivelse og omfang av analysen*, hvor man innhenter mer spesifikk informasjon rundt analyseobjektets funksjoner, hvilke verdier som er relevante, hvilke farekilder som bær vurderes, sikkerhets- og barrierefunksjoner, hvor detaljert risikoanalysen skal være.

Det tredje trinnet er å *identifisere farekilder og mulige uønskede hendelser*. I dette trinnet, som i følge Refsdal et. al (2014) er et av de viktigste trinnene i risikoanalysen, skal man identifisere mulige farekilder og trusler som er relevante, herunder trusselagenter, samt mulige uønskede hendelser som kan inntreffe. Det fjerde trinnet er *utvelgelse av relevante uønskede hendelser*, hvor man velger ut hvilke hendelser som er mest relevante basert på ulike kriterier, samt definere hva en typisk hendelse er. Det femte og sjette trinnet er å *bestemme konsekvensene av, og frekvensene til, de uønskede hendelsene*. Det syvende trinnet er *følsomhets- og usikkerhetsanalyser*, hvor man ser på inngangsstørrelsene og hvilke usikkerheter det er i resultatene. Det åttende og endelige trinnet er *risikobilde og rapportering*, hvor en sammenstilling av avdekkede uønskede hendelser fremstilles, og ser på hvilke kommunikasjonskrav som stilles til rapporten, herunder om den skal være åpent tilgjengelig eller ikke, og hvem som er målgruppen.



Figur 3 - Generisk variant av Bowtie etter Aven et. al (2010) s. 13

Når man først skal i gang med en risikoanalyse, vil et naturlig førsteskritt, i følge Aven et. al. (2010) være å kartlegge mulige initierende hendelser (Aven et al., 2010, s.55). Initierende hendelser forstås her som en mulig trussel eller fare, og man vil derfor kunne se på de eventuelle trusler eller farer man ønsker å sikre seg mot. I følge Taylor et. al (2017) bør det første steget i en risikoanalyse innenfor IT-sikkerhet være vurdering av en virksomhets eksisterende informasjonsinfrastruktur, herunder IT-systemer. I dette ligger også å evaluere de prosessuelle og organisatoriske strukturene i virksomheten. Grunnlaget for dette er å se på strategien for skalerbarheten i systemene, eksempelvis ved økende bruk av IT-systemene, utvidelse av funksjonalitet i en løsning og lignende. Noe av utfordringen ved bruk av IT er forståelsen, eller mangel på sådan, for kompleksiteten av IT-sikkerhet.

2.5.2 Risikovurdering

Det finnes flere teorier rundt hva som ligger i en risikovurderingsprosess, og hvordan denne bør deles opp i underprosesser og –aktiviteter for å best mulig kunne avdekke og vurdere risikoene i et system. I følge Lysneutvalget er formålet med risikovurderinger ”*å prioritere begrensede ressurser i arbeidet med å oppnå ønsket sikkerhetsnivå*” (NOU 2015:13, s. 32).

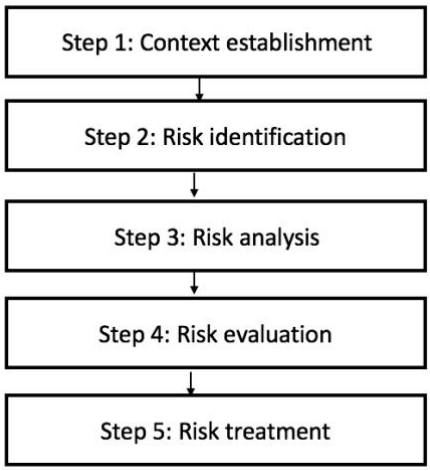
Busmunrud et al. (2015) beskriver hensikten med risikovurderinger som ”*å fremskaffe en beskrivelse av risiko som beslutningstagere kan bruke for å vurdere om risikoen er akseptabel, og eventuelt vurdere hvilke sikringstiltak som må settes inn for å bringe risikoen ned på et akseptabelt nivå. Denne beskrivelsen må kommuniseres på en slik måte at det er forståelig for beslutningstagerne*” (Busmunrud et al. 2015, s. 69). Videre poengteres det at

ansvaret for dette tilligger risikoanalytikerne, som må påse at beslutningstagerne oppfatter resultatet av risikovurderingen korrekt.

Aven et al (2010) beskriver risikovurdering som:
Risikoanalyse + Risikoevaluering = Risikovurdering (Aven et. al 2010, s. 20).
Hvor risikovurdering etterfølges av risikohåndtering. Risikovurdering er således der man forsøker å modifisere risiko ved implementering av virkemidler og tiltak. Risikoevaluering er evaluering av resultatene fra risikoanalysen (Aven 2015).

I følge Rausand og Utne (2014) er risikovurdering en samlet prosess i tre overordnede faser som, i tillegg til å omfatte risikoanalyse og – evaluering, også inkluderer selve planleggingen av disse. Etter disse tre fasene, og som en del av den større *risikostyringsprosessen*, kommer også risikokontroll og –reduksjon. Som forberedelse til en risikoanalyse inngår å finne og avdekke mulige interessenter, scopet for vurderingen og tidsplanen. I selve risikoanalysefasen inngår farekilder og uønskede hendelser som kan treffe analyseobjektet. I tillegg å se på hvilke sikkerhetsbarrierer som kan redusere eller hindre sannsynligheten for at en hendelse inntreffer elle konsekvensene av denne, samt å se på eventuelle konsekvenser og det estimerte frekvensbildet av disse. Deretter følger risikoevalueringsfasen der man beskriver risikoene avdekket, vurderer disse og foreslår mitigerende, eller risikoreduserende tiltak so kan iverksettes for å komme til et akseptabelt risikonivå.

Refsdal et. al (2015) definerer risikovurdering som en prosess i fem steg, hvis aktiviteter til sammen har som formål å dokumentere risiko tilknyttet ”noe” spesifikt, herunder eksempelvis deler av et system eller en organisasjon.



Figur 4 - Egen skisse etter Refsdal et. al (2015), s.16

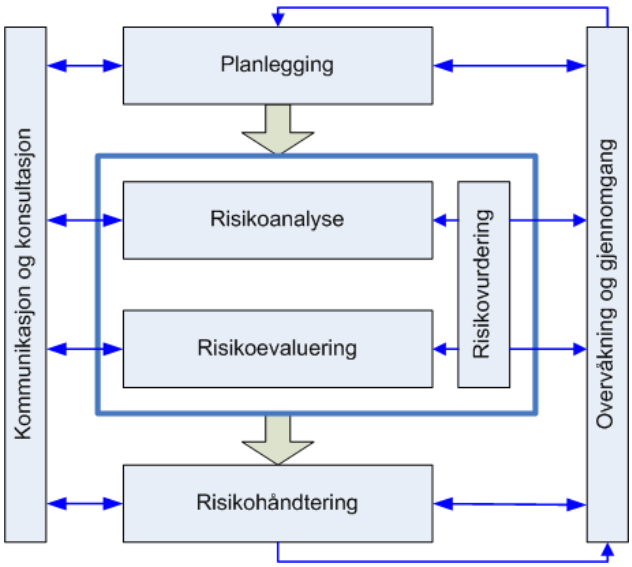
Risikovurderingsprosessen starter, i følge Refsdal et. al (2015) med en forberedende aktivitet i kontekstetableringen. I dette første steget i risikovurderingsprosessen er formålet blant annet å avklare og dokumentere scopet for vurderingen, hvilke interne og eksterne kontekster som er relevante for vurderingen, herunder prosesser rundt det spesifikke systemet som lovverk, interessenter og formålet for selve vurderingen. Deretter følger risikoidentifisering, som innebærer å dokumentere risikoer og eventuelle årsaker til at risikoen oppstår. Videre er selve risikoanalysen, som er alle aktivitetene man gjennomfører for å kunne avgjøre hvilket nivå de ulike risikoene man identifiserte i forrige steg ligger på, herunder å estimere hvilken sannsynlighet det er for at en hendelse inntreffer, samt hvilke konsekvenser en slik hendelse kan få. Det fjerde steget i risikovurderingsprosessen er en risikoevaluering, som innebærer å vurdere risikoene man har analysert opp mot risikokriterier som foreligger. Deretter skal risikoene vurderes opp mot hverandre, for blant annet å avgjøre hvilke risikoer som eventuelt bør aggregeres. Det femte og siste steget i risikovurderingsprosessen Refsdal et. al (2015) skisserer, er risikobehandlingen. I risikobehandlingen skal mitigerende og risikoreduserende tiltak beskrives.

I følge Refsdal et. al (2015) er det særlig to aspekter som skiller risikovurderinger av cybersystemer fra risikovurderinger generelt. Disse relaterer seg til cyberspace i seg selv, og hva det betyr med hensyn til hvilke trusler det at cyberspace har et globalt nedslagsfelt kan by på, samt det potensielt høye antallet trusler og trusselkilder, være seg av ondsinnet natur eller ikke. I praksis innebærer dette blant annet at risikoidentifiseringssteget i

risikovurderingsprosessen deles i to, der man skiller mellom ondsinnede og ikke-ondsinnede risikoer (Refsdal et. al 2015, s. 35). Med ondsinnede risikoer menes her risikoer som følge av tilsiktede angrep, og ikke-ondsinnede risikoer handlinger som følger av utilsiktede hendelser

2.6 Risikostyring

Aven (2015) sier at ”*Med risikostyring forstås alle tiltak og aktiviteter som gjøres for å styre risiko. Risikostyring handler på den ene siden om å få innsikt i risikoforhold, effekt av tiltak, grad av styrbarhet av risiko osv., og på den andre siden metoder, prosesser og strategier for å kunne kartlegge og styre risikoene*.” (Aven 2015, s. 13). Risikostyring er i følge Aven (2015) således todelt, der man på én side fokuserer på risikoene og tiltakene, og på den andre siden det strategiske og prosessuelle i forbindelse med kartlegging og styring av risikoer. Og hvor formålet er å balansere det å skape verdier med det å unngå tap (Aven 2015, s. 14).
I dette ligger å ta beslutninger om risiko, hva som er akseptert og ikke, også innenfor blant annet definerte økonomiske og praktiske rammer. Dette igjen, avhenger av virksomhetens mål og visjoner (Aven et al. 2008). Videre påpekes det at ledelsens rolle i risikostyringsarbeidet er sentral. Det å lykkes med risikostyring innebærer at det foreligger en forankring hos ledelsen. Utover dette er en overordnet videre strategi for risikostyringen nødvendig. Prosesser og rutiner må etableres, og det må foreligge en styringsstruktur der det tydelig fremkommer roller og ansvar. Videre må risikostyringsprosessen forankres i organisasjonen, i analyse- og støttesystemer, og så i kommunikasjon og arbeid som er med på å utvikle kompetanse og motivasjon i den aktuelle organisasjonen (Aven et al. 2008).



Figur 5 - Risikostyringsprosess ISO 2005 (Aven et al. 2010, s. 20)

Aven (2015) hevder videre at risikostyring gjennomføres som styringsprosesser tradisjonelt gjør, og vil derfor innbefatte blant annet situasjonskartlegging, fastsetting av målformuleringer, utredninger av alternativer, analysering og konsekvensvurdering før man velger løsning. For å kunne gi tilstrekkelig beslutningsstøtte, skal det gjennomføres ulike analyser, hvor prosessen i seg selv er iterativ og vil kunne bli gjenstand for forbedringer underveis (Aven, 2015).

Aven (2015) presenterer videre fem suksessfaktorer for risikostyring. Den første av disse er betydningen av å forstå de grunnleggende prinsippene. I dette ligger forståelse blant annet for hva risiko og usikkerhet er og betyr, og videre også hva kost-nytteanalysens basis er, usikkerhet og risikoanalysens resultater (Aven 2015, s. 161). Han hevder mange ledere og eksperter innen risikoanalyse og –styring ikke forstår ”*de fundamentale byggeklossene innen fagområdet*” (Aven 2015, s. 161). Han stiller seg videre spørsmålet hvordan risikoanalyser med hell da skal kunne anvendes i en beslutningskontekst (Aven 2015, s. 162).

Den andre suksessfaktoren er å ha fokus på usikkerhet, kunnskapsstyrke og potensielle overraskelser (sorte svaner). I dette ligger en hensiktsmessig måte å presentere usikkerheter på, da ledere og beslutningstakere kan, og er vant med, å forholde seg til usikkerhet. Usikkerheten må derfor presenteres på en hensiktsmessig måte, slik at underlaget er godt nok for beslutninger (Aven 2015).

Den tredje suksessfaktoren Aven (2015) presenterer, er bruk av sensitivitets- og robusthetsanalyser, hvor sensitivitetsanalysene tar utgangspunkt i endringer i inngangsparameterne, og ser effekten av disse har på resultatet, mens robusthetsanalysene ser på ”*hva som må til av endring i en størrelse*” for å påvirke konklusjonen (Aven 2015, s. 165).

Den fjerde suksessfaktoren er bruk av kost-nytteanalyser. Aven (2015) advarer mot at kost-nytteanalyser ikke alltid entydig er det beste, da den baserer seg på en risikonøytral tankegang med en forventningsbasert strategi. Imidlertid argumenterer Aven (2015) videre for at det alltid vil være usikkerhet, og at det innebærer en avveining mellom risikosøkende og risikoavers, hvor usikkerheten blir viktig i balansen mellom ulike hensyn.

Den femte og siste suksessfaktoren er bruk av beslutningskriterier, risikoakseptkriterier og andre krav. I dette ligger at for å kunne ta gode beslutninger, er man avhengig av klarhet i beslutningskriteriene. Det kan være mange hensyn som kan påvirke beslutninger, herunder både strategiske vurderinger rundt utvikling i marked og teknologi, men også eksempelvis omdømme, sikkerhet og lønnsomhet. Det er ikke alltid mulig å skulle vurdere alle relevante faktorer. På én side har man kriteriet hvor man skal "*balansere alle relevante hensyn*" og på motsatt side "*utstrakt bruk av spesifikke krav*", eksempelvis risikoakseptkriterier for å forenkle beslutningsprosessen (Aven 2015, s. 167). Ved sistnevnte vil kriteriene etableres før, før man gjennomfører risikoanalyser og måler opp mot de etablerte kriteriene. Der resultatene av analysen ikke oppfyller kriteriene, må enten tiltak iverksettes eller man avviser løsningen. Oppfyller man derimot kriteriene, foreligger det ikke noe press om å redusere risiko. Selv en risikostyring uten bruk av risikoakseptgrenser fordrer at man setter krav og tiltak for å forenkle beslutningsprosessene (Aven 2015).

2.7 Trusselvurderinger

Det vil under presenteres teori rundt trusler, trusselaktører og trusselanalyser. Det er her valgt å hovedsakelig fokusere på trusler, i stedet for farer.

Formålet med en trusselvurdering er å beskrive trusselbildet man står overfor, med utgangspunkt i de verdier man ønsker å beskytte (NSM 2016). I dette ligger å fokusere på de intensjoner eventuelle trusselaktører kan ha for å angripe virksomheten, samt hvilken kapasitet de har til å gjennomføre et angrep (NSM 2016).

2.7.1 Trusler og trusselaktører

I følge Aven et. al (2010) er en fare og en trussel i risikosammenheng knyttet til en uønsket hendelse, nærmere bestemt den initierende hendelse. Begrepet trussel benyttes gjerne i forbindelse med handlinger som er villede, eksempelvis en terrorhandling, mens farer vanligvis benyttes i forbindelse med ulykkeshendelser som brann og fall. Dette innebærer at farer er knyttet til safety-delen av sikkerhet, og trusler til security-delen (Aven et. al, 2010).

Det er nødvendig å forstå hvem virksomhetens trusselaktørene er, og hvorfor de eventuelt nettopp skulle utgjøre en trussel mot virksomheten. Dette innebærer å se på eventuelle motiver og intensjoner som kan gjøre seg gjeldende, herunder eksempelvis hevn, spionasje,

politisk agenda eller økonomisk vinning. I tillegg til intensjoner, er også trusselaktørens evne til å gjennomføre et angrep knyttet til trusselaktørens kapasitet (Refsdal et. al 2015, s. 65). Videre, for å kunne identifisere ondsinnede risikoer, er det i følge Refsdal et. al (2015) nødvendig å forstå hvordan motparten kan komme til å angripe, hvilke sårbarheter vedkommende kan komme til å utnytte og hva som kan skje dersom vedkommende lykkes i angrepet.

