UiT
NORGES
ARKTISKE
UNIVERSITET

Institutt for ingeniørvitenskap og sikkerhet

Beskyttelse av sensitiv informasjon

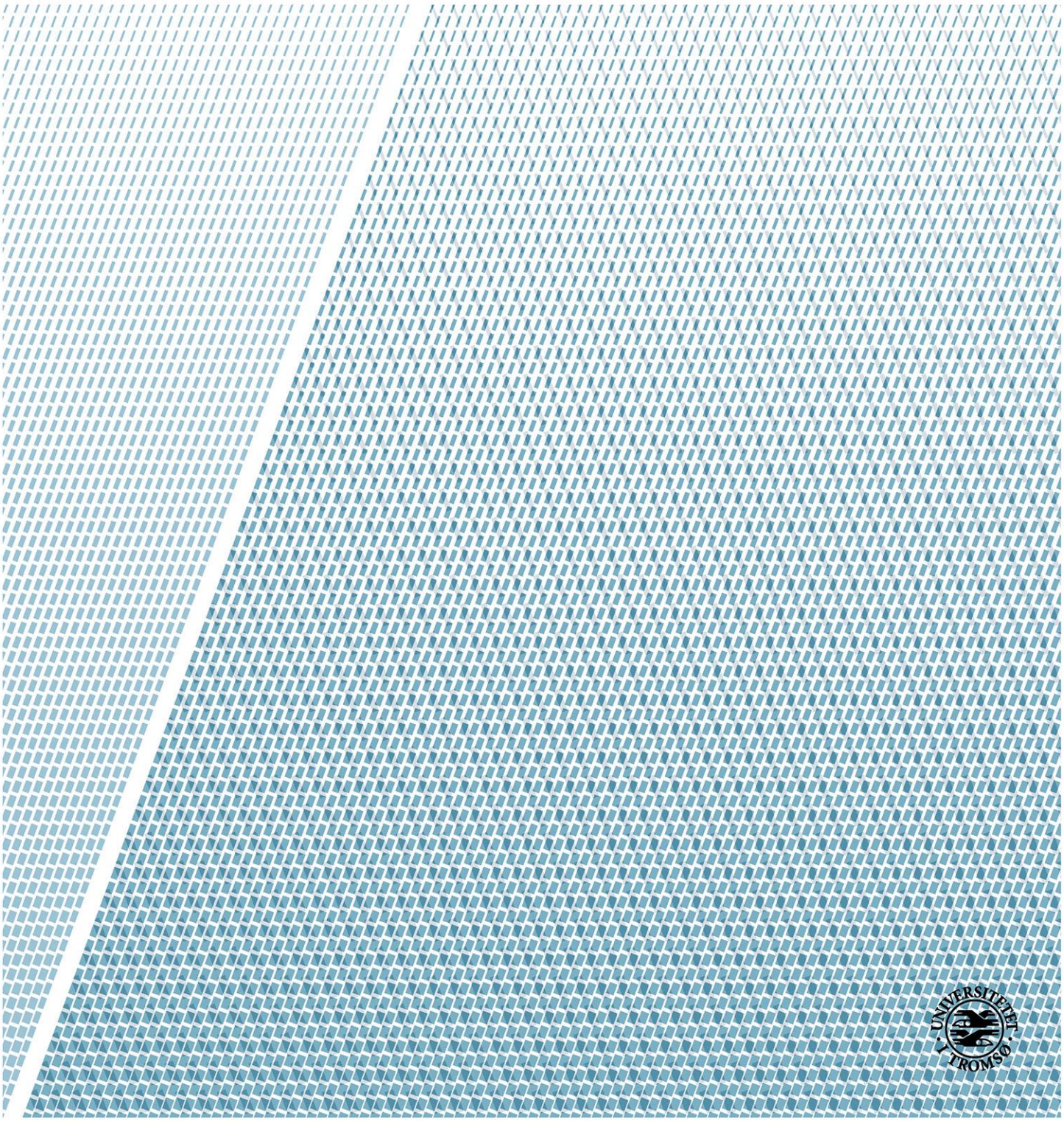
En studie av norske nettselskapers beskyttelse av sensitiv informasjon

Marta Helene Eskeland Kruke

Masteroppgave i samfunnssikkerhet, fordypning i sikkerhet og beredskap i nordområdene

Juni 2017

Antall ord: 23 577



Sammendrag

I dag tar de fleste tilgangen til strøm for gitt. Vi forventer at komfyren skal fungere når vi lager middag, at det er varmt vann i dusjen og at lyset tennes når vi trykker på bryteren (Statnett, 2014, 28.11). Nettselskapene i Norge jobber for å opprettholde en sikker og stabil strømforsyning. Dette arbeidet inkluderer beskyttelse av sensitiv informasjon, altså opplysninger om energiforsyningen som kan brukes til å skade anlegg eller påvirke funksjoner som har betydning for energiforsyningen (beredskapsforskriften, 2013).

Min studie har fokus på de sikringstiltakene, barrierene, som implementeres i nettselskapene for å beskytte sensitiv informasjon. I tillegg beskrives viktigheten av ansattes kollektive bevissthet for at barrierenes funksjon skal kunne opprettholdes. Oppgaven svarer på følgende problemstilling: ***Hvordan bruker norske nettselskaper barrierer for å forhindre uønsket innsyn i sensitiv informasjon og hvordan påvirker de ansattes kollektive bevissthet barrierenes funksjon?***

I den forbindelse har jeg gjennomført tre intervjuer i tre nettselskaper, samt ett i Norges vassdrags- og energidirektorat (NVE). Innsamlede intervjudata er diskutert sammen med sekundærdata (rapporter, risikobilder, NOUer med mer), egne observasjoner, samt teori på (1) intenderte og ikke-intenderte handlinger og hendelser, (2) barrierer og (3) kollektiv bevissthet.

Oppgaven konkluderer med at samtlige nettselskaper har innført barrierer av fysisk, teknisk og operasjonell karakter for å hindre lekkasje av sensitiv informasjon. Disse barrierene brukes i et samspill. En teknisk brannmur er ubrukelig hvis en utro tjener på innsiden i et selskap plugger inn en minnepinne med skadevare, eller lekker sensitiv informasjon til utenforstående. Fysiske sperringer og adgangskontroll i inngangspartiet i selskapenes kontorbygg er bortkastet hvis en slurvete ansatt ukritisk slipper gjester gjennom med sitt ansattkort, eller låner ut sitt ansattkort. Jeg argumenterer i denne oppgaven for at kollektiv bevissthet hos ansatte har en slags overordnet rolle for å hindre uønsket innsyn i sensitiv informasjon. Dette fordi mange barrierer vil miste sin funksjon hvis ansatte ikke har fokus på informasjonsbeskyttelse. «Sikkerheten i selskapenes IT-systemer blir ikke bedre enn 'det svakeste leddet' i verdikjeden» (Hagen m.fl., 2017, s. 12). Vi mennesker gjør feil, med og uten vilje. Et selskap som jobber mot kollektiv bevissthet vil jobbe for trusselbevissthet og barrierebevissthet, noe som gjør at de ansatte har en forståelse for eksisterende trusselsituasjon, samt svakheter i sikkerhetsbarrierer og behov for nye barrierer der det trengs.

Samtidig er påliteligheten til strømleveransen i Norge god. Det kan tyde på at det etableres barrierer som holder trusselaktører ute. Barrierene fungerer i et samspill hvor mangfoldighet og redundans er stikkord som gjør beskyttelsen av sensitiv informasjon mer robust. For at barrierene skal være relevante og holde, og dermed beskytte sensitiv informasjon, må ansatte i kraftbransjen ha en kollektiv bevissthet med tanke på både trusler og barrierer; de må være bevisste på verdien som må beskyttes (verdibevissthet), på truslene mot verdiene (trusselbevissthet) samt på de barrierer som må etableres for å beskytte verdiene mot trusselaktørene (barrierebevissthet).

Forord

Denne oppgaven markerer avslutningen på mitt toårige masterstudie i Samfunnssikkerhet ved Universitetet i Tromsø. De siste to årene har vært både innholdsrike og utfordrende, kanskje spesielt det siste semesteret. Jeg har lært at å skrive en masteroppgave er krevende, fra start til slutt. På veien har jeg imidlertid fått hjelp og støtte fra mange gode venner og familie! Jeg vil takke min veileder, Maria Hammer, for hjelp og gode kommentarer gjennom hele løpet. Videre vil jeg takke alle mine intervjuobjekter for innholdsrike og hyggelige intervjuer. Jeg kan si helt sikkert at oppgaven ikke ville blitt den samme uten dere! Spesielt én av kontaktpersonene mine i ett selskap fortjener ekstra oppmerksomhet. Jeg vil ikke nevne navn, men vedkommende takkes for mail-utveksling, tilgjengelighet og dekking av reiseutgifter. I tillegg vil jeg rette en stor takk til min flotte familie. Marit, Bjørn Ivar, Ingrid og Maren; dere er viktige! Sist, men ikke minst, TUSEN TAKK til mine studiekollegaer og venner i Tromsø. Mye kaffe, makrell i tomat, faglige diskusjoner, bordtennis og tull&tøys har gjort susen! Dere er knall, lykke til videre.

Marta Helene Eskeland Kruke

Tromsø, 01.06.2017

Innhold

Figuroversikt:

Tabelloversikt:

Oversikt over vedlegg:

1. INNLEDNING

1.1 Problembeskrivelse og problemstilling

I dag tar de fleste tilgangen på strøm for gitt. Vi forventer at komfyren skal fungere når vi lager middag, at det er varmt vann i dusjen og at lyset tennes når vi trykker på lysbryteren (Statnett, 2014, 28.11). Teknologisk utvikling og digitalisering har forenklet hverdagen for de aller fleste og er å anse som en driver for utvikling, innovasjon, vekst og produktivitet (NOU2015:13, 2015). Den tyske sosiologen Ulrich Beck hevder at vårt samfunn har utviklet seg fra et industrisamfunn til et risikosamfunn, en utvikling som bringer ukjente utfordringer (Beck, 1992). Vår økte bruk av digital teknologi går hånd i hånd med digitale trusler i alle samfunnssektorer (Fridheim, Hagen & Henriksen, 2001[1]; Meld. St. 37 (2014-2015), 2015). Dagens cyber-angrep blir stadig mer sofistikerte, målrettede og koordinerte (Choo, 2011; Zheng & Lewis, 2015; Skopik m.fl., 2016). Vi beveger oss bort fra hobby-hacking og over på organiserte og standhaftige cyber-angrep (Farwell & Rohozinski, 2011; Tankard, 2011; Skopik m.fl., 2016). I juni 2010 ble dataormen Stuxnet sluppet (Kushner, 2013). Stuxnet spionerte på og omprogrammerte prosesser innen kraftverk, trafikksystemer og fabrikker rundt om i verden med det formål å samle informasjon som gjorde den kapabel til å ta kontroll over, eller fjernstyre, såkalte «Supervisory Control and Data Acquisition»-systemer, SCADA (Kushner, 2013). SCADA-systemer er en kombinasjon av fysiske prosesser og programvare som kontrollerer og overvåker industrielle prosesser[2] (NVE, 2016a).

I 2014 var norsk olje- og energibransje under alvorlige og målrettede dataangrep (Meld. St. 37 (2014-2015), 2015). E-poster til en rekke virksomheter i bransjen prøvde å lure mottakerne til å åpne lenker som inneholdt virus (NSM, 2015a). Nasjonal sikkerhetsmyndighet (NSM) avdekket alvorlige sårbarheter i norsk kritisk infrastruktur i 2014 (NSM, 2015a).

Samme år, i 2014, gikk flere nettgiganter sammen om å opprette Kraft Computer Emergency Response Team (KraftCERT)[3]. Dette er et felles organ for kraftbransjen som har som

[1] Sluttrapport etter BAS3. «Beskyttelse av samfunnet» (BAS) er en serie av prosjekter som ser på utfordringer innen beskyttelse av det norske samfunnet. Serien ble startet av FFI i 1994, og utgjør et samarbeid mellom flere aktører innen samfunnssikkerhet og beredskap i Norge (FFI, 2015, 25.2). Utfordringer knyttet til sårbarhet i kritisk infrastruktur er et hovedtema i flere av prosjektene. En utfyllende liste over publikasjoner i forbindelse med BAS finnes her: https://www.ffi.no/no/Publikasjoner/Documents/BAS-publikasjoner_feb15.pdf

[2] Systemene er vanlige innen lufttransport, trafikksignaler, produksjon, vannverk, energiforsyning med mer.

[3] Se underkapittel 5.3.4 for utdypende beskrivelser av KraftCERT.

oppgave å holde kraftbransjen oppdatert på sårbarheter og trusler (KraftCERT, 2015). De skal også bistå under eventuelle angrep. I 2015 skjedde et nytt cyberangrep i Ukraina, som førte til utenlandsk fjernstyring av SCADA-systemer (E-ISAC, 2016). Her mistet rundt 225.000 kunder strømmen etter at 30 transformatorstasjoner ble slått ut. KraftCERT analyserte hendelsen i Ukraina og konkluderte med at liknende kan skje i Norge (Johansen, 2016).

Det norske kraftsystemet er å anse som kritisk infrastruktur, som kan defineres som «teknologiske systemer som leverer løsninger og tjenester av stor betydning for samfunnet» (Engen m.fl., 2016, s. 138). Stabil tilgang på energi er grunnleggende for samfunnssikkerheten (DSB, 2016). Samfunnet er avhengig av strøm til blant annet oppvarming, kommunikasjon, transport, helse og finans, samtidig som kraftsektoren er avhengig av offentlig elektronisk kommunikasjon. Dette er et eksempel på gjensidig avhengighet som er et sentralt kriterium for at en hendelse skal kunne true samfunnssikkerheten (Kruke, Olsen & Hovden, 2005). Gjensidig avhengighet mellom sektorer og funksjoner gir avhengigheter som øker samfunnets sårbarhet: Digitale angrep rettet mot energiforsyningen vil derfor kunne ramme store deler av samfunnet hardt (Fridheim, Hagen & Henriksen, 2001; Meld. St. 37 (2014-2015), 2015).

I sluttrapporten til BAS3 (En sårbar kraftforsyning) poengteres det at samfunnets avhengighet av pålitelig kraftforsyning, i tillegg til et fremtidig usikkert trusselbilde, tilsier at det må iverksettes sårbarhetsreduserende tiltak (Fridheim m.fl., 2001). Det er behov for veletablerte organisatoriske, teknologiske og menneskelige sikringstiltak (Hagen m.fl., 2008; Bartnes m.fl., 2016) for å beskytte særlig viktig, eller sensitiv, informasjon i kraftbransjen. Sensitiv informasjon er all informasjon som kan brukes til å skade energiforsyningen (bfe, 2013). Dette kan være informasjon både i digital og analog form. Havner denne i gale hender kan kraftforsyningen skades, med store konsekvenser for samfunnet (NOU2015:13, 2015).

For å beskytte sensitiv informasjon trengs en «forsvar i dybden»-mentalitet hvor aspekter som ansatte, prosesser og teknologi inkluderes (Ernst & Young, 2011). James Reason (1997) beskriver «forsvar i dybden» som etterfølgende lag av beskyttelse hvor hvert lag beskytter mot mulig brudd i laget før. Reason (1997) argumenterer her for redundans og mangfoldighet innen barrierer. Redundans gir mange lag av beskyttelse, mens mangfold peker på variasjon i beskyttelse (Reason, 1997). Barrierer er fysiske eller ikke-fysiske forhold som skal forhindre, kontrollere eller begrense uønskede hendelser eller ulykker (Sklet, 2006). Barrierer kan dermed være alt fra kunnskap til tekniske brannmurer. Skulle en ansatt for eksempel være

slurvete i sin beskyttelse av sensitiv informasjon vil barrierer i form av prosesser eller teknologi kunne hindre uønsket innsyn i sensitiv informasjon. Mennesker er en av de viktigste enhetene i en organisasjon – men også en av de svakeste leddene i sikkerhetskjeden (Johnson, 2006). I følge Mathisen (2004) vil selv de sikreste sikkerhetssystemene være utrygge dersom operatørene har dårlige holdninger og ikke oppfører seg som de skal. Han får støtte av Mørketallsundersøkelsen gjennomført av Nasjonal Sikkerhetsmyndighet i 2016 (NSR, 2016). Funn fra undersøkelsen viser at ansattes feil og manglende kompetanse er en del av sikkerhetsbrister i flere hundre av de forespurte virksomhetene (NSR, 2016). Situasjonsbevissthet (Sarter & Woods, 1991; Jajodia m.fl., 2010) eller kollektiv bevissthet (Weick & Sutcliffe, 2007) blant ansatte i kraftselskaper blir derfor viktig for å holde fokus på både trusler mot kraftbransjen, samt for de sikkerhetstiltak eller barrierer som implementeres for å møte truslene. Kollektiv bevissthet beskrives av Weick og Sutcliffe som en kapasitet til å oppdage og forstå betydningen av svake signaler, samt effektivt respondere på dem (Weick & Sutcliffe, 2001). Dette kommer vi tilbake til i teorikapitlet.

På bakgrunn av de forholdene som nå er presentert er min problemstilling som følger:

Hvordan bruker norske nettselskaper barrierer for å forhindre uønsket innsyn i sensitiv informasjon og hvordan påvirker de ansattes kollektive bevissthet barrierenes funksjon?

For å kunne beskytte en verdi må man kartlegge hva som skal beskyttes, og hva/hvem verdien skal beskyttes mot. I denne studien vil jeg se på hvordan nettselskaper hindrer uønsket innsyn i sensitiv informasjon. Ulike aktører kan ønske innsyn i sensitiv informasjon av ulike grunner, og det vil være sentralt å kartlegge hvilke trusler og trusselaktører det her er snakk om. For å beskytte sensitiv informasjon mot disse aktørene implementeres det tiltak, eller barrierer, som skal hindre trusselaktørene tilgang. Det er derfor viktig med en bevissthet både om de trusler man står overfor, hvilke barrierer som er nødvendige for å møte truslene, samt tilstanden til de barrierer som er etablert. På bakgrunn av dette har jeg brutt ned problemstillingen i følgende forskningsspørsmål:

a) Hvilke trusler og angrep mot sensitiv informasjon står nettselskapene overfor?
b) Hva slags barrierer etableres for beskyttelse av sensitiv informasjon i nettselskapene?
c) Hvordan er den kollektive bevisstheten mtp. beskyttelse av sensitiv informasjon i nettselskapene og hvordan påvirker dette barrierenes funksjon?

1.2 Avgrensninger

Av mer enn 150 norske nettselskaper har jeg valgt ut 3. Intervjuene er nesten utelukkende gjennomført med respondenter fra nettselskapenes ledelse. Jeg har jobbet ut fra et ønske om å fokusere på bevisstheten i selskapenes overordnede barrierearbeid for å forhindre uønsket innsyn i sensitiv informasjon. Dette ligger til grunn for at jeg har avgrenset intervjuene til respondenter i selskapenes ledelse.

Jeg har avgrenset meg til nettselskaper, så andre aktører i kraftbransjen, for eksempel strømprodusenter, er ikke inkludert. Når det gjelder barrierer og barriereteori har jeg tatt på meg samfunnsfaglige briller under arbeidet med denne oppgaven. Teknologiske løsninger og oppbygning av digitale sikkerhetsprogrammer har dermed ikke vært i fokus. Jeg studerer det overordnede samspillet mellom barrierene fremfor deres funksjon på detaljnivå. I tillegg har jeg gjort en avgrensning når jeg beskriver sensitiv informasjon. Jeg startet ut med informasjonssikkerhet, men innså fort at dette er svært omfattende. Informasjonssikkerhet defineres gjerne som konfidensialitet[4], tilgjengelighet[5] og integritet[6] (DIFI, 2017, 14.3). Jeg avgrenser min studie til beskyttelse av sensitiv informasjon, noe som havner inn under konfidensialitet (utdypende informasjon finnes i underkapittel 2.5).

Videre foregår det en omfattende diskusjon rundt skytjenester i kraftbransjen. Skytjenester er en samlebetegnelse for forskjellige måter å drifte IT-systemer på. Vedlegg 1 ser på problematikk innen plassering av sensitiv informasjon «i skyen». Janne Hagen i Norges vassdrags- og energidirektorat anbefaler begrensninger i bruken av skytjenester når det kommer til sensitiv informasjon (Hagen, 2015). Ettersom mitt fokus ligger på beskyttelse av sensitiv informasjon (konfidensialitet), utgår skytjenester som et sikkerhetstiltak i denne oppgaven. Hadde jeg imidlertid sett på informasjonssikkerhet (både konfidensialitet, integritet og tilgjengelighet), ville det vært nødvendig med en diskusjon rundt kostnader versus nytte av skytjenestebruk. Informasjon lagret i skytjenester er i stor grad tilgjengelig, men kanskje ikke bare for selskapet internt…

[4] Informasjon skal ikke gjøres kjent for uvedkommende.
[5] Informasjon skal være tilgjengelig ved behov.
[6] Informasjon skal ikke blir endret utilsiktet eller av uvedkommende.

1.3 Tidligere forskning

Under problembeskrivelsen er det allerede presentert en del tidligere forskning. I tillegg til denne finnes det forskning på blant annet beredskap i informasjonssikring (Hagen m.fl., 2005; Barstad, 2016) og risiko og sårbarhet ved bruk av IKT i kraftforsyningen (Skotnes, 2015). Røyksund (2011) supplerer doktorgradsarbeidet til Skotnes med sin mastergradsavhandling om risikopersepsjon med tanke på angrep på driftskontroll-systemene i kraftbransjen, samt faktorer som spiller inn for valg av informasjonssikkerhetstiltak.

Videre beskrives håndteringspraksis og forståelse for informasjonssikkerhetshendelser (Line, 2015), samt organisatorisk prioritering av sikkerhets-prosedyrer, regler og struktur (Dhillon & Backhose, 2001; Albrechtsen & Grøtan, 2004; Hagen m.fl., 2008). Hagen m.fl. (2008) fant i sin studie av implementering og effektivitet innen organisatoriske informasjonssikkerhets-tiltak at tekniske og administrative forhold i større grad enn bevisstgjøringstiltak er prioritert og implementert i selskaper. Bevisstgjøringstiltak vurderes dog som de mest effektive organisatoriske tiltakene (Hagen m.fl., 2008). Av denne grunn kan forskning på bevissthet rundt barrierefunksjoner være viktig for beskyttelse av sensitiv informasjon i nettselskaper.

1.4 Struktur på oppgaven

Kapittel én argumenterer for problemstilling og forskningsspørsmål, samt klargjør nødvendige avgrensninger og tidligere forskning. Kapittel to starter med en beskrivelse av kraftsektoren, samt en kort innføring i hva «sensitiv informasjon» er. Videre presenteres mitt teoretiske grunnlag i kapittel tre hvor jeg har valgt teori på intenderte handlinger, barrierer og kollektiv bevissthet. I kapittel fire utdyper og beskriver jeg de metodiske valg og utfordringer som har gjort seg gjeldende i denne skriveprosessen. I kapittel fem presenteres min empiri fra intervjuer, dokumentstudier og observasjon. Dette diskuteres så i drøftingskapitlet (seks) sammen med teori. Kapitlet er inndelt etter forskningsspørsmålene. De viktigste konklusjoner, samt forslag til videre forskning presenteres i kapittel sju.

2. KRAFTSEKTOREN OG SENSITIV INFORMASJON

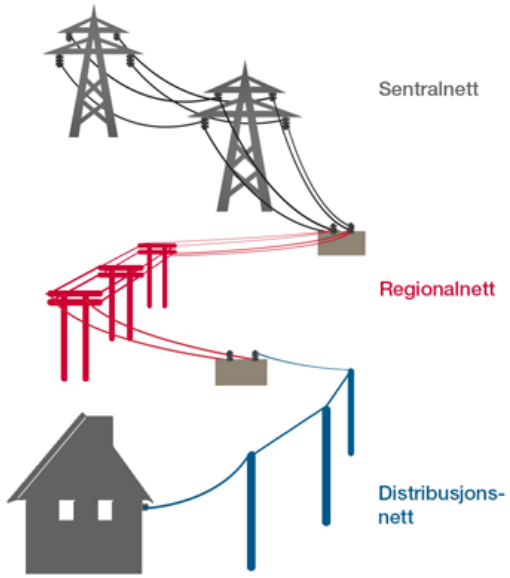
2.1 Nettselskap og kraftleverandør

Energibransjen består av nettselskaper, kraftleverandører, produsenter og andre tredjeparter (Fornybar, 2016; Hagen m.fl., 2017). Kraftleverandører er de selskapene vi kjøper strøm fra (Jansrud, 2013). I Norge finnes det over 115 kraftleverandører. Man kan velge mellom ulike kraftleverandører; for eksempel Ishavskraft AS, Hålogaland Kraft AS, Norgesenergi, Gudbrandsdal energi AS eller andre. Disse opererer i et konkurransemarked med forskjellige priser og avtalevilkår. Vi forbrukere velger en kraftleverandør uavhengig av hvor i landet vi bor. Strømmen i kontakten hjemme og kvaliteten på denne vil være lik uansett kraftleverandør (Fornybar, 2016).

Nettselskapene er, på sin side, ansvarlige for strømnettet i ulike geografiske områder og har monopol på sine tjenester innenfor sitt område. Man kan derfor ikke bytte nettselskap hvis man er misfornøyd med tjenestene som tilbys (Jansrud, 2013). Nettselskapene eier, bygger og drifter det lokale strømnettet som frakter strømmen fram til hvert enkelt hus (Fornybar, 2016). Eksempler på nettselskaper er BKK i Bergen, TrønderEnergi Nett i Trøndelag, Hafslund Nett i Oslo-området, Lyse Elnett i Stavanger og omegn eller Troms Kraft Nett AS i Troms. I Norge har vi over 150 nettselskaper (+/-). Nettselskapene reguleres av Norges vassdrags- og energidirektorat (NVE). NVE passer på at nettselskapene ikke tar for høy nettleie og at aktørene opererer i henhold til de lover og forskrifter som gjelder (Fornybar, 2016). Nettselskapene tar inn nettleie som kommer i tillegg til betaling for hver enkeltes individuelle strømforbruk. Nettleien dekker frakt av strømmen fra strømprodusent, via strømnettet, og inn til forbrukerens hus.

2.2 Kraftsystemet

Kraftsystemet i Norge består av sentralnett[7], regionalnett og distribusjonsnett (Hagen m.fl., 2017). Figur 1 er en forenklet skisse av de ulike nettene i kraftsystemet. Man kan tenke på sentralnettet som «motorvei» for norsk kraftforsyning. Sentralnettet binder landet sammen og gir alle landsdeler tilgang til en markedsplass (Andersen, Øberg, Veila, Sundheim, 2014). Videre er regionalnettet strømnettets «fylkesvei». Regionalnettet leder strøm fra sentralnettet til distribusjonsnettet. Distribusjonsnettet, kraftforsyningens «kommunalvei», sørger for kraftdistribusjon til sluttbrukerne (Andersen m.fl., 2014).

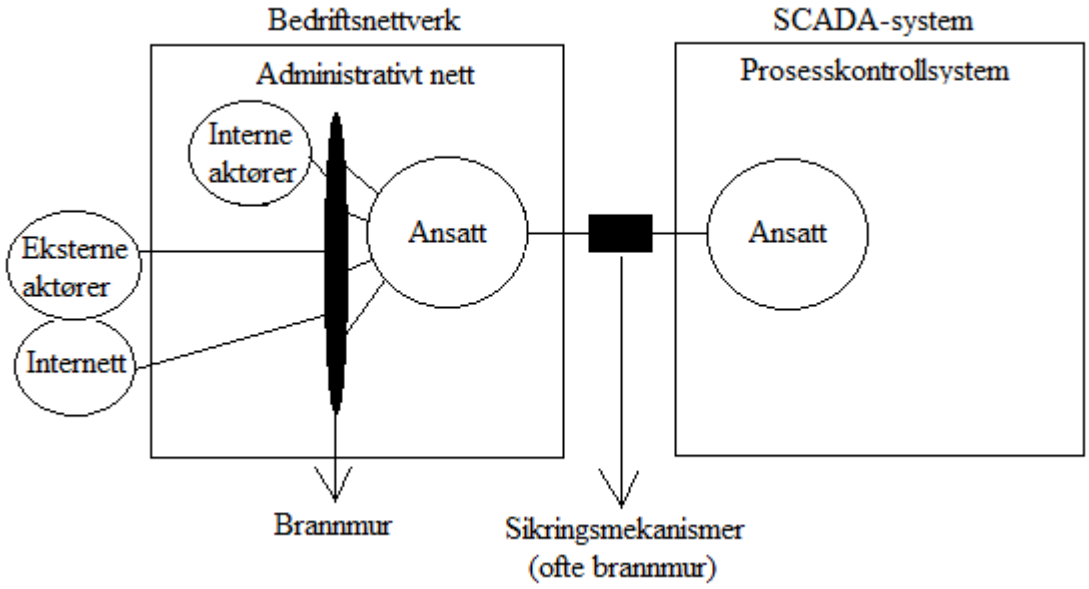


Figur 1 Kraftsystemet

2.3 Bedriftsnettverk og SCADA-system

I driften av sentralnettet og regionalnettet skilles det mellom bedriftsnettverk og Supervisory Control And Data Acquisition-systemer (SCADA-systemer), se figur 2. SCADA-systemer er industrielle kontrollsystemer for styring og overvåking av kraftforsyningen. Dette omfatter overvåking/styring av; driftssentraler, samband, servere med programvare, samt infrastruktur som fører i driftskontrollsystemet (Hovland, 2017). Bedriftsnettverket er det administrative nettet hvor henvendelser fra interne og eksterne aktører, samt Internett, bearbeides (Nygård, 2002).

[7] Også kalt transmisjonsnett.



