EKSTERN RAPPORT

Nr. 18/2021

Kraftbransjens leverandørkjeder – digital sikkerhet og sårbarhet i globaliseringens tidsalder

UiS og NTNU

NVE Ekstern rapport nr. 18/2021
Kraftbransjens leverandørkjeder – digital sikkerhet og sårbarhet i globaliseringens tidsalder

Utgitt av: Norges vassdrags- og energidirektorat
Redaktør: Janne Hagen
Forfatter: Sigrid Haug Selnes, Sina Rebekka Moen, Siyang Emily Ji og Ove Njå

Forsidefoto: Kraftledninger i Årdal. Foto: Helena Nynäs/NVE

ISBN: 978-82-410-2166-4
ISSN: 2535-8235
Saksnummer: 202104778

Sammendrag: Kraftforsyningen er avhengig av leverandører. Rapporten drøfter digital sårbarhet og sikkerhet i komplekse leverandørkjeder. Rapporten gir anbefalinger til hvordan kraftbransjen kan forstå digital sårbarhet i leverandørkjedene, og hvordan virksomhetene og myndigheten kan jobbe med å redusere sårbarhetene.

Emneord: IKT-sikkerhet, cybersikkerhet, leverandørkjede, digital sårbarhet

Norges vassdrags- og energidirektorat
Middelthuns gate 29
Postboks 5091 Majorstuen
0301 Oslo

Telefon: 22 95 95 95
E-post: nve@nve.no
Internett: www.nve.no

desember, 2021

Innhold

Figurliste

Tabelliste

Forord

Kraftforsyningen digitaliserer, og det digitale trusselbildet er i endring. I Norge og i verden ellers er det de siste årene blitt rettet økt oppmerksomhet på leverandørkjedesikkerhet. Cyberangrepet mot leverandørene Solarwinds og Volue er noen av hendelsene som har bidratt til at temaet sikkerhet i leverandørkjeder er satt på dagsorden. Riksrevisjonen, som leverte sin rapport i mars 2021 om NVEs arbeid med IKT-sikkerhet i kraftforsyningen, pekte også på leverandørene i sin rapport: NVEs oppfølging av leverandørene er mangelfull til tross for at de har stor betydning for IKT-sikkerheten i kraftforsyningen.

NVE har gjennomført en studie av leverandørkjedesårbarhet og sikkerhet sommeren 2021. Denne rapporten dokumenterer arbeidet. Arbeidet er utført av tre studenter med tilknytning til UIS og NTNU, og studentarbeidet er finansiert av de samme institusjonene. Professor Ove Njå har veiledet studentene i arbeidet med denne rapporten. NVE retter en spesiell takk til UIS og NTNU i denne sammenhengen.

Rapporten inngår NVEs FOU prosjekt 80415 «IKT-sikkerhetstilstanden i kraftforsyningen». Grunnlaget for analysen i denne rapporten er personlige intervjuer med ressurspersoner i kraftforsyningen, samt data fra litteraturstudier og spørreundersøkelser som NVE har gjennomført sommeren 2021.

NVEs FOU-prosjekt 80415 har også hatt en referansegruppe som har bestått av eksperter fra Nasjonal sikkerhetsmyndighet (NSM), KraftCERT, EnergiNorge, Nettalliansen, Elvia, Arva, SiraKvina, Statnett, Valider, Siemens, NC Spektrum, NTNU og UIS. Ekspertene har bidratt med innspill til arbeidet. NVE vil takke samtlige i referansegruppen for gode diskusjoner og for deres bidrag.

Rapportens konklusjoner vil bli vurdert og fulgt opp i NVEs videre arbeid med å følge opp Riksrevisjonens kritikk og problemstillingene knyttet til sikkerhet og sårbarhet i leverandørkjedene.

Anne Rogstad
Fungerende direktør,
Tilsyn- og beredskapsavdelingen

Eldri Naadland Holo
Seksjonsleder

Dokumentet sendes uten underskrift. Det er godkjent i henhold til interne rutiner.

Sammendrag

Kraftforsyningen er en kritisk samfunnsfunksjon og en viktig del av samfunnssikkerheten. Andre kritiske samfunnsfunksjoner er avhengig av kraftforsyning. I takt med den digitale utviklingen i sektoren er stadig flere systemer og prosesser styrt av IKT-systemer. Avhengigheten til lange og uoversiktlige digitale verdikjeder er dermed større. Leverandørkjedesikkerhet har fått økt oppmerksomhet de siste årene da internasjonale leverandører har vært utsatt for flere cyberangrep som har fått vesentlige konsekvenser. NSM og PST hevder i sine trusselvurderinger for 2021 at norske virksomheter også er risikoutsatte når det gjelder cyberangrep på kritiske samfunnsfunksjoner.

For å kunne forbedre arbeidet med leverandørkjedesikkerhet må virksomhetene ha en oversikt over hva sårbarhetene i leverandørkjedene er. Kompleksiteten i leverandørkjedene kan gjøre det vanskelig å ha oversikt over alle ledd i kjeden. Manglende oversikt gjør det utfordrende å vurdere hvor det bør settes inn sikkerhetstiltak. Problemstillingen som vi har arbeidet med i denne rapporten er:

Hva er de digitale sårbarhetene i leverandørkjedene til norsk kraftforsyning?

Digitale sårbarheter er identifisert gjennom ENISAs (2021) taksonomi relatert til leverandørkjedeangrep. Utfordringer knyttet til leverandørkjedeangrep sett fra virksomhetenes side er basert på informasjon fra nøkkelinformanter i kraftforsyningen. Utfordringer som kompleksitet, oversikt, avhengighet, tillit, bestillerkompetanse, resiliens og sikkerhetskultur er belyst i rapporten. Sårbarhetene er illustrert ved to ulike leverandørkjedemodeller. Studien dokumenterer et behov for at virksomhetene i kraftforsyningen finner praktiske tilnærminger til den kontinuerlige styringen av sikkerheten, og at leverandørkjedene krever økt oppmerksomhet. Rapporten gir anbefalinger til hvordan bransjen kan forstå digital sårbarhet i leverandørkjedene, og hvordan virksomhetene kan jobbe med å redusere sårbarhetene.

Anbefalingene dekker følgende tema:

Ikke styrbare forhold, herunder politisk risiko, internasjonale kriser, og endringer i leverandørkjeden: Virksomheter med betydelig innslag av systemer fra leverandørkjeder forbundet med politisk risiko bør kartlegge risiko, og sørge for at denne vurderingen følger sikkerhetsarbeidet og de kritiske prosessene som overvåkes.

Ved internasjonale kriser bør virksomheter med avhengighet til globale verdikjeder gjøre en sårbarhetsvurdering.

Virksomheter i kraftforsyningen bør overvåke leverandørkjedene involvert i viktig infrastruktur for virksomheten, slik at beredskapsløsninger kan planlegges og iverksettes ved kritiske endringer i kjeden.

Risikostyring i forkant av anskaffelser: NVEs retningslinjer; IKT-sikkerhet i anskaffelser og tjenesteutsetting i kraftbransjen (2020), er en sjekkliste som fungerer som et verktøy i en forberedende fase, selve anskaffelsesfasen, i implementerings- og forvaltningsfasen og i opphørsfasen. Informanter har påpekt at en lignende type sjekkliste rettet mot leverandørene bør utarbeides og komme fra NVE, slik at leverandører har samme fokus på sikkerhet når det kommer til bruk av underleverandører. Ved å lage en sjekkliste med status som veileder eller retningslinje vil NVE involvere seg i forhold som bidrar til leverandørkjedesårbarhet.

Risiko- og sårbarhetsvurderinger – en arena for samarbeid: I tillegg til å være et beslutningsstøtteverktøy bør kraftsektoren også se på risiko- og sårbarhetsvurderinger som en arena for samarbeid og læring. Det krever at virksomhetene bruker analyseprosessene på nye måter.

Kritiske prosesser i anskaffelser: NVE bør bidra til å utarbeide en veileder for å identifisere kritiske prosesser i anskaffelser, så vel som i ordinær drift. Disse prosessene må kontrolleres ved hjelp av funksjoner som identifiserer utfordringer i god tid før det blir reelle problemer, slik at utfordringene korrigeres på en god måte.

Forskningsbasert kunnskap om risikostyring: Det bør etableres forskningsbasert kunnskap om risikostyring med hensikt å utvikle bruken av risikoanalyser i risikostyringen av sektoren.

Systemtenkning i det daglige sikkerhetsarbeidet: NVE bør ta initiativ til å utvikle rammeverket for systemtenkning sammen med virksomhetene i kraftforsyningen og øvrige enheter med ansvar for IKT-sikkerheten. Leverandørkjedesikkerhet kan på denne måten bli del av daglig arbeidspraksis og bidra til læringsprosesser som utvikler virksomhetene.

Leverandørkjedene vil fortsette å være viktige for kraftforsyningen i fremtiden, og utfordringene avdekket i denne rapporten krever at det arbeides målrettet for å ivareta sikkerheten gjennom hele leverandørkjeden. Anbefalingene i denne rapporten er et bidrag til dette arbeidet.

Forkortelser og definisjoner

ACER	The Agency for the Cooperation between Energy Regulators
APT	Advanced persistent threat: statlig styrte grupper med kapasitet og evne til å gjennomføre målrettede cyberangrep mot utvalgte virksomheter.
Cybersecurity	Beskyttelse av ting som er sårbare gjennom IKT (fysiske komponenter, digitale systemer og informasjon).
DSB	Direktoratet for sikkerhet og beredskap
ENISA	European Union Agency for Cybersecurity
EPRI	Electric Power Research Institute
GCI	Global Cybersecurity Index
Integritet	Uttrykk for at IKT-systemene, informasjonen som behandles i systemene og tjenestene tilknyttet systemene, ikke endres utilsiktet eller uautorisert (NOU 2018:14, 2014)
ITU	International Telecommunication Union
Konfidensialitet	Uttrykk for at IKT-systemene, informasjonen som behandles i systemene og tjenestene tilknyttet systemene, kun er tilgjengelige for dem som rettmessig skal ha tilgang til dem (NOU 2018:14, 2014).
NIS	Direktiv om tiltak for et høyt felles sikkerhetsnivå i nettverk og informasjonssystemer i hele EU (2016).
NIS2	Forslag om å videreutvikle og erstatte NIS, med et utvidet virkeområde, hvor det skal innlemmes flere sektorer som anses som kritisk for økonomien og samfunnet. Skal styrke sikkerhet i forsyningskjeder for viktige informasjons- og kommunikasjonsteknologier.
NSM	Nasjonal sikkerhetsmyndighet
Redundans	Begrense funksjonstap gjennom alternative løsninger, forhindre konsekvenser av kjente og ukjente trusler.
Resiliens	Tilpasning, fleksibilitet og motstandsdyktighet slik at funksjoner kan opprettholdes ved kritiske sikkerhetshendelser.
Risiko	Kombinasjonen av konsekvenser av en aktivitet og usikkerheten rundt hva disse konsekvensene kan være.
SCADA-system	Supervisory control and data acquisition – (SCADA), er en betegnelse av systemer for styring og overvåkning av prosesser, i dette tilfellet ulike deler av kraftforsyningen.
Sikkerhetskultur	Et sett med verdier som deles av medarbeiderne i en virksomhet, og som er med å påvirke deres tanker og forventninger til sikkerhet.
Sårbarhet	Uttrykk for et systems (manglende) evne til å opprettholde sin funksjon dersom systemet utsettes for uønsket påvirkning.
Tilgjengelighet	Uttrykk for at IKT-systemene, informasjonen som behandles i systemene og tjenestene tilknyttet systemene, er tilgjengelige der, og når brukerne trenger dem (NOU 2018:14, 2014).
Tillit	Kjøperen stoler på at leverandøren leverer produktet i tide, at det har rett kvalitet, og riktig pris.

1 Innledning

1.1 Kraftbransjen – system, aktører og funksjoner

Denne rapporten er en del av NVEs FOU prosjekt 80415; «IKT-sikkerhetstilstanden i kraftforsyningen», og dekker temaet leverandørkjedesårbarhet og leverandørkjedesikkerhet. Etikkinformasjonsutvalget har definert *leverandørkjede* (Etikkinformasjonsutvalget, 2019): «Med utgangspunkt i EUs og OECDs begrepsbruk definerer vi leverandørkjeden som alle vare- og tjenesteytende virksomheter som leverer innsatsfaktorer til en virksomhet, og har en direkte tilknytning til selskapets forretningsvirksomhet, produkter eller tjenester. Leverandørkjeden omfatter de aktiviteter, organisasjoner, aktører, teknologier, informasjon, ressurser og tjenester som er involvert i prosessen med å flytte og bearbeide et produkt fra råvarestadiet til et ferdig produkt. I dette inngår transport, agenter og andre mellomledd». Digitalt sårbarhetsutvalg har definert en *digital verdikjede* defineres som; «en struktur av leveranser mellom virksomheter, hvor hver leveranse enten er en digital tjeneste, software eller hardware» (NOU 2015:13).

Kraftforsyningen er i seg selv en kritisk samfunnsfunksjon som andre kritiske samfunnsfunksjonene er avhengig av. Sektoren er svært viktig for samfunnets overordnede funksjonalitet (DSB, 2016). Elektrisiteten må leveres med rett spenningskvalitet, og den må leveres til forbrukerne når forbrukerne trenger den.

Norsk kraftforsyning har en høy grad av leveringspålitelighet (i snitt 99,99%). Pålitelige og sikre digitale systemer er viktige hjelpemidler for å kunne opprettholde høy grad av leveringssikkerhet og kvalitet. I kraftsektoren skiller vi mellom administrative IT-systemer og driftskontrollsystemer, vanligvis betegnet operasjonell teknologi (OT). I kraftforsyningen ser vi at det er økte investeringer i digitale løsninger, i form av IT-systemer og digitale verktøy som benyttes aktivt gjennom hele kraftforsyningens verdikjede (NOU 2015:13, 2015). Sårbarheten i sammenkoblede IT-systemer avgjøres av det svakeste leddet, noe som underbygger viktigheten av å tenke helhetlig og inkludere alle deler av systemet når aktører vurderer risiko i verdikjeder og leverandørkjeder (NVE, 2017).

1.2 Hvorfor er kraftforsyning et komplekst system?

Folk som jobber i kraftbransjen, vil i mange tilfeller være uenig i at kraftforsyning er et komplekst system. Ren energi fra vind/vann omformet til elektrisitet hos forbruker er veldefinert og teknisk enkelt å forstå. Kompleksitet handler ikke om dette. Kompleksitet er knyttet til vår evne til å predikere hvordan kraftforsyningen vil fungere i et fremtidsperspektiv, gitt alle komponentene, enhetene, undersystemer og systemet som helhet. Det er mange aktører og funksjoner som skal fungere og kommunisere seg imellom. Dette løses i økende grad av digitale systemer som gir høy effektivitet, samtidig som aktørene mister innsikt i hvordan prosessene foregår. Det gir flere såkalte «ukjente sekvenser, eller ikke-planlagte og uventede sekvenser, som enten er ikke-synlige eller umiddelbart ikke til å forstå (Perrow, 1999). Kraftbransjen er eksponert for (Leveson, 2016):

- Samhandling mellom systemkomponenter (som kan være hvordan ulike programmer kommuniserer seg imellom i ulike IT og styresystemer)
- Endringer over tid (oppdateringer og ny teknologi, for eksempel ved innføring av 5G)
- Strukturelle og funksjonelle nedbrytninger som ikke er konsistente (globale leverandørkjeder, verdensomspennende kriser og avhengighet til kritiske komponenter, se eksemplene om SolarWinds og Volue i kapittel 1.3).

- Ingen direkte eller åpenbare koplinger mellom årsak og virkning (vanskelig å avdekke årsaksforhold til svikt, konfidensialitet, tilgjengelighet eller integritet)

Kraftbransjen er i utvikling. Vi hevder at selv om det er åpenbart velfungerende systemer og kontrollfunksjoner som sikrer bransjens høye leveringspålitelighet, så må denne økende kompleksiteten anerkjennes og utfordres. Denne rapporten ser på leverandørkjedenes bidrag til økt kompleksitet.

Digitaliseringsprosessene i kraftsektoren har ført til at flere sentrale funksjoner i dag støttes av IKT-løsninger som integreres i systemene og mellom systemene. Det konstrueres lange digitale verdikjeder med komplekse samhandlingsmønstre og avhengighetsforhold. Dette fører til en betydelig økning i bransjens totale kompleksitet. Sårbarheter kan oppstå i alle ledd, forplante seg videre i verdikjeden, og gjøre bransjen mer utsatt for cybertrusler (NOU 2015:13, 2015).

IKT-sikkerhet i kraftforsyningen må både forankres i vurderinger av ekom-sårbarhet og mer direkte rettede sårbarheter i kraftsektoren, på grunn av den store avhengigheten mellom disse samfunnsfunksjonene. Svikt i telekommunikasjonssystemene vil også kunne ramme virksomheter i kraftforsyningen der hvor evnen til å utveksle informasjon, evnen til å integrere informasjon fra mange sensorer og aktuatorer og den relaterte robustheten blir forstyrret. Nettverksangrep og sosial manipulasjon kan resultere i uautorisert avlytting av eller tilgang til informasjon. Ved innføring av 5G vil kapasiteten i datanettet øke, nye tjenester kunne bli tatt i bruk og avhengighetene til ekom bli enda større. Dette bil bidra til at usikkerheten øker i de kritiske samfunnsfunksjonenes integrerte løsninger. Når vi snakker om IKT-sikkerhet i kraftforsyningen er det ofte koplet til direkte angrep på og svikt i de digitale systemene konstruert for å styre selve produksjonen av elektrisk kraft eller drifte kraftnettet. Kraftforsyningen har komplekse logiske-fysiske strukturer, for eksempel gjennom driftskontrollsystemene, og kritiske objekter, for eksempel transformatorstasjoner. Mange virksomheter skal samvirke for at forsyningssikkerheten skal opprettholdes. Denne kompleksiteten underbygger behovet for fokus på sikkerhet i leverandørkjeder, ettersom det i hovedsak er leverandørkjedene som leverer komponenter og IT-tjenester. Her ligger kraftforsyningens totale kompleksitet, de er utsatt for uønsket påvirkning eller angrep som påvirker tilkoblede enheter i kraftforsyningen.

