Etablering av beredskap på IKT-sikkerhet i energiforsyningen

Linn Soo Jin Jeanette Barstad

Masteroppgave i Samfunnssikkerhet

Juli 2016

Universitetet i Stavanger

MASTERGRADSSTUDIUM I
SAMFUNNSSIKKERHET

MASTEROPPGAVE

SEMESTER:

VÅREN 2016

FORFATTER:

LINN SOO JIN JEANETTE BARSTAD

VEILEDER:

JANNE HAGEN

TITTEL PÅ MASTEROPPGAVE:

Etablering av beredskap på IKT-sikkerhet i energiforsyningen

EMNEORD/STIKKORD:

IKT-sikkerhet, energiforsyning, beredskap, ROS-analyser, krisehåndtering, kompleksitet, NAT, HRO, sårbarhet, kritisk infrastruktur, hendelseshåndtering

SIDETALL:

STAVANGER …….
DATO/ÅR

FORORD

Denne oppgaven markerer slutten på to hektiske, utfordrende, givende, krevende og til tider frustrerende år på master i Samfunnssikkerhet, på Universitetet i Stavanger, og et semester på Københavns Universitet i Danmark. Det er oppholdet i København som gjorde at jeg fikk interessen for IKT-sikkerhet, og det har vært et meget interessant halvår med masteroppgaveskriving.

Først og fremst vil jeg takke alle informantene som har sagt ja til å stille opp på denne oppgaven. Uten dere hadde det ikke vært mulig å skrive denne oppgaven. Deretter rettes en stor takk til min tålmodige veileder, Janne Hagen, som gjennom hele løpet har vært støttende og oppmuntrende.

Disse to årene hadde ikke vært mulig å gjennomføre hadde det ikke vært for den fantastiske studiegruppen min: Tonje, Ole Morten, Chris, Mathias og Espen. Tusen takk for alle faglige og sosiale diskusjoner, latterkramper og støttende ord – hadde ikke vært mulig uten dere!

Sist men ikke minst, min kjære familie og mine kjære venner, dere er fantastiske! En spesiell takk rettes til Karoline, Ida og Eli for korrekturlesing og tilbakemeldinger.

Stavanger, 10. juli 2016

Linn Barstad

SAMMENDRAG

Hendelsen i Ukraina hvor flere hundretusen plutselig ikke hadde strøm, økte bevisstheten rundt evnene til hackere. Norge har heldigvis ikke end opplevd en alvorlig hendelse Energiforsyningen er en av de viktigste samfunnsfunksjonene vi har, og en viktig del av den kritiske infrastrukturen. Med den stadig økende digitaliseringen av samfunnet, og implementeringen av IKT-systemet er vi mer utsatte enn før. Driftskontrollsystemene som er i bruk i dag ble egentlig ikke konstruert for å være på internett, noe som har gjort at sikkerhet ikke ble bygget inn fra begynnelsen av. Før ble kraftanlegg styrt manuelt, nå fjernstyres alt. Dette gjør at trusselbildet har endret seg for energiforsyningen: ikke bare må ta høyde for fysiske trusler, men også digitale. IKT-hendelser må det etableres beredskap på, på lik linje som fysiske hendelser. Det er et forholdsvis nytt felt og dermed er det mindre erfaring på hvordan man skal etablere beredskap på IKT-sikkerhet.

Studiens problemstilling er: *Hvordan kan energiforsyningen etablere god beredskap på IKT-sikkerhet?* Formålet med denne oppgaven er å etablere mulige suksesskriterier for etablering av beredskap på IKT-sikkerhet. Denne studien består av et datagrunnlag som er innhentet ved å bruke en kvalitativ metodetilnærming. Datagrunnlaget består av ni intervju og relevante dokumenter. Det teoretiske grunnlaget for denne oppgaven er begrepsforklaring av risiko, sårbarhet og trussel, beredskapsteori, *Natural Accidents Theory* og *High reliability Theory.*
Det er kommet frem til fem retningslinjer for hvordan man kan etablere god beredskap på IKT-sikkerhet:

1. ROS-analyser og verdivurdering er de viktigste elementene i identifiseringsfasen, og legger føring for resten av prosessen. Her må det nedsettes en analysegruppe som går gjennom potensielle IKT-trusler. Analysene må tilpasses trusselbildet og jevnlig oppdateres.
2. Beredskapsplanen må øves og trenes på. Og man gi folk ansvar for det de har til daglig ettersom de vil gjennomføre kjente oppgaver bedre. Man må vite hvilke ressurser man har tilgjengelige, både interne og eksterne. Dersom det oppstår en hendelse, og man ikke har denne kompetansen in-house, må man vite hvem man skal kontakte.
3. IKT-trusler kan endre karakter over tid, derfor må det hele tiden være fokus på kompetanseheving. I tillegg må man tilrettelegge for at virksomheten og dens ansatte er oppdaterte på sikkerhetsrutiner.
4. Sikkerhetstankegangen må gjennomsyre hele virksomheten, fra topp til bunn, og fra bunn til topp. Det er viktig at den samme forståelsen er gjennomgående i hele organisasjonen.
5. IKT-sikkerhet må ha likt høyt fokus som mer tradisjonell fysisk beredskap. Man kan ikke bli bedre på noe dersom det ikke blir prioritert. Dialog mellom ledelse, IT-avdeling og beredskapsstab må vektlegges.

INNHOLDSLISTE

Figur- og tabelloversikt:

Liste over forkortelser:

AMS: Avanserte måle- og styringssystemer

BDO: Binder, Djiker, Otte & Co (i dag er det kun forkortelse som brukes)

CERT: Computer Emergency Response Team

DSB: Direktoratet for samfunnssikkerhet og beredskap

IKT: Informasjons- og kommunikasjonsteknologi

IT: Informasjonsteknologi

JD: Justis- og beredskapsdepartementet.

NorSIS: Norsk senter for informasjonssikring

NOU: Norges offentlige utredninger

NSM: Nasjonal sikkerhetsmyndighet

NSR: Næringslivets sikkerhetsråd

NVE: Norges vassdrags- og energidirektorat

OED: Olje- og energidepartementet

POD: Politidirektoratet

ROS: Risiko- og sårbarhetsanalyse

SCADA: Supervisory Control and Data Acquisation

St.meld.: Stortingsmelding

1 INNLEDNING

”De sa det var umulig. Nå klarer russiske hackere å slå av strømnettet” (Johansen, 2016). Dette var overskriften som frontet *Aftenpostens* forside den 15. januar, 2016. I en liten by i Ukraina forsvant plutselig strømmen, lille julaften. Ute var det kaldt, og det ble spådd enda kaldere av meteorologene. Minst 30 transformatorstasjoner ble slått ut, og over 80 000 husstander, bedrifter og andre virksomheter ble rammet. Cyberangrepet var utført på en avansert måte, hvor hackerne først brøt seg inn i SCADA-systemet, deretter ble datamaskiner og servere infisert av datavirus. På denne måten ble kontrollen over styringssystemene tatt. I tillegg ble kundetelefonsentralene utsatt for et DDoS-angrep, eller et såkalt tjenestenektangrep (E-ISAC og SANS, 2016). Kraftselskapene som ble påvirket av angrepet gikk over til manuell styring, ettersom SCADA-systemene blir brukt til å automatisere prosessen. Dette var en nødvendig handling, og de hadde gjenopprettet tjenester etter 3-6 timer (Kovacs, 2016). KraftCERT, kraftbransjens støttefunksjon for dataangrep, og Hafslund uttalte at lignende kan skje i Norge, mens Nasjonal Sikkerhetsmyndighet (NSM) undersøkte hendelsen for å finne ut hvilke konsekvenser den kan ha for Norge, avklaring av årsakssammenhengen og ”(…) hvilke tiltak som eventuelt kan redusere risikoen (…)” (Hans Christian Pretorius, NSM, i epost til Aftenposten, i Johansen, 2016).

Grunnleggende samfunnsfunksjoner er avhengige av at flere systemer alltid skal fungere. Vann, strøm, telefon, internett er blant noen av de funksjonene vi ser på som grunnleggende, og som vi ikke kan se for oss å være uten. Ettersom de aller fleste områdene i samfunnet vårt i dag er avhengig av teknologi, finnes det flere ting som må kontrolleres slik at daglig drift alltid går rundt. IKT-sikkerhet er derfor blitt en stadig større del av samfunnet vårt, og instanser må være forberedt og ha tatt høyde for denne type sikkerhet. Energiforsyningen er en av de viktigste samfunnsfunksjonene vi har, og forstyrrelser og nedetid kan få store konsekvenser for andre bransjer, som finans og helse, ettersom det er stor gjensidig avhengighet mellom de viktige samfunnsfunksjonene (Aven, Boyesen, Njå, Olsen & Sandve, 2013).

På grunn av økt fokus på informasjons- og kommunikasjons teknologi (IKT; videre begrepsavklaring presenteres i kapittel 2.2) er det nødvendig å integrere IKT-sikkerhet på en bedre måter i beredskapsplanene til energiforsyningen. I følge BDO (2010) er det viktig med god virksomhets- og risikostyring, og effektiv beredskap. Å være forberedt på det ukjente er

en viktig del av beredskapsplanene, selv om man ikke kan vite hva man skal være forberedt på (Alexander, 2002). IKT-sikkerhet er forholdsvis nytt, og det er ofte man ser at selv de enkleste tiltak ikke blir etterfulgt i bedrifter, selv om de er nedfelt i planverk (NSR, 2014). Et godt planverk er en del av en god kontinuerlig planleggingsprosess. Planverket skal hele oppdateres, og ikke ligge og støve på en hylle (Lunde 2014). For å kunne holde tritt med den teknologiske utviklingen, samt beskytte sine verdier er det derfor høyst nødvendig at energiforsyningen utvikler en god digital beredskap (Hagen, 2014). Videre påpeker Hagen (2014) hvordan man etter 22.juli innførte ny IKT-strategi, overføring av ansvar til Justis- og beredskapsdepartementer, men at det fremdeles finnes utfordringer i forhold til nasjonal beredskap.

1.1 PROBLEMSTILLING

På bakgrunn av det overnevnte er følgende problemstilling valgt for denne oppgaven:

Hvordan kan energiforsyningen etablere god beredskap på IKT-sikkerhet?

For å kunne svare på problemstillingen er det valgt tre forskningsspørsmål

1. Hvilke IKT-relaterte sårbarheter og trusler er energiforsyningen utsatt for?
2. Hva sier litteratur og eksperter om etablering av god beredskap?
3. Hvilke organisatoriske utfordringer er det til IKT-sikkerhet og beredskap?

Studien fokuserer på energiforsyningen som en del av kritisk infrastruktur og en viktig samfunnsfunksjon, uten at det er hovedfokus på virksomhetene i selve forsyningen.

For å kunne svare på problemstillingen og forskningsspørsmål, er det nødvendig å kartlegge hvordan situasjonen er, og hvilke vurderinger som er blitt gjort av situasjonen i forsyningen. Derfor er det blitt innhentet informasjon fra rapporter og dokumenter som sier noe om det. Deretter er det valgt semistrukturerte intervju for å få førstehåndsinformasjon fra eksperter og rådgivere om hvordan opplever situasjonen. Gjennom teori om komplekse system og høy-pålitelige organisasjoner kan man si noe om hvordan denne teorien ser på forsyningen, i tillegg til hva teori om beredskap og krisehåndtering sier om beste praksis for IKT-sikkerhet.

1.1.1 Avgrensninger:

Fokuset i denne oppgaven legges på organisering og planlegging rundt det å etablere en god beredskap på IKT-sikkerhet. Dermed vil det også fokuseres på relaterte sårbarheter og trusler, samt hvilke utfordringer som finnes til beredskap og IKT-sikkerhet. Energiforsyningen er en stor sektor, og dermed inneholder flere tekniske komponenter og system. Det er av den grunn nødvendig å poengtere at dette ikke vil være en teknisk oppgave, hvor de tekniske systemene blir grundig studert. Det vil bli kort fortalt hva et Supervisory Control and Data Aquisation system (SCADA-system er), og det vil bli fokusert på sårbarheter man kan finne i systemer, ettersom de blir koblet opp mot hverandre. Derimot vil det ikke forklares hvordan alt henger sammen på en videre detaljert måte. Hovedfokuset i denne oppgaven vil være de organisatoriske forholdene rundt IKT-sikkerhet og hvilke synspunkter eksperter fra både myndighetsorganer, uavhengige organisasjoner, rådgivere og spesialister på området informasjonssikkerhet har. Grunnen til dette er at det er valgt å fokusere på beredskap, og for å kunne planlegge og etablere en god beredskap i en organisasjon, må alle områder i organisasjonen med, også det tekniske Dermed er det viktig å ha en forståelse om hva som finnes i organisasjoner av systemer, ressurser og andre elementer, men det må også ses i et helhetlig bilde.

På grunn av økende teknologi og implementering av nye løsninger er IKT-sikkerhet et felt som er i stadig utvikling. Dermed er det valgt teori ut i fra hvilke sårbarheter som finnes i systemer som gjør at det utfordrende å unngå ulykker (*Natural Accidents Theory:* Perrow, 1999; Sagan, 1993), og teori som fremlegger om hvordan man kan organisere seg sikker (*High Reliability Theory*: Sagan, 1993; Rijpma, 1997, Aven et al, 2014). Dermed er det interessant å undersøke om virksomheter innenfor energiforsyningen er klare for nye utfordringer som relateres til deres virksomhet, som man tradisjonelt kan peke på har bestått mest av fysiske hendelser som svikt, sabotasje og uvær (NOU 2015:13, 2015). I tillegg vil det bli forklart hvordan man kan etablere beredskap, og hvilke elementer som skal være med. Det vil ikke gis detaljerte forklaringer på alle elementene ettersom det ikke er samlet inn spesifikke analyser og planer i forbindelse med denne oppgaven, men det vil basere seg på utsagn fra intervju og rapporter. På bakgrunn av dette er det interessant å undersøke om virksomheter innenfor energiforsyningen er klare for nye utfordringer som relateres til deres virksomhet, som man tradisjonelt kan peke på har bestått mest av fysiske hendelser som svikt, sabotasje og uvær.

Det vil heller ikke gjennomgås aspekter rundt krisekommunikasjon. Krisekommunikasjon handler om hvordan man skal nå ut med riktig informasjon til befolkningen, og skal være med på å begrense usikkerhet rundt ansvarsforhold (NOU 2015:13, 2015). Dette er et område som kvalifiserer for en helt egen oppgave, og grunnet plass- og tidsmangel var det ikke hensiktsmessig å forske på dette. Det anbefales dog at dette området blir studert og knyttet opp mot IKT-sikkerhet.

Formål med oppgaven

IKT-sikkerhet og beredskap er så langt jeg forstår, lite utforsket. Formålet med denne oppgaven er å etablere noen mulige suksesskriterier for beredskap på IKT-sikkerhet i energiforsyningen. Hensikten med å studere denne tematikken er å kunne tydeliggjøre problemstillinger og tvil som kan finnes hos virksomheter i energiforsyningen. Dette vil selvsagt ikke bli løsningen på problemet, men et forslag til hvilken tilnærming man kan ha til beredskap på IKT-sikkerhet. Til syvende og sist er det alltid opp til virksomheter selv å vurdere hva som er relevant for deres fremdrift.

1.2 Tidligere forskning

Når det gjelder den tema for den valgte problemstillingen, beredskap på IKT-sikkerhet i energiforsyningen, virker det ikke som det finnes mye forskning på nøyaktig det området. NOU 2015:13 (2015) tar opp viktige problemstillinger som omhandler tematikken, men den går ikke i dybden på disse. Videre finnes det en artikkel (Hagen et al., 2005) om nye utfordringer knyttet til beredskap i informasjonssamfunnet. Når det gjelder andre type tematikker som også vil gå under IKT-sikkerhet og beredskap, finnes det blant annet studier gjort på sikkerhet og sikring av prosesskontrollsystemer fra petroleumssektoren (Johnsen, 2012; Jaatun et al., 2008), og SCADA-systemer (Krutz, 2006). På forskning om IKT-sikkerhet i energiforsyningen finnes det studier som omhandler økende bruk av IKT, risikostyring og cyberangrep på driftskontrollsystemer i Norge (Nygård, 2004; Røyksund, 2011; Skotnes, 2015). I tillegg er det gjort studier som omhandler kompleksiteten til IKT og den menneskelige faktoren (Hagen, 2009). Med tanke på beredskap og beredskapsplanlegging finnes det mye litteratur og forskning, som presenterer blant annet hvordan man bør planlegge for å få en god beredskap, beskriver hva beredskap med mer (et utvalg: Perry og Lindell, 2007; Alexander, 2009; Lunde, 2014; DSB, 2001). I tillegg finnes det også rapport på et komparativ studie på cyberkrisehåndtering og krisehåndtering, som

sammenligner og problematiserer forskjellene på tradisjonell krisehåndtering og cyberkrisehåndtering (Trimintzios et al. 2014).

Denne oppgaven vil dermed bidra til et felt som det tilsynelatende ikke finnes så mye forskning på fra før.

2 BAKGRUNN OG KONTEKST

I dette kapittelet gis en presentasjon av bakgrunnen og konteksten for studien.

Hendelsen i Ukraina, ble beskrevet i Johansens (2016) artikkel i *Aftenposten* som ”(…) det første store dataangrepet som i betydelig grad har påvirka sivilbefolkningen” (Johansen, 2016). Det er ikke første gang man ser at et hackingangrep får fysiske følger. Dataormen, Stuxnet i 2010 hadde som hensikt å sabotere et atomanlegg i Iran. Som det ofte er med dataangrep, er det vanskelig å finne frem til den opprinnelige kilden, og selv om man har visse spor, kan man være ikke helt sikre. Ringvirkningene av ormen spredte seg langt utover det man trodde var hovedmålet, og spesielt med ormen var at den siktet seg inn på samme type driftskontrollsystemer som blir brukt i den norske kraftbransjen, SCADA-systemer (Hamnes 2010). Stuxnet-angrepet førte til økt oppmerksomhet på sårbarheter i industrikontrollsystemer, og av totalt kjente sårbarheter, ble 80 prosent oppdaget etter Stuxnet-hendelsen, i følge The Industrial Control Systems Cyber Emergency Response Team (ISC-CERT) (NOU 2015:13, 2015).

Her i Norge har man enda ikke sett et stort målrettet angrep, men i 2014 ble Statnett utsatt for et dataangrep, som ble stoppet av en observant ansatt. Nasjonal sikkerhetsmyndighet (NSM) gikk ut og fortalte at norske selskaper i olje- og energibransjen var utsatt for et dataangrep hvor angriperne hadde sendt ut epost med farlige filer som inneholdt skadevare, til over 50 selskaper. I verste fall kunne disse gitt tilgang til systemer og ha gjort store ødeleggelser. Statnett har blant annet 11 000 kilometer med høyspent linjer, og driver sentralforsyningen, i tillegg til å sikre kraftforsyningen (NRK, 2014).

Stadig flere nasjoner utvikler cyberstrategier som del av sine militære strategier, og Politiets sikkerhetstjeneste (PST) sa i 2014 at nye land nå driver med ulovlig etterretningsvirksomhet i Norge. I følge NSM er en av hovedtruslene spionasje, hvor man benytter målrettet trojanere for å infiltrere system og stjele informasjon (NRK, 2014). I ”1. Halvårsrapport 2015”, påpeker NSM at ”det er store sårbarheter i norske IKT-systemer, og konsekvensene av mangelfull IKT-sikkerhet er at store verdier kan gå tapt. Derfor er det behov for omfattende satsing på IKT-sikkerhet” (NSM, 2015, s. 4).

Energiforsyningen sies å være den mest kritiske infrastrukturen ettersom den er grunnleggende for all type produksjon, tjenester som er avhengig av datamaskiner og elektroniske kommunikasjon (Hagen og Albrechtsen, 2009; Skotnes, 2015). Kritisk infrastruktur ble i 2000 definert av Willoch-utvalget som:

> (…) systemer som når de ikke fungerer vil ha en sterk negativ effekt på samfunnet (forsvar, velferdstjenester, næringsliv). Kritisk infrastruktur inkluderer blant annet informasjons- og kommunikasjonsteknologi (IKT), systemer for elektrisk kraft, gass og olje, bank og finans, transport og vannforsyning" (NOU 2000:24, 2000, s. 20).

Lysneutvalget la "Rammeverk for kritisk infrastruktur og kritiske samfunnsfunksjoner (KIKS-rammeverket, utgitt av DSB i 2012), og beskrev det på denne måten: "Kritiske samfunnsfunksjoner er de funksjoner som dekker samfunnets og befolkningens grunnleggende behov. Kritisk infrastruktur er de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner" (NOU 2015:13, 2015, s. 19). Som NSM (2015) påpeker blir det vanskeligere å oppdage angrep og trusselaktørenes kompetanse økes.

2.1 Energiforsyningen

Teknologi er grunnmuren til samhandling på tvers av alle sektorer i dagens samfunn. Utviklingen av informasjonsteknologi har gitt det norske samfunnet og dets innbyggere betraktelige gevinster. Bruken og implementeringen av IKT-systemer har gitt et bredere tjenestetilbud, og økt bruk av IKT har gjort at samfunnet blir mer sårbart. Utviklingen av IKT og dens integrering i samfunnet har gjort oss mer avhengige, men er i tillegg en viktig del av energiforsyningen for å imøtekomme samfunnets krav til drifts- og forsyningssikkerhet. I dag kommer cirka 98.5 prosent av elektrisitetsproduksjonen fra vannkraft (NOU 2015:3, 2015). Stabil strømforsyning er viktig for samfunnssikkerheten i Norge og IKT blir stadig mer integrert i drift, styring, overvåking og beredskap (BDO, 2010).

Det overordnede ansvaret for energiforsyningen ligger hos Olje- og energidepartementet (OED), mens det er Norges vassdrags- og energidirektorat (NVE) som har ansvar for forvaltning, i tillegg til at de er beredskapsmyndighetet for forsyningen. NVE fører dermed tilsyn med sikkerhet og beredskap, i forhold til de kravene som er satt i beredskapsforskriften (Beredskapsforskriften, 2013). Statnett er den største kraftprodusenten og har ansvar for

systemansvaret i Norge, som skal legge til rette for effektivt kraftmarked sørge for tilfredsstillende leveringskvalitet, og er dominerende eier av sentralnettet (NOU 2015:13, 2015; Skotnes, 2015). NVE og DSB har sammen ansvaret for sikkerheten i den norske energiforsyninga, og DSBs ansvar er i hovedsak el-sikkerhet og krav til kraftsystemet og dets komponenters tekniske og fysiske tilstand (Meld. St. 22, 2008).

4.1.1 SCADA-system

SCADA-systemer blir i dag brukt for å automatisere kontroll over prosesser i kraftproduksjon og nettdrift og fjernstyrer og overvåker disse. I tillegg tilbyr en real-time overvåking og kontroll med minimale forsinkelser. Fordelene ved bruk av SCADA-systemer er at kommunikasjons- og tilkoblingsmuligheter til utenforstående nettverk, som internett er mulig (Krutz, 2006). SCADA-systemene ble ikke designet med spesiell tanke på sikring, og heller ikke for å kunne være motstandsdyktig mot internett tilkobling (Goodman, 2015). Dette gjør at disse systemene er mer sårbare for angrep eller feilhandlinger fra både eksterne og interne kilder, grunnet tilkoblingen til internett. Det finnes flere komponenter innenfor et SCADA-system, hvor også den menneskelige faktoren er viktig; menneskelig operatører kontrollerer og overvåker systemet. Tidligere var kontrollsystemer og administrative systemer adskilt, og ikke tilkoblet eksterne nettverk. Men med utviklingen i teknologi er det blitt mulig å fjernstyre anlegg, kontra manuell styring, som bemannede kraftstasjoner. Dette har ført til at man har gått fra isolerte kraftstasjonsnettverk, hvor man har brukt proprietære hardware og software system, til PC-baserte system ved bruk av standard software, nettverksprotokoller og internett (Krutz, 2006). SCADA-systemer kobles opp mot administrative systemet via en brannmur, og denne koblingen gjør at man får ekstern tilgang, og dermed er mer utsatt for hacking.