Figur 2 Skisse over SCADA-system og bedriftsnettverk (basert på Nygård, 2002)

Tidligere var administrativt nett og SCADA-systemene helt separate. Dette var hensiktsmessig ettersom enhver kobling til et annet nettverk introduserer risiko for sikkerhetsbrist, spesielt hvis koblingen skaper mulig tilgang fra/til Internett (US Department of Energy, 2001). Som vi ser av figur 2, er det i dag kobling mellom administrativt nett og SCADA-systemer (Fridheim m.fl., 2001; Nygård, 2002; Hagen m.fl., 2017). Dette gjøres for å få bedret funksjonalitet og tilgjengelighet på data mellom nettene, men det skaper også en mulighet for ekstern tilgang til SCADA (f.eks. via Internett). Det kan i tillegg argumenteres for en redusert oversikt over hvem som har tilgang til ulike tjenester på innsiden i et selskap, og dermed økt sårbarhet for utro tjenere (Nygård, 2002). I tillegg har økt kompleksitet og krav til effektivitet gjort selskapene avhengige av eksterne aktører. Her beskrives aktører innen vedlikehold, samt fjerntilgang (NOU2015:13, 2015). SCADA-systemene er opprinnelig ikke utviklet med tanke på sikkerhet, noe som har ført til mye sikringsarbeid mot uautorisert tilgang etter hvert som systemene har blitt koblet til andre IKT-systemer og Internett (NOU2015:13, 2015).

2.4 Roller og ansvar

Olje- og energidepartementet (OED) har det overordnede ansvaret for energiforsyningen i Norge (NOU2015:13, 2015). Norges vassdrags- og energidirektorat (NVE) er underlagt OED

og har reguleringsmyndighet i elektrisitetssektoren. De fører tilsyn med sikkerhet og beredskap i kraftbransjen. Videre har statsforetaket Statnett SF systemansvaret for det sentrale strømnettet (OED, 2015), ref. figur 1. De bygger nettet og sørger for momentan kraftbalanse og god leveringskvalitet i hele landet (OED, 2015).

2.5 Sensitiv informasjon

Beredskapsforskriften beskriver sensitiv informasjon som «spesifikk og inngående opplysninger om energiforsyningen som kan brukes til å skade anlegg eller påvirke funksjoner som har betydning for energiforsyningen, herunder (bfe, 2013, § 6-2):

a) Alle system som ivaretar viktige driftskontrollfunksjoner, herunder også nødvendig hjelpeutstyr som samband.
b) Detaljert informasjon om energisystemet...
c) Detaljert informasjon om klassifiserte transformatorstasjoner med tilhørende koblingsanlegg, herunder anleggets oppbygning og drift.
d) Oversikt over fordelingsnett til samfunnskritiske funksjoner.
e) Nøyaktig kartfesting av jordkabler.
f) Forebyggende sikkerhetstiltak mot bevisst skadeverk.
g) Lokalisering av reserve driftssentraler og andre særskilte beredskapsanlegg for ledelse og drift.
h) Detaljerte analyser av sårbarhet som kan brukes til bevisst skadeverk.
i) Beredskapsplaner for å håndtere bevisst skadeverk.
j) Samlet oversikt over reservemateriell, reserveløsninger eller reparasjonsberedskap av betydning for håndtering av bevisst skadeverk.»

Sensitiv informasjon foreligger på papir, i elektronisk form eller lagret på annen måte (bfe, 2013). Hva som er sensitiv informasjon om energiforsyningen varierer (NVE, 2013). Informasjon som i utgangspunktet ikke er sensitiv kan for eksempel bli sensitiv i sammenstilling med annen informasjon hvis dette sammen gir en så spesifikk kjennskap til et anlegg eller system at det kan brukes til å skade energiforsyningen.

Kraftforsyningen har en egen beredskapsorganisasjon (KBO)[8] som består av NVE og de virksomheter som står for kraftforsyningen. Dette omfatter alle enheter som eier eller driver kraftproduksjon med tilhørende vassdragsregulering, overføring og distribusjon av elektrisk kraft og fjernvarme (NVE, 2013). KBO jobber med å «etablere, opprettholde og videreutvikle system og rutiner for effektiv avskjerming, beskyttelse og tilgangskontroll for sensitiv informasjon. Beskyttelse skal omfatte tiltak mot avlytting og manipulering fra uvedkommende» (bfe, 2013, § 6-3). Beskyttelse og tilgangskontroll bør omfatte administrative tiltak, tekniske tiltak, tiltak for bevisstgjøring og opplæring (NVE, 2013).

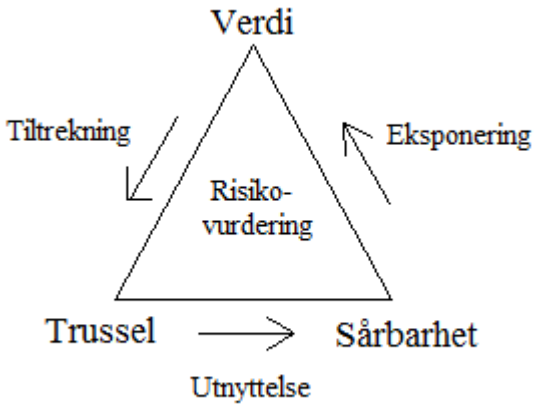
KBO-enheter som setter ut oppdrag til leverandører og andre må passe på at bestemmelsene innen informasjonssikkerhet og taushetsplikt etterleves (bfe, 2013). Det er KBO-enhetenes eget ansvar å forsikre seg om at leverandører ivaretar kravene til korrekt håndtering av sensitiv informasjon (NVE, 2013). Når det gjelder anbudsinnbydelser, skal disse begrenses så langt det er mulig. Dette for å hindre at sensitiv informasjon om energiforsyningen blir offentliggjort gjennom anbudsdokumentene (NVE, 2013).

Som nevnt i innledningen, er beskyttelse av sensitiv informasjon bare en liten del av informasjonssikkerhet, under konfidensialitet. Det er viktig å ha i bakhodet at beskyttelse av informasjon er sammensatt. Et nettselskap med fullstendig konfidensialitet kan låse ned all sensitiv informasjon, fjerne internettilkobling og fjerne alle ansatte. Dette ville beskyttet sensitiv informasjon fra uønsket innsyn. En slik radikal strategi for å beskytte sensitiv informasjon vil imidlertid ikke være mulig for et verdiskapende selskap i dagens samfunn. Informasjonssikkerhet handler også om integritet og tilgjengelighet av informasjon, og fullstendig konfidensialitet vil fjerne all tilgjengelighet av vedkommende informasjon. Motsatt vil høy grad av tilgjengelighet (for eksempel ved skylagring) kanskje øke effektiviteten, men også sjansen for at informasjon kommer på avveie (dvs. brudd på konfidensialitet) eller blir endret på en ukontrollert måte (dvs. svekket integritet) (NOU2015:13, 2015).

[8] Omfatter alle enheter som eier eller driver kraftproduksjon med tilhørende vassdragsregulering, overføring og distribusjon av elektrisk kraft og fjernvarme (NVE, 2016, 15.4).

3. TEORI

Innen risiko-, sårbarhets- og verdianalyser av ondsinnede handlinger gjøres det gjerne verdi-, trussel- og sårbarhetsvurderinger. «Trefaktormodellen» viser sammenhengen mellom verdi, trussel og sårbarhet (Engen m.fl., 2016).



Figur 3 Risikotrekanten (basert på NSM, 2016b)

Trefaktormodellen er basert på veiledere fra Nasjonal sikkerhetsmyndighet (NSM), Politidirektoratet, Politiets sikkerhetstjeneste (PST) og Norsk Standard 5832 (Engen m.fl., 2016). Figur 3 er en modifisert versjon av «risikotrekanten» som presenteres av NSM. Risiko defineres av norsk standard som et «uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen» (NS 5830:2012). Sentrale verdier er gjerne relatert til liv og helse, miljø, materielle og økonomiske verdier (Engen m.fl., 2016). Et eksempel på en verdi kan være sensitiv informasjon, jf. figur 3. Denne tiltrekker seg trusselaktører, jf. figur 3. En trussel defineres av the Council of the Society for Risk Analysis (SRA) som en risikokilde, ofte brukt i relasjon til «security»-forhold (men også i relasjon til «safety»-aspekter som for eksempel jordskjelv), se delkapittel 3.1 (Aven m.fl., 2015). I relasjon til angrep kan trussel defineres som en intensjon til å iverksette et angrep med en intensjon om å gjøre skade, skape frykt, smerte eller elendighet (Aven m.fl., 2015).

Trusselaktører kan ønske å utnytte sårbarheter i systemet for å få tak i sensitiv informasjon, jf. figur 3. Sårbarhet er «…et systems forutsetninger for eller manglende evne til å fungere under og etter at det utsettes for en uønsket hendelse» (Engen m.fl., 2016, s. 47). Sårbarhetene eksponerer den beskyttelsesverdige verdien. Jeg vil på bakgrunn av dette og forskningsspørsmålene mine presentere teori innen (1) Intenderte handlinger og ikke-

intenderte hendelser (*trusselaktører/angrep*), samt (2) barrierer (*sårbarhet*sbegrensning). I tillegg vil teori på (3) kollektiv bevissthet være sentralt for å realisere barrierer (etablering og opprettholdelse av barrierer) som hindrer trusselaktører i å nå verdien som skal beskyttes.

3.1 Intenderte og ikke-intenderte handlinger

Engen m.fl. (2016) skiller mellom to typer sikkerhet; «safety» og «security». «Tradisjonell» sikkerhet (safety) handler om sikkerhet i forhold til helse, miljø og sikkerhet (HMS), ulykker og naturlige hendelser (flom, orkan, jordskjelv, skred osv.). Security handler på sin side om sikkerhet i forhold til ondsinnede handlinger og trusler. Ondsinnede handlinger kalles også tilsiktede eller villede, mens ikke-intenderte handlinger kan omtales som utilsiktede eller ubevisste. Intenderte handlinger rammer oss fordi noen har en intensjon om å iverksette dem (Engen m.fl., 2016). Eksempler kan være terrorisme, sabotasje, spionasje, kriminalitet, vandalisme og selvdestruktiv atferd (Hovden, 2004). Dette innebærer både trusler fra utsiden (terrorisme, sabotasje, mm.) og innsiden (selvdestruktiv atferd av utro tjenere) i en organisasjon. Her plasseres selvdestruktiv atferd i kategorien intenderte handlinger, og henviser til innsidere som ønsker å gjøre skade. Sidney Dekker beskriver «bad-apples» (Dekker, 2006) som både inkluderer ansatte som intendert og ikke-intendert gjør skade i en organisasjon. Mange uønskede hendelser befinner seg i en gråsone mellom kategoriene «intenderte» og «ikke-intenderte» (Kruke m.fl., 2005). Uaktsomme aktører bryter lover og regler uten at de ønsker de negative konsekvensene (Kruke m.fl., 2005). I sin Law of Unintended Consequences beskriver Robert Merton fem kilder til «ikke-ønskede» konsekvenser (Merton, 1936):

Ignorance (uvitenhet): Alle mennesker tar valg hver dag hvor man forholder seg til et mangelfullt informasjonsgrunnlag. Vi handler som oftest ikke ut fra vitenskapelig kunnskap, men heller ut fra mening og estimering. Situasjoner som krever umiddelbar handling vil ofte involvere uvitenhet rundt visse aspekter av situasjonen, noe som kan føre til uønskede konsekvenser.

Error (feil): Feil kan forekomme i hvilken som helst fase av en målrettet handling. Merton eksemplifiserer med vaner; antagelsen om at handlinger som tidligere har ledet til et resultat, også vil fortsette å gjøre det.

Imperious immediacy of interest (ignorering av mulige side-effekter av en intendert handling): Noen ønsker en intendert konsekvens av en hendelse, og ignorerer dermed andre, ikke-intenderte effekter.

Basic values (grunnleggende verdier): En person handler ut fra fundamentale verdier, uten å vurdere konsekvensene av handlingen. Et eksempel kan være at ærlige mennesker (grunnleggende verdi), kan havne i trøbbel for å ha delt informasjon de burde ha holdt hemmelig (ikke-ønsket konsekvens).

Self-destructing predictions (selvødeleggende fordommer): En prediksjon kan bli feil fordi selve prediksjonen endrer situasjonen. Innen økonomi er det for eksempel slik at hvis folk antar, predikerer, at økonomien vil gå dårlig i fremtiden kan de velge å begrense sitt forbruk og heller spare penger. Dette kan være en selvødeleggende prediksjon ettersom deres begrensede forbruk vil resultere i dårlige økonomiske tider.

Av disse er det uvitenhet og feil, punkt 1 og 2, som har fått mest fokus (Hollnagel, 2004), noe som også er gjeldende i denne oppgaven. Ulike tiltak for å forhindre uvitenhet og feil vil begrense handlingsrommet til trusselaktører (Engen m.fl., 2016). Barrierer er slike tiltak.

3.2 Barrierer

En barriere har gjerne vært brukt for å beskytte mennesker og eiendom fra fiender og naturlige farer (Sklet, 2006). Sikkerhetsbarrierer er fysiske og/eller ikke-fysiske forhold som forhindrer, kontrollerer eller begrenser uønskede hendelser eller ulykker:

«*Physical and/or nonphysical means planned to prevent, control, or mitigate undesired events or accidents*» (Sklet, 2006, s. 505).

Konseptet rundt barrierer som grunnlag for ulykkesanalyse ble introdusert i Gibson sin energimodell i 1961 (Rosness m.fl., 2004). Haddon videreutviklet modellen da han presenterte ti strategier for forhindring av ulykker (Haddon, 1980). Disse handler om å redusere selve faren (strategi 1, 2, 3, 4, 7), barrierer (5, 6) og beskyttelse/rehabilitering av ofre (8, 9, 10) (Haddon, 1980).

Barrierer kan klassifiseres som aktive/passive (Hollnagel, 1999; Kjellén, 2000), systemiske/fysiske/administrative (Bento, 2001), tekniske/operasjonelle (Engen m.fl., 2016) eller materielle/ikke-materielle/funksjonelle/ symbolske (Hollnagel, 2004). James Reason

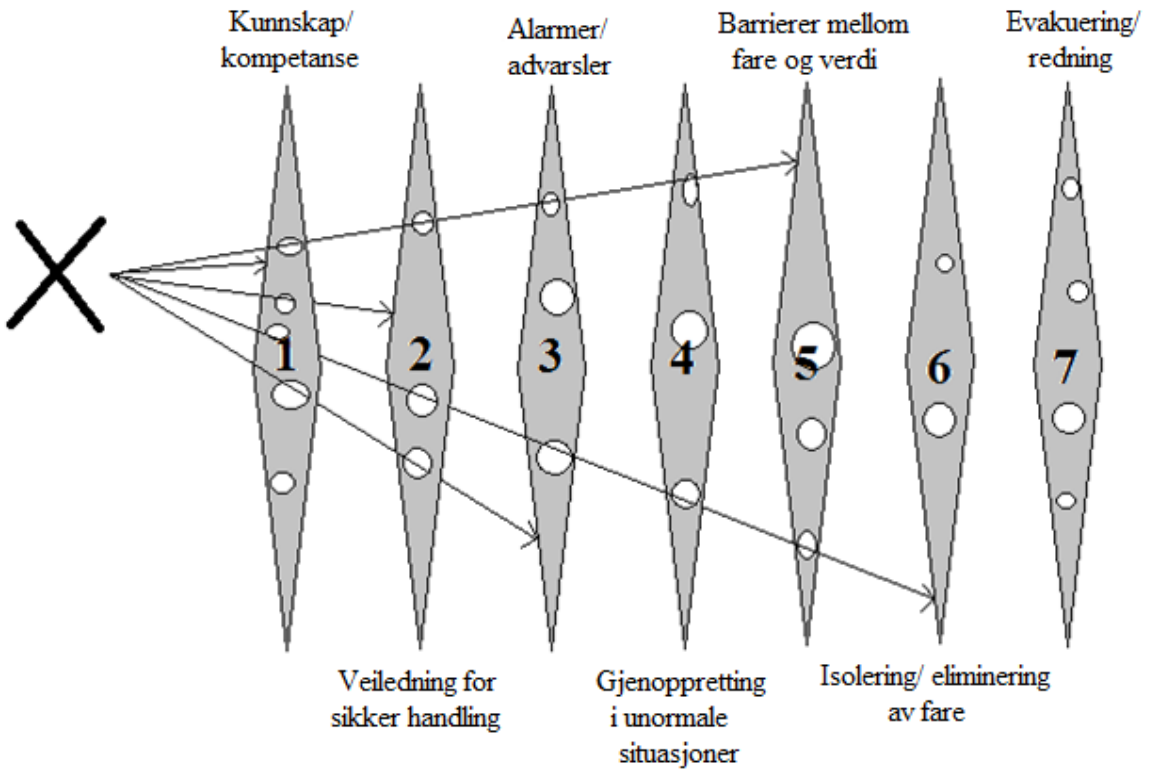
skiller mellom harde og myke barrierer (Reason, 1997). Harde barrierer inkluderer tekniske enheter, fysiske barrierer, testing, alarmer og låser. Myke barrierer omfatter en kombinasjon av papir og mennesker; lovgivning, tilsyn, regler og prosedyrer, trening, opplæring, øvelser, brifinger, administrativ kontroll, sertifisering og ledelsens oversikt (Reason, 1997).

Hollnagel skiller videre mellom barrierefunksjoner som er forebyggende og beskyttende. Forebyggende barrierer skal hindre en uønsket hendelse i å skje, eller dempe fremveksten av de faktorer som sammen kan resultere i en uønsket hendelse (Svenson, 1991). Beskyttende barrierer skal skjerme miljøet og mennesker i miljøet, samt systemet i seg selv fra konsekvensene av en uønsket hendelse (Hollnagel, 1999). Hvor skillet går mellom forebyggende og beskyttende barrierer, vil avhenge av den initierende hendelsen. I noen tilfeller kan en og samme barriere derfor være både forebyggende og beskyttende, avhengig av ståsted (Hollnagel, 1999; Badreddine m.fl., 2014). Opplæring og øvelse er typiske barrierer som kan virke forebyggende, samt beskyttende og konsekvensreduserende når en uønsket hendelse har inntruffet.

High Reliability Organizations (HRO) er organisasjoner som lykkes i å unngå alvorlige ulykker i komplekse og tette koplede høyteknologiske systemer[9] (Rochlin m.fl., 1987; LaPorte & Consolini, 1991). Mennesker vil alltid gjøre feil, og organisasjoner må kompensere for disse feilene med utgangspunkt i noen konkrete forhold: Sikkerhet og pålitelighet må ha høyeste prioritet i hele organisasjonen; redundans er viktig for å kompensere for feil; sterk organisasjonskultur; kontinuerlig læring (prøving/feiling); og desentralisering (Rochlin m.fl., 1987; LaPorte & Consolini, 1991; LaPorte, 1994; Weick m.fl., 1999). Operasjonell redundans handler om evnen til å utføre en oppgave selv om primærenheten feiler (Rochlin m.fl., 1987). Redundans skapes ved en kombinasjon av duplisering (to enheter som gjør det samme) og overlapping (to enheter med felles funksjonelt område). Det er ulike former for redundans (Rochlin m.fl., 1987): Teknisk redundans (flere tekniske enheter kan gjøre samme jobb), forsyningsredundans (tilgjengelig reservedeler og ekstrautstyr), beslutningsredundans (intern kryssjekk innen beslutningstaking samt duplisering og overlapping skulle en beslutningsenhet settes ut av funksjon). Reason (1997) beskriver forsvar i dybden hvor redundante og mangfoldige barrierer beskytter mot sammenbrudd av barrieren i front (Reason, 1997).

[9] En kontrast til HRO-tankegangen er Charles Perrows teori rundt NAT (Normal Accident Theory). Perrow argumenterer for at ulykker er uunngåelige i et høyteknologisk system med komplekse systemer og tette koplinger (Perrow, 1999).

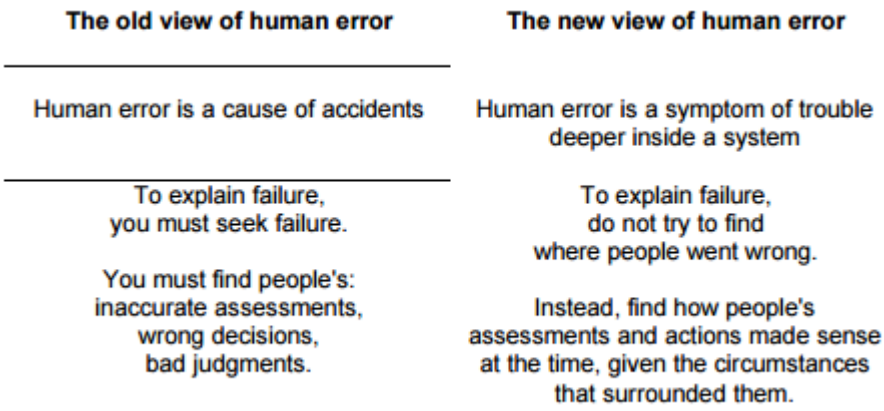
Redundans gir mange lag av beskyttelse, mens mangfold peker på variasjon i beskyttelse. En kjede av barrierer kan da ha følgende sekvensielle uttrykk:



Figur 4 Redundans og mangfold (basert på Swiss Cheese; Reason, 1997)

«Swiss Cheese-modellen» er en barrieremodell som viser at hver barriere har svakheter og hull (Reason, 1997). Figur 4 er en forenklet modell basert på «Swiss Cheese-modellen». «X», til venstre, symboliserer en trusselaktør. Når for eksempel barrierer innen kunnskap, kompetanse og veiledning feiler i å stanse trusselaktøren, skal alarmerende barrierer varsle og gjenoppretting iverksettes. Er faren fortsatt forestående, vil fysiske barrierer stå mellom faren og potensielt tap. Andre barrierer har som mål å isolere eller eliminere faren. Skulle alle disse barrierene feile, vil evakuering og redning være aktuelt. Samspillet og overlappingen i disse barrierene gjør at systemer tåler enkle feil, både av teknisk, operasjonell og menneskelig karakter (Reason, 1997). For at redundans skal fungere, må barrierene være uavhengige av hverandre slik at ikke alle kan settes ut av spill som følge av en enkelt hendelse (Reason, 1997). Her kommer mangfoldet inn. «Swiss Cheese» illustrerer at flere barrierer kan settes ut av spill samtidig. Her presenteres ulike barrierer som hullete osteskiver (Reason, 1997), vist i figur 4 med hull i barrierene. Ideelt sett ville osteskivene vært tette, uten feil og mangler. I den virkelige verden har imidlertid hvert lag, hver barriere, sine svakheter som visualiseres

gjennom hullete osteskiver i «Swiss Cheese». For å forklare hvordan hullene dannes, kan man peke på aktive feilhandlinger fra operatører i første linje samt latente forhold (Reason, 1997), eller latente feil (Turner, 1976). Sammenfallende latente forhold/feil og aktive feilhandlinger kan føre til sammenbrudd i et sikkerhetssystem, eller et system med forsvar-i-dybden (Engen m.fl., 2016). Mennesker gjør aktive feilhandlinger som direkte påvirker sikkerheten i et system. Latente forhold/feil er bakenforliggende sårbarheter som dannes over tid og som får anledning til å ligge uoppdaget og kanskje akkumulere. Denne akkumuleringsfasen kan kalles for inkubasjonsperiode (Turner, 1976). Eksempler på latente forhold/feil kan være dårlig design, hull i overvåking, uoppdagede produksjonsfeil eller svikt i vedlikehold (Reason, 1997). I dag konkluderer få granskere med aktive feilhandlinger som årsak til ulykker. Aktive feilhandlinger ses gjerne som en konsekvens av andre, bakenforliggende, forhold. Sidney Dekker diskuterer årsaksforklaringer i et MTO-perspektiv (Dekker, 2006). Han skiller mellom «the Old View» og «the New View» (Dekker, 2006), se figur 5.



Figur 5 To syn på menneskelig feil (Dekker, 2000)

«The Old View» peker på menneskelige feil som årsaker til uønskede hendelser (Dekker, 2000). Med denne bakgrunn er man på jakt etter dårlige vurderinger og feilslutninger hos ansatte, eller såkalte «bad apples». «The New View» ser menneskelige feil som et symptom på trøbbel dypere i systemet (Dekker, 2000). Dekker introduserer et prinsipp kalt «The local rationality principle» som handler om at folk gjør fornuftige valg gitt deres kunnskap, oppmerksomhet og mål (Dekker, 2006). Å kunne forstå folks handlinger betyr å se deres situasjon fra innsiden; å skjønne hvorfor deres beslutning ga mening da den ble tatt (Dekker, 2006). Dekker spør: «Bad people in safe systems, or well-intentioned people in imperfect

systems?» (Dekker, 2006). Her vil «bad people in safe systems» inngå i «the old view», mens «well-intentioned people in imperfect systems» er sentralt for «the new view».

Nå har teori rundt intenderte og ikke-intenderte handlinger og hendelser blitt presentert, i tillegg til barriereteori (inkludert årsaker til mangler i barrierer). Hva så med hvordan den kollektive bevisstheten påvirker barrierefunksjoner og derigjennom sikkerheten?

3.3 Kollektiv bevissthet

Weick og Sutcliffe (2007) refererer også til «Swiss Cheese-modellen», men da i sammenheng med forskning på kollektiv bevissthet. Hver gang et hull i en barriere er på linje med et hull i en annen barriere har man en situasjon som ikke skal oppstå, en feil å ta tak i og dermed en mulighet til å stanse en eskalerende utvikling som kan lede til en ulykke. Weick og Sutcliffe beskriver kollektiv bevissthet som en kapasitet til å oppdage den essensielle betydningen av svakheter og effektivt respondere på dem:

«*The capacity to see the significant meaning of weak signals and to give strong responses to weak signals*» (Weick & Sutcliffe, 2001, s. 3).

Mitnick og Simon (2002) mener at man ikke bør stole på tekniske sikkerhetssystemer og brannmurer for å beskytte informasjon. Man bør se etter den mest sårbare siden. Her vil man vanligvis finne at sårbarheten har med medarbeiderne å gjøre. Det er mennesker som designer, bygger, opererer, opprettholder og styrer teknologi (Reason, 1997). For at medarbeiderne skal forstå betydningen av svake signaler og svare på dem må de være tilstede i «nuet». Weick m.fl. (1999) peker på bevissthetens *kvalitet*, og at dette er vel så sentralt som konserveringen av bevissthet (Weick m.fl., 1999). En organisasjon med kollektiv bevissthet vil ha kapasitet til å forvente farer og hendelser før de slår inn, en bevissthet som kan brukes til å realisere barrierer for å redusere sårbarhet (Kjellén & Albrechtsen, 2017). Videre vil organisasjonen også være i stand til å svare raskt og effektivt etter at en uønsket hendelse har gjort seg gjeldende. I henhold til Weick m.fl. (1999) oppnås kollektiv bevissthet i en organisasjon gjennom fem kognitive prosesser; Preoccupation with failure (fokus på feil), reluctance to simplify interpretations (motvilje mot forenkling av tolkninger/forståelse), senstivity to operations (årvåkenhet/fokus på operasjoner), commitment to resilience (evne til resiliens) og underspecification of structures (desentralisering). Disse kognitive prosessene,

som blir utdypet i det følgende, ligger til grunn for pålitelighet i en organisasjon (Weick m.fl., 1999).

3.3.1 Fokus på feil

Et viktig ledd i alt sikkerhetsarbeid er å utnytte alle feil til å lære (Weick & Sutcliffe, 2007). Dette innebærer å følge med på svake feilsignaler som kan være tegn på større problemer innad i systemet (Weick & Sutcliffe, 2007). Systemer er ikke er trygge i utgangspunktet og sikkerhet må skapes med/av folk (Dekker, 2006). Å oppdage feil er én ting. Å rapportere eller kommunisere feil er en annen (Turner, 1978; Reason, 1997; Weick & Sutcliffe, 2007). I sin forskning på feilstyring beskriver Reason (1997) kommunikasjon som en «General Failure Type». Feil kan skje når nødvendige kommunikasjonskanaler ikke eksisterer, ikke fungerer eller ikke brukes regelmessig. Barry Turner argumenterer på samme måte i sitt informasjonsprosesseringsperspektiv hvor ulykker skjer som følge av mangelfull prosessering av informasjon (Turner, 1976). Reason peker på rapporteringskultur for å få til rapportering av uønskede hendelser, feil og nesten-ulykker (Reason, 1997). En organisasjon som er opptatt av feil vil bruke alle feil som grunnlag for læring (Weick m.fl., 1999), også avvik. Tinmannsvik beskriver avvik som «snarveier» i forhold til planlagt måte å jobbe på. På denne måten nærmer man seg grensen for sikker atferd (Tinmannsvik, 2008), man migrerer mot grensen for sikker drift (Rasmussen, 1997). Avvik kan skje ved formell fravikelse eller ved uformelle avvik (stille avvik) (Tinmannsvik, 2008). Uformelle avvik er gjerne noe man ikke snakker så mye om. Man utvikler en arbeidspraksis som avviker fra det som står beskrevet i prosedyrer (Tinmannsvik, 2008). Stille avvik er en uformell praksis som kan innebære at man opererer med et lavere sikkerhetsnivå enn det som er planlagt i systemet. Å synliggjøre avvik, og legge til rette for åpenhet rundt avvik, kan være effektivt for å utvikle en mer robust arbeidspraksis (Tinnmannsvik, 2008). En organisasjon som er opptatt av feil vil avsette mye ressurser til å kartlegge avvik og derigjennom få til en sikker arbeidspraksis.

3.3.2 Motvilje mot forenkling av tolkninger/forståelse

I alle organisasjoner gjøres det forenklinger for å løse komplekse problemer (Turner, 1978; Weick m.fl., 1999). Ved å gjøre forenklinger, øker imidlertid sannsynligheten for uønskede hendelser (Weick & Sutcliffe, 2007). Vi ser det våre fortolkninger tillater oss å se (Weick & Sutcliffe, 2007). Hvordan vi opplever verden vil avhenge av de erfaringer vi har og den

kunnskapen vi sitter med (Rollenhagen, 1997). Det kan argumenteres for at vi bruker ulike sett briller som tillater oss å se ulike aspekter ved ulykker (Rollenhagen, 1997). Forenklinger gjør at vi mister detaljfokus og det begrenser de ansattes evne til å se uønskede konsekvenser av det de foretar seg (Weick m.fl., 1999). Forenklinger kan dermed øke sannsynligheten for eventuelle uønskede hendelser ettersom ansatte ikke tenker selv og tilsidesetter intuisjon eller mageføelse. Dette kan tillate akkumulering av avvik og tap av verdifulle advarselstegn. Utfordringen vil her være å oppdage hvilke aspekter av en truende hendelse som kan ignoreres og hvilke som må tas hensyn til (Weick m.fl., 1999).