1.3 Noen relevante hendelser

Leverandørkjedesikkerhet har fått økt oppmerksomhet de siste årene, i takt med at internasjonale leverandører i økende grad er utsatt for kryptoskadevare og cyberangrep som får konsekvenser for flere ledd i leverandørkjeden. EUs institutt for cybersecurity, ENISA, har analysert 24 leverandørkjedeangrep fra januar 2020 til starten av juli 2021 (ENISA, 2021). Leverandørkjedeangrep krever minst to angrep. For det første må leverandøren angripes, for deretter å utnytte det som oppnås i et angrep mot kundene, i vårt tilfelle virksomheter i norsk kraftsektor og deres verdier. ENISA viser da til fire nøkkelelementer som alltid må være med i en analyse av leverandørkjedeangrep:

1. Leverandør – enhet utenfor kraftforsyningen som leverer et produkt eller tjeneste til en virksomhet i kraftforsyningen.
2. Leverandørverdier (assets) - viktige komponenter eller enheter som leverandøren benytter i sin produksjon eller tjenestetilbud.
3. Kunde (virksomhet i kraftforsyningen) – bruker av produktet eller tjenestene som leverandøren tilbyr.

4. Kundens verdier (assets) – viktige verdier, enheter eller elementer som eies eller disponeres av virksomheten i kraftforsyningen.

Tidslinjen for angrepene analysert av ENISA viser at 33% av angrepene ble rapportert i 2020, og 66% ble rapportert mellom januar og juli 2021. Dataene indikerer en trend hvor leverandørkjedeangrep øker, og ENISA anslår at vi i 2021 kan få en firedobling i antall leverandørkjedeangrep (ENISA, 2021). I forhold til norsk kraftforsyning gir dette et behov for sektoren å være enda mer kontrollerende overfor leverandørkjedene til sektoren. En av årsakene til denne trenden er ifølge ENISA at virksomheter i ulike sektorer har styrket sine forsvar mot cyberangrep og at det dermed er enklere å gå via leverandørkjeder. Angrepene på SolarWinds og Volue er eksempler på leverandørkjedeangrep som fikk store konsekvenser.

SolarWinds er et amerikansk IT-selskap, og leverandør av programvaresystemet Orion, som brukes til styring av informasjonssystemer. Orion har over 33 000 brukere i hele verden (Jibilian & Canales, 2021). Selskapet er ansvarlig for å oppdatere og vedlikeholde programvaresystemet, og sender oppdaterte versjoner til sine kunder. I 2020 installerte over 18.000 kunder en oppdatering som var utsatt for et omfattende og sofistikert dataangrep, hvor hackere satte inn en skadelig kode i Orions oppdateringsfil. Da oppdateringen ble installert hos kundene, åpnet den samtidig en bakdør i systemet, som videre kunne brukes av hackerne til å installere skadelige programmer. Senere skulle det vise seg at det gikk over et år fra operasjonen startet til den ble oppdaget, og at angriperne mellom mars og desember 2020 hadde tilgang til bakdøren i systemet. Over 100 selskaper ble rammet, blant annet flere amerikanske departementer og Microsoft (Oladimeji & Kerner, 2021). Virksomhetene som ble aktivt hacket kan ha sensitiv informasjon på avveie. Informasjonen kan brukes til senere angrep, eller til å kreve løsepenger. Angrepet viser hvor store konsekvenser sårbarheter i ett innslagspunkt kan ha, og hvordan angripere gjennom en slik tilgang kan ramme et stort antall virksomheter, også andre leverandører i leverandørkjedene (som Microsoft). Det kan ta flere år å kartlegge omfanget, og det kan ta flere år før systemene kan anses som sikre. Arbeidet med å redusere konsekvensene av angrepet kostet over 150 millioner kroner i første kvartal av 2021, og SolarWinds forventer at sluttsummen vil ende på flere milliarder. Også norske virksomheter har installert oppdateringen fra Orion, men det er så langt ikke påvist skade i norske virksomheter (NSM, 2021).

Volue er en internasjonal leverandør av virksomhetskritiske programvare- og teknologitjenester for energi-, strømnett – og infrastrukturmarkedet. Selskapet ble i mai 2021 utsatt for et cyberangrep. Angriperne fikk tilgang til Volues systemer via innloggingsdetaljene til en ansatt hos en kunde, og infiserte systemet med programvaren Ryuk. Ryuk er en typisk programvare for løsepengeangrep, som nekter en bruker eller organisasjon tilgang til filer eller servere på maskinen. Filene krypteres, og angriperne krever betaling for å gi tilgang til dekrypteringsnøkkelen. Angrepet på Volue ble oppdaget etter få timer, og Volue satte umiddelbart i gang operasjon «Stop & recover». De greide i løpet av kort tid å stoppe angrepet, få oversikt over omfanget og gjenopprette data. I løpet av de neste dagene ble de aller fleste kundene ansett som trygge, og det er ingen indikasjon på at det ble hentet ut data under angrepet (Volue, 2021). Volue valgte å være åpne om angrepet allerede samme dag, og har fått ros både nasjonalt og internasjonalt for sine åpne videokonferanser hvor de har orientert om prosessen.

Volue tapte mellom 30-40 millioner kroner på angrepet (Infront TDN Direkt, 2021). Det kunne potensielt ha fått store konsekvenser for hundrevis av kunder, men den raske responsen førte til at kundene i svært liten grad ble påvirket, og at det kun var Volue-teknologi som ble rammet. Hendelsen er likevel et eksempel på hvordan et leverandørkjedeangrep kan forløpe, ved at angriper gjennom en kunde kan ramme leverandøren, og potensielt forplante den infiserte programvaren videre i leverandørkjeden og ut til kunder.

Disse eksemplene er relativt like, da det i begge tilfeller er brukt skadelig programvare, men det finnes et stort spekter av ulike angrepsmetoder som vi presenterer i kapittel 2.2.

1.4 Problemstilling

Med den digitale utviklingen har kritiske samfunnsfunksjoner blitt avhengige av lange og uoversiktlige digitale verdikjeder. Underleverandører i et land vil kunne arve sårbarheter fra andre land. En digital verdikjede er en oversikt over både fysisk infrastruktur, hvem som eier, vedlikeholder og opererer ulike deler av denne, en oversikt over de digitale tjenestene som utveksles mellom disse delene, samt software og hardware (Njå, Sommer, Rake, & Braut, 2020). Utviklingen skaper endringer i samfunnets risiko- og sårbarhetsbilde, og med dette opplever vi nye trusler, eksempelvis kan maskiner og infrastruktur i Norge angripes av anonyme aktører i andre land. Sårbarhet defineres som «*et uttrykk for de problemer et system får 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 2000:24, 2000). For å kunne forbedre arbeidet med leverandørkjedesikkerhet, må virksomhetene først ha en oversikt over hva sårbarhetene i leverandørkjedene er, og hvor i leverandørkjeden de ulike sårbarhetene kan oppstå. Vi har derfor arbeidet med følgende problemstilling:

Hva er de digitale sårbarhetene i leverandørkjedene til norsk kraftforsyning?

Det å skaffe en oversikt over sårbarhetene og etablere et begrepsapparat for ulike typer sårbarheter i leverandørkjedene til norsk kraftforsyning er vesentlig når virksomhetene i sektoren skal evaluere sine egne systemer og funksjoner. Leverandørkjedene som blir benyttet må beskrives og undersøkes i seg selv, men virksomhetene må også avdekke hva de kan ha innsikt i og hva som ikke er mulig å fullt ut kontrollere.

Hensikten med denne rapporten er å utfordre virksomhetene i norsk kraftbransje til å kjenne til egne systemer, etablere strukturfunksjoner og ha evne til å kontrollere strukturfunksjonene. Det handler om å ha oversikt over egne systemer og ansvaret som følger dem. Gjennom systembegrensninger og sensorfunksjoner vil virksomhetene kunne ta ansvar og bygge inn en praksis for sikkerhetstenkning. Denne rapporten peker på disse mulighetene som da er et skritt videre enn tradisjonell risikostyring som Lysneutvalget (DSB, 2020) beskriver i sine anbefalinger til risikostyring i digitale verdikjeder. Det er en første tilnærming til å bygge resiliente virksomheter ved hjelp av systemtenkning (Njå, Sommer, Rake, & Braut, 2020) (Leveson, 2016).

Kraftbransjens digitale systemer er i stor grad produsert, levert og driftet av leverandører. Undersøkelser viser at bransjen i stor grad er avhengig av leverandørene, da mange virksomheter selv ikke har kompetanse eller kapasitet til å følge opp alle systemene de benytter selv. Feil og sikkerhetshendelser hos leverandører rammer også selskap i kraftbransjen. 8 av 10 virksomheter i kraftsektoren oppgir at de er avhengig av leverandører for å håndtere hendelser (NVE, 2018). Å ta hensyn til IKT-sikkerhet i anskaffelser og tjenesteutsetting er derfor nødvendig for å beskytte seg mot tilsiktede og utilsiktede hendelser.

1.5 Rapportens oppbygging

Kapittel 1 gir informasjon om bakgrunnen for studien, og en kort introduksjon til temaer som utdypes senere i rapporten. Her presenteres også problemstillingen vi har søkt å svare på i dette prosjektet. Kapittel 2 presenterer rapportens metode og datagrunnlag. Her beskrives fremgangsmåten, fremdriften og datagrunnlaget for undersøkelsen. Vi presenterer ENISAs taksonomi relatert til

leverandørkjedeangrep, og vi utdyper hva som menes med komplekse systemer.

I kapittel 3 har vi utviklet to modeller som viser typiske leverandørkjeder. Den første viser en modell med sterk hovedleverandør av komponenter, og den andre en distribuert leverandørkjede.

Kapittel 4 tar for seg faktorer med betydning for IKT-sikkerhet. Her knyttes teori opp mot empiri fra intervjuer og litteraturstudier. Viktige redegjørelser i dette kapittelet er økonomisk globalisering, resiliens, risikostyring og sikkerhetskultur. I dette kapittelet beskriver vi hva som skjer på cybersikkerhetsområdet i USA, Kina og EU.

Kapittel 5 presenterer digitale sårbarheter i leverandørkjedemodeller. Grunnlaget er intervjuer med eksperter. Modellene inkluderer eksempler på hvor trusler og sårbarheter kan ramme leverandørkjeden.

Kapittel 6 inkluderer blant annet utfordringer med å holde oversikt over leverandørkjeden, kraftforsyningens avhengighet til IT-systemer, leverandørkjedenes kompleksitet, viktigheten av å stole på leverandører, redundans og tilstrekkelig bestillerkompetanse.

Kapittel 7 utdyper digital sårbarhet i leverandørkjeder. Dette inkluderer ikke-styrbare forhold og risikostyring både i forkant av en anskaffelsesbeslutning og risikostyring i hele levetiden. Vi presenterer et sett av anbefalinger som kan møte utfordringene vi har identifisert.

Kapittel 8 konkluderer med viktige funn fra undersøkelsen.

2 Studiet av kraftbransjens leverandørkjeder

2.1 Arbeidet med studien

Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen har vært viktig i arbeidet med denne rapporten. Riksrevisjonen mener at oppfølgingen av leverandører er mangelfull, til tross for at leverandørene har stor betydning for IKT-sikkerheten i kraftforsyningen. Ettersom mange selskaper i energisektoren helt eller delvis har tjenesteutsatt driften av IKT-systemer, vil IKT-sikkerheten og beredskapen til virksomhetene i kraftforsyningen også være avhengig av leverandørenes IKT-sikkerhet. Kompetanse på IKT-sikkerhet og evne eller mulighet til å føre tilsyn med leverandørenes IKT-sikkerhet er to vesentlige utfordringer (Riksrevisjonen, 2021).
I denne studien har vi undersøkt hva som oppfattes og beskrives av sårbarhet knyttet til leverandørkjedene i norsk kraftbransje. Vi har spesielt fokusert på IT-systemene (de administrative), siden OT-systemene er underlagt vesentlige restriksjoner og at vi som forfattere har begrenset tilgang til informasjon. Imidlertid skiller ikke datamaterialet vårt så sterkt på hvilke digitale funksjoner som er sårbare, og dermed kan vi anta at mye som beskrives av sårbarhetene også kan overføres til OT-systemer.

Vi har gjort litteratursøk med søkeord som "supply chain risk management", "cybersecurity", "supply chain energy power supply", "supply chain attack". Søkene har resultert i et relativt lite antall treff, og underbygger antakelsen om at det er behov for mer forskning på området. Litteraturen dekker i større grad fysiske leverandørkjeder, eksempelvis i transport og handel, og dekker i mindre grad digitale leverandørkjeder. Det eksisterer flere norske og internasjonale utredninger som vi har benyttet. Vi har benyttet rapporter og artikler utgitt av EU-organisasjoner, som handler om regulering og anbefalinger til fremtidig arbeid med cybersikkerhet.

Parallelt med denne studien gjennomførte NVE to surveyer i kraftbransjen med hensikt å avdekke IKT-sikkerhetstilstanden i kraftforsyningen (NVE, 2021). NVE utviklet sine spørreskjemaer i nært samarbeid med representanter for virksomheter i kraftforsyningen og andre som er involvert i arbeid med å avdekke trusler og sårbarheter i bransjen. Spørreundersøkelsene inkluderte spørsmål om sikkerhetstilstanden og sikkerhetsledelse, og er besvart av henholdsvis 117 og 134 respondenter. Respondentene ble bedt om å svare på bakgrunn av erfaringer fra de siste 12 månedene (NVE, 2021). Dialogene, surveyinstrumentene og litteraturstudien dannet grunnlaget for dybdeintervjuer med et utvalg av nøkkelinformanter. Disse gav oss muligheten til å utfordre nye områder som kunne være forbundet med sårbarhet. På denne måten oppstod problemstillinger som stadig krevde mer systemkunnskap om kraftsektoren.

Informantene er strategisk valgt, på bakgrunn av deres kunnskap og kompetanse, se vedlegget. Det er gjennomført totalt 11 intervjuer, og vi har i noen tilfeller hatt kontakt i etterkant for utdypende informasjon eller oppfølgingsspørsmål. Informantene representerer nettselskaper, kraftprodusenter, leverandører og andre relevante aktører i kraftbransjen.
Analysen av data består av kategorisering av informasjon, med formål om å identifisere sårbarheter og å finne ut hvorfor og hvordan bransjen blir eksponert for farer og trusler. Litteraturstudier og data fra intervjuer er systematisert og sammenlignet gjennom å sammenstille svarene. Ved hjelp av denne metoden har det vært mulig å få oversikt over sammenfallende eller avvikende svar fra informanter, i tillegg til at det har bidratt til å danne et helhetlig bilde av hvordan litteraturen beskriver

kunnskapsstatus for dagens cybersikkerhet, og hvordan virksomhetene i den norske kraftsektoren opplever det i praksis.

2.2 Taksonomi relatert til leverandørkjedeangrep

For å kunne drøfte problemstillinger omkring sårbarhetene i kraftforsyningen med hensyn til leverandørkjeder, behøver vi et omforent begrepsapparat. I EU er dette utviklet gjennom ENISA, og for oss ble det viktig å bruke dette apparatet i vårt arbeid med norsk kraftbransje. Vi presenterer derfor denne taksonomien, både for å forstå våre videre analyser, men også som utgangspunkt for virksomhetene sine egne analyser om samme tema. Taksonomien er ment å hjelpe virksomheter å forstå de ulike delene av et leverandørkjedeangrep, og ikke minst å kunne detektere om de er utsatt for et leverandørkjedeangrep (ENISA, 2021).

En trussel kan defineres som «*en mulig årsak til en uønsket hendelse*» (NOU 2015:13, 2015). Å sikre seg mot en uønsket hendelse innebærer at vi må ha et måleapparat, slik at vi kan uttrykke og måle behovet for beskyttelse av informasjonssystemer. De tre sentrale sikkerhetsmålene er *konfidensialitet*, *tilgjengelighet* og *integritet*. Konfidensialitet handler om beskyttelse mot at sensitiv informasjon blir kjent for uvedkommende. Tilgjengelighet handler om å sikre at informasjon og tjenester er tilgjengelig ved behov. Integritet handler om at informasjon er troverdig og at tjenester og systemer fungerer slik de er tiltenkt.

2.2.1 Leverandørangrep

Et leverandørkjedeangrep defineres som en kombinasjon av to angrep; først et angrep mot en leverandør, og deretter angrep på kunden eller andre leverandører som inngår i kjeden. Dermed er både leverandøren og kunden mål for angrepet, og virksomheter kan være sårbare for leverandørkjedangrep selv om deres egen IKT-sikkerhet er god, fordi inngangen kan være gjennom andre aktører i leverandørkjeden (ENISA, 2021). ENISA har fra januar 2020 til juli 2021 kartlagt leverandørkjedeangrep og identifisert ulike angrepsteknikker.

Leverandøren og leverandørens verdier (assets)	
Angrepsteknikker brukt for å kompromittere leverandørkjeden	Leverandørens verdier som er mål for leverandørkjedeangrepet
Skadelig programvare	Eksisterende programvare
Sosial manipulasjon (social engineering)	Programvare-bibliotek
Brute-Force-angrep	Kode
Utnytte programvaresårbarhet	Konfigurasjoner
Utnytte konfigurasjonssårbarhet	Data
Open-Source Intelligence (OSINT)	Prosesser
	Hardware/maskinvare
	Mennesker
	Leverandør

Tabell 1. Taksonomi for leverandørkjedeangrep.

Tabell 1 viser angrepsteknikker som er brukt for å kompromittere leverandørkjeden, og hvilke verdier hos leverandøren som har vært mål for angrepet.

Videre presenterer ENISA ulike angrepsteknikker som er brukt for å kompromittere leverandøren i en leverandørkjede, og påpeker at flere av disse kan bli brukt i ett og samme angrep.

Angrepsteknikker brukt for å kompromittere en leverandørkjede	
Skadelig programvare	For eksempel spionprogrammer brukt til å stjele identifikasjon fra ansatte.
Sosial manipulasjon (social engineering)	For eksempel phishing, falske søknader, typosquatting, WiFi-etterligning, overbevise leverandør til å gjøre noe.
Brute-Force-angrep	For eksempel gjette et SSH-passord, gjette en web-pålogging.
Utnytte programvaresårbarhet	For eksempel SQL-injeksjon eller utnyttelse av bufferoverflod i en applikasjon (overskrive minnet).
Utnytte konfigurasjonssårbarhet	For eksempel utnytte et konfigurasjonsproblem.
Fysisk angrep eller modifikasjon	For eksempel modifisere maskinvare, fysisk inntrenging.
Open-Source Intelligence (OSINT)	For eksempel søk på nettet for identifikasjon, API-nøkkel, brukernavn.
Forfalsking	For eksempel etterligning av USB med ondsinnede formål.

Tabell 2. Angrepsteknikker for å kompromittere en leverandørkjede.