NSM (2016) anbefaler å kategorisere potensielle trusler som spionasje, sabotasje, terrorhandlinger og annen alvorlig kriminalitet. Med spionasje menes målrettet og fordekt informasjonstyveri, eksempelvis ved bruk av IT-systemer. I dette kan blant annet cyberspionasje ligge. Spionasje kan være et mål i seg selv, herunder ved informasjonstyveri, eller som ledd i planlegging av andre alvorlige, tilsiktede handlinger som terror og sabotasje (NSM 2016, s. 14). Spionasje vil dermed kunne ramme konfidensialiteten til informasjonen som er utsatt. Med sabotasje menes skade på infrastruktur, data eller lignende. Sabotasje er målrettet, og vil kunne gå utover informasjonens og infrastrukturens integritet eller tilgjengelighet. Terrorhandlinger innebærer blant annet fare for liv og helse, ødeleggelse og skade på systemer og prosesser som understøtter kritiske samfunnsfunksjoner. I annen alvorlig kriminalitet ligger andre straffbare handlinger som inkluderer både organisert kriminalitet og annen kriminalitet, og som kan få store konsekvenser for verdier som mennesker og samfunn (NSM 2016, s. 14).

2.7.2 Trusselanalyser

Trusselanalyser er gjerne et av de første stegene i en risikoanalyse, hvor formålet er å kartlegge trusler gjennom en trusselidentifikasjon. I tilfeller der fokuset er farer snarere enn trusler, kalles det en fareidentifikasjon (Aven et. al 2010, s. 55). Datatilsynet anbefaler her å gjennomføre en trusselvurdering for å avdekke hvilke trusselaktører som er mest aktuelle i relasjon til de verdier man sitter på, og hvilke angrepsvektorer som er mest relevante for disse[3]. En fare ved denne delen av risikoanalysen, er at den kan bli gjentagende. I følge Aven et. al (2010, s. 55) er det ikke uvanlig å kopiere avdekkede trusler fra én analyse til neste, dersom systemene analysene omfatter, ligner hverandre. I slike tilfeller står man i fare for

[3] https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/internkontroll-og-informasjonssikkerhet/iverksette-styringssystem-for-informasjonssikkerhet/

ikke å få vurdert de rette truslene for det aktuelle systemet, fordi ulike systemer, selv med alle fellestrekk de kanskje har, også kan ha egenarter som gjør dem utsatt for andre trusler og farer. Følgelig vil man potensielt overse viktige trusler rettet mot det spesifikke systemet. Det finnes flere ulike måter å identifisere initierende hendelser på, men felles for disse er i følge Aven et. al. (2010) at de er strukturerte, være seg som følge av sjekklistegjennomgang av definerte sikkerhetskrav eller lignende.

For å få et bedre informasjonsgrunnlag, anbefaler NSM (2016) å benytte flere kilder for innhenting av informasjon om trusler, samt å vurdere kildens troverdighet. Dette vil gi bedre informasjonsgrunnlag. Det finnes en rekke offentlige kilder for informasjon om trusselbilder, herunder både fra myndigheter, organisasjoner og private selskap (NSM 2016).
NSM (2016) anbefaler videre en trinninndelt trusselvurdering:

Trinn	**Aktiviteter**
1	Informasjonsinnhenting
2	Identifisere relevante trusselaktører
3	Vurdere intensjon og kapasitet for relevante trusselaktører
4	Fastsette trusselnivå for trusselaktører basert på steg 3
5	Begrunn valg av trusselaktør og trusselnivå.
6	Kommenter vurderingens usikkerhet

Figur 6 - Fritt etter NSMs anbefalte fremgangsmåte for trusselvurdering (NSM 2016, s. 16)

3. Metode

I dette kapittelet vil det redegjøres for hvordan studien ble lagt opp. Herunder vil valg av metode begrunnes og forklares.

Oppgavens problemstilling er som følger:
I hvilken grad benyttes risiko- og trusselvurderinger aktivt i arbeid med informasjonssikkerhet, og spesifikt som input til hendelseshåndtering ved tilsiktede angrep?

For å kunne besvare problemstillingen, er det formulert tre forskningsspørsmål:

4. Hvordan gjennomføres det strategiske arbeidet med sikkerhet, herunder risiko- og trusselvurderinger?
5. Hva trengs som input i arbeidet med overvåkning og hendelseshåndtering av tilsiktede angrep?
6. På hvilken måte er det tilrettelagt for samhandling på tvers av strategisk og operativt sikkerhetsarbeid?

3.1 Valg av metode

Hensikten med forskning er "*å frembringe gyldig og troverdig kunnskap om virkeligheten*" (Jacobsen 2018, s. 15). Til dette trengs en strategi, og strategien er metoden. Videre bruker man metoden som et slags hjelpemiddel for å samle inn empiri og beskrive virkeligheten (Jacobsen, 2018).

Kvantitativ metode har de fordelene er at dataene er standardiserte, og er dermed enkle å behandle og gruppere. I følge Jacobsen (2018) vil standardisert informasjon også føre til at man kan smale inn større mengder data uten at det blir uforholdsmessig krevende. Man får en viss kritisk avstand til det eller de man ønsker å undersøke (Jacobsen 2018). En kvantitativ metode ville medført at spørsmålene som skulle stilles måtte være komplette på det tidspunkt de ble sendt ut til intervjuobjektene, og at det var et tilstrekkelig antall relevante objekter som ville besvart disse spørsmålene. Fordelene med en slik metode ville vært at man, med et større datagrunnlag, lettere kunne sammenlignet svarene mottatt, og sett om man kunne se noen generelle trekk på tvers av sektorer og organisasjoner.

Blant fordelene med en kvalitativ tilnærming er i følge Jacobsen (2018) at de er fleksible i den forstand at problemstillingen kan justeres etter hvert som man får mer informasjon. I tillegg åpner det for nyanser, all den tid informantene oppfatter og opplever ulike ting. Samtidig er det en ressurskrevende tilnærming som kan ta lang tid, og som ofte medfører at man må ta til takke med relativt sett få informanter (Jacobsen 2018). Få informanter/respondenter medfører også et generaliseringsproblem. En kvalitativ metode egner seg i følge Jacobsen (2018) når man ønsker å komme frem til hvordan noe fortolkes og forstås, og der man ønsker å få frem forståelsen av noe og se sammenhenger (Jacobsen 2018).

I denne oppgaven har hensikten vært å finne ut av risiko- og trusselvurderingenes rolle i IT-sikkerhetsarbeidet, herunder med spesiell vekt på hvorvidt, og i så fall i hvilken grad, de brukes inn i arbeidet med overvåkning og hendelseshåndtering av tilsiktede angrep.
For best å besvare oppgaven er det valgt å benytte kvalitativ fremfor kvantitativ metode. I dette ligger blant annet å basere seg på å gjennomføre lengre intervjuer av enkelte utvalgte informanter som er vurdert å ha interessant og viktig erfaring og kompetanse på området denne oppgaven omhandler. I tillegg var det vel så viktig å få informasjon om hva informantene mente var årsakene til at man handler som man gjør i de ulike virksomhetene. Og denne informasjonen fordrer i stor grad mulighet til å grave dypere i informantenes innsikt. Områdets modenhet som helhet, manglende – og/eller underrapportering av hendelser, sensitiviteten rundt arbeid IT-sikkerhetsarbeid og kompliserte prosesser er videre viktige årsaker til at det ble valgt en kvalitativ metode for å innhente informasjon. Et praktisk aspekt som medførte at kvalitativ metode ble vurdert mest hensiktsmessig, er det forholdsmessig lave antallet som til daglig jobber med, og har kunnskap om, temaet.

3.1.1 Områdets modenhet

Til tross for at informasjonssikkerhet som område har en lengre historie har informasjonssikkerhet på IT-siden en relativt sett kort historie. Det er flere årsaker til dette, herunder blant annet den raske utviklingen og eskalerende endringstakten inne digitalisering (NOU 2015:13). I tillegg har utviklingen gått såpass raskt at man neppe så for seg hvor omfattende området har blitt, og at det dermed nå er tvingende nødvendig med sikkerhet rundt informasjonsinfrastrukturen for å sikre dataene.

Mye av dette kan muligens tilskrives ITs inntog på nær sagt alle områder av samfunnet på kort tid, hvilket kan ha medført at teknologien er et stykke foran organisasjoners evne til å omstille seg. Når organisasjoner både skal levere en stabil tjeneste til publikum, samtidig som at det skal forbedre publikumstjenester, i tillegg til at de gjerne skal innovere litt også, faller fort det prosessuelle og formelle gjennom.

3.2 Innsamling av data

Metoden som er valgt, er først og fremst valgt ut fra hva som er mest hensiktsmessig for å belyse de temaer og problemstillinger som ønskes besvart i denne oppgaven. I følge Jacobsen (2018) ligger noe av styrkene ved kvalitativ metode i at det ikke er forskerens premisser som vektlegges, men snarere den eller de som undersøkes. Utover dette har tidsaspekt og ressurstilgjengelighet innenfor oppgavens avgrensinger naturligvis vært hensyntatt.

I denne oppgaven er det derfor valgt en kvalitativ metode med intervju av utvalgte relevante informanter. Utgangspunktet var eksplorerende, i den forstand at intervjuobjektenes betraktninger medførte oppfølgingsspørsmål, og dermed i større grad ble styrt av de svar som ble mottatt, enn av forhåndsdefinerte spørsmål. Det var mulig for intervjuobjektene å drodle rundt hva de mente kunne være viktige aspekter ved temaene som ble bragt frem.

Intervjuene ble gjennomført på en semistrukturert måte. Dette innebærer at spørsmålene som ble stilt var relativt sett åpne, og gav intervjuobjektene mulighet til å reflektere rundt temaene som ble tatt opp. Hensikten med en semistrukturert variant av intervjuene, var å la intervjuobjektene selv få komme med relevant informasjon, også rundt temaer og forhold som falt utenfor de direkte spørsmålene som ble stilt, men som likevel var relevante. Bakgrunnen for å gå for en semistrukturert intervjumetode var for øvrig også å unngå å komme i situasjoner der informasjon kunne omfattes av sikkerhetsloven, herunder ved krav om å gradere informasjonen, og dermed ikke kunne dele den. Fordi det ikke var gitt at spørsmål formulert før møtet ville være tilstrekkelig til å få relevant informasjon, var det avgjørende å la intervjuobjektene snakke fritt, slik at oppfølgingsspørsmål kunne stilles basert på informasjon som kom underveis. I tillegg var det mulig å bygge videre på informasjon gitt av andre intervjuobjekter, herunder ved å stille spørsmål om ett intervjuobjekt kjente seg igjen i et annet intervjuobjekts refleksjoner rundt et tema.

Intervjuguiden var grovt sett delt i fire deler for å strukturere opp intervjuene. Disse fire delene var for øvrig nært knyttet opp mot de tre forskningsspørsmålene.

Den første delen av intervjuguiden gikk på begrepsavklaring og spørsmål om virksomhetenes ISMS. Heri ligger blant annet informantenes forståelse av sårbarhet,

Den andre delen av intervjuguiden omhandlet virksomhetenes prosesser for risiko- og trusselanalyser, samt prosesser for risikohåndtering og hendelseshåndtering, om og hvordan de ulike organisasjonene gjennomfører risiko- og trusselanalyser, hvilke metoder som eventuelt benyttes, samt blant annet hvorvidt det i organisasjonen foreligger formelle prosesser for dette, eller om det gjennomføres ved behov eller ut fra andre hensyn. Og ikke minst om utfallene av risiko- og trusselanalysene følges opp. I tillegg ble det undersøkt om virksomhetene har, og følger opp, risikoregister.

Den tredje delen av intervjuguiden tok for seg virksomhetenes sikkerhetsorganisering, samhandling mellom utøvende og strategiske sikkerhetsfunksjoner, formelle prosesser for hendelseshåndtering ved tilsiktede angrep, herunder øvelser, samt hvilken samhandling de utøvende sikkerhetsfunksjonene har med andre tilsvarende utøvende sikkerhetsfunksjoner samt myndigheter.

Den fjerde og siste delen av intervjuguiden omhandlet hva slags input som går til overvåkning og hendelseshåndtering ved tilsiktede angrep. I dette ligger hvorvidt risikoprosessene benyttes, og hvis så, i hvilken grad og på hvilken måte. Hvorvidt trusselanalyser benyttes som input i overvåknings- og hendelseshåndteringsarbeidet mved tilsiktede nagrep. I tillegg hva som påvirker beslutninger som tas rundt fokus for overvåkning, hvilken rolle ledelsen spiller i planlegging og prioriteringer i arbeide med overvåkning og hendelseshåndtering av tilsiktede angrep, og hvilke prosessuelle utfordringer virksomheten møter i dette arbeidet. Som input her ble også innspill til ny sikkerhetslov diskutert.

3.4 Valg av informanter

I følge Jacobsen (2018) vil noen informanter gi bedre informasjon enn andre. Kildens nærhet til det fenomenet som undersøkes bør derfor vurderes, samt hvilken kunnskap til det aktuelle

fenomenet de ulike respondenten har, og deres vilje til å avgi korrekt informasjon (Jacobsen 2018, s. 230).

Valg av informantene var strategisk. Det var ønskelig med informanter som hadde bred erfaring innen IT-sikkerhet, både på strategisk og teknisk side. Dette var viktig for å kunne se på hvordan input fra styrende side blir brukt av den utøvende siden i arbeid med IT-sikkerhet generelt, og i forhold til tilsiktede angrep spesielt. Informantene fra strategisk IT-sikkerhetsarbeid og fra utøvende IT-sikkerhetsarbeid ville kunne ha både ulik kjennskap til egen virksomhet, ulikt forhold til trusselanalyser og ulikt perspektiv på hvilke utfordringer man opplever i sikkerhetsarbeidet.

Det var derfor viktig at informantene hadde et definert forhold til både trusler mot egen virksomhet, et strukturert arbeid med IT-sikkerhet, og enten allerede en definert gruppe som jobber aktivt med å overvåke hendelser, eller et påbegynt arbeid med å etablere en slik gruppe. I tillegg var det ønskelig å ha informanter som hadde erfaring som IT-sikkerhetsledere, all den tid disse gjerne har det overordnede perspektivet på hvordan IT-sikkerhet sees av virksomhetens ledelse. I tillegg vil disse ofte også ha en mening om hvorfor man har valgt én strategi over en annen, og hvorfor man har valgt å innrette IT-sikkerhetsarbeidet på en spesifikk måte.

Samtlige av informantene jobber direkte med informasjonssikkerhet til daglig, men som gruppe har de ulikt daglig fokus. Flere av informantene hører klart til på den strategiske siden av IT-sikkerhetsarbeidet. Disse har sålede fokus først og fremst på rutiner, prosesser, styringssystem for informasjonssikkerhet, sikkerhetsholdninger og –kultur, revisjoner og risikovurderinger. To av informantene tilhører den operative og tekniske delen av IT-sikkerhetsarbeidet, og har hovedsakelig fokus på blant annet overvåkning av trafikk i, inn og ut av nettverket, sårbarheter og logger, og å avdekke og håndtere uønskede hendelser, være seg tilsiktede eller ikke. Noen av informantene har et sikkerhetslederansvar. Dette innebærer at de leder sikkerhetsarbeidet i sin virksomhet, som regel også enten IT-sikkerhetsstaben, eller både det strategiske og utøvende IT-sikkerhetsarbeidet. I tillegg har de ansvar for den overordnede IT-sikkerheten i sin virksomhet. Dette innebærer blant annet rapportering til ledelsen.