3.3.3 Årvåkenhet/ fokus på operasjoner

Årvåkenhet handler om å være tilstede, å kunne respondere på en uoversiktlig realitet som finnes i mange systemer (Weick & Sutcliffe, 2007). Normal drift vil avsløre svakheter og på den måten gi gratis læringsmuligheter. En slik tankegang muliggjør problemløsning på et overkommelig nivå før problemene eskalerer (Rosness m.fl., 2004). Årvåkenhet kan relateres til situasjonsforståelse (Endsley, Bolté og Jones, 2003). Situasjonsforståelse kan defineres som «the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future» (Endsley m.fl., 2003, s. 13). Det handler om å være oppmerksom på hva som skjer rundt en og forstå hva denne informasjonen betyr nå og i nær fremtid (Endsley m.fl., 2003). Kollektiv bevissthet går utover situasjonsforståelse på den måten at kollektiv bevissthet handler om det store bildet hvor vi inkluderer både eksisterende forventninger, kontinuerlig nyansering etter hvert som ny erfaring opparbeides, og et fokus på fremtiden (Weick & Sutcliffe, 2007).

3.3.4 Evne til resiliens

Resiliens kan defineres som evnen til å gjenkjenne, tilpasse seg og absorbere variasjon, endringer, forstyrrelser og overraskelser (Hollnagel m.fl., 2006). Resiliente organisasjoner søker ny kunnskap og har kontroll over ressurser som kan lindre, lette, moderere, redusere og/eller minske overraskelser (Weick & Sutcliffe, 2007). Det er beskrevet mange typer resiliens innenfor samfunnssikkerhet (Pettersen & Schulman, 2016). Bhamra m.fl. (2011) presenterer en tabell med definisjoner på resiliens fra ulike forskere som bruker begrepet i forskjellige kontekster. Stikkord som går igjen er evnen til å absorbere endring, tilpasningsdyktighet, evnen til å opprettholde funksjonalitet, begrense skade og motvirke

variasjon (Bhamra m.fl., 2011). I henhold til Weick og Sutcliffe involverer resiliens tre egenskaper (Weick & Sutcliffe, 2007):

Evnen til å absorbere belastning og bevare funksjonsevnen til tross for motgang; indre motgang (raske endringer, dårlig lederskap, ytelsespress, produksjonspress mm.) og ytre motgang (økt konkurranse, krav fra interessenter).

Evnen til å gjenopprette/ «bounce back» fra uheldige hendelser. Systemets evne til å absorbere og takle en overraskelse, fremfor å kollapse.

Evnen til å lære av, og dermed vokse på, erfaring fra tidligere. Mange systemer responderer på uroligheter med nye regler som skal forhindre at nettopp disse hendelsene skjer igjen. Det kan argumenteres for at en slik respons vil svekke systemets fleksibilitet (Reason, 1997). High Reliable Organizations (HRO's) responderer gjerne med læring og opparbeiding av ny erfaring, metoder som bevarer systemets fleksibilitet (Weick & Sutcliffe, 2007).

En resilient organisasjon vil ha fokus på mental øving, utvikling av responsferdigheter, samt læring fra tidligere hendelser (Weick & Sutcliffe, 2007). Det er avgjørende at de ansatte stiller spørsmål ved hva som skjer fremfor å late som om de forstår (Schulman, 1993). Dette leder oss til neste punkt, nemlig «deference to expertise» (Weick & Sutcliffe, 2007) eller «underspecification of structures» (Weick m.fl., 1999).

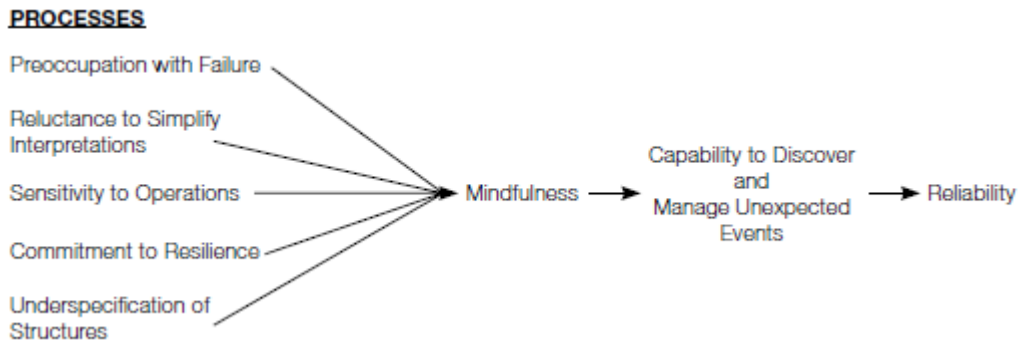
3.3.5 Desentralisering (deference to expertise)

Beslutningstaking basert på kunnskap og kompetanse fremfor hierarkisk plassering er en viktig egenskap i en HRO (Roberts m.fl., 1994). Ulik grad av desentralisering er beskrevet av mange forskere (Rochlin m.fl., 1987; LaPorte & Consolini, 1991; 't Hart, Rosenthal & Kouzmin, 1993; Dynes, 1994; LaPorte, 1994; Weick m.fl., 1999). Reason (1997) skriver om viktigheten av en fleksibel subkultur hvor beslutningstaking finner sted på mange nivåer i organisasjonen avhengig av situasjonen. Weick m.fl. (1999) beskriver desentralisering hvor de argumenterer for viktigheten av at de som forstår en situasjon best – håndterer situasjonen, uavhengig av hvor de befinner seg i det organisatoriske hierarkiet (Weick & Sutcliffe, 2007). Det handler om *ekspertise* fremfor *eksperter* (Weick & Sutcliffe, 2007). I noen tilfeller vil ekspertene ha mest ekspertise, men ikke alltid. Poenget med desentralisering er at arbeiderne som jobber «hands on», i den spisse enden, i en organisasjon gjerne kan ha en bedre forståelse for en gitt situasjon enn de som jobber høyere oppe i hierarkiet, i den butte enden. «…under

conditions of disaster, decentralization and even improvisation is a more applicable response [than bureaucratization and centralization of political authority]» (Britton, 1989, s. 9). Ledere i organisasjoner bør *spørre* fremfor å fortelle, *foreslå* fremfor å beordre og *delegere/desentralisere* fremfor å sentralisere når organisasjonen står overfor en uønsket hendelse (Dynes, 1974).

Som en oppsummering har vi sett at fokus på feil handler om å være opptatt av feil og lete eller avvik, for å benytte disse som læringsmuligheter. Motvilje mot forenkling av tolkninger handler om de forenklinger vi gjør i hverdagen og vår bevissthet om dette. Videre vil årvåkenhet/fokus på operasjoner peke på oppmerksomhet rundt aktiviteter og operasjoner. Resiliens omhandler absorbering av feil og endringer slik at disse ikke får anledning til å utvikle seg og bli større problemer. Desentralisering peker på sin side på utnyttelse av ekspertise og på det at ekspertise ikke trenger å henge sammen med hierarkisk posisjon.

En pålitelig («reliable») organisasjon anerkjenner at mennesket vil gjøre feil. Organisasjonen må derfor kompensere for disse feilene med utgangspunkt i de fem presenterte kognitive prosessene. Disse danner grunnlaget for kollektiv bevissthet, en bevissthet som gjør at pålitelige organisasjoner er i stand til å oppdage og håndtere uventede begivenheter, se figur 6 (Weick m.fl., 1999).



Figur 6 Kollektiv bevissthet som grunnlag for pålitelighet (Weick m.fl., 1999)

4. METODE

I dette kapitlet vil jeg beskrive og begrunne de metodiske valg jeg har tatt før og underveis i dette prosjektet. Jeg starter med beskrivelse av forskningsdesign og –strategi. Videre kommer en presentasjon av mine datakilder samt en diskusjon rundt validitet og reliabilitet i mine undersøkelser og data. Avslutningsvis vil jeg beskrive styrker og svakheter ved mine metodevalg.

4.1 Forskningsdesign og -strategi

Jeg har arbeidet eksplorativt i gjennomføringen av dette masterprosjektet. Et eksplorativt design er utforskende og passer godt til forskning hvor selve problemet er dårlig forstått og hvor det finnes lite teori om problemstillingen (Ghauri & Grønhaug, 2002). Min intensjon har vært å utforske og studere beskyttelse av sensitiv informasjon i kraftbransjen. Gjennom en eksplorativ tilnærming har jeg *utforsket* og formet prosjektet etter hvert som min forståelse av fenomenet har økt. Veien har på mange måter blitt til mens jeg har gått, noe som har gitt stadige endringer i problemstilling og forskningsspørsmål. Utformingen av problemstillingen har hos meg vært en kontinuerlig prosess. Thagaard (2009) beskriver utformingen av problemstillingen som noe av det vanskeligste og mest krevende ved hele forskningsprosessen. Dette kan jeg kjenne meg igjen i. Min forståelse for problemer knyttet til beskyttelse av sensitiv informasjon har utviklet seg, og opprinnelig(e) problemstilling(er) har blitt utdatert og oppdatert. Jeg startet for eksempel ut med beskyttelse av sensitiv informasjon mot intenderte angrep. Det viste seg imidlertid at tap av sensitiv informasjon også skjer som følge av ikke-intendert slurv på innsiden i selskaper. Tidligere problemstillinger tok ikke høyde for dette.

En forskningsstrategi er ment å gi en prosedyre for besvarelse av forskningsspørsmål (Blaikie, 2010). Til tross for at jeg valgte en eksplorativ tilnærming, så valgte jeg å basere intervjuguiden (vedlegg 4 og 5) på generell teori om intenderte angrep, risikostyring og risikopersepsjon. Selv om jeg ikke visste hva jeg ville finne, tenkte jeg at oppgaven overordnet ville peke i denne retningen. På bakgrunn av dette kan man si at mitt innledende arbeid i prosjektet bar preg av en deduktiv strategi. Det viste seg imidlertid at intervjuguiden ble en begrensning som gjorde det vanskelig å få tak den dybden jeg ønsket i intervjuene; både fordi noen av spørsmålene/temaene tydelig engasjerte intervjuobjektet mer enn andre, i

tillegg til at noen respondenter ble usikre av begreper som persepsjon eller risiko. Jeg innså dermed et behov for å justere spørsmålene basert på inntrykkene fra de første intervjuene. Intervjuene ble da i større grad samtalepreget hvor intervjuobjektene selv snakket ganske fritt innen noen forhåndsbestemte temaer. Dette ble viktig for å skape en intervjusituasjon hvor jeg opplevde å få tak i data som både mine respondenter og jeg opplevde relevant. Dette peker meg i retning av en åpen, induktiv forskningsstrategi, hvor man går «fra empiri til teori» (Jacobsen, 2005). En induktiv forskningsstrategi innebærer at man samler inn data før disse så relateres til forskningsspørsmål (Blaikie, 2010). Mine respondenter og data pekte meg i en annen retning enn først planlagt, og jeg har som forsker «fulgt etter». Med utgangspunkt i innsamlet empiri, har jeg plassert dataene inn i et revidert teoretisk rammeverk for å svare på spørsmål som kontinuerlig har vært i endring. Dette kan peke i retning av det Blaikie (2010) kaller abduksjon. Jeg opplever at mine intervjuobjekters uttalelser på denne måten har blitt ivaretatt, at jeg har tatt svarene deres på alvor. Jeg har hatt fokus på å løfte frem mine intervjuobjekters forståelser og ikke «presse» dataene inn i et forhåndsdefinert, teoretisk rammeverk som ikke oppleves relevant for mine intervjuobjekter. Dette ville heller ikke vært relevant for meg som forsker. En slik strategi har passet godt med mitt eksplorative design. Jeg har vært interessert i mine intervjuobjekters «innsideforståelse» for beskyttelse av sensitiv informasjon, noe som ble enklere da jeg valgte å la dem snakke ganske fritt. Jeg har på den måten tatt utgangspunkt i den sosiale verden som aktørene oppfatter (Blaikie, 2010). Jeg vil med denne bakgrunn argumentere for at min eksplorative tilnærming har ført meg fra en deduktiv strategi til en abduktiv strategi i denne oppgaven.

4.2 Datakilder

Helt enkelt kan man tenke seg at kvantitative undersøkelser gir tall, mens kvalitative undersøkelser gir ord (Blaikie, 2010). Jeg har gått for ord, altså kvalitativ undersøkelse. Mine data kommer fra intervjuer og dokumentstudier. Jacobsen (2005) skriver at han behandler dokumentundersøkelser som en kvalitativ metode. Mine intervjudata er *primærdata*, data som er innhentet av meg (Blaikie, 2010). Videre kan risikobilder, lover, forskrifter, rapporter, analyser mm. kategoriseres som *sekundærdata* eller *tertiærdata*, altså data som er innhentet og/eller analysert av andre (Blaikie, 2010). Gjennom dokumentstudier har jeg fått en forståelse av hvordan sensitiv informasjon skal og bør ivaretas i kraftbransjen. Videre har intervjudataene fortalt mer om hvordan sensitiv informasjon *faktisk* ivaretas i norske

nettselskaper og hvilke utfordringer de opplever. I tillegg har jeg selv besøkt selskapene. Jeg har her hatt muligheten til å oppleve hvordan selskapene tar i mot eksterne gjester, adgangskontrollsystemet, hvordan adgangsregistrering fungerer, hvor seriøse de er på å passe på gjester, med mer. Dette vil supplere mine intervjudata og dokumentstudier.

4.2.1 Intervjuer

Jeg har gjennomført til sammen 10 kvalitative intervjuer, se intervjuoversikt under (tabell 1). Kvale (2002, s. 17) skriver at «hvis du vil vite hvordan folk betrakter verden…, hvorfor ikke tale med dem?». Innen det kvalitative intervjuet er formålet å få en forståelse for intervjuobjektets verden (Kruuse, 1996; Jacobsen, 2005).

Respondenter

Jeg har vært i kontakt med Norges vassdrags- og energidirektorat (NVE) samt tre norske nettselskaper (A, B og C), se tabell 1. Disse selskapene er av ulik størrelse, med ulik oppbygning og ulikt antall ansatte. En respondent fra selskap B forklarer at «*det er et veldig stort spenn i norske kraftbedrifter; fra nesten enmannsforetak til Statnett som er mange tusen*».

Tabell 1 Intervjuobjekter

Informant/ Respondenter	**Stillingstittel**	**Relevant erfaring (fra bransjen)**
NVE	• Sjefsingeniør.	>20 år.
Selskap A	• IKT-sikkerhetskoordinator. • Avdelingsleder Kvalitet og HMS. • Prosjektingeniør for transformator-stasjoner.	>20 år. >20 år. >10 år.
Selskap B	• IT-sjef. • Avdelingsleder på driftskontroll. • Driftsingeniør.	>10 år. >20 år. >10 år.
Selskap C	• Avdelingsleder for sentral infrastruktur. • Fagsjef, informasjonssikkerhet. • Seniorrådgiver i informasjonssikkerhet.	>20 år. >20 år. <10 år.

I tabell 1 presenteres intervjuobjektene jeg har snakket med i selskapene. Høyre kolonne viser intervjuobjektenes relevante erfaring fra bransjen. Dette er ikke nødvendigvis antall år de har jobbet i den stillingen som beskrives, det kan være antall år de har arbeidet i kraftbransjen eller jobbet med informasjonssikkerhet og liknende. Her vil «>» bety «mer enn», mens «<» betyr «mindre enn». Samtlige intervjuobjekter har erfaring med informasjonssikring i bransjen. Jacobsen (2005) skriver at personer med direkte kjennskap til et fenomen som oftest kalles «respondenter». Jeg kaller dermed mine intervjuobjekter fra nettselskapene for respondenter. Disse jobber med sikring av informasjon til daglig, i større eller mindre grad. Hele bransjen forholder seg til taushetsplikt, som etter energiloven og beredskapsforskriften gjelder for enhver (energiloven, 1990; bfe, 2013). Videre er «informanter» personer med god kunnskap om det fenomenet som studeres (Jacobsen, 2005). Jeg velger dermed å omtale mitt intervjuobjekt fra NVE som informant. Videre er intervjuobjekter en samlebetegnelse for alle dem jeg har intervjuet (både respondenter og informant).

Ni av ti intervjuer ble gjennomført ansikt-til-ansikt. Jacobsen (2005) beskriver her et klima av fortrolighet, noe som kan være vanskelig over telefon eller Internett. Det siste intervjuet ble gjennomført over Skype. Grunnet tekniske problemer kunne intervjuobjektet se meg, men jeg fikk ikke opp bilde av ham/henne. Jeg mistet dermed muligheten til å observere hvordan intervjuobjektet opptrådte. Når man intervjuer noen ansikt-til-ansikt kan man enklere fornemme når man kan be om mer utdypende svar og når dette bør unngås. Jeg opplevde imidlertid ikke at mitt Skype-intervju føltes særlig annerledes enn de øvrige, og jeg ser ikke på intervjudataene fra dette intervjuet som noe dårligere enn resten.

I utvelgelsen av respondenter snakket jeg med én kontaktperson i hvert selskap. Jeg beskrev prosjektet, ønsket fremgangsmåte og et ønske om å intervjue noen med kunnskap om, og erfaring med, informasjonssikkerhet. Mine kontaktpersoner tok dermed kontakt med tre potensielle respondenter i sitt selskap. Mine respondenter ble derfor valgt ut på bakgrunn av forhåndsdefinerte kriterier og relevans (Neuman, 2000) fremfor representativitet, i en form for strategisk («purposive») utvelgelse (Neuman, 2000).

I de siste respondentintervjuene i nettselskapene opplevde jeg en form for metning i datainnsamlingen. Da de siste respondentene beskrev mange av de samme problemstillingene som de første, ble det vurdert at det ikke var hensiktsmessig eller nødvendig med flere intervjuer i nettselskapenes ledelse.

Samtlige intervjuobjekter har signert et samtykkeskjema (vedlegg 3) hvor deres underskrift slår fast at de opplysninger som kommer frem i intervjuet kan brukes i masteroppgaven. Alle intervjuer ble tatt opp på bånd og transkribert i etterkant. Videre har samtlige intervjuobjekter fått sitt transkriberte intervju på mail. Dette for å være sikker på at ingen feil eller misforståelser har forekommet.

Samtlige intervjuer var av semi-strukturert karakter og foregikk dermed på en uformell og samtalebasert måte mellom meg og intervjuobjektet. Semi-strukturert, eller halvstrukturert, tilnærming til intervjuet vil gi intervjuet en retning samtidig som det åpner for mulighet til å følge opp det som opptar intervjuobjektene (Thagaard, 2009). Dette ga meg mulighet til å justere spørsmålene mine etter hvert som intervjuene skred frem. Intervjuene ble dermed en form for læringsprosess for meg i denne eksplorative studien.

Blaikie skriver at intervjuer, uansett form, tar intervjuer og intervjuobjekt bort fra intervjuobjektets naturlige setting (Blaikie, 2010). Det var viktig for meg at flest mulig intervjuer fant sted hos nettselskapene for; å oppnå en mest mulig naturlig intervjusituasjon og dermed få best mulig innsikt i intervjuobjektets «verden», samt å med egne øyne få noen inntrykk av deres verden. I løpet av intervjuene føltes det også naturlig å la intervjuobjektene fortelle om det de opplever som vellykket eller vanskelig innen sikring av sensitiv informasjon, uten for mye styring fra min side. Jeg oppdaget raskt at intervjuguiden ble underordnet, og mange av intervjuene ble heller tema-basert fremfor spørsmålsfokusert. Jeg opplevde at denne intervjustrukturen fungerte veldig bra, både fordi det gav meg muligheten til å spinne videre på interessante utsagn som dukket opp underveis og fordi hele intervjusituasjonen ble mer avslappet. Det gav også en god mulighet for å få innsyn i hva mine intervjuobjekter opplevde å være reelle utfordringer med hensyn til sikring av sensitive data. Ulempen med denne strategien er at enkelte av intervjuene måtte bli nokså lange for at jeg skulle få de data jeg trengte. Lengden på intervjuene varierer fra 40 til 75 minutter. Ytterligere fordeler og ulemper ved dette vil diskuteres under «validitet og reliabilitet».

4.2.2 Dokumenter

Ved bruk av sekundærdata beskriver Jacobsen (2005) en utfordring knyttet til et misforhold mellom den informasjonen vi kan bruke, og det vi ønsker å bruke den til. Sekundærdataene er samlet inn med en annen hensikt enn min egen. Disse sekundærdataene er imidlertid, sammen med mine primærdata, valgt ut på bakgrunn av relevans for prosjektet. Dokumentene er

styrende for beredskap, informasjonssikring mm. i energisektoren. De er utarbeidet av myndigheter eller instanser som er underlagt myndighetene (Olje- og energidepartementet, Norges vassdrags- og energidirektorat), nasjonale ekspertorgan (Nasjonal sikkerhetsmyndighet) eller europeiske ekspertisesentre innen informasjonssikring (The European Union Agency for Network and Information Security). Det kan argumenteres for at dette er troverdige institusjoner (institusjoner med stor grad av kredibilitet) som ikke har egeninteresser som gjør dem tjent med informasjonsforvrengning. Det er å forvente at norske myndigheter ønsker god informasjonsbeskyttelse i norske selskaper og bedrifter. Med dette i bakhodet har jeg brukt følgende dokumenter:

Tabell 2 Dokumentoversikt

Dokument	**Organisasjon**	**Årstall**
Beredskapsforskriften (Bfe); Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen.	Olje- og energidepartementet (OED)	2013
Veiledning til forskrift om forebyggende sikkerhet og beredskap i energiforsyningen.	Norges vassdrags- og energidirektorat (NVE)	2013
Regulering av IKT-sikkerhet; Et helhetlig og fremtidsrettet sikkerhetsregime for forsyningssikkerhet i en digitalisert energisektor.	NVE	2017
NOU2006:6. Når sikkerheten er viktigst; Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner.	Departementenes sikkerhets- og serviceorganisasjon Informasjonsforvaltning	2006
NOU2015:13 Digital sårbarhet – sikkert samfunn.	Departementenes sikkerhets- og serviceorganisasjon Informasjonsforvaltning	2015
Nettfisking og sosial manipulasjon.	Norges sikkerhets-myndighet (NSM)	2012
Helhetlig IKT-risikobilde 2016.	NSM	2016
Risiko 2017; Risiko og sårbarheter i en ny tid. En vurdering av sårbarheter og risiko i Norge.	NSM	2017
ENISA Threat Landscape Report 2016: 15 Top Cyber-Threats and Trends.	The European Union Agency for Network and Information Security (ENISA)	2017

4.2.3 Observasjon

I forbindelse med dette prosjektet har jeg vært på besøk i kontorlokalene til tre norske nettselskaper, samt NVE. Jeg fikk dermed observere hvordan de tar imot gjester; registrering, besøkslapp, sperringer i inngangsparti, konstant/ ikke-konstant følge med en ansatt, bruk/ikke-bruk av nøytrale møterom med mer. Dette er viktige barrierer som supplerer mine intervju- og dokumentdata om selskapenes fysiske sikringstiltak og beskyttelse av sensitiv informasjon fra eksterne aktører. Det kan i denne sammenheng argumenteres for triagulering,

at vi kontrollerer data og funn ved kombinasjon av metoder, intervjuere og/eller kontekster (Jacobsen, 2005).

4.3 Validitet og reliabilitet

Reliabilitet handler om forskningsresultatenes troverdighet, mens validitet defineres som sannhet, riktighet og styrke (Kvale & Brinkmann, 2009).

4.3.1 Reliabilitet

Kvale skriver at reliabilitet ofte behandles i sammenheng med spørsmålet om hvorvidt et resultat kan reproduseres av andre forskere på et senere tidspunkt (Kvale & Brinkmann, 2009). Kan vi stole på dataene vi har samlet inn? (Jacobsen, 2005). En generell kritikk av kvalitative studier er at studiene vanskelig kan reproduseres som, for eksempel, et eksperiment i et laboratorium. Reproduksjon i kvalitativ forskning er i henhold til Kvale (1996) en illusjon. Det samme kan sies om mitt prosjekt. Det kan imidlertid argumenteres for andre måter å kontrollere reliabiliteten i prosjektet mitt. Man kan spørre seg om det finnes trekk ved undersøkelsen som har gitt oss de resultatene vi har fått. Jeg valgte å spille inn samtlige av mine intervjuer på lydopptak. Det kan argumenteres for at dette påvirker intervjuobjektenes svar. Jacobsen (2005) skiller mellom undersøkereffekt og kontekseffekt. Man får en undersøkereffekt når selve undersøkelsen har en effekt på det fenomenet som studeres (Jacobsen, 2005). Mine intervjuer har handlet om informasjonsbeskyttelse, og det er mulig at min undersøkelse som innebefattet lydopptak kan ha gjort intervjuobjektene mindre veltilpass, mer «up tight». Om dette var tilfellet eller ikke i mine intervjuer er vanskelig å si ettersom jeg ikke prøvde uten lydopptak. Jeg opplevde at noen av intervjuobjektene fremsto som veldig «politisk korrekte» og kontinuerlig henviste til definisjoner og dokumenter, mens andre i større grad svarte ut fra egne erfaringer og tanker. Jacobsen (2005) skriver at lydbånd vil være å foretrekke. Menneskelig hukommelse er ikke skapt for å lagre store mengder informasjon over tid. Innspilling av intervjuene har gjort det mulig for meg å kunne forsikre meg om at informasjonen er forstått og gjengitt så riktig som mulig.

En kontekseffekt vil på sin side handle om sammenhengen informasjonen samles inn i (Jacobsen, 2005). Alle mine intervjuer ble gjennomført i selskapenes egne kontorlokaler, noe som er en naturlig kontekst for mine intervjuobjekter. På den annen side foregikk sju av ti intervjuer på nøytrale møterom, ikke på intervjuobjektenes kontor eller arbeidspult. De tre

siste intervjuene foregikk dog på et kontor, men kontoret tilhørte ingen av mine intervjuobjekter. Videre var samtlige intervjuer avtalt god tid i forveien, så intervjuobjektene var forberedt på møtet. Ett selskap ville ha intervjuguiden før jeg kom, og én av respondentene i dette selskapet hadde svart skriftlig på flere av spørsmålene før vi startet intervjuet. Jacobsen (2005) beskriver planlagt/overraskende intervju som en dimensjon innen kontekseffekter. I min studie har intervjuene vært planlagte, og samtlige foregikk på formiddagen når både intervjuobjekter og intervjuer var opplagt.

I en diskusjon rundt reliabiliteten i mine semi-strukturerte intervjuer kan bruken av ledende spørsmål være sentralt. Jeg fokuserte bevisst på å unngå ledende spørsmål i mine intervjuer, men gjennom transkriberingen ser jeg at ledende spørsmål har forekommet. Dette faller veldig naturlig når man opererer med en samtalebasert intervjuform. Jeg vil imidlertid argumentere for at ledende spørsmål ikke utelukkende er negativt. I de fleste tilfeller hvor mine spørsmål var av ledende karakter var det for å få bekreftet noe jeg var usikker på eller for å slå fast at jeg hadde skjønt det intervjuobjektet sa. Kvale og Brinkmann (2009) skriver at ledende spørsmål på denne måten ikke alltid reduserer intervjuenes reliabilitet, men at det snarere kan styrke den.

Reliabilitet omhandler målenøyaktighet og er viktig for presisjon, objektivitet og dermed påliteligheten i undersøkelsene (Kruuse, 1996). Innen kvalitativ metode kan det stilles spørsmål ved objektiviteten. Vil det for eksempel være mulig med fullstendig objektivitet i en intervjusituasjon? Det kan imidlertid argumenteres for at dette er vanskelig i kvalitative studier da det er vanskelig for en forsker å opptre på samme vis flere ganger selv om studien er lik. Under dataanalyse vil det i tillegg alltid være et element av skjønn (Jacobsen, 2005).

Jeg har hatt et fokus på bevissthet i denne oppgaven, bevissthet i mtp. trusler og barrierer. Mine funn samsvarer med funn hos Hagen m.fl. (2008); at tiltak innen bevissthet er sentralt innen informasjonssikkerhet og at bevissthetsstyrkende tiltak ikke alltid prioriteres så høyt som de burde. At flere uavhengige forskere har kommet frem til sammenfallende funn er å anse som en styrke for en undersøkelses reliabilitet. Jacobsen (2005) argumenterer for en gyldighetstest som går ut på å sjekke egne funn mot andre. Sammenfallende eller likelydende funn kan styrke gyldigheten i resultatene (Jacobsen, 2005).

4.3.2 Validitet

Validitet dreier seg om hvorvidt en metode egner seg til å undersøke det som skal undersøkes (Kvale & Brinkmann, 2009). Validitet deles gjerne inn i intern gyldighet og ekstern gyldighet (Jacobsen, 2005).

Intern gyldighet går ut på om resultatene kan oppfattes som riktige, eller intersubjektive (Jacobsen, 2005). Jacobsen (2005) argumenterer for bruk av begrepet *intersubjektiv* fremfor *riktig* – for hva kan egentlig anses som sannhet? Samtlige av mine intervjuobjekter mottok sitt intervju i transkribert form i etterkant av intervjuprosessen. Dette for å forsikre at ingen feil eller misforståelser hadde oppstått i transkriberingsprosessen. Her fikk intervjuobjektene også mulighet til å tilføye eller kommentere hvis noe var mangelfullt eller uklart. Kun én respondent svarte med ønskede endringer som så ble tatt til etterretning. En slik runde styrker undersøkelsens interne validitet fordi sannsynligheten øker for at intervjuobjektene vil kjenne seg igjen i beskrivelsene mine.

Kvale og Brinkmann (2009) beskriver metoder for å kryssjekke validitet. Dette for å styrke gyldigheten i egne data (Jacobsen, 2005). I mitt forskningsarbeid var det også interessant å observere hvordan mine intervjuobjekter tok i mot meg som gjest i deres kontorbygg. Dette er sentralt i en sammenlikning med intervjuobjektenes beskrivelse av beskyttelse av informasjon fra eksterne personer. Kombinasjonen av observasjon og intervju kan anses som en form for kryssjekk. Når de respondentene som hadde avvik innen innsidesikring faktisk lot meg sitte alene på et fullt utstyrt kontor – kan dette være en styrking av gyldigheten i mine data om mangelfull innsidesikring. Hvis dette i tillegg beskrives som et kjent avvik i offentlig rapporter og risikobilder har jeg en slags «trippel styrking» av den påstanden jeg fronter.