ENISA vektlegger at angrepsteknikker refererer til hvordan angrepet foregår, men ikke hva som ble angrepet. Angrepsteknikkene er utviklet fra de 24 hendelsene som forfatterne av ENISA-studien undersøkte. Taksonomien skiller dermed på passord funnet fra nettet (OSINT) eller ved systematiske angrep (Brute-force), men er ikke opptatt av om for eksempel passordet fra nettet var lekket, var et «default» passord eller passord solgt på det svarte markedet.

Leverandørverdier (assets) som mål for leverandørkjedeangrep	
Eksisterende programvare	For eksempel; programvare brukt av leverandøren, web-servere, applikasjoner, databaser, monitoreringssystemer, sky anvendelser, fast program. Denne kategorien dekker ikke programvare-bibliotek.
Programvare-bibliotek	For eksempel; tredjeparts bibliotek, programvare-pakker installert fra tredjeparter.
Kode	For eksempel; kilde-kode eller programvare produsert av leverandøren.
Konfigureringer	For eksempel; passord, API-nøkler, brannmur-regler, URL.
Data	For eksempel; informasjon om leverandøren, sensorverdier/-målinger, sertifikater, persondata – kunder/leverandører, andre persondata.
Prosesser	For eksempel; oppdateringer, sikkerhetskopiering eller valideringsprosesser, prosesser knyttet til godkjenning/signering av sertifikater.
Hardware, maskiner	For eksempel; maskinvare utviklet av leverandøren, chips, ventiler, USBs.
Mennesker	For eksempel; målrettet mot spesifiserte individer med tilgang til data, infrastruktur eller til andre mennesker.

Tabell 3. Leverandørverdier (assets) som mål for leverandørkjedeangrep.

Det som er spesielt med disse leverandørverdiene er at de har en kopling til sluttmålet hos virksomheten i kraftsektoren. En analyse må derfor ta utgangspunkt i denne helhetlige forståelsen. Basert på tilgjengelighet og åpenheten om leverandørene vil disse analysene ha ulike utfordringer. ENISA klarte å spore omlag halvparten av de studerte angrepene til konkrete «miljøer».

2.2.2 Kundeangrep (virksomheter i kraftforsyningen)

Kunde (virksomhet i kraftforsyningen) og kundens verdier (assets)	
Angrepsteknikker brukt for å kompromittere kunden	Kundens eiendeler som er mål for leverandørkjedeangrepet
Tillitsforhold [T1199] Drive-by Compromise (spesifikke målgrupper) [T1189] Phishing [T1566] Skadelig programvare Fysisk angrep eller modifikasjon Forfalskning	Data Personlig informasjon Åndsverk Programvare Prosesser Frekvensområde Finans Mennesker

Tabell 4. Kundeangrep (virksomheter i kraftforsyningen).

Taksonomien fra leverandørkjedeangrep sammenfaller enkelte ganger med generell taksonomi (MITRE ATT&CK, 2021). Som da er angitt med sin kategori i parentes i tabell 4.

ENISA beskriver ulike angrepsteknikker for å kompromittere en kunde, hvor noen av teknikkene sammenfaller med angrepsteknikkene som brukes mot leverandører.

Angrepsteknikker brukt for å kompromittere en kunde	
Tillitsforhold	For eksempel; stole på sertifikat, stole på automatisk oppdatering, stole på automatisk sikkerhetskopiering.
Drive-by Compromise (angriper spesifikke målgrupper)	For eksempel; skript på et nettsted for å infisere brukere med skadelig programvare.
Phishing	For eksempel; meldinger som etterligner leverandøren, falske oppdateringsvarsler.
Skadelig programvare	For eksempel; Trojan (RAT), bakdør, løsepengevirus.
Fysisk angrep eller modifikasjon	For eksempel; modifisere maskinvare, fysisk inntrenging.
Forfalskning	For eksempel; lage en falsk USB, modifisere et hovedkort, etterligning av leverandørs personell.

Tabell 5. Angrepsteknikker for å kompromittere en kunde.

Kundeverdiene i tabell 6 er sluttmålet for leverandørkjedeangrepene, og det er viktig å identifisere hvilke verdier som er både utsatte og sårbare hos virksomhetene i kraftforsyningen, og å oppdatere cybersikkerhetsstrategien til å omfatte leverandørkjeden (ENISA, 2021).

Kundeverdier (assets) som mål for leverandørkjedeangrep	
Data	For eksempel; utbetalingsinformasjon, video-feeds, dokumenter, e-poster, flyreiseinformasjon, salgsdata og finansdata, intellektuell eiendom (patenter, bedriftshemmeligheter).
Persondata	For eksempel; kundedata, ansatt-registreringer, identifikasjonsdata/legitimasjon.
Programvare	For eksempel; tilgang til kundens produkt kildekode, modifiseringer av kundens programvare.
Prosesser	For eksempel; dokumentasjon av interne driftsprosesser og konfigureringer, nye prosesser for å hindre skadelig effekt, skjema-dokumentasjon.
Båndbredde	For eksempel; bruk av båndbredde til Distributed Denial of Service (DDoS), sende søppelpost eller å infisere andre i en stor skala.
Finans	For eksempel; stjele kryptovaluta, stjele/kapre bank-konti, pengeoverføringer.
Mennesker	For eksempel; målrettet mot spesifikke individer på grunn av deres posisjon eller kompetanse.

Tabell 6. Kundeverdier (assets) som mål for leverandørkjedeangrep.

2.3 Om kompleksitet og usikkerhet[1]

IKT-systemer og -infrastrukturer inngår i stadig lengre og mer komplekse verdikjeder gjennom å være integratoren i så godt som alle samfunnsinfrastrukturer og -funksjoner. I tillegg er disse IKT-baserte funksjonene svært komplekse i seg selv. Kompleksitet er en form for sårbarhet det er vanskelig å beskytte seg mot. Det er derfor svært viktig at vi er i stand til å kommunisere usikkerhet som økt kompleksitet fører med seg, ved gjennomføring og bruk av risikobaserte vurderinger. Det er viktig at beslutningstakerne forstår den usikkerheten som følger av at for eksempel ingeniørene forstår at de ikke har full oversikt over deler av et IKT-system, som inngår i en sentral funksjon i et militært kommando- og kontrollsystem eller i en styringsfunksjon i kraftforsyningen. At usikkerhet[2] kan vurderes og kommuniseres på tvers av kompetanseområder i denne typen sammenhenger er svært viktig for beslutningstakernes evne til å ta gode avgjørelser i tid og rom. De vurderinger som gjøres med hensyn til usikkerhet må også være sporbare og etterprøvbare til enhver tid.

2.3.1 Perspektiver på kompleksitet

Under beskriver vi noen perspektiver som vi mener er viktige når vi skal vurdere og beskrive ulike faktorer knyttet til kompleksiteten i et system eller en infrastruktur. Faktorene er ikke ortogonale, så noen sårbarheter som skyldes kompleksitet vil kunne høre inn under flere av perspektivene. Vi synes likevel det er hensiktsmessig å detaljere litt mer hva vi legger i begrepet kompleksitet. Valget av perspektiver er inspirert av arbeider gjort av Nancy Leveson (2011) og Charles Perrow (1984), i tillegg til erfaring fra risikobaserte analyser og vurderinger FFI selv har gjennomført innen blant annet Forsvaret, jernbanen, kraftforsyningen og vannforsyning.

1. Samspillskompleksitet – systemsammenhenger og -relasjoner (rom)

[1] Dette delkapitlet er i hovedsak skrevet av Kjell Olav Nystuen, FFI, basert på tidligere arbeider FFI har gjort og hans foredrag i faget «Infrastruktur og sårbarhet» ved UiS.

[2] Usikkerhet kan defineres som noe som kan betviles og diskuteres (Njå, Sommer, Rake & Braut, 2020), og har et ulikt innhold om vi betrakter fortiden, nåtiden eller fremtiden. Usikkerhet om fremtiden er koplet til risiko og er ofte en del av beslutningsgrunnlaget for eksempel i investeringer av delsystemer til kraftforsyningen. Vi viser til Njå, Sommer, Rake & Braut (2020) for en grundigere presentasjon av usikkerhet.

2. Koplingskompleksitet – integrasjonskompleksitet fysisk digitalt (tid)
3. Organisatorisk kompleksitet – eiere, operatører, outsourcing, kompetanse med mer (rom)
4. Verdikompleksitet (verdikjeder i tid og rom)
5. Dynamisk kompleksitet – endringsintensitet teknologi og strukturer (tid)

Samspillkompleksitet:
Samspillkompleksitet sier noe om hvordan avhengighetene er mellom og innad i de tekniske systemene. Med samspill (interactions) mener vi:

- Interne avhengigheter som kan betraktes som et sett med aktiviteter mellom elementer eller funksjoner i et system eller en infrastruktur. Et eksempel på dette kan være at en svitsj er avhengig av en kontroller for å rute trafikk i et datasenter.
- Eksterne avhengigheter til andre (komplekse) infrastrukturer, der man er avhengig av ressurser eller tjenester fra disse andre infrastrukturene. Dette kan typisk være ekom, skytjenester, kraft og tidstjenester. En feil i disse grunnleggende tjenestene kan gjør at mange ulike infrastrukturer kan svikte samtidig.
- Eksterne avhengigheter mellom systemer og infrastrukturer fordi de trenger data fra hverandre. For eksempel vil det kunne være en avhengighet mellom en infrastruktur som skal styre varmekabler i gater og meteorologisk institutt sin sensorinfrastruktur, fordi førstnevnte vil ha god nytte av værdata.
- Eksterne avhengigheter mellom infrastrukturer fordi de bruker samme maskinvare og/eller programvare. En sårbarhet som utnyttes her kan fort ramme mange ulike infrastrukturer.

Bruk av skytjenester vil kunne føre til at samspillkompleksiteten øker. Det er mange interne avhengigheter mellom elementene i et datasenter. Datasentrene er også avhengig av kraftinfrastrukturer, og bruk av skytjenester fører som regel til en økt avhengighet av ekom. Deler av skyinfrastrukturen driftes og vedlikeholdes ofte fra utlandet.

Det at ulike systemer og infrastrukturer bruker samme datasenter kan medføre at en tilsiktet eller utilsiktet hendelse som rammer skyinfrastrukturen kan gi en eller flere feil i andre systemer og/eller infrastrukturer. Disse kan gjerne være vanskelig å forutse, og i noen tilfeller vil konsekvensene kunne eskalere.

Koblingskompleksitet:
Koblingskompleksitet sier noe om i hvilken grad koblingene mellom tekniske systemer og organisatoriske elementer er tidskritiske. Sammenkoblinger/tilbakekoblinger mellom elementer og funksjoner i systemer og infrastrukturene kan være tette eller løse. Ved tette koblinger vil en handling ett sted ha umiddelbare og gitte effekter et annet sted. Dette kan være fordi det er bestemt hvordan handlingen skal håndteres på forhånd, eller fordi det ikke er rom for fleksibilitet når handlingen skal håndteres. Tette koblinger tolererer ikke forsinkelser og tillater ikke slakk. Dette er i motsetning til løse koblinger som responderer saktere. Løse koblinger er dermed mer robuste med tanke på feilhåndtering, og vil fremstå som en slags buffer. Tette koblinger vil bidra til høy kompleksitet, mens løse koblinger vil bidra til det motsatte.

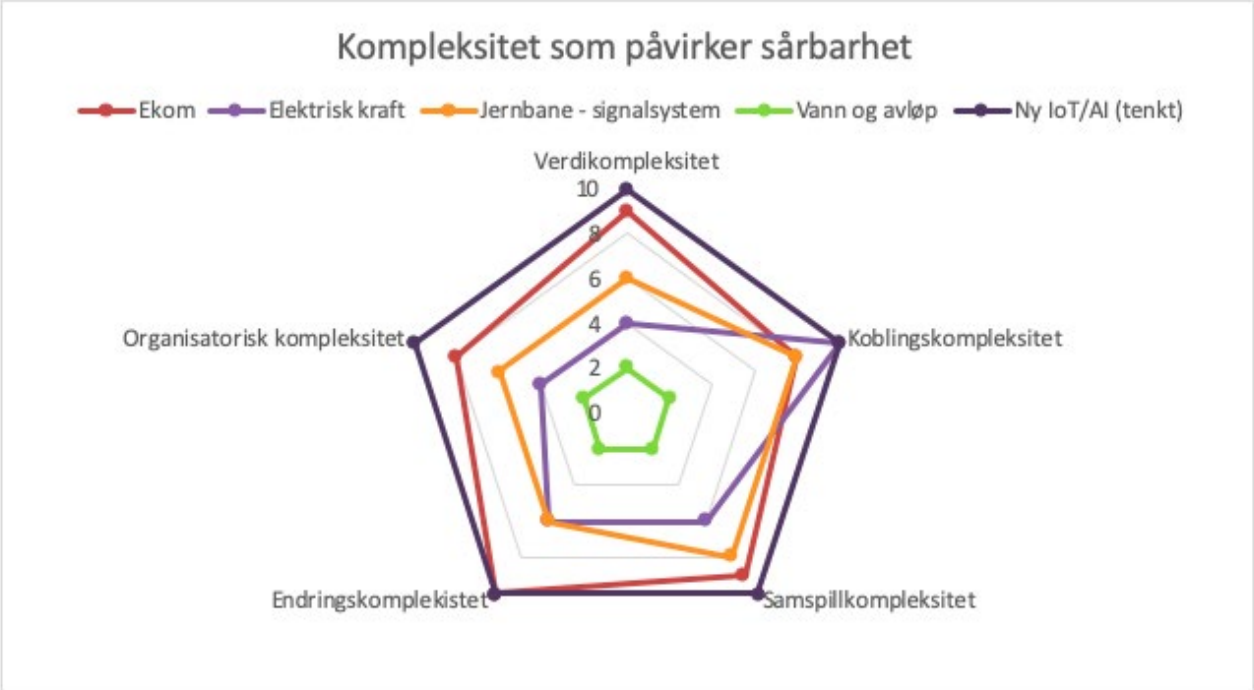
Det er ikke ventet at koblingskompleksiteten vil endres i noen særlig grad ved å benytte strategisk partnerskap i seg selv, men økt digitalisering vil kunne gi tettere koblinger og høyere koblingskompleksitet.

Organisatorisk kompleksitet:
Organisatorisk kompleksitet sier noe om hvordan avhengighetene er mellom de involverte organisasjonene, og mellom de involverte organisasjonene og de tekniske systemene. Det kan være mange involverte aktører for å levere en tjeneste. Det kan være private virksomheter, offentlige instanser og utenlandske virksomheter, og ofte en kombinasjon av disse. Det er i dag mange eksempler på at virksomheter splittes opp og/eller at deler av virksomheten tjenesteutsettes. Dette kan for eksempel utnyttes av en trusselaktør som ønsker å komme seg inn i en verdikjede. Organisatorisk kompleksitet kan blant annet gjøre det vanskelig å ha oversikt over hvor data havner og gi uklare ansvarsforhold. Jo flere aktører som er involvert jo større vil den organisatoriske kompleksiteten bli.

Verdikompleksitet:
Verdikompleksitet sier noe om hvordan et teknisk system eller infrastruktur eller et organisatorisk element bidrar oppover i verdikjeden. Verdi kan for eksempel være velvære for individer eller stor produksjonskapasitet for en produksjonsbedrift. Hvis man har god oversikt over hvilke verdier infrastrukturen bidrar til, vil verdikompleksiteten være lav. Har man derimot liten oversikt over dette, fordi infrastrukturen for eksempel blir brukt av mange, både indirekte og direkte, vil verdikompleksiteten være høy.

Et eksempel fra forsvarssektoren. For strategisk partnerskap mellom forsvarssektoren og private aktører vil verdikompleksiteten øke. Som tidligere nevnt vil det ligge andre verdier i en skyinfrastruktur enn Forsvarets. Dette kan gjøre at Forsvaret kan bli rammet selv om ikke målet med et angrep var å ramme Forsvaret. Det samme gjelder for private aktører som kan bli utilsiktet offer for nasjonalstatens handlinger. En (sky)tjeneste kan også fort bli brukt til mer enn først tenkt. Dette kan føre til at tjenester har større verdi enn man er klar over. En annen form for verdikompleksitet kan også oppstå fordi det forsvarssektoren ønsker å beskytte og regner som verdi ikke samsvarer med det leverandøren regner som verdi. For eksempel vil private aktører gjerne ha økonomiske motiver når de vurderer sine verdier. Vi kan tenke oss lignende partnerskap i kraftforsyningen mellom leverandører og virksomheter i sektoren.

Dynamisk kompleksitet:
Dynamisk kompleksitet sier noe om hvordan tekniske systemer, organisatoriske elementer og koblinger endrer seg over tid. Disse endringene kan være knyttet til alt fra hvor ofte det skjer programvareoppdateringer, hvor ofte den fysiske infrastrukturen endres, hvor ofte det skjer endringer i hva infrastrukturen brukes til, til hvor ofte det skjer organisatoriske endringer, eksempelvis gjennom oppkjøp. Ved bruk av for eksempel kommersiell skyinfrastruktur som del av en IKT-basert funksjon vil forekomsten av slike endringer øke.



Figur 1. Kompleksitet i infrastrukturer (Nystuen, 2021).

2.3.2 Sammenligning av kompleksitet i samfunnsinfrastrukturer

Kompleksitet er forsøksvis illustrert gjennom spindelvevdiagrammet vist over. Hver akse representerer hver av kompleksitetsfaktorene. Til grunn for denne konkrete vurderingen for hver av infrastrukturene ligger en forståelse av hvordan sårbarheter i form av kompleksitet og usikkerhet i integrerte IKT-baserte funksjoner vil kunne påvirke funksjonen i infrastrukturene. Nivåene er her å se som relative sammenlignet med en tenkt IoT-basert infrastruktur. Disse kunne også vært absolutte størrelser basert på en eller annen form for norm som beskriver topp og bunn.

Til grunn for en tenkt IoT basert samfunnsinfrastruktur finnes en høy forekomst av moderne IoT, skytjenester, AI-baserte funksjoner og moderne kommunikasjonstjenester som for eksempel 5G.

For ekom-infrastrukturen ligger det til grunn en 5G-type infrastruktur, som er en svært avansert infrastruktur som bygger på avanserte teknologier og strukturer. Her inngår også mange aktører og kunnskap i strukturer det vil være vanskelig å ha oversikt over.

Jernbanen kommer også relativt sett høyt opp på grunn av innføringen av det nye ERMTS-baserte signalsystemet. Dette gir en høyeffektiv fremføring av tog, men sterk integrasjon av avanserte IKT-baserte funksjoner gir også høy kompleksitet.