2.2 IKT-sikkerhet

For å forklare hva IKT-sikkerhet er og hva det innebærer er det valgt å fokusere på Lysne-utvalget sine forklaringer fra, NOU 2015:3. Det finnes flere begrep som blir brukt om hverandre når det kommer til digitalt sikkerhetsarbeid, eksempelvis, IKT-sikkerhet, informasjonssikkerhet, cybersikkerhet. I 2012 ble det publisert en nasjonal cyberstrategi, hvor begrepet informasjonssikkerhet ble brukt (Departementene, 2012). I Norges offentlige utredninger (2015:3, 2015), *Digitalt sårbarhet – sikkersamfunn*, forklares det at, ”informasjonssikkerhetsbegrepet handler om sikring av informasjon, uavhengig av om den er

digital eller analog". Både nasjonalt (Forsvarsdepartementet) og internasjonalt er ofte begrepet cybersikkerhet brukt i forbindelse med å, "(..) beskytte "alt" som er sårbart fordi det er koblet til, eller på en annen måte er avhengig av informasjon- og kommunikasjonsteknologi" (ibid.)

Fra denne definisjonen ser man at IKT-sikkerhet handler om å beskytte IKT og informasjonen i informasjonssystemer for uønskede hendelser. Definisjonen Justis- og beredskapsdepartementet (JD) bruker er; "Med IKT-sikkerhet forstås sikring av informasjons- og kommunikasjonsteknologi i forhold til konfidensialitet, integritet og tilgjengelighet. Denne sikringen innebærer tiltak på både menneskelig, teknisk og organisatorisk nivå" (JD, 2015, s. 3) De tre sikkerhetsmålene, konfidensialitet, tilgjengelighet og integritet kan beskrives som følger (NOU 2015:14, 2015, s. 34):

- Konfidensialitet: beskyttelse mot at uvedkommende blir kjent med informasjon som kun er ment for de som har fått tilgang på den. Eksempel på brudd på konfidensialitetsprinsippet er spredning av private bilder som man har fått adgang til via hacking.
- Tilgjengelighet: informasjon og tjenester er tilgjengelige når det trengs. Eksempel på brudd på tilgjengelighetsprinsippet kan være at en tjener ikke har tilstrekkelig med ressurser til å håndtere antall oppkoblinger, som også er et eksempel på utilsiktet tjenestenekt.
- Integritet: innebærer at informasjonen man får er til å stole på, og at systemer og tjenester fungerer slik det skal. I tillegg skal kun informasjon endres av de som har lov til det. I tillegg har man *autensitet*, som handler om at opphavet til den informasjonen vi mottar er sikret. Også relatert til integritet har man *non-repudiation*, eller ikke-fornektelig, som vil si at en digital handling ikke skal kunne benektes i ettertid, eksempelvis signering av kontrakt.

Når man bruker ordet *kompromittert*, vil det si at det mistenkes brudd, eller at det har vært brudd på sikkerhetsmålene. Det er dog viktig å huske på at det aldri er helt mulig å overholde alle sikkerhetsmålene, men at dette burde etterstrebes. I kapittel 5, empirikapittelet, vil informasjonssikkerhet og IKT-sikkerhet bli brukt om hverandre, det vil også sikkerhetshendelser og IKT-hendelser. I alle andre deler, vil det det konsekvent brukes IKT-sikkerhet og IKT-hendelser, men for å ikke endre for mye på utsagn til informanter vil deres

egne ord bli brukt. Som nevnt finnes det mange synonym for IKT-sikkerhet, men det vil i denne oppgaven, som i NOU 2015:13, bli brukt IKT-sikkerhet.

2.2.1 IKT-kriminalitet

Et av hovedproblemene med økt digitaliseringen er at det ikke finnes landegrenser i cyberspace. Dermed er det ikke nasjonal suverenitet som gjelder lenger. Dette beskrives videre i Politidirektoratets (2015) strategi, hvor det vektlegges viktigheten for at hvert land må ha egne regler og tiltak. IKT-kriminalitet, eller datakriminalitet, har ikke en klar definisjon, men POD viser til at første del handler om kriminalitet som er rettet mot datasystemer, og den andre handler om bruk av data eller datasystem som redskap for å utføre en kriminell handling (Politidirektoratet, 2015: 21). Dermed er første del straffbare handlinger hvor datasystemet er objektet for handlingen, eksempelvis SCADA-systemet, mens den andre delen handler om straffbare handlinger hvor man bruker data/datasystem som redskap, et eksempel på dette kan være uttak av penger fra en bankkonto. Strategien (Politidirektorater, 2015), påpeker videre at skillene mellom disse to til tider uklare.

2.2.2 Tilsiktede og utilsiktede hendelser

Det er viktig å skille mellom tilsiktede og utilsiktede hendelser, spesielt når det gjelder forutsigbarhet og konsekvens. Etter hvert har man opplevd flere naturhendelser, som fortsatt er en stor trussel mot den norske energiforsyningen, men dette er hendelser man for så vidt ikke kan gjøre noe med, utenom å være forberedt på dem. Utilsiktede hendelser deles i NOU 2015:13 inn i to kategorier, naturhendelser og svikt. Det finnes flere former for svikt, og en kategori er mennesket. Det er viktig å huske på at mennesket gjør feil, selv om intensjonen er god. Som NOUen påpeker, finnes det en klar sammenheng mellom svak lederforankring, menneskelige feilhandlinger og organisatoriske, som årsaker til mangelfullt sikkerhetsarbeid og uønskede hendelser i IKT-system. I tillegg handler svikt også om organisatorisk svikt, og Mørketallsundersøkelsen (MU) (2014) viser at det finnes manglende kunnskap om informasjonssikkerhet i virksomheter. Systemsvikt derimot, går ofte ut på at en enkeltkomponent bryter sammen. Dette kan for eksempel skje med overbelastning. Videre finnes det også eksempler på hvordan systemsvikt og menneskelige feil gjør at hendelser forplanter seg videre til andre system, noe som kan få katastrofale følger (NOU 2015:13, 2015). Tilsiktede hendelser derimot, handler om digitale angrep, og har som hensikt å skade

eller påvirke personell, materiell eller IKT-prinsippene. Dette er straffbare handlinger, og kan både være målrettede og ikke-målrettede handlinger.

2.2.3 Mørketallsundersøkelsen

Mørketallsundersøkelsen (MU) er en undersøkelse som blir utført annethvert år, og siste ble publisert i 2014. Det er forventet en ny utgave av undersøkelsen, september 2016. Undersøkelsen blir utført av Næringslivets Sikkerhetsråd (NSR), og formålet med undersøkelsen er å forebygge kriminalitet i og mot næringslivet. Den skal opplyse og informere om kriminelle og sikkerhetsmessige trusler og trender som forventes sett i fremtiden, og kartlegge IT-sikkerhetshendelser og omfanget av sikringstiltak i norske virksomheter. Hver undersøkelse har et informasjonssikkerhetsutvalg. Til undersøkelsen som ble utført i 2014, ble den sendt til virksomheter i både privat og offentlig sektor, hvor 932, av et bruttoutvalg på 4500 virksomheter svarte. Dette gir da en svarprosent på 15.5 % (NSR 2014:3).

Hovedfunnene fra Mørketallsundersøkelsen i 2014 viser at det finnes store mørketall i estimerte hendelser og anmeldte hendelser, og dermed er det vanskelig å få et bilde over hva virksomheter har rapportert og hva de faktisk blir utsatt for. Statistikk fra Nasjonal sikkerhetsmyndighet (NSM, 2015) viser at det ble varslet om 160000 hendelser i 2013, hvor 5000 ble håndtert, av disse var 51 alvorlige hendelser. Data fra Mnemonic viser at blant deres kunder ble det oppdaget 11000 hendelser. Sammenligner man loggdataene fra disse to viser det derimot at det oppleves flere datainnbrudd enn det som har blitt rapportert i undersøkelsen. I tillegg viser undersøkelsen at det kan tyde på at det eksiterer en manglende kunnskap hos virksomheter om informasjonssikkerhet og at virksomhetene ikke har god nok oversikt over hvilke verdier de besitter (NSR, 2014).

2.3 Energiloven og beredskapsforskriften

Energiloven og beredskapsforskriften regulerer sikkerhet og beredskap i kraftbransjen, herunder informasjonssikkerhet. Beredskapsforskriften, slik den er i dag, ble tatt i bruk 01.januar 2013, og har i tillegg en omfattende veiledning som skal gjøre det enklere for kraftbransjen å vite hva som forventes for at kravene i forskrifta skal være oppfylt. Energilovens § 9-3 og kapittel 6 i beredskapsforskriften omhandler spesifikt IKT-sikkerhet, som forklart i NOU 2015:13 (2015), ”Dette omfatter identifisering og håndtering av

kraftsensitiv informasjon og opplysninger om energiforsyningen som kan brukes til å skade anlegg eller påvirke funksjoner som har betydning for energiforsyningen (NOU 2015:13, 2015, s. 132). Kraftsensitiv informasjon blir definert i forskriften som, ”(…) spesifikk og inngående opplysninger om energiforsyningen som kan brukes til å skade anlegg eller påvirke funksjoner som har betydning for energiforsyningen (…)” (Beredskapsforskriften, 2013, s. 11). Under dette inngår blant annet system som ivaretar driftskontrollfunksjoner, enlinjeskjema, transformatorstasjoner, reserve driftssentraler, analyser av sårbarheter og beredskapsplaner for håndtering av bevisst skadeverk, med mer.

Videre handler kapittel 7 i beredskapsforskriften om krav til sikring av driftskontrollsystemer som er kritiske for overvåking og styring av energiforsyningen. Det er plikt til å beskytte driftskontrollsystemet, og det finnes tre klasseinndelinger av driftskontrollsystem, hvor klasse 3 er har de høyeste kravene for sikring, som også blir gjennomgått i kapittel 5.

2.4 Nye problemstillinger i energiforsyningen

NVE er i dag i gang med vurderinger om forskriften skal revideres, ettersom det har kommet nye elementer som trenger videre spesifisering, fordi det både har kommet ny teknologi, og fordi det har oppstått nye problemstillinger som forskriften må spesifisere. I denne sammenhengen er det spesielt snakk om automatiske avanserte måle- og styringssystemer (AMS), personvern, skylagring, logging og hendelseshåndtering (Hagen, 2015). I tillegg er også kapittel 2 i beredskapsforskriften viktig, ettersom det er dette kapittelet som fastsetter krav til beredskapsplikt. Fra Hagen (2015) sin rapport kommer det frem anbefalinger om at forskriften bør revideres med hensyn til AMS, og spesielt bryterfunksjonaliteten.

3 TEORETISK RAMMEVERK

I dette kapittelet vil det teoretiske rammeverker denne oppgaven baserer seg på bli presentert. Først presenteres det en oversikt over begrep (risiko, sårbarhet, trussel), før en beskrivelse av beredskap og beredskapsplanleggingsprosessen blir fremlagt. For å kunne si noe om systemer og ulykker i komplekse system er det valgt å ta med *Natural Accidents Theory* (Perrow, 1999), som ser på sårbarheter ved komplekse system. Det som ofte blir forklart som motpolen til NAT (Aven et al. 2014) er *High Reliability Theory* (Sagan, 1993; Rijpma, 1997) eller høy-pålitelig organisasjon, som fokuserer mer på hvordan man organiseres, og kommer med løsninger for å unngå ulykker.

3.1 Risiko, sårbarhet, trusler

Herunder vil det bli presentert definisjoner på risiko, sårbarhet og trussel.

3.1.1 Risiko

Oppfattelse og forståelse kan variere mye, og ord som risiko, sannsynlighet, konsekvens, usikkerhet, er viktig å ha klart definert slik alle innad i en organisasjon har samme forståelse. Risikostyring handler om å systematisk prøve å styre fremtidsutviklingen, og ”kan forstås som "alle tiltak og aktiviteter som gjøres for å styre risiko” (Aven, sitert i Lunde, 2014, s. 25). Det finnes flere tilnærminger til forståelse av begrepet risiko, og Aven og Renn (2010), presenterer en liste med ti forskjellige tilnærminger. Ofte er risiko delt inn i to kategorier, hvor risiko er utrykt gjennom sannsynlighet og forventede verdier (den tradisjonelle teknisk-naturvitenskapelige tilnærmingen), og gjennom hendelser/konsekvenser og usikkerhet. Derfor presenterer de sin definisjon som, ”Risk refers to uncertainty about and severity of the consequences (or outcomes) of all activity with respect to something that humans value” (Aven og Renn, 2010, s. 3). I denne definisjonen tar man høyde for både uønskede og ønskede resultater, usikkerhet istedenfor sannsynlighet og forventet verdi, i tillegg til at det også fokuseres på berørte interesser heller enn spesifikke konsekvenser. Ettersom den tar inn usikkerhetsdimensjonen, kan man vurdere om en risiko er lav, og bruke sannsynlighet som et verktøy til å utrykke usikkerheten: det vil alltid eksistere en usikkerhet. Velger man å bruke sannsynlighet som en måte å måle på, er det vanlig å utrykke risikobegrepet gjennom sannsynlighet og konsekvens (Aven og Renn, 2010; Aven et al, 2013; Lunde, 2014).

3.1.2 Sårbarhet

Sårbarhet forstås i Meld. St. 17 (2001-2002) (2002) som ”(…) begrenset evne til å tåle påkjenninger eller påvirkninger som kan resultere i betydelige negative avvik fra normal funksjon for det system som den den sårbare komponent inngår i. Graden av sårbarhet beskriver hvor lett det er å påføre slik skade” (s. 28). Sårbarheten kan brukes om alle nivå, og alt fra enkeltkomponent til system i sin helhet. Lysneutvalget (2015) bruker definisjonen til Sårbarhetsutvalget (2000) som definerer sårbarhet som, ”et utrykk for de problemer et system for med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet” (NOU 2000:20, 2000, s. 18). Aven et. al (2013) presenterer også en mer generell definisjon, som også omhandler robusthet: ”Et systems evne til å opprettholde sin funksjon når det utsettes for påkjenninger” (s. 124). Et viktig poeng er systemets evne til å gjenoppta sin virksomhet, ettersom energiforsyningen er en del kritisk infrastruktur og mange sektorer og private personer av avhengige av strøm. Lysneutvalget (2015), bruker også en forståelse om robusthet, som kan minne om Aven et.al (2013) sin definisjon, hvor det blir vektlagt motstandskraften systemet har, hvor påkjenninger her kan bli forstått som uønska hendelser. Det finnes også flere måter å utrykke sårbarhet på, som er viktig å påpeke ettersom det er en stor del av planleggingen å vite man egentlig mener. Sårbarhet kan bli utrykket kvalitativt; faren for at barriere helt/delvis skal bli ødelagt og kvantitativt; pålitelighet/tilgjengelighet og effektivitet.

3.1.3 Trussel

Begrepet trussel brukes i Meld. St. 17 (2001-2001) (2002), ”(…) om produktet av kapasitet og intensjon i en situasjon hvor en kjent statlig eller ikke statlig aktør antas å ha kapasitet og intensjon til å gjennomføre en handling som kan medføre omfattende skader på liv, helse, miljø og materielle verdier” (s. 28). I tillegg kan trussel ses på som årsak til uønska hendelse, og NSM beskriver begrepet som ”en tilsiktet handling” (NSM, 2015 SIDETALL). Uønskede hendelser derimot, kan både være tilsiktede og utilsiktede hendelser (forklart i bakgrunn og kontekstkapittelet). Når det kommer til digitale sårbarheter, har Lysneutvalget (2015) sett på flere nivåer av systemer (NOU 2015:13, 2015, s. 31):

1. Sårbarheter som knyttes direkte til IKT-systemer, både logiske og fysiske feil. Slike sårbarheter kjennetegnes ved svakheter, feildesign eller feilimplementering.
2. Sårbarheter i selve samfunnsfunksjonene som er forårsaket av svikt i IKT-systemet, og ved at svakheter arves av feil i IKT-systemer.

I tillegg finnes det sårbarhet som en hver tid samfunnet vil stå ovenfor, faller i en av to kategorier:

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

For å redusere sårbarheten er det nødvendig å gjennomføre sårbarhetsreduserende, og kjent som risikoreduserende tiltak, men selv da kan man sitte igjen med det som kalles restsårbarhet eller restrisiko. Risiko og sårbarhet blir til tider brukt om hverandre, og ofte innenfor IT-sektoren blir sårbarhet brukt ofte brukt, ettersom man har en sårbarhet om det for eksempel finnes sikkerhetshull om et system har en svakhet (Rausand og Utne, 2014) ISC-CERT varsler blant annet om sårbarheter i IT- og komponentsystem, og prosesskontrollsystemet. Og som nevnt innledningsvis er det en observert økning i angrep på prosesskontrollsystemer etter Stuxnet (NOU, 2015:13, 2015). Som Lunde (2014, s. 34) poengterer, strides det om bruken av dette begrepet oppfyller sin hensikt, ettersom det i fagmiljøet har blitt hevdet at det kan forstås som siste rest av risiko. Selv om man prøver å utrede all risiko og sårbarhet, vil det alltid være noe igjen man aldri kan helt fjerne;

- Vi har lyktes med å identifisere alle uønskede hendelser som kan inntreffe,
- Vi har lyktes med å identifisere alle mulige årsaker eller konsekvenser som tilhører de uønskede hendelsene vi har identifisert,
- Vi har lyktes med å etablere barrierer som fjerner all risiko,
- Etablerte barrierer holder nødvendig kvalitet over tid.

Videre deler han så inn restrisikoen i fem kategorier, som gjør det oversiktlig å se hvilke kategorier av hendelser man aldri helt kan beskytte seg mot: 1. Villede menneskelige handlinger, 2. Menneskelige feilhandlinger, 3. Materiellsvikt, 4. Annen påvirkning, 5. Uidentifiserte hendelser. Det er på bakgrunn av dette at beredskapen etableres (Lunde, 2014, s. 34).

3.2 Beredskap

Sårbarhetsutvalget, Willochutvalget, definerte i 2000 beredskap som, ”(…) tiltak for å forebygge, begrense eller håndtere kriser og andre uønskede hendelser” (NOU 2000:24, 2000, s. 20). Lunde (2014) påpeker videre at denne definisjonen er god fordi den også åpner for at beredskap er både sannsynlighetsreduserende og konsekvensreduserende. Videre nevner han at med å være sannsynlighetsreduserende kan man etablere beredskap for å

redusere at en faresituasjon eskaleres til en uønsket hendelse, og for å redusere konsekvenser av allerede inntruffet hendelse. (Lunde, 2014). Perry og Lindell (2007) og Alexander (2009) påpeker at selv om man har planer, betyr ikke dette at man er forberedt, eller har en beredskap (*preparedness*, oversatt til beredskap). Planlegging bør være en kontinuerlig prosess; planen i seg selv representerer et spesifikt tidspunkt i planleggingen. Planleggingsprosessen driver med pågående overvåking av trusselbildet og teknologi (Alexander, 2009; Perry og Lindell 2007; Lunde, 2014). Å være forberedt er, kan kobles til det som Wildawsky (1991, s. 77) definerer som *anticipation* "(…) predict and prevent potential dangers before damage is done". Selv om man ikke vet hva fremtiden vil bringe, handler det om evnen til å kunne planlegge for at noe uventet skal skje og unngå farer. Videre kunne håndtere og være fleksible når en hendelse er i gang, eller har skjedd, omtaler Wildawsky (ibid.) som"(…) capacity to cope with unanticipated dangers after they have become manifest, learning to bounce back". Dette er to begrep som inkorporerer det beredskap handler om.

Å være beredt er et resultat av en prosess hvor et samfunn (eller en virksomhet) ser på alle svakheter. Sårbarhet, ressurser og organisatoriske struktur kan endre seg over tid. Ytelsesevne kan forsvinne over tid om det ikke øves og trenes, og disse handlingene opprettholder beredskapen. Lunde (2014), og Perry og Lindell (2007) nevner videre at beredskapsplanlegging er drevet at sårbarhetsvurdering og risikoredusering. Før man går i gang med selve etablering av beredskap, må man gjennomføre ROS-analyser og verdivurderinger. Sårbarhetsvurdering, eller risiko- og sårbarhetsanalyser (ROS) innebærer å dokumentere kjente trusler, men også å identifisere nye trusler. Verdivurderinger innebærer å finne ut hva som er skjermingsverdig informasjon, objekt, hvilken grad de er skjermingsverdige og hvordan man skal finne rette beskyttelsestiltak for dette (NSM, 2009). Som nevnt, sitter man igjen med en restrisiko, og det er her man etablerer en beredskap, fordi uønskede hendelser kan inntreffe uavhengig av de risikoreduserende tiltakene som er iverksatt. Dermed må det finnes en tydelig sammenheng mellom ROS-analysene og beredskapsplanen, fordi for å oppnå en robust beredskapsplan må man ta resultater fra ROS-analyser videre (Lunde, 2014; NVE og Proactima, 2010).

3.2.1 De nasjonale beredskapsprinsippene

Angrepet på Utøya og regjeringskvartalet 22. juli satte beredskapsevnen til samfunnet på prøve, og er et av hovedtemaene i Melding til Stortinget, 29 (Meld. St. 29, 2014?). Etter hendelsen så man et økende behov for samvirke på tvers av sektorer, ettersom samfunnet er blitt mer komplekst og det er avhengigheter på tvers av sektorer. Tre beredskapsprinsipper ble innført i St. Meld. 17 (2001-2002), men det mangler her presisering av hvor viktig det er med samvirke mellom de forskjellige aktørene. Derfor ble det i Melding til Stortinget 29, innført et fjerde prinsipp, nemlig samvirke, og det fjerde prinsippet skal være på lik linje med de tre andre. Likhetsprinsippet utfyller ansvarsprinsippet, og nærhetsprinsippet må også ses i sammenheng med ansvarsprinsippet. De fire prinsippene er som følger (Meld. St. 29 (2011-2012), 2012, s. 39; Lunde, 2014, s. 48-49):

- Ansvarsprinsippet: den myndighet, etat eller virksomhet som til daglig har ansvar for et område, også har ansvaret for nødvendige beredskapsforberedelser og for den utøvende tjeneste ved kriser og katastrofer. Det beste er om den som er tildelt ansvarsområde om de som skal samarbeide er plassert samme sted i en beredskapssituasjon som i daglig drift.
- Likhetsprinsippet: Organisasjonen man opererer med under krise, skal være mest mulig lik den man har til daglig. En beredskapsorganisasjon som er bygget om så nært som mulig til den organisasjonen man benytter daglig, er enklere å forholde seg til i hektiske beredskapssituasjoner.
- Nærhetsprinsippet: Kriser skal organisatorisk håndteres på det lavest mulige nivået. Det vil si at den som har størst nærhet til en krise, vil ha best forutsetninger for å forstå og håndtere den. Prinsippet skal dermed sikre tilstrekkelig og nødvendig beslutningsmyndighet lengst ute i organisasjonen.
- Samvirkeprinsippet: stiller krav til at myndigheter, virksomheter, og etater har et selvstendig ansvar for å sikre et best mulig samvirke med relevante aktører, i arbeid med forebygging, beredskap og krisehåndtering. Prinsippet er bærebjelken i offentlig beredskap, men bør også benyttes i private virksomheters beredskapsorganisasjoner

3.3 Planlegging og etablering av beredskap

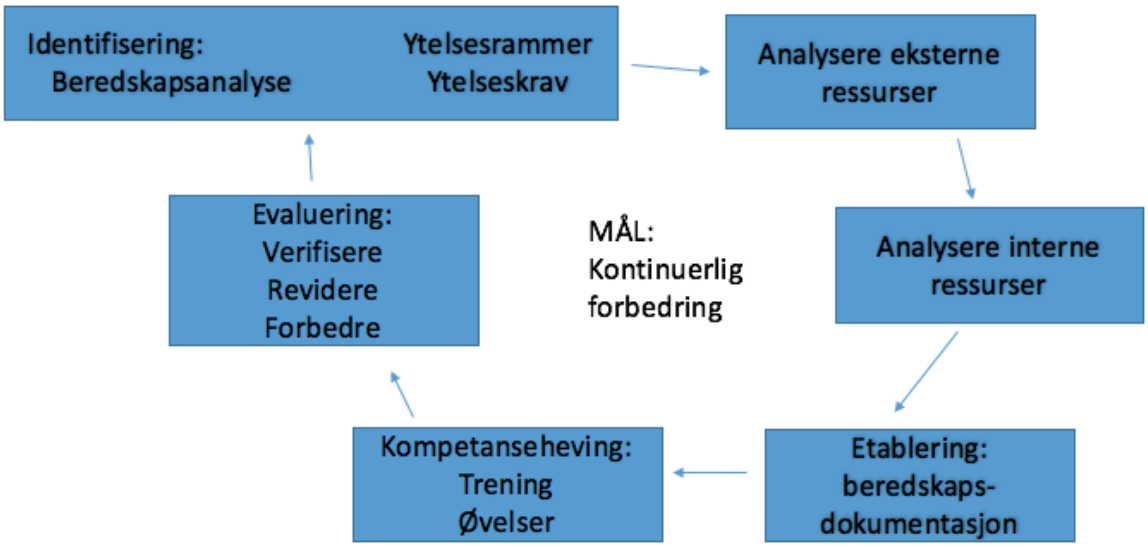
Det finnes mange ulike kilder på hvordan man skal gjennomføre planleggingsprosessen på beredskapsplanlegging, men stort sett inngår de samme elementene. Derfor benytter denne oppgaven Perry og Lindell (2003), Lunde (2014), veileder fra NVE og Proactima (2010), og veileder fra DSB (2001)

For å kunne etablere en planleggings- og beredskapsprosess er det viktig at man sikrer en analytisk og praktisk tilnærming til tre aktiviteter: identifisering, etablering og evaluering. Det finnes mange ulike fremstillinger av hvordan hele beredskapsetablering/-planlegging/-arbeid ser ut, og derfor har det i denne oppgaven blitt valgt å bruke figur 3, til Lunde (2014, s. 53) (forenklet versjon, visuelt sett), som er en visualisering av en modell som blir brukt i petroleumsindustrien. Modellen kalles også av Proactima som "beredskapshjulet", og er omtrent lik den Lunde (2014) presenterer i sin bok, med et par unntak. Denne vil bli supplert med annen litteratur, men selve fremstillingen av modellen er brukt fordi den inneholder sentrale elementer, som eksempelvis modellen i DSB sin veileder for "Systematisk sikkerhets- og beredskapsarbeid i kommunene" (DSB, 2001) ikke har. I tillegg er Lundes (2014), *Praktisk krise- og beredskapsledelse*, en mer praktisk tilnærming til beredskapsplanlegging, og ses derfor på som mer oversiktlig og direkte, fremfor andre teoretiske tilnærminger. Modellen har syv faser:

1. Identifisering: beredskapsanalyse
2. Ytelsesrammer og ytelseskrav
3. Analyse av eksterne ressurser
4. Analysere interne ressurser
5. Etablering: beredskapsdokumentasjon
6. Kompetanseheving: trening og øvelser
7. Evaluering: verifisere, revidere og forbedre.