Innen validitet kan man videre spørre seg om man har fått tak i de riktige kildene (Jacobsen, 2005). Samtlige av mine intervjuobjekter møter problemstillinger knyttet til informasjonssikring mer eller mindre hver dag. Ettersom jeg skriver om nettselskapers beskyttelse av sensitiv informasjon kan det tenkes at intervjuer med noen «ute på stasjonene/ sentralene» kunne vært interessant. Figur 2 i starten av oppgaven viser at det finnes en link mellom det administrative systemet og SCADA-systemene. Trusselaktører som har forberedt et angrep godt vil dermed kunne utnytte ansatte i hele nettselskapet for å få tak i nødvendig informasjon som for eksempel kan bidra til strømstans. Jeg vil ikke argumentere for feil valg

av intervjuobjekter i denne oppgaven, men det kan tenkes at inkludering av andre intervjuobjekters svar kunne gitt et mer utfyllende bilde.

Ekstern validitet handler om overførbarhet fra en organisasjon eller kontekst til en annen. Et naturlig spørsmål i denne sammenheng er om mine funn er overførbare til andre settinger (Jacobsen, 2005). Er de resultatene jeg har funnet i mine tre nettselskaper overførbare til andre norske nettselskaper? Dette betegnes av Jacobsen (2005) som generalisering fra utvalg til populasjon. Resultater som bygger på 3 nettselskaper (av over 150) kan ikke regnes som representative for norske nettselskaper. Likevel ser jeg at flere synspunkter går igjen hos flere av intervjuobjektene fra de ulike nettselskapene, og det *kan peke i retning* av et generelt trekk hos selskapene. De beskriver for eksempel mange av de samme truslene. Det er nærliggende å tenke at disse truslene også er gjeldende for andre nettselskaper. Nettselskapene i denne studien forholder seg også til de samme myndighetskravene; som er gjeldende for alle norske nettselskaper. Når det gjelder spesifikke utfordringer i hvert enkelt selskap med sikring av sensitiv informasjon er det trolig vanskeligere å se direkte overføringsverdi. Respondenter fra samtlige nettselskaper i denne studien har imidlertid pekt på svakheter ved ROS-analyser som metode; samt manglende oppfølging av de tiltak som kommer ut av slike analyser. Dette kan resultere i manglende etablering av barrierer for eksempel innen beskyttelse av sensitiv informasjon. Et større forskningsprosjekt vil kunne se på dette (se «videre forskning» i siste del av konklusjonskapitlet).

4.4 Etiske betraktninger

Både energiloven og beredskapsforskriften beskriver sensitiv informasjon og hvordan denne skal behandles av aktørene i kraftbransjen. Som intervjuer har jeg unngått å stille spørsmål som ville kunne gitt svar av sensitiv karakter. Dette ble klarlagt med intervjuobjektene i forkant av intervjuene. Et samtykkeskjema ble signert av begge parter (vedlegg 2). Samtykkeskjemaet slår fast at jeg skal kunne bruke de data som fremkommer i intervjuene såfremt jeg ikke nevner navn på intervjuobjekter og selskaper. Det var et ønske fra respondenter og selskaper om anonymisering. Dette gjelder for alle nettselskaper som inngår i denne studien. I NVE er kun navnet på informanten anonymisert. Informanten fra NVE har godkjent publisering av navn på NVE som offentlig tilsynsmyndighet. Som et videre ledd i anonymiseringen vil jeg omtale alle intervjuobjekter som «han»/ «ham» i denne oppgaven.

Innen nettselskapene refererer jeg til uttalelser og sitater fra respondentene i selskap A, B og C. Jeg nevner stillingstitlene til de ulike respondentene i tabell 1. Jeg har imidlertid valgt ikke å nummerere respondentene (respondent 1, respondent 2, osv.). Tanken bak dette er at aktører i selskapene selv kanskje forstår hvilke respondenter jeg har snakket med ut fra de stillingstitlene som presenteres i tabell 1. Ved ikke å nummerere respondentene vil det ikke være mulig å følge uttalelser fra én bestemt person gjennom hele oppgaven. På den annen side kan det argumenteres for en svakhet innen gyldighet at leser ikke får vite *hvem* (stilling, ansiennitet) som kommer med de ulike utsagnene. Jeg sto her overfor en etisk problemstilling, og droppet nummerering av respondenter som en ekstra barriere innen anonymisering. Jeg holder på denne måten mitt løfte om anonymisering overfor respondentene.

Å betegne selskapene som A, B og C har vært viktig for at intervjudataene skal kunne publiseres offentlig i en masteroppgave. Spørsmål som «hvor er dere mest sårbare?» og svar som «vi er dårlige på inngangskontroll» bør, naturlig nok, ikke kombineres med navn på selskap. Noen steder har jeg unngått fullstendig å oppgi om de diskuterte forholdene kommer fra selskap A, B eller C. Det var gunstig for meg å sende transkribert intervjumateriale til samtlige intervjuobjekter i etterkant av intervjuene. På denne måten kunne de sjekke at ingen av opplysningene var sensitive, samt få mulighet til å peke på opplysninger som kan lede direkte til deres selskap. Dette var gunstig for å få sikret at jeg ikke utleverer sensitiv informasjon, samtidig som jeg fikk sjekket at jeg hadde forstått intervjuene riktig. Én respondent svarte med kommentarer på forhold som vedkommende ikke ønsket inkludert i oppgaven.

Alle intervjuer ble spilt inn på lydopptak. Lydopptakene er kun hørt av meg og vil bli slettet umiddelbart etter at sensur har falt.

4.5 Styrker og svakheter ved valgt metode

En styrke i dette prosjektet er den velvilje og interesse jeg har møtt i kraftbransjen. Det virker å være stor interesse for sikkerhet og forskning på sikkerhet blant mine intervjuobjekter. Det var derfor ikke vanskelig å få innpass i aktuelle nettselskaper og i NVE. Jeg har snakket med ni intervjuobjekter i tre nettselskaper, hvor de fleste har en lederstilling, samt en sjefsingeniør fra NVE. På dette grunnlag kan jeg selvsagt ikke generalisere mine funn til hele energibransjen; hverken til andre nettselskaper eller til alle deler av nettselskaper som inngår i

denne studien. Selv om det kan ses på som en svakhet at det kun er gjennomført ni intervjuer av respondenter i nettselskapers ledelse, opplevde jeg en form for metning i datainnsamlingen. De siste respondentene jeg intervjuet beskrev mange av de samme problemstillingene som de første. Det ble således vurdert at det ikke var hensiktsmessig med flere intervjuer ved hovedkontorene til nettselskapene. Dette fordi ytterligere intervjuer av ansatte på hovedkontorene mest trolig ville styrket allerede innsamlet data. Det kan imidlertid tenkes at intervjuer med aktører i den spisse enden, de som arbeider ute på kraftanleggene, kunne gjort oppgaven mer nyansert. Ved også å inkludere ansatte i den spisse enden måtte jeg trolig ha begrenset antall selskaper. Med denne bakgrunn, og en opplevelse av at dataene som er samlet inn belyser problemstillingen på en god måte, har jeg vurdert utvalget som godt nok.

Det har også vært enkelt å få tak i relevante dokumenter som supplerer mine intervjudata. Det kan anses som en styrke i dette prosjektet at det finnes mange direktiver og instrukser som presenterer forventninger til nettselskapenes risikovurderinger og implementering av sårbarhetsreduserende barrierer.

5. EMPIRI

I dette kapitlet vil jeg presentere et samspill av empiri fra intervjuer, dokumentstudier og egne observasjoner. En respondent i selskap C beskriver et fokus på risikotrekanten (se innledning til teorikapitlet)[10] hvor risikovurderinger gjøres på bakgrunn av verdi-, trussel- og sårbarhetsvurderinger. Denne inndelingen ligger til grunn for de tre underkapitlene som til sammen utgjør empirikapitlet. Jeg starter med en kort redegjørelse av sensitiv informasjon som verdi og hvorfor denne tiltrekker seg trusselaktører (5.1). Videre kommer en gjennomgang av sentrale trusselaktører (5.2) som ønsker å utnytte sårbarheter innen informasjonsbeskyttelse i nettselskapene. Neste underkapittel omhandler tiltak som selskapene iverksetter for å begrense de sårbarhetene som kan eksponere sensitiv informasjon (5.3). Alle sitater som er direkte hentet fra transkriberte intervjuet står i kursiv.

5.1 Sensitiv informasjon som verdi

Hva er sensitiv informasjon og hvorfor er denne ettertraktet av trusselaktører? En respondent i selskap B beskriver sensitiv informasjon som;

> «*…forskjellig type informasjon. En ting er sensitiv informasjon som er knyttet opp mot den fysiske infrastrukturen, kraftsystemet. Det andre er hvordan vi styrer/overvåker kraftsystemet. Det tredje er egentlig forretningsmessig informasjon; om selskapet og anskaffelser og den type ting...*».

Dette underbygges av beredskapsforskriften 2013 som sier at sensitiv informasjon er all informasjon som kan brukes til å skade energiforsyningen (bfe, 2013). Detaljer rundt sensitiv informasjon er beskrevet i underkapittel 2.5. Informasjon knyttet opp mot kraftsystemet kan være ettertraktet av aktører som vil sabotere norsk kraftforsyning. Kraftforsyningen er å anse som en kritisk samfunnsfunksjon (DSB, 2016), og sabotering av kraftforsyningen kan anses som en grov kriminell handling eller terror.

I en rapport fra NVE kommer det frem at statlige aktører utgjør en stadig større trussel (Hagen, 2015); Etterretningsvirksomhet for å innhente informasjon om kritisk infrastruktur skjer kontinuerlig. Informasjon om kritisk infrastruktur kan brukes i et våpenkappløp hvor

[10] Denne samsvarer med det Engen m.fl. (2016) kaller «trefaktormodellen».

stater jobber for å utvikle skadevare som kan brukes til å skade eller forstyrre kritiske samfunnsfunksjoner (Hagen, 2015).

I tillegg trekker respondenten fra selskap B frem forretningsmessig informasjon. Min informant fra NVE nevner beskyttelse av forretningshemmeligheter; informasjon om hvordan norske nettselskaper opererer. En annen respondent i selskap B beskriver konkurranser og beskyttelse av hemmeligheter også innad i kraftbransjen; «*…man vet jo også at i store anbudskonkurranser så er det konkurrerende parter som har prøvd å få tak i informasjon om konkurrenter og tilbud, så det pågår jo*». En tredje respondent i samme selskap forklarer at selskapet er i konkurranse med andre nettselskaper og at all informasjon som kan brukes i denne konkurransen er sensitiv for dem. De selskapene som leverer den billigste strømmen får en økonomisk fordel, noe som skaper en form for konkurranse mellom selskapene. Respondenten påpeker her et skille mellom informasjon som er sensitiv ifølge beredskapsforskriften og informasjon som er bedriftssensitiv som følge av konkurranse mellom selskapene. Respondenten understreker at selskapene ikke konkurrerer på informasjonssikkerhet og IKT-sikkerhet, da dette er områder hvor de ikke kan renonsere på sikkerheten.

Som et siste punkt kan sensitiv informasjon være verdifull for aktører som ønsker økonomisk gevinst. Disse er kanskje ikke interessert i selve informasjonen, men de kan utnytte kraftbransjens verdsettelse av informasjonen. Respondenter fra samtlige nettselskapene som inngår i denne studien beskriver angrep som krypterer («låser») informasjon. Her vil angriper kreve betaling for å dekryptere («låse opp») informasjonen.

Det er ulike betydninger av hva sensitiv informasjon er, og de ulike betydningene er tett koblet mot trusselaktører og deres agenda.

5.2 Trusler og angrep som utfordrer beskyttelse av sensitiv informasjon

Trusselaktører stiller med forskjellig motivasjon, ressurstilgang samt grad av kunnskap og organisering. Jeg vil se på dem som jobber for å få tak i informasjon (1) digitalt, gjennom cyberspace, samt dem som opererer som innbruddstyver og vil ha informasjon i (2) fysisk/analog form.

Min informant fra NVE forteller at digitalisering skaper avhengighet. Sluttrapporten etter BAS3 peker på at vår digitaliserte virkelighet gjør at sentrale funksjoner i samfunnet enkelt

kan lammes, uten at landegrensene våre fysisk krenkes (Fridheim m.fl., 2001). Flere respondenter peker umiddelbart på digitale trusselaktører når informasjonssikring diskuteres. En respondent fra selskap B forteller at trusselaktører kan få tak i mye informasjon hvis de går den digitale veien. En oversikt over det digitale trussellandskapet i Europa i 2016 presenteres i vedlegg 2 (ENISA, 2017a). Trussellandskapet er utarbeidet av The European Union Agency for Network and Information Security, et europeisk ekspertisesenter for cyber-sikkerhet (ENISA, 2017b). Samtlige av respondentene i nettselskapene beskriver kontinuerlige digitale angrep fra ondsinnede utsidere (aktører på utsiden av selskapet). Mørketallsundersøkelsen 2016 fastslår at e-postangrep forekommer stadig oftere (NSR, 2016). Fortløpende phishing-angrep beskrives av respondenter i samtlige nettselskaper; «*…Senest i dag var det en kollega som viste meg det. Det skjer hele tiden*» (respondent fra selskap B). Phishing[11] er en form for e-postangrep hvor en hacker sender mail til utvalgte IKT-brukere (NSM, 2016a). Hensikten kan være å få tilgang til ulike typer informasjon, for eksempel personlig informasjon, informasjon om arbeidsgiver, informasjon fra datamaskinen til den som åpner mailen eller informasjon fra datanettverket man er koplet opp til (NSM, 2012). Denne informasjonen kan så brukes til sabotasje eller svindel på et senere tidspunkt (NSM, 2016a), for eksempel til direktør-phishing[12]. Direktør-phishing er en form for svindel hvor en trusselaktør har kartlagt økonomisjefer eller andre ansatte med ansvar på forhånd (NSM, 2016a). En respondent i ett av nettselskapene beskriver for eksempel et nylig tilfelle av direktør-phishing hvor lederen i selskapet fikk en e-post som så ut som den kom fra økonomidirektøren med krav om hjelp til å overføre penger til en konto. Svindelforsøket ble oppdaget og pengene ble ikke overført i dette tilfellet. NSM har imidlertid tall som viser at mange norske virksomheter har betalt store summer til utlandet som følge av direktør-phishing (NSM, 2016a). I selskap C forklarer en respondent at det kan være vanskelig å oppdage disse angrepene når en mail er skreddersydd til en person; «*…de har gjort research; kanskje på hvor jeg skal på ferie eller kanskje jeg skulle delta på en konferanse, ikke sant. De vet… Jeg kjenner igjen informasjonen. Kanskje det kommer fra en jeg kjenner i tillegg*». Dette er en form for sosial manipulasjon som har vist seg å være effektiv.

Videre beskrives løsepengevirus som et intendert angrep hvor en ondsinnet programvare låser og krypterer filene på en datamaskin (NSM, 2017b). Her mister medarbeidere tilgang til

[11] «Fisking» på norsk: Kriminelle aktører agn og krok for å få tilgang til ulik informasjon.
[12] CEO-svindel/ toppsjefsvindel/ «whaling»/ en form for spear-phishing.

dokumentene sine og får et krav om å betale løsepenger innen en tidsfrist for å få kontroll over egne filer igjen (Brekke, 2016). Løsepengevirus vil ofte ikke stjele den låste informasjonen, kun låse den og dermed gjøre den utilgjengelig for selskapet. Det finnes imidlertid noen former for løsepengevirus, såkalte «ransomware-parasitter», som både kan skru av antivirus-programmer og stjele brukerens sensitive informasjon. I tillegg kan løsepengevirus benyttes av avanserte aktører som avledningsmanøver eller sabotasje (NSM, 2017b). Respondenter fra samtlige av mine selskaper har kjennskap til, og erfaring med, løsepengevirus. En respondent fra selskap B eksemplifiserer med «CryptoLocker», et løsepengevirus som krypterer (låser) filer og tilbyr dekrypteringsnøkkelen mot betaling: «*…ute i kontornett er det CryptoLocker og alle mulige andre virus som malware og inntrengningsforsøk daglig*» (respondent, selskap B). I selskap A beskriver en respondent CryptoLockers slik:

> «*Vi har hatt det hele tiden. Det er mer til irritasjon. Vi må… brukerne får noen timer. De må vente på at filene restore, få back-up. Det er ikke verre enn det. Noen har kanskje mistet noen filer*».

Selskapene jobber med back-up, og CryptoLockers fremstår ikke som en stor trussel for eksponering av sensitiv informasjon. Under løsepengevirus nevnes kun CryptoLocker av mine respondenter. Ingen av mine respondenter har nevnt ransomware-parasitter som stjeler sensitiv informasjon.

Variasjonen er stor i ressurstilgang, metode og motivasjon hos digitale trusselaktører. Mindre teknisk avanserte angripere, såkalte «script kiddies» eller sosiale hackere, bruker gjerne allerede eksisterende hackerverktøy eller sosial manipulasjon. Sosial manipulering handler om å få tak i informasjon ved å lure noen. Script kiddies er individuelle, ikke-profesjonelle hackere som kanskje har anerkjennelse i hackermiljøet som mål med sin aktivitet. En respondent i selskap C forklarer at; «*…Før var det veldig fokus på disse 'script kiddies'… Det bare håndterer du. Hvis du feiler på DET, da har du driti deg ut, liksom… Det lyser rødt lang vei»*. Script kiddies beskrives ikke som en alvorlig trussel i nettselskapene, men det er verre med «*…de som banker på døra en gang i måneden…»* (samme respondent, selskap C). Respondenten peker her på de som jobber i det skjulte, de mer sofistikerte angriperne. NOU2015:13 beskriver «sofistikerte angripere» som statlige grupper eller andre som ønsker informasjon av politiske/militære grunner (NOU2015:13, 2015). Sofistikerte angripere kan gjerne styre avanserte vedvarende trusler (AVT), eller advanced persistent threats (APT);

målrettede angrep for å etablere bakdører, spre skadevare og hente skjermingsverdig informasjon (NSM, 2016a). Sofistikerte angripere er ofte ressurssterke trusselaktører som bruker tid på systematisk hacking over tid, gjerne fokusert på ett mål. Sofistikerte angripere kan være oppdaterte på hva som foreligger av sikringstiltak og sårbarheter i selskaper. De kan videre ha med seg et omfattende nettverk av profesjonelle hackere, og ofte kan en sofistikert angriper være vesentlig flinkere til å finne sårbarheter i programvare enn selskapenes analytikere (som jobber med etablering av sikringstiltak). NSM skriver at «angriperne utvikler sine teknikker raskere enn utviklingen av mottiltak. Dette er i praksis et våpenkappløp og vi forventer at slike angrep vil øke fremover» (NSM, 2015b, s. 17). I selskap B forklarer en respondent at avanserte, målrettede angrep direkte rettet mot deres selskap sikkert vil forekomme, og at risikoen for dette avhenger av den politiske situasjonen.

En respondent fra selskap A forklarer at ressurssterke aktører som klarer å bryte seg inn og overta SCADA-systemer kan, for eksempel, overta styring av flyplasser eller av rakettsystemet i Forsvaret. Disse SCADA-systemene er ganske like SCADA-systemene i kraftbransjen. Respondenten forklarer at det finnes aktører som har brukt betydelige midler for å hacke SCADA-systemer i forsvarssammenheng, og at disse har vært farlig nær. Det skal videre lite til for å anvende de samme metodene på andre SCADA-system; for eksempel trafikksystem eller infrastruktur innen kraftbransjen. Respondenten er klar på at det her er snakk om stater som kan være interessert i å ta ut både forsvarssystemer og infrastruktursystemer. I forbindelse med ønske om å ta ut sentrale systemer i Norge er fremmede stater søkende etter statshemmeligheter og sensitiv informasjon (spesielt innen romfart, forsvars-, olje- og energisektoren) (NSM, 2016a). Dette vil kunne brukes politisk, økonomisk eller militært (etterretningstjenesten, 2016). Digitale etterretningsoperasjoner mot Norge fremstår som teknisk avanserte og målrettede, og det vil være sentralt for norsk etterretningstjeneste å følge statlige, eller statlig sponsede, trusselaktører (etterretningstjenesten, 2016).

Mellom script kiddies og sofistikerte angripere finnes hacktivister som ønsker å fremme politiske budskap, cyberterrorister som er ideologisk motiverte grupper med ønske om å ramme samfunnsfunksjoner med vold, eller aktører som utnytter tekniske sårbarheter for å oppnå tilgang til utstyr. Videre har man «Crime as a service», et globalt marked for kjøp/salg av tjenester for å understøtte IKT-kriminalitet (NOU2015:13, 2015).

I tillegg til eksterne aktører peker en respondent fra selskap B på interne trusler; «*Først og fremst interne trusler; misfornøyde ansatte, folk som er på vei ut, konsulenter*[13]». I sin beskrivelse av ansatte som en trussel nevner respondenten blant annet ansatte som handler uforvarende og ubevisst, samt ansatte som presses fra utsiden. Disse kan kategoriseres som innsidere, personer med tilgang til interne systemer og informasjon; både ansatte og konsulenter (NSM, 2016a). Den amerikanske programvareprodusenten Veriato har gjennomført en undersøkelse[14] for å forstå innsidetrusler og dermed finne løsninger som kan hindre dem. Intendert datalekkasje gjennomført av privilegerte innsidere med tilgang til sensitiv informasjon, beskrives som en av de verste innsidetruslene (Veriato, 2016). Denne typen innsidere kan omtales som utro tjenere (beskrives av respondenter fra selskap A og C). 3 av 10 norske virksomheter har avdekket utro tjenere blant egne ansatte[15] (NSR, 2015). Ifølge undersøkelsen til Veriato er imidlertid ikke-intendert datalekkasje den innsidetrusselen selskaper er mest redd for (Veriato, 2016). Mennesket er gjerne «det svakeste leddet» (NOU2015:13, 2015), og innsideres uaktsomhet og feilslutninger kan kompromittere informasjon eller virksomhet (NSM, 2016a). Slurv er en form for innsidetrussel som kan skape smutthull som i neste omgang kan utnyttes av ondsinnede utsidere til digitale eller fysiske angrep. I tillegg har økt sammenkobling på tvers av sektorer og kobling til Internett økt skadepotensialet ved slurv (NOU2015:13, 2015).

Truslene og angrepene avhenger av trusselaktørenes hensikter; Phishing-angrep, overvåking og tyveri av sensitiv informasjon fra sofistikerte angripere, sosial manipulasjon, ransomware-parasitter eller ugunstig aktivitet, både intendert og ikke-intendert, fra utro tjenere kan gjennomføres for spesifikt å få tilgang til sensitiv informasjon. Dette kan benyttes i en planleggingsprosess hvor fremtidig sabotasje, svindel, overtakelse/styring av kraftforsyningen eller politisk spill er målet. På den annen side vil som oftest løsepengevirus (CryptoLockers), script kiddies, direkte sabotører eller cyberterrorister i større grad ha direkte økonomisk vinning, status eller skade som formål og det kan tenkes at disse ikke har et ønske om å sanke informasjon i forkant. Det er her et spørsmål om indirekte eller direkte skade forårsaket av

[13] Rådgivere i konsulentbyråer som tilbyr sin kunnskap i en begrenset periode.
[14] Publikumbasert forskning i samarbeid med 300.000 medlemmer i et informasjonssikkerhetsfellesskap på LinkedIn og Crowd Research Partners (Veriato, 2016).
[15] KRISINO-undersøkelse (Kriminalitets- og sikkerhetsundersøkelsen i Norge), 2015. Undersøkelsen bygger på et utvalg ledere og sikkerhetsansvarlige i 2000 private virksomheter og 500 offentlige virksomheter (NSR, 2015).

innsidere og digitale trusselaktører. Hva så med fysiske trusler mot informasjon lagret i fysisk form i nettselskapene?

Innen «fysisk» informasjon skiller jeg her mellom analog og digital informasjon. Analog informasjon lagres i papirform (utskrevne papirer; bøker, bilder, kart, tegninger), mens digital informasjon er lagret på et fysisk medium som for eksempel eksterne minnepinner eller harddisker. Denne formen for informasjonslagring skiller seg fra skylagring i den forstand at informasjonen er fullstendig adskilt fra Internett eller andre plattformer som gjør informasjonen tilgjengelig for andre enn dem som er fysisk i nærheten av enhetene/papirene. Skylagring diskuteres ikke i detalj i denne oppgaven ettersom skylagringstjenester ikke er å foretrekke av sikkerhetshensyn når det er snakk om sensitiv informasjon. Se ellers argumentasjon rundt avgrensning i forhold til skylagring i innledningen, samt i vedlegg 1.

Analog informasjon kan utsettes for skade, ødeleggelse, tyveri (ENISA, 2017a). Papirkopier, kartutskrifter, eksterne lagringsenheter eller liknende kan fysisk skades/ødelegges eller stjeles. Mistet eller stjålet utstyr (laptoper og minnepinner) står for rundt 40 % av bekreftede datatap (ENISA, 2017a). En respondent i selskap B peker på leverandører som mottar nødvendig informasjon på Ipader. Dette gir dem tilgang til nettet; «*…og det er jo sensitiv informasjon som ligger der. Hva skjer når de slutter?...Hva om de mister ipaden?*». Denne trusselen får ikke tilstrekkelig oppmerksomhet av sluttbrukere og organisasjoner. ENISA (2017a) har publisert en rapport som slår fast at det finnes en manglende forståelse mellom realitet og bekymringsnivå: Sikkerhetseksperter klassifiserer alvorlighetsgraden av utstyrstap for lavere enn hva som er nødvendig (ENISA, 2017a). I tillegg kan man lese at ansatte mister utstyr hundre ganger oftere enn ved tyveri (ENISA, 2017a).

Innsidere, både utro tjenere og uaktsomme ansatte, kan indirekte bidra til å skade virksomheten ved intendert eller ikke-intendert å lekke sensitiv informasjon i analog form. Informasjonen kan brukes av dem selv (utro tjenere) eller av andre (uaktsomme ansatte) i en større skadeprosess hvor målet kan være sabotasje, svindel, overtakelse/styring av kraftforsyningen eller politisk spill.

5.3 Tiltak

Digitale sårbarheter skaper et kappløp mellom trusselaktører og beskyttere (NOU2015:13, 2015; NSM, 2015b; ENISA, 2017a). Trusselaktøren vil hele tiden tenke nytt og finne ukjente

metoder for å bryte gjennom de sikringsmekanismer som beskytteren har satt opp. Samtidig vil beskytteren alltid ønske å være i forkant. Beskytteren må derfor kontinuerlig være oppdatert på det trusselbildet som foreligger og bygge opp sikringstiltak deretter. Jeg vil nå presentere noen fysiske, tekniske og organisatoriske tiltak for å sikre sensitiv informasjon. I tillegg beskrives bransjesamarbeid (som inkluderer fokus på både fysiske, tekniske og organisatoriske forhold).

5.3.1 Fysiske sikringstiltak

Som gjest, eller observatør, kan jeg si at samtlige av de nettselskaper jeg har besøkt har adgangskontroll i form av vektere og fysiske sperringer (gjerde og registrering av adgangskort) i resepsjonen. Videre har alle selskapene områder med begrenset adgang, og alle besøkende skal ha en lapp på brystet som forteller hvem de er, og hvem de besøker. Ett av selskapene i denne studien opererer med ulike fargekoder på adgangs-/besøkskort. Kortet skal til enhver tid være synlig, og fargene forteller hvor i bygget man har adgang.

For å forhindre «one point of failure»[16] (respondent i selskap B) skal det foreligge sikkerhetskopier av dokumenter og programvare fjernlagret på et sikkert sted (bfe, 2013). Dette er viktig for å hindre at samme hendelse kan medføre at både original versjoner og sikkerhetskopi blir utilgjengelig (NVE, 2013, s. 147). En respondent i selskap C forklarer at mye sensitiv informasjon i papirform foreligger ute på sentralene, og at sentralene låses. Videre er det vanlig å låse dokumenter inn i safe. I selskap B beskriver en respondent låste arkiver med analog informasjon hvor arkivenes lokasjon er hemmelig. Respondenten forteller imidlertid at alle som jobber eller har jobbet i selskapet vet om plasseringen. I tillegg mener han at det er lett for gjester å plukke opp slike opplysninger hvis man beveger seg «i gangene» på deres arbeidsplass.

5.3.2 Tekniske sikringstiltak

Tekniske sikringstiltak er i denne oppgaven digitale verktøy for å beskytte en verdi fra tilsiktede og utilsiktede digitale hendelser (NOU2015:13, 2015). Samtlige selskaper har brannmurer som overvåker trafikken ut og inn fra en datamaskin for å blokkere uønsket nettverkstrafikk (NOU2015:13, 2015). Videre beskrives Intrusion Prevention Systems (IPS) som et analyseverktøy hvor henvendelser som passerer brannmuren blir analysert. IPS-

[16] Et uttrykk i IT-verdenen hvor kollaps i en del av et system vil stanse hele systemet.

systemet kan identifisere en rekke nettverksbaserte angrep som annen teknologi ikke oppdager. Antivirus er et tredje tiltak. Antivirus fungerer slik at programmer leter etter, og forsøker å ødelegge, skadevare. For å teste og kontinuerlig oppdatere tekniske sikringstiltak gjennomføres penetration-tester («pen-tester»). Pen-tester er simulerte angrep hvor profesjonelle hackere leter etter sikkerhetssvakheter i et datasystem. Både selskap B og C beskriver pen-tester som del av arbeidet for å forbedre og styrke sikkerheten rundt digital informasjon. En respondent fra selskap B sier følgende:

> *«…vår typiske risikoevaluering er en reell penetrasjonstest, hvor vi leier inn profesjonelle hackere som prøver å ta oss i alle vinkler, stjele informasjon fra oss…alt fra prosess til IT til hva som helst. Også jobber vi oss gjennom disse tiltakene. Implementerer tiltak…»*

I etterkant gjør de re-testing, da gjerne med en annen aktør for å finne flest mulig svakheter og dermed tette flest mulig hull. Respondenten forteller videre at dette gjøres jevnlig. Hver 18. måned gjøres det en grundig test i tillegg til mindre tester innimellom. En respondent fra selskap C slår et slag for pen-tester, fordi det er noen som gjør noe fysisk, og resultatene foreligger umiddelbart. Respondenten sammenlikner med ROS-analyser hvor man tenker seg frem til ulike scenarier. Til sammenlikning mener respondenten at pen-tester ikke innbefatter like mange diskusjoner som innen utarbeidelse av ROS-analyser; «*…Du kan ikke diskutere de [resultatene fra pen-tester]. Det er ikke noe diskusjon på «kan det skje?», de [profesjonelle, innleide hackerne] gjorde det. De kom gjennom, det er facts*». Respondenten mener at dette gir mer til dem som jobber operativt enn ROS-analysene. Han understreker imidlertid at kombinasjonen av metoder er nyttig. Pen-testen ser ikke på rutiner, den er heller en teknisk metode.