Kraftforsyning kommer noe lavere fordi vi i hvert fall så langt vurderer bruken av IKT-baserte funksjoner som noe mer forsiktig enn i de andre tilfellene. Koblingskompleksiteten er svært høy både relativt og absolutt. Det å øke de andre kompleksitetsfaktorene vil totalt sett kunne øke usikkerheten over hva som er akseptabelt for en så kritisk infrastruktur. Utviklingen i kraftforsyningen viser at bransjen nå er i ferd med å innføre nye former for IKT-baserte funksjoner. Til grunn for dette ligger behov for stadig mer effektiv utnyttelse av infrastrukturen, som følge av økt behov for fornybar energi

og det grønne skifte. Dette gjør kraftforsyningen til en infrastruktur mer eksponert for risiko, kompleksitet og usikkerhet, som krever behov for analyse og bedre styring.

Vannforsyningsinfrastruktur kommer derimot lavt ut når det gjelder kompleksitet i denne sammenstillingen, som følge av lav avhengighet av integrerte IKT-baserte funksjoner. Årsaken til dette er at vannforsyningen i hovedsak er basert på gravitasjonskraft for å fremføre vannet, gjennom dammer, høydebasseng og rørsystemer på veien fra reservoar til forbruker. Selv om IKT-baserte funksjoner er viktige i vannbehandling, alarmsystemer osv., er de i mindre grad kritisk for instantan leveranseevne (dekke behovet i virkelig tid), som er grunnlaget for denne klassifiseringen.

Det er imidlertid viktig å understreke at bruken av denne fremgangsmåten for å vurdere kompleksitet og usikkerhet, gjøres for å illustrere en sammenligning av noen viktige samfunnsinfrastrukturer. Vurderingene er ikke absolutte og må brukes med forsiktighet. Ved fullstendig bruk at en slik fremgangsmåte er det også viktig at argumentasjonen for hver enkelt vurdering blir gjort på en strukturert og metodisk måte for at dette skal ha relevans for en gitt beslutningstager.

3 Leverandørkjedemodeller

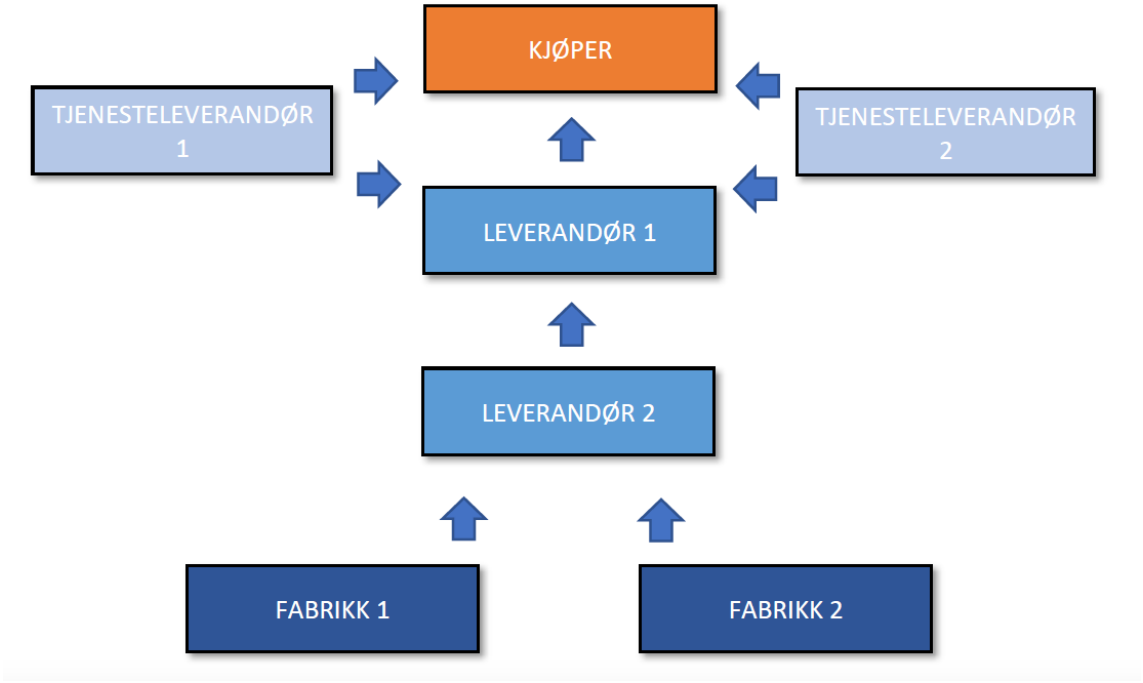
Etikkinformasjonsutvalget definerer leverandørkjeden som; «… alle vare- og tjenesteytende virksomheter som leverer innsatsfaktorer til en virksomhet, og har en direkte tilknytning til selskapets forretningsvirksomhet, produkter eller tjenester. Leverandørkjeden omfatter de aktiviteter, organisasjoner, aktører, teknologier, informasjon, ressurser og tjenester som er involvert i prosessen med å flytte og bearbeide et produkt fra råvarestadiet til et ferdig produkt. I dette inngår transport, agenter og andre mellomledd». Dette er en generell definisjon som går på tvers av alle sektorer. Vi tolker det slik at leverandørkjeden er en kritisk forutsetning for virksomhetene i den norske kraftforsyningen, og at dette avhengighetsforholdet må analyseres nærmere.

ENISA beskriver en leverandørkjede på følgende måte: «Leverandørkjeder er økosystemet av prosesser, mennesker, organisasjoner og distributører som er involvert i å skape og levere en endelig løsning eller produkt». Når det kommer til cybersikkerhet omhandler dette ressurser som hardware (maskinvare) og software (programvare), lagring både lokalt og på skytjenester, distribusjonsmekanismer som webapplikasjoner, og administrasjonsprogramvare (ENISA, 2021). Informanter har trukket frem ulike utfordringer og sårbarheter knyttet til leverandører og leverandørkjeder, som de mener kan utgjøre en fare for cybersikkerheten. Spesielt kompleksiteten i leverandørkjedene er trukket frem. Kompleksiteten påvirker muligheten for å holde oversikt og kontroll. Leverandørkjedene får stadig større bredde, og kapasitetsmessig blir det nesten umulig å ettergå alle ledd eller alle underleverandører, og de fleste har ikke mulighet til å gjennomføre revisjon på egenhånd. Dette medfører ifølge informanter en usikkerhet som må møtes med å ta innover seg det risikobildet bransjen faktisk står overfor, og å ta bevisste valg når det gjøres avtaler med leverandører eller kjøpes tjenester og produkter.

Under presenteres to ulike modeller som illustrerer 1) en leverandørkjede med sterk hovedleverandør, og 2) et distribuert leverandørnettverk. Modellene er basert på data fra intervjuer, og har kommet frem ved diskusjoner med leverandører og representanter for virksomheter som bestiller IKT-systemer. De er ikke helthetlige fremstillinger av faktiske leverandørkjeder, men eksempler på hvordan de kan se ut. Modellene brukes i kap. 5 for å vise hvor sårbarheter og trusler kan ramme ulike deler av leverandørkjeden og forplante seg videre til andre deler av systemet.

3.1 Sterk hovedleverandør av komponenter

I kraftsektoren finner vi noen sterke hovedleverandører av komponenter. OT-systemene er blitt mer digitaliserte og dermed mer avhengige av IKT-systemer enn tidligere. I denne modellen betrakter vi en kjøper i den norske kraftbransjen, en kraftprodusent, som har behov for å kjøpe komponenter til sitt kontrollanlegg. Virksomheten kjøper i denne modellen komponenter fra en sterk hovedleverandør. I dette tilfellet er leverandørkjeden, inkludert fabrikkene, eid av hovedleverandøren. Komponentene de leverer kan eksempelvis være datamaskiner eller annen hardware til bruk i kontrollfunksjoner og vern, som kontroller strømspenningen i anlegg og kontrollerer brytere som kan koble ut systemet hvis det oppstår feil eller for høy spenning. I tillegg må kjøper gå til anskaffelse av IKT-systemer som støtter opp om komponentene, for eksempel IKT-systemer for fjernstyring, drift og overvåking (SCADA). Disse kjøpes fra tjenesteleverandører som ikke er eid av hovedleverandøren.



Figur 2. Modell av sterk hovedleverandør av komponenter

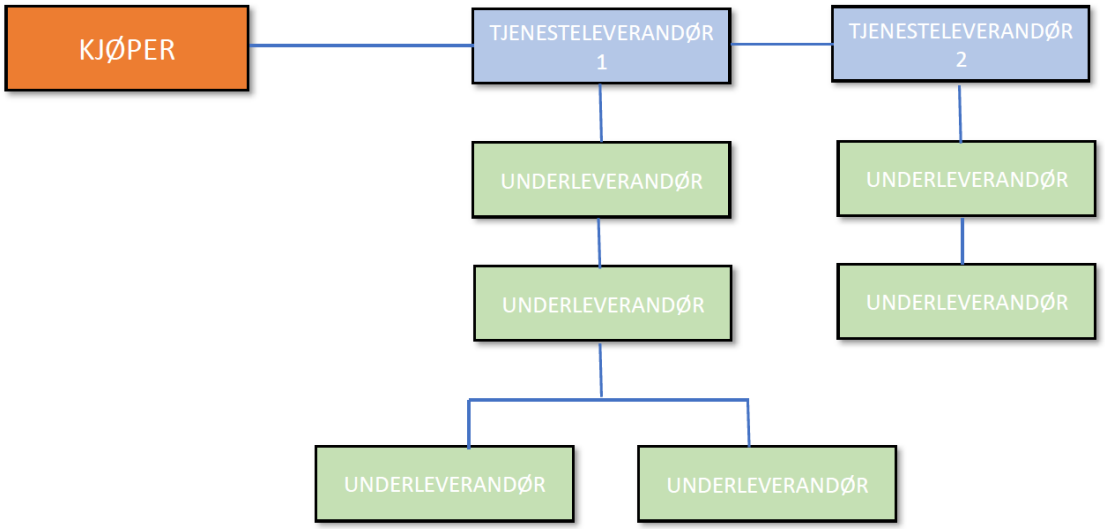
I dette eksempelet ser vi for oss at hovedleverandøren er leverandør 1. Leverandør 1 eier også leverandør 2, som er en underleverandør, men likevel tilhører samme selskap. Her er leverandør 1 selger av komponenter, og kan også være en totalleverandør av kontrollanlegg. Leverandør 2 monterer og setter sammen komponentene. Fabrikkene som produserer komponentene befinner seg i Europa, men det kan også være kopifabrikker i andre deler av verden, eksempelvis i Asia. Her produseres komponenter i sikret miljø.

Komponentene transporteres fra fabrikk til mottaker. Mottaker er ofte en montør (leverandør 2) som setter komponentene sammen før det transporteres videre til kunde. Her installeres og settes komponentene i drift av leverandør 1. Rollen til leverandør 1 i kraftforsyningen er å designe og sette opp anlegg, eksempelvis kontrollanlegg, og leverandør 1 har ansvar for at det skal fungere som tiltenkt. Leverandør 1 veileder kunden i å sette opp kontrollanleggene i henhold til kraftberedskapsforskriften (KBF). KBF handlet tidligere kun om det operasjonelle, men inkluderer nå mer IKT og datasikkerhet. Det krever at kunden tar et større ansvar for rett bruk av systemene, og at sikkerheten ikke kan ivaretas av leverandør alene. Ved totalleveranser av anlegg har leverandør større ansvar for sikkerheten enn hvis leverandøren kun leverer delkomponenter. Ved totalleveranser kan leverandøren også bidra med IKT-sikkerhetsløsninger. Det krever et samarbeid og et delt ansvar for å opprettholde sikker drift i totalsystemet. Ved mindre leveranser er det kjøpers ansvar å sette nye komponenter inn i det eksisterende systemet, og leverandør har ikke kontroll over hvordan dette gjøres, og heller ikke ansvaret for sikkerheten i systemet som helhet. I disse tilfellene har leverandøren kun ansvar for leveransen, og ikke oppfølging av riktig bruk. Leverandørens ansvar er å respondere på bestillers innkjøpsordre, og er avhengig av at kunden stiller sikkerhetskrav i bestillingen. Innkjøpere vi har snakket med forholder seg til virksomhetens retningslinjer for anskaffelser, og ved innkjøp av produkter som er nødvendig for drift av strømnett eller produksjon, brukes en tilleggsveileder for anskaffelser til kritisk infrastruktur. Veilederen beskriver hvilke krav som må stilles til leverandør, blant annet spesifikasjoner for IT-systemet og sikkerhetsavtaler, og en fremtidsavtale som sier noe om leverandørens rolle og ansvar i tiden etter kjøpet. Regelverket stiller også krav om at det skal være maksimalt to ledd med underleverandører, og at komponenter ikke kan produseres i land som av NSM, PST eller etterretningstjenesten er vurdert til å kunne påføre norske

interesser skade. Leverandør 1, som er brukt som utgangspunkt for denne modellen, oppgir at de ikke samarbeider med land som er forbundet med risiko, og at de har mulighet til å dokumentere leverandørkjeden fra start til slutt.

3.2 Distribuert leverandørnettverk

Modellen i figur 3 viser et distribuert leverandørnettverk av tjenesteleverandører, hvor hovedleverandørene med tilhørende underleverandører er representert. I denne modellen er det i motsetning til figur 2 ingen sterk hovedleverandør, men mange ulike leverandører. Disse leverandørene med hver sine tjenester danner en leverandørkjede som bidrar til det helhetlige systemet som kjøper trenger. I en distribuert modell vil kjøper og tjenesteleverandør 1 ha mindre kontroll og styring over sine underleverandører, og må i større grad ha tillit til at underleverandørene lenger ned i kjeden har oversikt. Avtaler gjøres mellom kjøper (kunde) og tjenesteleverandør 2, og sikkerhetskravene stilles også direkte til disse, men ikke til deres underleverandører. Kjøperen i denne modellen, nettselskap, kjøper i hovedsak programvare eller IKT-systemer, men også noen komponenter. Et eksempel på programvare kan være systemer for å holde oversikt og kontroll over AMS (avanserte måle- og styringssystemer) som måler strømforbruket i den enkelte husstand og sender målerverdiene videre til Elhub.



Figur 3. Modell av distribuert leverandørnettverk av IT-tjenester.

I denne modellen har vi tatt utgangspunkt i at tjenesteleverandør 1 og tjenesteleverandør 2 er hovedleverandører, og underleverandørene leverer utstyr som settes sammen av tjenesteleverandør 2. Tjenesteleverandør 1 er i dette eksempelet et mellomledd, som har som rolle å sørge for et felles driftsselskap og felles programvare for nettselskapene i forbindelse med bruk av AMS. Tjenesteleverandørene og underleverandørene i denne modellen er spredd over større geografiske områder enn modell 1, og holder til i flere land både i Europa og Asia. Ved å bruke tjenesteleverandør 1 som forvalter av en felles infrastruktur, vil nettselskapene ha færre underleverandører å forholde seg til.

Forvalteren (tjenesteleverandør 1) sørger også for å innhente nødvendig informasjon fra leverandør og underleverandører, og bidrar med å opprette kontakt mellom nettselskap og leverandør ved behov. På denne måten er det også nyttig for underleverandørene, som får tilbakemeldinger og forslag til forbedringer, noe som ifølge informanter bidrar til å opprettholde sikkerheten gjennom hele

leverandørkjeden. Det er likevel til slutt kjøperen (nettselskapet) som har ansvaret for sikkerheten, og for å bruke IKT-tjeneste på rett måte. Tjenesteleverandør 1 har ikke relasjon til andre enn virksomhetene som er deres kunder og eiere, men prioriterer å bidra til et godt samarbeid, og er nettselskapenes representant i kommunikasjon med underleverandører. Samlet sett har de større kapasitet og flere ressurser til å følge opp dette arbeidet, enn de enkelte nettselskapene har hver for seg, spesielt de som er av mindre størrelse.

4 Faktorer med betydning for IKT-sikkerhet

I dette kapitlet innfører vi begrepet faktorer med betydning for IKT-sikkerhet. Med faktorer mener vi viktige karakteristikker ved leverandørkjedesårbarheten, men uten at vi eksplisitt kan knytte konkrete sårbarheter til begrepet. Det handler om underliggende forhold som bidrar til organisering, utvikling, regulering og realisering av leverandørkjedene til norsk kraftforsyning.

4.1 Økonomisk globalisering

Økonomisk globalisering defineres som funksjonell integrasjon av økonomisk aktivitet på tvers av landegrenser (Sæther, 2017). Funksjonell integrasjon innebærer ulike former for avhengighet mellom aktører, og dette ser vi mellom kjøper og leverandør i modellene vi presenterer i kapittel 3, samt mellom leverandører og underleverandører. I tillegg kan veksten i økonomisk globalisering sees i lys av flere sentrale geopolitiske endringer. For eksempel har Kina åpnet sin økonomi for utenlandske direkteinvesteringer og ønsket vestlig kapital og industri velkommen. Flernasjonale selskaper har mulighet til å flytte eiendeler på tvers av landegrenser. Informasjons- og kommunikasjonsteknologi har bidratt til økonomisk globalisering. Raskere og større informasjonsstrømmer har gitt økte muligheter for koordinering av økonomisk aktivitet og økt mulighet til kontroll og oppfølging av resultater (Sæther, 2017).

Økonomisk globalisering er en viktig premiss for å opprettholde internasjonale verdikjeder, og en viktig grunn til at leverandørkjedene har utviklet seg til det de er i dag. Handelsmønstre handler om hvem som selger hva og til hvem. Dette er bestemt av forskjeller i produktivitet, forskjeller i faktortilgang, stordriftsfordeler og utvalg av mer produktive bedrifter. Et etablert mønster er at mye av teknologien som produseres og brukes i store deler av verden er produsert i Asia, i hovedsak i Kina, men også i andre verdensdeler. Industriutviklingen i Kina skjer i høyteknologiske bransjer og i 2014 representerte dette nær halvparten av Kinas eksport. Eksporten av IKT-produkter passerte USA allerede i 2004 (Mjøset & Skarstein, 2016). Teknologiske endringer har gjort det mulig å splitte opp produksjonsprosessen og legge ulike deler av prosessen der det er mest kostnadseffektivt. Produksjon i vesten har derfor i stor grad blitt utkonkurrert, da mange varer og tjenester kan fabrikkeres billigere andre steder (Knutsen & Haugen, 2017).