I tillegg har den som et overordnet mål om kontinuerlig forbedring.

3.3.1 Prosess for etablering av beredskap



Figur 1: Prosess for etablering av beredskap (Visualisert i Lunde, 2014, s. 53)

Fase 1: Identifisering

I identifiseringsfasen (Lunde, 2014), er det nødvending å gå gjennom ambisjoner og mål som virksomheten har, i tillegg til å få oversikt over hvilke lover og forskrifter som gjelder. For energiforsyningen er det energiloven §9-3, beredskapsforskriften som gjelder for informasjonssikkerhet og beredskap (NOU 2015:13, 2015). Deretter går man over i det Lunde (2014) kaller en beredskapsanalyse, som inneholder definerte fare- og ulykkessituasjoner krav til beredskap og tiltak. Perry og Lindell (2003) sier at er det nødvendig for beredskapsplanleggingens kartlegging, at den er basert på troverdig informasjon om trusler, og respons. Trusselvurderinger bør gjøres kontinuerlig. Herunder kommer ROS-analyser, hvor det må kartlegges hvilke risiko og faremomenter som finnes, og hvor sårbarheter for svikt ligger. Denne analysen vil gi en beskrivelse av status, og fungerer som en forutsetning for videre planlegging (DSB, 2001).

Fase 2: Ytelsesrammer og ytelseskrav

I tillegg må det settes som sier noe om hvilke situasjoner det skal etableres beredskap på, og ytelseskrav for å bestemme hvilken respons og håndtering man skal ha på de bestemte beredskapssituasjonene (Lunde, 2014). Dette er også det som vil bli gjort i en ROS-analyse, og den restrisikoen man sitter igjen med, er situasjoner det må etableres beredskap på. I tillegg bør man kartlegge hvilke ressurser som finnes som virksomheten kan benytte for å

etablere beredskap, både eksterne og interne. Samt, hvilke risikovillighet som finnes, altså hvilken risiko man kan utsette innsatsressurser for (Lunde, 2014).

Fastsette mål for sikkerhet og beredskap for hvordan virksomheten kan styrke sitt arbeid med dette. Her bør hovedmålene si noe om hvilke ambisjoner man har til skadeforebyggende- og skadereduserende tiltak. Disse tiltakene baseres på det man har avdekket i ROS-analysene, og vil dermed si noe om hva som må videre arbeides av planer og tiltak. I tillegg må man avklare hvilke oppgaver som skal fordeles. Som nevnt bygges beredskap på ansvarsprinsipper, og dermed må man avklare hva ansvar hvem skal ha for sikkerhets- og beredskapsplanlegging. Derfor bør beredskapsaktiviteter delegeres slik at det følger det ordinære linjeansvaret (DSB, 2001). Som nevnt, skal det opprettes beredskap på de hendelsene som ikke kan bli håndtert gjennom daglig drift (Lunde, 2014). Når en hendelse inntreffer, der det også vanlig at man setter inn beredskap, men at man kaller planene som er gjort for denne type hendelser for krisehåndteringsplaner. Herunder er respons og tiltak, som kan ses i sammenheng med det Lune (2014) beskriver som innsats, innsatskriterier og respons.

Fase 3 og 4: Analyse av eksterne og interne ressurser

Videre skal det gjennomføres en analyse av hvilke eksterne og interne ressurser som finnes, og hvilke tiltak som skal benyttes for å etablere en respons som tilfredsstiller ytelseskrav og ytelsesrammer. Målet er å finne ut hvordan man på best mulig måte kan håndtere hendelsene som er fastsatt. Eksterne ressurser kan være redningstjenester og nødetater, andre offentlige ressurser som kommunale beredskapsressurser og offentlige spesialiserte- og spesialtjenester (Lunde, 2014; Perry og Lindell 2007). For energiforsyningen er blant annet NSM, NVE, NorCERT og KraftCERT viktige ressurser. Deretter må man kartlegge hvilke interne ressurser man har. Internt i virksomheter finnes det prosesser og kompetanse som man bør videreføre som en del av beredskapen. I tillegg til de internt eksisterende ressursene man har, er man nød til å etablere noe for å kunne fylle inn gapet der det mangler tilfredsstillende respons. Eksempler på dette kan være innsatspersonell for håndtering av umiddelbar førsteinnsats og spesialkompetanse som knyttes til virksomhetens særegne operasjoner (Lunde, 2014; DSB, 2001).

Fase 5: Etablering

Videre sier Lunde (2014) at etableringsfasen har som formål å organisere og videreføre identifiseringsarbeidet som er gjort, samt kvalifisere ressursene i beredskapen. I denne fasen er det to viktige elementer, den første er å dokumentere beredskapsressursene, og sikre at disse ressursene læres opp, trenes og øves. Under beredskapsdokumentasjon er det viktig at alle dokumenter som er blitt utarbeidet, blir tatt med. Som nevnt tidligere skal man ta med eksterne ressurser, og dermed må man også legge ved forpliktende avtaler hvor det stadfestes, dersom det er private aktører. Er det offentlige aktører er de som regel pliktige til å bistå. Den andre er beredskapsstrategi, som er et mer overordnet dokument som sier noe om hvilke prinsipp og føringer man ønsker å jobbe etter i sitt beredskapsarbeid (DSB, 2001). Deretter kommer beredskapsplaner, som er det dokumentet det jobbes aktivt med under i en beredskapssituasjon. Dette plandokumentet skal inneholde beskrivelser av ulike ledelsesnivå, enheter og funksjoner i beredskapsorganisasjonen. Detter er et av de viktigste dokumentene som må jobbes med under planleggingsprosessen, og det er også et dokument som alle i en organisasjon må gjøre seg kjent med. En beredskapsplan kan ikke være for detaljert, og skal i følge Dynes (1993) være dynamisk. Den skal også være praktisk utformet bruke. Den bør inneholde: varsling og mobilisering, håndtering og risikoreduksjon, demobilisering og normalisering (Lunde, 2014; Perry og Lindell, 2003).

Fase 6: Kompetanseheving

Vel så viktig som planlegging, er øving, trening og opplæring i de planene man har etablert, ellers så er det av ingen nytte når involverte ressurser ikke vet hva som må og skal gjøres. Opplæringen bør gjennomføres på individ-, gruppe- og organisasjonsnivå. På individnivå må både internt og eksternt personell få beredskapsopplæring, og det må fokuseres på kompetanseheving og ferdighetstrening i de oppgavene den enkelte skal ha. Det bør også dokumenteres hvilke forventninger man har til individer i forhold til hvilke ferdigheter og forskjellige funksjoner som finnes. På gruppenivå må koordinering innenfor samhandling dokumenteres, og det må øves slik at man ser at enheter har felles forståelse for oppgavene, i tillegg til at kompetansen hos enheten dekker oppgavene som skal gjennomføres. På organisasjonsnivå, må samhandling og koordinering komme på plass blant de ulike enhetene i beredskapsorganisasjonen, samt bør de eksterne aktørene trekkes inn, slik at det også øves og trenes (Lunde, 2014). Perry og Lindell (2003) understreker også hvor viktig det er å ha en treningskomponent i planen, og at det må være en essensiell del. De påpeker i tillegg hvordan en treningsdel også kan være en god måte å sjekke og få tilbakemelding på om det finnes

potensielle problemer i planen. Når det kommer til øvelser, påpeker Lune (2014) at det finnes tre typer øvelser: refleksjonsøvelser, også kalt *table tops*, hvor man samler forskjellige aktører for å diskutere aktuelle problemstillinger, hvor målet er å komme frem til en felles forståelse om hvordan virksomheten kan respondere på en mest effektiv måte. Simuleringsøvelser skal gi deltakere øvelse på reelle forhold, og denne øvelsen bør legges opp så nært beredskapssituasjoner som mulig; verifikasjonsøvelser har som mål å verifisere at organisasjonen har evne til å respondere på beredskapssituasjoner i forhold til ytelseskrav og beredskapsdokumentasjon. Denne øvelsen er viktig for videre evaluering av prosessen. Fokus på kompetanse og øvelse er også noe som blir vektlagt i DSB (2001) sin veileder.

Fase 7: Evaluering

I den siste fasen, evaluering, skal man evaluere om beredskapen oppfyller det formålet som er satt. Evalueringen er en viktig del av verifikasjonsøvelsene, og selve evalueringsdelen har fire steg:

1. Verifisering om organisasjonen holder et tilfredsstillende nivå og evne,
2. Evaluere om det under verifikasjonen har oppstått behov for å endre den etablerte beredskapsprosessen,
3. Revidere dokumentasjon i henhold til de endringene man har oppdaget,
4. Dokumentere endringer, og så endre beredskapsdokumentasjonen slik at de nye endringene kommer på plass i planene (Lunde, 2014).

Dette er en viktig del av prosessen, og det er også derfor den ses på som en kontinuerlig prosess med tanke på opprettholde effektiviteten (Perry og Lindell, 2003). Om beredskapen ikke klarer å respondere på de rammer som er satt, eller man ser at det finnes områder hvor man kan forbedres, er det mulig å gjennomføre flere kompetansehevende aktiviteter, endre organisering av ressurser, eller endre interne krav. Modellen som er illustrert er derfor visualisert som en sirkel, nettopp fordi det skal være en kontinuerlig prosess, som ikke skal legges bort og avsluttes. Målet skal alltid være kontinuerlig forbedring (Lunde, 2014; Perry og Lindell 2003; Alexander 2009).

3.4 Natural Accidents Theory

Charles Perrow, først publisert i 1984, hevder at det før eller siden vil oppstå systemulykker i høyteknologiske system, og at risiko aldri kan bli eliminert i disse. (Aven, Boyesen, Njå, Olsen og Sandve, 2013, s. 60). Høyrisikoteknologier har noen karakteristikker som tilsier at

uansett hvor effektive sikkerhetsmekanismer er, er en form for ulykke uunngåelig, noe som er likt cyber. Perrow argumenterer: I et anlegg med flere komponenter (deler, prosedyrer, operatører), hvor to eller flere feil mellom komponentene som har en innvirkning på hverandre skjer på en uventet måte. I tidsrommet finner man ikke ut hvordan de ble påvirket, og dermed får man ikke gjort noe for å rette feilene, og skaperne av systemet var ikke klare over at dette kunne skje. I noen systemer, vil derimot ikke ulykken spre seg videre fordi det finnes en del slakk, men om systemet er tett koblet er gjenoppretting fra den opprinnelige forstyrrelsen ikke mulig (Perrow, 1999).

Perrow hevder at for systemene som han eksemplifiserer vil verken bedre organisering eller teknologiske løsninger gjøre dem mindre utsatt for systemulykker. Av denne grunn er komplekse sammenhenger og tette koblinger kvalifisert til, det han kaller, normalulykker, eller systemulykker. Forklaringen av en ulykke er en ikke-intendert og uønskede hendelse som forårsaker skader på mennesker og/eller materiell. For at en hendelse skal kunne sies å være en ulykke må den svekke personens og/eller objektets evne til å fungere like godt som før hendelsen inntraff. Ulykken er en svikt eller en feil i et definert system som ødelegger den pågående eller den fremtidige driften av systemet. Perrow deler så inn det han kaller systemer, i fire deler: 1. Del, minste enhet av systemet (eks. ventil), 2. Enhet, samling av deler som til sammen utgjør eksempelvis en generator, 3. Subsystem, samling av enheter som utgjør et system, eksempelvis et kjøleanlegg bestående av generatorer, pumper, rør, mennesket er òg en del av subsystemet 4. Systemet, det totale systemet, eksempelvis et kjernekraftverk. Dermed følger definisjonen, ”An *accident* is a failure in subsystem, or the system as a whole, that damages more than one unit and in doing so disrupts the ongoing or future output of the system. An *incident* involves damage that is limited to parts of a unit, whether the failure dirupts the system or not” (Perrow 1999, s. 66). Dermed kan man se at en uønsket hendelse, *incident,* begrenses til del og enhet i systemet (selv om det kan stoppe produksjonen), mens en ulykke, *accident,* vedrører subsystemet og det totale systemet, som medfører en stopp i produksjon. (Perrow, 1999, s. 64-66).

Med interaksjoner menes samhandlinger basert på beslutningslinjer og informasjonsflyt, hvor det finnes påvirkninger mellom mennesker og maskiner. I lineære produksjonslinjer er det enkelt å oppdage feil, og man vet hva som foregår på hver stasjon. Detter også mulig å ta høyde for i ROS-analyser, og dermed kan man redusere sårbarheten i systemet (Hagen, Fridheim og Nystuen, 2005). Derimot vil komplekse interaksjoner ha ukjente, ikke-planlagte

og uventede sammenhenger som ikke er lette å forstå, og kompleksiteten øker. SCADA-systemer, er eksempler på dette siden de er integrerte med administrative systemer, og støttesystemer til leverandører. Ofte vil man øke kompleksitet for å minske kjente feil, men dette er også en hovedkilde til feilene. Det er interaksjonene som avgjør om de er komplekse eller lineære (Perrow, 1999).

For å forklare komplekse system, må man se på hvordan et system håndterer det Perrow kaller "hidden transactions". Lineære system har også skjulte transaksjoner, men de foregår innen kjente og segregerte deler. Derimot, når man prøver å automatisere og redusere antall kontrollpunkter, minsker man systemets fleksibilitet. Komplekse system er mer effektive enn lineære system på grunn av mindre slakk, mindre toleranse for lavkvalitets ytelse, og flere multi-funksjonelle komponenter (ibid.). Med tette koblinger forklares med tidsavhengige prosesser hvor man ikke kan skru av produksjon, og koblingene har liten slakk, hvor ressurser ikke kan erstattes og svikt vil føre til nedstenging av produksjon. I system med tette koblinger må slakk, buffere og andre erstatninger tas høyde på forhånd, og bli designet inn i systemet, og på grunn av tidspress finnes det få muligheter for improvisasjon. Derimot i systemer med løse koblinger finnes det mer slakk og dermed flere utveier og muligheter til å finne erstatninger selv om det ikke var planlagt. I tillegg kan løs koblede systemer bedre inkorporere feil og dermed justere seg uten at det fører til destabilisering. (Aven et al, 2013; Perrow, 1999).

I følge Hagen, Fridheim og Nystuen (2005) går samfunnskritiske funksjoner og kritisk infrastruktur mot Perrow sin beskrivelse av kompleksitet og tette koblinger, spesielt IKT-systemer. Og de understreker hvordan energiforsyningen har blitt til et komplekst og tett koblet system, hvor tidligere hadde man bemannede stasjoner, som ble kontrollert manuelt. I dag er derimot dette arbeidet automatisert og automatisering og fjernkontroll har gjort at kraftsystemet kan bli styrt av en håndfull mennesker på kontrollsentre på en effektiv måte. SCADA-systemer støtter opp hele kjeden av strømlevering, og systemet har også gått fra å være et lukket system til et åpent ved å være tilkoblet det administrative systemet og internett. De peker også på hvordan kompleksiteten til IKT-systemer gjør det vanskelig å etablere omfattende barrierer for all relevante trusler, og identifisere suksessfulle angrep og dets konsekvenser. I tillegg peker de på at det er å forvente at avhengigheten til IKT øker i energiforsyningen (Hagen et al., 2005).

3.5 High Reliability Theory

”High Reliability Theory” (HRT) fokuserer på at organisasjonsdesignet kan utvikle pålitelige systemer selv om enkeltkomponenter er upålitelige. Teorien ble utviklet av en gruppe forskere ved University of California, Berkeley, men har blitt beskrevet av flere forskere som Marone og Woodhouse (1986); La Porte og Consolini (1991); Roberts (1989; 990); Wildawsky (1988) (presentert i Aven et al., 2014). Forskere har studert hvordan et utvalg av høyrisiko-organisasjoner på en sikker måte kan håndtere høyrisiko teknologier. Fokuset i teorien er på organisasjonsdesign, og organisasjoner kan da designes på en måte som gjør de sikre, og den har sitt utsprang fra høyteknologiske systemer, som kjernekraftindustri (Aven et al., 2014). Høypålitelige organisasjoner, som teorien også blir kalt (HRO) «(…) centralize the design og decision premises in order to allow desentralized decision making» (Weick, 1987, sitert i Rijpma, 1997, s. 15), og bruker redundans til å støtte opp feil i deler og menneskelige handlinger.

I følges Scott D. Sagan (1993) finnes det tre retninger innen HRT. Tross forskjellig forskningspraksis, er det enighet omkring fire faktorer som bidrar til høy grad av sikkerhet. Det går ikke ut på at mennesket er fult ut rasjonelt, derimot at en organisasjon kan designes og administreres kan kompensere for kjente menneskelige svakheter, og dermed være mer rasjonell og effektiv enn individer. Høyrisiko-organisasjoner blir sett på som rasjonelle i den forstand at de har sterke formaliserte strukturer, og er rettet mot oppnåelse av klare og presise mål, som i denne sammenhengen vil være ekstremt pålitelige og sikre operasjoner. I tillegg er systemene nokså lukket, med tanke på at de prøver å minimere påvirkning som utenforstående aktører og miljø kan ha på oppnåelse av disse målene (Sagan, 1993). Det finnes fire betingelser som er nødvendige for en pålitelig og sikke organisasjon (Aven et al, 2014; Sagan, 1993):

Sikkerhet som objektiv hos ledelsen

Sikkerhet og pålitelighet skal ha høyest prioritet hos formelle og uformelle ledere; sikkerhet og pålitelighet som mål skal gjennomsyre hele organisasjonen. Det påpekes at for å oppnå høy pålitelighet må man ha høyt nivå av redundans og konstant trening, noe som er økonomisk kostbart, og dermed er det mer lønnsomt for store organisasjoner å opprettholde dette, kontra mindre organisasjoner. I tillegg, om sikkerhet og pålitelighet skal ha høyest

prioritet, i tillegg må kommunikasjonen fra ledere til resten av organisasjonen være klar og tydelig (Wildawsky 1991; La Porte, sitert i Sagan, 1993).

Behov for redundans

Høyt nivå av redundans i både personal og tekniske sikkerhetstiltak, flere og uavhengige kommunikasjonskanaler, beslutningstaking og implementering kan i teorien gjøre at selv enkeltkomponenter i en organisasjon som er utsatt for feil, kan gi et høypålitelig system. Redundans er hovednøkkelen til en høypålitelig organisasjon. Videre er det viktig å ha teknisk redundans i form av duplisering (to enheter som utfører samme oppgave, eksempelvis to driftssentraler), og reservedeler som kan brukes om hoveddelen ikke skulle være tilgjengelig, og menneskelig redundans (flere i personalet kan utføre samme oppgave). I tillegg må man ha teknisk overlapp (to enheter med noen felles funksjonsområder, eksempelvis). Kommunikasjonssystemer som blir brukt på daglig basis kan gi slakk om der er nødvendig. Menneskelig overlapp handler om overlappende ansvar; selv om de faste oppgavene er forskjellige, er det nødvendig at noen mennesker har overlappende ansvar for å kryss-sjekke hverandres oppgaver. kilde

Desentralisering, kultur og kontinuitet

Selv om redundans kan øke reliabiliten er det fremdeles nødvendig å minske alvorlighetsgraden av individuelle komponentfeil, for å unngå å stresse redundante systemer utover deres kapasitet. Ledelses- og operasjonsstrategier er derfor vektlagt, som en måte å redusere dette. Sagan (1993) peker på tre karakteristikker. Først er desentralisering av beslutningstaking viktig for å respondere på en rask og passende måte. Her gjelder nærhetsprinsippet, og tanken om at den som er nærmest problemet skal ta avgjørelser. Det er viktig at overordnede, kan delegere ansvar til underordnede i en krise, slik at den blir håndtert på lavest mulig nivå. For det andre handler det om å etablere en «reliabilitetskultur» i organisasjonen som setter pålitelighet høyt og som oppmuntrer alle nivå i organisasjonen. Øvelse, trening og læring skal gi høy pålitelighet. Organisatorisk redundans vil si at individer skal ha forskjeller med hensyn til kultur, opplæring og erfaringsbakgrunn. Blir feil oversett av en person, kan det bli oppdaget av en annen person med en annen type bakgrunn. Det blir vektlagt at kolleger rådfører og korrigerer hverandre. Til sist må kontinuitet på trening og simulering vektlegges av øvelser som bidrar til å minske feil.

Organisatorisk læring

Den siste faktoren som er nødvendig for høypålitelighet er vilje til å lære. Man må tilpasse rutiner og prosedyrer over tid, gjennom prøving og feiling, og simuleringer. Fra tidligere ulykker skal man ta med seg læring og erfaring, og man kan supplere med simuleringer og analyser, og dermed kan organisasjonen lære å unngå lignende hendelser. I følge Wildawsky (1991) kan man gjennom prøving og feiling luke ut latente feil slik at man unngår de store farene, i tillegg minsker man omfanget av uforutsette farer. Ved å håndtere mindre risiko som blir oppdaget gjennom prøving og feiling på mindre skala, er man også bedre rustet til å håndtere ukjente risikoer.