Sensornettverk, et tiltak for kontinuerlig å følge med på all datatrafikk i et selskap beskrives av respondenter i selskap A og B. Et sensornettverk består av sensorer som til enhver tid skanner systemer for unormal aktivitet, også av autentiserte brukere. Et eksempel på et sensornettverksystem er Varslingssystem for Digital Infrastruktur[17] (VDI) fra Norges nasjonale cybersenter (NorCERT; den operative delen av Nasjonal Sikkerhetsmyndighet,

[17] «Sensornettverket - Varslingssystem for digital infrastruktur (VDI) - består av sensorer utplassert hos virksomheter som ansees som en del av kritisk infrastruktur i Norge… Sensornettverket driftes fra NorCERT som er den operative delen av NSM som daglig håndterer dataangrep» (NSM, 2017a).

NSM) (NOU2015:13, 2015). En respondent i ett selskap forklarer at de er en del av VDI-nettet til NSM. Respondenten forteller at det finnes mønstre mellom applikasjoner og brukeratferd og at sensornettet kontinuerlig leter etter avvik fra normalen. Avvik varsles til en manuell 24/7-cyber-driftsoperasjon som vurderer dem. Det er av avgjørende betydning at sensorene får hyppige oppdateringer om nye ondsinnede koder.

En respondent i selskap A beskriver beskyttelse av sensitiv informasjon gjennom et tofaktor-system[18] hvor brukeren logger inn ved å taste inn brukernavn, eget passord og et generert passord (bankID på mobil er et tofaktor-system). Flere separate autentiseringsfaktorer kompliserer påloggingen og virker dermed ekstra beskyttende på de data som sikres av to-/flerfaktor-pålogging. I en NVE-rapport påpekes det at en trusselaktør som får tilgang til interne systemer gjennom for eksempel e-poster med lenker og vedlegg som inneholder skadevare, vil ha begrensede muligheter til å hente ut sensitiv informasjon takket være flerfaktor-autentisering (Hagen m.fl., 2017). I utgangspunktet er dette tiltak som bedre sikrer informasjon, men det kan slå begge veier. Respondenten fra selskap A beskriver en utfordring med å plassere informasjon på riktig «plattform», og at ansatte kan gjøre feilvurderinger:

> «*…vi hadde lagt informasjon i en database. Så noen hadde funnet ut at den burde være lettere tilgjengelig utenfor systemet vårt fordi den innehold bare [ikke-sensitiv] informasjon. Men da la de ut hele det området med en sånn enfaktor-pålogging. Da er det plutselig lettere tilgjengelig, sensitiv informasjon*».

Her skulle en ansatt flytte noe informasjon fra en godt beskyttet database (med tofaktor-autentisering) til en database med enfaktor-autentisering. Vedkommende endte imidlertid opp med å uaktsomt flytte en større datamengde enn ønsket, og noe av denne informasjonen var av sensitiv karakter. Mennesker gjør feil (NOU2015:13, 2015), og dette må inkluderes i risikovurderinger (Hagen m.fl., 2017). For å begrense potensielle skader ved feil som dette – eller andre – brukes logging.

Logging er et system hvor alle endringer i systemer og komponenter lagres (Hovland, 2017). En respondent fra selskap A forteller at alle handlinger i systemene lagres ved logging. På den måten kan de spore en endring tilbake til en konkret ansatt. NVE skriver at systemer vil svikte som følge av feil eller målrettede angrep. Det vil alltid finnes restrisiko, noe som understreker

[18] Mindre hemmelig informasjon kan beskyttes ved hjelp av enfaktor-pålogging hvor man kun trenger brukernavn og passord.

viktigheten av gode loggrutiner (NVE, 2017, 27.3). Logging og analyse av loggene (logganalyse) kan gi risikoreduksjon i form av tidlig oppdagelse av feil, samt læring fra uønskede hendelser i etterkant. Dette vil også gjøre det enklere å sikre bevis ved en eventuell anmeldelse (Hagen m.fl., 2017). Respondenten fra selskap A beskriver videre en ny ordning hvor man skal, ikke bare bør, ha et system[19] for å overvåke loggene. Overvåkingssystemet varsler automatisk om det skjer noe mistenkelig. Selskap B peker på logging av leverandører. Han forklarer at leverandører har koder som kontinuerlig sjekkes av et analyseprogram. Hvis leverandøren endrer koden uten å si ifra, vil dette raskt oppdages.

5.3.3 Organisatoriske sikringstiltak

Under organisatoriske tiltak vil jeg beskrive forståelse/kunnskap rundt beskyttelse av sensitiv informasjon blant ansatte, verdivurderinger, kommunikasjon mellom ledelse og ansatte, tilgangssikring, ROS-analyser, samt internt og eksternt tilsyn.

Samtlige respondenter i denne studien beskriver tiltak for å styrke bevisstheten rundt informasjonssikring. Internrevisjoner både på informasjonssikkerhet og andre temaer nevnes av respondenter i selskap A og C. I henhold til en respondent i selskap C har selskapet et obligatorisk informasjonssikkerhetskurs som alle nyansatte skal gjennom. De får her en gjennomgang av det trusselbildet bransjen står overfor, hvorfor informasjonssikring er viktig, hva som er sensitiv informasjon, med mer. Ingen av de andre selskapene beskriver et liknende kurs for nyansatte, men en respondent i selskap A forteller om bevissthetskampanjer med nano-learning hvor

> «*…du får litt informasjon hele tiden om ting du bør gjøre og tenke på innen informasjonssikkerhet. På intranettet har vi informert. I tillegg jobber vi med sikkerhetsrutiner og standarder for å holde et godt nivå av informasjonssikkerhet*».

I selskap B forklarer en respondent at de har mange sikkerhetsrelaterte aktiviteter planlagt for de ansatte i 2017.

Til tross for mange gode tiltak beskriver respondenter fra samtlige nettselskaper i denne studien utfordringer innen informasjonssikkerhetsforståelse og forbedring av denne innad i selskapene. I selskap C forklarer en respondent at det er vanskelig å få ansatte til å forstå at alle sitter i samme båt, og at valg og handlinger i andre avdelinger enn sikkerhetsavdelingen

[19] SIEM-systemer (Security Information and Event Management).

kan ha betydning for selskapets totale informasjonsbeskyttelse. En respondent i selskap B forklarer at selskapet er løst organisert, med mange små miljøer som hver har ansvar for sitt. Mennesket er gjerne det svakeste leddet, og vi gjør alle feil. En utfordring for mange virksomheter er dermed manglende kunnskap om informasjonssikkerhet[20] (NOU2015:13, 2015), noe som inkluderer manglende kunnskap om beskyttelse av sensitiv informasjon. Taushetsplikt overfor sensitiv informasjon gjelder for enhver (bfe, 2013). *Enhver* er alle som måtte få tilgang til sensitiv informasjon om energiforsyningen (NVE, 2013). Dette gjelder alle opplysninger om energiforsyningen som kan brukes til å skade eller påvirke anlegg/funksjoner med betydning for kraftforsyningen (bfe, 2013). Det kan dermed argumenteres for at de fleste som arbeider i kraftbransjen i større eller mindre grad forholder seg til informasjonssikring og taushetsplikt. En respondent fra selskap A forteller at mange av hans kollegaer mest sannsynlig ikke vet hvilken informasjon de behandler i hverdagen som er å anse som sensitiv. Uklarheter på denne fronten kan gjøre det vanskelig å være bevisst på å holde hemmelig informasjon skjult; «*…det er noen [dokumenter] det står stemplet 'kraftsensitiv informasjon' på, og så henger de [ansatte] det opp på veggen der man kan gå og kikke inn i vinduet*» (respondent i selskap A). Hvis folk ikke vet hva som er hemmelig vil de kunne være uforsiktige med hva de sier, både i mobiltelefonen og ellers. Videre skal alle nettselskapene jeg har vært i kontakt med selv identifisere hva som er sensitiv informasjon og hvor denne befinner seg (bfe, 2013; NVE, 2013). Det er altså opp til hvert enkelt selskap å definere hva de mener er kraftsensitiv informasjon (uttalt av respondent fra selskap B). Dette problematiseres av en respondent i selskap A; «*De [NVE] kunne vært mer spesifikk på kraftsensitiv informasjon; hva det egentlig er*». I selskap B etterlyses også mer presise formuleringer og krav fra NVE, og en respondent eksemplifiserer dette slik;

> «*Som for eksempel nettsensitive data. Her finnes det egne regler… Men hva er nettsensitiv data? Det står noen eksempler på det, men det har vært en diskusjon i bransjen i 10 år og er fortsatt en diskusjon. Ingen er presise… Det der er et problem, vi vet ikke hva som er nettsensitivt. Vi tolker og antar alle sammen. Og så tørr ikke NVE å være helt tydelige*».

Han mener at ulike tolkninger og antagelser er å anse som en utfordring i sektoren, og det oppstår usikkerhet. Mange virksomheter har ikke kjennskap til, eller oversikt over, alle

[20] Konfidensialitet (hemmelighold av sensitiv informasjon), integritet og tilgjengelighet (DIFI, 2017, 14.3).

verdiene de har (NOU2015:13, 2015). En annen respondent i selskap B forteller at han savner en ordentlig informasjonsklassifisering og gjennomgang av selskapets ressurser. Han henviser til generell risikostyringslitteratur og sier at man ikke kan drive risikostyring uten å gå gjennom hva man har og hva det er verdt, for så å klassifisere det. Respondenten forklarer videre; «*…jeg savner kanskje litt helt overordnet risikostyring, fra ledelsen. Men det kan godt hende at de bare er dårlige til å kommunisere hva de gjør. Men jeg tror egentlig ikke det*».

Også i selskap C nevnes forholdet mellom ansatte og ledelsen. Her trekkes det frem utfordringer med formidling av risikonivåer og aggregering av risiko fra detaljerte ROS-analyser og oppover i systemet. Dette kan henge sammen med ulike kompetansenivåer i selskapet:

> «*Når man gjør risikoanalyser på et lavt nivå i organisasjonen, så må man operere med konsekvensskalaer som er forståelige på det nivå, altså…ofte er det 'fungerer systemet eller ikke?', mens høyere opp i organisasjonen er det 'går det utover forretningsprosessen eller ikke?'…*».

Ulike kompetansenivåer kan gi misforståelser. Å kunne kommunisere tydelig og forståelig til alle i et selskap er komplisert. Respondenten slår fast at selskapet kan bli bedre på dette området.

Respondenter fra to av tre selskaper i studien beskriver en utfordring knyttet til ansatte som ikke er bevisste på hvem de slipper inn som «*bare skal inn og fikse ett eller annet*». I to av tre nettselskaper ble mine intervjuer gjennomført på nøytrale møterom. Det siste selskapet hadde dobbelbooket møterommet. Vi endte derfor opp på kontoret til en bortreist ansatt. På kontorpulten lå det mange papirer og utskrevne e-poster. Her var ulike navn og andre opplysninger lett tilgjengelige. Jeg vet ikke om noe av det som lå på pulten eller sto i permer i bokhylla var av sensitiv karakter, men det var lett tilgjengelig for en «student som skriver masteroppgave» (om norske nettselskapers beskyttelse av sensitiv informasjon). Under ett av de tre intervjuene i dette selskapet forlot respondenten meg fordi han skulle ut for å ordne noe. Vedkommende var borte i et par minutter. En respondent i dette nettselskapet forteller at de har hatt avvik innen byggsikring, og hvem de slipper inn. En respondent fra dette selskapet forklarer at det spesielt gjelder folk som kommer for å gjøre en jobb hos dem, gjerne vindusvaskere eller elektrikere. Dette beskrives som noe av det mest utfordrende i vedkommende selskap.

Slurv innen tilgangssikring beskrives videre av en respondent i selskap B. Her pekes det på konsulenter og eksterne partnere som har fått tilgang til innsiden, men som ikke fratas denne tilgangen etter endt oppdrag:

> «*…Man ser flere ganger at konsulenter eller eksterne partnere som jobber i felt for oss slutter og at ingen melder fra. Da har de fortsatt aktiv tilgang i våre domener og sånne ting. Det er slurv, ren sånn prosesslurv, og det er viktig. Å sikre de banale tingene der*».

Alle enhetene i Kraftforsyningens beredskapsorganisasjon (KBO) «…skal ha et oppdatert beredskapsplanverk tilpasset virksomhetens art og omfang» (bfe, 2013, § 2-5). En respondent fra selskap B forteller at selskapet har innsett at den neste krisen kommer, og at de derfor har utarbeidet kriseplaner for ulike scenarioer. Selskapet trener på ulike scenarioer og lærer av dem. Respondenten beskriver innøvde beredskapsrutiner, forberedte prosedyrer og definerte bemanninger. På oppfølgende spørsmål om hvilke prosedyrer de har, svarer respondenten at de opererer med fire beredskapsnivåer: Grønn, gul, rød, sort. Han forklarer videre at selskapet har egne regelsett til hvert nivå, og at alle vet hva de skal gjøre og hvilke tiltak som skal implementeres på de ulike nivåene/sonene. Selskapet ligger som regel i grønn sone. Skjer det noe uønsket som gjør at selskapet går over i gul sone, vil de få et varsel fra NVE eller NSM. Her implementeres for eksempel tiltak som styrker brannmurene («ekstra IT-vakt»). I rød sone isolerer selskapet SCADA-systemet fra det administrative nettet. I tillegg kalles ekstramannskaper inn. I sort sone trekkes all IT ut, og manuell kobling av SCADA-operasjonen iverksettes. En respondent i selskap A forklarer at de klarer å drive strømnettet selv uten SCADA-systemene. Skulle SCADA-systemene stanse for eksempel som følge av teknisk feil vil nettselskapet miste oversikten over kraftdistribusjonen, men en del anlegg vil fortsatt fungere, og strømleveransen vil fungere manuelt (respondent i selskap A). Det er imidlertid verre hvis trusselaktører overtar kontrollen over SCADA-systemene. Respondenten i selskap B oppsummerer sin beskrivelse av beredskapsrutiner og beredskapsnivåer med å fortelle at alle prosedyrene er forhåndsdefinerte eller forhåndsbestemte; lyser den røde lampa så skal SCADA-systemet isoleres, her finnes det ikke rom for skjønn.

> «*Det er veldig sånn, dette vet alle hva er. Alle regelsettene er definerte; det trenes på, det øves på. Litt med den hensikt at de skal vite akkurat hva de skal gjøre når vi går i rødt, og det skal skje av seg selv. Det skal skje fort…beredskapsnivåene skal sitte i ryggmargen*» (en respondent i selskap B).

En annen respondent fra samme selskap understreker at man aldri kan planlegge nøyaktig mtp. hendelser som kan skje. Han forteller imidlertid at kraftbransjen kontinuerlig håndterer beredskapssituasjoner, og siden de øver på det og driver med det, så «*…blir vi mye flinkere til å improvisere når det først skjer noe*». Han tror noe av det viktigste er å ha så mye kunnskap at man skjønner når man må be om hjelp. Dette kan være både på organisatorisk nivå, og på ansatt-nivå. I tillegg beskrives en mailordning i selskap A hvor de ansatte kan sende en beskjed til sikkerhetsansvarlige hvis de for eksempel er usikre på innholdet i mottatte mailer.

Beredskapsforskriften (bfe) slår fast at alle enheter i KBO[21] skal gjennomføre risiko- og sårbarhetsanalyser (ROS-analyser) knyttet til ekstraordinære forhold (bfe, 2013). Disse skal være såpass omfattende at «…enheten kan identifisere risiko og sårbarhet ved alle funksjoner, anlegg og tiltak av betydning for å oppfylle kravene i forskriften. Analysene skal minimum gjennomgås årlig og oppdateres ved behov» (bfe, 2013, § 2-4). Samtlige selskaper i dette studiet gjennomfører ROS-analyser i større eller mindre grad. En respondent fra selskap C forteller at de velger ut noen områder de gjør ROS-analyser på. Det kreves mange ulike faggrupper når analysene gjøres. Respondenter fra alle selskaper peker på en form for brainstorming innen ROS-arbeidet. En respondent i selskap B forklarer at ROS-analyser er viktige for å tenke og lære. Videre vil det variere hvilke risikovurderinger de gjør, samt hvem som er med i utformingen av vurderingene (uttales av respondent fra selskap C). En annen respondent fra selskap C beskriver et samarbeid med eksterne aktører i arbeidet med analysearbeidet; «*…vi leier ofte inn noen som gjør risikoanalyser og kjører ROS-analysene for oss, liksom Norske Veritas[22] eller noe*». Han mener at det er vanlig å ha noen som fasiliterer ROS-analysene. Selskapet selv kommer med de fleste innspillene, mens fasilitatoren (for eksempel Det Norske Veritas) kan, med utgangspunkt i sin erfaring, stille spørsmål eller komme med poenger som selskapet selv kanskje ikke har sett.

Beredskapsforskriften fastslår at selskaper skal iverksette «nødvendige sikrings- og beredskapstiltak ut fra stedlige forhold og samfunnsmessig betydning» på bakgrunn av ROS-analyser (bfe, 2013, § 3.5.1). Samtlige selskaper beskriver utfordringer innen etterlevelse av

[21] Kraftforsyningens beredskapsorganisasjon; enheter med vesentlig betydning for drift eller gjenoppretting av sikkerhet innen kraftsektoren (Energiloven, 1990). «Alle enheter i KBO har en selvstendig plikt til å sørge for effektiv sikring og beredskap og iverksette tiltak for å forebygge, begrense og håndtere virkningene av ekstraordinære situasjoner» (DSB, 2016).
[22] Det Norske Veritas (DNV): Frittstående og uavhengig stiftelse som jobber for å beskytte liv, eiendom og miljø.

tiltak og forbedringsforslag som kommer ut av ROS-analyser. En respondent fra C forklarer at de gjerne fokuserer på å kjøre så og så mange ROS-analyser og pen-tester[23] uten å gjøre så mye med de funnene som avdekkes i slike analyser. En respondent i selskap B mener at ROS-analyser er spesielt utfordrende som følge av to forhold; For det første etterlyser respondenten mer samarbeid og dialog i bransjen for å gjøre arbeidet med ROS-analyser mer optimalt. I tillegg må selskapet og de ansatte ta aktivt eierskap til arbeidet. Dette er nødvendig for at arbeidet med ROS-analyser ikke skal bli en ren skrivebordsøvelse som kun gjennomføres fordi den må ligge i skuffen ved tilsyn fra NVE. En respondent i selskap C tror noe av problemet med ROS-analysene kan ligge i manglende oversikt. Fremfor å bruke excel-ark i ulike avdelinger har selskapet nå tatt i bruk det web-baserte risikostyringssystemet «EasyRisk» (respondent fra selskap C). Risikostyringssystemet er utviklet av Det Norske Veritas (DNV, 2013). Systemet gir et kontinuerlig øyeblikksbilde av et selskaps risikosituasjon (DNV, 2013). Verktøyet gjør det enklere å se helheten av ROS-analyser og tiltak: «*EasyRisk; der ting ligger inne og jeg kan faktisk gå inn å se 'hvordan er risikobildet mitt, hvilke tiltak har vi som vi må jobbe med?'».* En respondent i selskap A tror problemet med utarbeidelsen av ROS-analyser er at de fleste synes arbeidet er kjedelig og blir veldig rutinepreget. En annen respondent fra selskap A forteller at de vil fokusere på barrierestyring. Respondenten forklarer at de gjør risikoanalyser for å finne barrierer som skal iverksettes (tiltak for å beskytte selskapet og dets verdier fra trusler og farer). Det er imidlertid ikke vits å gjøre risikoanalyser for å komme frem til barrierer som ingen i selskapet bruker. Respondenten eksemplifiserer med nedlåsing av sensitiv informasjon i safe på kontoret. Dette er en barriere for at ikke sensitiv informasjon skal forsvinne. Denne barrieren vil imidlertid være ubrukelig hvis ingen låser disse safe-ene. Han konkluderer med at

> «*…selv om man har iverksatt [barrierer] så må man ha måling/kontroll av at barrierene faktisk blir etterlevd. Det tror jeg er den største svakheten. Det er mange som bare kjører ROS-analyser og putter den i en skuff. Eller; de har satt i gang/implementert, men det dør vekk etter kort tid. Det tror jeg er den største svakheten med risikoanalyser. Det er det*».

[23] «Penetration tests». Selskapet leier inn profesjonelle hackere som leter etter sårbarheter i systemene deres. Dette beskrives ytterligere senere.

En respondent fra selskap B forteller at forrige gang selskapet gjorde en grundig ROS-analyse, fikk de godt over hundre tiltak som de ikke hadde sjanse til å gjennomføre på et år. Respondenten påpekte at en ny analyse ville gi mange av de samme funnene, og at det dermed ikke er effektivt å gjennomføre ny analyse hvert år, noe de heller ikke gjør i det selskapet. Respondenten forteller at ROS-analyser er viktige tiltak for å tenke, men at hvis man ikke tenker, lærer og implementerer tiltak på bakgrunn av læring så blir det kun en skrivebordsøvelse. En annen respondent i B beskriver en mer målrettet prosess; «*Det å teste, måle, gjøre tiltak og re-måle er en prosess vi bruker mye mer [enn ROS]*». Tester beskrives av flere selskaper. En respondent fra selskap C mener at fremfor å tenke seg fram til hva som kan skje, bør man gjøre noe fysisk og se hva som faktisk skjer. Han slår et slag for penetration-tester som er beskrevet som et tiltak for å teste tekniske barrierer. Respondenten understreker viktigheten av en kombinasjon av metoder. En annen form for testing og re-testing beskrives i to av tre nettselskaper (beskrives av respondenter i selskap B og C); et test-angrep på e-post som sendes ut til ansatte i selskapet. I selskap B beskrives forklarer en respondent at

> «*Vi skapte et phishing-angrep til alle ansatte. Og så at mer enn 10 % klikker på det. Greia var at du skulle åpne et PDF-dokument som sa at du måtte autentiseres fordi den var kryptert. Du måtte taste inn ditt brukernavn og passord. Det var det 5 % som gjorde. Det har vi tenkt å gjenkjøre og så skal vi gjøre en e-læringskampanje. Så skal vi gjøre det en gang til*».

Dette er et effektivt tiltak for å få de ansatte til å tenke informasjonssikkerhet i hverdagen, for at informasjonssikkerhet skal sitte i ryggmargen (B). I selskap C ble test-mailen sendt til en del utvalgte. Hvem som trykket seg inn og hva de gjorde ble tracket. E-posten var dårlig skrudd sammen, og respondenten mener at alle burde skjønt at de ikke skulle trykke, «*Men det gjør de allikevel*» (en respondent i selskap C).

Samtlige selskaper beskriver tilsyn og arbeid med avvik. Det gjennomføres både eksterne og interne tilsyn. Informanten fra NVE forklarte at de gjennomfører jevnlige tilsyn med nettselskapene og sjekker at de ivaretar kravene i bfe når det gjelder informasjonssikkerhet og beskyttelse av kraftsensitiv informasjon. I henhold til informanten fra NVE gjennomfører NVE stedlige og skriftlige tilsyn. Et stedlig tilsyn innebærer fysisk oppmøte hos nettselskapene hvor det stilles en del spørsmål. Her har NVE gjerne tema de ønsker å gå spesielt inn på (uttalt av respondent i selskap C). Tilsynet avsluttes med en muntlig

gjennomgang av hva NVE har funnet. I etterkant mottar selskapet en rapport som dokumenterer dette. Skriftlige tilsyn innebærer besvarelse av en del spørsmål som er sendt fra NVE. Selskapene besvarer spørsmålene og får beskjed om avvik etter hvert som NVE gjennomgår svarene. En respondent fra selskap B forklarer at tilsynet er basert på selvrapportering uansett metode. Nettselskapene får en frist på å lukke avvikene, og bekreftelse på lukket avvik må sendes til NVE. Som oftest godkjennes dette av NVE, men i noen tilfeller kan de ta en stikkprøve eller be om detaljert dokumentasjon på hvordan avviket er lukket. I tillegg forteller respondenter fra samtlige nettselskaper i denne studien at det gjennomføres interne tilsyn, eller internrevisjoner/-kontroller av forskjellig karakter.

En respondent i selskap B forklarer at det brukes mye tid og ressurser på brannmurer, policy-arbeid og ROS-analyser. Han forklarer at nesten alle angrep mot selskapet handler om phishing av et eller annet slag; person-dedikert phishing eller sosial manipulasjon av en eller annen grad. Derfor bør sikring av sensitiv informasjon i større grad handle om intern kompetanse, aktiv overvåking, samarbeid og deling av informasjon med andre bransjer.

5.3.4 Bransjesamarbeid

Samtlige selskaper er opptatt av samarbeid, og det pekes spesielt på plattformer som KraftCERT[24], NorCERT[25], FSK[26] (Forum for informasjonsSikkerhet i Kraftbransjen) og interne plattformer mellom selskapene i eget konsern. KraftCERT er et kompetansemiljø som kan gi råd og bistå selskaper i kraftbransjen ved større IKT-hendelser (NOU2015:13, 2015). KraftCERT beskrives som en «paraplyorganisasjon» hvor man deler informasjon og spleiser på sikkerhetskompetanse (respondent fra selskap B). Respondenten fortsetter med at de i KraftCERT «*…diskuterer vi hendelser i etterkant; hva kunne vi gjort annerledes, hvordan kunne vi stoppet det tidligere, debrief-aktig varianter*». En annen respondent fra selskap B mener at KraftCERT er nyttig ettersom det er vanskelig å forberede seg på det ukjente, og at nettverk som KraftCERT også kan være til stor hjelp når det først skjer noe.

[24] KraftCERT jobber med informasjonsdeling for at kraftbransjen skal være oppdatert på sårbarheter og truser, samt være i stand til å oppdage og håndtere digitale trusler (KraftCERT, 2015).
[25] Norges nasjonale cybersenter; den operative delen av NSM (NSM, 2017c). NorCERT håndterer dataangrep mot samfunnsviktige virksomheter og informasjon. I tillegg drifter NorCERT VDI (nasjonalt sensornettverk).
[26] FSK har 21 medlemsbedrifter blant de største kraftprodusentene og nettselskapene i Norge (NOU2015:13, 2015). De jobber med aktiviteter relatert til informasjonssikkerhet i kraftforsyningen slik dette er definert i bfe.

> «*Hele founderen i [poenget med] KraftCERT er samarbeid, et samarbeid som er tuftet på verdikjedekompetanse i det som er kraftproduksjon og distribusjon av kraft, som er egne verdikjeder. Det er et av de viktigste tiltakene. Egentlig er tiltaket informasjonsdeling og bransjesamarbeid, å bli ett lag når det kommer til sikkerhetshåndtering*».

En respondent fra selskap A forklarer at man kan være med i KraftCERT på ulike måter. Han ser på KraftCERT som en slags dugnad for å kunne ha et organ som følger med mer enn det de selv klarer i bransjen. Som medlem sponser man organisasjonen mot at man får en del varsler. I tillegg kan man delta på årlige eller halv-årlige møter som er informative og nyttige. Ett av nettselskapene i dette studiet opplevde nylig et CEO-phishing-angrep (spear-phishing) hvor de fikk spesifikt varsel fra KraftCERT om dette angrepet. En leder i nettselskapet fikk en e-post som så ut som den kom fra selskapets økonomidirektør med fullt navn og språk på norsk. «Økonomidirektøren» ba om hjelp til å overføre penger, og det hastet. Mailaktiviteten kom fra utlandet, og KraftCERT fanget opp signalene inn mot landet. Mailen så veldig ekte ut, men pengene ble ikke overført. På denne måten kan samarbeidet i KraftCERT være nyttig. En respondent fra selskap A forklarer at de daglig følger med på logger og får rapporter på hvem som «*banker på døren*». Det er imidlertid vanskelig å vite hva som er målrettet. Her kan samarbeidet med KraftCERT være veldig verdifullt (samme respondent i selskap A). En respondent i selskap C beskriver et trusselfokus i KraftCERT, og trekker frem Forum for informasjonssikkerhet i kraftforsyningen (FSK) som en plattform for diskusjon om hvordan man bør beskytte seg mot disse truslene.

FSK nevnes også av respondenter fra samtlige tre selskaper i denne studien. Flere respondenter i selskap C beskriver FSK som et bransjespesifikt fagforum for virksomheter i kraftsektoren. En respondent i selskap A skisserer forumet som et bredt samarbeid hvor både energiselskaper, nettselskaper og en del leverandører er med. Respondenten sier at FSK er et åpent forum; «*…vi er veldig åpne overfor hverandre fordi store deler av de møtene er lukket for andre enn kraftbransjen. Så vi kan være åpne. Der får man et inntrykk av hvordan andre jobber*». Samtaler med andre som jobber med de samme problemstillingene som en selv kan være nyttige. På spørsmål om NVE er tilstede svarer respondenten at det var NVE som i sin tid tok initiativet til dette forumet. Han fortsetter med å forklare at NVE kjenner sin besøkelsestid. Møtene består som regel av en åpen del og en lukket del. NVE og leverandører

får være tilstede i den åpne delen, nettselskaper er tilstede i den lukkede. Respondenten opplever dette som nyttig.

I tillegg beskrives NorSIS' sikkerhetsmåned i oktober av flere respondenter i både selskap A og C. Her var fokus på bevissthet rundt informasjonssikkerhet. Både oppgaver i et quest-back-system (selskap A) og lærerike foredrag (selskap C) nevnes her.

6. DISKUSJON

I dette kapitlet vil jeg drøfte funnene mine opp mot oppgavens teoretiske rammeverk. Kapitlet er inndelt etter forskningsspørsmålene mine og vil gå inn på trusler, barrierer og kollektiv bevissthet. Jeg argumenterer for at kollektiv bevissthet har en overordnet rolle innen beskyttelse av sensitiv informasjon i den forstand at ansatte i nettselskapene må være bevisste på verdiene i selskapet (kraftsensitiv informasjon), de må være bevisste på det trussellandskapet som foreligger, samt på sårbarhetsreduserende barrierer.