Modulære verdikjeder produserer varer etter ønske fra forbrukerne, og på denne måten forholder virksomhetene seg til færre leverandører og har tettere relasjoner til disse (Naume, 2015). Modulære verdikjeder er kjent i elektronikkindustrien, hvor sluttproduktet er satt sammen av standardiserte komponenter fremstilt etter kjøpers spesifikasjoner. I dette tilfellet har leverandører ansvaret for teknologien og produksjonsutstyret, og bærer dermed risikoen hvis noe går galt i produksjonen (Knutsen & Haugen, 2017). Dette virker også å være tilfellet i kraftbransjen, hvor mange selskaper benytter seg av få leverandører, som de har god relasjon og tillit til. Informanter i studien peker dog på at leverandører krever at kjøpere av produkter har et ansvar for at disse brukes riktig. Når det kommer til produkter som krever IT-støtte vil dette for eksempel si at kjøpere har ansvar for å oppdatere programvare på produktene.

Mange leverandører er store multinasjonale selskaper, mens mange selskaper i den norske kraftsektoren er små. Dette kan gjøre det vanskelig å få gjennomslag for sikkerhetskrav og å gjennomføre sikkerhetsrevisjoner. En utfordring er også at flere selskaper i kraftforsyningen benytter seg av samme leverandør av IKT-systemer, som betyr at et angrep mot en leverandør eller et system

vil kunne påvirke flere selskaper. Dersom hendelser rammer flere selskaper samtidig er det også en risiko for at leverandørene ikke har dimensjonert beredskap for dette.

4.2 Digital sårbarhet, risiko og trusler i globale verdikjeder

Cyberangrep mot leverandørkjeder har økt i omfang og angrepene har blitt mer sofistikerte. Alle virksomheter som har sine systemer koblet til internett må dermed forholde seg til disse truslene. Norge står overfor et komplekst risikobilde hvor fremmede stater og andre aktører forsøker å utnytte sårbarheter i funksjoner, virksomheter og systemer (NSM, 2021). Motivene for cyberangrep kan være å påvise sårbarheter, utøve makt og politisk press, eller økonomisk gevinst. Cyberangrep kan være tilfeldige, ved at aktørene sender ut et virus til mange ulike organisasjoner og slår til der de lykkes med å få tilgang, eller de kan være rettet mot spesifikke mottakere (NOU 2015:13, 2015).

De viktigste utviklingstrekkene er ifølge NSM at det digitale risikobildet er skjerpet, det er tydeligere risiko knyttet til sammensatte trusler, og Covid-19-pandemien har forsterket det eksisterende risikobildet. NSM viser til at de nye sårbarhetene og avhengighetene som trusselaktører kan utnytte, kommer av rask digitalisering og lange digitale verdikjeder som understøtter funksjoner i samfunnet. I tillegg til et skjerpet digitalt risikobilde, kan strategiske investeringer fra land Norge ikke har sikkerhetssamarbeid med, få negative konsekvenser for nasjonale sikkerhetsinteresser. Strategiske investeringer fra utenlandske foretak brukes for å få innpass i prosesser og tilgang til sensitiv informasjon, teknologi og kompetanse. Dette kan gi legitim tilgang til informasjon og teknologi som videre kan bli benyttet for illegitime formål (NSM, 2021).

Aktørers kapasitet og kapabilitet til å gjennomføre nettverksoperasjoner med alvorlige konsekvenser for Norge vurderes å være høy. Nettverksoperasjoner består som regel av spionasje og innhenting av informasjon. Informasjonen kan utnyttes i nær fremtid, eller det kan være en del av en langsiktig operasjon hvor selve angrepet ikke iverksettes før etter mange år. Kraftsektoren er ifølge NSM risikoutsatt for slike nettverksoperasjoner.

Forfatterne av NOU 2015:13 mener at digitaliseringen i kraftforsyningen også fører til at det blir tettere koblinger mellom systemer og nettverk. Det gjør at systemene blir mer komplekse, og dermed blir det vanskeligere å ha full oversikt. Mangelen på oversikt kan også føre til mangel på kunnskap om samhandlingen mellom de ulike systemene, eller det kan føre til feil bruk, se for øvrig kap. 2.3 for ulike kompleksitetsdimensjoner.

4.3 Styring og regulering av cybersikkerhet

4.3.1 EUs tilnærming til IKT-sikkerhet

EØS-avtalen trådte i kraft i 1994 og er ryggraden i Norges forhold til den europeiske integrasjonsprosessen. Med EØS-avtalen er Norge tilsluttet EUs indre marked, hvilket innebærer en viss harmonisering med EUs regelverk, tekniske krav og produktspesifikasjoner (Claes & Førland, 2015).

Europakommisjonen påpeker at leverandørkjedesikkerhet er en utfordring når det kommer til cybersikkerhet. EUs cybersikkerhetsstrategi ser på tre verktøy (regulatoriske, investeringer og politiske initiativer) som er knyttet til tre pilarer:

1. Resiliens, teknologisk suverenitet og lederskap (herunder NIS 2 direktivet, som inneholder mer vekt på leverandørkjedesikkerhet).
2. 3Bygge operasjonell kapasitet for å forhindre, avskrekke og respondere (krisehåndteringsrammeverk, medlemslandenes cyberetterretning, cyberforsvarspolitiske rammer).
3. Samarbeid for å fremme et globalt og åpent cyberspace (EU-ledelse på standarder, normer og rammeverk i standardiseringsorganer, cyberkapasitetsbygging, dialog og diplomatisk nettverk).

EU representerer 26% av det globale cybersikkerhetsmarkedet, men opptil 30% av europeisk etterspørsel er møtt av selskaper med hovedkontor utenfor unionen. EUs arbeid med cybersikkerhet består blant annet av kompetansesenteret for cybersikkerhet som skal forvalte midlene som er planlagt for cybersikkerhet under «Digital Europe» og «Horizon Europe 2021-2027». Kompetansesenteret hjelper til med å koordinere cybersikkerhetsarbeidet, støtte felles investeringer fra EU, medlemsstatene og industrien, og støtte distribusjon av produkter og løsninger. Horizon Europe inkluderer hardware, software og leverandørkjedesikkerhet som finansieringsprioritet. Videre inkluderer Digital Europe sertifiseringsordninger som finansieringsprioritet, herunder å støtte små og mellomstore bedrifter med å sertifisere sine produkter (Ubelhör, 2021). I tillegg til dette prioriteres implementeringen av NIS-direktivet.

Videre finner vi nettverk av nasjonale koordineringssentre. Disse er utpekt av medlemsstatene som det nasjonale kontaktpunktet med mål om nasjonal kapasitetsbygging og kobling til eksisterende tiltak. Det finnes også kompetansenettverk, som er store, åpne grupper med cybersikkerhetsinteressenter fra både forskning, privat sektor, offentlig sektor, samt sivil og militær sektor. CyberSec4Europe er et EU-initiativ som ser på styring av et kompetansenettverk som inkluderer styringsdesign, forskning, innovasjon og industri, samt opplæring, trening og standardisering. I tillegg til dette kommer kommunikasjon og nettverksbygging. Norge bidrar til initiativet gjennom NTNU og SINTEF (CyberSec4Europe, 2021).

Den tredje energipakken (EU) etablerte et byrå for koordinering av reguleringsfunksjoner i gass- og elektrisitetsmarkedet; *The Agency for the Cooperation between Energy Regulators (ACER).* Byrået skal over tid sikre koordinering av felles regler for gass og elektrisitet (Claes & Førland, 2015). Sikker energiforsyning står høyt på EUs dagsorden. Et cyberangrep i et land kan forårsake strømbrudd eller skader på infrastruktur eller påvirke det digitaliserte systemet, og dermed få konsekvenser over større geografiske områder. ACERs rolle i cybersikkerhetsarbeidet er å gi råd med utgangspunkt i EU-regelverk, å dele informasjon med energiregulatorer, og kapasitetsbygging. Dette inkluderer beredskap, håndtering og oppbygging etter uønskede hendelser. I tillegg er ACERs cyberspesialister ledende globale nettsikkerhetseksperter som legger til rette for fremtidig standardiseringsarbeid som kan være nødvendig for effektiv gjennomføring av reguleringen (ACER, 2021).

Flere informanter i studien mener at å ha et felles regelverk for IKT-sikkerhet, og at alle som skal ha en rolle i kraftforsyningen må sertifiseres, er et godt rammeverk. Imidlertid vil det å være sertifisert ha store administrative kostnader for små organisasjoner, og kan derfor være vanskelig å gjennomføre. Dette viser at kraftbransjen ønsker å ha god IKT-sikkerhet, men at gjennomføringen kommer til kort i kost-nytte-vurderingen. Hvis forslaget til ACER får gjennomslag, og blir EØS relevant, vil reglene bli en del av norsk regelverk. ACERs retningslinjer for sektorspesifikke regler for cybersikkerhet ved grenseoverskridende elektrisitetsflyt ble publisert 22. juli 2021, og tar sikte på å sette klare og objektive prinsipper for utviklingen av en nettkode (ACER, 2021). Denne nettkoden inkluderer felles regler om minimumskrav, planlegging, overvåking, rapportering og krisehåndtering. En fare ved krav

om sertifisering kan være at fokuset på å bli sertifisert og å etterleve kravene kan blir større enn fokuset på å jobbe aktivt med sikkerhet (Hagen, 2018).

ACER har kartlagt cybersikkerhetsområder som skal vurderes, og hvilke enheter som skal være underlagt krav i de angitte cybersikkerhetsområdene. To av disse cybersikkerhetsområdene omfatter leverandører og lyder som følger; *"Forpliktelser knyttet til leverandørkjedesikkerhet» og "avansert leverandørkjedesikkerhet i form av produktverifisering".* Disse skal definere krav til leverandørkjedesikkerhet for å sikre at de som eier ressurser og/eller de som driver ressursene på vegne av eierne kan kontrollere hele leverandørkjeden. Dette må gjøres ved å sette opp klare innkjøpsmaler og anskaffelsesprotokoller i henhold til relevante innkjøpsregler (ACER, 2021).

NIS-direktivet er en del av EUs cybersikkerhetsregulering og EU-lovgivning om cybersikkerhet som beskytter informasjonsteknologi og datasystemer. Målet er å øke det generelle nivået av cybersikkerhet i EU. I desember 2020 ble det lagt frem et nytt forslag, NIS 2-direktivet, for å forbedre resiliens og IKT-hendelsesrespons. NIS 2 skal blant annet inkludere flere sektorer, erstatte nåværende identifiseringsprosesser, justere sikkerhetskrav, samt utvide risikostyring i leverandørkjeder.

Når det kommer til risikostyring har toppledelsen ansvar for avvik, viktige selskaper er pålagt sikkerhetstiltak og å varsle om hendelser. Leverandørkjedesikkerhet trekkes frem som et av de viktigste sikkerhetstiltakene. I nasjonale cybersikkerhetsstrategier er medlemsstater pålagt å vurdere cybersikkerhet i leverandørkjeder når det kommer til IKT-produkter og tjenester. Sektorer som dekkes av direktivet bør utføre risikoanalyser av leverandørkjedene for å identifisere kritiske IKT-tjenester, systemer, produkter og relevante trusler og sårbarheter (European Commission, 2020).

EU kommisjonen har identifisert fem kriterier som virksomheter i norsk kraftforsyning bør vurdere for å identifisere hvilke leverandørkjeder (system) det bør utføres risikoanalyse av:

- I hvilken grad viktige enheter bruker og stoler på spesifikke kritiske IKT-tjenester, systemer eller produkter.
- Relevansen av spesifikke kritiske IKT-tjenester, systemer eller produkter for å utføre kritiske eller sensitive funksjoner, inkludert behandling av personopplysninger.
- Tilgjengeligheten av alternative IKT-tjenester, systemer eller produkter.
- Motstandsdyktigheten (resiliensen) til leverandørkjeden for IKT-tjenester, systemer eller produkter mot uønskede/forstyrrende hendelser.
- Potensiell fremtidig betydning for enhetens aktiviteter ved nye IKT-tjenester, systemer eller produkter.

Vi kjenner igjen kompleksitetsdimensjonene i kap. 2.3. Videre skal medlemsland i EU vedta en rekke retningslinjer som del av den nasjonale cybersikkerhetsstrategien. Retningslinjen om å vedta en policy er sentral. Dette inkluderer cybersikkerhet i leverandørkjeden for IKT-produkter og tjenester. Risikostyring skal sikre et sikkerhetsnivå for IKT-nettverk og informasjonssystemer. Artikkel 19 i direktivet handler om en EU-koordinert risikovurdering av kritiske leverandørkjeder av spesifikke kritiske IKT-tjenester, systemer eller produkter. Europakommisjonen skal identifisere de spesifikke kritiske IKT-tjenestene, systemene eller produktene som kan være gjenstand for den koordinerte risikovurderingen.

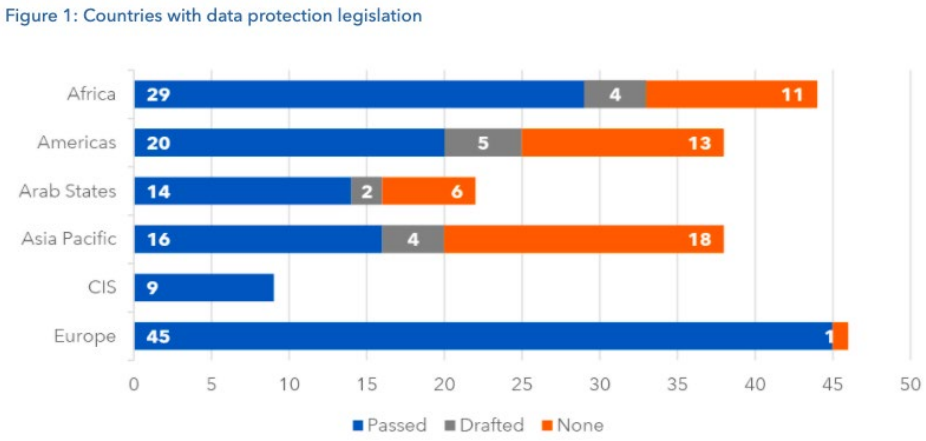
4.3.2 Internasjonal tilnærming til IKT-sikkerhet utenfor Europa

USA og Kina er viktige handelspartnere og leverandører av digital teknologi, og International Telecommunication Union (ITU)s kartlegging av cybersikkerhetstilstanden i landene er dermed et nyttig hjelpemiddel. Gjennom teknologi-anskaffelser blir virksomheter avhengig av leverandører, og ifølge NSM medfører dette en produktrisiko fra land som Norge ikke har et sikkerhetssamarbeid med, som for eksempel Kina.

Global Cybersecurity Index (GCI) er et initiativ fra ITU, som er FNs spesialbyrå for IKT. GCI måler de 193 ITU-medlemsstatenes og Palestinas forpliktelse til cybersikkerhet. Målet er å hjelpe landene med å identifisere forbedringsområder og oppmuntre dem til å iverksette tiltak gjennom å øke bevisstheten om cybersikkerhet over hele verden. GCI måler juridiske tiltak, tekniske tiltak, organisatoriske tiltak, og kapasitetsutviklings- og samarbeidstiltak for å få et bedre bilde på cybersikkerhetstiltak. Kapasitetsutviklingstiltak omfatter bevisstgjøring rundt statlig støtte til små og mellomstore bedrifter, ettersom de spiller en betydelig rolle i digital økonomi og i leverandørkjeder i en periode med et skifte mot e-handel.

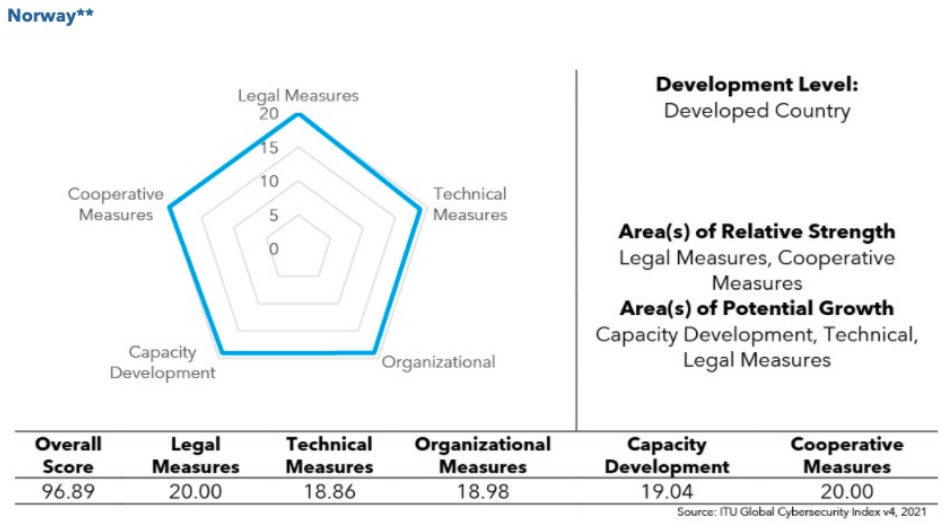
ITU mener at et viktig aspekt i utviklingen av nasjonale cybersikkerhetsstrategier er klare mål om beskyttelse av kritisk infrastruktur. En nasjonal cybersikkerhetsstrategi bør rette oppmerksomhet mot risikostyringen som skal redusere sannsynligheten for eskalering av en hendelse med store konsekvenser. Strategien sier ikke noe om krav til datagrunnlag og datakvalitet som risikostyringen skal baseres på (ITU, 2020). Målemetodene som brukes i GCI er grove, og dersom landene ikke sender informasjon til ITU, gjennomfører ITU selv datainnsamlingen og analysen.

Diagrammet under viser at 133 land har personvernlovgivning. Lovverket skal tilpasses risikobildet, og må dermed oppdateres jevnlig. Lovverket i andre land kan påvirke leverandørkjeder ved at underleverandører må opptre i samsvar med kravene nasjonalt, og disse nasjonale kravene samsvarer nødvendigvis ikke med norske krav. Dette er noe som må vurderes ved anskaffelser og tjenesteutsetting til utlandet, spesielt om landet ikke har personvernlovgivning i det hele tatt.



Figur 4. Land med personvernlovgivning (ITU, 2020).