3.5.1 NAT og HRT

I følge NAT er ulykker unngåelige i komplekse system med tette koblinger, uansett hva organisasjonen gjør for å forhindre dette, mens HRT hevder organisasjoner kan påvirke betydelig forebygging av ulykker. Rijpma (1997) presenterer en sammenligning av de to teoriene, hvor han påpeker at selv om de har forskjellig utgangspunkt og tilsynelatende motpoler, kan de fremdeles komme frem til samme konklusjon. Han påpeker at kompleksitet og tett kobling påvirker reliabiliten ved å øke behovet for redundans, slakk og organisatorisk læring. Dog, på den andre siden kan kompleksitet og tett kobling også minske reliabiliteten av de organisatoriske strategiene fordi kompleksitet kan nøytralisere effekten av redundans og svekke den organisatoriske læringen. HRT kan øke redundans med informasjonen om forutanelsen om antall komplekse interaksjoner, hvis slakk er ivaretatt, samtidig også redundans nivået av kompleksitet ved å introdusere tvetydighet og forekomsten av feil på samme tid. Derfor peker Rijpma (1997) på at begge teorier kan gi bedre forståelse av forhindring av ulykker og reliabilitet, om de blir brukt sammen: HRT kan forhindre ledelse fra pessimismen som finnes i NAT, mens NAT kan redusere optimismen med tanke på reliabilitetsøkende strategier. Han understreker i tillegg at det ikke enda er nok forskning på om forebygging av ulykker og reliabilitet egentlig vil være motstridende i organisasjonsdesign og beslutningstaking, men at begge perspektiv henger logisk sammen med plausible antagelser.

Sagan (1993) har også evaluert de to teoriene, og stiller seg spørsmål til hvilket av de to perspektivene som passer best med virkeligheten. Han understreker også at teoriene gir både hypotetiske og empiriske eksempler som støtter opp deres argument, men fordi ingen av dem

presenterer et presist estimat av sannsynligheten av seriøse ulykker i farlige teknologier, er det ikke mulig å fastsette et presist nummer av ulykker hvis oppdager, kan støtte eller svekke teoriene. Han fremhever også hvor lite presist språkbruken er i forhold til sannsynlighetsestimater, men at de to teoriene har samme estimat på sannsynlighet for farlige ulykker, selv om konklusjonene deres et vidt forskjellige. Sagan (1993) stiller gjennomgående spørsmål hvor for han etterspør eksempler på hva effekten av tiltak har vært: hva var effekten av å legge til ekstra sikkerhetsenheter? Forebygget den en ulykke slik HRT tilsier, eller var redundans roten til problemet, slik som NAT tilsier. Gjennom en studie innenfor det amerikanske atomvåpensystemet ble det avdekket en rekke nesten-ulykker, som kunne ha ført til katastrofer. Han peker på at elementer av HRT var til stede, og at siden det var nesten-ulykker har systemet funket. Individuelle feil vil alltid oppstå, som er grunnen til at man bygger inn redundans (Sagan, 1993; Rijpma, 1997).

4 METODE

Dette kapittelet vil ta for seg de valgene som har blitt tatt i forskningsprosessen: fra forarbeid til gjennomføring av datainnsamling og bearbeiding av datamateriale. Det vil belyses hvordan disse valgene bidrar til å besvare problemstillingen for oppgaven, og hvilke utfordringer som har oppstått underveis. Problemstilling for oppgaven er: Hvordan kan energiforsyningen etablere god beredskap på IKT-sikkerhet?

4.1 Forskningsdesign og forskningsstrategi

Denne studien ble gjennomført fra perioden februar 2016 til juli 2016, hvor det underveis i prosessen er blitt gjort flere endringer før endelig resultat. Formålet med studien har vært å undersøke hvordan energiforsyningen kan utarbeide god beredskap på IKT-hendelser, ettersom disse skiller seg ut fra fysiske hendelser (NOU 2015:13, 2015). Å utarbeide et forskningsdesign er, ifølge, Blaikie (2011) et teknisk dokument som skal være en guide for å utføre forskningen. Den skal inneholde alle sentrale beslutninger og redegjørelser til hvorfor disse beslutningene er tatt. Det skal også være en sammenheng mellom problemstilling og forskningsspørsmål, teori, empiri og konklusjon. Som Maxwell (2008) poengterer, bør kvalitative forskningsdesign være fleksible for endring underveis i forskningsprosessen. Funn i datamaterialet kan for eksempel føre til at problemstilling med fordel bør justeres for å være mest mulig relevant for det feltet man ønsker å studere. Dette ble tydelig i denne studien, da det var nødvendig å gjøre flere enderinger underveis i forskningsprosessen for endelig resultat. Gjennom hele prosessen har beredskap og krisehåndtering, med spesielt fokus på IKT vært sentrale fokusområder. Interessen for å skrive om IKT kom etter et fag på Københavns Universitet som handlet om cybersikkerhet. I tillegg var det interessant å undersøke energiforsyningen fordi det er en viktig, om ikke den viktigste, kritiske infrastrukturen. Til tross for at det har vært nødvendig å gjøre flere endringer i innfallsvinkel og problemstilling, har det overordnede tema vært konstant. Ettersom det er et nytt forskningsområde har det også hatt en betydning for hvordan flere problemstillinger har måttet endres på. Forskningsdesignet har fungert som en rettesnor, og har gjort at fokuset ble holdt gjennom hele prosessen.

Formålet med denne studien har vært å undersøke hvordan energiforsyningen kan etablere beredskap på IKT-sikkerhet og -hendelser, ved å kartlegge ut hvilke sårbarheter og trusler som finnes, hvordan eksperter og litteratur ser på beredskap, og utfordringene knyttet til IKT-

sikkerhet og beredskap. I følge Johannessen, Tufte og Christoffersen (2010), kan man ved å bruke eksplorative undersøkelser utvikle et nytt perspektiv og bidra til å se virkeligheten med nye øyne. Ved å velge den nevnte problemstillingen søker studien å utforske forhold, ettersom eksisterende kunnskap er mangelfull. I tillegg er det vanlig for eksplorative studier å identifisere problemstillinger som kan være interessante å forske videre på. Det er valgt å bruke case-studie hvor studieobjektet og analyseenhet er beredskap på IKT-sikkerhet i energiforsyningen, hvor man gjennomfører studie av analyseenhet (Johannessen, Tufte og Christoffersen, 2010; Yin 2007). For å kunne undersøke problemstillingen var det nødvendig å forstå hvordan forskjellige aktører ser på beredskap, men også hvordan andre faktorer innenfor energiforsyningen som sårbarheter og utfordringer, kompleksitet i systemer, og andre faktorer som har noe å si for hvordan man planlegger beredskap. I tillegg var det også vesentlig å finne ut hvilket syn man har på IKT-sikkerhet, ettersom det legger grunnlag for hvordan man tenker beredskapsplanlegging i forbindelse med det.

Forarbeid

Ettersom jeg ikke har en bakgrunn i IKT eller energiforsyningen var det nødvendig å sette seg inn i fagfeltet før arbeidet med problemstilling begynte. Som Johannessen og kolleger (2010) nevner bør forskningen drives av nysgjerrighet og interesse. Derfor var det nødvendig å gjøre et grundig forarbeid. Ikke bare for å innhente kunnskap om hvordan energiforsyningen i Norge fungerer, men også for å innhente kunnskap om IKT, og hvordan utviklingen i de siste årene har vært; både i Norge og andre land i verden. Gjennom databasesøk fikk jeg innsikt i hva som fantes på den aktuelle problematikken. Derfor ble det brukt mye tid på å lese gjennom rapporter. Hovedinteressen for energiforsyningen kom fra to foredrag som ble holdt på Samfunnssikkerhetskonferansen i Stavanger, januar 2016 og videre ble interessen for IKT styrket på NSM sin Sikkerhetskonferanse i Oslo, mars 2016. Betydningen ved å ha vært på disse to konferansene gjorde også at jeg fikk en bedre helhetsforståelse om forskjellige problemstillinger knyttet både til samfunnssikkerhet, IKT og energiforsyningen. I tillegg fikk jeg også anledning til å delta på NVE sin beredskapskonferanse. Dermed fikk jeg enda mer tilspissede observasjoner, og fikk i tillegg bekreftet en del informasjon som ble sagt under intervju.

4.2 Data og datainnsamling

Datainnsamlingen for denne studien ble utført fra studiens begynnelse, februar, til juni. I følge Blaikie (2011) kan data deles inn i tre grupper; primær, sekundær og tertiær, hvor primærdata er data forskeren selv har samlet inn, sekundærdata er data som hovedsakelig er samlet av andre forskere, mens tertiærdata er data som er samlet inn og analysert av andre forskere. Triangulering ved å samle inn data fra flere ulike kilder, gjør det mulig å belyse problemstillingen fra flere ulike vinkler, og reduserer sjansen for at funn kun er et resultat av tilfeldighet eller feilkilder ved en type metode (Maxwell, 2008).

4.2.1 Dokumentstudier

Ettersom jeg ikke har en bakgrunn fra IT eller IKT, var det nødvendig å samle inn så mye informasjon som mulig på forhånd. Dette ble gjort ved å studere og gjennomgå en rekke dokumenter som for å få et oversiktsbilde over situasjonen i energiforsyningen, i tillegg til et helhetsbilde av IKT-sikkerhet, og problematikken som eksisterer rundt dette forholdsvis nye feltet. Dokumentene som er hentet inn er offentlige dokumenter som ligger tilgjengelig for alle (eks. NOU:2015:13, 2015; Politidirektoratet, 2015; Departementene, 2012). I tillegg til norske dokumenter og rapporter, var det viktig å se på internasjonale publikasjoner i tillegg for å få bedre forståelse om temaet (ENISA, 2014). Det brukes internasjonal forskning som grunnleggende informasjon i mange norske rapporter. Det er ikke gjennomført *analyse* av dokumentene, med analyse menes at innholdet i dokumentene ikke er delt opp og satt i tema, men heller et dokumentstudie, hvor det er blitt lest gjennom dokumenter og tatt notater under veis.

Et spesielt viktig dokument for denne oppgaven har vært NOU, 2015:13, *Digital sårbarhet – sikkert samfunn*. Dette er fordi det er en utredning som er veldig ny, og dermed er oppdatert på situasjonen både i energiforsyningen og andre sektorer. I tillegg er det vektlagt IKT-sikkerhet, og dermed gir en samlet forståelse på alle problemstillinger knyttet til IKT-sikkerhet. Flere dokumenter og rapporter er også brukt som empirisk grunnlag, og er med på å styrke empirien som blir presentert i denne oppgaven.

4.2.2 Intervju og gjennomføring av intervju

Hensikten med å intervjue er å finne ut hva folk tenker, som vi ellers ikke kan finne ut ved å kun observere (Patton, 1990). Det er blitt gjennomført ni intervjuer, hvor to er virksomheter

fra energiforsyningen, og de resterende syv med eksperter. Intervjuene ble avholdt i april og mai, tre på telefon og Skype, mens de seks andre ble utført ansikt til ansikt. Det ble på forhånd utarbeidet en intervjuguide som, på forespørsel av de fleste informantene, ble sendt på forhånd. Intervjuguiden ble utarbeidet med semi-strukturerte spørsmål (se vedlegg 1), og delt opp etter tema. Semistrukturerte intervju har en liste med tema som bør bli gjennomgått, men samtidig tilbyr det mulighet til å endre på rekkefølge på både tema
og spørsmål. Som Patton (1990) påpeker, betyr det altså ikke at man må følge intervjuguiden, men man skal ikke legge til andre tema enn de som står oppfør. I tillegg har man en intervjuguide for at mer eller mindre samme informasjon vil bli innsamlet i alle intervjuene. I følge Kvale (1996), er fordelen med å ha semistrukturerte spørsmål er at man bedre åpner for en dialog med informanten, og man låser seg ikke til og slavisk følge alle spørsmålene, men det blir mer som å ha en uformell samtale. I alle intervju var dette ønskelig, ettersom det er enklere både for informant og intervjuer å komme med oppfølgingsspørsmål. Selv om det etter intervjuene ble gjennomført ble gjort en endring av problemstillingen, er denne endringen gjort med tanke på den informasjonen som ble innhentet. Likevel ble det innhentet tilstrekkelig informasjon til å kunne jobbe med den problemstillingen som er presenter i denne oppgaven.

4.2.3 Valg av informanter

Valg av informanter ble gjort strategisk (Patton, 1990). Formålet med strategisk utvalg var å sikre rik informasjon på tema fra et relativt lite utvalg (Kvale og Brinkmann, 2009). Dermed ble sentrale aktører innenfor IKT-sikkerhet spurt om å delta i denne studien. Selv om det alltid er en mulighet for at alle aktuelle kandidater ikke kan stille til intervju, ses utvalget av informanter på som en kunnskapsrik gruppe om det valgte temaet. Informanter ble kontaktet både per telefon og epost, og alle informanter gav meg anledning til å sende oppfølgingsspørsmål på epost i etterkant, noe som derimot ikke ble benyttet. De gav også samtykke på at intervjuene kunne bli tatt opp på båndopptaker, noe som ble gjort på alle intervju. De ble også tilbudt å få sendt epost med bekreftelse om at opptaket ble slettet etter at oppgaven var ferdig, noe som også ble gjort, selv for de som sa at det ikke var nødvendig. Ved å bruke båndopptaker sikrer man seg at all informasjon som ble gitt under intervju, bevares slik at intervjuer kan gjennomgå den senere. Intervjuene ble transkribert i etterkant for videre analyse. Som nevnt ble det gjennomført ni intervju, med ti informanter, ettersom

det ene intervjuet hadde to informanter tilstede. Tabell 1 gir en presentasjon av informantene som deltok i studien.

NVE	Sektormyndighet
KraftCERT	Energiforsyningens egen CERT funksjon.
Nettselskap	Nettselskap i energiforsyningen.
Produksjonsselskap	Produksjonsselskap i energiforsyningen.
NSM	Sentral myndighetsaktør, med særlig ansvar for oppfølging av IKT-sikkerhet.
NorSIS	Uavhengig virksomhet som jobber for å styrke IKT-sikkerhet i samfunnet.
NSR	Privat organisasjon, representerer norsk næringsliv. Deltar i forebyggende og utviklende arbeid. Ansvarlig for Mørketallsundersøkelsen.
BDO	IT-revisjon og – risikostyring, sikkerhet og beredskap.
Mnemonic	Privat organisasjon, spesialist på IKT-sikkerhet.

Tabell 1: Presentasjon av informanter.

Alle informantene som deltok i denne undersøkelsen var personer som i tillegg til IKT-sikkerhet, hadde kjennskap til, eller arbeidet med beredskap. Selv om ikke alle informantene er direkte tilknyttet energiforsyningen har de likevel kompetanse og erfaring som kan overføres til energiforsyningen. Det viste seg også at alle informantene hadde god kjennskap til energiforsyningen, og dermed fikk jeg samlet inn verdifull data.

Ettersom informant er et hankjønnsord (en informant) vil derfor alle informantene bli omtalt med det personlige pronomenet ”han”, for å holde en nøytral linje gjennom hele presentasjonen av empirien og informanter.

4.3 Datareduksjon, analyse og fortolkning av data

Etter å ha gjennomført intervjuer og samlet inn viktige rapporter, var det nødvendig å redusere mengde data. Som Johannessen et al. (2010) påpeker, er det nødvendig å redusere informasjonsmengden slik at det blir håndterlig. Dette kan ofte være en utfordring for kvalitative data, ettersom den som har samlet inn data også bør analysere og fortolke dem. Dataanalysen har to hensikter, den første er å organisere data etter tema, den andre hensikten er å analysere og tolke. Derfor ble intervjuene ble transkribert. Deretter ble transkripsjonene redusert og satt opp i tematiske bolker etter det teoretiske rammeverket som ble valgt for oppgaven. For kvalitative, i motsetning til kvantitative data, finnes det ingen løsning på hvordan dette skal gjøres (ibid.). Empirien ble fremstilt etter de samme temaene som ble satt opp i dataanalysen slik at det ikke skulle oppstå noen forvirringer når dataene skulle omstruktureres. En viktig moment med tolkning av data er at det naturligvis kan forekomme at forsker feiltolker, eller kun oppdager det som er kjent fra før av, og dermed går glipp av verdifull informasjon.

4.4 Reliabilitet og validitet

Reliabilitet (pålitelighet) omhandler om resultatet fra en studie og undersøkelsens data i form av hvordan de brukes, samles inn og bearbeides (Johannessen et al., 2010). Med dette menes nøyaktigheten, eller kvaliteten av undersøkelsens data. For å teste reliabiliteten kan man eksempelvis gjøre undersøkelsen om igjen, for å se om man får de samme resultatene (etterprøvbarhet), men, som Johannessen et al. (2010) påpeker, er dette ofte vanskeligere i kvalitative studier. Dette er fordi man ikke bruker helt strukturerte metoder. I denne oppgaven er det blitt benyttet dokumentstudier og intervju. Med tanke på at store deler av empirien er bygget opp på data som er innhentet, kan det knyttes noen problemstillinger til det. Først og fremst var ikke intervjumetoden helstrukturert, men semistrukturert, dermed oppstår det spørsmål underveis som kommer naturlig i samtalen man har. Siden hvert intervju ikke er likt, til tross for intervjuguide, kan det da fremkomme informasjon fra noen som ikke fremkommer i andre. Dog, intervjuguide er med å øke reliabiliteten, kontra det å ikke ha en. I tillegg kan man trekke frem hvilket forhold informantene hadde til den valgte tematikken. Det er også viktig å nevne at all informasjon man får fra intervju er en subjektiv mening, hvor informanten blir spurt om sitt synspunkt, dermed kan det, avhengig av hvem man snakker med i samme organisasjon, komme frem ulike svar. Et annet sentralt moment er hvor lang erfaring en informant har i forhold IKT-sikkerhet og beredskap. Blant annet vil en person

som har jobbet lenge med denne problemstillingen ha et annet syn enn en som er ny på området. Dette understreker det igjen problematikken med intervju. Med tanke på dokumentene som er brukt, anses disse for å styrke reliabiliteten ytterligere, fordi de fremstår som mer objektive, og de fleste er skrevet av et utvalg mennesker, som også øker objektiviteten. Det har, etter beste evne, blitt brukt forskningsdokumenter, men i noen tilfeller har det også blitt brukt andre type dokumenter, eksempelvis årsrapporter

Validitet, i følge Bryman (2004) handler om en måling egentlig måler det man tror det måler; handler om gyldigheten og sammenheng mellom problemstillingen som er satt opp, og dataene som er samlet inn (Johannessen et al., 2010). Man kan dele inn i troverdighet (intern validitet) og overførbarhet (ekstern validitet). Man kan såfremt ikke måle kvalitative data, men som Johannessen et al. (2010) påpeker er validitet et spørsmål om forskerens fremgangsmåter og funn reflekterer formålet med studien. Det ses på som en styrke for den interne validiteten at det i denne oppgaven er blitt brukt metodetriangulering; dokumentstudier, intervju og observasjoner. I tillegg har også informasjonen blitt diskutert i fortrolighet med veileder. En svakhet er dog at siden jeg er alene om å skrive denne oppgaven er det mine tolkninger som ligger til grunn, og ingen andre sine. Derimot er det på intervju blitt spurt om de samme temaene, og også blitt spurt om synspunkter på informasjon hvor jeg ikke har vært sikker. I tillegg har jeg brukt veldig mye tid på å lese og studere dokumenter angående tematikken, slik at jeg skal kunne forstå det bedre. Det å delta på konferanser har også gjort at jeg har fått bedre forståelse for konteksten. Overførbarhet handler om hvorvidt man kan overføre kunnskap til andre områder enn det som studien er innenfor (Johannessen et al., 2010). Ettersom denne studien handler om beredskap på IKT-sikkerhet, hvor teori om beredskap, system og organisatoriske faktorer, kommer sammen, ses dermed overføringsmulighetene som store ettersom prinsippene vil være de samme uansett hvilken type organisasjon eller virksomhet det gjelder, såfremt det er bruk av IKT-systemer.

4.5 Etiske betraktninger

Siden det finnes klare krav fra Sikkerhetslov, Energilov og Beredskapslov og – forskrift, om hvordan sensitive opplysninger skal håndteres er det unngått å spørre om noe som kan vedrøre dette. Dermed er det også en sjanse for at informasjon som kunne ha vært til interesse for studien ikke ble innhentet. Spesielt med tanke på intervjuene med virksomhetene i energiforsyningen og deres tanker rundt IKT-sikkerhet og beredskap.

Alle opplysninger er behandlet konfidensielt slik at ingen skal kunne gjenkjenne enkeltinformanter eller virksomheter i energiforsyningen. Informasjon skal ikke kunne skade virksomhetene, dette blir dermed ivaretatt med at verken navn på virksomhet, geografisk beliggenhet eller navn på informant ble nevnt. Med tanke på eksperter og deres organisasjonene, er navnene deres holdt anonyme, men alle har gitt samtykke på at organisasjonen de representerer kan bli brukt. Informanter signerte på forhånd et samtykkeskjema, hvor de også er gjort oppmerksomme på at lydopptak blir slettet etter innlevert oppgave. Lydopptakene er i tillegg tatt opp på en analog båndopptaker. Informanter blir betegnet som ”informant 1”, ”informant 2”, og blir som nevnt tidligere alle referert til som "han".

4.6 Styrker og svakheter ved valgt metodebruk

På grunn av begrensninger på omfanget av oppgaven har det ikke vært mulig å få snakket med mer enn et visst antall mennesker i forbindelse med intervjudata. Totalt er det snakket med ti personer, hvor kun to er fra virksomheter. Det var ønskelig å ha med flere virksomheter fra energiforsyningen, noe som dessverre ikke lot seg gjøre. Selv om det kan ses på en mangel at ikke flere virksomheter innen energiforsyningen er tatt med i studien, viste det å være vanskelig å få virksomheter til å stille opp til intervju. Dermed kan ikke dette utvalget sies å være generaliserende for hele energiforsyningen, men det gir et bilde over hvordan man forstår IKT-sikkerhet og beredskap. Det hadde vært ønskelig å intervjue flere, og om man hadde valgt en kvantitativt studie, kunne man ha nådd ut til flere enn ved å bruke en kvantitativ spørreundersøkelse. Derimot går kvalitative intervjuer mer i dybden og dermed får man innhenter informasjon som det gjennom kvantitative spørreundersøkelser ikke hadde vært mulig å hente inn. Ved å ha semistrukturerte, åpne spørsmål er det muligheter for både intervjuer og informanter å tilføye informasjon. Det gjør at datainnsamlinga kan ha produsert viktig informasjon, man ellers ikke hadde fått tilgang på. Likevel, på grunn av antall rapporter som denne oppgaven også baseres til, er det mulig å gi et slags bilde over hvordan situasjonen er. Det er viktig at rapportene har blitt brukt på en aktiv måte, for å gi et mer objektivt bilde. Gjennom intervju får man subjektive meninger, som ikke trenger å være representative for virksomheten. Selv om det er blitt intervjuet åtte stykker som sitter på mer overordnet nivå, definert som rådgivere/eksperter, er det fortsatt viktige organisasjoner som

ikke er inkludert, eksempelvis Energi Norge og Kraftforsyningens beredskapsorganisasjon, som også er gode representanter med innblikk i hvordan sektoren fungerer. Til tross for dette ses de åtte som er blitt intervjuet som representative med tanke på kunnskap og kompetanse.

5 EMPIRI

I det følgende vil det gis en presentasjon av datainnsamlingen. Empirien består av data fra intervju og data innhenter fra dokumenter. Empirien er delt opp i fem tema: 1. Trusselbildet, 2. Beredskap og IKT-beredskap, 3. System, teknologi og kompleksitet, 4. Kompetanse, og 5. Samvirke og informasjonsdeling.