6.1 Intenderte og ikke-intenderte trusler

Hvilke trusler og angrep mot sensitiv informasjon står nettselskapene overfor?

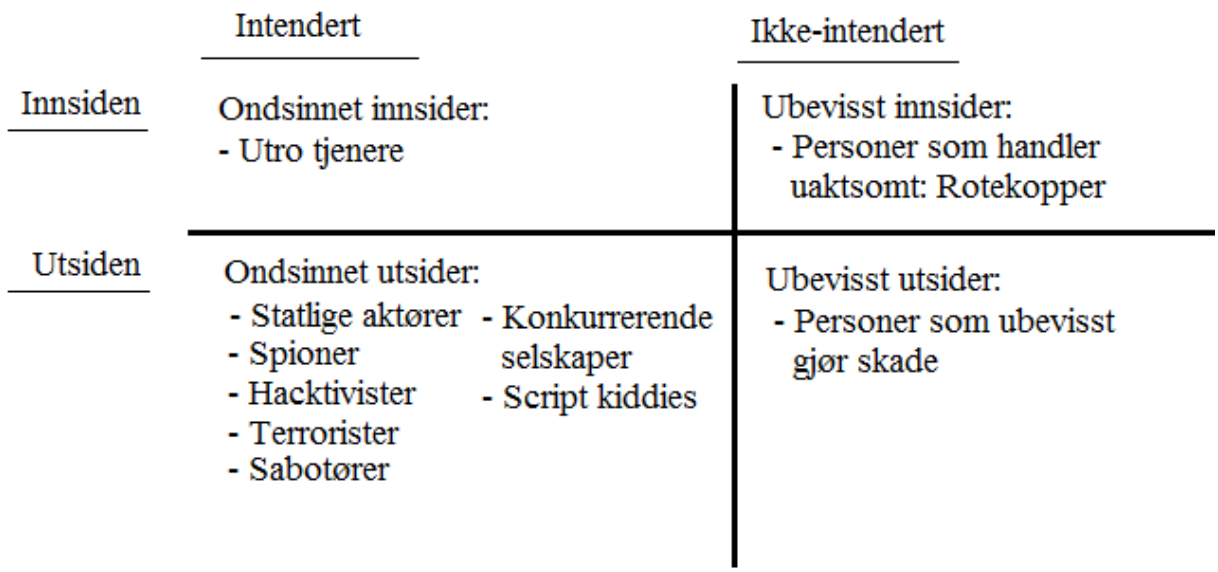
Trusler beskrives ofte i sammenheng med villede handlinger (security), selv om begrepet også kan brukes i en diskusjon av ikke-villede hendelser (safety) (Aven m.fl., 2015). Alle aktører (bevisste/ubevisste) og angrep (direkte/indirekte) som bidrar til uønsket innsyn i sensitiv informasjon kategoriseres i denne oppgaven som trusler. Trusselaktørenes handlinger kan være intenderte eller ikke-intenderte (Engen m.fl., 2016). Jeg vil nå presentere trusler og angrep mot sensitiv informasjon i nettselskapene, både på *innsiden* (interne) og *utsiden* (eksterne) i/av et nettselskap.

Alle innsidere kan utgjøre en trussel ettersom de har tilgang på mye informasjon (NSM, 2016a). Her kan det skilles mellom ansatte som bevisst ønsker å gjøre skade, og ansatte som uaktsomt, indirekte, skader selskapet gjennom slurv og uvitenhet. Det at en respondent uttrykte bekymring for at misfornøyde ansatte skal kunne skade selskapet er i tråd med kriminalitets- og sikkerhetsundersøkelsen i 2015 som viser at 3 av 10 norske virksomheter har avdekket utro tjenere blant egne ansatte (NSR, 2015). Slike upålitelige ansatte kategoriseres som «bad apples» i Dekkers «The old view»-teori. Han skriver at komplekse systemer ville fungert fint hadde det ikke vært for upålitelig oppførsel fra utro tjenere (Dekker, 2006). «Bad apples» i Dekkers forståelse (2006) trenger imidlertid ikke bare å være utro tjenere. Ubevisste innsidere er også relevante innsidetrusler, eller «bad apples». En ubevisst innsider prøver ikke bevisst å kompromittere informasjon eller virksomhet. Vedkommendes vurderinger og handlinger, som havner i en gråsone mellom intenderte og ikke-intenderte handlinger (Kruke m.fl., 2005), gjør ham/henne til en trussel mot hemmelighold av sensitiv informasjon (NSM, 2016a). Uaktsomhet på innsiden er for eksempel en form for ikke-intendert slurv som kan

legge til rette, eller «åpne døren», for eksterne trusselaktører på jakt etter sårbarheter i selskapenes informasjonsbeskyttelse. Uaktsom slurv av medarbeidere kan således medføre kompromittering av sensitiv informasjon. En ansatt i selskap A som, ved en feiltakelse, plasserte sensitiv informasjon i en database uten tilstrekkelig beskyttelse, er et godt eksempel på dette. Uaktsomhet trenger imidlertid ikke bare å være direkte slurv. Ansatte som ikke vet hva som er å anse som sensitiv informasjon tyder på mangelfull kunnskap om verdier i selskapet, en mangel som kan relateres til hva Merton kaller uvitenhet i sin Law of Unintended Consequences (Merton, 1936). Ikke-intenderte handlinger, som at en student fikk gjennomføre intervjuer på en fraværende medarbeiders fullt utstyrte kontor, har likhetstrekk med hva Merton beskriver som feil og ignorering av mulige sideeffekter. En ikke-intendert effekt kunne vært at den eksterne studenten fikk tilgang til analoge data på kontoret (dokumenter, kart, diagrammer osv.) og kanskje også data på eksterne minnebrikker eller harddisker. En av respondentene ble plutselig nødt til å ordne noe og forlot den besøkende på kontoret. Situasjoner som krever umiddelbar handling kan involvere uvitenhet rundt visse aspekter av situasjonen, noe som kan føre til uønskede konsekvenser (Merton, 1936). Dette var en målrettet handling, og feil kan forekomme i hvilken som helst fase av en målrettet handling, jf. feil (Merton, 1936). På den annen side opereres det med nedlåsing av sensitive papirkopier og bruk av passordbeskyttelse på safe og datamaskiner, så det kan tenkes at ingen sensitive opplysninger var tilgjengelig på kontoret og at dette dermed ikke kan anses som et eksempel på feil, uvitenhet eller ignorering av sideeffekter (Merton, 1936).

På innsiden finnes altså utro tjenere og «rotekopper» som slurver, er uvitende eller som på andre måter handler uaktsomt. På utsiden finnes det ondsinnede aktører som kan samarbeide med utro tjenere, utnytte de sårbarhetene som uaktsomme innsidere skaper eller handle helt på egenhånd. Respondentene i denne studien snakker om daglige angrep (CryptoLocker, phishing, spear-phishing med mer). Noen kan ha som formål å bruke sensitiv informasjon som våpen (sofistikerte angripere; statlige aktører; etterretningsvirksomhet, spioner), noen vil fronte politiske meninger (hacktivister), noen ønsker å skade samfunnsfunksjoner med vold (terrorister, sabotører), mens andre vil ha tak i sensitiv informasjon av økonomiske årsaker (konkurrerende selskaper) eller få anerkjennelse i hacker-miljø («script kiddies»). Uansett metode og hensikt kan alle de ondsinnede utsiderne kategoriseres som kriminelle, hackere eller innbruddstyver – alt etter hvordan de velger å gå frem.

Som en oppsummering kan trusselaktørene kategoriseres som «innsidere» eller «utsidere» som handler intendert eller ikke-intendert, se figur 7.



Figur 7 Trusselaktører: Innsiden/utsiden/intendert/ikke-intendert

Ubevisste utsidere kan være aktører på utsiden som handler ut fra andre hensikter og er uvitende om utilsiktede sideeffekter, uvitende om at hans/hennes digitale eller fysiske handlinger kan lekke eller gi enklere tilgang til sensitiv informasjon. Det kan for eksempel tenkes at tidligere konsulenter med adgang til datasystemer uforvarende kan påvirke systemene.

Det kan argumenteres for at et samspill av intenderte og ikke-intenderte handlinger kan gi tilgang til ulik informasjon og programvare som i verste fall kan gjøre norsk kraftforsyning mer sårbar. Hvordan beskytter nettselskapene seg mot slike trusler? Samtlige selskaper jeg har snakket med har innført barrierer for å beskytte informasjon.

6.2 Barrierer

Hva slags barrierer etableres for beskyttelse av sensitiv informasjon i nettselskapene?

Barrierer er fysiske og/eller ikke-fysiske forhold som brukes for å beskytte mennesker og eiendom fra fiender og naturlige farer, ved å forhindre, kontrollere eller begrense uønskede hendelser eller ulykker (Sklet, 2006). Informanten fra NVE beskriver spear-phishing-angrep som målrettet e-post for å få folk til å klikke på en lenke eller åpne et vedlegg. Hvis en

virksomhet ikke har oppgradert all programvare og dette vedlegget åpnes kan man få skadevare i systemet. Det kan her pekes på brudd i to barrierer; (1) kunnskap hos den ansatte som mottok mailen (vedkommende burde ikke åpnet den), og (2) oppgraderinger i programvare (all programvare skulle være oppdatert). Dette kan kategoriseres som brudd i en myk og en hard barriere (ref. Reason, 1997). Det kan argumenteres for at både kunnskapen hos den ansatte som mottok mailen, og oppgraderinger av programvare i nevnte eksempel, er å anse som forebyggende barrierer etter Hollnagels inndeling (1999). Jeg vil ta med meg inndelingene i harde/myke (Reason, 1997) og forebyggende/beskyttende (Hollnagel, 1999) barrierer i drøftingen av hva slags barrierer som etableres for beskyttelse av sensitiv informasjon i nettselskapene.

6.2.1 Harde barrierer

Innen harde barrierer vil jeg starte med å dele inn i fysiske og tekniske barrierer av forebyggende karakter. Deretter beskrives beskyttende barrierer. Forebyggende barrierer skal hindre en uønsket hendelse i å skje (Svenson, 1991), mens beskyttende barrierer skal skjerme miljø og mennesker fra konsekvensene etter en uønsket hendelse (Hollnagel, 1999).

Innen forebyggende tiltak har samtlige nettselskaper satt opp redundante barrierer. Redundans handler om evnen til å utføre en oppgave selv om primærenheten feiler (Rochlin m.fl., 1987). Innen beskyttelse av analog informasjon vil en hard barriere kunne være fysiske gjerder eller sperringer i inngangspartiet. Dette gjør det vanskelig for uvelkomne å ta seg inn i kontorbygget. Her finnes det imidlertid potensielle hull i barrierene (jf. barrieremodell, figur 4); det kan for eksempel tenkes at sperringene kan være åpne på grunn av teknisk feil. Eventuelt kan en ansatt ha sluppet uvedkommende gjester inn. Barrierer som her kan fungere redundant er låste dører og safe-er som fysisk skiller trusselaktøren (gjesten) fra verdien (den sensitive informasjonen) samt fargekoder på besøkskortene som viser tilgangsbegrensninger. Dette kan ses på som en form for overlapping av tiltak (Rochlin m.fl., 1987).

Uønskede digitale henvendelser fra ondsinnede utsidere kan stanses av brannmurer eller IPS, som til dels kan fungere som dupliserende barrierer i forståelsen til Rochlin m.fl. (1987). Et tiltak som implementeres for å teste de tekniske barrierene er pen-tester. Dette virker forebyggende ettersom faktiske sårbarheter i for eksempel brannmurer eller IPS raskt tettes. Skulle et angrep passere både brannmur og IPS, vil flerfaktor-autentisering kunne fungere som en overlappende, redundant barriere som kan hindre trusselaktøren i å få tilgang til

sensitiv informasjon. Her kan det argumenteres for mangfold (variasjon i beskyttelse) i barrierene ettersom brannmurer og IPS tar imot og vurderer henvendelser utenfra. Flerfaktor-autentisering er i større grad et innsideverktøy. Barrierene har ulike funksjoner, og kan beskytte mot sammenbrudd av barrieren i front (Reason, 1997).

Som en hard, forebyggende barriere mot innsidere som trusselaktører har samtlige selskaper rutiner for logging og logganalyse. Ved logging lagres alle handlinger som gjøres, og de kan spores tilbake til en konkret ansatt. Logganalyser vil kunne vise ugunstig aktivitet både hos ansatte og leverandører som kan konfronteres, og eventuelle sikkerhetsbrudd kan ordnes opp i før det utvikler seg og kan føre til tap av sensitiv informasjon. I tillegg kan logganalyser være verdifulle i etterkant av en hendelse; det blir enklere å undersøke uønskede hendelser, lære av dem samt sikre bevis ved en eventuell anmeldelse (Hagen m.fl., 2017).

Logging og logganalyser[27] kan også være en beskyttende barriere. Disse kan gjøre det mulig å oppdage at sensitiv informasjon er plassert i en database hvor den ikke er tilstrekkelig beskyttet. Plassering av sensitiv informasjon i en database som kun var beskyttet av enfaktor-autentisering er eksempel på en ikke-intendert hendelse som kan oppdages med logging. Ingen systemer er sterkere enn svakeste leddet (NOU2006:6, 2006). Logging og logganalyser kan være en beskyttende barriere som kan begrense de negative konsekvensene ved denne type feilhandlinger før det får store konsekvenser. Logging og logganalyse kan også øke mulighet for læring og dermed forhindre fremtidige hendelser av samme karakter.

6.2.2 Myke barrierer

For at de harde barrierene skal fungere trengs det myke barrierer som lover, regler, tilsyn, trening, opplæring, administrativ kontroll, brifing med mer (Reason, 1997). Om disse følges vil avhenge av selskapene. Beredskapsforskriften, ROS-analyser, interne sikkerhets-instrukser, tilsyn fra NVE, internrevisjoner, test-mailer, øvelser, informasjonssikkerhetskurs, konferanser, møtevirksomhet og sikkerhetsmåned vil kunne kategoriseres som myke barrierer ifølge kategoriseringen til Reason (1997). Det kan imidlertid argumenteres for at beredskapsforskriften og ROS-analyser har en slags overordnet posisjon hvor de heller avdekker sårbarheter som gir behov for barrierer, fremfor å være en barriere i seg selv. Bfe

[27] Det finnes også en ny ordning hvor man skal ha et system for å overvåke loggene. Dette systemet varsler automatisk om det skjer noe mistenkelig.

peker blant annet på krav innen ansvar, beredskap, ROS-gjennomgang, varsling og rapportering, øvelser, internkontroll, kompetanse, sikringsplikt, identifisering av sensitiv informasjon, personkontroll, sikkerhetskopier med mer (bfe, 2013). ROS-analyser har på sin side som mål å avdekke risiko og sårbarheter i funksjoner og anlegg. Både bfe og ROS-analyser vil således peke på behov for barrierer (både harde og myke). Den grundige ROS-analysen i selskap B, som resulterte i godt over hundre tiltak som de ikke hadde sjans til å gjennomføre påfølgende år, viser manglende etablering og oppfølging av tiltak. De tiltakene som her ble avdekket, men ikke fulgt opp, kan anses som sårbarheter eller hull i «Swiss Cheese-modellen» (Reason, 1997). Manglende oppfølging av tiltak kan også resultere i manglende barrierer.

Tap av sensitiv informasjon kan være et resultat av de manglende sikringsbarrierene som kunne vært etablert hadde ROS-analysen vært oppdatert og relevante barrierer blitt etablert for å møte de truslene som ROS-analysene gav informasjon om. Manglende ROS-analyser og/ eller mangelfull oppfølging av analyser kunne blitt oppdaget under tilsyn av NVE. Her har vi et eksempel på hvordan hull i barrierer (osteskiver) kan lede til en uønsket hendelse. Mangelfulle analyser, manglende oppfølging av analyser og mangelfullt tilsyn av hvordan nettselskaper gjennomfører analyser kan understøtte Dekkers (2006) «new view»-teori hvor han hevder at menneskelige feil gjerne er et symptom på svakheter dypere i systemet.

De ansatte som ikke har kjennskap til hva som er å anse som sensitiv informasjon kan peke i retning av mangelfulle (eller ikke-eksisterende) barrierer som informasjonssikkerhetskurs, kompetanseheving, regler og prosedyrer, administrativ kontroll, sikkerhetsmåned med mer. Disse barrierene kan fungere opplærende og styrke kunnskapen og kompetansen hos ansatte med det resultat at de ansatte kan tenke mer forebyggende, være mer «på hugget» og ha beskyttelse av informasjon «i pannebrasken» (ref. en respondent fra selskap B).

KraftCERT, NorCERT og FSK er eksempler for plattformer for bransjesamarbeid i sektoren. Det kan argumenteres for at bransjesamarbeid fungerer som både forebyggende og beskyttende barrierer ved hjelp av kunnskapsgenerering gjennom møter, foredrag, konferanser, varslingsmailer, samtaler med mer. Læring, erfaring og deling av informasjon er sentralt. I tillegg er dette viktige forum for hendelseshåndtering (beskyttende barriere). Under et CEO-phishing-angrep fra utenlandske aktører fikk ett av mine selskap varsler fra KraftCERT som fanget opp signalene inn mot landet. I slike tilfeller kan bransjesamarbeid fungere som en redundant barriere i et mangfold av fysiske, tekniske og menneskelige

barrierer. Skulle CEO-mailen passere alle brannmurer i et selskap, kan varsler fra KraftCERT hindre en ubevisst leder i å åpne mailen. Det samme argumentet gjelder for phishing-mailer eller liknende som sendes til andre ansatte. I to av tre nettselskaper i denne studien beskrives en mail-ordning hvor de ansatte kan sende en beskjed hvis de er usikre på innholdet i mottatte e-poster. Dette kan virke forebyggende og forhindre uønskede hendelser.

Bransjesamarbeid på tvers i kraftbransjen derfor fungere som en forebyggende og beskyttende barriere. En forutsetning for et godt bransjesamarbeid er imidlertid at det eksisterer en felles bevissthet i bransjen rundt trusler og barrierer for å forhindre uønsket innsyn i sensitiv informasjon.

6.2.3 Oppsummering

Med utgangspunkt i Hollnagels skille mellom forebyggende og beskyttende barrierer (1999), og Reasons inndeling i harde og myke barrierer (1997) kan barrierene kartlagt i nettselskapene i denne studien struktureres som vist i tabell 3. Jeg vil argumentere for at krav fra beredskapsforskriften og tiltak som utkommer av ROS-analyser både kan være av hard og myk karakter, samt både forebyggende og beskyttende.

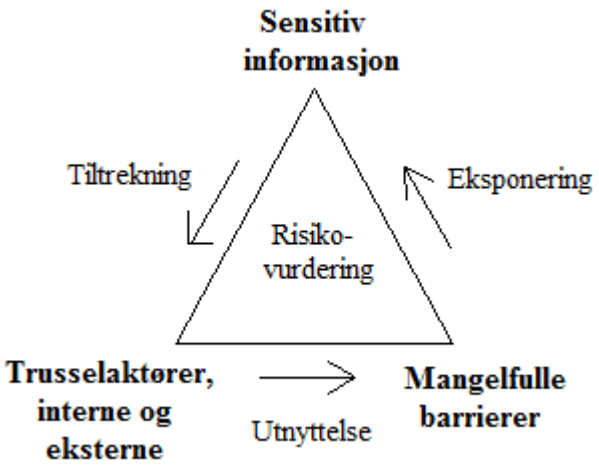
Tabell 3 Harde/myke/forebyggende/beskyttende barrierer

	HARDE BARRIERER	**MYKE BARRIERER**
PREVENT/ FOREBYGGE	Fysiske tiltak: Adgangskontroll (Securitas-personell), gjesteregistrering, fysiske sperringer/ gjerder i inngangsparti, adgangskort for ansatte og besøkskort for gjester, låste dører, safe. Tekniske tiltak: Brannmurer, Intrusion Prevention Systems (IPS), anti-virus, sensornettverk, flerfaktorautentisering, logging.	Interne sikkerhetsinstrukser, eksterne tilsyn fra NVE, internrevisjoner, test-mailer, informasjons-sikkerhetskurs, konferanser, møtevirksomhet, taushetserklæringer, sikkerhetsmåned, bransjesamarbeid.
PROTECT/ BESKYTTE	Logging og logganalyse. Flerfaktorautentisering.	Bransjesamarbeid. Mail-ordning.

Det kan imidlertid argumenteres for at samtlige beskyttende barrierer også har en forebyggende effekt. Har imidlertid et virus eller en e-post med skadevare infisert et datasystem og startet data-lekkasje kan beskyttende barrierer som logging, logganalyser, flerfaktor-autentisering, bransjesamarbeid og mail-ordninger stanse lekkasjen raskt og dermed hindre ytterligere eksponering eller tap av sensitiv informasjon. I tabell 3 er barrierene «satt i

bås» for å strukturere og enklere presentere dem. Det er imidlertid slik at barrierene fungerer om-en-annen i nettselskapene. Videre er trusselbildet dynamisk, i kontinuerlig endring. Dette krever kontinuerlig endring i, og oppdatering av, barrierene. Harde og myke barrierer fungerer i et samspill, både redundante og mangfoldige (Reason, 1997). Redundans skapes gjennom en kombinasjon av duplisering (to enheter som gjør det samme) og overlapping (to enheter med felles funksjonelle område) (Rochlin m.fl., 1987). Det kan argumenteres for at ulike tekniske barrierer kan fungere dupliserende, mens samspillet mellom fysiske, tekniske og menneskelige barrierer til en viss grad kan virke overlappende. Skulle en hacker nå gjennom tekniske barrierer som brannmurer og IPS med en phishing-mail bestående av skadevare, vil bør ansatte med god sikkerhetskunnskap unngå å åpne mailen og melde den til IT-avdelingen. Uvedkommende som kommer seg gjennom de fysiske sperringene i resepsjonen i kontorlokalene til et selskap er brudd i fysiske barrierer. Her kan prosedyrer som krever nedlåsing av sensitiv informasjon kunne hindre den uvedkommende i å få tak i denne informasjonen. I tillegg kan ansatte som har sikkerhetsforståelse langt framme i pannebrasken, reagere på at en ukjent person beveger seg i korridorene uten følge eller adgangskort. Et siste eksempel omhandler ondsinnede innsidere som jobber med etablering av bakdører eller deling av sensitiv informasjon på annen måte. Vedkommende har allerede passert barrierer som er etablert for beskyttelse av ytre vegg. Her vil logger, logganalyser og overvåking av logger kunne avdekke uønsket aktivitet før informasjon har blitt lekket eller bakdører er etablert.

Det kan argumenteres for at mange av de barrierene som kategoriseres som «myke» til dels er iverksatt for å styrke kompetansen hos de ansatte. Etableres det et overordnet fokus på verdi, trusler og sårbarhet, jf. risikotrekanten (NSM, 2016b), kan man argumentere for kollektiv bevissthet rundt både sensitiv informasjon som verdi, rundt interne og eksterne trusselaktører, samt rundt manglende eller mangelfulle barrierer som sårbarhet, jf. figur 8.



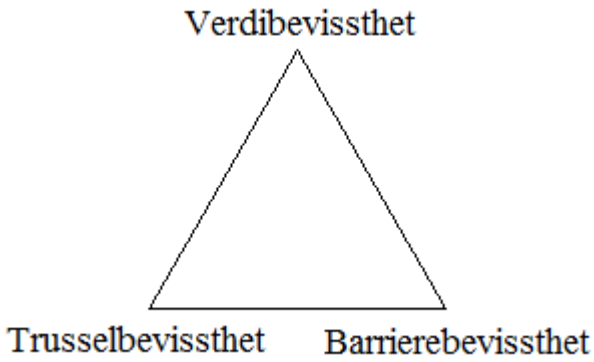
Figur 8 Modifisert versjon av risikotrekanten

Denne modifiserte risikotrekanten tas med til neste underkapittel; kollektiv bevissthet.

6.3 Kollektiv bevissthet

Hvordan er den kollektive bevisstheten mtp. beskyttelse av sensitiv informasjon i nettselskapene og hvordan påvirker dette barrierenes funksjon?

Risikotrekanten (NSM, 2016b) og trefaktormodellen (Engen m.fl., 2016) er som nevnt sentrale for risikoanalyser i forbindelse med tilsiktede, ondsinnede handlinger. Kollektiv bevissthet beskrives av Weick og Sutcliffe som en kapasitet til å oppdage og forstå betydningen av svake signaler, samt effektivt respondere på dem (Weick & Sutcliffe, 2001). I det ligger en forståelse av at det finnes sårbarheter. Opererer man med en form for verdi, noe man vil beskytte, så vil ethvert forhold med potensiale til å forårsake en uønsket hendelse (skade/ta verdien) være trusler. En naturlig respons på en slik risikovurdering vil være å øke bevisstheten rundt trusselen, rundt de verdier som krever beskyttelse, samt rundt hvordan sårbarheten kan reduseres gjennom barrierebygging – som blokkerer trusselaktørers adgang til verdiene (se figur 9).



Figur 9 Bevissthetstrekant

I denne modifiserte bevissthetstrekanten, som er inspirert av trefaktormodellen, er trussel erstattet med trusselbevissthet, sårbarhet er byttet ut med barrierebevissthet og verdi er endret til verdibevissthet. Beskyttelse av sensitiv informasjon, konfidensiell informasjon (DIFI, 2017, 14.3), er en sentral del av informasjonssikkerhet. En respondent fra selskap B forteller at de fleste av hans kollegaer ikke har noe særlig forhold til informasjonssikkerhet og at dette «*…er utenfor det som normalt ligger i pannebrasken [hos de ansatte]*». For å kunne etablere en bevissthet rundt verdiene i et selskap er det behov for en verdigjennomgang. Mange virksomheter har ikke kjennskap til, og oversikt over, alle verdiene de har (NOU2015:13, 2015). En respondent i selskap B forteller at han savner en ordentlig informasjonsklassifisering og gjennomgang av selskapets ressurser, mens en respondent i selskap A mener at mange ansatte ikke vet hvilken informasjon de behandler i hverdagen som er å anse som sensitiv. Dette kan peke i retning av manglende fokus på feil, forenklinger og svekket årvåkenhet eller fokus på operasjoner (Weick & Sutcliffe, 2007). At ansatte i nettselskapene kan anse sitt sikkerhetsarbeid som ubetydelig fordi de ikke arbeider i selskapets sikkerhetsavdeling (uttalt av en respondent i selskap C), tyder også på en forenklet forståelse av sikkerhetsarbeidet i selskapet. I beredskapsforskriften står det imidlertid at sensitiv informasjon skal beskyttes av taushetsplikt, noe som gjelder for enhver (energiloven, 1990; bfe, 2013; NVE, 2013). *Enhver* er alle som måtte få tilgang til sensitiv informasjon om energiforsyningen (NVE, 2013). Det kan argumenteres for at ansatte som ikke vet hva som er taushetsbelagt informasjon heller ikke kan forstå når de selv blir en trussel mot beskyttelse av sensitiv informasjon; på den måten kan mangelfull årvåkenhet resultere i fokus på feil (Weick & Sutcliffe, 2007). Det kan derfor utvikles en arbeidspraksis som avviker fra det som beskrives i beredskapsforskriften, en praksis som kan kategoriseres som stille avvik

(Tinmannsvik, 2008). Et slikt avvik, hvor faktisk arbeidspraksis ikke samsvarer med prosedyrer (Tinmannsvik, 2008) karakteriseres av Reason (1997) som latente forhold, og av Turner (1976) som latente feil. Stille avvik og latente forhold/feil kan innebære at man har et lavere sikkerhetsfokus enn det som er planlagt, en situasjon som øker sårbarheten mtp. trusselaktører. Det kan tenkes at det å sette seg tilstrekkelig inn i beskyttelse av sensitiv informasjon krever noe tid og innsats av hver ansatt, og at dette stiller økte krav til selskapene. Mangel på slik innsats kan medføre at de latente forhold/feil ikke blir oppdaget, at avvikene får anledning til å etablere seg som fast praksis – en praksis som avviker fra etablerte prosedyrer. Dette kan tyde på manglende årvåkenhet, en forenklet forståelse av situasjonen samt mangelfullt fokus på feil (Weick & Sutcliffe, 2007). Dette virker også å være tilfellet ifm. de vurderingene som ble gjort av min respondent som valgte å bruke et fullt utstyrt kontor med lett tilgjengelige papirer og dokumenter - til intervjuer om informasjonssikkerhet med en utenforstående. Er det å anse som avvik innen selskapets informasjonssikkerhetsprosedyrer at den ansatte ikke hadde en oppdatert situasjonsforståelse (Endsley m.fl., 2003) som dekket alle elementene som ligger i et informasjonssikkerhetsmiljø? I så fall tyder også dette på mangelfull årvåkenhet og fokus på feil (Weick & Sutcliffe, 2007).

Verdibevissthet vil være nødvendig for å kunne ha forståelse for *alle elementene i miljøet* (Endsley m.fl., 2003), og bør suppleres med bevissthet om aktuelle trusler for å kunne etablere og opprettholde barrierer. Innen bevissthet om trusler, trusselbevissthet, kan det argumenteres for viktigheten av ROS-analyser som kartlegger farer, trusler, risiko og sårbarhet i selskapene. Samtlige nettselskaper i denne studien gjennomfører ROS-analyser. Det er imidlertid eksempler på manglende oppdateringer av ROS-analyser samt manglende oppfølging av funn som avdekkes i analysene. Dette kan gi avvik som peker i retning av mangelfull trusselbevissthet og barrierebevissthet, samt mangelfull årvåkenhet, forenklinger av situasjonsforståelse og mangelfull opptatthet av feil (Weick & Sutcliffe, 2007). Dette kommer klarere til uttrykk ved at en respondent i selskap B etterlyser en følelse av eierskap til ROS-analysearbeidet. En annen respondent i samme selskap mener selskapet består av mange mindre miljøer hvor alle har fokus på sitt. Trusselbevisstheten blant de ansatte i selskapet kommer av en evne til å se sine egne arbeidsoppgaver i sammenheng med hva de andre gjør i selskapet, at det er en kollektiv tilnærming til årvåkenhet, motstand mot forenkling av aktiviteter (inkludert truslene) og fokus på feil (Weick & Sutcliffe, 2007). Uttalelsen fra en

respondent i selskap C om at ansatte i andre avdelinger enn sikkerhetsavdelingen ikke anser sitt arbeid som betydelig i en sikkerhetssammenheng kan peke i retning av mangelfullt eierskap til ROS-analysearbeidet i selskapet. En manglende evne til å se etter feil og trusler kommer også frem når en respondent i selskap B forklarer at manglende eierskap kan ligge til grunn for at ROS-analysearbeidet fort blir en skrivebordsøvelse som kun gjennomføres fordi den må ligge i skuffen ved tilsyn fra NVE. Dette reduserer årvåkenheten (Weick & Sutcliffe, 2007) til de ansatte og kan medføre en manglende situasjonsforståelse mtp. trusselbildet, men også i forhold til det arbeidet som pågår med å etablere og vedlikeholde barrierer for å møte truslene. En respondent fra selskap C beskriver et samarbeid med Norske Veritas i arbeidet med analysearbeidet. Det kan tenkes at innspill utenfra kan være gunstig i en analyseprosess, så lenge ikke sensitiv informasjon blir spredt til eksterne aktører. Innspill fra konsulenter utenfra kan også redusere eieforholdet til analysene, samt årvåkenheten til de ansatte (Weick & Sutcliffe, 2007).