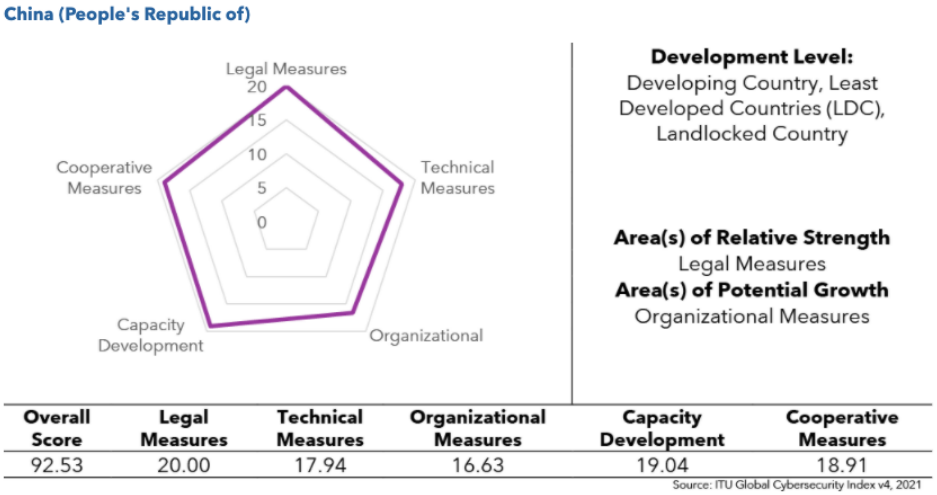
Som vi ser i figur 5 under scorer Norge høyt på de ulike tiltakene. ITU mener at tekniske tiltak er et område Norge kan bli bedre på, som for eksempel å opprette Computer Emergency Response Teams (CERTs). Dette finnes allerede i kraftsektoren i Norge med KraftCERT som jobber for god og effektiv hendelseshåndtering og informasjonsdeling mellom relevante selskaper.



Figur 5. GCI resultater Norge (ITU, 2020)

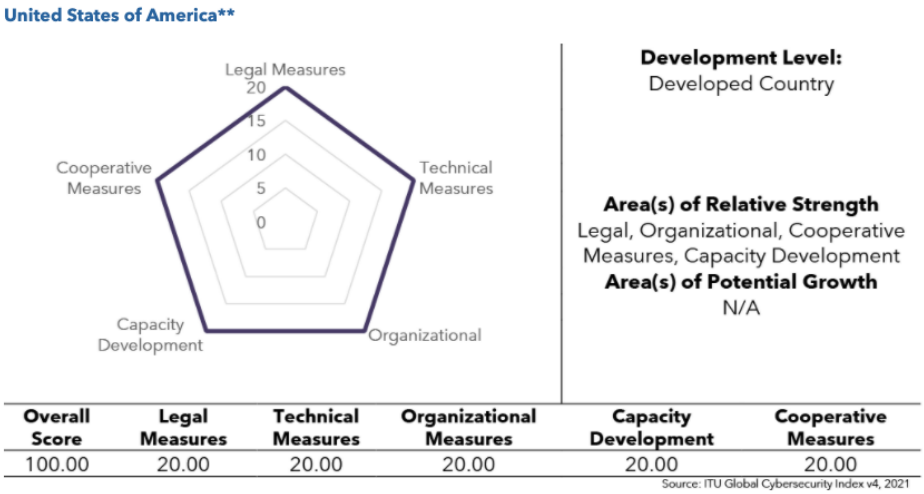
Norge er rangert som nummer 17. Norge har ikke levert informasjon som ITU har etterspurt (ITU, 2020).

Kina har i det siste hatt en økt satsning på sikkerhet, noe som kommer frem gjennom ITUs GCI-vurdering. Kina scorer 92.53 og er rangert som nummer 33. Dette viser at Kina har reguleringer, men etterlevelsen av disse blir ikke målt.



Figur 6. GCI resultater Kina (ITU 2020)

Også USAs resultater på GCI reflekterer deres satsing på cybersikkerhet. USA scorer 100 og ligger helt øverst. Modellen under viser at USA får full score på alle tiltakene.



Figur 7. GCI resultater USA (ITU, 2020).

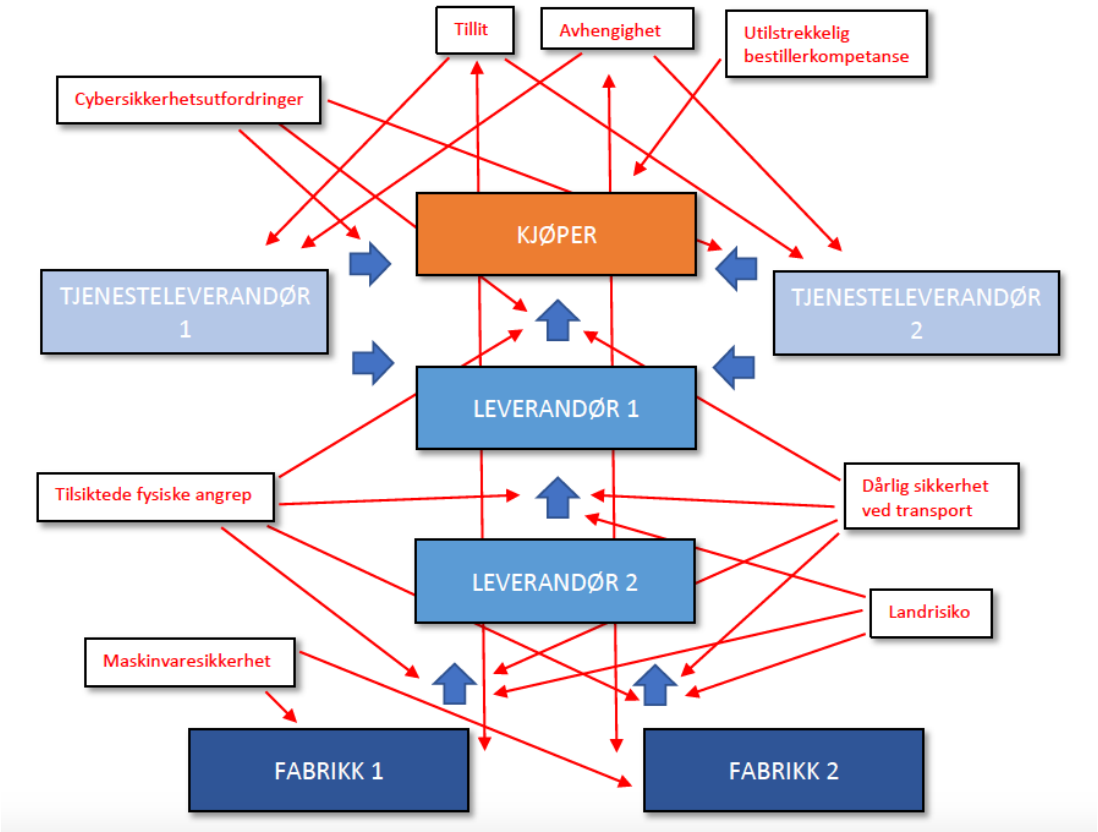
I mars 2021 publiserte amerikanske EPRI (Electric Power Research Institute) en artikkel om fremtidens kraftsystem og hvorfor vi trenger en ny visjon for cybersikkerhet. EPRI peker på at andre sektorer blir mer avhengige av elektrisitet, dette gjelder for eksempel transport. For å muliggjøre det fremtidige systemet som i større grad avhenger av elektrisk kraft, må kraftsektoren revidere cybersikkerhet knyttet til OT og beskytte seg mot angrep som kan ødelegge infrastrukturen. Hendelser, som for eksempel SolarWinds, viser at sikkerhetstilnærmingen til cybersikkerhet ikke er god nok. Videre peker EPRI på at skiftet til fornybar energi skaper flere sårbarheter i energiforsyningen.

Vi ser at IKT-teknologi har blitt integrert i OT-systemer, noe som krever mer kompetanse i blant annet systemforståelse og forståelse av avhengigheter mellom ulike fagmiljøer. Ikke minst krever det trening for personer som opererer systemene eller kjøper systemene. Cybersikkerhet er en utfordring her fordi det benyttes skytjenester for å håndtere data mellom disse systemene. Endringene som følger av økt digitalisering påvirker ikke bare teknologi, men også prosesser og menneskelig kompetanse. Derfor må prosjektplaner identifisere hvilke utfordringer menneskelige ressurser møter, samt inkludere cybersikkerhetsutfordringene ved introduksjon av ny teknologi og nye prosesser, slik at sårbarheter ikke gir utilsiktede konsekvenser som følge av økt digitalisering (EPRI, 2021). Det å forstå systemene og analysere hvordan kompleksitetene beskrevet i kap 2.3 er håndtert blir en viktigere oppgave.

5 Digitale sårbarheter i leverandørkjedemodeller

5.1 Sårbarheter ved sterk hovedleverandør av komponenter

I denne modellen peker de røde pilene på hvor sårbarheter og utfordringer kan ramme leverandørkjeden. Disse er basert på uttalelser fra informanter, som har svart på hva de anser som de største utfordringene for leverandørkjedesikkerhet. Ettersom modellen viser en sterk hovedleverandør av komponenter, går sårbarhetene og utfordringene utover de inkluderte digitale sårbarhetene. De digitale sårbarhetene kommer i hovedsak inn som cybersikkerhetsutfordringer mellom kjøper og tjenesteleverandør. Digitale sårbarheter vil likevel kunne oppstå mellom kjøper og hovedleverandør av komponenter, da leverandør kan sitte på sensitiv informasjon.



Figur 8. Modell av sterk hovedleverandør av komponenter med tilhørende sårbarheter og utfordringer.

Tillit, avhengighet og bestillerkompetanse har blitt tatt opp gjentatte ganger av de ulike informantene vi har snakket med, og utdypes nærmere i kapittel 6. Svak bestillerkompetanse er en utfordring som ligger hos kjøperen, mens tillit og avhengighet, som vist i modellen, gjennomsyrer hele kjeden. Informanter etterlyser blant annet kompetanseheving på sikkerhet hos bestillere, og ikke minst bedre kommunikasjon med IT-avdelingene. Kompetanseheving kan sette bestillere i stand til å stille krav eller utfordre leverandøren.

Som nevnt tidligere er tilliten til leverandørene høy i den norske kraftbransjen, men informanter forteller at det også kan være en ulempe da det kan føre til at de ikke kontrollerer i like stor grad som de ville gjort dersom leverandøren var ny og nivået på tillit lavere. Tilsiktede fysiske angrep og

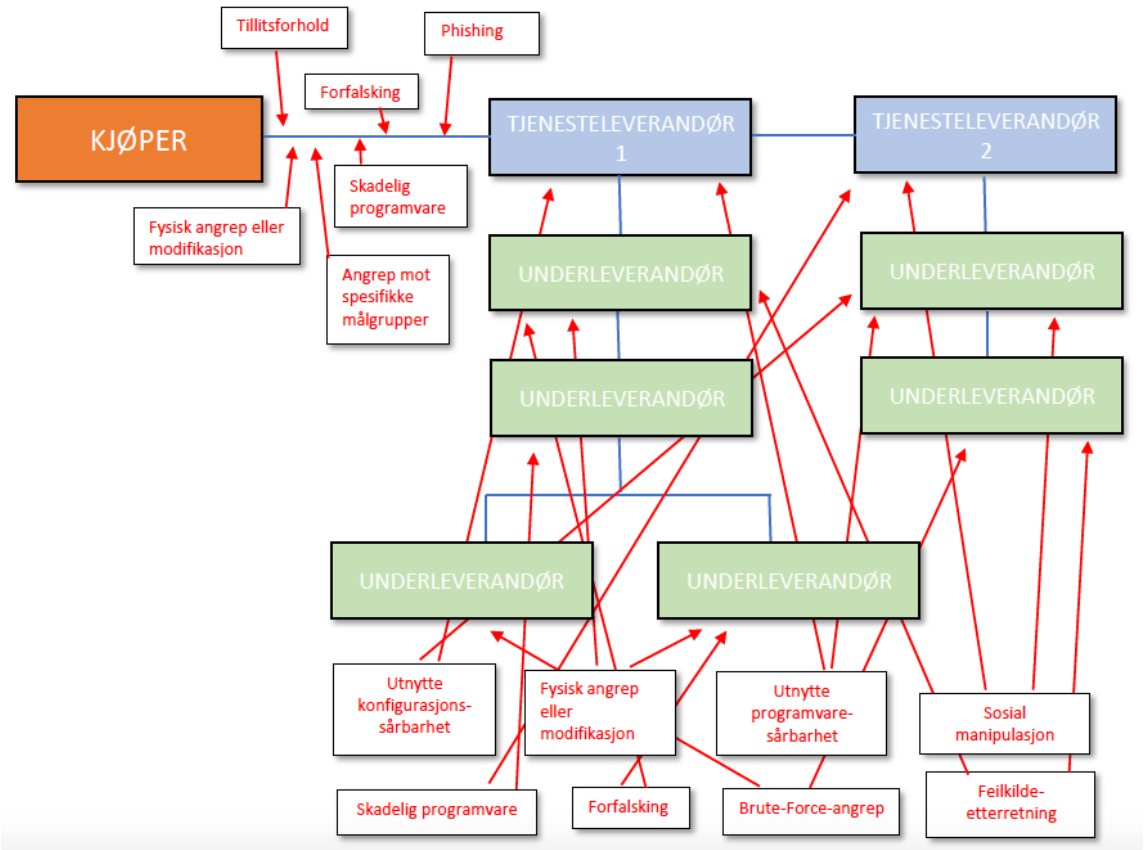
cyberangrep er inkludert i modellen med bakgrunn i ENISA sin rapport. Landrisiko er inkludert og blir også omtalt i kapittel 7. Kjøper kan gjøre landvurderinger når kjøper gjennomfører risikovurderinger. Det kan bidra til at leverandører og underleverandører opererer i land som ikke utgjør en trussel for den samfunnskritiske funksjonen kraftsektoren har.

Dårlig sikkerhet ved transport kan eksempelvis være dårlig sikrede konteinere eller lastebiler, og kan føre til at uvedkommende kan få tilgang til utstyr eller komponenter. Her er det ifølge informanter vanskelig å holde kontroll. Dette gjelder også ved fabrikkene, hvor maskinvaresikkerheten kan være utilstrekkelig. En informant uttaler at de ikke vet hvordan kontrollen eller sikkerheten er når utstyr sendes til en tavlebygger, eller om tavlebyggeren har prosedyrer for å ivareta sikkerheten. De vet for eksempel ikke om utstyret hos tavlebyggeren er overvåket til enhver tid eller om det er mulig for uvedkommende å manipulere maskinvare dersom en montør snur ryggen til eller forlater rommet. Det beste de kan gjøre er å først laste inn programvare når anlegget er kommet fram til endelig mottaker, og er plassert trygt bak lukkede dører. Vurderingen blir ifølge informanten hvor det skal legges inn barrierer slik at risikoen for uønskede hendelser kan reduseres mest mulig.

Tilsiktet fysisk manipulasjon kan skje både i designfasen, på fabrikken, på veien mellom fabrikk og leverandør 2, mellom leverandør 2 og leverandør 1, og hos kjøper. Dette viser at sårbarheter kan ramme alle ledd i leverandørkjeden. Sikkerheten ved transport er noe leverandører problematiserer i større grad enn nettselskaper og kraftprodusenter. Det samme gjelder bestillerkompetanse, hvor leverandøren etterlyser spesifikke sikkerhetskrav, mens kjøpere forteller at de forholder seg til virksomhetens egne retningslinjer, som beskriver minimumskrav. I tillegg oppgir de fleste å benytte seg av veiledere fra NVE og grunnprinsippene til NSM, men ser ikke behov for å gå ut over anbefalingene som er gitt her. Tillitsforhold er derimot tillagt større vekt hos kjøpere (nettselskaper og kraftprodusenter), som mener tillit til aktører som inngår i leverandørkjeden er både svært viktig og noe de i stor grad har.

5.2 Sårbarheter ved distribuert leverandørnettverk

Figur 9 illustrerer mulige trusler mot en slik leverandørkjede, basert på ENISAs (2021) oversikt over trussellandskapet for leverandørkjeder, som viser ulike angrepsvektorer for trusselaktører (se tabellene i kapittel 2).



Figur 9. Modell av distribuert leverandørnettverk av IT-tjenester med tilhørende trusler.

De røde pilene mellom tjenesteleverandør og kjøper viser de ulike angrepsteknikkene ENISA har pekt på, som brukes for å kompromittere en kunde (se tabell 3), henholdsvis tillitsforhold, forfalskning, phishing, fysiske angrep eller modifikasjon, angrep mot spesifikke målgrupper og skadelig programvare. Pilene som peker mot tjenesteleverandører og underleverandører er angrepsteknikkene beskrevet i tabell 2. Dette er trusler mot alle leverandører og underleverandører, og kan også forekomme samtidig. Informanter forteller at phishing er svært vanlig, og noe de opplever ofte. Når det gjelder de andre angrepsteknikkene er det få eller ingen i den norske kraftbransjen som har opplevd at deres virksomhet har blitt utsatt for disse, og har ingen eksempler på andre spesifikke typer angrep eller på at sårbarheter har blitt utnyttet. En informant omtaler det som støy, men ikke alvorlige hendelser. Flere påpeker at det er viktig å ikke bare tenke på de store hendelsene, men de små og hverdagslige som skjer ofte, og som dermed kanskje har størst mulighet, statistisk sett, til å kunne gi konsekvenser. Det er som regel menneskene som gjør feil, mener en informant. De glemmer å logge av, glemmer å bruke to-faktor autentisering eller har for enkelt passord, som potensielt kan bidra til at en angriper finner en vei inn i systemet. Ifølge en informant er det viktig å ikke bli for opptatt av systemer og krypto og lange passord, det hjelper ikke hvis man ikke har bevisstheten og kulturen internt i bedriften. Vi må ikke undervurdere mennesket, som kan være både det svakeste og det sterkeste leddet i kjeden. Menneskelige og tilfeldige feil er også lettere å beskytte seg mot, mener informanten. Angripere med intensjon og kapasitet til å gjennomføre målrettede angrep vil sannsynligvis greie det.