5.1 Trusselbildet: trusler, sårbarheter, utfordringer

Hagen (2015) understreker at truslene mot samfunn og individ har økt i takt med digitalisering av samfunnet, hvilket setter større krav til myndigheters og virksomheters risikostyring. Hagen (2015) trekker frem trusler som identitetstyveri, svindel, industrispionasje og etterretningsvirksomhet. Informant fra produksjonsselskap forteller at det er vanskelig å orientere seg om hva som er et trusselbilde, og påpeker at det er andre i landet som sitter på mer informasjon, og nevner politiet og forsvaret som aktuelle instanser. Når han blir spurt om hvilke IKT-relaterte trusler han ser på som gjeldende for selskapet sitt, nevner han hacking. Det forklares hvordan hacking av styringssystemene som brukes på fjernstyring blir muligjort, og hvorvidt dette kan få konsekvenser for anleggene. Informant fra nettselskap forteller videre at selskapet ser på det å komme seg inn i driftskontrollsystemet som en reell trussel, og at et komplekst trusselbilde gjør det vanskelig å holde tritt med trusselaktørene. Begge to nevner hvordan løsepengekreving for nedlåste systemer kan være en potensiell trussel, og informant fra nettselskap nevner i tillegg faren for at trusselaktør kan komme seg inn i system ved å manipulere faktureringsinformasjon.

NSM (2016) har sin forklaring av hvordan dataangrep utføres, og peker på epost som en vei inn i systemet Dette refereres ofte til som *phishing*, eller infiserte nettsider. Spionasje er som oftest den mest kraftfulle og vedvarende trusselen, hvor målet dreier som omkring å skaffe informasjon om produksjon, metoder og teknologiske muligheter. Rapporten understreker i tillegg at angrep som er avdekket i 2015 holder et mer avansert og komplekst nivå enn tidligere. Informant fra KraftCERT nevner i den sammenheng angrepet på Ukraina, som viste hvor mye forarbeid som var lagt ned. Selv sier han og informant fra Mnemonic at man foreløpig ikke har sett så store hendelser i Norge. Informant fra NVE legger til at han tror systemet er robust og godt beskyttet med regelverk. I tillegg sier informanten fra NVE at det ikke vil være vanskelig å forutse konsekvensene av et eventuelt angrep på alle linjene som

går inn til Oslo. Han understreker at driften av anleggene er viktigst, og trekker frem Norges desentraliserte produksjon som oppbyggende for et robust nettverk.

Det er enighet mellom informantene fra NSR, NorSIS og NSM om at kompleksiteten i trusselbildet er problematisk. Disse utsagnene styrkes av NSM (2016) sin rapport hvor det understrekes at metodebruken og kompetansenivået til trusselaktørene er betydelig mer avansert. Informant fra NorSIS nevner i tillegg en økning i angrep på mennesker, og forteller at mer avansert teknologi gjør det vanskeligere å angripe systemet. I disse tilfellene vil det være mer hensiktsmessig å angripe mennesker. Dette blir også påpekt i *Datakrimstrategien*, hvor sosial manipulering nevnes som et verktøy for å få inn ondsinnet kode. Videre trekkes frem metoder som innebærer fristelser, tiltrekning, sympati, tillit, autoritet, frykt og knapphet (Politidirektoratet, 2015). Informant fra NorSIS nevner blant annet økning i datingsvindel.

NSR, NorSIS, NSM og BDO nevner ganske spesifikt hvor vesentlig avhengigheten til leverandørene har blitt. På grunn av den økende avhengigheten til leverandører, samt en mulig mangel på bestillerkompetanse in-house, er en bedring av sistnevnte nødvendig. Informant fra Mnemonic mener forøvrig at manglende kompetanse hos leverandørene er et problem. Bestillerkompetanse er et viktig tema som blir tatt opp i *Mørketallsundersøkelsen* (NSR, 2014). Undersøkelsen viser at små virksomheter kommer dårligst ut når det gjelder å følge opp leverandører, og god bestillerkompetanse blir fremhevet som avgjørende for å sikre data hos underleverandør. Mange har drift av IT-løsninger hos underleverandører, og undersøkelsen nevner i tillegg flere hendelser hvor man har kommet seg inn via underleverandør (NSR, 2014). Informant fra produksjonsselskapet peker også på problematikken som oppstår når flere i bransjen har samme leverandører. Det vil i praksis kunne bety at en hendelse vil kunne ramme alle.

Informanten fra NSM understreker at det tidligere ble brukt lukka SCADA-systemer, og at brukerne muligens mangler forståelse for at disse funksjonene nå er online. Dette betyr at kompetansen på dette feltet må økes. Informanten fra KraftCERT nevner i denne sammenheng at det er vesentlig at informasjon blir delt og kommunisert. Alle informantene er enige om at det finnes betydelige utfordringer knyttet til informasjonssikkerhet, hvor informanten fra NVE i tillegg trekker frem at NVE ikke har samme syn på informasjonssikkerhetskulturen innad i direktoratet. Disse uoverensstemmelsene kan igjen skape problemer for virksomheter. Han utdyper med å fortelle om velvillighet hos mange,

men understreker samtidig at det finnes andre som er mindre velvillige. Selv om sikkerhetskulturen ikke er festet hos alle, burde det tilstrebes at alle har den samme forståelsen. Dette blir støttet av informanten fra nettselskapet, basert på hans opplevelse av en kultur hvor man ofte mottar motstridende informasjon.

5.2 Beredskap og IKT-beredskap

Kapittel 2, generelle krav, i beredskapsforskriften stadfester hvordan virksomheter er pliktige til å ha en beredskapsleder som skal sørge for nødvendig planlegging og utøvelse av beredskapsarbeidet, en beredskapskoordinator som skal være administrativt kontaktpunkt til beredskapsmyndigheten (NVE), og en IKT-sikkerhetskoordinator som skal være faglig kontaktpunkt til beredskapsmyndigheten. Videre stadfester den at man har beredskapsplikt, skal utføre risiko- og sårbarhetsanalyser, skal ha beredskapsplanlegging, varsle og rapportere, gjennomføre øvelser, ha informasjonsberedskap, samt ha evaluering etter øvelser og ekstraordinære situasjoner. I tillegg skal man ha et internkontrollsystem som dokumenter etterlevelse av krav i energiloven, kapittel 9, og energilovforskriften (Beredskapsforskriften). I henhold til beredskapsplikten, skal det arbeides med forebyggende sikkerhet og beredskap, og §2-4 plikter virksomhetene til å gjennomføre ROS-analyser, hvor man skal identifisere risiko og sårbarhet ved alle funksjoner, samt tiltak for å oppfylle kravene i forskriften. Kapittel 2, § 2-2, , punkt 2.2.6 i veilederen (NVE, 3013) som går spesifikt inn på IKT-sikkerhetskoordinator, vektlegger hvordan IKT-sikkerhet er et stadig viktigere tema, og derfor skal virksomheter ha god faglig kompetanse på IKT-sikkerhet og IKT-beredskap, og IKT-trusselbildet.

5.2.1 ROS, beredskap, planlegging

Informant fra produksjonsselskap sier at for dem betyr beredskap at de skal klare å håndtere plutselig oppståtte situasjoner, som de med ordinær linje er ute av stand til å håndtere. I tillegg nevner han at dette krever et planverk som må være innøvd i forkant av aktuelle hendelser. Han nøler på spørsmål om planlegging, men sier at alle er kjente med sine oppgaver, og at de har (som de er pålagt) beredskapsleder, beredskapskoordinator og IKT-leder. De har en kobling mellom ROS-analysene sine og beredskapsplanene, og han forteller om en sammenheng mellom lagte planer og reelt utfall, samt påpeker at det blir gjort en risikovurdering i slike tilfeller. På spørsmål om det blir utført verdivurderinger, nøler han litt før han svarer, og spør om det er kroneverdi det er snakk om. Han forteller videre at

produksjonsselskapet har gjennomgått og vurdert hva som skal forsikres, og hvilken forsikringspremie som skal brukes. Det blir understreket at de gjør en jobb i forbindelse med forsikring og reservedeler, og beregning av kostnader for tapt produksjon. Beredskapsforskriften bygger på beredskapsprinsippene, som vil si at hvert enkelt selskap skal håndtere sine problem, og at det er deres ansvar. ROS-analyser godkjennes ikke av NVE, men informant forteller at disse skal vises frem ved tilsyn. Videre nevner han at det bør være en kobling mellom ROS-analyser og beredskapsplan, og at man bør se for seg styringshjulet.
God beredskap på IKT-hendelser innebærer å skape forebyggende driftskontrollsystemer, og at rutiner etableres. Videre informerer informanten at det er knapt med tid, hvilket underbygger behovet for gode sikkerhetsvurderinger og – rutiner. Han understreker at sikkerhet ikke burde gå på bekostning av økonomiske kutt. Videre peker han på at kraftsektoren har blitt den viktigste infrastrukturen, noe som burde gjenspeiles i sikkerhetstiltakene. Informanten mener at det er feil at utviklingen har gått mot færre ansatte, når menneskelig redundans innehar en slik viktighet i styringen av IKT-systemer.

KraftCERT sier beredskapsorganisasjon setter sammen, og jobber ikke konstant sammen hele tiden, mens det gjør de. Dermed sier han at de gjør det litt enklere på noen områder siden de ikke trenger å omstille seg. Informanten forteller at en viktig del av beredskapen er å trene heller enn å øve. På denne måten vil man være i bedre stand til å ta raske avgjørelser som angivelig er mindre preget av feil. Hva angår ivaretagelse av sikkerhet sier han at dette vil være avhengig av de ulike virksomhetene. Han trekker frem høy kostnad på kommersielle løsninger som et problem, men understreker samtidig at løsningene ikke nødvendigvis trenger å være kostbare. Det viktigste vil være å identifisere noe som gir løsninger raskt, slik at man får mandat av ledelsen til å fortsette. Han påpeker at enkelte virksomheter har sine ansatte ”in-house” (i bedriften), mens andre har ”outsourcet” del av sin bemanning. Det er imidlertid bra at sikkerhetsleder ikke kan outsources. Videre forteller han at sikkerhetslederen må komme til gode avtaler med outsourcingsselskapet om prosedyrene for loggføring og dataisolering.

Et relatert problem er fargekoding av beredskapsnivåer (risikoakseptkriterier). Nivåer for beredskapsorganisasjonen reflekterer ikke nødvendigvis nivåene som finnes hos KraftCERT. Beredskapsledelsen er vant til et fysisk beredskapsnivå, hvilket kan føre til at disse ikke forstår omfanget og alvoret på gult nivå 1. Han nevner i tillegg at fysisk sikkerhet og informasjonssikkerhet ikke sammenfaller på en hensiktsmessig måte.

De to informantene fra BDO er enige om at beredskap handler om å lære av tidligere hendelser, bli bedre som følge av dette, være fremsynt, ta innover seg nye trusler, og jobbe på en proaktiv måte med disse elementene. De vektlegger viktigheten av øvelse og trening, samt utvikling av beredskapsplaner. Informasjon og informasjonssystem har større verdi, og trusselbildet endres da i forhold til dette, som føret til at bransjen som en helhet må jobbe mer aktivt med IT-beredskap. Når det kommer til kobling mellom ROS-analyser og beredskapsplaner, forklarer det at dette bestemmes av hvilket nivå det er. Kriser er ofte dynamiske, som kan føre et annet utfall enn det man opprinnelig forventet. På IT-siden er det avhengig av hvilken kompetanse man har til rådighet i håndteringen av en situasjon. Dette kan være alt fra å ringe til leverandører til å tilkalle egne ansatte for å starte med feilsøking. Dermed munner alt ut i ROS-analysen, hvor evnen til å oppdage og håndtere er viktig. Etter informant 1 sin erfaring er beredskapsplaner for IKT-sikkerhet svært underutviklet, hvor få IT-hendelser egentlig blir omtalt i beredskapsplanen. Dette begrunnes med at planene ofte har nye elementer, og at de ansatte ikke har et forhold til innholdet. En typisk karakteristikk for selskapene som har jobbet mye med IT er at det er en god kobling mellom IT-avdeling og toppledelse. IKT-systemer er ulikt satt opp, og man må jobbe med tilpasset beredskap. Herunder faller viktigheten av å bruke god tid på planlegging. I tillegg burde det gis økt fokus på å etablere en positiv varslingskultur, hvor brukerne blir informert om viktigheten av å si ifra, samt bli minnet på at alle kan gjøre feil. Hovedmålet vil være å oppdage feil ved et tidlig tidspunkt, hvilket kan muliggjøre en effektiv håndtering av eventuelle feil i systemet.

Informant fra NSR snakker innledningsvis om verdivurdering, og hvor viktig det er å vite hvilke verdier man har og hvilke konsekvenser det vil få om det faller bort, blir borte, eller blir kopiert. Han peker på en tendens som ofte blir sett i offentlig sektor, nemlig at sektoren er bevisst verdier i sin virksomhet, men ikke i forhold til en tredje part. Han sier at det må være en kobling mellom ROS-analyser og beredskapsplanen, og en verdivurdering. Han utdyper at dette vil gjenstå som det viktigste, og det er lite hensiktsmessig å beskytte noe man ikke ser verdien i. NSM sier seg også enig i bruk av verdivurderinger, og heller enn å vurdere alt, må man finne de kritiske verdiene og legge betydelige sikkerhetstiltak på dem. Videre nevner han 5832, sikringsanalyse, og ISO-standard på ROS-analyser. Samtidig påpekes det at en bruk av disse prinsippene fører til en ROS-analyse bestående av verdi, risiko, sårbarhet og trusselvurdering. Hos NSR er budskapet å endre på elementer som er endringsbare: sårbarheten og konsekvensreduserende tiltak. Videre påpeker han at det er gjennom ROS-

analyser man velger hvilken risiko man vil ta, restrisikoen er det som i teorien utgjør hva man må ha beredskap for. I ROS-analysen jobber man med scenarioer og hvilke konsekvenser diverse hendelser vil ha. I tillegg er viktig å finne ut hvor lang tid det tar før man er tilbake til normalen dersom en ulykke inntreffer. Han understreker at det er her man må legge inn beredskap. Eksempelvis hvor raskt man responderer og hva man skal respondere med. En suksessfull ROS-analyse vil beskrive hva man kan bli utsatt for, selv om man aldri kan sikre seg hundre prosent. Han understreker at det viktigste er verdivurderingene hvor man må ta høyde for hva man har hvor, konsekvenser av om andre får innsyn, hvordan man er beskyttet, og om man kan beskyttes ytterligere. Han understreker også at tillit er viktig. Når det kommer til IKT-sikkerhet, tror han at de fire rådene fra NSM (se tabell 1) vil fungere som gode retningslinjer. Her vil små ting gi store gevinster.

Slik stopper du en stor del av alle angrep:
• Oppgrader program og maskinvare. Nyere produktsversjoner har tettet flere sikkerhetshull enn gamle, og er bedre på sikkerhet.
• Vær rask med å installere sikkerhetsoppdateringer. Kunnskap om nye sårbarheter sprer seg raskt. Derfor bør systemeiere være tilsvarende raske med å oppdatere. Før noen bruker sårbarhetene til å bryte seg inn.
• Ikke tildel sluttbrukere administratorrettigheter. De fleste vanlige brukere har ikke behov for å installere programvare på maskinen. Overlat administrasjon og distribusjon av programvare til de som kan det.
• Blokker kjøring av ikke-autoriserte programmer. Bare la brukere kjøre godkjente programmer ved å bruke verktøy som Windows AppLocker.

Tabell 2: Effektive tiltak mot dataangrep (NSM, 2015, s. 9; NSR, 2014, s. 4).

Informanten fra NorSIS sier at det er vanlig at man finner en beredskapsplan på arbeidsplassen, hvor det kritiske spørsmålet er om man har øvd og testet den ut. Han er av den oppfatningen at det er viktig å ha en beredskapsevne. I tilfeller hvor planen ikke er optimal, vil en involvert aktør som har øvd på beredskap være en viktig ressurs. Han legger også til at virksomheten bør tilstrebe å få planen utviklet av sine egne, heller enn å ansette eksterne konsulenter som ikke skaper en plan som ikke blir brukt. Han nevner videre at man må ha et forhold til samfunnssikkerhetsprinsippene, spesielt nærhet til håndtering. Det er en dårlig idé å ha en beredskapsorganisasjon og kriseorganisasjon som ikke er en del av det

daglige virket, for da blir det en skjevhet mellom metodikktilnærming og lignende. Han understreker at alle som har et definert trusselbilde mot seg må ha en beredskaps- og krisehåndteringsevne og kapasitet som sin primære jobb. I praksis vil dette bety at enkelte har et daglig ansvar, hvor andre har et ansvar som tas frem i nødvendige situasjoner.

Når det gjelder ROS-analyser, viser han til at det finnes to faglige skoler. Den første måten å vurdere en trussel på følger Norsk standard (NS) 5814, og konsekvens og sannsynlighet. Hans personlige mening er at det er en uegnet metode, fordi de truslene det er snakk om ikke er tilfeldige, ”man kan ikke trille terning på om Russland skal angripe Telenor”. Den andre måten er å vurdere trussel etter den informasjonen man har, og gjøre en verdi- og sårbarhetsvurdering. Ifølge informanten er dette to forskjellige ting, hvor førstnevnte er en årlig vurdering og den sistnevnte er en daglig metode som brukes av forsvaret. Med en slik tilnærming kan man ha en beredskapsplan som er litt overordnet, og så ha en dag-til-dag risikoanalyse basert på håndteringen av det som skjer. Man må uansett være observant på at beredskapsplanen ikke blir bokhyllefyll. Når det kommer til risikoakseptnivå, er det også noe som skiller de to metodene fra hverandre. NS-5814 krever at ledelsen avgjør et akseptnivå omtrent før arbeidet begynner, mens den andre avgjør det mer fra dag til dag. Han forklarer at ”risikoapetitten” endrer seg, og at det må inn i det dynamiske som skal vurderes, og at det er det som er verdivurderingen. Han mener at samspillet mellom hvilke krav ledelsen setter til sin virksomhet, og at det avhenger av hva den operative ledelsen sier om hvor viktige datasystemet er viktig for beredskap på IKT-hendelser.

Informanten fra NSM legger forhåndsplanlegging som grunnlag for godt beredskap. Man må vite hvem som skal gjøre hva og når. En detaljert beredskapsplan er ikke tilstrekkelig, fordi det sjelden vil være mulig å si noe spesifikt om hva som kan komme til å skje. ROS-analyser må inkluderes, helt ned til banale ting (hva er man villig til å akseptere?). Beredskapsplanen må være løsere, men likevel oversiktlig nok til at alle er informert om hvilket ansvar de har. Det må i tillegg trenes på ulike scenarioer. Det skal være en kobling mellom ROS-analyser og beredskapsplaner, men man kan ikke ta alle risikoer å lage en handlingsplan på hver eneste, det ville blitt massivt og uoversiktlig. Det viktigste er å ikke tildele folk oppgaver og roller som de ikke har til daglig. Når det kommer til beredskapsprinsippene, sier han at store organisasjoner kan drive med det hele tiden, basert på at man er ikke i konstant krise. Man må allikevel ha en beredskapsledelse, og jo lavere man kommer - jo vanskeligere blir det.

Informanten forteller videre at en virksomhet som har ressurser til teambuilding for ledergruppa vil også frembringe ressurser til å kunne trene på beredskap.

Mnemonic sier at generelt kan man være mer bevisste og bedre forberedt på uønskede hendelser og håndteringen av disse. Uønskede hendelser kan være fysiske, ondsinnede og menneskerelaterte, eller ødeleggende tilfeldigheter. Mnemonic tilbyr rådgivning på ROS-analyser både på et teknisk og et organisatorisk nivå. Førstnevnte verifiserer om de aktuelle systemene holder et tilstrekkelig teknisk nivå, mens vurderinger på et organisatorisk nivå undersøker hvorvidt organisasjonen har fornuftige rutiner og praksiser for å ivareta informasjonssikkerhet.

5.2.2 Håndtering, rapportering, varsling

I Beredskapsforskriften § 3-4 står det at KBO-enheter har ansvar for oppgaver og plikter gitt under energiloven, herunder planlegging og håndtering av ekstraordinære situasjoner og gjenoppretting av normalsituasjon. Mørketallsundersøkelsen (NSR, 2014) påpeker også hvordan egne ansattes evne til oppfølging av alarmer og logger anses som virksomhetenes viktigste kilde til å oppdage hendelser, og en anbefaling fra undersøkelsen er at man etablerer rutiner for hendelsesrapportering. Hagen (2015) påpeker videre i sin rapport at energiforsyning må overvåke og logge alt som er av betydning for informasjonssikkerheten, og at man må ha fullstendig sporbarhet på hendelser.

Når det gjelder informasjonssikkerhetshendelser, skal alle hendelser rapporteres etter kapittel 2-6 i Beredskapsforskriften, og alle KBO-enheter skal varsle myndighetene. NVE sier videre at de har håndtert hendelser som de har blitt rapportert, og på informasjonssikkerhet har man vært mye klarere på veiledning, som igjen er avhengig av tillit. Selve hendelseshåndteringen er selskapene sitt eget ansvar (jmf. ansvarsprinsippet). Selv sier han at han syns de har hatt god oppfølging, men at det de ikke har oversikt over mørketallene (MU Trekk inn her). Samtidig understrekes det at NVE har fulgt opp hendelser basert på deres forståelse for situasjonen. Han skulle også ønske at forståelsen fra sikkerhetsmiljøet hadde vært større for hva NVE evner å gjøre.

Når det kommer til hendelseshåndtering, sier informant fra produksjonsselskap at han dessverre ikke kjenner rutinene godt nok, ettersom han nettopp begynt i innehavende stilling. Videre på spørsmål om sikkerheten er ivaretatt, sier han at han ikke tror på at det er god

ivaretagelse av IKT-sikkerhet. Han forteller om en vektlegging av mer generell sikkerhet, hvor ansatte i anlegg er mer opptatt av at det ikke skal oppstå skader og at uvedkommende ikke skal kunne komme inn på anleggene. Videre forteller han at ikke tror de er særlige gode på bevisstgjøring omkring bruk av USB-minnepinner. Gode rutiner på å minne ansatte på dette sier han er en ferskvare, og at det er en stund siden de hadde kampanjer som omtalte dette. Dermed må det komme nyere holdningskampanjer som spesielt peiler seg inn mot hva man skal tillate. Her må IKT-arkitektene komme med løsninger som fungerer. Informant fra nettselskap forteller at de har logger som registrerer det som skjer. Disse loggene blir tatt opp og gjennomgått i møter. Konsernet har tidligere hatt denne oppgaven, men han sier at de sikter på å gjøre dette selv i fremtiden. Da åpner samtidig spørsmålet om hvorvidt man har den nødvendige kompetanse til å gjennomgå dem.

KraftCERT og Mnemonic sier at hendelseshåndtering kan skje på flere måter. KraftCERT sier det enkleste er å identifiseres feil, skadevare, virus, eller noe som ikke fungerer, for så å ta kontakt med de aktuelle virksomhetene. Prosedyren startes ved å stille spørsmål med et mål om innhente informasjon, samt for å kunne kartlegge situasjonen. Han sier de i først og fremst prøver å gi råd slik at de han isolere hendelsen. For mer alvorligere hendelser vil de dra ut til virksomheten. Noen ganger får de indikatorer fra andre sikkerhetsmiljøer, mens andre indikatorer kommer fra utenlandske partnere. Det vil naturligvis øke mistenksomheten dersom mange tar kontakt samtidig. Det hender i tillegg at logger blir analysert, og skadevare blir undersøkt. Er det eksempelvis blitt sendt ut svindelepost, er det interessant for dem å finne ut hvor målrettet dette der. Det viktigste er å vite hvem man skal kontakte for å få fortgang i prosessen, hvilket Mnemonic er enig i. Mnemonic påpeker også at man må ha oversikt over situasjonen for å vite hva man skal gjøre før man kan iverksette aktive tiltak. Dette vil naturligvis baseres på hvor avansert angrepet er, men i noen tilfeller kan det være nok å trekke ut kabler. Derfor må man være bevisst på typen hendelse man står ovenfor. Han poengter at en gjennomsnittlig organisasjon ikke investerer penger i sikkerhetshendelser, og da finner man ikke ut noe om hverken aktør, årsak eller konsekvenser. Han legger til at god beredskap handler om å ha en plan på hvordan man skal håndtere sikkerhetshendelser, hvilket innebærer at man etablere rutiner, verktøy og prosesser som er tilpasset dette.