I denne oppgaven ble det gjennomført syv intervjuer. Det er flere faktorer som har medført at antallet gjennomførte intervjuer ble på syv, herunder oppgavens omfang. I tillegg var antallet relevante og tilgjengelige informanter innen aktuelle fagområder utslagsgivende. Det ble også gjort begrensninger med hensyn til hvilke sektorer som var valgt ut. Dette, i kombinasjon med at intervjuobjektene måtte ha relevant erfaring og kjennskap til områder som ble dekket av oppgavens tema, medførte at gruppen med relevante intervjuobjekter ble ytterligere redusert. I tillegg er det gjerne slik at ressurser innenfor IT-sikkerhet samles, samt at IT-sikkerhetsoppgaver ofte aggregeres til driftsleverandører, offentlige og private, som leverer tjenester til flere organisasjoner. Dette medfører en ytterligere innsnevring av antall personer som kunne være relevante å intervjue.

Antallet intervjuer ble vurdert å være tilfredsstillende i det henseendet å belyse oppgavens problemstilling. Det relativt sett lave antallet informanter gjør at det ikke kan generaliseres på grunnlag av de svar som er mottatt. Imidlertid var hensikten først og fremst å se på et utvalg sektorer, og hvordan risiko- og trusselvurderinger gjennomføres i noen av sektorene som også drifter kritisk infrastruktur eller forvalter kritisk informasjon. Det var for øvrig særlig interessant å se på hvordan risikovurderinger og trusselanalyser benyttes aktivt, herunder både opp mot ledelse og inn mot arbeid med tilsiktede angrep. Altså ville det å ta for seg andre sektorer og andre informanter kunne gi andre svar.
I følge Jacobsen (2018) er utvalget av informanter eller respondenter i kvalitative metoder formålsstyrt. Dette betyr at det er formålet med undersøkelsen som er avgjørende for hvem som bør intervjues.

Under følger en tabell som viser en oversikt over de ulike intervjuene, hvilken sektor de kommer fra, og hvilken roller intervjuobjektene har i de ulike virksomhetene de er ansatt i. Både informantene og virksomhetene er anonymiserte. Sektor er angitt fordi dette vil kunne påvirke svarene som ble gitt. Ulike sektorer har ulik historikk, og vil kunne ha ulik oppfatning av viktigheten av aspekter ved IT-sikkerhetsarbeid, og hvordan de forstår ulike faktorer som trusler, verdier og annet som kan påvirke hvordan man jobber med risikovurderinger og trusselanalyser, samt hvordan man jobber med overvåkning og håndtering av tilsiktede angrep. For å sikre anonymiteten til intervjuobjektene, er rollebetegnelsen generisk. Flere av informantene har erfaring fra flere sektorer, men kryss er markert der de hørte hjemme i perioden for gjennomført intervju.

Nummer	Sektor			Type intervju	Varighet på intervju
	Helse	Forsvar og justis	Finans		
1	**X**			Møte	Ca 1t
2			**X**	Møte	Ca 1t
3			**X**	Telefonmøte	Ca 1,5t
4		**X**		Møte	Ca 1,5t
5		**X**		Telefonmøte	Ca 1t
6	**X**			Telefonmøte	Ca 1t
7			**X**	Telefonmøte	Ca 1t

Tabell 1 - Oversikt over informanter

3.5 Avgrensninger

I denne oppgaven er det kun sett på forhold rundt IT-sikkerhet. Dette innebærer at fysisk sikkerhet og de samfunnskritiske funksjonene de undersøkte sektorene forvalter, er ikke en del av oppgaven. I tillegg er oppgavens fokus rundt overvåkning og hendelseshåndtering rundt tilsiktede angrep mot informasjonsinfrastrukturen. Det betyr at forhold som anses for utilsiktede hendelser, som ulykker, ikke er en del av oppgaven.

Det ble derfor kun gjennomført intervjuer av informanter fra virksomheter som faller under finanssektoren, helsesektoren og justis- og forsvarssektoren. Bakgrunnen for dette var at alle disse sektorene drifter og forvalter informasjon og infrastruktur som anses for å være kritisk. Dette innebærer dog ikke at alt av informastruktur og informasjon virksomheter i disse sektorene drifter og forvalter faller under definisjonen kritisk infrastruktur.

3.6 Intervjuene

Alle intervjuene ble gjennomført individuelt og personlig, enten ved intervju ansikt-til-ansikt eller per telefon. I dette ligger at det kun var oppgavens forfatter og én informant per intervju. Intervjuene ble videre gjennomført på en semistrukturert måte. I dette ligger at det på forhånd ble utarbeidet en intervjuguide (se vedlegg A) der temaene for intervjuene var definerte, og åpningsspørsmål for de ulike temaene var skrevet. Intervjuguiden ble benyttet som en referanse under intervjuene, der det var ønskelig at informantene reflekterte over de ulike temaene, og besvarte spørsmålene basert på egne erfaringer fra de organisasjoner de selv enten har vært, eller er en del av, samt sine subjektive meninger rundt fordeler og ulemper ved

innretningen i sin(e) organisasjon(er), hva som skal til for at det skal optimaliseres og lignende. Intervjuguiden fungerte således som en rettesnor underveis i intervjuene, slik at det var mulig å spore tilbake til relevante temaer dersom informantene beveget seg for langt utenfor tema, som "huskelapp" slik at alle intervjuene var innom de samme temaene, og informasjon fra informantene derfor kunne sammenstilles og analyseres, samt

Det første intervjuet som ble holdt, ble gjennomført på som en slags pilot. Dette innebar at intervjuguiden ble testet, og justeringer ble gjort som følge av de svar og eventuelle uklarheter som ble oppdaget underveis i dette intervjuet. Pilotinformanten var klar over at oppfølgingsspørsmål kunne bli stilt på et senere tidspunkt som følge av at det ble gjort endringer etter dette intervjuet. Dette ble gjort for å få sammenlignbare data fra de ulike informantene, ettersom pilotintervjuet også var ønskelig å benytte i oppgaven. Det viste seg imidlertid at det ikke ble nødvendig, da det ble gjort lite justeringer av intervjuguiden etter pilotintervjuet, og de endringer som ble gjort, var å flytte temaer og spørsmål i forhold til hverandre slik at det ble en bedre glid, og temaer og spørsmål som naturlig påkalte hverandre ble tatt opp

De fleste informantene kom til som følge av forespørsel sendt per mail eller telefon. I forbindelse med forespørsel om intervjuer per mail, ble en presentasjon av oppgavens tema, intervjuguiden, personvernskjema, samt samtykkeerklæring, sendt over per mail. Valget om å sende intervjuguiden ut på forhånd hadde flere årsaker. For det første var det ønskelig å fremstå åpen. Mange områder og detaljer innen informasjonssikkerhet for organisasjoner som jobber med kritisk infrastruktur er i beste fall taushetsbelagt, og i ytterste konsekvens gradert informasjon. Ved å sende over intervjuguiden, hadde organisasjonene mulighet til å vurdere om dette var noen de kunne være med på, og om det var noe de følte behov for å diskutere seg imellom før de eventuelt kunne bidra, eksempelvis om det var temaer de måtte styre unna, informasjon de måtte være påpasselig med og eventuelle andre lignende temaer de måtte ta stilling til. For det andre var det ønskelig å få informanter som til daglig befatter seg med de ulike temaene for oppgaven. I så tilfelle var det å utlevere intervjuguiden nødvendig, slik at organisasjonene hadde mulighet for å finne rette ressurser.

Noen av informantene kom til som følge av bekjentskaper. Disse ble kontaktet direkte, hvorav noen av disse har jobbet som konsulenter innenfor sikkerhet ved relevante organisasjoner, men som ikke er ansatt ved noen av disse organisasjonene. Imidlertid ble det vurdert at de har

en såpass interessant bakgrunn og kompetanse, at det var ønskelig å ta disse med som informanter. De har opparbeidet seg en unik spesialkompetanse innen for enkelte av de ulike temaene som tas opp i oppgaven, i tillegg til at de som konsulenter har hatt mulighet til å høste erfaring fra flere av organisasjonene og/eller sektorene, og har hatt mulighet til å sammenligne erfaringen fra flere av disse sektorene, ofte også over tid.

Alle intervjuene tok om lag én time, og ble gjennomført enten ved personlig møte eller per telefon. Telefonmøtene ble satt opp i hovedsak enten grunnet lange avstander mellom informant og intervjuer, eller i andre tilfeller for å spare tid da flere av informantene er travle, og det var vanskelig å finne ledig tid til å møtes. Når man gjennomfører et intervju oppstår spørsmålet om man skal benytte opptak eller ikke. I følge Jacobsen (2018) har opptak den fordel at man lettere kan få med seg det informantene sier under intervjuet, og ikke minst ha øyekontakt. Samtidig kan enkelte oppleve å bli skeptiske til å bli tatt opp, og det fordrer følgelig at man ber om tillatelse først.

Det finnes også fordeler og ulemper ved bruk av notater. Fordelen er at det er enklere å gå tilbake til et tema man tidligere har forlatt, og ta opp igjen tråden dersom det kommer informasjon i sammenheng med andre temaer og spørsmål, som også er interessante i forhold til svar på tidligere temaer og spørsmål. Det er en kjensgjerning at mennesker som jobber med informasjonssikkerhet i utstrakt grad er veldig bevisst på både hvem som får tilgang til informasjon og hvordan denne skal brukes. På den annen side binder det å ta manuelle notater intervjueren i større grad enn ved å bruke båndopptager, der intervjueren og intervjuobjektene i større grad kan relaterer seg til hverandre.

Selv om det er gode grunner til å benytte opptak, ble det, av flere årsaker, besluttet å ikke benytte opptak under intervjuene. For det første var noen av informantene skeptiske, og ettersom det var flere informanter, var det ønskelig å gjennomføre intervjuene så likt som mulig, slik at grunnlaget også ble forholdsvis sammenlignbart. For det andre ble noen av intervjuene gjennomført på områder med en del støy, som ville påvirket kvaliteten på opptakene, samt at andre intervjuer igjen ble gjennomført via telefon, og blikkontakt dermed ikke var relevant likevel. I tillegg var det ønskelig å knytte de ulike svarene til intervjuguiden direkte, slik at oppfølgingsspørsmålene fulgte temaene. Det ble derfor tidlig vurdert lite hensiktsmessig å benytte opptak, ettersom det var nødvendig å ta notater under intervjuene uansett.

Under intervjuene ble intervjuguiden hyppig brukt både av særlig intervjuer, men i noen tilfeller også av informantene. Noen av informantene hadde forberedt seg, og tatt notater i intervjuguiden. For intervjueren ble intervjuguiden benyttet både som "huskeliste" for holde intervjuene strukturerte, samt også til å ta notater underveis i intervjuene. Oppklaringsspørsmål ble stilt både i forbindelse med informantenes forklaringer, samt der det var nødvendig med avklaringer.

Notatene fra intervjuene ble gjennomgått og renskrevet samme dag som respektive intervju ble holdt. Ettersom notater ble tatt underveis i intervjuene, var det lite endringer av notatene. Da notatene ble renskrevet og gjennomlest på nytt, var det enklere å også få tid til å reflektere mer over hva informantene sa, og sette deres observasjoner og tanker i perspektiv, både i forhold til betraktningene til de andre informantene, men også i forhold til teori og egne betraktninger. Av personvernhensyn ble alle intervjuene anonymisert. All lagring ble gjort lokalt og ved bruk av nøkler for å skille de ulike intervjuene fra hverandre, men samtidig anonymt.

3.7 Tolkning av data

Når man tolker informasjon, setter man informasjonen i sammenheng.
Ved bruk av kvalitativ metode, vil dataunderlaget være vanskeligere å kategorisere og strukturere, og derigjennom analysere. For å holde fokus, ble de tre forskningsspørsmålene benyttet for å sortere informasjonen. Ettersom informantene under intervjuene tidvis gikk frem og tilbake mellom de ulike temaene, ble nettopp forskningsspørsmålene brukt for å sortere informasjonen, dele informasjonen inn i logiske segmenter og analysere dem deretter. Da var det lettere å analysere informasjonen fordi den ble kategorisert likt for informantene, men beholdt samtidig sammenhengen de ulike informantene hadde dedusert seg frem til informasjonen. Da dataene skulle analyseres, var det særlig fokus på begrunnelsene for hvorfor ulike valg er tatt, eventuelt hva informantene mener er årsaken til at noe gjøres som det gjør, til valg som er tatt etc. I tillegg var det interessant å se likheter og forskjeller, altså der informantene rapporterer om sammenfallende trender, betraktninger og observasjoner og lignende, og der informantene tilsvarende rapporterte avvikende fra hverandre.

3.8 Validitet og reliabilitet

For å kunne trekke konklusjoner med utgangspunkt i dataene innhentet, er det nødvendig å måle datakvaliteten. Å sjekke validitet og reliabilitet er de vanligste måtene å sjekke dette på. Med validitet menes gyldighet, og med reliabilitet menes pålitelighet (Jacobsen 2018). Grunnet metodens iboende egenskaper, er det ikke mulig å fremprovosere de samme resultatene flere ganger ved bruk av kvalitativ metode.

IT-sikkerhetsmiljøet er lite, og oppgavens forfatter har forholdsvis god kjennskap til noen av sektorene som er omfattet av oppgaven. Det har derfor underveis i oppgaven, og særlig i forbindelse med gjennomføring av intervjuer, vært viktig å være klar over de bias og forutinntatte holdninger som kunne gjøre seg gjeldende. I tillegg har det vært nødvendig å reflektere i hvordan dette kan ha hatt innvirkning på relasjonen til de ulike informantene.

Intervjuene ble ikke gjennomført identisk. Noen av intervjuene ble gjennomført ansikt-til-ansikt, mens andre foregikk per telefon. En slik forskjell kan potensielt påvirke svarene man får. Et intervju gjennomført ansikt-til-ansikt kan eksempelvis oppfattes mer som en samtale enn et intervju over telefon, all den tid den som blir intervjuet kan påvirkes av intervjueren (Jacobsen 2018).

Av anonymitetshensyn kan ikke informantene knyttes direkte til en sektor, en virksomhet eller en rolle. Dette kan være en svakhet da man blant annet ikke får sett sammenhengen mellom et utsagn og informantens posisjon. Alle informantene ble plukket ut som følge av kompetanse og erfaring innenfor det aktuelle området. Dersom utvalget var mer tilfeldig, ville antageligvis svarene vært annerledes.

3.9 Etiske refleksjoner

I følge Jacobsen (2018) er ligger det i informert samtykke en grunnleggende forutsetning hvor informant skal delta frivillig har krav på privatliv og korrekt gjengivelse (Jacobsen 2018, s. 49). Disse hensynene er tatt underveis i prosessen. All informasjon er lagret uten kobling mellom informant og svar, og alle informantene kunne trekke seg når som helst i prosessen.

4. Empiri

I dette kapittelet vil empirien basert på gjennomførte intervjuer presenteres. Empirien vil presenteres samlet, og vil fremlegges som svar på de ulike forskningsspørsmålene til denne oppgaven. Der alle informantene har svar entydig, er svarene samlet. Der det er avvik enten som følge av tilknytning til ulike sektorer, er hvor det er spesielle avvik innad i én sektor, vil dette fremkomme. Forskningsspørsmålene, og herunder også presentasjon av empirien, vil presenteres i følgende rekkefølge:

1. Hvordan gjennomføre det strategiske arbeidet med sikkerhet, herunder risiko og trusselvurderinger?
2. Hva trengs som input i arbeidet med overvåkning og hendelseshåndtering av tilsiktede angrep?
3. På hvilken måte er det tilrettelagt for samhandling på tvers av strategisk og operativt sikkerhetsarbeid?

Informasjon om de aktuelle virksomhetene:
Alle sektorene omfattet i denne oppgaven har egne CERT-er, enten i egen virksomhet eller i overordnet i sin sektor. Samtlige av sektorene har operative/utøvende IT-sikkerhetsteam team som overvåker logger, sårbarheter og den generelle sikkerheten i infrastrukturen, enten i egen virksomhet eller i samarbeidende virksomhet. Samtlige av virksomhetene har strategiske IT-sikkerhetsteam som tar seg av de prosessuelle aktivitetene som risikovurderinger, risikoregistre, risikohåndtering, rapportering, revisjoner og andre strategiske oppgaver som kommer med arbeid med IT-sikkerhet.