Undersøkelser som er gjort i forbindelse med dette prosjektet viser at kjøpere og hovedleverandører i stor grad føler seg trygge på at underleverandørene ivaretar den digitale sikkerheten, da de opplever at hendelser hos underleverandør blir rapportert og håndtert raskt, de er gode til å etterleve sikkerhetskrav, og tar forbedringsforslag fra kjøper til følge. Det er likevel nødvendig med styringssystemer for å opprettholde kontroll, oppdage sårbarheter og lukke dem raskt. Flere aktører i

kraftbransjen peker på kompleksitet i systemet som en av de største utfordringene i en leverandørkjede. Kompleksiteten gjør det vanskelig å holde oversikt, og det kan oppstå problemstillinger som man ikke vet om, og dermed heller ikke kan gjøre noe med. For eksempel kan det være innbrudd i et system hvor inntrengeren har logget seg inn på samme måte som ansatte, og er der for å rekognosere. Det vil være vanskelig å oppdage så lenge inntrengeren ikke aktivt utfører handlinger i systemet. Det vil alltid være en restrisiko, og usikkerheten rundt hva restrisikoen består av kan ifølge informanter utgjøre en trussel mot leverandørkjedene. Det er vanskelig å sikre god oversikt over systemet og å kunne avdekke hvor det er mest sårbart. Tiltak bør settes inn der risikoen er størst. Det er viktig å få frem at ikke alle vi har snakket med er like bekymret for kompleksiteten, og flere hevder at de har god oversikt over både systemer og leverandørkjeder. Andre mener at kraftbransjen henger etter når det kommer til IKT-sikkerhet og ikke minst når det gjelder å fullt ut anerkjenne trusselbildet generelt og mulige målrettede trusler og angrep mot kraftbransjen.

Sentralisering versus desentralisering av leverandørkjeder er en viktig debatt. I tilfeller hvor det er en sterk hovedleverandør kan det være lettere å holde oversikt over leverandørkjeden da leverandøren selv er eier av underleverandør og fabrikker. Dette gjør kjeden mindre kompleks med hensyn til organisasjoner og den preges i større grad av tillit. Samtidig vil det også være lettere for hovedleverandør å stille krav lenger ned i kjeden. Er leverandørnettverket mer distribuert blir bildet mer komplekst da virksomhetene benytter ulike tjenesteleverandører med tilhørende underleverandører. Men disse forenklede argumentene har nyanser som gjør at hver leverandørkjede bør analyseres ut fra sine egenskaper.

6 Utfordringer i leverandørkjeder

6.1 Oversikt

Å ha oversikt og innsikt i egne systemer er viktig i styring av risiko og sikkerhet. Det første av NSMs grunnprinsipper for IKT-sikkerhet er å identifisere og kartlegge styringsstrukturer, leveranser og understøttende systemer, kartlegge enheter og programvare, og kartlegge brukere og behov for tilgang (NSM, 2020). Hensikten er forstå virksomhetens leveranser og tjenester, slik at ansatte kan sette søkelys på og prioritere sikkerhetstiltak i tråd med virksomhetens behov. Oversikt utfordres av kompleksitet og mangel på transparens, og ikke minst lange digitale verdikjeder. NVE Rapport (90/2018) om IKT-sikkerhet ved anskaffelser og tjenesteutsetting i energibransjen, beskriver energiselskapers leverandører sin plikt til å holde full oversikt over sine underleverandører. Dette skal være enklere når det kommer til programvare enn maskinvare da maskinvare ofte har lengre og mer komplekse verdikjeder. Det er også nødvendig å ha kontroll over avhengigheter som går utenfor landets grenser, for å sikre funksjonalitet i systemer som understøtter viktige samfunnsfunksjoner ved en eventuell tilspisset sikkerhetspolitisk situasjon. Behovet for oversikt over digitale verdikjeder avhenger av kritikaliteten til den funksjonen den understøtter (DSB, 2020). Kraftforsyning er definert som samfunnskritisk funksjon og dermed er oversikt viktig for å sikre funksjonalitet i systemene som understøtter kraftforsyningen.

Nesten alle informantene synes det er vanskelig å ha transparens gjennom hele leverandørkjeden ved bruk av mange underleverandører. Det er mulig å revidere ett ledd, mens videre bakover finnes flere underleverandører som det er vanskeligere å stille krav til. Kontrakten skrives mellom kjøper og hovedleverandør, og ansvaret for underleverandørene ligger dermed hos hovedleverandøren og ikke kjøperen. Kjøper har begrensede muligheter og rettigheter til å stille krav til underleverandørene. Leverandører i andre land er underlagt nasjonalt lovverk og andre sikkerhetskrav, og de er ikke nødvendigvis villige til å dele sine interne dokumenter eller gi innsyn til virksomheter i andre land.

6.2 Avhengighet

Mange informanter hevder at kraftbransjen er svært avhengig av leverandørene, spesielt IKT-løsninger og kompetanse. Avhengighet til eksterne systemer og infrastruktur utgjør en sårbarhet for kraftforsyningen. Ved en gradvis effektivisering over tid, hvor personell blir erstattet med IKT, forsterkes avhengigheten til annen infrastruktur, for eksempel ekom.

Funksjoner som blir operert fysisk vil etter hvert fjernstyres. Driftskontrollsystemene som tidligere var helt uavhengig av andre IKT-systemer, er nå avhengige av digitale støttefunksjoner som gjør at digitale signaler kan gjøres om til fysisk handling (NOU 2015:13, 2015).

Den digitale utviklingen kan føre til kompetansetap på manuell drift og gammel teknologi. Dette kan også være en utfordring hos leverandørene. Informanter forteller at det kanskje bare er en eller to personer som fortsatt har kunnskap om de eldste systemene, noe som gjør dem både personavhengige og sårbare. Det fører til at de er avhengige av at de digitale systemene fungerer og er sikret til enhver tid. I tilfeller hvor alternativ drift ikke er mulig, utgjør dette en stor sårbarhet. Avhengigheten til leverandører forsterkes ved at ikke alle virksomheter har ressurser til å drifte IKT-systemene selv. Da er virksomheten avhengig av leverandørenes kompetanse, noe som utfordrer evnen til å holde oversikt, spesielt ved bruk av skytjenester. Utfordringen ved at kompetansen ligger hos leverandørene gjør det også vanskeligere å bytte leverandør, ettersom tilgangen til relevant kompetanse forsvinner ved avtalens slutt. Dette øker avhengigheten til eksisterende leverandører, og kan gjøre det vanskelig og

kostbart å bytte (Halvorsen & Selnes, 2020). Flere av informantene forteller at de har brukt de samme leverandørene i mange år, og at det oppleves som en fordel. Kjøper og leverandør har over tid utviklet gode relasjoner og tillitsforhold, noe som gjør kjøperne tryggere på at leverandørene vil reagere og varsle dersom det oppstår nye sårbarheter eller sikkerhetsbrudd.

Avhengigheten til digitale løsninger kan se ut til å øke i tiden som kommer. Dersom det innføres en ny digital løsning, vil det sannsynligvis være behov for å også digitalisere tilstøtende systemer for å gjøre dem kompatible. Dette vil også øke avhengigheten til leverandører og eksterne aktører, i tilfeller hvor driften av slike systemer er tjenesteutsatt.

6.3 Tillit

Lysne (2018) beskriver forholdet mellom kjøper og leverandør av elektrisk utstyr og tjenester som et tillitsforhold, hvor tillit i denne sammenhengen betyr at kjøperen stoler på at leverandøren leverer produktet i tide, at det har rett kvalitet, og riktig pris. Kjøperen må også stole på at leverandøren vil sørge for sikkerhetsoppdateringer gjennom hele produktets levetid. Ved bruk av for eksempel skytjenester må brukeren kunne stole på at informasjonen er trygt lagret, eller sørge for å ikke dele sensitiv informasjon med leverandører de ikke har full tillit til. Tillit kan ifølge Lysne bygges opp gjennom et langvarig forhold til leverandøren, eller at leverandøren har dokumentert kompetanse og kvalitet på digital sikkerhet, i tillegg til et bra omdømme. Samtidig er det ikke slik at så fort man stoler på en leverandør vil denne være trygg å bruke. Tryggheten avhenger av balansen mellom risikoen man eksponerer hverandre for (Lysne, 2018).

Angriper kan for eksempel utnytte det eksisterende tillitsforholdet. KraftCERT påpeker at sårbare tillitsforhold mellom kunder og leverandører oftere blir mål for trusselaktører (KraftCERT, 2021). ENISA (2021) skriver i sin rapport at rundt 62% av angrep på kunder utnyttet tillitsforholdet til leverandører. ENISAs rapport er ikke begrenset til kraftbransjen, men den er likevel med på å vise en trend og hvilket trusselbilde vi står ovenfor.

Informantene peker på at i den norske kraftbransjen er det flere leverandører som har vært med lenge, og som kjøperne har tillit til. Det gjør at kjøperne ikke er like gode til å sette krav til folk de kjenner, sammenlignet med når de setter krav til ukjente leverandører. Når virksomhetene har benyttet seg av samme leverandører over lenger tid bygges det tillit, mens det kapasitetsmessig er vanskelig å kontrollere sikkerheten og sikre transparens.

Leverandører kan bli utnyttet, slik som i SolarWinds-hendelsen, men vi har ikke sett eksempler på leverandører som bevisst har gjennomført angrep mot kunder. Med uønskede hendelser knyttet til leverandørene, for eksempel at tredjeparter tar seg inn og sender ut oppdateringer, antar brukerne at de får programvareoppdateringer fra en sikker kilde. Problemstillingen vil her være hvordan slike hendelser kan forhindres og oppdages.

Informanter påpeker at det er viktig å holde seg oppdatert på risikobildet, og ha et økt fokus på underleverandører. Det er også viktig å huske på at menneskelige eller utilsiktede feil kan forekomme, og at hendelser i leverandørkjeder ikke nødvendigvis skjer fordi vedkommende ikke var til å stole på, men fordi det er vanskelig å sikre seg fullstendig mot uhell eller feil.

6.4 Markedsdominans og mangel på redundans

Ved behandling og lagring av kraftsensitiv informasjon i utlandet kreves vurdering av hvilken informasjon som er så kritisk at den ikke bør lagres utenfor Norge (NOU 2015:13, 2015). For å ha oversikt og vurdere verdikjeden må redundans inkluderes, slik at eventuell svekkelse av IKT-leverandører, ikke medfører konsekvenser for samfunnet. Man kan likevel ha tilsynelatende redundante løsninger, men man må ta høyde for at disse løsningene kan dele sårbarheter lenger ned i verdikjeden (DSB, 2020).

Virkemidler innen risikostyring knyttet til IKT er preventive tekniske sikkerhetstiltak, som omfatter sikkerhetskopier og redundans, antivirus, sikkerhetsoppdateringer, brannmur, kryptografi og overvåking. Redundans er et viktig virkemiddel som øker sikkerheten gjennom eksempelvis duplikasjoner, overlapp og reservesystemer som kan kompensere for eventuelle feil. På denne måten kan pålitelige systemer sikres selv ved upålitelige komponenter (Njå, Sommer, Rake, & Braut, 2020). Markedsdominans kan befinne seg hos hovedleverandører, og i kraftbransjen finner vi noen sterke hovedleverandører av komponenter i driftkontrollssystemer og digitale strømmålere. I tillegg til dette har leverandører av kontorstøtteprogramvare, som Microsoft, en dominerende markedsstilling i Norge. Microsoft ble rammet av angrepet mot SolarWinds i 2020.

6.5 Bestillerkompetanse

Bestillerkompetanse handler om å ha tilstrekkelig forståelse av virksomhetens behov, kvalitet på produktene som skal kjøpes, regelverk og IKT-sikkerhet i anskaffelsen. Det vil si at bestiller må ha tilstrekkelig kompetanse både ved innkjøp av komponenter og IKT-tjenester. Figur 10 angir hvorvidt virksomheter i kraftbransjen kjøper basispakken fra leverandører av IKT-tjenester. Diagrammet viser at de fleste virksomhetene oppgir at de kjøper avanserte sikkerhetstjenester utover det som tilbys i basispakken, mens 11% vet ikke hvilke IKT-tjenester de de kjøper.

Figur 10. Kjøper virksomheter basispakken fra leverandører av IKT-produkter?

I NVE Rapport Nr. 90/2018 om IKT-sikkerhet ved anskaffelser og tjenesteutsetting i energibransjen blir energiselskapene utfordret på hva som kjennetegner en god leverandør og leverandører svarer på hva som er en god kunde (Kirkebø & Ljøsne, 2018). Leverandørene mener kundene må ha et faglig

fokus og et gjennomtenkt forhold til produktet de skal kjøpe, og at de setter sikkerhet som førsteprioritet. Bestillere på sin side mener at de ikke alltid har mulighet til å ha sikkerhet som førsteprioritet, da de også må forholde seg til pris, kvalitet på produktet og brukervennlighet. Virksomhetene har et budsjett å forholde seg til og et ansvar for å forvalte pengene riktig ut ifra et samfunnsperspektiv. Pris vektes derfor som regel nærmere 60 prosent, og kvaliteten utgjør de resterende 40 prosent når innkjøp og bestillinger vurderes.

Innkjøpere må ha kompetanse til å stille de riktige spørsmålene slik at de tenker sikkerhet hele tiden. Det er dette som er utfordringen, ikke nødvendigvis evnen til å sette krav og å gjennomføre anskaffelser.

Informanter mener det sjelden stilles strenge krav til IT-sikkerhet når det gjøres innkjøp. Kravene er gjerne generelle eller at leveransen skal være i henhold til eksempelvis ISO-standard. Her kan alle leverandørene bare svare «ja», og når alle da oppfyller kravene er det som regel slik at de billigste vinner. Det blir også påpekt av leverandører at de aldri har opplevd å bli kontrollert på den tekniske leveransen. Leverandørene kan levere i henhold til en standard, men kan ikke garantere for denne uten å vite hvordan kundene tar denne i bruk i anleggene. Flere mener at innkjøpere hadde vært tjent med kursing i sikkerhet i anskaffelser, men dette koster penger, og når virksomhetene ikke har opplevd store uønskede hendelser er de kanskje ikke motivert til å bruke ressurser på dette.

NSMs landvurdering er viktig å ta i betraktning når det gjøres anskaffelser, men det kan være vanskelig å vite hvor alle komponenter kommer fra. Informanter påpeker at man har styrket seg på dette området med rådgivere som jobber tettere på prosjekter og stiller krav til leverandører, samt at innkjøp også har mer om dette i kontrakter for å styrke mulighetene for oppfølging. Det kommer også frem at digital sikkerhet kommer høyere på agendaen fordi ledelsen vet at konsekvensene kan bli store, selv om de ikke har opplevd dette selv.

6.6 Resiliens – en ønsket verdi for kritisk infrastruktur

Resiliens handler om fleksibilitet, og beskrives som organisasjoners evne til å lære og til å ha en proaktiv tilnærming til sikkerhet. Resiliens er evnen til tilpasning ved utfordrende og skiftende forhold. En resilient virksomhet evner å opprettholde en viss funksjonalitet ved kritiske sikkerhetshendelser, og å gjenopprette sin virksomhet ved forstyrrelsens slutt. Vi kan også se på det som systemets evne til å forutse, tilpasse seg og komme seg fra uønskede hendelser slik at systemet kan gjenoppta sin opprinnelige funksjon (t'Hart & Sundelius, 2013).

Kraftforsyningen bør vektlegge resiliens, ettersom manglende evne til å kunne opprettholde en viss funksjonalitet vil kunne få store konsekvenser for resten av samfunnet. Å være resilient innebærer å ha innebygd cybersikkerhet i systemet, også rettet mot OT. Det er utfordringer knyttet til å oppnå resiliens da kraftbransjen består av mange aktører. Det er vanskelig å utvikle et sett med retningslinjer som er anvendbare og favner alle.

Iboende cybersikkerhet for å oppnå resiliens er en ambisiøs visjon, men et viktig mål for kritisk infrastruktur. EPRI påpeker at status quo for cybersikkerhet ikke vil fungere med dagens trender. Praksiser og systemene i energiforsyning må kritisk vurderes. Første steg er å dokumentere og kartlegge hvor vi står i dag og identifisere gapene, slik at interne industrikrav kan identifiseres, og gjøre virksomhetene i stand til å ta beslutninger som kan optimalisere OT-cybersikkerhetsinvesteringer. Visjonen og kartleggingen krever deltakelse fra alle interessenter, også leverandører (EPRI, 2021). Det er behov for omfattende analyser i kraftsektoren.

6.7 Risikostyring og sikkerhetskultur

Kraftberedskapsforskriften skal sikre forsvarlige beredskapsmessige hensyn for at kraftforsyningen skal kunne opprettholde sin funksjonalitet under ekstraordinære påkjenninger (Kraftberedskapsforskriften, 2012). Forskriften ble revidert i 2019, og stiller krav til IKT-sikkerhet, blant annet gjennom forskriftens § 6-9 som stiller særskilte krav til sikring og risikovurdering av digitale informasjonssystemer. Kravene bygger på NSMs Grunnprinsipper for IKT-sikkerhet. Kraftberedskapsorganisasjonen (KBO) er en nasjonal beredskapsorganisasjon som er hjemlet i energiloven. Kraftberedskapsforskriften stiller en rekke sikkerhets- og beredskapskrav krav til KBO-enhetene. Kravene dekker organisering, risikovurdering, beredskapsplanlegging og øvelser, digital sikring, sikring av driftskontroll, fysisk sikring og reparasjonsberedskap med mer. (Kraftberedskapsforskriften, 2012).

6.7.1 Risikostyring

NVE (2021) har undersøkt IKT- sikkerhetstilstanden i kraftbransjen, og kartlagt i hvilken grad bransjen har opplevd at cyberangrep har hatt konsekvenser for funksjonaliteten til driftskontrollsystem, kraftproduksjon eller strømnett. Undersøkelsen viser at tre prosent av de spurte (fire selskap) har opplevd uønskede hendelser i driftskontrollsystemet som har hatt konsekvens for funksjonen til driftskontrollsystemet. Åtte prosent har opplevd uønskede IKT-hendelser i administrative IT-systemer. Årsakene til IKT-sikkerhetshendelsene har i 11 tilfeller vært knyttet til hendelse hos leverandør eller tredjepart. Teknisk svikt eller sikkerhetsbrudd av ansatt eller innleid personell, har stått for en hendelse hver. Av disse som har opplevd IKT-sikkerhetshendelser i løpet av de siste 12 månedene svarer 10 av selskapene at de har satt inn tiltak i form av tekniske sikkerhetstiltak, endring av rutiner eller opplæring.

Beredskapsledere i selskapene som har deltatt i undersøkelsen har fått spørsmål om virksomheten har en IKT-sikkerhetsstrategi. 80 prosent svarer at de har det, mens 20 prosent mener at de ikke har en egen strategi for IKT-sikkerhet. Likevel svarer nesten alle at de i stor grad eller i noen grad anser IKT-sikkerhet som en del av sikkerhetskulturen, og at IKT-hendelser tas opp på ledermøter. Det kommer også frem at 36 prosent av beredskapslederne mener de har et stort behov for kompetanseheving og opplæring i informasjonssikkerhetsledelse.