Beredskap på IT-hendelser utfordrende med mange forhold å ta hensyn til. Eksempler kan være brudd på personvern, innbrudd, eller at noen får informasjon. Dette forteller informanten fra BDO. En utfordring de peker på er å ha en evne til å oppdage, for eksempel,

innbrudd når dette skjer. De viser til tidligere tilfeller hvor det har gått så lang tid fra man har blitt infisert til man har oppdaget at data har blitt stjålet, at beredskapen blir en annen. Dette vil lede til en etterforskning av hva som har skjedd. Dersom man oppdager at noen har brutt seg inn i systemet for kort tid siden, vil det være nødvendig med en beredskap for det håndtering av situasjonen har blitt tenkt gjennom på forhånd.

Mørketallsundersøkelsen 2014 viser at evnen til å oppdage at noe er galt er forholdvis dårlig. Derimot om man analyserer data fra sensorer fra de selskapene som har det, ser man at det er over 60 prosent som har en hatt hendelse. NSR understreker at her er det snakk om evnen til å avdekke, og ikke viljen til å rapportere. Han sier videre at NSR er skeptiske til rapporteringsplikt, for hva får man igjen for det? Det understrekes at myndighetene ikke er klare til å ta i mot. Dette er også noe som blir poengtert av NorSIS, som forteller at man må diskutere hva som skal være målet med rapportering. Om man skal rapportere må det være for at det skal generere noe tilbake, og kunne bli brukt i læring, bistand, erfaring til CERT, og gode tiltak tilbake. Om dette blir gjort vil man ikke trenge rapporteringsplikt fordi folk vil gjøre det uansett. NorSIS peker videre på at om man klarer å trene en beredskapsorganisasjon og kriseorganisasjon på å se og håndtere det som er ukjent, vil man også være i stand til å oppdage informasjonssikkerhetshendelser. Han nevner Stuxnet, og sier at det fantes elektroniske spor om man bare hadde visst hva man skulle se etter. Av grunner som disse må man derfor alltid ha fokus på at det er noe ukjent man ser etter. Dermed kan man sette seg i en posisjon hvor man kan håndtere veldig avanserte ting som vi i dag kanskje ikke har kunnskap om. Hendelseshåndteringen blir heller ikke så bra om det er motvilje mot å dele informasjon i CERT-strukturen.

Informant fra NSR sier at logging er dårlig, og at dette i utgangspunktet skal være et verktøy for å kunne håndtere og forbedre. Et viktig verktøy som ikke alltid fungerer, og som ikke vil ha noen verdi før man har kompetente brukere som evner å oppfatte eventuelle avvik i loggene. NSM peker på at dette ikke fungerer i forhold til konfidensialitetsprinsipper, ettersom man stjeler informasjon. NorSIS sier det bør utføres av noen som er trent for dette formatet og at dersom man skal drive med dette burde man ha det som sin primære oppgave. Han eksemplifiserer det med å si at det ikke er lett for en driftstekniker å forstå hendelseshåndtering. I tillegg sier han at man kan kjøpe en hendelseshåndteringstjeneste, men om man skal gjøre det selv må man ha en enhet med kunnskap, personell og trening.

5.2.3 Øvelser

I beredskapsforskriften § 2-7, står det «Alle KBO-enheter skal gjennomføre øvelser med slikt innhold og omfang at enheten vedlikeholder og utvikler sin kompetanse til å håndtere aktuelle ekstraordinære situasjoner. Virksomheten skal ha en flerårig øvelsesplan og gjennomføre minimum én årlig øvelse» (Beredskapsforskriften, 2013, s. 4). Øvelsesmomentet blir også vektlagt i DSB (2001) sin veileder, hvor blant annet veilederen peker på effektiviteten av å teste beredskapen.

Informant sier at øvelser skal evalueres, og dette er et forskriftsfestet krav fordi man skal videreføre kompetansen for læringen. Hans oppfattelse er at bransjen stadig blir bedre på evalueringer og ROS-analyser, for jo mer det jobbes med dette, desto bedre blir kvaliteten. Man skal hele tiden jobbe for å bli bedre. BDO sier øving på IT-hendelser er noe som blir gjort, selv om det godt kunne blitt gjort mer. ROS-analyser og beredskapsøvelser er bra for å trenge ledergruppa slik at de er bevisste på hva som kan skje. De påpeker at selv om det ikke reflekterer virkeligheten til punkt og prikke, gir dette en god mulighet for å trene opp, diskutere, reflektere og drøfte strategier. De mener at myndighetene muligens kan være mer tydelige på dette. De påstår også at det å gjennomføre regelmessige risikovurderinger og regelmessige øvelser, IT-øvelser, er noe ikke mange nok selskaper gjør. De påpeker at går i riktig retning, men at man hele tiden må jobbe mot å bli bedre. Dette innebærer å øke mengde øvelser, samt sørge for åpenhet rundt deling av erfaringer og informasjon. Informant fra produksjonsselskapet sier seg enig i fordelene med øving, og peker spesielt på hvordan man trening fører til mer trygghet og ro skulle en situasjon oppstå. I etterkant av øvelsene bruker det å være noen runder med evaluering, hvor forbedringspunkter blir satt opp. Mnemonic kan fortelle at noen øver, men at det dessverre mangler kompetanse på hvordan å håndtere sikkerhetshendelser/informasjonssikkerhetshendelser. Han påpeker at et av områdene er at man ikke har oversikt over hvem som skal gjøre hva, og hvilket ansvar man har, i tillegg til at man da ikke øver tilstrekkelig på det. Han nevner i tillegg at det er individuelle forskjeller i hvilke problemstillinger man mestrer best.

NSR nevner spesifikt at uansett hva beredskapsplanen skal dekke, være seg informasjonssikkerhet, drift, naturskader, må det øves. Man øver på de grep som skal gjøres, og for å begrense konsekvenser og gjenopprette. Har man en beredskapsplan som ingen kjenner, vil den ikke være til hjelp for når en krise oppstår. I slike tilfeller vil man ikke

nødvendigvis ha tid til å bla gjennom en plan. I tillegg understreker han at en øvelse ikke bare er en øvelse, men at det skal læres og evalueres, hvor hovedhensikten er å teste planen og justere den. Med tanke på hyppighet på øving, sier han at jo oftere jo bedre, men at en storskala øvelse blir vanskelig. Da er det bedre å øve på mindre deler. I tillegg skal man huske på at ROS-analyser og verdivurderinger skal være dynamiske dokumenter, og om det er endringer i trusselbildet, må man revidere og ta hensyn til dette. Han nevner også at det er mye læring i *table top* øvelser, hvor man spiller inn scenarioer og har ulike grupper som skal gjøre ulike ting, til slutt presenterer man løsningene og diskuterer dem. NORSIS eksemplifiserer måten man kan gjennomføre IKT-øvelser og sier man spille inn og gjerne gjøre det som en større hendelse. Han understreker at man er nødt for å gjøre det på et høyt nok nivå. Forekomst av virus et eksempel på et lavt nivå. Informanten har tro på utviklingen av et scenario hvor det brukes cybervirkemidler. Dette blir anbefalt av NorSIS, men informanten har også inntrykk av at brukere med høy modenhet opplever at de nasjonale øvelsene på IKT har holdt et lavt nivå. Veileder fra Difi () peker også på hvilke type øvelser man kan gjøre, og i fullskalaøvelser gjør man øvelsen med teknisk utstyr, hvor oppgaver som skal bli utført i en virkelig hendelse blir øvd på. Som NorSIS nevner, kan også noen elementer av en øvelse gjennomføres, men at scenarioet må være relevant.

5.3 System, teknologi, kompleksitet

Som Hagen et al (2005) påpeker, går energiforsyningen mot å bli et komplekst system, og det vil bli vanskeligere å forstå og forutse effekten av enkle komponentfeil i det totale systemet. Dermed vil det bli vanskeligere å vite hvilke beredskapsdimensjoner man skal sette inn. Informanten fra NVE nevner hvordan en av særegenhetene til kraftbransjen er systembiten som til en hver tid skal fungere, men tror det er mulig å ha et sikkert system til tross for den økende kompleksiteten. I slike situasjoner må man jobbe på en bestemt måte. Han peker på at kompleksitet gir flere muligheter for feil, og at utfordringen er å finne riktig sikkerhetsnivå. BDO sier at et hundre prosent sikkerhetsnivå ikke vil være mulig. Når kraftbransjen kobler sammen systemene sine øker også inngangsportene, men det en grunn til at det kobles sammen er også for å øke oversikten. Kraftbransjen står ovenfor dilemmaer hele tiden, og han sier at det bekymrer han mer når virksomheter sier de har stålkontroll. Det nevnes videre at myndighetene har oppmuntret om å utnytte de teknologiske mulighetene som finnes, samtidig som de har akseptert at det finnes en viss risiko for at systemene kan kompromitteres. Videre nevner de at det viktigste er at man kan kunne stole på

driftskontrollsystemet. De understreker også at jo mer man bygger ut, jo flere øyne og ører før man. Dette er positivt for beredskapen, men, men kan by på problemer for sikkerheten. Kompleksitet er også en interessant diskusjon, og det stilles spørsmål ved om det er positivt at det skal bygges større. I tillegg nevnes det hvorvidt integrasjon er svaret, eller om desintegrering er mer hensiktsmessig. Informanten mener at flere bør ta denne diskusjonen på hvor grensa skal gå: hvor komplekst skal man ha IKT-infrastrukturen før man mister kontroll?

NorSIS nevner at det finnes to sider til denne saken. Den ene er at systemer blir mer avanserte og gir større muligheter til de som skal beskytte dem, samtidig som det skal holdes en situasjonsoversikt. Samtidig er kompleksitet noe det er vanskelig for oss som mennesker å forholde oss til, og det vil være større mulighet for glipp. Informanten nevner at mer kompleks teknologi fører til vanskeligheter for dem som skal gjennomføre et target-angrep ettersom det er flere ting å ta hensyn til. Kanskje ser vi at dette fører til flere angrep på mennesker. Kompleksitet kan ikke unngås av den enkle grunn at dette er en følge av den teknologiske utviklingen. Med mindre man får støttesystemer som fjerner utfordringene til kompleksitet, vil teknisk systemsikkerhet bli vanskeligere. Han mener at vi må erkjenne at sikkerheten vil være mer enn bare det tekniske. Herunder forklarer han at robustheten i mennesket vil kunne oppdage unormale ting, samt forhindre at noen skal kunne manipulere oss. Av grunner som disse mener enkelte at menneskelig faktorer er viktigere å ta hensyn til enn de tekniske elementene i systemsikkerheten. NVE peker også på hvordan det menneskelige elementet er vesentlig, ettersom det alltid er en kobling tilbake til mennesket, noe som også Mnemonic understreker. Han sier alvorlige sikkerhetshendelsene skjer fordi man ikke har klart å sikre det menneskelige element i det hele. Derfor gjelder det å ha sikkerhetsventiler som oppdager når mennesket gjør feil.

Videre peker NVE på at man må ha redundante system, hvor driftskontrollsystem vet hvor sentralen ligger, men ikke hvor reserven ligger. Dette er også informasjon som blir beskyttet av forskriften. Han peker videre på at Norge er komplekst i den forstand at vi har mange produsenter. Dette gir imidlertid også økt robusthet, og informanten sier at det er viktig å ha en kraftforsyning som kan drives selv om man mister overføringslinjene. Informanten . mener at man bør kunne bygge systemer på en robust og sikker måte, som for eksempel automatisk oppdaterer seg, og at det må være et samspill mellom krav og effekten av dem. NSM viser også til at har man en vilje til å tenke det verste, håndtere det med redundans eller

systemer, kan man være forberedt på hva man gjør når en angriper lykkes. Han sier at man må i større grad bygge sikkerhet inn i bunnen av systemet, og at det derfor er et problem når mange system er bygget av folk som tenker funksjonalitet, fremfor sikkerhet.

KraftCERT sier han kunne tenkt seg mer transparente systemer, og understreker at selv ikke *open source* er det enkleste å få innsyn i. Nyere system har eksempelvis bedre logging som til en viss grad gjør det mulig å se hva som skjer, sier han. Han legger vekt på at man skal dra nytte av den økte digitaliseringen, man må henge seg på, men man må ha kontroll på prosessene. Han sier også at man må skape en forståelse for den risikoen som finnes og få større transparens i hva som foregår. Det trekkes i tillegg frem at man kanskje burde ha noe som drev kontrollert med penetrasjonstesting. På spørsmål om teknologi gjør det enklere eller vanskeligere å oppdage hendelser, er meningene delte. KraftCERT mener det absolutt gjør det enklere å oppdage hendelser, selv om man må ha visse evner og, kompetanse på området. Mnemonic sier at teknologi hverken gjør det enklere eller vanskeligere, men at det handler om evnen til å forstå hvordan ting normalt skal se ut. Dette er BDO enige i. De sier det handler om hvordan man har rigget seg til med tanke på sensorer, og evnen man har til å oppdage.

5.4 Kompetanse

I beredskapsforskriften kapittel 4-2 står det tydelig at alle KBO-enheter ”skal ha personell med nødvendig kompetanse som kreves for å kunne håndtere ekstraordinære situasjoner på en sikker og effektiv måte” (BfK, 2013, s. 6), og at for å dekke dette kravet må man ha en plan som angir kompetansebehovet. Informant fra produksjonsselskap sier at han er usikker på hvordan kompetansen til bransjen er, men påpeker at det er et felt som utvikles raskt, i tillegg til at de fleste som jobber i everk, nettselskap, produksjonsselskap, ikke har dette som hovedjobb. Informant fra nettselskap sier det er viktig å holde tritt med kompetansen, og nevne at selskapet nylig har ansatt to personer for å styrke denne delen av virksomheten sin. Begge har IT-kompetanse. Samtidig trekker han også fram hvor avhengige de er av eksterne eksperter. Han påpeker at man ikke kan ha en avdeling som alltid er på topp, og at mindre selskaper som ikke har mulighet til å ansette noen på heltid, ikke vil ha en sjanse. Begge informantene sier at man må være bevisst på bestillerkompetanse.

KraftCERT sier seg enige med informant fra nettselskap om at det er begrenset hvor mye man kan forlange av små- og mellomstore selskap, og spesielt på hendelseshåndtering. I tillegg sier informant at folk i selskaper må kurses, og at dette er noe som myndighetene bør koste på seg. Mnemonic nevner i tillegg at man ikke kan kreve at selskaper har spesialistkompetanse på informasjonssikkerhet, men at det må finnes kompetanse på egne systemer. Dette står også fastslått i beredskapsforskriften. Samtidig sier syv informanter at det også er vanskelig å si hvordan kompetansenivået i forsyninga er, men informant fra NVE peker på at det en del kompetanse som forsvinner ut med generasjonen som nå skal pensjoneres.

Videre påpekes det både av NVE, BDO og NSM at det er like fokus på IKT-sikkerhet i utdanningen, og NVE sier blant annet at man kunne begynne å jobbe inn sikkerhetsbiten allerede på videregående skole. Det er i tillegg behov for mer forskning på sikkerhetsspørsmål, som burde skape rom for et samspill mellom forskning og undervisning. Samtidig peker også NVE, BDO og NSM på at det trengs enda mer forskning på beskyttelse av driftskontrollsystem. Mnemonic sier at de har ansatte som er med i forskningsmiljø innenfor prosess- og styringssystemer, og at det blir diskutert hvorvidt det skal igangsettes nye prosjekter for å starte system som gjør det bedre å lettere å sikre kritisk infrastruktur. I tillegg blir også etterutdanning nevnt av fire informanter, og hvordan det må jobbes for å øke bevissthetsnivået på IKT-sikkerhet.

En annen problemstilling som også blir nevnt av informant fra NVE er hvordan man er nødt til å skape en felles forståelse mellom forskjellige miljø IT-miljø og sikkerhetsmiljø, og at sikkerhetskulturen må gjennomsyre hele organisasjonen. NOU 2015:13 peker også på hvordan fagmiljøer innen IKT-sikkerhet og prosess er adskilte. Dette er en utfordring for både samhandling og sikkerhetsarbeideren (NOU 2015:13, 2015). BDO peker på hvordan det finnes forskjellige fora hvor man kan diskutere IKT mer, både bilateralt og nasjonalt. De fremhever hvor viktig åpenhet og samarbeid er for å styrke kompetansen. De nevner forum for informasjonssikkerhet i kraftforsyninga, Nettalliansen, sitt fokus på å stå sterkere i forhold til bestilling av IT-systemer. Når det gjelder forståelse av de digitale sårbarhetene, og en virksomhetsevne til å beskytte seg, er det også noe som blir tatt opp i NOU:2015:13. Her blir det nevnt hvordan man må bruke ressurser på adekvate tiltak.

Alle informantene er enige om at opprettelsen av KraftCERT er en positiv utvikling, men samtidig sier informant fra nettselskap at han har mer tro på et kompetansesenter, hvor det er virksomhetenes eget ansvar å holde seg oppdaterte enn at dette skal reguleres gjennom forskriften (Beredskapsforskriften). Han går tydelig ut på at forskriften også burde være en rammeforskrift, som bør si at man har ansvar for å ha nødvendig kompetanse på den ene eller på den andre måten. BDO nevner også for øvrig at det nok kommer til å komme flere regionale kompetansesenter, ettersom avstandene i Norge er store.

5.5 Samvirke og informasjonsdeling

Samvirkeprinsippet kom etter erfaringer man gjorde seg med 22.juli, og er likestilt med de tre andre prinsippene.

Informant fra produksjonsselskap sier at IKT er et stort område, og at han ikke vet hvor god samhandlingen er på tvers. Informasjon fra nettselskap sier at samvirke mellom dem og myndighetsorganer er litt forskjellig ettersom noen gir gode svar, andre gjør ikke. Derimot ser informant fra NVE samvirket som veldig godt. Og nevner at de har god kontakt med KraftCERT, og er med i KBO, hvor alle virksomheter også er underlagt. KraftCERT nevner også hvor god kontakt det er mellom KraftCERT og NVE, men sier derimot at det varierer hvordan samvirket er mellom dem og leverandører. Noen av leverandørene ser ikke noe poeng i å samarbeide, mens konsulenter er interessert. Han sier det er nødvendig å legge et internasjonalt press på dette. Han nevner også hvordan det kanskje ikke er den mest ideelle delen å være så strenge på sektorer, og at man burde se for seg en mer helhetlig tekning. BDO peker også på at om man skal få til et bedre samvirke er man nødt for å inkludere private kompetansemiljøet, og sier i den sammenhengen at Stuxnet ble oppdaget av private sikkerhetsselskaper. De mener at samvirket er viktig for å få mer kunnskap om hvilke ressurser som finnes, noe som også NSR poengterer. Som KraftCERT, peker han også på hvordan det er problematisk med sektorCERT-er, ettersom det alltid vil være noen som faller utenfor sektoren.

Informanten fra NorSIS mener at samvirket ikke er godt nok, og sier at de i NorSIS står for at samvirket og åpenhet kan føre til et mer robust samfunn. NorSIS etterlyser også en samarbeidsplattform for å utveksle sensitiv informasjon. NSM sier også at samvirket kan bli bedre, og at det er viktig at man ikke konkurrer på sikkerhet. Han nevner også at NSM har

fått kritikk for å ikke ta mer overordnet ansvar. NSR sier også at det er behov for koordinering på informasjonssikkerhet og datakriminalitet fordi det er mange aktører som er involvert. Her sier også Mnemonic at myndighetene er et stykke fra å ha informasjonssikkerhet i fokus, spesielt fra Stortinget.

På informasjonsdeling sier informant fra produksjonsselskap at de avhengige av de felles samlingene som blir arrangert av Energi Norge med tanke på driftskontrollsystemer. NVE opplever at det deles mye informasjon, og at det er en god kommunikasjon mellom virksomhetene. Når det gjelder KraftCERT, understreker han viktigheten av at det var sektoren selv (Hafslund, Statnett og Statkraft) som opprettet CERT'en, og at de oppfordrer alle sine medlemmer til å dele informasjon, slik at det blir normalen. I forhold til informasjonsdeling sier også BDO at det er viktig at informasjon fra NSM deles over til sektorene, og fra sektorene ut til bransjene. NSR støtter at bransjen selv ikke er flinke nok til å dele informasjon om ulykker og nesten-ulykker, hvilket sannsynligvis henger sammen med virksomhetenes omdømme. Man behøver for øvrig ikke å dele alle detaljer, men det ville vært hensiktsmessig å gi indikatorer på hva andre kan se etter. Å holde tilbake informasjon kan skape en illusjon om en virksomhet som har kontroll, når det virkeligheten kan handle like mye om hemmelighold fra virksomhetens side. Både NSR og BDO ser på opprettelsen av KraftCERT som veldig positivt, og håper det kan hjelpe til med informasjonsflyt, samt bidra til at man kan finne nye løsninger og lære av andre.

6 ANALYSE OG DRØFTING

Det følgende avsnittet vil presentere analyse og drøfting av det empiriske materialet som ble redegjort for i kapittel 5, i lys av det teoretiske rammeverket som ble presentert i kapittel 4. Analysen vil bli delt inn i tre deler. Inndelingen vil følge forskningsspørsmålene presentert i kapittel 1. Hele det teoretiske rammeverket vil bli brukt gjennomgående for analyse og drøfting.

6.1 Hvilke IKT-relaterte sårbarheter og trusler er energiforsyningen utsatt for?

For å svare på forskningsspørsmål 1 vil det bli presentert to underdeler, trusler og sårbarheter.

6.1.1 Trusler

IKT er blitt en stadig større del av samfunnet og energiforsyningen. Innen kritisk infrastruktur er energiforsyningen en av bærebjelkene i samfunnet vårt, samtidig som det finnes stor gjensidig avhengighet blant de fleste kritiske infrastrukturene i Norge. Med den økte digitaliseringen av samfunnet implementeres det flere teknologiske løsninger som skal gjøre flere funksjoner mer effektive. SCADA-systemet er et godt eksempel på dette, men det må også understrekes at det var et system som ikke ble bygget for å være tilkoblet internett. Dermed finnes det en stor sårbarhet med tanke på tilkobling til internett. Som empirien viser, finnes det flere typer av IKT-trusler som blir nevnt, som også stemmer overens med det som blant annet ble rapportert fra både NSM og Politidirektoratet. Spesifikke trusler som nevnes er spesielt hacking, som blir brukt for å få tilgang på informasjon om produksjon og metoder, samt for overtagelse av driftskontrollsystemer. Hacking er i tråd med trusselbegrepet fra Melding til Stortinget (2002), hvor intensjonen av hacking kan være å påføre skade på liv, helse, miljø og materielle verdier. Hacking vil også være en tilsiktet straffbar handling og er som regel en målrettet handling, hvor trusselaktør vil ha tilgang på sensitiv informasjon eller utgjøre skade (jmf. Ukraina og Stuxnet). Informanter fra virksomheter sier det er vanskelig å ha en oversikt over trusselbildet, som også understreker problematikken med å ha tilstrekkelig kompetanse på IKT-sikkerhet. Rapport fra NSM (2015) viser også til vanskeligheten av å oppdage angrep som kan tolkes som at trusselaktørene stadig blir mer avanserte i sine angrepsmåter. Derfor er også angrep på mennesker en stadig større trussel og kompetansen må heves i virksomheter.

Selv om empirien viser at det ikke har vært en større IKT-hendelse her i Norge, viser den også hvordan kompleksiteten i trusselbildet har endret seg, blant annet i form av flere avanserte angrep som tar lengre tid å detektere. I høyrisikoteknologier er det ikke mulig å eliminere all risiko og etter hvert som man går mot mer teknologi med flere tette koblinger, burde man forvente en systemulykke (Perrow, 1999). Stadig tettere koblinger og komplekse interaksjoner gjør at man blir mer utsatt, og med sammenkoblingen av SCADA-system og administrative system gjør at man også øker hovedkildene til feil. Før driftet man anlegg manuelt, og alle anlegg var bemannet, som kan ses i lys av Perrow (1999) sitt lineære system. Man visste hva som foregikk på hver stasjon og kunne ha ROS-analyse for hver enkelt. SCADA-systemene er automatiserte og mindre fleksible med flere skjulte transaksjoner. Oppstår det en feil kan systemet ha problemer med å finne ut hvor den kommer fra, og på grunn av tidspress kan det få katastrofale følger, eksempelvis kan et område være uten strøm. Tidsbegrensingene i disse systemene gjør at konsekvensene løper raskt, mens man kan ha problemer med å oppdage hendelser. Driftskontrollsystemene er rangert etter størrelse, hvor klassifisering 3 er den som må ha best sikringstiltak. Samtidig, ser man i lys av HRO, skal høyrisiko-organisasjoner kunne klare å ha et organisasjonsdesign som gjør at de på en sikker måte kan håndtere høyrisikoteknoliger. ROS-analyser er et godt verktøy for dette, i tillegg er man nødt til å ha en sikkerhetsforståelse som går gjennom hele organisasjonen. Ved hjelp av beredskapsverktøy kan man kompensere for menneskelige svakheter og ha en høy grad av pålitelighet.