Informantene som er intervjuet tilhører sektorer som forvalter infrastruktur og systemer som faller under sikkerhetsloven, eller på vegne av kunder som har det. De har derfor god kjennskap til denne. Flere av informantene har jobbet direkte med infrastruktur underlagt sikkerhetsloven, mens andre har jobbet med virksomhetens tilstøtende infrastruktur.

4.1 Hvordan gjennomføres det strategiske arbeidet med sikkerhet, herunder risiko og trusselvurderinger?

4.1.1 Sårbarheter

For å avklare det som ofte ligger til grunn for mye av IT-sikkerhetsarbeidet, startet alle intervjuene med at informantene forklart hva de selv legger i sårbarhet.
Samtlige av informantene hadde en klar formening om hva sårbarheter var. Noen av informantene satte sårbarheter fra en IT-sikkerhetskontekst også i et større perspektiv, og forklarte hvordan sårbarheter innen IT-sikkerhet skiller seg fra sårbarheter i et større henseende, herunder i et samfunnssikkerhetsperspektiv.

Sårbarhet må forstås i en kontekst, og innenfor informasjonssikkerhet er en sårbarhet ofte knyttet opp mot programvare, og er en feil eller mangel som kan utnyttes av en eventuell trusselaktør. Sårbarheter ble også knyttet opp mot verdier, herunder de verdier en virksomhet skal levere. I en slik kontekst ble sårbarhet beskrevet som manglende evne til å motstå eller tåle et avvik eller en påkjenning, altså avvik i en tjenesteleveranse som i sin tur kan medføre tap av verdier eller større skader.

Sårbarhet ble også koblet mot svakhet, der sårbarhet både ble beskrevet som en svakhet, enten i et system, en prosess eller en organisasjon, som kan føre til skade på en asset eller verdi. Én av informantene beskrev videre det han oppfatter som forskjellen mellom en sårbarhet og en svakhet, hvor han mener at det som skiller sårbarhet fra svakhet, er at en sårbarhet i større grad enn en svakhet, har en trusselaktør knyttet til seg. Og at en svakhet er noe man kan velge å leve med, mens en sårbarhet kan eskalere til noe større, og utgjør derfor en risiko.

4.1.2 ISMS

Alle informantene rapporterte at deres virksomhet har et ISMS, med ett unntak hvor ISMS-et var under implementering. I virksomhetene hvor det foreligger et ISMS, besvarte informantene variert med hensyn til i hvilken grad ISMS-et var levende og kjent for de ansatte i organisasjonen.

Informantene som har tilknytning til virksomheter innen finans, rapporterte alle at ISMS-et var levende, i bruk og kjent for ansatte i virksomheten. ISMS-et ble jevnlig revidert og

oppdatert, og ble aktivt benyttet både i forbindelse med drift, innkjøp av nye løsninger og i prosjekter.

Informantene med bakgrunn fra virksomheter innen særlig én sektor rapporterte at det forelå et ISMS, men at det var bare delvis levende. Noen av dokumentene i ISMS-et blir jevnlig revidert og oppdatert, og det produseres nye dokumenter. Det er særlig de styrende dokumentene som gjennomgås ofte. De mer lokale og tilpassede dokumentene har ingen jevnlig gjennomgang, og oppdateres på et ad hoc-basis, hvorav noen av disse ikke har vært oppdatert på over tre år. ISMS-et er i tillegg i liten grad kjent og i bruk i de tilknyttede virksomhetene. I tillegg er det en kombinasjon av kultur der medarbeidere i liten grad oppsøker informasjon kombinert med at språkbruken i ISMS-et er lite tilgjengelig. Andre aspekter som ble nevnt var at verktøyet ISMS-et ligger i, ikke er optimalt. Det presenterer dokumentene som flate filer og er dermed noe vanskelig å finne. I tillegg gir verktøyet lite innsyn i hvor mange som har lest dokumentene.

4.1.3 Risikoanalyser

Alle informantene rapporterte at det gjennomføres risikoanalyser i virksomheten, med unntak av én informant som rapporterte at innføring av en slik prosess på tidspunkt for intervju var under utarbeidelse. Det var imidlertid noe varierende i hvilken grad risikoanalyser gjennomføres, på hvilken måte de gjennomføres, herunder hvordan prosessen var, hvorvidt trusselanalyser er en strategisk del av disse og hva slags metode som er tatt i bruk. Risikoanalyser går også både under betegnelsen risikovurdering og ROS, men hva som skiller disse fra hverandre var ikke entydig, og aktivitetene informantene rapporterte beskrev, sammenfalt mer eller mindre, til tross for ulik definisjon.

Noen av informantene, herunder hovedsakelig med tilknytning til finanssektoren, rapporterte at det gjennomføres aktivt risikoanalyser for alle nye og endrede løsninger, samt at det gjennomføres revisjoner av disse hvert år. Gjennomførte sikkerhetsbaserte risikoanalyser er et krav til prosjektene, og ansvar og eierskap er tydelig, kjent og forankret i organisasjonen. Risikoanalysene følger en prosess med fastsatte steg, der selve analysen enten er forenklet, herunder består av en sjekkliste, eller større, der man basert på initiell sjekkliste avgjør hva som må analyseres videre. I disse virksomhetene er risikoanalysene en generell rapport der man avdekker risikoscenarier og beskriver disse. I dette ligger innhenting og klassifisering av

utløsende hendelser, risikoer og trusler, klassifisering av risikoene, man analyserer og beskriver sannsynlighet og konsekvens. Deretter beskrives forslag til tiltak for risikoer som overstiger et gitt nivå i risikoaksepttabellene, og eier av tiltakene defineres. Den forenklede varianten, en sjekkliste, kommer i forkant av risikoanalysen, og er med på å avgjøre hvorvidt en videre risikoanalyse er nødvendig, eller om man aksepterer et eventuelt avvik. Disse risikoanalysene omfatter både det veldig IT-tekniske, men også samspill mellom prosess, kultur og teknologi.

En annen gruppe av informantene tilhørende en annen sektor, herunder hovedsakelig med tilknytning til helsesektoren, forklarte at de også gjennomførte risikoanalyser på IT-siden for alle prosjekter. I alle prosjekter gjennomføres det minst to risikoanalyser, hvorav den første tidlig i prosessen, er av mer overordnet art. Den andre, og siste, har derimot til hensikt å avdekke risikoer tilknyttet den IT-tekniske løsningen. Denne fremstilles som en rapport, og finner sted langt ut i prosjektene, gjerne like før ibruktagelse av applikasjonen eller systemet. Denne risikoanalysen har som formål å blant annet å se på om tjenesten kan tas i bruk med de svakheter løsningen har på det aktuelle tidspunktet.

Ettersom risikoanalysen kommer sent i prosjektprosessen, medfører det dog at alle tiltak normalt må løses etter at produktet eller endringen er tatt i bruk. Denne risikoanalysen ser på både det tekniske, men også forholdet og grensegangene mellom den tekniske delen av løsningen opp mot prosesser og organisasjon. Også her avdekker man mulige hendelser, trusler, risikoscenarier og beskriver disse, for deretter å klassifisere risikoene, og man beskriver sannsynlighet og konsekvens. Tiltak blir beskrevet, og en ansvarlig får ansvaret for å implementere tiltakene.

Én av informantene jobber med å innføre en risikovurderingsprosess der analysene vil følge virksomhetens leveranser. En slik metode skal sikre at alle risikoanalyser som gjøres mot informasjonsinfrastrukturen rapporteres opp mot virksomhetens overordnede leveranser, slik at alle risikoene vurderes etter hvilken påvirkning disse har for etterlevelse av de leveranser virksomheten har forpliktet seg til. I en slik setting vil ikke risiko rapporteres for risikoens del, og det blir lettere å vurdere og prioritere risiko basert på den totale påvirkning det har på disse leveransene.

Samtlige av informantene beskrev ulike varianter av kvalitative vurderinger og/eller sjekklister. Ingen av informantene tilhørte virksomheter som benytter kvantitativ risikoanalyse innenfor informasjonssikkerhetsnivået.

4.1.4 Trusselanalyser

Samtlige av informantene opplyste at trusselanalysene ikke følger en spesifikk og definert metode. Noen av informantene opplyste dog at de jobber aktivt med å få på plass en mer styrt prosess for trusselanalyser, slik at disse vil kunne bli mer etterprøvbare. Trusselanalysene følger i dag risikovurderingsprosessen. Imidlertid opplyste noen av informantene at selv som del av risikoanalysene gjøres det lite *faktisk* trusselvurdering. Det foreligger verken metode eller noe intervall for trusselanalyser.

Det ble opplyst fra flere av informantene at det mottas mange trusselanalyser fra ulike CERT-miljøer eller i diverse formelle og uformelle kanaler, men disse blir ikke nødvendigvis hverken spesifikt vurdert inn mot egen virksomhet, eller benyttet som del av risikoanalysene. Én av informantene opplyste imidlertid om at det gjennomføres en rekke trusselanalyser både basert på mottatt informasjon fra formelle og uformelle kanaler, samt egne vurderinger.

Enkelte av informantene kunne rapportere at de årlige revisjonene av risikoanalysene inneholder en vurdering av endringer i trusselbildet, og at det er egne punkter for gjennomgang av trusselbildet og hvordan en eventuell endring påvirker risikoene. Imidlertid medfører manglende økonomisk støtte og kapasitet at det er begrenset med virkninger av disse revisjonene.

En av informantene diskuterte hvorfor de ved dennes virksomhet ikke gjennomfører trusselanalyser. Mangel på kompetanse og ressurser er en viktig del av det.
"Vi har en metode å gjøre risikovurderinger hvor de som skal behandle risikovurderingene i svært liten grad er vant med å bli utfordret på etterprøvbarheten i vurderingene. Dette medfører at man kunstig manipulerer sannsynlighet og konsekvensverdier for å oppgradere eller nedgradere vurderingene for å oppnå et annet mål".

Samme informant opplyste at man ikke bruker forhold som burde være kjente, ikke empiriske data som hendelser, logginnslag, avvik, oppetider etc., og i begrenset grad kontroller for modenhet. Informanten opplyste videre om at det er ønskelig å gå i retning av å bruke

risikoanalysene til å se på hendelse i fortid, nåværende modenhet og analyse av trusselaktørers fremtidige evne og vilje. Detter er ikke på plass ennå, men er en vei det er ønskelig å gå. Det er ikke stor vilje til å se på trusselanalyser som et verktøy, fordi man trives godt med at risikovurderingene er vage og lite etterprøvbare. Det er kunder, medarbeidere og innleide konsulenter som vil tildele farger, men ikke sannsynligheter. Det bør være mulig å se på fremtid med en viss usikkerhetsmargin, og det jobbes nå med å få kundene til å forplikte seg til dette, slik at man kan vurdere med kvantifiserbare tall for hvordan fremtiden vil kunne være.

4.1.5 Risikohåndtering

Alle informantene rapporterte at det enten jobbes aktivt, eller skal jobbes aktivt, med risikohåndtering. Imidlertid var det varierende i hvor stor grad dette i praksis fungerer, kontra hvordan det formelt er ment å fungere.

Én informant opplyste at det for hver risiko skal opprettes en sak i et saksbehandlingssystem. Denne skal følges opp til risikoen er lukket. Et risikoregister vil opprettes i forbindelse med at de skal etablere risikovurderingsprosessen. Dette risikoregisteret vil være knyttet opp mot de faktiske risikoanalysene, og vil være koblet til en overordnet leveranse, ikke den eller de tekniske moduler risikoen er avdekket i. Denne prosessen er imidlertid ikke iverksatt per i dag.

Én av informantene rapporterte om at risikoanalysene sendes oppover til leder eller direkte til en egen sikkerhetsgruppe, som vil håndtere risikoene derfra. Avhengig av risikoenes art, vil noen risikoer løses på teknisk side, mens andre vil kunne sendes opp til ledergruppen. Sistnevnte særlig dersom risiko er av særlig alvorlig art, eller vil kreve strategiske avgjørelser. Risikoregisteret benyttes aktivt av lederne.

Én av informantene opplyste om at det i dennes virksomhet finnes en prosess for risikohåndtering, og at denne er aktivt i bruk. Imidlertid foreligger det en meget stor arv av tiltak fra gamle risikoanalyser. Og denne arven er større enn evnen til å håndtere dem, hvilket gjør at ikke alle risikoer og tilhørende tiltak nødvendigvis følges opp i praksis likevel.

En annen gruppe av informantene rapporterte om at det i deres virksomheter er slik at risikoregisteret benyttes aktivt for å overvåke og vurdere risiko. Med årlig gjennomgang av risikoanalyser, og risikoregister, hvor risikoene kommer til virksomhetens øverste ledelse, sikres fokus. Ansvar for håndtering av risikoer tilligger linjen, men er delegert fra toppledelsen og nedover til virksomhetens operasjonelle struktur. Dette innebærer at ledere på alle nivåer skal ha kjennskap til risikoer i egen virksomhet. Videre innebærer dette at verdier skal beskyttes gjennom tiltak for å påse at sikkerhetsrisikoene er i tråd med virksomhetens risikoapetitt. Egen gruppe som jobber med risikohåndtering, herunder å følge opp at tiltak iverksettes. En sikkerhetskoordinator for de ulike områdene i virksomheten støtter sikkerhetsarbeidet gjennom operasjonalisering av sikkerhetskrav, herunder oppfølging av tiltak på eget område.

4.1.6 Ledelsens rolle og involvering

Det ble rapportert om ledelsesinvolvering i varierende grad for de ulike virksomhetene. Innenfor én sektor ble det rapportert motstridende, hvor én informant rapporterte at ledelsesinvolveringen er begrenset innenfor deler av risikohåndteringen, særlig på den tekniske siden der man mangler eskaleringsvei til ledelsen. Én annen informant fra samme sektor kunne rapportere at ledelsen i dennes virksomhet tidvis er tungt involvert i risikohåndteringen. Det ble videre informert om at man den senere tid har fått gjennomslag for å få sikkerhet inn på agendaen i ledermøtene. Samtidig har man et regionalt styringssystem hvor sikkerhetsmål og –strategi ligger til grunn, hvor man har en strategi om at ondsinnede hendelser ikke skal godkjennes og aksepteres. Imidlertid er det en erkjennelse at man ikke vil klare å forhindre alle mulige ondsinnede hendelser i å inntreffe. Men man skal ha en deteksjonsstrategi. Fokuset har historisk vært på nettverkssiden, men man har, de siste årene, jobbet målrettet med endepunktsikring. I dette ligger en implisitt trusselforståelse, men man har da også et styrende dokument hvor dette defineres som et fokus, og hvor krav om deteksjon skal ligge ufravikelig til grunn, og så bygger man respons på toppen av dette.

Når det gjelder trusselhåndtering, rapporterte begge at dette var på et ad hoc-basis. Innen for hendelseshåndtering, derimot, kunne ledelsen være tungt involvert da denne inngår som en del av beredskapsapparatet. Imidlertid vil ledelsesinvolveringen kunne variere i noen grad, avhengig av hendelsens art og alvorlighetsgrad.

Innenfor en annen sektor ble det rapportert at ledelsen er tungt involvert innen risiko- og hendelseshåndtering, og hvor arbeid rundt dette er forankret i toppledelse. Det er en klar ansvarsfordeling fra topp til bunn når det gjelder IT-sikkerhet. Samtidig ble det av en annen informant poengtert at dette samtidig også kan variere fra virksomhet til virksomhet innen sektoren.

4.2 Hva trengs som input i arbeidet med overvåkning og hendelseshåndtering av tilsiktede angrep?

4.2.1 Prosesser for hendelseshåndtering ved tilsiktede angrep

Alle informantene opplyste om at det foreligger, eller skal foreligge prosesser for hendelseshåndtering i deres respektive virksomheter.