En overordnet trusselbevissthet i et nettselskap er et sentralt fundament innen sikkerhetsarbeidet som gjøres for å møte truslene selskapet står overfor; gjennom etablering og vedlikehold av barrierer. En overordnet trusselbevissthet er således viktig for en kollektiv barrierebevissthet. En kollektiv barrierebevissthet handler om å tolke informasjon og situasjon (Turner, 1976), og på den måten være tilstede i «nuet» (Weick m.fl., 1999) når det gjelder behov for, og feil i, barrierer. Også her er ROS-analyser et tema. Respondenter fra flere selskaper forklarer at ROS-analyser gjennomføres, for så å puttes i en skuff. Noen tiltak implementeres, men de dør bort etterhvert. Dette kan tyde på mangelfullt fokus på feil og mangelfull årvåkenhet (Weick & Sutcliffe, 2007), samt mangler ved informasjonsprosesseringen (Turner, 1976) i selskapene. Det kan også tyde på at tilsynsbarrieren ikke fungerer tilfredsstillende. En respondent fra selskap B forteller at ROS-analyser er en læringsprosess, men at hvis man ikke lærer av prosessen eller tar funnene til etterretning så blir det kun en skrivebordsøvelse. Hvis ROS-analysene ikke oppdateres hyppig nok, eller funnene ikke jobbes med, kan det tenkes at nødvendige barriereetableringer og -oppgraderinger ikke blir utført.

Systemer er ikke trygge i utgangspunktet, og sikkerhet må skapes (Dekker, 2006). Samtlige nettselskaper opererer med myke barrierer som for eksempel interne prosedyrer og regler. Nettselskapene har for eksempel inngangskontroller i sine kontorbygg og regler for å begrense adgangen til eksterne gjester. Disse barrierene vil imidlertid ikke fungere

tilfredsstillende om barrierebevisstheten rundt dem er mangelfull. Igjen kan vi vende tilbake til mitt eksempel hvor jeg fikk anledning til å sitte alene på et kontor i et av selskapene. Dette kan tyde på mangelfull årvåkenhet og fokus på feil (Weick & Sutcliffe, 2007), en mangelfull bevissthet rundt de barrierer som er etablert for å forhindre eksterne aktørers frie adgang til innsiden i kontorbygget deres. Dette kan også være et eksempel på manglende trusselbevissthet som igjen påvirker barrierebevisstheten. Dekker beskriver «the local rationality principle» hvor folk ofte gjør fornuftige valg gitt egen kunnskap, oppmerksomhet og mål (Dekker, 2006). Hvis min kontaktperson i dette selskapet tenkte at bruk av kontoret var fornuftig, kan det kanskje peke på ufullstendige regler/prosedyrer i selskapet, eller manglende strukturer for å styrke ansattes årvåkenhet. Dette kan relateres til det Dekker (2000) kaller «the New view», at menneskelige feil er symptomer på trøbbel dypere i systemet (Dekker, 2000).

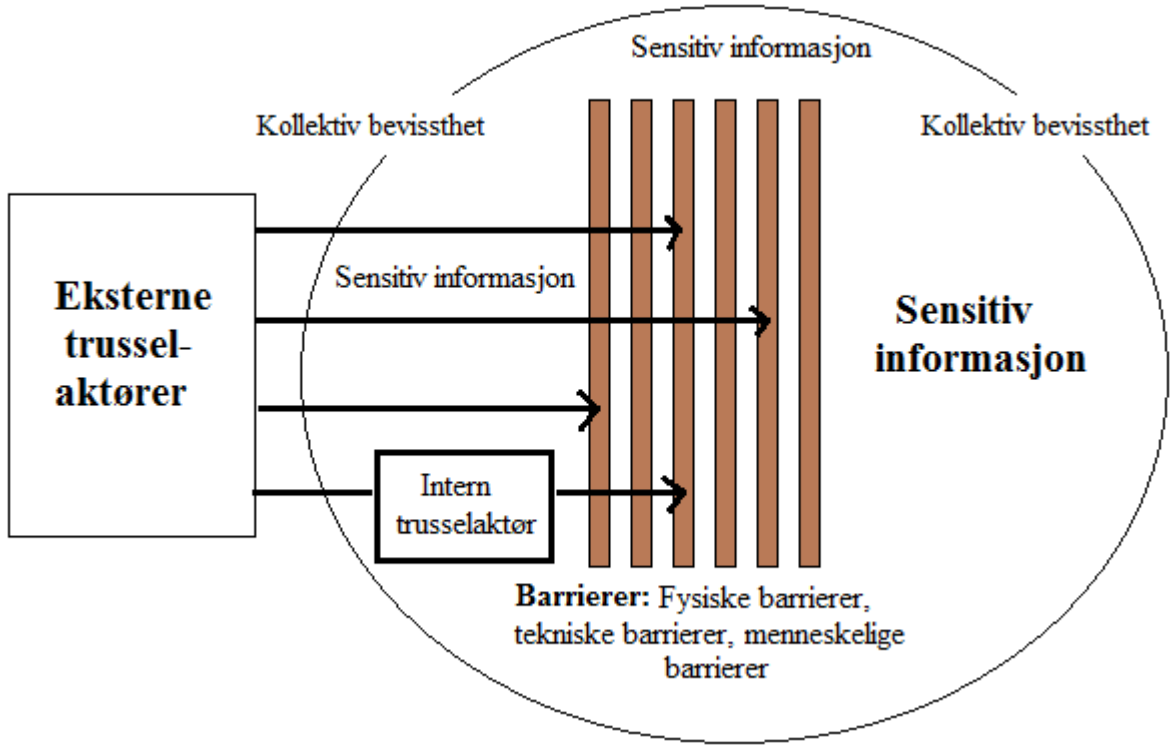
Videre beskriver samtlige selskaper bevissthetsstyrkende tiltak og risikoanalyser som skal forhindre feil og sørge for bedre håndtering og læring i etterkant av de feil som er gjort. Avvik og rapportering både internt i nettselskapene og eksternt (NVE) peker på at det er fokus på feil (Weick & Sutcliffe, 2007). NVE skal sjekke at kravene i beredskapsforskriften tas seriøst. Avvik noteres, tas til etterretning i selskapene og lukkede avvik bekreftes. Det er fokus på bransjesamarbeid og deling av kunnskap og kompetanse, det satses på bevissthetsstyrkende tiltak som sikkerhetsmåned og informasjonssikkerhetskurs og det planlegges ytterligere sikkerhetsrelaterte aktiviteter for å øke kompetanse og bevissthet blant ansatte. Dette peker på et ønske om læring, kompetanseheving, fokus på feil med mer som kan styrke ansattes evne til å forstå svake feilsignaler og svare på dem (Weick & Sutcliffe, 2001). En respondent fra selskap C uttrykker et ønske om også å fokusere på det som går bra; «*…vi fokuserer veldig på de tingene som går galt. Men hva med alt som går bra? Hvorfor går det bra*?». Mine respondenter snakker om daglige angrep[28], og en respondent i selskap B beskriver en evne til improvisering som er utviklet takket være erfaring med hendelseshåndtering over tid. Dette kan være et eksempel på tilstedeværelse og gode responser på de utfordringer selskapene daglig står ovenfor (Weick & Sutcliffe, 2007), i tillegg til god årvåkenhet og evne til resiliens (Weick & Sutcliffe, 2007). Ettersom nettselskapene utsettes for hyppige angrep, og vi sjelden hører om alvorlige tap av sensitive data i norske nettselskaper, kan det peke på at

[28] CryptoLocker, phishing, spear-phishing mm.

respondenter i denne studien har rett når de argumenterer for at den norske kraftbransjen er flinke til å motstå angrep og gjenopprette gjenopprette (bounce back) driften etter uønskede hendelser. En respondent fra selskap B beskriver de ansatte som selskapets ytre forsvar. I selskap B beskrives en test-mail som ble sendt til ansatte i selskapet. Hele 90 % av de ansatte valgte ikke å åpne mailen. Dette tester de ansattes årvåkenhet og gjør selskapene som helhet mer motstandsdyktige (Weick & Sutcliffe, 2007). Det kan argumenteres for et fokus på mental øving, utvikling av responsferdigheter og læring, noe som igjen kan øke de ansattes, og derigjennom selskapets, resiliens (Weick & Sutcliffe, 2007). Dette viser evne til å forstå viktigheten av god årvåkenhet rundt ugunstige mailer og viktigheten av ikke å åpne disse, jf. trusselbevissthet. Trening og øvelser kan øke de ansattes kompetanse (Weick & Sutcliffe, 2007) og således bidra til å gjøre kunnskapsrike ansatte til en barriere skulle phishing-mailer passere tekniske sikkerhetsbarrierer som brannmurer og IPS.

6.4 Oppsummering av drøfting

Kollektiv bevissthet beskrives som en kapasitet til å oppdage og forstå betydningen av svake signaler, samt effektivt respondere på dem (Weick & Sutcliffe, 2001). I dette ligger det en anerkjennelse av at verden er dynamisk. Et selskap må således ta på alvor det dynamiske trusselbildet, samt etablere barrierer som kan møte de trusler som kommer ut av analysene. Den kollektive bevisstheten i selskapet må bygges på en bevissthet rundt selskapets verdier, samt trusselbildet og barriereetablering. Trusselbevissthet kan forstås som en kapasitet til å oppdage trusler og opprettholde kunnskap om mulige uønskede handlinger og/eller hendelser. Her kan det argumenteres for trusselbevissthet rundt både interne og eksterne trusler, noe som inkluderer en forståelse for at en selv kan være en trussel. Barrierebevissthet kan forstås som en kapasitet til å iverksette og opprettholde nødvendige barrierer for å møte uønskede handlinger og/eller hendelser. Barrierebevissthet i denne forståelse bygger derfor på trusselbevissthet. Det kan derfor argumenteres for at kollektiv bevissthet har en overordnet rolle innen beskyttelse av sensitiv informasjon, se figur 10.



Figur 10 Beskyttelse av sensitiv informasjon ved hjelp av kollektiv bevissthet og barrierer

Den kollektive bevisstheten er en evne hos de ansatte og hos selskapet som helhet, en evne til å se det store trussel- og barrierebildet i relasjon til de verdier som må beskyttes (for eksempel sensitiv informasjon). Dette inkluderer eksterne forhold (trusler) og interne forhold (trusler, barrierer og verdier). Dette illustreres i figur 10 ved vilkårlig plassering av «kollektiv bevissthet» på grensen mellom inndelingen i interne og eksterne forhold. Videre defineres sensitiv informasjon som alle opplysninger som kan brukes til å skade selskapet eller selskapets aktiviteter, og det kan argumenteres for at slik informasjon finnes i hele selskapet, men at den mest kritiske informasjonen (**fet skrift**) beskyttes av mange redundante og mangfoldige barrierer.

7. KONKLUSJON

7.1 Problemstilling og forskningsspørsmål

Hvordan bruker så norske nettselskaper barrierer for å forhindre uønsket innsyn i sensitiv informasjon og hvordan påvirker de ansattes kollektive bevissthet barrierenes funksjon?

Kraftbransjens høyeste mål er forsyningssikkerhet, nemlig trygg og pålitelig strømforsyning. Påliteligheten til strømleveransen i Norge er god. Det kan tyde på at det gjøres en del godt arbeid innen beskyttelse av sensitiv informasjon, informasjon som kan brukes av trusselaktører til å skade kraftbransjen. Barrierer etableres for at trusselaktører skal holdes ute. Nettselskapene i denne studien opererer med fysiske, tekniske og operasjonelle barrierer som fungerer i et samspill hvor mangfoldighet og redundans er stikkord som gjør beskyttelsen av sensitiv informasjon mer robust. For at barrierene skal være relevante og holde, og dermed beskytte sensitiv informasjon, må ansatte i kraftbransjen ha en kollektiv bevissthet med hensyn til både verdier som skal beskyttes, trusler mot disse verdiene og relevante barrierer for å forhindre at trusselaktører får tilgang til de beskyttelsesverdige verdiene.

Denne studien viser at ansattes kollektive bevissthet er av avgjørende betydning for harde, myke, forebyggende og beskyttende barrierers funksjon. Etablering og opprettholdelse av barrierer er utfordrende om de ansatte i nettselskapene ikke er bevisste på verdiene som må beskyttes, samt på det trusselbildet som til enhver tid foreligger.

Denne studien viser at det, blant nettselskapene, finnes usikkerhet om verdier som skal beskyttes, om truslene rettet mot disse verdiene og om barrierer som skal møte truslene og dermed beskytte verdiene. Det fremkommer at ansatte ikke vet hva som er sensitive data og det etterlyses verdigjennomganger. Videre er det kartlagt usikkerhet blant de ansatte rundt truslene i bransjen. Truslene kan være både interne og eksterne, og trusselbildet endres kontinuerlig i takt med digitalisering og teknologisk utvikling. Samtlige selskaper er pålagt å gjennomføre ROS-analyser for å kartlegge farer, trusler, risiko og sårbarhet. Respondenter i denne studien beskriver ROS-analyser som sjeldent oppdateres, manglende oppfølging av funn i ROS-analysene, manglende eierskap til ROS-analyser samt en tanke om at arbeidet med ROS-analyser er rutinepreget og kjedelig. Dette kan gjøre at ROS-arbeidet får mindre oppmerksomhet enn hva som er nødvendig, noe som kan svekke ansattes trusselbevissthet.

Barrierebevissthet, en kapasitet til å iverksette og opprettholde nødvendige barrierer for å møte uønskede handlinger/hendelser, må ses i sammenheng med verdi- og trusselbevissthet.

Manglende kunnskap og kompetanse, mangler i ROS-arbeid, åpning av ugunstige mailer, mangelfull følging av besøkende osv. kan peke i retning av forbedringspotensial også innen barrierebevissthet. Når det er sagt avdekker denne studien også at bransjen er under kontinuerlige digitale angrep fra ondsinnede utsidere og at det jobbes mye med verdi-, trussel- og barrierebevissthet gjennom sikkerhetskurs for nyansatte, tester, øvelser, bransjesamarbeid med mer. Det er av største betydning at kraftbransjens ansatte har fokus på sikring av sensitive data *helt fremst i pannebrasken*!

7.2 Forslag til videre forskning

Diskusjoner rundt sensitiv informasjon, sikker strømforsyning og intenderte angrep (spesielt digitale) er viktige, og vil bli viktigere i årene som kommer. Jeg oppfordrer derfor til videre forskning på disse temaene! Jeg vil også anbefale videre forskning på den kollektive bevisstheten blant de vanlige ansatte i den spisse enden i kraftbransjen, gjerne en kvantitativ undersøkelse med konkrete spørsmål om trusselbevissthet, verdibevissthet og barrierebevissthet. Et relevant tema som ble diskutert med mine intervjuobjekter, men som ike ble beskrevet i denne oppgaven, er AMS (smarte strømmålere) og beskyttelse av sensitiv informasjon. De smarte strømmålerne er på god vei inn i norske husstander og bedrifter, og innen 1. januar 2019 vil alle være på plass. Strømmålerne er svært nøyaktige og innrapporterer strømforbruket hver time (med mulighet for enda hyppigere innrapportering). En husholdnings strømbruk følges dermed til punkt og prikke; når står førstemann opp om morgenen? Når er huset tomt? Når settes det på en vaskemaskin? At slik informasjon blir så spesifikk og er tilgjengelig for andre enn dem i husholdningen reiser en del spørsmål, også etiske, som kan danne grunnlag for forskning. Videre er etableringen av ElHub interessant. ElHub er en IKT-løsning for informasjonsutveksling mellom aktørene i kraftmarkedet hvor mye informasjon vil samles på ett sted. Hvilke utfordringer finnes her? Dette har jeg i liten grad inkludert i min oppgave, men i ettertid tenker jeg at dette kunne vært spennende å gå dypere inn i. I tillegg har flere av mine respondenter frontet diskusjoner ved sikkerheten rundt bruk av skytjenester og outsourcing. Her ligger det svært aktuelle forskningsmuligheter.

Som en konkret oppfølging av egne funn anbefaler jeg videre forskning på ROS-analyser som metode. Er dette effektivt? Flere av mine respondenter peker på rutinepreg og ineffektivitet når ROS diskuteres. Et større forskningsprosjekt vil kunne se på dette, og gjerne i sammenheng med trusselbevissthet, barrierebevissthet og bevissthet i forhold til sensitiv informasjon (dvs. verdibevissthet).

8. REFERANSELISTE

Albrechtsen, E. & Grøtan, T.O. (2004). Gammeldags tenkning i moderne organisasjoner? Om IKT-sikkerhet i kunnskapsorganisasjoner. I Lydersen, S. (Red.), *Fra flis i fingeren til ragnarokk*. (s. 335-355). Trondheim: Tapir Akademisk.

Andersen, S., Øberg, M. M., Veila, S., Sundheim, H. (2014). *Energiskolen; Lærehefte*. Statnett. Hentet fra http://www.statnett.no/Global/Dokumenter/Milj%C3%B8%20og%20samfunn/Energiskolen/statnett_l%C3%A6rehefte_oppslag.pdf

Aven, T., Ben-Haim, Y., Andersen, H. B., Cox, T., Droguett, E. L., Greenberg, M., Guikema, S., Kroeger, W., Renn, O., Thompson, K. M. & Zio, E. (2015). The Council of the Society for Risk Analysis (SRA). *Committee on Foundations of risk analysis: SRA glossary*. Hentet fra http://www.sra.org/sites/default/files/pdf/SRA-glossary-approved22june2015-x.pdf

Badreddine, A., Ben Romdhane, T., Aymen Ben HajKacem, M., Ben Amor, N. (2014). A new multi-objectives approach to implement preventive and protective barriers in bow tie diagram. *Journal of Loss Prevention in the Process Industries.* 32(2014). 238-253. Hentet fra: http://ac.els-cdn.com/S0950423014001557/1-s2.0-S0950423014001557-main.pdf?_tid=13d567c4-281b-11e7-b7ae-00000aacb361&acdnat=1492948422_1e77957e1fc7b127aacad2a3f0e79956

Barstad, L. S. J. J. (2016). *Etablering av beredskap på IKT-sikkerhet i energiforsyningen*. (Mastergradsavhandling). UiS. Stavanger. Hentet fra https://brage.bibsys.no/xmlui/bitstream/handle/11250/2423619/Barstad_Linn_Soo_Jin_Jeanette.pdf?sequence=3

Bartnes, M., Moe, N. B. & Heegaard, P. E. (2016). The future of information security incident management training: A case study of electrical power companies. *Computers & Security*. *Science Direct*. 61(2016). 32-45. Hentet fra http://ac.els-cdn.com/S0167404816300530/1-s2.0-S0167404816300530-main.pdf?_tid=c9fed5fa-a8ad-11e6-9739-00000aacb360&acdnat=1478937685_5d34ca988691372e7223e649a156cdab

Beck, U. (1992). *Risk Society; Towards a New Modernity*. London: Sage Publications Ltd.

Bento, J-P. (2001). Menneske – teknologi – organisasjon. Veiledning for gjennomføring av MTO-analyser. I *kurskompendium for Petroleumstilsynet*. Oljedirektoratet.

Beredskapsforskriften. (2013). *Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften).* Hentet fra https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157

Bhamra, R., Dani, S. & Burnard, K. (2011). Resilience: the concept, a literature review and future directions. *International Journal of Production Research.* 49(18). 5375–5393. Hentet fra https://www.researchgate.net/publication/233227061_Resilience_The_Concept_a_Literature_Review_and_Future_Directions

Blaikie, N. (2010). *Designing social research.* UK: Polity.

Brekke, A. (2016, 25.6). Slår alarm om løsepengevirus. *NRK*. Lest 12.4.17. Hentet fra https://www.nrk.no/norge/slar-alarm-om-losepengevirus-1.13012359

Britton, N. R. (1989). *Constraint or Effectiveness in Disaster Management? The Bureaucratic Imperative Versus Organizational Mission*. Sydney: The university of Sydney. Hentet fra http://cidbimena.desastres.hn/docum/crid/Febrero2005/pdf/eng/doc192/doc192-a.pdf

Choo, K-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*. 30(8). 719-731. Hentet fra http://ac.els-cdn.com/S0167404811001040/1-s2.0-S0167404811001040-main.pdf?_tid=201d37b4-a981-11e6-8a25-00000aab0f02&acdnat=1479028453_108ce4edc4300422c02000dcc2065073

Computenext. (2013). *When to use SaaS, PaaS, and IaaS*. Lest 26.5.17. Hentet fra https://www.computenext.com/blog/when-to-use-saas-paas-and-iaas/

Dekker, S. (2000). *The Field Guide to Human Error*. Draft, august 2000. Hentet fra http://www.leonardo-in-flight.nl/PDF/FieldGuide%20to%20Human%20Error.PDF

Dekker, S. (2006). *The Field Guide to Understanding Human Error*. Aldershot: Ashgate.

Dhillon, G. & Backhose, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*. 11(2). 127-153.

DIFI. (2016, 16.6). *Skytjenester (cloud) - offentlig anskaffelse av skytjenester*. Lest 23.5.17. Hentet fra https://www.anskaffelser.no/it/temaer-it/skytjenester-cloud

DIFI. (2017). *Informasjonssikkerhet*. Lest 14.3.17. Hentet fra https://www.difi.no/fagomrader-og-tjenester/informasjonssikkerhet

DNV. (2013, 9.4). DNV GL - Software launches a complete risk management solution. Lest 18.5.17. Hentet fra https://www.dnvgl.com/news/dnv-gl-software-launches-a-complete-risk-management-solution-28589

DSB. (2016). *Samfunnets kritiske funksjoner. Hvilken funksjonsevne må samfunnet opprettholde til enhver tid?* (DSB RAPPORT. Versjon 1.0). Hentet fra https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-2_januar.pdf

Dynes, R. (1974). *Organized Behavior in Disasters*. Delaware: Disaster Research Center.

Dynes, R. (1994). Community Emergency Planning: False Assumptions and Inappropriate Analogies. *International Journal of Mass Emergencies and Disasters*. 12(2). 141-158.

E-ISAC. (2015). *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Washington DC. Hentet fra https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Endsley, M. R., Bolté, B. & Jones, D. G. (2003). *Designing for situation awareness: An Approach to User-Centered Design*. USA: CRC Press, Taylor & Francis Group.

Energiloven. (1990). *Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven)*. Hentet fra https://lovdata.no/dokument/NL/lov/1990-06-29-50

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

ENISA. (2017a). *ENISA Threat Landscape Report 2016: 15 Top Cyber-Threats and Trends*. (Final version 1.0. ETL 2016). Januar 2017. Hentet fra https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

ENISA. (2017b). About ENISA. Hentet fra https://www.enisa.europa.eu/about-enisa

Ernst & Young. (2011). Data loss prevention; Keeping your sensitive data out of the public domain. *Insights on governance, risk and compliance*. Hentet fra http://www.ey.com/Publication/vwLUAssets/EY_Data_Loss_Prevention/$FILE/EY_Data_Loss_Prevention.pdf

Etterretningstjenesten. (2016). *FOKUS 2016: Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer*. Hentet fra https://forsvaret.no/fakta_/ForsvaretDocuments/Fokus%202016.pdf

Farwell, J. P. & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival*. 53(1). 23-40. Hentet fra http://www.tandfonline.com/doi/pdf/10.1080/00396338.2011.555586?needAccess=true

FFI. (2015, 25.2). Beskyttelse av samfunnet. Lest 15.5.17. Hentet fra https://www.ffi.no/no/Forskningen/Avdeling-Beskyttelse/BAS/Sider/default.aspx

Fornybar. (2016). Energimarkedet. Lest 17.3.17. Hentet fra http://www.fornybar.no/kraftmarkedet#markedet2

Fridheim, H., Hagen, J. & Henriksen, S. (2001). *EN SÅRBAR KRAFTFORSYNING; Sluttrapport etter BAS3*. (FFI/RAPPORT-2001/02381). Hentet fra http://www.ffi.no/no/Rapporter/01-02381.pdf

Ghauri, P. N. & Grønhaug, K. (2002). *Research Methods in Business Studies; A Practical Guide* (2. utgave). London: FT Prentice Hall Europe.

Haddon, W. (1980). The Basic Strategies For Reducing Damage From Hazards of All Kinds. *Hazard Prevention*.

Hagen, J. (2015). *Teknologiskifte i energiforsyningen; Studie om muligheter og sårbarheter*. (Rapport nr 118-2015). NVE. Hentet fra http://publikasjoner.nve.no/rapport/2015/rapport2015_118.pdf

Hagen, J., Albrechtsen, E. & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*. 16(4). 377 – 397. Hentet fra http://www.emeraldinsight.com/doi/pdfplus/10.1108/09685220810908796

Hagen, J., Fridheim, H. & Nystuen, K. O. (2005). New challenges for emergency preparedness in the information society. *Telektronikk.* 101(1). 48-54.

Hagen, J., Hermansen, O., Toftegård, Ø., Pettersen, J.-M., Steen, R., Paulsen, S. L. (2017). *Regulering av IKT- sikkerhet: Et helhetlig og fremtidsrettet sikkerhetsregime for forsyningssikkerhet i en digitalisert energisektor*. (26-2017). NVE. Hentet fra http://publikasjoner.nve.no/rapport/2017/rapport2017_26.pdf

Hollnagel, E. (1999). *Accident Analysis and Barrier Functions*. Project TRAIN. Hentet fra https://www.it.uu.se/research/project/train/papers/AccidentAnalysis.pdf

Hollnagel, E. (2004). *Barrier and accident prevention*. UK: Ashgate

Hollnagel, E., Woods, D. D. & Leveson, N. C. (2006). *Resilience engineering: Concepts and precepts*. UK: Ashgate.

Hovden, J. (2004). Sikkerhet i forskning og praksis: Et utfordrende mangfold med Sikkerhetsdagene som arena. I Lydersen, S., Albrechtsen, E., Hovden, J., Sklet, S. (Red.), *Fra flis i fingeren til ragnarokk* (31-50). Trondheim: Tapir Akademiske Forlag.

Hovland, K. (2017). *Logging og logganalyse i energiforsyningen* (Studentrapport, nr. 1-2017). NVE. Lest 1.2.17. Hentet fra http://publikasjoner.nve.no/rapport/2017/rapport2017_01.pdf

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

Jajodia, S., Liu, P., Swarup, V. & Wang, C. (Red.). (2010). *Cyber Situational Awareness: Issues and Research.* New York: Springer. Hentet fra http://download.springer.com/static/pdf/334/bok%253A978-1-4419-0140-8.pdf?originUrl=http%3A%2F%2Flink.springer.com%2Fbook%2F10.1007%2F978-1-4419-0140-8&token2=exp=1478936876~acl=%2Fstatic%2Fpdf%2F334%2Fbok%25253A978-1-4419-0140-8.pdf%3ForiginUrl%3Dhttp%253A%252F%252Flink.springer.com%252Fbook%252F10.1007%252F978-1-4419-0140-8*~hmac=635219d6b8258efd5088b4243d929827e78864a8b048beed7551a8096b2fba74

Jansrud, J. (2013, 14.3). Kraftleverandør og nettselskap, hva er forskjellen? Gudbrandsdal Energi. Hentet fra https://www.ge.no/2013/03/14/kraftleverandor-og-nettselskap-hva-er-forskjellen/

Johansen, P. A. (2016, 15.1). De sa det var umulig. Nå klarer russiske hackere å slå av strømnettet. *Aftenposten*. Lest 9.2.17. Hentet fra http://www.aftenposten.no/verden/De-sa-det-var-umulig-Na-klarer-russiske-hackere-a-sla-av-stromnettet-13199b.html

Johnson, E.C. (2006). Security awareness: switch to a better programme. *Science Direct*. 2006(2). 15–18. Hentet fra http://ac.els-cdn.com/S1353485806703373/1-s2.0-S1353485806703373-main.pdf?_tid=e121a47c-a67a-11e6-81c5-00000aacb35d&acdnat=1478695917_1bb155c1f09b6dd584d2a11b83766193

Kjellén, U. (2000). *Prevention of accidents through experience feedback*. London/ New York: Taylor & Francis.

Kjellén, U. & Albrechtsen, E. (2017). *Prevention of Accidents and Unwanted Occurrences: Theory, Methods, and Tools in Safety Management*. NW: Taylor & Francis.

KraftCERT. (2015). KraftCERT. Lest 12.5.17. Hentet fra https://www.kraftcert.no/

Kruke, B. I., Olsen, O. E., Hovden, J. (2005). Samfunnssikkerhet – forsøk på en begrepsfesting. ISBN: 82-490-0347-0

Kruuse, E. (1996). *Kvalitative forskningsmetoder: I psykologi og beslægtede fag*. København: Dansk psykologisk Forlag.

Kushner, D. (2013). The Real Story of Stuxnet. Hentet fra http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

Kvale, S. (1996). *InterViews: An Introduction to Qualitative Research Interviewing*. CA: Sage Publications.

Kvale, S. (2002). *Det kvalitative forskningsintervju.* Oslo: Gyldendal Norsk Forlag AS.

Kvale, S. & Brinkmann, S. (2009). *Det kvalitative forskningsintervju*. 2. utg. Oslo: Gyldendal Akademisk.

LaPorte, T. R. (1994). A strawman speaks up: Comments on The Limits of Safety. *Journal of Contingencies and Crisis Management.* 2(4). 207-211. Hentet fra http://onlinelibrary.wiley.com/doi/10.1111/j.1468-5973.1994.tb00045.x/epdf

LaPorte, T. R. & Consolini, P. M. (1991). Working in Practice but Not in Theory: Theoretical Challenges of "High-Reliability Organizations". *Journal of Public Administration Research and Theory*. 1(1). 19-48.