Dermed peker informanter fra BDO at det handler om å finne riktig sikkerhetsnivå. NorSIS påpeker også at kompleksitet er vanskelig å forholde seg til for mennesker, som kan være med å påvirke hvorfor feil lettere skjer. Som Hagen et al. (2005) og samtlige informanter understreker, er det heller ikke en mulighet for å unngå kompleksiteten, man må derfor stole på robustheten mennesker har til å detektere unormale ting. Sikkerhet må også handle om mer enn den tekniske systemsikkerhetsbiten, ettersom det ofte er mennesker koblet inn når feil skjer. Dermed blir redundans i system, med blant annet duplisering (Sagan, 1993), desto viktigere. Menneskelig redundans og teknisk redundans er to komponenter som må fokuseres på om man vil oppnå en høypålitelig organisasjon (Sagan, 1993).

Det finnes ukjente elementer og risikoer man ikke vet om per nå og derfor er det desto viktigere å kunne planlegge for noe ukjent. Alle informanter er enige om at evnen til å forutse ligger i gode ROS-analyser og verdivurderinger. I følge Lunde (2014) og Perry og Lindell

(2007) må man dokumentere kjente trusler, men også identifisere nye trusler. For å kunne planlegge på en robust måte må man ha en kobling mellom ROS-analyser og beredskapsplan. Om man ikke identifiserer nye trusler faller litt av poenget med å ha en beredskapsplan bort ettersom de kjente truslene allerede er tatt høyde for. Å være forberedt handler om å se utover de kjente rammene, og bare på den måten kan man oppnå en robusthet i planene sine. Gjennom Aven og Renns (2010) definisjon på risiko, ser man også at både usikkerhet, ønskede og uønskede resultater er tatt med. Dette understreker igjen behovet for å kunne tenke seg tankene rundt hva som kan skje, om noe man ikke kjenner til oppstår. Evnen til å håndtere en trussel er også viktig. Når det gjelder IKT-relaterte trusler er man i tillegg nødt til å inneha kompetanse på dette området, eventuelt ha eksterne tjenester. Jamfør Beredskapsforskriften (2013) er det også lovfestet at man skal ha en IKT-sikkerhetskoordinator i tillegg til faglig kompetanse. Desto mer kompetanse man har gjennomgående i organisasjonen, desto mer forberedt er man på en hendelse, og desto større evne har man til å håndtere den. Med tanke på nærhetsprinsippet og HRT-tankegang, skal man kunne håndtere enn hendelse på lavest mulig nivå fordi det er de som har størst nærhet til en krise som har best forutsetninger for å forstå og håndtere.

6.1.2 Sårbarheter

Ettersom kompleksiteten øker i IKT-systemene i energiforsyningen, vil også sårbarhetene øke dersom man ikke klarer å redusere disse. Som Lysneutvalget (2015) poengterer, finnes det flere typer av sårbarheter, avhengig av hvilken tilnærming man har. I forrige delkapittel ble det diskutert truslene og sårbarhet knyttes nært opp til disse. Når det gjelder sårbarheter som knyttes direkte til IKT-systemer nevnes automatiseringen av SCADA-system, som har svakheter i form av at de ikke er designet med sikring som første prioritet. På grunn av tette koblinger gjør det også at en sårbarhet som finnes på et sted i systemet kan forplante seg til andre deler av systemet. Perrow (1999) poengterer hvordan slakk og buffere må tas inn på forhånd fordi de er dårlige på å inkorporere feil. Mennesket er også en del av sårbarhetene til systemet fordi selv om systemene er automatiserte må det fremdeles menneskelig overvåking til for å kunne detektere feil. Er ikke en driftsperson i stand til det, vil denne feilen forplante seg videre og potensielt ta ut hele systemet. Dog, som man så med hendelsen i Ukraina ble man nødt til å gå over til manuell kontroll av anleggene. Her ble mennesket en form for redundans. Som nevnt av informanter er menneskelig manipulering blitt en økende metode

for å få tilgang på systemer. Dersom man ikke er obs på bruk av USB-pinner og økning i *spear phishing* eposter, skal det ikke mye til før en uønsket aktør er inne i systemet.

Som påpekt av informant fra NSR og NSM, er tabellen presentert i kapittel 5 (tabell 2), en oversikt over enkle råd man kan gjøre for å minske sårbarheter, og dermed gjøre veien inn i et system mindre tilgjengelig. Ofte er programvare og maskinvare utdaterte, og de sikkerhetshullene som da finnes er tilgjengelige fordi man ikke har oppdatert til seneste versjon. Det er en grunn til at sikkerhetsoppdateringene kommer og det er for å lukke eventuelle sårbarheter som finnes i system som blir brukt i virksomheter. Det kommer frem fra samtlige informanter og Mørketallsundersøkelsen (2014) at virksomheter ikke er flinke til å oppdatere program- og maskinvaren. Som Lysneutvalget (2015) påpeker, er den digitale verdikjeden i den norske energiforsyningen avhengig av synkronisering mellom produksjon og forbruk av elektrisitet, noe IKT-systemer er med på å understøtte. Skulle det dermed oppstå en feil i en av delene vil det ha påvirkning for hele verdikjeden. Dette betyr da at om en aktør lenger nede i kjeden ikke forstår at svikt i et ledd vil ha konsekvenser som strekker langt utover sin enhet, vil det oppstå ubalanse og potensielt kan det påvirke forsyningssikkerheten. Det betyr også at ledelsen er nødt for å kunne avdekke sårbarheter lenger nede i verdikjeden. For at sikkerhet skal gjennomsyre organisasjonen må ledelsen ha sikkerhet som objektiv (Sagan, 1993). Avdekking av sårbarheter er dessuten noe virksomheter skal gjøre under fase 1, identifisering, hvor ROS-analysene som gjøres er nødt til å gjennomføres på en grundig måte (Lunde, 2014; Beredskapsforskriften, 2013), fordi det legger grunnlag for etablering av beredskap.

Et annet moment som blir trukket frem av alle informanter er øking i avhengighet til leverandører. Siden ikke alle virksomheter har kapasitet til å ha IKT-avdeling som sitter fast i bedriften er det mange som benytter seg av eksterne leverandører, men som informant fra produksjonsselskap påpeker er det mange som bruker samme leverandør. Om det skulle oppstå svikt hos leverandør vil det da berøre flere virksomheter i energiforsyningen. I tillegg blir det fremhevet hvor viktig det er å ha bestillerkompetanse. En annen sårbarhet er at leverandører er ansvarlige for en tjeneste, men virksomheter må også vite hva de skal bestille, og om det de har bestilt er riktig; det må tørres å stille krav til leverandører. Informant fra Mnemonic påpeker også at leverandører ikke er kompetente nok, som også er et problem. Som både forskriften, beredskapsteori og HRT påpeker, må man hele tiden etterstrebe nok kompetanse og hele tiden holde seg oppdatert.

6.2 Hva sier litteratur og eksperter om etablering av god beredskap?

Beredskapsforskriften pålegger alle KBO-enheter å ha beredskap og alle informantene var enige om viktigheten rundt det å ha beredskapsplaner på plass. Blant ekspertene var det ganske lik oppfatning om hva som skulle være med i en beredskapsplan og hvile fokusområdet man må ha. Denne delen vil bli presentert med de samme fasene som figur 1, i kapittel 3.3, planlegging og etablering av beredskap.

Beredskap for produksjonsselskapet er å kunne ta høyde for plutselig oppståtte situasjoner med vanlig linje ikke klarer å håndtere. For informantene fra BDO er det å kunne være gode på det som har rammet virksomheten tidligere, samt være fremsynt. Mnemonic sier virksomheter godt kan være mer bevisst på uønskede hendelser og håndtering av disse, for NSM handler det om god forhåndsplanlegging.

6.2.1 Fase 1: Identifisering

I identifiseringsfasen skal det gjennomgås mål og ambisjoner, samt hvilke lover og forskrifter som gjelder. For energiforsyningen er det Energiloven og Beredskapsforskriften som gjelder. Sikkerhet og pålitelighet bør være øverste mål for virksomheten (Sagan, 1993), og dermed blir det, som informant fra NVE påpeker, feil å kutte i antall ansatte som jobber med sikkerhet. Videre i fase 1 skal man gå over til å definere fare- og ulykkessituasjoner og denne informasjonen må være basert på troverdig informasjon. Å holde seg oppdatert på trusselbildet ble nevnt som vanskelig, men det er viktig å vite hva man skal beskytte seg mot. Risiko er et begrep som kan bety forskjellige ting etter hvilken definisjon man legger til grunn, derfor er det også viktig at det er en felles forståelse for hvilke begrep man bruker. Aven og Renn (2010) sin definisjon, hvor både usikkerhet, ønskede og uønskede hendelser og berørte parter inkluderes, ses på som en god definisjon som ivaretar de viktigste momentene. Dog, det beste er nok å ha en kombinasjon av denne definisjonen, sammen med en sannsynlighet og konsekvens definisjon. I ROS-analyser må man ta høyde for både ukjente og kjente momenter, samt identifisere nye trusler. Alle informantene er enige om at det må finnes en kobling mellom ROS-analyser og beredskapsplaner, i tillegg til at det også må gjøres en verdivurdering: man må vite hva man skal beskytte og hvorfor, hvis ikke er det ikke noe poeng å utføre en verdivurdering. Det man da vil beskytte må det legges betraktelige sikkerhetstiltak på. Informant fra NSR, NSM og NorSIS påpeker viktigheten av denne

vurderingen. I tillegg understeker alle informanter viktigheten av å ha et fungerende og oppdatert planverk.

Planlegging, og evnen til å forutse og håndtere (Wildawsky, 1991) er sentrale elementer som må legges til grunn for en effektiv plan. Det er restrisikoen man skal etablere en beredskap på fordi uønskede hendelser kan inntreffe. Å ha klare mål og forståelse for dette er en viktig oppgave for ledelsen. Som informant fra NSR påpeker er det ikke så mye man kan gjøre med trusselaktøren, men man kan redusere sårbarhet og sette inn konsekvensreduserende tiltak. Som nevnt er det viktig å holde seg oppdatert på trusselbildet, og informantene fra BDO påpeker at det er et behov for å jobbe mer aktivt med IKT-beredskap, og at de erfarer at beredskapsplanene med IKT-hendelser er underutviklet. Slik situasjonen er for energiforsyningen i dag kan det føre til store konsekvenser. Om ROS-analysene ikke er oppdaterte og tar med aktuelle problemstillinger kan det få katastrofale følger, skulle det skje noe. KraftCERT påpeker også hvordan det tilsynelatende er et krasj mellom fysisk beredskap og beredskap på IKT-sikkerhet. I identifiseringsfasen er dette noe som må jobbes aktivt med.

6.2.2 Fase 2: Ytelsesrammer og ytelseskrav

Etter å ha utført ROS-analyser må man bestemme hvilke situasjoner (ytelsesrammer) det skal etableres beredskap på, og hvilken respons og håndtering (ytelseskrav) man skal ha på de valgte situasjonene. Beredskapsforskriften (2013) lovfester at virksomheter skal ha beredskapsleder, beredskapskoordinator og IKT-sikkerhetskoordinator. Så fremt en virksomhet har noen som sitter med beredskap hele tiden er dette interne ressurser man kan benytte seg av for å etablere beredskap. Ikke alle virksomheter har noen som jobber med dette hundre prosent, og mange leier også inn eksterne aktører, dette blir da eksterne ressurser. Til tross for dette skal man kunne sette klare rammer for hva man ønsker å oppnå med beredskapen man etablerer**.** Det man avdekker i ROS-analysen og verdivurderingene skal det settes tiltak på (Lunde, 2014).

Oppgaver skal fordeles og her er ansvarsprinsippet viktig fordi man må avklare hvem som skal ha hvilket ansvar. Dette må bygge på kompetanse, men i tillegg bør nærhetsprinsippet gjelde slik at om det skulle oppstå en hendelse så vil den bli håndtert på en desentralisert måte. Man skal etterstrebe håndtering av kriser på lavest mulig nivå, dette er også i tråd med HRT tankegang (Sagan, 1993; Lunde, 2014; Meld. St. 29 (2011-2012), 2012). Flere informanter påpeker også hvordan man ikke kan delegere oppgaver til noen som ikke har det

som oppgave til daglig, dette vil skape forvirring i en eventuell håndtering av situasjon. For å skape redundans i organisasjonen er det også viktig å ha overlapp mellom ansvarsområdet, noe som blir vektlagt av HRT (Sagan, 1993). Med tanke på ansvars- og nærhetsprinsippet kan den potensielt føre til krasj mellom overordnede og underordene i organisasjoner, ettersom det ofte er vanlig at desto lenger man kommer opp i situasjonen, jo mer ansvar får de. Skal man derimot følge nærhetsprinsippet og desentralisert beslutningstaking (jmf. HRT) blir dette motstridende. I tillegg tolkes det fra intervju som at IT-avdelingen er separert fra beredskapsavdeling, men på IKT-sikkerhet må man inkludere de som har kompetanse.

Om det skulle oppstå en hendelse må man sette inn beredskap eller iverksette krisehåndteringsplaner. Informanter fra KraftCERT og Mnemonic påpeker hvor viktig det er å ha evnen til å oppdage at noe er unormalt, og at denne evnen til å detektere er en av de viktigste mulighetene til å stoppe et angrep og håndtere det. Alle IKT-hendelser skal rapporteres til NVE, etter forskriften. Dette stiller dog informant fra NSR og NorSIS seg litt skeptiske til fordi de stiller til spørsmål hva som er grunnen til at man skal rapportere om man ikke får noe tilbake for det. Mørketallsundersøkelsen (2014) viser også at antall rapporterte hendelser er langt fra antall oppdaget datainnbrudd, den viser også at evnen til å oppdage er forholdsvis lav. Logging, som er et verktøy for å oppdage unormal aktivitet, er i følge informant fra NSR også dårlig. Her forutsetter det også at man har kompetent personal som kan overvåke loggene. BDO peker også på at om man oppdager har det noen ganger gått så lang tid fra innbrudd til oppdaging, noe som kan få store følger for resten av systemet, hvor tidspress også spiller en stor rolle (Perrow, 1999). Dersom virksomheter ikke har kompetanse selv til å håndtere IKT-hendelser må de vite hvem som kan og hvem de skal kontakte. KraftCERT er en CERT-funksjon som ble opprettet av sektoren selv og dermed er det viktig at virksomheter bruker denne funksjonen. Eventuelt bruke selskaper som Mnemonic som er eksperter på IKT-sikkerhet. Det er på høy tid å innse viktigheten i å investere i gode håndteringsrutiner, spesielt som kompleksiteten øker og man går mot enda mer automatisering (AMS).

6.2.3 Fase 3 og 4: Analyse av eksterne og interne ressurser

For energiforsyningen er viktige eksterne ressurser blant annet NSM, NorCERT, KraftCERT og NVE. NVE er sektormyndighet og har mandat til å sette i gang beredskap, og KraftCERT er som sagt sektorens egen CERT-funksjon. I tillegg kan også eksterne ressurser være nødetatene, samt andre kommunale beredskapsressurser. Dette er viktig å ha avklart fordi

man ikke vet når man plutselig skulle trenge assistanse. Derfor må det også inngås formelle avtaler med disse instansene (Lunde, 2014). Når det kommer til interne ressurser, påpekte informant fra NVE at den generasjonen som er på vei ut av bransjen innehar mye informasjon og kunnskap som dessverre ikke har blitt skrevet ned og at dette er et tap for bransjen. Den videre utviklingen av IKT må derfor prioritere å få inn ny kompetanse, eventuelt øke den interne kompetansen slik at virksomheten vet hva de driver med. Når det gjelder KraftCERT har de eksistert rundt et år og har tre ansatte per dags dato. Informanten sier at han tror de kommer til å ha en økning i henvendelser, noe som også må føre til at de også blir større.

Det skal i tillegg analyseres hvilke tiltak som skal etableres slik at responsen imøtekommer ytelseskrav og ytelsesrammer satt i fase 2, for å vite hvordan best mulig håndtere en hendelse (også nevnt i fase 2). Informant fra produksjonsselskap nevner at han ikke tror sikkerheten er ivaretatt på IKT-hendelser og at generell sikkerhet vektlegges mer. Dette er noe som er blitt nevnt også av andre informanter. Dette er en problemstilling som ikke er særlig bra når det kommer til IKT-sikkerhet og håndtering av hendelser. I tillegg sier informant fra KraftCERT at et annet problem knyttet til håndtering er fargekoding av risikonivåer (risikoakseptkriterier), fordi nivåene til beredskapsorganisasjonen ikke stemmer overens med de nivåene som KraftCERT opererer med. Dette kan være fordi de er vant til fysisk beredskap, og kanskje ikke ser alvoret. Detter blir videre diskutert i kapittel 6.3.

6.2.4 Fase 5: Etablering: beredskapsdokumentasjon

I etableringsfasen skal man formalisere avtale med eksterne ressurser, ettersom alle dokument som har med beredskap skal dokumenteres. Dersom det trengs at ressurser må læres opp og trenes, skal dette gjøres og dokumenteres i denne fasen. Beredskapsplanen er det viktigste beredskapsdokumentet organisasjonen innehar. Som nevnt skal det være en kobling mellom ROS-analyser og beredskapsplan og denne planen skal inneha beskrivelser av ledelsesnivå, enheter og funksjoner (Lunde, 2014). Informant fra NorSIS understreker at det er viktig at dette dokumentet ikke blir bokhyllefyll, innforstått at det skal kunne være en anvendelig plan. Den skal ikke være for detaljert, men en dynamisk plan (Dynes, 1993). Planen skal inneholde informasjon om varsling og mobilisering, håndtering og risikoreduksjon, demobilisering og mobilisering (Lunde, 2014; Perry og Lindell, 2003). Når det kommer til varsling sier informantene fra BDO at man er nødt til å bli flinkere til å varsle hendelser; det må inn en bedre sikkerhetskultur hvor det er greit å gjøre feil, så lenge man varsler om det. Vel så viktig er det også å varsle nesten-ulykker, slik at man kan ta bedre

høyde for disse i nye ROS-analyser. Dette går også under hovedmålet for beredskapsplanlegging som er å hele tiden forbedre seg. Ettersom man ikke kan sikre seg hundre prosent er det viktig å ha et tilrettelagt planverk hvor man tar høyde for det man kan, og øver og trener på det. Skulle det oppstå en situasjon som er helt ukjent, har man uansett en viss redundans og pålitelighet dersom organisasjonen er trent i sine oppgaver i en ekstraordinær situasjon. Et viktig moment er også fokuset på å komme tilbake til normalen og gjenopprette systemet til mer eller mindre slik man hadde det før krisen inntraff (såfremt det er mulig).

Som nevnt tidligere må sikkerhet gjennomsyre hele organisasjonen og dette er ledelsen sitt ansvar. Alle i en organisasjon må gjøre seg kjent med beredskapsplanene, og derfor er det også viktig at den blir skrevet på en måte som er forståelig. Dermed kan den ikke inkludere overflødige detaljer, men den skal være direkte og praktisk å bruke. Kun da vil den oppnå sitt formål. I tillegg er man nødt til å bli bedre på å inkludere IKT-hendelser.

6.2.5 Fase 5: Kompetanseheving: trening og øvelser

For å kunne ha en plan som fungerer når en unormal situasjon inntreffer, er man nødt til å ha evnen til å håndtere, men det viktigste er at man har øvd og trent på planen. Dermed må man fokusere på opplæring på alle nivå, og det må fokuseres på kompetanseheving. Bevisstheten må også økes, og man må minne ansatte på gode rutiner. Informant fra produksjonsselskap poengterer at han ikke tror ansatte er særlig bevisste på bruk av USB-minnepinner (dette var årsaken til Stuxnet), og at gode rutiner er en ferskvare. Gjennom Beredskapsforskriften (2013) er man også pliktet til å gjennomføre øvelser for å vedlikeholde og utvikle kompetansen, og virksomheter skal ha en øvelsesplan. Det kommer frem fra empirien at noen øver, andre gjør ikke, og at det noe som kan bli mer etterspurt. IKT-øvelser kan spilles inn. Dermed menes det at dette er noe myndighetene kan være mer tydelige på. Difi sin veileder på IKT-øvelser beskriver hvordan man kan gjennomføre og planlegge disse.

Et viktig moment er at hele organisasjonen har en felles forståelse for oppgavene som skal utføres, og derfor må øvelser til på alle nivå. I tillegg påpeker NorSIS viktigheten av at scenarioene som brukes til øvelser må gjennomføres på høyt nok nivå for at det skal være en relevans i det. Med tanke på tidligere nevnte problemstillinger rundt deteksjon og håndtering er IKT-øvelser spesielt viktige. Og selv om man øver er man også nødt til å trene, noe informant fra NSR vektlegger. Øvelse og trening for kompetanseheving er også noe som blir

vektlagt i HRT (Sagan, 1993), og gjennom prøving og feiling kan man også luke ut latente feil. Ettersom IKT-sikkerhet er et nyere fokusfelt er det desto viktigere at man øver og trener. Selv om Perrow (1999) mener man ikke kan gjøre noe for å unngå systemulykker, vil man i det minste ved å øve, minske muligheten for at feil forplanter seg for langt i systemet. Som informanter påpeker må man også ha en evalueringskomponent, hvor man går gjennom eventuelle funn fra øvelser. Evaluerer man ikke, har man ikke særlig nytte av øvelsen. Om det oppdages faktorer som ikke er tatt med i beredskapsplanen, må man legge inn dette.

6.2.6 Fase 7: Evaluering: verifisere, revidere, forbedre

Siste fasen handler om evaluering av planverk og beredskap. Hensikten med å evaluere er å teste og justere planen, om det skulle trenges. Informant fra NSR påpeker at man ikke er flinke nok til å evaluere planverket, og da vil samme problemer oppstå igjen og igjen. Virksomhetene må også evaluere for å se om målene de har satt seg er reelle, og om de er oppnåelige. Det nytter ikke å ha et planverk som ikke blir brukt fordi det er utdatert. Det kan virke som det jobbes for å bedre evalueringer og ROS-analyse, i følge informant fra NVE. Noe som dog kan ses på som en utfordring fra virksomhetene er at ROS-analysene deres ikke skal godkjennes av NVE, men vises frem på tilsyn. I følge NVE er dette fordi Beredskapsforskriften (2013) bygger på ansvarsprinsippet. Informant fra nettselskap poengterer for øvrig også at det kan være vanskelig å forholde seg til veiledningen til forskriften og de svar man får fra NVE, ettersom de varierer avhengig av hvem man spør.