Informantene fra helsesektoren opplyste at fokus rundt sikkerhetstruende hendelser, herunder med aktører med et visst fokus og vilje til å gjennomføre et angrep, er høyt i sektoren. Det finnes en del prosesser for hendelseshåndtering, hvorav man blant annet har scenariebaserte modeller hvor man jobber ut fra prosesser og varslingslister, samt tiltak på hypotesedrevet sikkerhetsarbeid. Det gjennomføres imidlertid ikke jevnlig øvelser. Beredskapsapparatet og beredskapsprosedyren slår inn ved uønskede sikkerhetshendelser. Disse definerer blant annet ulike nivåer for beredskap, samt rammene for beredskapsledelse. Er hendelsen av en viss kritikalitet, vil man se på hvilke konsekvenser denne hendelsen har for virksomheten, og deretter vurdere hvor høyt på skalaen, eller på hvilket nivå, hendelsen er. Er hendelsen vurdert høyt nok eller kritisk nok, vil administrerende direktør gå inn som beredskapsleder.

Én informant opplyste om at det, i dennes virksomhet, gjennomføres tester for å avdekke tilsiktede angrep, og har dedikerte enheter som jobber jevnlig for å avdekke angrep og andre IT-sikkerhetshendelser. Dersom en sikkerhetshendelse oppstår pekes det ut en kriseleder, og hendelsen vil håndteres av en kriseorganisasjon hvis hovedoppgave er å ivareta liv og helse, samt gjenopprette normalforretningsdrift så raskt som mulig. En slik kriseorganisasjon med en kriseleder, etableres helt uavhengig av om den aktuelle sikkerhetshendelsen er tilsiktet eller ikke. Man prøver her å påse at den normale driften forstyrres minst mulig mens hendelsen pågår. Kriseorganisasjonen øver jevnlig på kriser. Resultatene av kontrollaktivitetene rapporteres både underveis i øvelsen og etter øvelsen, både i egen linje og til sikkerhetsleder. Ansatte bidrar i håndteringen av sikkerhetshendelser både direkte, og ved å

rette seg etter ordre fra ledere og eventuelt myndigheter. Dette gjelder også ved øvelser. En annen informant fra finanssektoren opplyste om at de også jevnlig gjennomfører øvelser med deres leverandører. Én av informantene var ikke kjent med at det gjennomføres øvelser rundt sikkerhetshendelser generelt, eller tilsiktede hendelser spesielt, i dennes virksomhet.

Én av informantene innenfor justis- og forsvarssektoren opplyste om at de, ved dennes virksomhet, har en egen hendelsesprosess med eskaleringspunkt. I tillegg har man begynt å utarbeide playbooks for å håndtere ulike hendelser og scenarioer, hvor man nå jobber med scenariene. I tillegg er det som mål, ved større hendelser, at man følger de fire beredskapsprinsippene. Hvis man skal håndtere en krise, bør man ha samme organisasjon som ellers, slik at man slipper å havne i en situasjon der man får en leder som ikke kjenner den dagligdagse situasjonen. Det jobbes aktivt med ny beredskap i virksomheten, og dette vil også omfatte tilsiktede angrep. En annen informant fra samme sektor opplyste at ved denne virksomhet gjennomføres det øvelser hvor man trener på alle typer hendelser, både tilsiktede og utilsiktede. Disse øvelsene gjennomføres jevnlig. I tillegg har virksomheten et IRT-team som håndtere hendelser der.

4.2.2 Risikoprosessens og risikoanalysenes rolle i arbeid med overvåkning og hendelseshåndtering

Informanter fra helsesektoren, opplyste om at det per i dag nesten ikke foreligger noen praktisk håndtering av risikovurderinger som input i arbeidet med overvåkning og hendelseshåndtering. Én av informantene opplyste om at risikovurderingsprosessen har i liten grad identifisert trusselaktører som risiko. Dette skyldes flere forhold, blant annet at den aktuelle sektoren har hatt fokus på andre forhold, herunder tap av konfidensialitet og integritet som følge av feil, og ikke like fullt som følge av tilsiktede handlinger. Det at en trusselaktør med overlegg ønsker å forvolde skade, er en forholdsvis ny tanke i virksomheten, og har kommet som følge av en modning over tid, men som også veldig brått i det siste har gjort seg gjeldende.

Det ble videre forklarte at prosessen, i det store, tidligere har tatt for seg at konsekvensene stort sett treffer den registrerte, hvor den registrerte har en stor immateriell verdi i å ønske konfidensialitet. Samtidig har prosessen i for liten grad inkorporert etterretningsbiten. Verdien for en tredjepart trenger ikke være det samme som for den registrerte, men snarere som ledd i

å kartlegge, bygge relasjonsdatabaser mellom innbyggere eller på andre måter drive strategiske og langvarige etterretningsoperasjoner. Informanten uttalte at *"Jeg tror man nå i større grad tar for seg at verdiene våre ikke bare har en verdi for den registrerte."*.
Imidlertid ble det rapportert at det i risikoanalysenes tiltak ofte angis behov for økt overvåkning, herunder etablering av logger og trigging på gitte parametere, for ulike systemer. Dette tas inn som en del av risikohåndteringen.

Informantene fra finanssektoren var klare på at risikoprosessen i seg selv ikke er direkte eller formelt i bruk i arbeid med overvåkning og hendelseshåndtering ved tilsiktede angrep. Imidlertid rapporterte én av informantene fra denne sektoren at det til en viss grad benyttes der det foreligger direkte tiltak som berører overvåkningsarbeidet, eksempelvis ved tiltak som innebærer økt logging, men at risikoanalysene i seg selv normalt ikke benyttes videre.

Noen informanter rapporterte at sammenknyttede grupper og mindre grad av segmentering mellom strategiske og operative ressurser, gjør at output ett sted kan bli input et annet sted. Informantene fra justis- og forsvarsrelatert sektor opplyste at det er nærliggende at risikoanalyser benyttes for arbeid med overvåkning og hendelseshåndtering av tilsiktede angrep, blant annet fordi prosessene og arbeidet som gjøres innenfor sikkerhet i stor grad er organisert sammen.

4.2.3 Trusselanalyser i overvåkningsarbeid og hendelseshåndtering

Informantene fra de ulike sektorene responderte noe ulikt på hvordan trusselanalyser utarbeides og benyttes i sine respektive virksomheter.

Informantene fra finanssektoren opplyste at trusselkataloger jevnlig overleveres til gruppene som gjennomfører risikoanalyser, men lite andre vei. Disse trusselkatalogene er hovedsakelig basert på informasjon mottatt fra formelle og uformelle kanaler, og innebærer ikke en egen vurdering av hvordan dette eventuelt kan treffe virksomheten spesifikt, eller hvilke systemer som er mest utsatt.

Informantene fra helsesektoren beskrev en adhoc-basert håndtering av trusselanalyser. Konkrete trusselanalyser gjøres adhoc, og følgelig blir bruken av disse videre i et strukturert

arbeid for å overvåke og håndtere tilsiktede hendelser, også adhoc. Én av informantene pekte på den hypotesedrevne incident-responsen, der det ligger en implisitt forståelse av en trusselaktørs evne og vilje til å gjennomføre angrep. Imidlertid er denne lite prosessdreven. Det betyr dog ikke at ikke de som sitter i operative sikkerhetsfunksjoner i dag ikke har en sterk trusselfølelse, og jobber med den trusselinformasjonen de mottar fra formelle og uformelle kanaler. Men denne er for alle praktiske formål adhoc-styrt, og basert på hva de aktuelle ressursene vet der og da, og er ikke kontrollert og målbar. Kombinert med et til dels lite strukturert arbeid med trusselanalyser i risikoanalysearbeidet, blir totalen at bruken av trusselanalyser i overvåkningsarbeid og hendelseshåndtering av tilsiktede angrep adhoc-basert. De som sitter på operativ/utøvende IT-sikkerhetsfunksjoner mottar imidlertid trusselinformasjon fra formelle og uformelle samarbeidspartnere.

Informantene med bakgrunn fra justis- og forsvarssektoren opplyste at trusselanalysene benyttes i ganske stor grad i arbeid med overvåkning og hendelseshåndtering. I dette ligger både trusselanalysene som kommer fra den operative siden, herunder informasjon fra formelle og uformelle kanaler, samt trusselanalysene som kommer som produkt fra risikovurderingsprosessen, i forbindelse med risikoanalysene.

Det ble videre presisert av noen av informantene at for å kunne forbedre arbeidet overvåkning og håndtering av tilsiktede angrep, er det særlig forbedrede trusselanalyser som er avgjørende. I tillegg til økt teknisk kompetanse, og ikke minst verktøy for blant annet å avdekke angrep tidlig.

4.2.4 Prosessuelle utfordringer i møte med tilsiktede angrep

En informant innenfor helsesektoren påpekte at én av de store utfordringene er hvordan et angrep treffer. Under et angrep, ble alle som skulle drifte og levere tjenester omallokert til ulike prosesser for å håndtere angrepet, herunder beredskap. En annen ting er at det er ulikt risikoakseptansenivå mellom de ulike kundene, hvilket også innebærer at man oppfatter trusselaktører ulikt. Utslag av dette treffer risikovurderingsprosessen. Når man leverer en felles tjeneste, ønsker man at de som skal konsumere denne tjenesten forstå risiko og trusler likt, og at prioriteringene er like. Men slik er ikke alltid tilfelle hos oss. De forstår kanskje ikke hvorfor en trusselaktør er interessert i en type verdi, fordi de ikke har gjennomført gode nok verdivurderinger. Mangelen på gode verdivurderinger gjør at man har en begrenset eller

hemmer prosess for hendelseshåndtering, fordi de som eier verdien ikke selv har definert det som en verdi.

Innenfor finanssektoren, rapporterte én av informantene at det er en tendens til at tilsiktede angrep oppdages litt for sent. En teori rundt årsaken til dette var at det er mangel på ressurser til å lese ut logger og drive overvåkning på dette området. Imidlertid bidrar alle ansatte når det oppstår sikkerhetshendelser eller farer, og alle retter seg etter ordre fra ledere og myndigheter. Dette gjelder også ved øvelser. Generelt vurderer man i den aktuelle virksomheten sikkerhetsrisiko med grunnlag i tre faktorer:

1. Verdien som skal beskyttes
2. Trusselen mot den aktuelle verdien
3. Sårbarheter i virksomhetens forsvar

De øvrige informantene opplyste om at de ikke egentlig opplever at det skal være særlig mange prosessuelle utfordringer i møte med tilsiktede angrep, all den tid sikkerhet generelt, og med hensyn til tilsiktede angrep spesielt, tas svært alvorlig i sektoren. Eventuelle tilsiktede angrep vil gå ”helt til topps” uansett, og vil dermed bli prioritert og få de ressurser og midler som trengs. I tillegg opplyste én av informantene at ved dennes virksomhet er det forholdsvis flat organisasjonsstruktur, hvilket innebærer at eventuelle vanskeligheter prosessuelt vil bli justert umiddelbart dersom det skulle oppstå en hendelse. Det er lite pekelek, man fokuserer heller på å løse et problem sammen.

4.3 På hvilken måte er det tilrettelagt for samhandling på tvers av strategisk og operativt sikkerhetsarbeid?

4.3.1 Ledelsens rolle

Ledelsens rolle innen samhandlingen mellom de strategiske IT-sikkerhetsteamene og de operative/utførende IT-sikkerhetsteamene varierte noe fra sektor til sektor, særlig med tanke på at det er ulike organisering av sikkerhetsorganisasjonene både mellom sektorene og innen hver av sektorene, på virksomhetsnivå. Innenfor helse ble det opplyst at det foreligger et oppdragsdokument fra eier, hvor informasjonssikkerhet er spesifikt nevnt, og er én av prioriteringen der. Man har fått på plass styrende dokumenter hvor den operative/utførende siden av sikkerhetsarbeidet er synliggjort, blant annet på deteksjonssiden.

Videre ble det fra finanssektoren opplyst at ledelsen gjennomgår sikkerhetstilstand jevnlig i den øverste ledergruppen, og øverste ledelse inne IT vedtar standarden for sikkerhet generelt. Sikkerhetsleder er premissgiver, og representerer øverste ledelse for områdene under, som har det operative og utøvende ansvaret. Men det er ingen direktekobling mellom de strategiske og operative/utførende sikkerhetsteamene. En annen informant fra denne sektoren opplyste at det operative/utførende virket var utenfor dennes virksomhet, men at det var plassert i en samarbeidende virksomhet.

Informantene med tilhørighet innen for justis- og forsvarssektoren opplyste at de strategiske sikkerhetsteamene og de operative/utførende sikkerhetsteamene jobber tett sammen og har felles ledere og forholdsvis flat struktur.

4.3.2 Samhandling mellom operativt IT-sikkerhetsteam og strategisk IT-sikkerhetsteam

Informantene fra helsesektoren forklarte at den operative delen av sikkerhetsteamene er en produksjonsenhet med egne vaktlag, dette innebærer at det er underlagt IT. Disse igjen er delt i to, hvorav ett lag sitter på driftssiden, mens det andre laget sitter med angreps-/sikkerhetshendelser. Samhandlingen mellom disse operative gruppene og de strategiske sikkerhetsteamene gjelder i hovedsak rapportering på enkelte måleparametere som gjerne er tilknyttet ytelse av kontroller som er besluttet implementert.

I følge to av informantene, begge med tilhørighet i finanssektoren, er det begrenset med samhandling mellom de operative IT-sikkerhetsteamene og de strategiske IT-sikkerhetsteamene. I arbeidet med å overvåke og avdekke trusler, er det ingen direktekobling mellom disse IT-sikkerhetsteamene. Selv om de er organisert i samme virksomhet, er felles ledelse noen nivåer over, og således ikke direkte over de utøvende IT-sikkerhetsressursene. Én av informantene opplyste videre om at det har vært en del omstrukturering i den senere tid, som igjen har medført at samhandling som har vært etablert over tid til dels er brutt nå, med nye ressurser som ikke har rukket å etablere tilsvarende samhandling på tvers av teamene. En annen av informantene opplyste om at det foreligger en formell linje mellom de strategiske og operative/utførende IT-sikkerhetsteamene, blant annet ved overlevering av trusselkatalog fra operativt/utførende til strategisk IT-sikkerhetsteam.

En annen informant fra finanssektoren opplyste at i dennes virksomhet, er det på visse områder forholdsvis tett samhandling mellom strategiske og operative/utførende IT-sikkerhetsteam, og at dette blant annet skyldes at virksomheten har observatørrolle i en del fora som forvaltes og drives av en operativ part. Disse deler derfor en del informasjon på tvers av organisasjonsstrukturer og virksomheter. I tillegg er de samlokalisert, og har dermed en del uformell informasjonsutveksling på tvers.

Øvrige informanter, med tilhørighet innen justis- og forsvarssektoren var forholdsvis samstemte, og opplyste at samhandlingen mellom operative sikkerhetsteam og strategiske sikkerhetsteam i deres virksomheter er god, og de ligger under samme enheter eller med forholdsvis nære ledere. Oppgavene er splittet mellom teamene, der de operative har en tydeligere teknisk profil, mens de strategiske teamene har oppgaver som innebærer risikoarbeid, ISMS, ledelse, rapportering, arbeid med sikkerhetskultur og lignende. Det at disse teamene er formelt underlagt de samme lederne, innebærer et i utgangspunktet tett samarbeid der output fra én gruppe er like input til en annen gruppe.

5. Drøfting

I følgende kapittel vil det forsøkes å besvare problemstillingen for oppgaven gjennom de tre forskningsspørsmålene.

I hvilken grad benyttes risiko- og trusselvurderinger aktivt i arbeid med informasjonssikkerhet, og spesifikt som input til hendelseshåndtering ved tilsiktede angrep?

Drøftingen baserer seg på teorien presentert i kapittel 2, og empirien fra de gjennomførte intervjuene, presentert i kapittel 4.

Kapittelet er inndelt i de tre forskningsspørsmålene, på samme måte som i kapittel 4, hvor empirien ble presentert. Dette for å lettere å kunne drøfte meg frem til et svar på hovedproblemstillingen.

7. Hvordan gjennomføres det strategiske arbeidet med sikkerhet, herunder risiko- og trusselvurderinger?
8. Hva trengs som input i arbeidet med overvåkning og hendelseshåndtering av tilsiktede angrep?
9. På hvilken måte er det tilrettelagt for samhandling på tvers av strategisk og operativt sikkerhetsarbeid?