Line, M. B. (2015). *Understanding information security incident management practices; A case study in the electric power industry*. (Doktorgradsavhandling). NTNU. Trondheim.

Mathisen, J. (2004). *Measuring Information Security Awareness – A survey showing the Norwegian way to do it*. (Mastergradsavhandling). Stockholms Universitet, Kungl Tekniska Högskolan, Høgskolen i Gjøvik. Hentet fra https://brage.bibsys.no/xmlui//bitstream/handle/11250/143904/1/Mathisen_-_Measuring_information_security_awareness.pdf

Meld. St. 37 (2014-2015). (2015). *Globale sikkerhetsutfordringer i utenrikspolitikken: Terrorisme, organisert kriminalitet, piratvirksomhet og sikkerhetsutfordringer i det digitale rom*. Oslo: Det kongelige utenriksdepartementet. Hentet fra https://www.regjeringen.no/contentassets/bdf4bd40d57d4dc79409de87419a2217/no/pdfs/stm201420150037000dddpdfs.pdf

Merton, R. K. (1936). The Unanticipated Consequences of Purposive Social Action. *American Sociological Review*. 1(6). 894-904. Hentet fra https://pdfs.semanticscholar.org/dc9f/6f377a93108e8ad73be1e9c0111428a5a8b9.pdf

Mitnick, K.D. & Simon, W.L. (2002). *The art of deception – controlling the human element of security*. Indiana: Wiley Publishing, Inc.

Neuman, W. L. (2000). *Social Research Methods; Qualitative and Quantitative Approaches*. (4 utg). Boston: Allyn and Bacon.

NorSIS. (2014, 8.9). Nasjonal sikkerhetsmåned i oktober. Lest 29.4.17. Hentet fra https://norsis.no/nasjonal-sikkerhetsmaned-oktober/

NOU 2006:6. (2006). *Når sikkerheten er viktigst: Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner*. Oslo: Departementenes servicesenter. Informasjonsforvaltning. Hentet fra https://www.regjeringen.no/contentassets/c8b710be1a284bab8aea8fd955b39fa0/no/pdfs/nou20062006000600dddpdfs.pdf

NOU 2015:13. (2015). *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden*. Oslo: Departementenes sikkerhets- og serviceorganisasjon. Informasjonsforvaltning. Hentet fra https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou20152015013000dddpdfs.pdf

NSM. (2012). Nettfisking og sosial manipulasjon [brosjyre]. Hentet fra https://www.nsm.stat.no/globalassets/dokumenter/brosjyrer/phishing_nyn_web.pdf

NSM. (2015a). *RISIKO 2015; Nasjonal sikkerhetsmyndighet*. (NSM RISIKO 2015). Hentet fra https://www.nsr-org.no/getfile.php/Dokumenter/Eksterne%20publikasjoner/NSM_Rapportomsikkerhet_2015-WEB-oppslag.pdf

NSM. (2015b). *Kappløp om sikkerhet. Årsrapport 2015*. (NSM ÅRSRAPPORT 2015). Hentet fra https://www.nsm.stat.no/globalassets/rapporter/arsrapporter/nsm-2015-nett-oppslag-endelig.pdf

NSM. (2016a). *Helhetlig IKT-risikobilde 2016*. (HELHETLIG IKT-RISIKOBILDE 2016). Hentet fra https://www.nsm.stat.no/globalassets/rapporter/nsm_helhetlig_ikt_risikobilde_2016_web_enkel.pdf

NSM. (2016b). *RISIKO 2016; Kan sikkerhet styres? En vurdering av sårbarheter og risiko i Norge*. (RISIKO 2016). Hentet fra https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2016.pdf

NSM. (2017a). Varslingssystem for digital infrastruktur (VDI). Hentet fra https://nsm.stat.no/norcert/varslingssystem-for-digital-infrastruktur-vdi/

NSM. (2017b). *Risiko 2017: Risiko og sårbarheter i en ny tid. En vurdering av sårbarheter og risiko i Norge*. (NSM RISIKO 2017). Hentet fra http://www.asis.no/pdf-dokumenter/nsm_risiko_2017_lr_2703_enkelts.pdf

NSM. (2017c). *Norges nasjonale cybersenter – NorCERT*. Lest 15.4.17. Hentet fra https://nsm.stat.no/norcert

NSR. (2015). *Kriminalitets- og sikkerhetsundersøkelsen i Norge*. Hentet fra https://www.nsr-org.no/getfile.php/Dokumenter/NSR%20publikasjoner/Krisino/krisino_2015_utskrift.pdf

NSR. (2016). *Mørketallsundersøkelsen 2016 – Informasjonssikkerhet, personvern og datakriminalitet*. Lest 9.11.16. Hentet fra http://www.nsr-org.no/getfile.php/Bilder/M%C3%B8rketallsunders%C3%B8kelsen/morketallsundersokelsen_2016.pdf

NS 5830:2012. *Samfunnssikkerhet: Beskyttelse mot tilsiktede uønskede handlinger; Terminologi.* Oslo: Standard Norge.

NVE. (2013). *Veiledning til forskrift om forebyggende sikkerhet og beredskap i energiforsyningen* (Veileder nr. 1-2013). Hentet fra http://publikasjoner.nve.no/veileder/2013/veileder2013_01.pdf

NVE. (2016a). *IKT-systemers rolle og betydning for strukturen i kraftbransjen; Konsulentrapport utarbeidet for NVE*. (Rapport nr 32-2016). Hentet fra http://publikasjoner.nve.no/rapport/2016/rapport2016_32.pdf

NVE. (2016, 15.4). Kraftforsyningens beredskapsorganisasjon (KBO). Lest 6.2.17. Hentet fra https://www.nve.no/damsikkerhet-og-energiforsyningsberedskap/energiforsyningsberedskap/organisering-av-energiforsyningsberedskap/kraftforsyningens-beredskapsorganisasjon-kbo/

NVE. (2017, 27.3). Energiforsyningen må ha god oversikt over hva som skjer i sine digitale systemer. Lest 25.5.17. Hentet fra https://www.nve.no/nytt-fra-nve/nyheter-sikkerhet-og-energiforsyningsberedskap/energiforsyningen-ma-ha-god-oversikt-over-hva-som-skjer-i-sine-digitale-systemer/

Nygård, A. R. (2002). *Risk management in SCADA-system*. (Mastergradsavhandling). Stockholms Universitet, Kungl Tekniska Högskolan, Høgskolen i Gjøvik. Hentet fra https://brage.bibsys.no/xmlui/bitstream/handle/11250/143918/nyg%C3%83%C2%83%C3%82%C2%A5rd_-_Risk_management_in_SCADA-_system.pdf?sequence=1&isAllowed=y

OED. Olje- og energidepartementet. (2015). *Fakta 2015: Energi- og vassdragsressurser i Norge*. Hentet fra https://www.regjeringen.no/contentassets/fd89d9e2c39a4ac2b9c9a95bf156089a/1108774830_897155_fakta_energi-vannressurser_2015_nett.pdf

Perrow, C. (1999). *Normal Accidents. Living with High-Risk Technologies*. New Jersey: Princeton University Press.

Pettersen, K. A. & Schulman, P. (2016). Drift, adaptation, resilience and reliability: Toward an empirical clarification. *Safety Science*. Hentet fra http://ac.els-cdn.com/S0925753516300108/1-s2.0-S0925753516300108-main.pdf?_tid=6bb63f2a-460e-11e7-b06b-00000aacb35f&acdnat=1496241521_764bfe28887230567611c15886760bd8

Rasmussen, J. (1997). Risk Management in a Dynamic Society: A Modelling Problem. *Safety Science*. 27(2/3), 183-213.

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

Regjeringen. (2014, 13.12). *Hvor skal offentlig sektor lagre og behandle data?* Hentet fra https://www.regjeringen.no/no/tema/statlig-forvaltning/ikt-politikk/hvor-skal-offentlig-sektor-lagre-og-behandle-data/id2353784/

Roberts, K. H., Stout, S. K., Halpern, J. J. (1994). Decision Dynamics in Two High Reliability Military Organisations. *Management Science*. 40(5). 614 – 624.

Rochlin, G. I., LaPorte, T. R., Roberts, K. H. (1987). The Self-Designing High-Reliability Organization: Aircraft Carrier Flight Operations at Sea. *Naval War College Review.* 51(3). 207-211.

Rollenhagen, C. (1997). Sambanden manniska, teknik och organisation - en introduktion. Utbildningshuset studentlitteratur.

Rosness, R., Guttormsen, G., Steiro, T., Tinmannsvik, R. K., Herrera, I. A. (2004). *Organisational Accidents and Resilient Organisations: Five Perspectives: Revision 1*. (STF38 A 04403). Hentet fra https://www.sintef.no/globalassets/upload/teknologi_og_samfunn/sikkerhet-og-palitelighet/rapporter/stf38-a04403.pdf

Røyksund, M. (2011). *Informasjonssikkerhet i kraftforsyningen.* (Mastergradsavhandling). UiS. Stavanger. Hentet fra https://brage.bibsys.no/xmlui/handle/11250/184580

Sarter, N. B. & Woods, D. D. (1991). Situational Awareness: A Critical But Ill-Defined Phenomenon. *The International Journal of Aviation Psychology*. 1(1), 45-57. Hentet fra http://web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=b79df4a3-9d43-4049-a537-be61d2b4ca90%40sessionmgr107&vid=1&hid=123

Schulman, P. R. (1993). The Negotiated Order of Organizational Reliability. *Administration and Society. SAGE Journals*. 25(3). 353–372.

Sikkerhetsloven. (2001). *Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven)*. Hentet fra https://lovdata.no/dokument/NL/lov/1998-03-20-10

Sklet, S. (2006). Safety barriers: Definition, classification, and performance. *Journal of Loss Prevention in the Process Industries.* 19(5). 494–506. Hentet fra http://ac.els-cdn.com/S0950423005001968/1-s2.0-S0950423005001968-main.pdf?_tid=1005218e-186c-11e7-b379-00000aab0f02&acdnat=1491223986_024231e5c2e0e90a9fafa5431c13adbe

Skopik, F., Settanni, G. & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security* 60(2016), 154-176. Hentet fra http://ac.els-cdn.com/S0167404816300347/1-s2.0-S0167404816300347-main.pdf?_tid=806e8992-a81e-11e6-8236-00000aab0f26&acdnat=1478876143_e905f5ef409b663c159fc70f03d11ba5

Skotnes, R. Ø. (2015). *Challenges for safety and security management of network companies due to increased use of ICT in the electric power supply sector*. (Doktorgradsavhandling). UiS. Stavanger. Hentet fra

https://brage.bibsys.no/xmlui/bitstream/handle/11250/2374441/Ruth_Skotnes.pdf?sequence=1&isAllowed=y

Statnett. (2014, 28.11). Det var en gang… Lest 30.5.17. Hentet fra http://www.statnett.no/Samfunnsoppdrag/Neste-generasjon-kraftsystem-magasin/Det-var-en-gang/

Svenson, O. (1991). The accident evolution and barrier function (AEB) model applied to incident analysis in the processing industries. *Risk Analysis*. 11(3). 499-507. Hentet fra file:///C:/Users/Marta%20Helene/Downloads/Svenson%20-%20The%20accident%20evolution%20and%20barrier%20function%20(1).pdf

't Hart, P., Rosenthal, U., & Kouzmin, A. (1993). Crisis Decision Making: The Centralization Thesis Revisited. *Administration & Society*. 25(1). 12-45.

Tankard, C. (2011). Persistent threats and how to monitor and deter them. *Network Security*. 2011(8). 16-19. Hentet fra http://ac.els-cdn.com/S1353485811700861/1-s2.0-S1353485811700861-main.pdf?_tid=958f41c8-a840-11e6-9cde-00000aab0f27&acdnat=1478890782_0e2147b0c6e6904143d2742c2c7648d7

Thagaard, T. (2009). *Systematikk og innlevelse. En innføring i kvalitativ metode*. 3. utgave. Bergen: Fagbokforlaget Vigmostad & Bjørke AS.

Tinmannsvik, R. K. (Red.). (2008). *Robust arbeidspraksis - Hvorfor skjer det ikke flere ulykker på sokkelen?* Trondheim: Tapir akademisk forlag.

Turner, B. (1976). The Organizational and Interorganizational Development of Disasters. *Administrative Science Quarterly*. 21(3). 378-397. Conell University: Johnson Graduate School of Management.

Turner, B. (1978). *Man-made Disasters.* London: Wykeham Science Press.

US Department of Energy. (2001). *21 Steps to Improve Cyber Security of SCADA Networks*. (202/287-1808). Hentet fra https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf

Veriato. (2016). *Insider Threat. Spotlight report*. LinkedIn Group Partner; Information Security. Hentet fra http://www.veriato.com/docs/default-source/whitepapers/insider-threat-report-2016.pdf

Weick, K. E. & Sutcliffe, K. M. (2001). *Managing the Unexpected: Assuring High Performance in an Age of Complexity*. USA: Jossey-Bass.

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

Weick, K. E., Sutcliffe, K. M. & Obstfeld, D. (1999). Organizing for High Reliability: Processes of Collective Mindfulness. *Research in Organizational Behavior,* Vol. 1, 81-123.

Zheng, D. E. & Lewis, J. A. (2015). *Cyber Threat Information Sharing: Recommendations for Congress and the Administration.* (A Report of the CSIS Strategic Technologies Program). Hentet fra https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/150310_cyberthreatinfosharing.pdf

VEDLEGG 1

Skytjenester

Det foregår en omfattende diskusjon rundt skytjenester i kraftbransjen. Skytjenester kan være (NOU2015:13, 2015):

1. **Programvare** som tjeneste (Software as a Service, SaaS): Bruk av SaaS vil gjerne begrense kostander innen innstallering, kontrollering og oppgradering av programvare (computenext, 2013). Eksempler på systemer som tilbys som SaaS er regnskapssystemer, e-postløsninger, arkivsystemer og kontorstøtte. Det fins også tjenester beregnet på konsumentmarkedet, f.eks. Dropbox, LinkedIn, iCloud og Facebook (DIFI, 2016, 16.6).
2. **Infrastruktur** som tjeneste (Infrastructure as a Service, IaaS): Brukere av IaaS kan outsource og bygge et «virtuelt datasenter» i skyen og ha tilgang til mange av de samme teknologiene og ressursegenskapene til et tradisjonelt datasenter uten å måtte investere i kapasitetsplanlegging eller fysisk vedlikehold og styring av det (computenext, 2013). Eksempler på systemer som tilbys som IaaS er lagringsplass eller prosessorkapasitet (regjeringen, 2014, 13.12).
3. **Plattform** som tjeneste (Platform as a Service, PaaS): En plattform hvor programvare kan utvikles og distribueres. PaaS-leverandører sammenfatter arbeidet med å håndtere servere, noe som gir brukerne et miljø hvor nettverksinfrastrukturen tas vare på. Eksempler på systemer som tilbys som PaaS er utviklingsmiljø eller database (regjeringen, 2014, 13.12).

Skytjenester oppleves effektive fordi de gir fleksibilitet og mobilitetsfrihet (NOU2015:13, 2015). Skytjenester vil imidlertid kunne medføre at data fysisk ligger utenfor Norges grenser og overføres gjennom infrastruktur i et tredjeland (Hagen m.fl., 2017). Hvis en skytjenesteleverandør er lokalisert i et land med en svakere lovgivning enn den norske, har nettselskapene ingen garanti for at myndighetene i landet ikke krever utlevering av sensitiv informasjon om norsk kraftforsyning (Hagen, 2015). Ved bruk av skytjenester kan det argumenteres for utfordringer innen kontrollering av hvem som har tilgang til informasjonen (Hagen, 2015; Hagen m.fl., 2017), både internt hos leverandøren og blant myndighetene i landet. Nettselskapene jeg har intervjuet behandler informasjon som er underlagt

beredskapsforskriftens bestemmelser, og på bakgrunn at forestående diskusjon finnes det her forhold som kan begrense bruken av skytjenester når det er snakk om sensitiv informasjon:

«Person som vil kunne få tilgang til informasjon som er sikkerhetsgradert etter lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven), skal være sikkerhetsklarert og autorisert.» (beredskapsforskriften, 2013, § 6-7)

Beredskapsforskriften setter klare føringer for selskapers kontroll med hvem som har tilgang til informasjonen og implementering av sikkerhet deretter. Rent juridisk vil det altså være vanskelig å benytte internasjonale skytjenester for sensitiv informasjon fordi det som hovedregel forutsetter at det involverte personalet kan sikkerhetsklareres i Norge (NOU2015:13, 2015). Det må gjøres verdivurderinger av informasjon før det bestemmes om informasjonen skal legges i skytjenester eller ikke (Hagen, 2015). I følge NSM er skytjenester noe som vil bli tatt mer og mer i bruk, og sannsynligvis ligger allerede mye sensitiv informasjon lagret i skyen (Hagen, 2015). Hagen anbefaler imidlertid begrensninger i bruken av skytjenester når det kommer til sensitiv informasjon (Hagen, 2015). Ettersom mitt fokus i denne oppgaven er på sikring av sensitiv informasjon vil jeg ikke inkludere skylagringstjenester som et sikringstiltak i denne oppgaven.

VEDLEGG 2

Trussellandskapet 2016

"ENISA Threat Landscape Report 2016: 15 Top Cyber-Threats and Trends" presenterer trussellandskapet i 2016 (ENISA, 2017a). The European Union Agency for Network and Information Security (ENISA) er et ekspertisesenter for cybersikkerhet i Europa (ENISA, 2017b).

Top Threats 2015	Assessed Trends 2015	Top Threats 2016	Assessed Trends 2016	Change in ranking
1. Malware	↑	1. Malware	↑	→
2. Web based attacks	↑	2. Web based attacks	↑	→
3. Web application attacks	↑	3. Web application attacks	↑	→
4. Botnets	↓	4. Denial of service	↑	↑
5. Denial of service	↑	5. Botnets	↑	↓
6. Physical damage/theft/loss	⊃	6. Phishing	⊃	↑
7. Insider threat (malicious, accidental)	↑	7. Spam	↓	↑
8. Phishing	⊃	8. Ransomware	⊃	↑
9. Spam	↓	9. Insider threat (malicious, accidental)	⊃	↓
10. Exploit kits	↑	10. Physical manipulation/damage/ theft/loss	↑	↓
11. Data breaches	⊃	11. Exploit kits	↑	↓
12. Identity theft	⊃	12. Data breaches	↑	↓
13. Information leakage	↑	13. Identity theft	↓	↓
14. Ransomware	↑	14. Information leakage	↑	↓
15. Cyber espionage	↑	15. Cyber espionage	↓	→

Legend: Trends: ↓ Declining, ⊃ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Figur 11 Oversikt og sammenlikning av trusselbildet i 2016 med 2015 (ENISA, 2017a, s. 7).

ENISA (2017a) sammenlikner trussellandskapet i 2015 med 2016. Vi ser at hyppigheten av phishing-angrep har holdt seg stabil, selv om den har rykket opp på lista. Løsepengevirus (ransomware) økte drastisk fra 2015 til 2016 og gikk fra 14. plass til 8. plass i 2016. Videre ser vi at innsidetrusler (både intendert og ikke-intendert) var på oppadgående i 2015, men

flatet ut i 2016 og rykket dermed nedover på oversikten. Lekket informasjon (information leakage) har også økt.

VEDLEGG 3

Samtykkeskjema

Jeg er masterstudent innen Samfunnssikkerhet ved Universitetet i Tromsø. Jeg jobber nå med min masteroppgave hvor jeg skal se på informasjonssikkerhet knyttet til villede angrep mot nettselskapers informasjonssystemer. I den forbindelse vil jeg gjøre flere intervjuer innen kraftbransjen. Jeg ønsker å stille spørsmål rundt erfarte trusler, risikopersepsjon, tiltak for å forhindre angrep m.m.

Jeg vil snakke med flere nettselskaper i dette prosjektet. Alle informanter vil bli anonymisert. Jeg ønsker å gjøre opptak av intervjuet for å få med meg alle opplysninger som kommer frem. Opptakene vil bli slettet etter at sensur foreligger.

Jeg ønsker å gjennomføre intervjuet hvor jeg tar utgangspunkt i noen forberedte spørsmål, samtidig som jeg er åpen for en diskusjon rundt andre relevante forhold knyttet til denne problematikken.

Informanten vil gis anledning til å godkjenne den delen av teksten som inkluderer vedkommendes svar før oppgaven ferdigstilles.

Informantens underskrift bekrefter at de opplysninger som kommer frem i intervjuet kan benyttes i masteroppgaven.

Marta Helene E. Kruke

Mail: mkr098@post.uit.no, tlf. 909 555 89

Masterstudent i Samfunnssikkerhet, UiT

Informant:

Mail:

VEDLEGG 4

INTERVJUGUIDE NETTSELSKAPER

INTRODUKSJON

Mitt navn er Marta Helene Eskeland Kruke. Jeg studerer Samfunnssikkerhet i Tromsø, og skriver nå en masteroppgave om informasjonssikkerhet i norske nettselskaper. Jeg vil gjerne få stille deg noen spørsmål rundt dette tema. Først vil jeg gjerne at vi ser på et **samtykkeskjema** jeg har med.

HOVEDDEL

1. Hvor lenge har du arbeidet i x?
2. Hva er din stilling i x?
3. Hvilken erfaring har du med informasjonssikkerhet fra tidligere og hvordan jobber du med dette i det daglige?

<u>Informasjonssikkerhet</u>

4. Hva forstår du med informasjonssikkerhet?
    a. Er dette en forståelse som du deler med dine kollegaer?
5. Hva er det dere spesielt ønsker å beskytte (konfidensialitet, integritet og tilgjengelighet)?
6. Hvem fører *tilsyn* med informasjonssikkerhetsarbeidet hos dere, både internt og eksternt?
    a. Hvordan implementeres resultatene fra tilsyn?
7. Hvordan vil du plassere x i forhold til andre norske nettselskaper når det kommer til fokus på informasjonssikkerhet?

<u>Intenderte angrep: Trusler og sårbarhet</u>

8. Hvilke intenderte trusler mot informasjonssystemene står dere overfor i hverdagen?
    a. Hvordan jobber dere for å møte disse truslene?
    b. På hvilke områder er dere sårbare? Hva mener x er risikoen for angrep på disse områdene?
    c. Hvordan har trusselbildet knyttet til sikring av sensitiv informasjon endret seg i takt med den teknologiske utviklingen (digitalisering)?

d. Informasjonsprosessering; Misforståelser og feil kan skje når medarbeidere sitter på ulik informasjon – eller forstår informasjon på forskjellig måte. Hvilke arenaer finnes internt for informasjonsdeling rundt **trusselbildet** og hva er de særlige utfordringene med denne informasjonsdelingen?

9. Hvordan er dere i stand til å håndtere et angrep på informasjonssystemene deres i dag?

<u>Risikostyring</u>

10. Har dere hatt angrep mot informasjonssystemene deres?
    a. Utdypning? Hvordan responderte dere? Konsekvenser i ettertid?
11. Risikostyring kan defineres som *alle tiltak og aktiviteter som gjøres for å styre risiko*. Hvilke tiltak/aktiviteter gjør dere for å håndtere/styre risiko knyttet til intenderte angrep mot informasjonssystemene?
    a. Hvilke krav stilles til informasjonssikkerhet hos dere?
        i. Hvordan jobber dere for å møte disse kravene?
    b. Hvilke risikoanalyser kjører dere? Hvor ofte?
    c. Har dere definert noen kriterier for akseptabel risiko (risikomatrise)?
    d. Hvem er ansvarlige og hvem bidrar til disse analysene internt i x?
    e. Hvordan brukes resultatene fra analysene internt?
    f. Hva er de særlige utfordringene med risikostyring (tid, økonomi, kompetanse, relevans)?
12. Risikostyring handler gjerne om å forberede seg til kjente trusler, men også å forholde seg til usikkerhet. Innen Samfunnssikkerhet sier vi gjerne at *den neste krisen aldri har skjedd før*. Hvordan er dere forberedt på det ukjente?

<u>Risikopersepsjon/ risikoforståelse og risikobevissthet</u>

13. Hvordan vurderer *du* som ansatt risikoen for intenderte angrep mot informasjons-systemene deres?
    a. Tror du dette synet også gjelder for dine kollegaer?
    b. Har dere arenaer for kommunikasjon rundt dette?
    c. Er «restrisiko» et kjent begrep for deg? Når tenker dere i X at «denne restrisikoen kan vi akseptere»?
14. Hvordan er ledelsens engasjement for å holde fokus oppe når det gjelder informasjonssikkerhet?

    a. Deler hele selskapet ledelsens engasjement?
15. Hvilke arenaer finnes internt og eksternt for å dele erfaringer og øke bevisstheten rundt informasjonssikkerhetsarbeid?
    a. Er dere medlem av KraftCERT?
        i. Hva vil dette innebære? Hvordan styrker dette medlemskapet X når det gjelder informasjonssikkerhet? Hvilke andre nettselskaper er medlem i KraftCERT?
16. Hva gjør dere i etterkant av et angrep?
    a. Hvilke særlige utfordringer finnes ved læring etter angrep (vilje til rapportering, premiering av varsling, skyldfordeling)?
17. Hvordan jobber x med kompetanseutvikling innen informasjonssikkerhet?
18. Hva gjør du i hverdagen for å forhindre angrep på deres informasjonssystemer?
    a. Er dette etter bestemmelser fra ledelsen?

AVSLUTNING

19. Har du noe å tilføye utover det jeg har spurt om?
20. Kan jeg ta kontakt senere på mail/telefon for å avklare eventuelle uklarheter og eventuelle oppdukkende spørsmål?

VEDLEGG 5

INTERVJUGUIDE NVE

INTRODUKSJON

Mitt navn er Marta Helene Eskeland Kruke. Jeg studerer Samfunnssikkerhet i Tromsø, og skriver nå en masteroppgave om informasjonssikkerhet i norske nettselskaper. Jeg vil gjerne få stille deg noen spørsmål rundt dette tema. Først vil jeg gjerne at vi ser på et **samtykkeskjema** jeg har med.

HOVEDDEL

1. Hvor lenge har du arbeidet i NVE?
2. Hva er din stilling i NVE?
3. Hva er din erfaring med informasjonssikkerhet og hvordan jobber du med dette i det daglige?

<u>Informasjonssikkerhet</u>

4. Hva forstår du med informasjonssikkerhet?
    a. Er dette en forståelse som du deler med dine kollegaer i NVE?
5. Hva er NVEs særlige ansvar for informasjonssikkerhet i kraftbransjen?
6. Hvordan vil du vurdere norske nettselskaper når det kommer til fokus på informasjonssikkerhet?
7. Hvilke krav stilles til informasjonssikkerhet i kraftbransjen?
8. Hvilke aktører fører *tilsyn* med **informasjonssikkerhetsarbeidet** i nettselskapene i kraftbransjen?
    a. Hvor ofte føres det tilsyn med informasjonssikkerhetsarbeidet?
    b. Hva er erfaringene med implementering av resultatene fra tilsyn?
        i. Teknisk/organisatorisk/opplæring.
    c. Hva er relasjonen mellom NVE og DSB når det gjelder tilsyn (tilsynsforum)?
9. Hvilke arenaer finnes i kraftbransjen for å dele erfaringer og øke bevisstheten rundt informasjonssikkerhetsarbeid?

Intenderte angrep: Trusler og sårbarhet

10. Hvilke intenderte trusler mot informasjonssystemene står nettselskaper overfor i hverdagen?
    a. På hvilke områder er nettselskaper sårbare? Hva mener NVE er risikoen for angrep på disse områdene?
    b. Hvordan har trusselbildet knyttet til sikring av sensitiv informasjon endret seg i takt med den teknologiske utviklingen (digitalisering)?
    c. Hvordan bidrar NVE for å møte disse truslene?
    d. Misforståelser og feil kan skje når ulike selskaper sitter på ulik informasjon – eller forstår informasjon på forskjellig måte. Hvilke arenaer finnes for informasjonsdeling rundt trusselbildet og hva er de særlige utfordringene med denne informasjonsdelingen?

Risikostyring

11. Hvilke tiltak/aktiviteter gjør NVE og nettselskapene for å håndtere/styre risiko knyttet til intenderte angrep mot informasjonssystemene?
    a. Hva slags pålegg har kraftbransjen mht. risikoanalyser, og hvilke risikoanalyser kjøres?
    b. Har dere definert noen kriterier for akseptabel risiko?
    c. Hvor ofte skal nettselskaper gjennomføre risikoanalyser?
    d. Finnes det arenaer for deling av resultater og erfaringer med analysearbeidet?
    e. Føres det tilsyn med gjennomføring og kvalitet på risikoanalyser i nettselskaper?
    f. Hva er de særlige utfordringene med risikostyring (tid, økonomi, kompetanse, relevans)?
12. Risikostyring handler gjerne om å forberede seg til kjente trusler, men også å forholde seg til usikkerhet. Innen Samfunnssikkerhet sier vi gjerne at *den neste uønskede hendelsen aldri har skjedd før*. Hvordan er nettselskapene forberedt på den neste uønskede hendelsen (angrep)?

Risikopersepsjon/ risikoforståelse og risikobevissthet

13. Hvordan vurderer *du* risikoen for intenderte angrep mot informasjonssystemene i nettselskapene?

    a. Tror du dette synet også gjelder for dine kollegaer?
    b. Har dere arenaer for kommunikasjon rundt dette?
14. Når angrep skjer, hvordan kartlegges, kommuniseres og integreres læringspunktene i bransjen?
    a. Hvilke særlige utfordringer finnes ved læring etter angrep (vilje til rapportering, premiering av varsling, skyldfordeling)?
15. Hvordan jobber kraftbransjen med kompetanseutvikling innen informasjonssikkerhet?
16. Rent praktisk; Hva gjør du i hverdagen for å forhindre angrep på deres informasjonssystemer?
    a. Er dette etter bestemmelser fra ledelsen (pålegg fra andre)?

AVSLUTNING

17. Har du noe å tilføye utover det jeg har spurt om?
18. Kjenner du noen andre i NVE jeg bør snakke med?
19. Kan jeg ta kontakt senere på mail/telefon for å avklare eventuelle uklarheter og eventuelle oppdukkende spørsmål?