6.3 Hva er utfordringene til IKT-sikkerhet og beredskap?

Gjennomgående er det blitt nevnt hvordan forholdet til IKT-sikkerhet ikke er så etablert siden det enda er et nytt område og alle virksomheter ikke har samme modenhetsnivå. Dermed er det desto viktigere at det er informasjonsdeling mellom sektorer og virksomheter, samt at det finnes et fungerende samvirke. Samvirkeprinsippet påpeker dette og er bærebjelken i beredskap. I tillegg stiller prinsippet krav til at det tas ansvar for å sikre et fungerende samvirke. Gjennom empirien kommer det frem at det er delte meninger om dette. Noen informanter mener at samvirket ikke er godt nok, og mener samvirke og åpenhet vil føre til et mer robust samfunn. Andre mener at det er fungerende, og spesielt NVE, KraftCERT og Mnemonic påpeker dette. Dette kan være fordi de har nærmere forhold til hverandre: KraftCERT er bransje-CERT, NVE er sektormyndighet og Mnemonic har vært med på opprettelsen til KraftCERT. Som nevnt tidligere er bestillerkompetanse et problem, og

KraftCERT sier også at de opplever at samvirket mellom dem og leverandører er. Noen av leverandørene sier det ikke er noe poeng i å samarbeide, mens konsulenter er interesserte. Informanten sier at det kanskje burde blitt lagt internasjonalt press på dette. Empirien viser også hvordan det kan være problematisk å være så strenge på sektorinndelingen, og at man burde se mer helhetlig på dette. Når det gjelder informasjonsdeling er det også delte meninger, men de fleste synes at den også kan bli bedre. Derimot etterlyser NorSIS en felles samarbeidsplattform for utveksling av sensitiv informasjon. Fra ekspertene sin side, er det enighet om at bransjen i seg selv ikke er flinke til å dele ulykker og nesten-ulykker, dermed kan ikke andre lære av deres erfaringer. I en beredskapsprosess er det viktig å innhente informasjon, og dersom denne type informasjon ikke blir delt bransjen seg i mellom, går mye verdifull læring tapt, og man kan heller ikke jobbe sammen for å finne en bedre løsning om det skulle skje flere ganger.

Et annet moment som viser seg å være en utfordring på IKT-sikkerhet og beredskap er den forskjellige forståelsen mellom IKT-miljø og sikkerhetsmiljø, og mangelen på kompetanseheving generelt. Informanten fra NVE påpeker nødvendigheten for å skape en felles forståelse mellom miljøene, som tross alt jobber mot samme mål. At man ikke skal konkurrere på sikkerheten er noe empirien viser, og dermed er åpenhet et viktig aspekt. Når det kommer til kompetanse på IKT-sikkerhet, er dette et felt som må oppdateres på alle nivå. Selv om det er enighet i at det er vanskelig å si noe om hvor mye kompetanse energiforsyningen har, er det fremdeles enighet om at den må forbedres. Trusselaktørene blir stadig mer avanserte og dermed må man holde tritt med utviklingen. Kompetanseheving nevnes både i beredskapsprosessen og HRT. I tillegg kommer det frem av empirien at det er lite fokus på IKT-sikkerhet i utdanning, på alle nivå, og at det også trengs mer forskning på beskyttelse av driftskontrollsystem. For å kunne håndtere og forstå kompleksiteten i systemene må man ha en evne til å forstå en helhet. Ved å øke kompetansen på alle nivå i en organisasjon kan man også se for seg at tendensen av menneskelige feil ikke vil være så fremtredende. Man må gå ut fra at om man gir personal informasjon og påminnelser om å opprettholde gode rutiner (noe som må gjøres kontinuerlig) så vil tallet på menneskelige feilhandlinger og svikt ikke øke.

Tidligere ble det nevnt at man ikke skal konkurrere på sikkerhet, og at det blir kuttet i ansatte som jobber med det. NSM (2015) understreker at det blir vanskeligere å oppdage angrep, og om man da ikke har tilgjengelig personal eller ressurser som kan håndtere dette er man ikke

godt nok beskyttet, og setter potensielt liv i fare. Sikkerhet koster, men kan ikke unnværes. Sikkerhet og pålitelighet er mål som skal gjennomsyre hele organisasjonen (Sagan, 1993), og for å kunne ha evnen til og både forutse og håndtere er man nødt til å ha de nødvendige ressursene på plass. Siden fokuset på IKT-sikkerhet økes er dette noe virksomheter også må tilpasse seg. Med den økte digitaliseringen kommer det også flere trusler og sårbarheter som man ikke har trengt å tenke over før nå. På den andre siden skal det også være en fordel for virksomheter å ta i bruk teknologi. Det kan tenkes at IKT-sikkerhet også nedprioriteres på grunn av manglende kunnskap og kommunikasjon mellom IT-avdeling og ledelse: informanter fra BDO sier at typisk for selskap som har gode beredskapsplaner på IKT er selskaper med god kobling mellom ledelse og IT-avdeling.

Når det gjelder kompleksiteten i system og teknologi vil den fortsette (Hagen et al., 2015). Ved å anvende et HRT perspektiv skal man altså kunne organisere seg for å kunne ta høyde for dette, selv om NAT mener det stikk motsatte. Derimot har Rijpma (1997) pekt på at en anvendelse av begge tilnærmingene kan være det som er mest lønnsomt i lengden. Selv om det kan virke som det er NAT som er den mest passende, er det stort fokus på organisasjonsdesign og viktigheten av å planlegge, analysere og gjennomføre øvelser. Dette er elementer av HRT, om av empirien ser man at det virker som de fleste har denne forebyggende tankegangen i mente. For IKT-sikkerhet vil det uansett være en utfordring å holde tritt med utviklingen fordi det går så fort. Dog, ved å ha gode analytiske evner, og vilje (optimisme) til å planlegge for ukjente hendelser, samtidig som man har stort fokus på tette koblinger og komplekse systemer (pessimistisk) skal det kunne være mulig å lage å ta høyde for uønskede hendelser.

7 KONKLUSJON

Denne oppgaven har forsøkt å besvare overordnet problemstilling: *Hvordan kan energiforsyningen etablere god beredskap på IKT-sikkerhet?*

Hensikten med denne studien var å undersøke en stadig økende tematikk i energiforsyningen, IKT-sikkerhet. Studien har undersøkt hvilke suksesskriterier som skal til for å ha en god beredskap på IKT-sikkerhet, og gjennom en kvalitativ datainnsamling har denne tematikken blir analysert og drøftet i lys av valgt teori. Studiens funn er at det er god forståelse på hva beredskap er, og hva den skal inneholde, men når det kommer til IKT-sikkerhet finnes det flere svakheter. Et sentralt poeng er at tross det økende fokuset på IKT er det fremdeles et nokså nytt område for mange, og virksomheter innehar ikke tilstrekkelig kompetanse og kunnskap. For å kunne bli gode på beredskap på IKT-sikkerhet må man øke fokus like mye på IKT-beredskap som fysisk beredskap. Derfor må det skapes en bedre dialog mellom IT-avdeling og beredskapsstab, og IT-avdeling og ledelse. ROS-analyser må oppdateres i tråd med det rådende trusselbildet, og dermed må man også innføre hendelser som vedrører IKT-sikkerhet, slik at det blir satt beredskap på disse.

Den økende kompleksiteten til systemene gjør det ikke enklere å oppdage angrep, men derfor er det også viktig at man innehar evnen til å detektere en hendelse, slik at man kan få avverget den. Derfor må kompetansenivået heves i hele energiforsyningen. Samvirke og informasjonsdeling er to måter dette kan gjøres på, men det viser seg også at fokus på IKT-sikkerhet må inn på utdanninger i tillegg. Skal nærhetsprinsippet gjelde, er man nødt til å inneha interne ressurser som kan håndtere dette. For oss mennesker er kompleksitet noe vanskelig å forholde seg til og desto viktigere er en riktig opplæring, samt beredskapsøvelser hvor det øves, trene sog evalueres. Sårbarhetene som finnes i et system må tas høyde for, og må avdekkes gjennom hele verdikjeden.

For å kunne ha en god beredskap på IKT-sikkerhet må sikkerhet gjennomsyre hele organisasjonen, noe ledelsen må være klare på. Dermed blir det risikabelt å kutte ned på sikkerhetspersonale fordi det blir sett på som kostbart. Trusselbildet er dynamisk og dermed trenger ressurser på sikkerhet. Vel så viktig er det å innføre en varslingskultur slik at hendelser og nesten-hendelser blir innrapportert. Disse hendelsene må vurderes og tas høyde for i ROS-analyser og beredskapsplaner. Her finnes læringspotensial som skal tas med i

videre arbeid. Etablering av beredskap er en kontinuerlig prosess, og målet er kontinuerlig forbedring. IKT-sikkerhet må forankres på høyeste nivå i ledelsen.

Basert på funn fra det foreliggende datamaterialet, kan en konkludere med fem retningslinjer til hvordan man kan etablere en god beredskap på IKT-sikkerhet:

6. ROS-analyser og verdivurdering er de viktigste elementene i identifiseringsfasen, og legger føring for resten av prosessen. Her må det nedsettes en analysegruppe som går gjennom potensielle IKT-trusler. Analysene må tilpasses trusselbildet og jevnlig oppdateres.
7. Beredskapsplanen må øves og trenes på. Og man gi folk ansvar for det de har til daglig ettersom de vil gjennomføre kjente oppgaver bedre. Man må vite hvilke ressurser man har tilgjengelige, både interne og eksterne. Dersom det oppstår en hendelse, og man ikke har denne kompetansen in-house, må man vite hvem man skal kontakte.
8. IKT-trusler kan endre karakter over tid, derfor må det hele tiden være fokus på kompetanseheving. I tillegg må man tilrettelegge for at virksomheten og dens ansatte er oppdaterte på sikkerhetsrutiner.
9. Sikkerhetstankegangen må gjennomsyre hele virksomheten, fra topp til bunn, og fra bunn til topp. Det er viktig at den samme forståelsen er gjennomgående i hele organisasjonen.
10. IKT-sikkerhet må ha likt høyt fokus som mer tradisjonell fysisk beredskap. Man kan ikke bli bedre på noe dersom det ikke blir prioritert. Dialog mellom ledelse, IT-avdeling og beredskapsstab må vektlegges.

7.1 Avsluttende bemerkninger og videre forskning

Denne studien er en av få kvalitative studier på IKT-sikkerhet og beredskap i kraftbransjen. Utvalg er åtte eksperter og to fra virksomheter. Mer kvalitativ forskning er nødvendig for å få en bredere forståelse av tema. En posisjon kan være å inkludere flere informanter fra energiforsyningen for å få et innsideblikk på hvordan IKT-sikkerhet og beredskap håndteres i praksis (eks. ledelse og ansatte). Det er mulig et slik utvalg ville gitt annen informasjon en den som foreligger i denne studien. Da dette er et understudert felt, kan innsikt fra kvalitative studier danne grunnlag for videre kvantitative studie på området. Det kan tenkes at teori om

Natural Accidents theory (NAT) og High Reliability Organization (HRO) kan benyttes som et rammeverk for kvantitative studier på IKT-sikkerhet i kraftbransjen.

8 BIBLIOGRAFI

Alexander, D. (2009). *Principles of Emergency Planning and Management.* England: Terra Publishing.

Aven, T., Boyesen, M., Njå, O., Olsen, K. H., & Sandve, K. (2014). *Samfunnssikkerhet.* Oslo: Universitetsforlaget.

BDO (2010). *Kraftf og fornybar energi.* Hentet (20.06.2016) fra http://www.bdo.no/kraftforsyning/

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

Blaikie, N. (2011). *Designing Social Research.* Cambridge, UK: Polity Press.

Bryman, A. (2004). *Social Research Methods.* New York: Oxford University Press.

Departementene (2012). *Nasjonal strategi for informasjonssikkerhet* (strategi). Hentet fra https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/nasjonal_strategi_infosikkerhet.pdf

Difi. (2016). *Veileder i planlegging og gjennomføring av IKT-øvelser* (veileder). Hentet fra https://www.difi.no/sites/difino/files/veileder_-_planlegging_og_gjennomforing_av_ikt-ovelser.pdf

DSB. (2001). *Systematisk samfunnssikkerhets- og beredskapsarbeid i kommunene* (veileder). Hentet fra http://www.dsb.no/Global/Publikasjoner/Tidligere/Andre/systematiskarbeidikommunene.pdf

DSB. (2012). *Sikkerhet i kritisk infrastruktur og kritiske samfunnsfunksjoner – modell for overordnet risikostyring* (KIKS-prosjektet – 1.delrapport). Hentet fra http://www.dsbinfo.no/DSBno/2012/Rapport/KIKS/

Dynes, R.R. (1993). "Disaster Reduction: The importance of adequate assumptions about social organization", i *Sociological Spectrum*, 13(1), 175-192.

E-ISAC og SANS. (2016). *Analysis of the Cyber Attack on the Ukranian Power Grid* (rapport). Henter fra https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

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#KAPITTEL_9

Goodman, M. (2015). *Future Crimes. Inside the digital underground and the battle for our connected world.* London: Corgi Books.

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

Hagen, J. M. (2009). *The Human factor behind the Security Perimeter – Evaluating the effectiveness of organizational infromation security measures and employees' contributions to security.* (Doktorgradsavhandling), Det matematisk-naturvitenskapelige fakultet, Universitet i Oslo, Oslo.

Hagen, J. M. & Albrechtsen, E. (2009). "Regulation of information security and the impact on top management commitment: A comparative study of the energy supply sector and the finance sector". I Martorell et al. (red), *Proceedings of Safety, Reliability and Risk Analysis: Theory, Methods and Applications* (s. 407-413). London: Taylor & Francis Group.

Hagen, J. (2014). Kronikk: Hva er status på Norges digitale beredskap? *NSR.* Hentet fra http://www.nsr-org.no/aktuelle-saker/kronikk-hva-er-status-paa-norges-digitale-beredskap-article407-110.html

Hagen, J. (red.) (2015). *Teknologiskifte i energiforsyningen. Studie om muligheter og sårbarheter* (NVE, rapport nr.: 118-2015). Oslo: Norges Vassdrags- og energidirektorat.

Hamnes, L. H. (2010, 08.10) Cyberkrigen er i gang. *Teknisk Ukeblad.* Hentet fra http://www.tu.no/artikler/cyberkrigen-er-i-gang/245547

Jaatun, M. G., Albrechtsen, E, Line, M. B. og Tøndel, I. A. (2008). "A framework for incident response management in the petroleum industry" i *International journal of critical infrastructure protection,* 2, 26-37. Hentet fra file:///C:/Users/Bruker/Downloads/Jaatun%20Integrated%20Operations%20A%20framework%20for%20incident%20response%20management%20in%20the.pdf

Johansen, P. A. (2016, 15.01). De sa det var umulig. Nå klarer russiske hackere å slå av strømnettet. *Aftenposten.* Hentet fra http://www.aftenposten.no/verden/De-sa-det-var-umulig-Na-klarer-russiske-hackere-a-sla-av-stromnettet-13199b.html

Johannessen, A., Tufte, P. A. og Christoffersen, L. (2010). *Introduksjon til samfunnsvitenskapelig metode.* Oslo: Abstrakt forlag AS.

Johnsen, S. O. (2012). *An Investigation of Resilience in Complex Socio-techinical Systems to improve Safety and Continuity in Integrated Operations.* (Doktorgradsavhandling), Fakultet for informasjonsteknologi, matematikk og elektronikk, Norges teknisk-naturvitenskapelige universitet, Trondheim.

Justis-og beredskapsdepartementet (2015). *Justis- og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet* (strategi). Hentet fra https://www.regjeringen.no/no/dokumenter/justis--og-beredskapsdepartementets-strategi-for-a-bekjempe-ikt-kriminalitet/id2413705/

Kovacs, E. (2017, 11.01) Ukraine Power Outage Not Directly Caused by Malware: Experts. *Security Week.* Hentet fra http://www.securityweek.com/ukraine-power-outages-not-directly-caused-malware-experts

Krutz, R. L. (2006). *Securing SCADA-systems.* (Doktorgradsavhandling). Indianapolis: Wiley Publishing. Hentet fra https://www.fer.unizg.hr/_download/repository/Securing_SCADA_Systems.pdf

Kvale, S. (1996). *Interviews: An introduction to Qualitative Research Interviewing.* California: SAGE Publications.

Kvale, S. og Brinkmann, S. (2009). *Det kvalitative forskningsintervju.* (T.M. Anderssen og J. Rygge, oversatt). Oslo: Gyldendal.

Lunde, I. K. (2014). *Praktisk krise- og beredskapsledelse.* Oslo: Universitetsforlaget.

Maxwell, J. A. (2008). "Designing a qualitative study", i *The SAGE handbook of applied social research methods,* (2), 214-253.

Meld. St. 17 (2001-2002). (2002). Samfunnssikkerhet - Veien til et mindre sårbart samfunn. Hentet fra https://www.regjeringen.no/no/dokumenter/stmeld-nr-17-2001-2002-/id402587/

Meld. St. 22 (2007-2008). (2008). Samfunnssikkerhet – samvirke og samordning. Hentet fra https://www.regjeringen.no/no/dokumenter/stmeld-nr-22-2007-2008-/id510655/?ch=1&q=

Meld. St. 29 (2011-2012). (2012). Samfunnssikkerhet. Hentet fra https://www.regjeringen.no/contentassets/bc5cbb3720b14709a6bda1a175dc0f12/no/pdfs/stm201120120029000dddpdfs.pdf

Meld. St. 25 (2015-2016). (2016). Kraft til endring. Energipolitikken mot 2030. Hentet fra https://www.regjeringen.no/contentassets/31249efa2ca6425cab08130b35ebb997/no/pdfs/stm201520160025000dddpdfs.pdf

Mnemonic. (2016). *Security Report 2016* (rapport). Oslo: Mnemonic AS.

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

NOU 2015:13. (2015). *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden.* Oslo: Departementenes sikkerhets- og serviceorganisasjon, Informasjonsforvaltning.

NSM. (2009). *Veiledning i verdivurdering* (veiledning). Oslo: Nasjonal sikkerhetsmyndighet.

NSM. (2015). *1. Halvårsrapport 2015.* Oslo: Nasjonal sikkerhetsmyndighet.

NSM. (2016). *Risiko 2016. Kan sikkerhet styres? En vurdering av sårbarheter og risiko i Norge.* Oslo: Nasjonal sikkerhetsmyndighet.

NSR. (2014). *Mørketallsundersøkelsen – Informasjonssikkerhet, personvern og datakriminalitet.* Oslo: Næringslivets Sikkerhetsråd.

NVE og Proactima (2010). *Veileder i risiko- og sårbarhetsanalyser i kraftforsyninga* (NVE Veileder nr: 2-2010). Hentet fra http://publikasjoner.nve.no/veileder/2010/veileder2010_02.pdf

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

Nygård, A. R. (2004). *Risk management in SCADA-system.* (Mastergradsavhandling), Norges teknisk-natuvitenskapelige universitet, Gjøvik.

Patton, M. (1990). *Qualitative Evaluation and Research Methods*. London: Sage Publications.

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

Perry, R. W. og Lindell, M. K. (2003). "Preparedness for Emergency Response: Guidelines for the Emergency Planning Process", i *Disasters, 27(4),* 336-250. DOI: 10.1111/j.0361-3666.2003.00237.x

Perry, R. W. og Lindell, M. K. (2007). *Emergency Planning.* USA: Wiley.

Politidirektoratet. (2015). *Overordnet nasjonal strategi for bekjempelse av datakriminalitet (Datakrimstrategien)* (publikasjon 2015/02). Hentet fra https://www.regjeringen.no/contentassets/4d2ba37bf2ae4cc9ac39afdf20a2f41b/datakrimstrategi_2015.pdf

Rijpma, J. A. (1997). Complexity. Tight-Coupling and Reliability: Connecting Normal Accidents Theory and High Reliability Theory. *Journal of Contingencies and Crisis Management, 5(1),* 15-23. DOI: 10.1111/1468-5973.00033

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

Sagan, S.D. (1993). *The Limits of Safety: Organizations, Accidents and Nuclear Weapons.* Princeton, NJ: Princeton University Press.

Skotnes, R. (2015). *Challenges for safety and security management of network companies due to increased use of ICT in the electric power supply sector.* (Doktorgradsavhandling), Det Samfunnsvitenskapelige Fakultet, Universitetet i Stavanger, Stavanger.

Totton, M. (2016). "How can you manage risks you don't know about?" i Mnemonic, (2016). (s. 26-28).

Trimintzios, P. (red.), Holfeldt, R, Koraeus, M. Uckan, B., Gavrila, R. og Makrodimitris, D. (2014). *Report on Cyber Crisis Cooperarion and Management* (rapport, ENISA). Hentet fra https://www.enisa.europa.eu/publications/ccc-study

Weick, K. E. (1987). "Organizational Culture as a Source of High Reliability", i *California Management Review 29(2).* 112-127.

Weick, K.E., Sutcliffe, K.M., Obstfeld, D. (1999). Organizing for high reliability: Processes of collective mindfullness. *Reasearch in Organizational* Behaviour, 21, 81-123. Hentet fra http://www.archwoodside.com/wp-content/uploads/2015/09/Weick-Organizing-for-High-Reliability.pdf

Wildavsky, A. (1991) *Searching for Safety.* New Brunswick, USA: Transaction Publishers.

Yin, R. K. (2007). *Fallstudier: Design och genomförande.* Malmö: Liber.

9 VEDLEGG

Vedlegg 1. Intervjuguide

Innledning

1. Kort om samtykkeskjema og intervjuet
2. Kort om organisasjonen informanten representerer

Dagens situasjon

1. Hvordan vil du beskrive dagens trusselbilde?
2. Hvordan tror du kraftbransjen selv ser på trusselbildet?
3. Hva betyr informasjonssikkerhet/IKT-sikkerhet for deg, og hvilken tilnærming har du til det?
4. Hvilke særegenheter har kraftbransjen, i forhold til andre bransjer?
5. Hvilke trusler mener du at kraftbransjen er utsatt for (generelt)?
    a. Hvilke informasjonssikkerhetstrusler er bransjen utsatt for?
        i. Eks. Tekniske feil, konkurs hos IT-driftsleverandøren
6. Hvilke tanker har du om kraftbransjen og raskt voksende teknologi, i forhold til informasjonssikkerhet?
    a. Tingenes internett (når alt kobles til og blir integrert)
    b. Hvilke trusler/utfordringer tror du kan bli mer aktuelle for kraftbransjen i fremtiden?
7. Hvordan ser du på kraftbransjens kompetanse på informasjonssikkerhet?
    a. Hva kan gjøres for å styrke kompetansen?

Beredskap generelt

1. Hva er beredskap for deg?
2. Planlegging?
3. Inkluderer dette også krisehåndtering?
4. Hva er koplingen mellom risikoanalysen og beredskapsplanen?
    a. Bør det være en kopling? Hva er svakheten og styrken ved en kopling?
    b. Hvordan er dette eventuelt i andre bransjer?
5. Øvelser er til for å trene og evaluere beredskapsplan, hva er viktigheten, nytten og læringen man kan ta av dette?
6. Hvordan fungerer beredskapsprinsippene, likhet, ansvar, nærhet og samvirke, i kraftbransjen?
    a. Hvordan kan disse forbedres, og hva skal da eventuelt til?

Samhandling

1. Hvordan er samhandlingen mellom leverandører, selskap, andre selskap i bransjen (hvis det er aktuelt), bransjeorganisasjoner, CERTer, og nødetater og andre myndigheter i krisehåndteringssituasjoner?
2. Hvordan kan man overføre erfaringer på tvers av sektorer, på best mulig måte?

Systemer

1. Hvilke utfordringer har bransjen når det gjelder informasjonssikkerhet, og hvor finnes de?

2. Praktisk informasjonssikkerhet (systemer i virksomheten som gjør at sikkerheten blir ivaretatt hele tiden): Er det mulig å lage systemer i en virksomhet som gjør at sikkerheten alltid blir ivaretatt?
    i. Hvordan kan det gjøres, med tanke på?:
        1. Kompetanse
        2. Leverandører
        3. Myndigheter
        4. Regelverk
3. Hva er viktigst av at systemene er tilgjengelige, men upålitelige, eller at de er helt nede?

Beredskapsforskriften i dag

1. Hvorfor er det nødvendig (etter din mening) å revidere forskriften, og hva blir eventuelt NSM sin rolle?
2. Hvilke vurderinger gjør du av beredskapsforskriften, slik den er i dag?
3. Hva er de utfordringene, som en revisjon av forskriften må ta høyde for?
4. Hvordan skal den revideres på best mulig måte?
5. Hvordan bør man ta høyde for problemstillinger som (i en ny revisjon)?
    a. Smarte strømmålere (AMS)
    b. Bruk av skylagring
    c. Personvern
    d. Logging
    e. Hendelseshåndtering
6. Mener du at Norge bør se til andre land, og deres erfaring?
7. Hva er god beredskap på IKT-hendelser?