Noen av forskningsspørsmålene er ytterligere splittet i mindre kategorier for å strukturere drøftingen.

5.1 Hvordan gjennomføres det strategiske arbeidet med sikkerhet, herunder risiko- og trusselvurderinger?

I følge Lysneutvalget (NOU 2015:13) handler IKT-sikkerhet om ”*å beskytte IKT og informasjonen i informasjonssystemene mot uønskede hendelser*” (NOU 2015:13, s. 34). Dette måles gjerne opp mot noen sikkerhetsmål, konfidensialitet, integritet og tilgjengelighet.

Felles definisjoner er viktig i en virksomhet, for å sikre at man forstår hverandre, og har mulighet til å agere når det trengs. Alle informantene hadde et klart bilde av hva de legger i

sårbarheter. For noen av dem var sårbarheter som konsept del av et større perspektiv, mens for andre gikk det helt spesifikt på IT-sikkerhetsdefinisjonen av sårbarheter, slik som skissert av Lysneutvalget (NOU 2015:13) og NSM (2018). Det at informantene la ulik definisjon til grunn da de beskrev sårbarheter, kan skyldes at informantgrunnlaget varierte fra teknisk IT-sikkerhetsressurser til sikkerhetsleder. Avhengig av rolle, kan det være nødvendig å ha ulik forståelse av hva en sårbarhet er, og hva den kan utgjøre for virksomheten. På den annen side kan det medføre manglende forståelse dersom én gruppe oppfatter sårbarheter som noe man aktivt, og teknisk, må løse fortløpende for å stagge en eventuell trussel, mens andre oppfatter at sårbarheter bør reduseres.

Alle informantene opplyste om at deres virksomheter har et ISMS, styringssystem for informasjonssikkerhet, med ett unntak hvor ISMS-et er under utarbeidelse. ISMS-et er viktig fordi det der fremkommer hvilke krav, rutiner og prosesser virksomheten har for informasjonssikkerheten, og er det som setter føringer for hvordan virksomheten skal forholde seg til informasjonssikkerheten i alle lag, fra teknisk til strategisk nivå. Vedlikehold av ISMS-et er i følge NSM (2015) tillagt informasjonssikkerhetsleder, hvorav dette også inkludere opplæring. Samtidig med at nær alle informanter rapporterte at de har et ISMS, ble det fra én informant rapportert at selv om de har et styringssystem, er det begrenset i hvilken grad det benyttes av virksomhetenes ansatte, og hvor ofte dokumentene i ISMS-et revideres. Det ble pekt i retning av at det blant annet foreligger en kultur hvor ansatte er lite oppsøkende med hensyn til å finne informasjon, samt at språkbruken i ISMS-et kan oppleves lite tilgjengelig. Kombinert med at filene presenteres som flate filer, og er vanskelige å finne, er alle faktorer som gjør ISMS-et lite tilgjengelig for brukerne.

5.1.1 Risikovurdering og –analyser

I følge Aven et. al (2010) har risikoanalyser ”*som mål å kartlegge og beskrive risiko*” (Aven et. al, 2010, s.13), der risiko er mulige, fremtidige hendelser, og dermed har en iboende usikkerhet ved seg. Alle informantene rapporterte at det gjennomføres risikoanalyser ved deres virksomheter, med ett unntak hvor man nå er i gang med å implementere risikovurderingsprosess. Det ble videre rapportert at gjennomføring av risikoanalyser er krav til prosjekter i forbindelse med nye og endrede løsninger. Risikoanalysene følger fastsatte steg, være seg i ulike deler av prosjektprosessene, og med en metodebruk som varierer etter fastsatte kriterier som når den gjennomføres og hva formålet med den er.

Aven (2010) advarer mot at det ikke er uvanlig at man gjennomfører risikoanalyser først og fremst på bakgrunn av krav om å risikoanalysere. Aven (2010) hevder videre at motivasjonen for å gjennomføre risikoanalyser bør være et godt beslutningsunderlag. Det kan argumenteres for at dersom man gjennomfører risikoanalyser på "løpebånd", herunder som følge av at det er krav om risikoanalyser i flere prosesser, vil det potensielt kunne medføre at kvaliteten reduseres fordi man er mer opptatt av å produsere enn å faktisk analysere. Imidlertid kan det at det er krav om gjennomføring av risikoanalyse i blant annet prosjektprosesser, også indikere at risikoanalyseprosessen er forankret, implementert og i bruk i virksomhetenes prosesser, uten at det implisitt betyr en reduksjon i kvalitet. Videre er den varierte bruken av metode for risikoanalyse, avhengig av hvor i prosjektprosessen man er, i tråd med Aven et. al (2010), som poengterer at formålet i stor grad er førende for hvilken risikoanalysemetode det er mest hensiktsmessig å benytte seg av.

Informantene rapporterte at man i risikoanalysene avdekker mulige hendelser, trusler, risikoscenarier og beskriver disse, for deretter å klassifisere risikoene, og vurderer sannsynlighet og konsekvens. Tiltak blir beskrevet, og det settes en ansvarlig som skal følge opp. Dette er mer eller mindre i tråd med Refsdal et als (2014) oppstilling av de ulike trinnene i en risikoanalyse. I dette ligger innhenting og klassifisering av utløsende hendelser, risikoer og trusler, klassifisering av risikoene, man analyserer og beskriver sannsynlighet og konsekvens. Deretter beskrives forslag til tiltak for risikoer som overstiger et gitt nivå i risikoaksepttabellene, og eier av tiltakene defineres. Det ble videre rapportert blant de fleste informantene at risikoanalysene fremstilles som en rapport, som igjen skal fungere som beslutningsunderlag for hvorvidt man skal ta løsningen i bruk med de svakhetene den har på det aktuelle tidspunktet eller ikke. Dette er i tråd med Aven (2010), at risikoanalysene skal være et godt beslutningsunderlag.

5.1.2 Trusselanalyser

Formålet med trusselvurderinger er å beskrive det trusselbildet man står overfor, med utgangspunkt i de verdier man ønsker å beskytte (NSM 2016). Det er også én av de første, og i følge Refsdal et. al (2015) én av de viktigste, stegene i en risikoanalyseprosess. Det fordrer ikke minst at man har klart for seg hvilke verdier man ønsker å beskytte.
Videre er det er nødvendig å forstå hvem virksomhetens trusselaktørene er, og hvorfor de eventuelt skulle utgjøre en trussel mot virksomheten. Dette innebærer i følge Refsdal et. al

(2015) å se på eventuelle motiver og intensjoner som kan gjøre seg gjeldende, herunder eksempelvis hevn, spionasje, politisk agenda eller økonomisk vinning. Trusselbildet er ikke alltid statisk, det kan endre seg over tid, avhengig av blant annet pågående saker i media, den politiske eller økonomiske situasjonen, eller det kan være andre faktorer som provoserer potensielle trusselaktører, og det kan være endrede faktorer som ligger utenfor virksomhetens eget påvirkningsområde, men som likevel kan ha stor innvirkning på hvilke trusler virksomheten kan utsettes for.

I tillegg til intensjoner, påpeker Refsdal et al (2015) at også trusselaktørenes evne og vilje til å gjennomføre et angrep knyttet til trusselaktørens kapasitet til å gjennomføre et angrep. Dette er også en faktor som kan endre seg over tid. En trusselaktør kan ha fått ny giv, eller hjelp fra andre trusselaktører. For å kunne identifisere ondsinnede risikoer, er det i følge Refsdal et. al (2015) nødvendig å forstå hvordan motparten kan komme til å angripe, hvilke sårbarheter vedkommende kan komme til å utnytte og hva som kan skje dersom vedkommende lykkes i angrepet. Det er derfor viktig å gjennomføre trusselanalyser med sikte på å avdekke nettopp hvordan situasjonen er her og nå., og hva en ny eller endret løsning kan bety i så måte. Flertallet av informantene opplyser om at trusselanalysene de gjennomfører, ikke følger en spesifikk og definert metode. Samt at de, til tross for forankret og implementert prosess for risikoanalyse, erkjenner at trusselanalysedelen av risikoanalysen ikke nødvendigvis innebærer en reell analyse av løsningene opp mot mulige trusselaktører og hendelser, samt en vurdering av hvilke konsekvenser slik hendelser vil ha, medfører at det kan argumenteres for at virksomhetene har lite innblikk i det reelle trusselbildet de står overfor. Nye løsninger implementeres, og nye sårbarheter introduseres i infrastrukturen, men uten at det gjennomføres analyser av hvordan disse sårbarhetene kan brukes for å ramme virksomhetene, ei heller hvilke tiltak som bør iverksettes for å enten redusere risiko for at en uønsket hendelse inntreffer, eller ha tiltak klare for å håndtere en uønsket hendelse skulle den inntreffe.

I følge Aven et. al (2010) er det ikke uvanlig å kopiere avdekkede trusler fra én analyse til neste, særlig dersom systemene analysene omfatter, ligner hverandre. I slike tilfeller står man i fare for ikke å få vurdert de rette truslene for det aktuelle systemet, fordi ulike systemer også kan ha ulike egenskaper som gjør dem utsatt for andre trusler og farer. Følgelig vil man potensielt overse viktige trusler rettet mot det spesifikke systemet.

Flere av informantene opplyste at de mottar trusselinformasjon via operativt/utøvende IT-sikkerhetsteam, ofte mottatt fra formelle og uformelle kanaler. Imidlertid vil denne typen trusselinformasjon være generell, og er ikke direkte tilknyttet implementering av ulike løsninger i virksomheten. Det vært naturlig at den typen trusselinformasjon som mottas fra ulike kanaler benyttes for videre analyse når det gjennomføres trussel- og risikoanalyser. Dette er videre i tråd med anbefalinger fra NSM (2016), som anbefaler å benytte flere kilder for innhenting av trusselinformasjon. Imidlertid stilles det der opp at man skal gjennomføre vurdering trusselinformasjonen.

Så lenge man snakker om risikoer, og med det innforstått fremtiden, vil det alltid være en viss grad av usikkerhet. I følge Renn (2008) finnes det dog ulike risikoer, hvor noen har en lavere grad av usikkerhet, eksempelvis de lineære risikoene, mens andre har en høyere grad av usikkerhet, eksempelvis de usikre risikoene. Dette er de svarte svanene, de vi kanskje ikke vet at vi ikke vet om, og som dermed er vanskelighet å forutse hendelser og konsekvenser av. Det ble opplyst fra én av informantene om at forhold som burde være kjente, som empiriske data, logginnslag, avvik, oppetider med mer, heller ikke benyttes som input til trussel- og risikoanalysene. Dette til tross for at virksomhetene sitter på mye av denne informasjonen i dag. Én av informantene pekte på at manglende strukturert gjennomføring av trusselanalyser skyldtes manglende kompetanse og ressurser. Som begrunnelse for manglende reelle trusselanalyser, ble det nevnt at det blant en del ikke er stor vilje til å se på trusselanalyser som et verktøy, fordi man trives godt med at risikovurderingene er vage og lite etterprøvbare. Det var imidlertid et ønske om å kunne se på fremtid med en viss usikkerhetsmargin. Interessant nok innebærer dette at man i det ene øyeblikket ikke benytter seg av kjent materiale som man har tilgjengelig, og som kan være med på å redusere usikkerheten, samtidig som at man ikke uten videre har vært komfortabel med analyser hvor usikkerheten kanskje er stor, men nødvendig.

Ulike hendelser kan endre på trusselbildet, og nye løsninger kan også øke eksponeringsflaten mot uønskede hendelser, og kan medføre behov for enten økt, eller en annen type, sikring. Det at virksomhetene i stor grad gjennomfører risikovurderinger og –analyser ved nye og endrede løsninger, indikerer at det gjennomføres tiltak som er relevant for, og tilpasset, den aktuelle løsningen. På den annen side, manglende konsekvent gjennomføring av trusselanalyser medfører at risikoanalysene kan ha svakheter overfor det aktuelle trusselbildet den enkelte løsning åpner for. Å bero seg på statiske tiltak som ikke er tilpasset det

trusselbildet virksomhetene til enhver tid er eksponert for, gir ikke bedre sikkerhet selv om man har gjennomført en risikoanalyse.

5.1 3 Risikostyring og -håndtering

Risikostyring er i følge Aven (2015) er todelt prosess hvor man på én side fokuserer på risikoene og tiltakene, og på den andre siden blant annet kartlegging og styring av risikoer. I dette ligger å ta beslutninger om risiko innenfor blant annet definerte økonomiske og praktiske rammer, avhengig av virksomhetens mål og visjoner. Videre påpekes det fra Aven (2008) at ledelsens rolle i risikostyringsarbeidet er sentral. Det å lykkes med risikostyring innebærer at det foreligger en forankring hos ledelsen. I tråd med dette rapporterte alle informantene at det jobbes aktivt med risikohåndtering og –styring. Unntaket her var virksomheten som jobber med å få på plass sikkerhetsarbeidet. Informantene rapporterte at risikoer som utgangspunkt skal rapporteres til ulike ledergrupper for vurdering og håndtering derfra. Videre forfekter Aven (2008) at risikostyringsprosessen må forankres i organisasjonen, i analyse- og støttesystemer, og så i kommunikasjon og arbeid som er med på å utvikle kompetanse og motivasjon i den aktuelle organisasjonen. Blant informantene kom det frem at det var varierende hvem som har det utøvende ansvaret, da det ved noen av virksomhetene er delegert fra toppledelse og ned igjen til linjeledelsen. Dette kan muligens skyldes størrelse på virksomhet, og at dess større virksomheten er, dess mer aggregert må rapporteringen til ledelsen være. Ellers rapporterte alle informantene om at ledelsen med jevne mellomrom presenteres for IT-sikkerhetsrisikoer, og at ledelsen har tilgang til, og benytter, risikoregistrene aktivt for å overvåke og vurdere virksomhetenes risikoarbeid, ved de virksomhetene som har tilgjengelig risikoregister. Dette medfører at ledelsen har tilgjengelig det beslutningsgrunnlaget som trengs for å agere.

5.1.4 Oppsummering

Det strategiske arbeidet innenfor risiko- og trusselvurderinger er forankret i prosesser, og gjennomføres delvis. I dette ligger at risikovurderinger, herunder risikoanalyser, med dertil tilhørende risikostyring, både gjennomføres, og det er rapporteres til ledelsen. Samtidig er det en kjensgjerning at det ble rapportert til dels store mangler ved gjennomføring av risikoanalyser. I dette ligger at det gjennomføres lite faktiske trusselanalyser. Gjennomgående er at trusselanalyser ikke samordnes og analyseres, men at trusselinformasjon mottas enten fra andre kilder eller ikke egentlig gjennomføres. Følgelig har virksomhetene en begrenset

oversikt over trusselbildet virksomheten står overfor. Risikoanalysene utføres således uten at man har faktisk har vurdert trusler. Utover dette rapporteres risikofunn oppover i organisasjonene, og det gjennomføres arbeid på tiltakssiden.

5.2 Hva trengs som input i arbeidet med overvåkning og hendelseshåndtering av tilsiktede angrep?

5.2.1 Hendelseshåndtering

I følge NSM (2015) kan man dele sikkerhetshendelser i tre kategorier, henholdsvis feil og mangler, avvik og sikkerhetstruende hendelser. Sikkerhetstruende hendelser er alvorlige hendelser som kan true konfidensialitet, integritet og tilgjengeligheten, med dertil påfølgende konsekvenser. Samtlige informanter opplyste om at det er et høyt fokus på sikkerhetshendelser generelt, og nær alle informantene opplyste om at det foreligger prosesser for hendelseshåndteringer generelt, og som også gjelder for tilsiktede angrep. Det følger av informantenes rapportering av beredskapsapparatet og krisestaber slår inn dersom den uønskede sikkerhetshendelsen er av høy nok kritikalitet, uavhengig av om det er et tilsiktet eller utilsiktet angrep.

Det følger av Engen et al. og Perry og Lindell at øvelser er viktige for å avdekke svakheter i beredskapsplanen, og for å forbedre beredskapsrespons. Og at dersom man under en øvelse ikke avdekker noen problemer, har man enten gjennomført øvelsen med et for enkelt scenario, eller at evalueringen i ettertid har vært for dårlig (Perry & Lindell 2003). Hensikten med en øvelse er å forbedre. En øvelse kan være både tid- og ressurskrevende, og, avhengig av størrelsen på øvelsen, krever kanskje eksplisitt prioritering for å bli gjennomført. Dette gjør seg særlig gjeldende dersom man også skal påse at andre aktører får deltatt. Imidlertid vil det å ikke øve ofte og bredt nok potensielt kunne medføre at mangler ved beredskapsplanene ikke avdekkes. Eksempelvis ved at manglende koordinering med andre aktører, både virksomhetsinterne og eksterne, skaper problemer og forsinkelser, at de rette ressursene ikke er allokert riktig, eller at beredskapsplanen er delvis utdatert eller annet lignende.

NSM (2015) skisserer eksempler på type øvelser som er relevante for sikkerhetshendelser, hvorav disse spenner fra begrensede og teoretiske skrivebordøvelser via spilløvelser til feltøvelser. Noen av disse er omfattende og er ressurskrevende, andre er begrensede og innebærer begrenset med ressursbruk. En informant innenfor påpekte at én av de store

utfordringene er hvordan et angrep treffer alle som skal drifte og levere tjenester, da disse omallokeres til ulike prosesser for å håndtere hendelsen, herunder beredskap.
Dette kan videre dermed tyde på manglende prioritering av IT-sikkerhetsøvelser, slik at utfordringer ikke oppdages før angrepet faktisk er blitt en realitet.

Selv om samtlige av informantene rapporterte om eksisterende prosesser for håndtering av uønskede sikkerhetshendelser, var det imidlertid ikke alle som rapporterte om at det gjennomføres øvelser, eller at det gjennomføres jevnlige øvelser. Dette kan tyde på at øvelser i de aktuelle virksomhetene enten er av mer sporadisk art, gjennomføres relativt sett sjelden, eller gjennomføres for begrensede scenarier som kanskje ikke inkluderer IT-sikkerhetspersonell. Ettersom håndtering av uønskede hendelser, basert på innspill fra flere av informantene, fremstår å håndteres av andre enheter enn der IT-sikkerhetspersonellet er organisert, samt at krise- og beredskapsapparat ofte har et mye bredere nedslagsfelt med hensyn til hva de skal håndtere av hendelser, er det mulig det gjennomføres jevnlige øvelser, men da ikke direkte relatert til uønskede IT-sikkerhetshendelser. Dette kan omfatte eksempelvis brann, naturkatastrofer, strømbrudd eller andre ikke-IT-sikkerhetsrelaterte scenarier.

Virksomheter som drifter og forvalter store mengder informasjon har et bredt spekter av mulige hendelser som krever ulik respons. En hendelse der deler av et bygg faller over ansatte, en vannlekkasje som enten gjør deler av bygnings- og eiendomsmassene ubrukelige eller som ødelegger maskinvare, eller brann som krever evakuering av ansatte, medfører til dels svært ulike aktivitetsmønstre under beredskapen. Virksomhetene har også et variert trusselbilde de skal forholde seg til. Kombinasjonen av det brede spekteret av hendelser virksomhetene skal håndtere, et variert trusselbilde, og store mengder informasjon som skal beskyttes, indikerer at øvelser bør gjennomføres jevnlig og med en viss hyppighet for å kunne dekke over de ulike scenariene innenfor en adekvat tidsperiode.

5.2.2 Risiko- og trusselvurderinger i overvåkning og hendelseshåndtering

I følge Aven et al. (2008) er risikoanalyser er et viktig element i et helhetlig arbeid med sikkerhet, både som selvstendig dokumentasjon, som et ledd i beslutningsprosesser og som innspill til en rekke andre tilstøtende prosesser, som eksempelvis beredskapsplanlegging. I dette kan man også argumentere for at generell hendelseshåndtering av tilsiktede angrep også faller inn under.

I følge Perry &Lindell (2003) gjennomføres risikoanalyser for å avdekke hvilke trusler eller farer man må forholde seg til. Dette er viktig input til beredskapsplanlegging. Likevel rapporterte de fleste informantene, med unntak av informantene fra forsvars- og justissektoren, at det er svært lite praktisk bruk av risikovurderinger og trusselanalyser som input til arbeidet med overvåkning og hendelseshåndtering, utover konkrete tiltak fra risikoanalysen om krav til logger for ulike løsninger. Som én av informantene påpeker, kan dette skyldes at man i risikovurderingsprosessen i liten grad har identifisert trusselaktører som risiko, og videre den hypotesedrevne incident-responsen, der det ligger en implisitt forståelse av en trusselaktørs evne og vilje til å gjennomføre angrep. Imidlertid er denne lite prosessdreven.

Hvis ikke trusselaktører er en tilstrekkelig del av risikovurderingene, mister man et sentralt aspekt ved bruken av risiko- og trusselanalyser i overvåkning og hendelseshåndteringen rundt tilsiktede angrep. I den grad det da gjennomføres trusselanalyser på innfall eller ved et plutselig oppstått behov, blir følgelig bruken av disse videre i et strukturert arbeid for å overvåke og håndtere tilsiktede hendelser, også adhoc og lite proessedrevet. Det betyr dog ikke at ikke de som sitter i operative sikkerhetsfunksjoner i dag ikke har en sterk trusselfølelse, og jobber med den trusselinformasjonen de mottar fra formelle og uformelle kanaler, som en informant påpekte, men den er for alle praktiske formål adhoc-styrt, og basert på hva de aktuelle ressursene vet der og da, og er ikke kontrollert og målbar. Kombinert med et til dels lite strukturert arbeid med trusselanalyser i risikoanalysearbeidet, blir totalen at bruken av trusselanalyser i overvåkningsarbeid og hendelseshåndtering av tilsiktede angrep adhoc-basert. De som sitter på operativ/utøvende IT-sikkerhetsfunksjoner mottar som nevnt tidligere imidlertid trusselinformasjon fra formelle og uformelle samarbeidspartnere. Dette er dog informasjon som ikke er analysert inn mot egen virksomhet eller de systemer man har der. Følgelig er de mer input til en videre trusselanalyse enn noe som umiddelbart kan benyttes i planlegging av overvåkning og hendelseshåndtering. Informantene fra finanssektoren opplyste at teamene som sitter på operative/utøvende IT-sikkerhetsfunksjoner jevnlig overleverer trusselkataloger til gruppene som gjennomfører risikoanalyser, er det lite overføring andre vei. Disse trusselkatalogene er hovedsakelig basert på informasjon mottatt fra formelle og uformelle kanaler, og innebærer heller ikke en egen vurdering av hvordan dette eventuelt kan treffe virksomheten spesifikt, eller hvilke systemer som er mest utsatt.

Innhenting av trusselinformasjon fra flere kilder er som tidligere nevnt i tråd med NSMs (2016) anbefalinger, men det følger videre at det skal foretas vurderinger. Imidlertid er det her ikke snakk om analyse eller vurdering fra virksomhetens side. Dette kan tyde på at trusselinformasjonen ikke brukes i tilstrekkelig grad, og at trusselinformasjonen ikke tilpasses den respektive virksomhet, og vurderes mot de løsningene man har der. Ulike systemer er eksponert for ulike sårbarheter, og bør følgelig ha en trusselanalyse som ser på hvilket totalt risikobilde den spesifikke løsningen er utsatt for, og ikke minst hva eventuelle sårbarheter og mulige angrep mot én løsning kan ha å si for infrastrukturen som helhet.

I Norge foreligger det fire prinsipper som samfunnssikkerhets- og beredskapsarbeidet er organisert etter (Engen et. al 2016). Disse er henholdsvis ansvarsprinsippet, likhetsprinsippet, nærhetsprinsippet og samvirkeprinsippet (St.meld. nr. 29 (2011-2012)). En informant fra justis- og forsvarssektoren var den eneste som henviste til disse fire prinsippene i forbindelse med IT-sikkerhetshendelser. I tillegg var disse informantene de eneste som rapporterte at sammenknyttede grupper og mindre grad av segmentering mellom strategiske og operative ressurser, gjør at output ett sted kan bli input et annet sted. Videre rapporterte de at det er nærliggende at risikoanalyser benyttes for arbeid med overvåkning og hendelseshåndtering av tilsiktede angrep, blant annet fordi prosessene og arbeidet som gjøres innenfor sikkerhet i stor grad er organisert sammen. Det følger her dog at det er noe usikkert i hvorvidt det fungerer slik i dag, eller om det er snakk om antagelser og planer. Utover det er det ikke utenkelig at organisatorisk nærhet, samt et sektorvis fokus som i større grad er innrettet mot ondsinnede aktører, faktisk kan ha påvirkning på disse prosessene.

Videre ble det nevnt at det at noen av virksomhetenes kunder har ulikt risikoakseptnivå, og dermed også oppfatter trusselaktører ulikt, treffer både risikovurderingsprosessen, men kan også hemme prosess for hendelseshåndtering. I følge Aven (2015) er den femte suksessfaktoren i risikostyring bruk av risikoaksept- og beslutningskriterier. Dette kan peke i retning av at det foreligger svakheter i den overordnede risikostyringen, dersom det foreligger ulikt risikoakseptnivå rundt en felles infrastrukturplattform.
For at man skal kunne få, og deretter utnytte, synergier på tvers av strategisk og operativt IT-sikkerhetsteam, og dermed også få et mer målrettet overvåkningsarbeid, må følgelig trusselanalysene inn som en sentral del av risikoanalysearbeidet. Det vil også på sikt styrke hendelseshåndteringen.

5.2.3 Oppsummering

Når det gjelder hva som trengs som input i arbeidet med overvåkning og hendelseshåndtering av tilsiktede angrep, var svaret i stor grad direkte koblet til manglene i trusselanalyser. Tilsiktede angrep dreier seg i stor grad om trusler og trusselaktører. Og det kan medføre alvorlige sikkerhetshendelser og påkalle beredskaps- og krisehåndtering. I alle tilfeller er trusselanalyser viktige. Utover det trengs også bedre verdivurderinger og et uttalt risikoakseptnivå.

5.3 På hvilken måte er det tilrettelagt for samhandling på tvers av strategisk og operativt sikkerhetsarbeid?

I følge NSM (2015) er det virksomhetens behov som avgjør hvordan sikkerhetsorganisasjonen bør se ut, men at det er forholdsvis vanlig å splitte de strategiske sikkerhetsfunksjonene fra de operative/utøvende. Imidlertid skal de utøvende sikkerhetsfunksjonene samarbeide tett med, og rapportere til, sikkerhetsstaben. Dette er nødvendig fordi de strategiske og utøvende sikkerhetsfunksjonene til sammen utgjør en form for sikkerhetsorganisasjon i virksomheten, og dermed sammen er med på å sikre virksomheten og dennes verdier.

Ledelsens rolle innen samhandlingen mellom de strategiske IT-sikkerhetsteamene og de operative/utførende IT-sikkerhetsteamene varierte noe fra sektor til sektor, særlig med tanke på at det er ulik organisering av sikkerhetsorganisasjonene både mellom sektorene og på virksomhetsnivå, innen hver av sektorene. Samtidig hadde alle virksomhetene ulike formelle og prosessuelle tiltak som hver for seg har innvirkning på informasjonssikkerhet som helhet, og implisitt også samhandlingen på tvers av de ulike sikkerhetsteamene. Dette inkluderer blant annet styringsdokumenter fra eiere og aktiviteter inn mot ledergruppene og ansvarsfordeling. Informantene fra finans- og helsesektorene rapporterte at samhandlingen mellom de operative/utøvende IT-sikkerhetsteamene og de strategiske IT-sikkerhetsteamene gjelder i hovedsak rapportering på enkelte måleparametere. Selv om de er organisert i samme virksomhet, er felles ledelse noen nivåer over.

I virksomhetene innen justis- og forsvarssektoren var det rapportert tettere samarbeid på tvers av sikkerhetsfunksjonene, hvor dette blant annet ble tilbakeført til at felles leder var

forholdsvis ”nær” det ansatte, organisatorisk. Ingen av intervjuobjektene rapporterte om noe dårlig forhold mellom de strategiske og utøvende sikkerhetsfunksjonene, men der justis- og forsvarssektorens organisasjonsstrukturen rundt sikkerhetsfunksjonene var forholdsvis flat, kort vei til nærmeste felles leder, og forholdsvis tett samarbeid, var det i tilfellet helse- og finanssektoren ikke organisert like tett sammen, og hadde mer et formelt og begrenset samarbeid. Muligvis kan den organisatoriske avstanden dette bli for stor rent praktisk, fordi disse funksjonene da rapporterer til ulike ledere som kan ha ulik prioritering og agenda.

5.3.1 Oppsummering

Vedrørende hvilken måte det er tilrettelagt for samhandling på tvers av strategisk og operativt sikkerhetsarbeid er det nødvendig med et mer helhetlig arbeid for å hente ut synergier på tvers av IT-sikkerhetsarbeidet som gjøres i virksomhetene. Dette for å sikre at det benyttes relevant informasjon i beslutninger, hendelses- og beredskapsarbeid og overvåkning. For at det skal skje, er det nødvendig å se på hvordan samhandlingen mellom strategiske og operative IT-sikkerhetsteam er.

6. Konklusjon

Formålet med prosjektet er å se på organisering av informasjonssikkerhetsarbeid blant aktører som forvalter kritisk infrastruktur og/eller informasjon, herunder med fokus på sikring mot tilsiktede angrep. I dette ligger angrep som er nøye planlagt, og hvor informasjonsteknologi enten er et middel eller et våpen. Det er her fokusert på sikring mot tilsiktede angrep, og hvordan dette håndteres i risikovurderinger.

6.1 Forskningsspørsmål og problemstilling

I denne oppgaven er følgende problemstilling forsøkt besvart:

I hvilken grad benyttes risiko- og trusselvurderinger aktivt i arbeid med informasjonssikkerhet, og spesifikt som input til hendelseshåndtering ved tilsiktede angrep?

For å kunne besvare denne problemstillingen, ble det utarbeidet noen forskningsspørsmål:

1. Hvordan gjennomføres det strategiske arbeidet med sikkerhet, herunder risiko- og trusselvurderinger?
2. Hva trengs som input i arbeidet med overvåkning og hendelseshåndtering av tilsiktede angrep?
3. På hvilken måte er det tilrettelagt for samhandling på tvers av strategisk og operativt sikkerhetsarbeid?

Det strategiske arbeidet innenfor risiko- og trusselvurderinger er forankret i prosesser, og gjennomføres delvis. I dette ligger at risikovurderinger, herunder risikoanalyser, med dertil tilhørende risikostyring, både gjennomføres, og det er rapporteres til ledelsen. Samtidig er det en kjensgjerning at det ble rapportert til dels store mangler ved gjennomføring av risikoanalyser. I dette ligger at det gjennomføres lite faktiske trusselanalyser. Gjennomgående er at trusselanalyser ikke samordnes og analyseres, men at trusselinformasjon mottas enten fra andre kilder eller ikke egentlig gjennomføres. Følgelig har virksomhetene en begrenset oversikt over trusselbildet virksomheten står overfor. Risikoanalysene utføres således uten at man har faktisk har vurdert trusler. Utover dette rapporteres risikofunn oppover i organisasjonene, og det gjennomføres arbeid på tiltakssiden.

Når det gjelder hva som trengs som input i arbeidet med overvåkning og hendelseshåndtering av tilsiktede angrep, var svaret i stor grad direkte koblet til manglene i trusselanalyser. Tilsiktede angrep dreier seg i stor grad om trusler og trusselaktører. Og det kan medføre alvorlige sikkerhetshendelser og påkalle beredskaps- og krisehåndtering. I alle tilfeller er trusselanalyser viktige. Utover det trengs også bedre verdivurderinger og et uttalt risikoakseptnivå.

Vedrørende hvilken måte det er tilrettelagt for samhandling på tvers av strategisk og operativt sikkerhetsarbeid er det nødvendig med et mer helhetlig arbeid for å hente ut synergier på tvers av IT-sikkerhetsarbeidet som gjøres i virksomhetene. Dette for å sikre at det benyttes relevant informasjon i beslutninger, hendelses- og beredskapsarbeid og overvåkning. For at det skal skje, er det nødvendig å se på hvordan samhandlingen mellom strategiske og operative IT-sikkerhetsteam er.

Den endelige konklusjonen er:
Risiko- og trusselvurderinger benyttes delvis aktivt i arbeid med informasjonssikkerhet, men i liten gard inn mot hendelseshåndtering. Dette skyldes i stor grad mangler i trusselanalyser.

6.2 Anbefalinger til videre forskning

Det anbefales å gjennomføre en undersøkelse av hvordan sikringsrisikovurderinger gjennomføres innenfor IT-sikkerhet ved noen flere sektorer. Det hadde vært interessant å se om funnene avviker, eller om de eventuelt kan gi mer innsikt i hvorfor man opplever de utfordringene som er avdekket i denne undersøkelsen.

7. Referanseliste

Aven, Terje (2015): *Risikostyring.* (2. opplag), Universitetsforlaget.no

Aven, T., Renn, O. (2010): *Risk, Governance and society concept, guidelines and applications* (1. Ed) Springer

Aven, Terje & Røed, Willy & Wiencke, Hermann S. (2008): *Risikoanalyse.* (1. opplag), Universitetsforlaget.no

Aven, Terje & Røed, Willy & Wiencke, Hermann S. (2010): *Risikoanalyse.* (2. opplag), Universitetsforlaget.no

Busmundrud, Odd & Maal, Maren & Kiran, Jo Hagness & Endregaard, Monica (2015): *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger*. Forsvarets forskningsinstitutt (FFI)

Engen, Ole Andreas H. & Kruke, Bjørn Ivar & Lindøe, Preben Hempel & Olsen, Kjell Harald & Olsen, Odd Einar & Pettersen, Kenneth Arne (2016): *Perspektiver på samfunnssikkerhet* (1. utgave), Cappelen Damm Akademisk

Datatilsynet.no [online]: Iverksette styringssystem for informasjonssikkerhet. Tilgjengelig fra https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/internkontroll-og-informasjonssikkerhet/iverksette-styringssystem-for-informasjonssikkerhet/ [Lastet ned 23.09.18].

Jacobsen, Dag Ingvar (2018): *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode*. (3. opplag), Cappelen Damm Akademisk

Jore, S. H. (2017): Safety and security – is there a need for an integrated approach? *Risk, Reliability and Safety: Innovating Theory and Practice – Walls, Revie & Bedford (Eds), Taylor & Francis Group, London* (Eds), 2017

NOU (2000:24). *Et sårbart samfunn – Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet.* Statens forvaltningstjeneste Informasjonsforvaltning, Oslo, 2000

NOU (2015: 13). *Digital sårbarhet – sikkert samfunn.* Departementenes sikkerhets- og serviceorganisasjon Informasjonsforvaltning, Oslo, 2015

NSM (2015): *Veileder – Sikkerhetsstyring, NSM [online]. Tilgjengelig fra:* https://nsm.stat.no/globalassets/dokumenter/veiledninger/veileder-i-sikkerhetsstyring--endelig.pdf [Lastet ned 11.07.18]

NSM (2016): *Håndbok - Risikovurdering for sikring, NSM [online]. Tilgjengelig fra:* https://nsm.stat.no/globalassets/dokumenter/handboker/risikovurdering_nsm_handbok_mars2016.pdf [Lastet ned 11.07.18]

NSM (2018): *Et sikkert digitalt Norge – IKT-risikobilde 2018, NSM [online]. Tilgjengelig fra:* https://nsm.stat.no/globalassets/rapporter/nsm_ikt-risikobilde_2018_web.pdf [Lastet ned 03.10.18]

Perry, Ronald W. & Lindell, Michael K. (2003) *Preparedness for Emergency Response: Guidelines for the Emergency Planning Process*, Disasters, 2003, 27

Rausand, Marvin & Utne, Ingrid Bouwer (2014): *Risikoanalyse – teori og metoder*. (2. opplag), Fagbokforlaget

Refsdal, Atle & Solhaug, Bjørnar & Stølen, Ketil (2015): *Cyber-Risk Management.* (1. ed), Springer International Publishing AG

Renn, O. (2008) *Risk Governance. Coping with Unertainty in a Complex World*. (1.ed) Earthscan Risk in Society

Taylor, Robert W. & Fritsch, Eric J. & Liederbach, John & Saylor, Michael R. & Tafoya, William L. (2017): *Cyber Crime and Cyber Terrorism.* (4. utgave), Pearson

Vedlegg A

Intervjuguide

Spørsmålene under er veiledende. Det vil komme flere oppfølgingsspørsmål til svar intervjuobjektene gir. Meningen med intervjuene er å få fagpersoners vurdering av de ulike temaene som tas opp.

Introduksjon

- Presentasjon
- Gjennomgang av samtykkeskjema

Del I Sårbarheter og ISMS

- Hva legger du i begrepet ”sårbarhet”?
- Har organisasjonen et levende ISMS?
    - Oppdateres denne jevnlig?
    - Er den kjent og i bruk for brukerne i organisasjonen?

Del II Prosesser for risiko- og trusselanalyser

- Kan du beskrive organisasjonens prosess for risikoanalyse?
    - Hvilke(n) metode(r) benyttes for risikoanalyser?
- Kan du beskrive organisasjonens prosess for trusselanalyser?
    - Metode for trusselanalyser
    - Hyppighet for trusselanalyser
    - Evt. hvorfor gjennomføres det ikke trusselanalyser?
    - Hvilken rolle har trusselanalysen i arbeid med risikoanalyse og -håndtering?
- Risikohåndtering
    - Prosess for håndtering av risikoer
    - Har organisasjonen risikoregister, og benyttes dette aktivt?
- Ledelsens rolle og involvering
    - I risikohåndtering
    - Trusselanalyser
    - hendelseshåndtering

- Håndtering av output fra risiko- og trusselanalyser

Del III Operativ sikkerhet og hendelseshåndtering

- Har organisasjonen egen CERT, operativ sikkerhet og hendelseshåndtering?
- Hvordan er organiseringen av operativ sikkerhet og evt. CERT i forhold til strategisk sikkerhet, og hva slags samhandling er det mellom disse to?
- Hva slags formelle prosesser for hendelseshåndtering ved tilsiktede angrep foreligger i organisasjonen?
    - Jevnlige øvelser?
    - Ulike scenarier?
- Hva slags samhandling med andre organisasjoner og myndigheter rundt trusselaktører og tilsiktede hendelser har organisasjonen?

Del IIII Input til overvåkning og hendelseshåndtering ved tilsiktede angrep

- På hvilken måte benyttes risikoprosessen i arbeidet med håndtering av eventuelle tilsiktede angrep?
- I hvilken grad, og på hvilken måte, benyttes risikoanalyser som input i arbeidet med overvåkning og hendelseshåndtering?
- I hvilken grad, og på hvilken måte, benyttes trusselanalyser som input i arbeidet med overvåkning og hendelseshåndtering?
- Hva påvirker hvilke beslutninger som tas mht. hvilket fokus man har rundt overvåkning av infrastrukturen med mer?
- Hvilken rolle har ledelsen i planlegging og prioriteringer som tas i forbindelse med overvåkning og hendelseshåndtering?
- Hva slags aktiviteter har organisasjonen iverksatt i tilknytning til sikkerhetsloven og hvordan denne påvirker organisasjonen?
- Hvilke prosessuelle utfordringer opplever virksomheten i møte med tilsiktede angrep?

Vedlegg B

Vil du delta i masterprosjektet

*” I hvilken grad benyttes risiko- og trusselvurderinger aktivt i arbeid med informasjonssikkerhet, og spesifikt som input til hendelseshåndtering ved tilsiktede angrep?”***?**

Dette er et spørsmål til deg om å delta i et masterprosjekt hvor formålet er å se på hvordan utvalgte virksomheter benytter risiko- og trusselvurderinger i arbeidet med overvåkning og hendelseshåndtering i forbindelse med tilsiktede angrep på informasjonsinfrastruktur. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Prosjektet er en masteroppgave i Risiko og sikkerhetsledelse, som er et erfaringsbasert masterstudie ved Universitetet i Stavanger. Oppgaven har et omfang på 30 studiepoeng, og skal leveres i slutten av oktober 2018.

Formålet med prosjektet er å se på organisering av informasjonssikkerhetsarbeid blant aktører som forvalter kritisk infrastruktur og/eller informasjon, herunder med fokus på sikring mot tilsiktede angrep. I dette ligger angrep som er nøye planlagt, og hvor informasjonsteknologi enten er et middel eller et våpen.

Den overordnede problemstillingen er ”I hvilken grad benyttes risiko- og trusselvurderinger aktivt i arbeid med informasjonssikkerhet, og spesifikt som input til hendelseshåndtering ved tilsiktede angrep?” hvor fokuset er brutt ned i følgende forskningsspørsmål:

- Hvordan gjennomføres det strategiske arbeidet med sikkerhet, herunder risiko- og trusselvurderinger?

- Hva trengs som input i arbeidet med overvåkning og hendelseshåndtering av tilsiktede angrep?
- På hvilken måte er det tilrettelagt for samhandling på tvers av strategisk og operativt sikkerhetsarbeid?

Hvem er ansvarlig for forskningsprosjektet?

Masteroppgaven gjennomføres som ledd i det erfaringsbaserte masterstudiet Risiko- og sikkerhetsledelse ved Universitetet i Stavanger (UiS).

Oppgaven skrives av: J. Angélique W. Colle

Hvorfor får du spørsmål om å delta?

Oppgavens hovedfokus er aktører og organisasjoner tilknyttet ulike former for kritisk infrastruktur og/eller informasjon.

Hva innebærer det for deg å delta?

Det er ønskelig å bruke kvalitativ metode til denne oppgaven. Dette skyldes både problemstillingens formulering, herunder at det er nærliggende å ta for seg flere sektorer som har til felles at de forvalter kritisk infrastruktur og/eller informasjon, og hvor det således vil være interessant å få en dypere innsikt i hvordan dette arbeidet utarter seg i de ulike sektorene. I tillegg er det forventet at det vil være vanskeligheter med å finne mengdeinformasjon på område.

I den forbindelse er det ønskelig å gjennomføre intervjuer med utvalgte ressurser som innehar relevante posisjoner innen strategisk og operativt sikkerhetsarbeid som risiko- og trusselvurderinger, håndtering av uønskede, tilsiktede hendelser innen informasjonsinfrastruktur eller organiseringen rundt slike hendelser.

Intervjuene vil ta ca. 45 – 60 minutter, og vil ha en relativt fri oppbygning der det er noen konkrete spørsmål det er ønskelig at intervjuobjektene besvarer sett fra eget/egen organisasjons ståsted.

Elektroniske og/eller manuelle/skriftlige notater vil tas under intervjuet, og lagres elektronisk. Eventuelle opptak vil slettes når oppgaven er ferdig og levert.

Navn og andre direkte identifiserbare opplysninger vil ikke publiseres i oppgaven.

Spørsmål under intervjuet vil eksempelvis kunne være:

- Kan du beskrive virksomhetens prosess for risiko?
- Gjennomføres det jevnlig trusselvurderinger, og benyttes disse aktivt?
- På hvilken måte benyttes risikoprosessen i arbeidet med håndtering av eventuelle tilsiktede angrep?
- Hvordan er samarbeid og informasjonsutveksling internt i sektoren og mot andre sektorer?
- Hvilke prosessuelle utfordringer opplever virksomheten i møte med tilsiktede angrep?

Det er frivillig å delta

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

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

- Kun oppgavens forfatter (student) og dennes veileder vil ha tilgang til de direkte identifiserbare opplysningene.
- Navn og kontaktinfo vil lagres på en egen liste med nøkkel til intervjunotatene, lokalt på en datamaskin, adskilt fra de respektive intervjunotatene.
- Intervjunotatene lagres med nøkkel, sektor og intervjuobjektets rolle/stilling, eksempelvis 45 - Kraft, organisasjon C, CERT-koordinator. Der organisasjonens navn

vanskelig kan skjermes i publiseringen, vil (kun) denne også fremgå sammen med intervjunotatene.

Ingen direkte identifiserbare personopplysninger vil publiseres, med mindre annet er avtalt direkte med intervjuobjektet.
Indirekte identifiserbare opplysninger som rolle, sektor og organisasjon vil dog kunne publiseres, men vil maskeres *så langt som mulig*, med mindre annet er avtalt direkte med intervjuobjektet.
Eksempel på fremstilling ved forsøk på skjerming: ”sikkerhetsanalytiker A i helsesektoren” eller ”CERT-koordinator B ved organisasjon 3 i kraftsektoren”, der hver organisasjon vil ha noen beskrivende ord.

I tilfeller der det er vanskelig eller uhensiktsmessig å maskere organisasjon, eksempelvis grunnet dennes posisjon, vil intervjuobjektene likevel søkes maskert så langt som mulig, blant annet ved å bruke generiske ord på rolle, med mindre annet er avtalt direkte med intervjuobjektet.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?
Prosjektet skal etter planen avsluttes 21.10.18, når oppgaven leveres.
Navn og kontaktinformasjon vil slettes ved prosjektets slutt.

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

- innsyn i hvilke personopplysninger som er registrert om deg,
- å få rettet personopplysninger om deg,
- få slettet personopplysninger om deg,
- få utlevert en kopi av dine personopplysninger (dataportabilitet), og
- å sende klage til personvernombudet eller Datatilsynet om behandlingen av dine personopplysninger.

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

På oppdrag fra Angélique Colle, elev ved Universitetet i Stavanger har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Hvor kan jeg finne ut mer?

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

- Universitetet i Stavanger ved:
    - Veileder: Jon T. Selvik,
        - Telefon: 51833599
        - Mail: jon.t.selvik@uis.no
    - Student: Angélique Colle
        - Telefon: 40 86 29 27
        - Mail: ja.colle@stud.uis.no / julie.colle@gmail.com
- NSD – Norsk senter for forskningsdata AS, på epost (personvernombudet@nsd.no) eller telefon: 55 58 21 17.

Med vennlig hilsen

Prosjektansvarlig (Forsker/veileder)

Eventuelt student

Vedlegg C

Samtykkeerklæring

Samtykke kan innhentes skriftlig (herunder elektronisk) eller muntlig. NB! Du må kunne dokumentere at du har gitt informasjon og innhentet samtykke fra de du registrerer opplysninger om. Vi anbefaler skriftlig informasjon og skriftlig samtykke som en hovedregel.

- *Ved skriftlig samtykke på papir, kan du bruke malen her.*

- *Ved skriftlig samtykke som innhentes elektronisk, må du velge en fremgangsmåte som gjør at du kan dokumentere at du har fått samtykke fra rett person (se veiledning på NSDs nettsider).*
- *Hvis konteksten tilsier at du bør gi muntlig informasjon og innhente muntlig samtykke (f.eks. ved forskning i muntlige kulturer eller blant analfabeter), anbefaler vi at du tar lydopptak av informasjon og samtykke.*

Hvis foreldre/verge samtykker på vegne av barn eller andre uten samtykkekompetanse, må du tilpasse formuleringene. Husk at deltakerens navn må fremgå.

Tilpass avkryssingsboksene etter hva som er aktuelt i ditt prosjekt. Det er mulig å bruke punkter i stedet for avkryssingsbokser. Men hvis du skal behandle særskilte kategorier personopplysninger og/eller de fire siste punktene er aktuelle, anbefaler vi avkryssingsbokser pga. krav om eksplisitt samtykke.

Jeg har mottatt og forstått informasjon om prosjektet *I hvilken grad benyttes risiko- og trusselvurderinger aktivt i arbeid med informasjonssikkerhet, og spesifikt som input til hendelseshåndtering ved tilsiktede angrep?*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☐ å delta i *(sett inn aktuell metode, f.eks. intervju)*
- ☐ å delta i *(sett inn flere metoder, f.eks. spørreskjema) – hvis aktuelt*
- ☐ *at opplysninger om meg publiseres slik at jeg kan gjenkjennes (beskriv nærmere) – hvis aktuelt*

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet, ca. *(oppgi tidspunkt)*

(Signert av prosjektdeltaker, dato)