IKT-sikkerhetskoordinatorer har besvart spørsmål om styringssystemer for informasjonssikkerhet, og 35 prosent svarer at de har et slik styringssystem. 59 prosent oppgir at de ikke har det, mens 6 prosent vet ikke. Ingen av KBO-enhetene er sertifisert i henhold til ISO 27001, som omhandler styringssystem for informasjonssikkerhet. Undersøkelsen viser også at 76 prosent av beredskapslederne kjenner til NVEs retningslinjer for IKT-sikkerhet i anskaffelser, og nesten halvparten mener at retningslinjene etterleves i stor grad. 59 prosent av beredskapslederne oppgir at de kjøper avanserte sikkerhetstjenester, mens 31 prosent kjøper basispakken. 10 prosent vet ikke. Resultatene må forstås i lys av selskapenes størrelse, da omtrent halvparten av selskapene som har deltatt er små, og har under 50 ansatte.

I tillegg til å ivareta konfidensialitet, tilgjengelighet og integritet, må virksomhetene også vurdere hva og hvem de ønsker å beskytte seg mot. Hvilket sikkerhetsnivå som er nødvendig for det aktuelle systemet kan først avgjøres etter å ha gjennomført en risikovurdering. Risikostyring handler om virkemidlene som kan benyttes for å kontrollere risiko, og risiko kan defineres som *"et uttrykk for*

konsekvens/utfall av uønskede hendelser og usikkerhet assosiert med hendelser og utfall" (Njå, Sommer, Rake, & Braut, 2020). Det kan likevel være slik at man må prioritere mellom ulike risikoreduserende tiltak, noe som innebærer en erkjennelse av at man ikke kan fjerne all risiko (NOU 2015:13, 2015). Dette påpeker også informanter, og mange sier at det er umulig å sikre seg hundre prosent mot en uønsket hendelse, og at aktører som har stor kapasitet kan gjennomføre angrep man ikke kan sikre seg mot.

Arbeidet med å redusere risiko og sårbarhet i digitale verdikjeder må inngå i virksomheters ordinære risikostyringsprosesser, som også bør inkludere ledelsen og beslutningstakere i virksomheten som helhet. DSB understreker at risikostyring i digitale verdikjeder er en kontinuerlig prosess som må gjentas regelmessig, spesielt ved endringer som kan påvirke risiko og sårbarhet, som for eksempel endringer i leverandørforhold (DSB, 2020). NSM har erfart at mange virksomheter har manglende kompetanse på gjennomføring av risikovurderinger, og manglende kunnskap kan medføre dårligere sikkerhetsstyring og manglende sammenheng mellom tiltak og risikobilde (NSM, 2021).

6.7.2 Sikkerhetskultur – et kritisk blikk på arbeidspraksis

Sikkerhetskultur handler om hvordan sikkerhet prioriteres i organisasjoner. Kraftforsyningen består av mange aktører, både store og små, interne og eksterne. Med digitalisering kan en se at sektoren må forholde seg til nye farer, trusler og sårbarheter som gjør at sikkerhet knyttet til teknologisk utvikling må prioriteres på alle nivå.

Organisasjonskultur defineres som "delte verdier (hva som er viktig) og tro (hvordan ting fungerer) som samhandler med en organisasjons strukturer og kontrollsystemer for å skape atferdsnormer (måten vi gjør ting på). Psykologen James Reason peker på fire underkomponenter som til sammen utgjør en informert kultur, og som sammenfaller med sikkerhetskultur, nemlig en rapporteringskultur, en rettferdig kultur, en fleksibel kultur og en læringskultur (Reason, 2016). Rapporteringskultur er spesielt viktig, og trekkes frem av informanter som en viktig faktor i sikkerhetsarbeidet, sammen med læringskultur. NSM mener at ved å motivere ansatte til å handle på en måte som ivaretar sikkerheten, vil de oppnå en god sikkerhetskultur som bidrar til at sikkerhetstiltak ivaretas av de ansatte. Ledelsen må gå foran som et godt eksempel, og gjøre øvrige ansatte bevisst på hva som er forventet av dem, og hvorfor (NSM, 2020). Underkomponentene som utgjør Reasons sikkerhetskultur, er idealer som både selskaper og leverandører i bransjen må strebe etter å oppnå, men som ikke nødvendigvis vil være målbare. Det kan være utfordrende å bruke tid og ressurser på noe som er vanskelig å måle.

I bransjen kan det også finnes organisatorisk motstand når sikkerhetskulturen innad i selskaper ikke er bra nok. Det kan da ta tid å lære opp og bygge opp støtte for endringer i teknologi, prosesser, samt kunnskap og ferdigheter. En grunn til at virksomhetene kan oppleve motstand er at det er vanskelig å måle om sikkerhetsarbeidet fungerer eller ei, når de ikke har blitt utsatt for et angrep. Mangel på synlighet påvirker derfor også rettferdiggjøringen av investeringer i cybersikkerhet (EPRI, 2021).

Om leverandørene har dårlig sikkerhet hjelper det lite om deres kunder er gode på dette området. Dette handler om å erkjenne trusselbildet man står ovenfor. Informanter sier at holdningsskapende arbeid gjøres, også på IKT-delen. Det påpekes likevel av flere at kompetanse om leverandørkjedesikkerhet er en utfordring, og noen etterspør en felles tilnærming til dette. Det er vanskelig å ha nok kompetanse i alle små nettselskap og at mange selskap skulle hatt kompetanse det ikke er mulig for den enkelte virksomhet å oppnå.

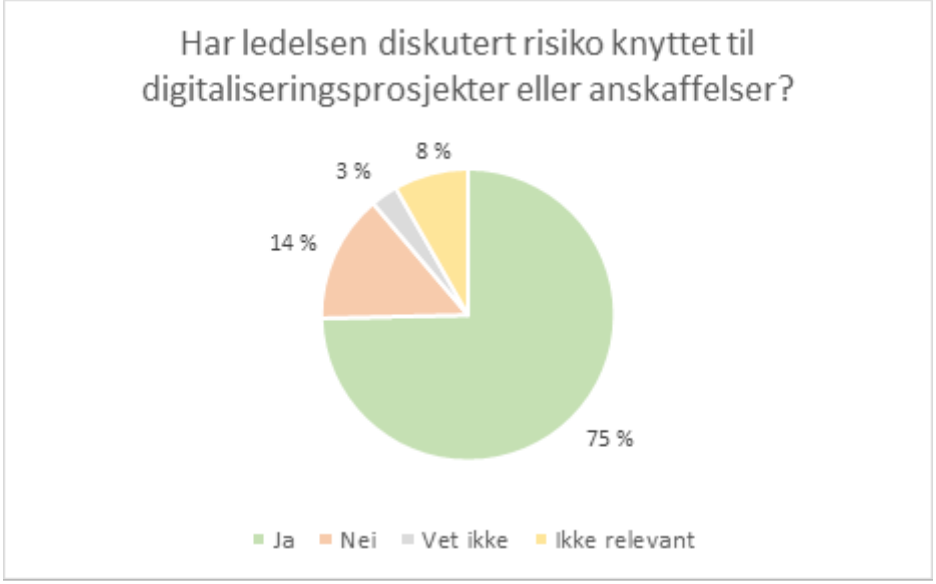
Informanter påpeker at det finnes trusselaktører som har kapasitet, og at det ikke lenger handler om *hvis* et angrep skjer, men om *når* det skjer. Virksomhetene er nødt til å minimere de enkle

sårbarhetene, og da må de også være bevisste på hva de enkle sårbarhetene er. Løsepengeangrep (ransomware), som vi har sett i nyere tid, er eksempler på at trusselaktører identifiserer sårbarheter, og går for den enkleste inngangen. Det er ikke nok å bare skrive kontrakter, om leverandørene fortsetter uten et bevisst forhold til sikkerhet. Dette innebærer blant annet at leverandører er åpne, og at de tidlig varsler om hendelser og tiltak slik at konsekvensene reduseres for alle berørte.

I 66% av tilfellene analysert i ENISA sin rapport om leverandørkjedeangrep har angripere fokusert på leverandørenes koder for å videre angripe kunder. Dette viser at organisasjoner bør ha et fokus på validering av tredjepartskode og programvare for å være trygge på at disse ikke er manipulert. Videre funn fra undersøkelsen viser at i 66% av angrepene visste ikke leverandørene hvordan de ble kompromittert, det vil si hvordan en angriper har kommet seg inn i systemene eller brutt sikkerhetsbarrierene. I kontrast til dette er det bare 9% av kundene som har blitt kompromittert gjennom leverandørkjedeangrep som ikke visste hvordan angrepene skjedde. ENISA påpeker et gap i modenheten i rapportering av cybersikkerhetshendelser mellom leverandører og sluttbrukervendte selskaper. Et hinder for kunnskap om angrepet vil også kunne være kompleksiteten i gjennomføringen av angrepene, og at de oppdages sent (ENISA, 2021). Av ENISAs analyserte saker har det ikke vært mulig å forfølge 42 % av angriperne til noen bestemt gruppering. Usikkerheten er høy, og det forsterker behovet for å kunne kontrollere leverandørene og stille krav til egne systemer i kraftforsyningen.

De aller fleste vi har snakket med, både leverandører, nettselskap og kraftprodusenter, mener at de har fokus på sikkerhetskultur, og at dette ofte handler om å kunne levere et produkt med troverdighet og tillit, og ikke kun konkurrere på pris. Det uttrykkes likevel usikkerhet rundt det samlede IT-sikkerhetsnivået i bransjen generelt. Det er ressurskrevende å gjennomføre penetrasjonstester eller kursing. Det krever også spesiell kompetanse som ofte ikke finnes internt i de minste virksomhetene. Informanter viser til en todeling av sikkerhetskulturen i bransjen i Norge, noe som trolig er sterkt knyttet til driftsbudsjett. De store selskapene har større muligheter til å sette av ressurser til dette, mens de små selskapene blir hengende etter og kan potensielt utgjøre en sårbarhet for kraftforsyningen som helhet. Samtidig er flere opptatt av at en del sikkerhetstiltak er gratis, og nevner blant annet innføring av to-faktor autentisering, økt bevissthet rundt viktigheten av å logge av nettverk og pc, restriksjoner rundt hvilke nettsider som kan åpnes på arbeidsplassen, og økt fokus på phishing e-post.

Diagrammet under viser at flertallet av selskapene som har svart på NVEs spørreundersøkelse knyttet til prosjektet har svart at ledelsen har diskutert risiko knyttet til digitaliseringsprosjekter eller anskaffelser. Selv om temaet har vært diskutert betyr ikke dette nødvendigvis at sikkerhetsarbeidet er tilstrekkelig.



Figur 11. Risiko knyttet til digitaliseringsprosjekter eller anskaffelser. (NVE, 2021)

NSM har gjennomført undersøkelser som indikerer at mange virksomheter ikke har forankret sikkerhetsarbeidet tilstrekkelig i virksomhetens ledelse (NSM, 2021). I følge EPRI må cybersikkerhetsvurderinger og tiltak bygges inn i design- og distribusjonsfaser. Dette handler om å gjøre cybersikkerhet mer modent både i enkelte selskaper, men også i bransjen. Standarder må overholdes hvor slikt er påkrevd, men målet vil gå utover dette, nemlig å nå iboende sikkerhet hvor sikkerhet er fullt integrert i alle prosesser, teknologi og ikke minst kultur (EPRI, 2021).

7 Hvordan forstå digital sårbarhet i leverandørkjeder – anbefalinger

I det avsluttende kapitlet vil vi oppsummere inntrykkene fra studien og gi noen anbefalinger til virksomheter i kraftforsyningen. Vi tror at sikkerhetstenkningen må få en ny form og at virksomhetene må finne en praktisk tilnærming til den kontinuerlige styringen av sikkerheten, hvor leverandørkjedene krever økt oppmerksomhet.

7.1 Ikke-styrbare forhold

Reguleringsregimer utenfor kontroll – politisk risiko

Når det kommer til leverandørkjeder er det en rekke forhold som ikke kan kontrolleres. Disse ikke-styrbare forholdene omhandler blant annet regulering, lov og rett. Ved bruk av leverandører i andre land må det tas hensyn til lover og reguleringer i andre steder av verden. Norge er et land med åpen økonomi og samfunnsutviklingen er derfor preget av internasjonale forhold. Politisk risiko kan defineres som usikkerhet om konsekvensene av politiske beslutninger, noe som blant annet kommer til syne gjennom markeder. Virksomheter med betydelig innslag av systemer fra leverandørkjeder forbundet med politisk risiko bør kartlegge denne risikoforestillingen[3], og sørge for at denne vurderingen følger sikkerhetskontrollstrukturen, se kapittel 7.4, og de kritiske prosessene som overvåkes.

Vurdering av internasjonale kriser

Ettersom digitalisering av systemer bygger på fysisk infrastruktur, eksempelvis maskinvare, vil momenter som klimaendringer, pandemier og andre kriser kunne være en sårbarhet i leverandørkjeder. Ved klimaendringer som skaper mer ekstremvær vil dette kunne skape utfordringer knyttet til leveranse av produkter. Covid-19 har skapt sine utfordringer i markedene. Under Covid-19-pandemien har vi erfart økt digitalisering, og de fleste næringer har blitt påvirket. NSM mener likevel at verdikjedene som understøtter viktige samfunnsfunksjoner og nasjonal sikkerhet er i mindre grad påvirket enn fryktet (NSM, 2021). Ved internasjonale kriser bør virksomheter med avhengighet til globale verdikjeder gjøre en sårbarhetsvurdering.

Store endringer i leverandørkjeden

Leverandørkjedearkitekturen kan endres ved oppkjøp og omorganiseringer, og eierskap kan endres under kontraktens levetid. Dette kan gjøre det utfordrende å se de digitale sårbarhetene nederst i leverandørkjeden. Dette vil komme mindre til syne i modell av sterk hovedleverandør da det i stor grad er samme virksomhet som har kontroll over kjeden gjennom eierskap. Det er likevel viktig for virksomheter i kraftforsyningen å overvåke leverandørkjedene av viktig infrastruktur for virksomhetens systemer og funksjoner, slik at beredskapsløsninger kan planlegges og iverksettes ved kritiske endringer i kjeden.

7.2 Risikostyring i forkant av anskaffelsesbeslutning

NSMs anbefaling til landvurdering

[3] Vi bruker risikoforestilling i stedet for risikobilde, fordi det uttrykker virksomhetens vurderinger av andre lands reguleringer og politiske stabilitet. Risikoforestilling er ikke et statisk bilde, men følger virksomhetens oppdaterte syn og kunnskap om disse forholdene (Njå, Braut, Rake, & Aanestad , 2012).

En viktig faktor i anskaffelsesprosesser, er å vurdere om det innebærer en risiko å sette ut tjenester til utlandet. I takt med globaliseringen og digitaliseringen, ser vi at stadig flere IKT-tjenester leveres av store globale aktører. Det innebærer at virksomheter, inkludert kraftbransjen, i større grad enn tidligere setter ut tjenester til virksomheter utenfor Norge, eller at underleverandørene setter ut sine tjenester til virksomheter i utlandet. NSM anbefaler derfor at landvurderinger bør være en del av risikovurderingen ved tjenesteutsetting, men erfarer at virksomheter ikke i tilstrekkelig grad inkluderer landvurderinger. NSM har derfor utarbeidet fire kriterier som bør inngå i den totale risikovurderingen ved tjenesteutsetting:

1. *Statlige styringsindikatorer.* Statlige styringsindikatorer måles etter seks parametere som til sammen sier noe om hvordan landets styresett utøves og forvaltes, og kan si noe om fremtidig utvikling i landet. Dette er viktig ettersom kontrakter ofte har varighet på flere år. Indikatorer tilhørende hvert område finnes på åpne kilder, slik at man enkelt kan benytte dem.
   - Korrupsjon: land måles og rangeres etter oppfattet grad av korrupsjon blant offentlige ansatte og politikere.
   - Politisk stabilitet: sier noe om sannsynligheten for at en stat vil bli destabilisert eller styrtet som følge av voldelige midler.
   - Lov og orden: omhandler hvorvidt lover og regler i samfunnet overholdes, og at man har tillit til disse. Gjelder blant annet overholdelse av inngåtte kontrakter, eiendomsrett, politi og domstoler, og sannsynligheten for vold og kriminalitet.
   - Regulatorisk kvalitet: sier noe om myndighetenes evne til å formulere og iverksette regulatoriske og politiske retningslinjer som fremmer og styrker utvikling av privat sektor.
   - Statens effektivitet: undersøker kvaliteten på offentlige tjenester og statsforvaltningen, grad av uavhengighet fra politisk press, og troverdighet til å gjennomføre politikk.
   - Fredelighet: Global Peace Index forsøker å måle fredelighet i et land, ved hjelp av indikatorer innen samfunnssikkerhet, nasjonale og internasjonale konfliktnivå og grad av militarisering.

2. *Cybersikkerhetstilstanden.* Cybersikkerhetstilstanden i ulike land kartlegges av Global Cybersecurity Index (GCI), og er senest oppdatert i 2020 (ITU, 2020). Sikkerhetstilstanden indikerer hvilke sikringsmekanismer vertslandet for tjenesten har etablert både organisatorisk og teknisk, for å håndtere tilsiktede og utilsiktede hendelser (NSM, 2019). Indeksen kan gi en pekepinn på hvordan de ulike landene vil kunne håndtere et digitalt angrep, og kan benyttes for å vurdere om det aktuelle landet har forutsetninger for å være godt rustet, ved hjelp av poengsummen de er gitt av GCIs ekspertpanel.

3. *IKT-infrastruktur og kompetanse.* Vurderingen av IKT-infrastruktur og kompetanse gir en indikasjon på om vertslandet har utbygde nasjonale IKT-tjenester som er nødvendig for at de skal kunne tilby en stabil og robust IKT-infrastruktur. Det er også nødvendig med en tilstrekkelig grad av kompetanse innen feltet. Begge parameterne måles av World Economic Forum.

4. *Forretningsstabilitet.* Forretningsstabiliteten vurderes ut fra om privat næringsliv i landet har råderett uten statlig innblanding, og sier noe om hvor lett eller vanskelig det er å drive privat virksomhet. Forretningsfriheten måles av World Bank. Vurderingskriteriet innebærer også en måling av finansiell frihet, og sier noe om omfanget av offentlige reguleringer av finansielle tjenester, graden av statlig inngripen i banker og andre finansielle virksomheter, og åpenhet til utenlandsk konkurranse. Høy rangering indikerer et effektivt bankvesen og uavhengighet fra statlig kontroll (NSM, 2019).

NSM påpeker at vurderingskriteriene kan ha ulik betydning for ulike virksomheter, og at man derfor bør vekte de ulike kriteriene med utgangspunkt i virksomhetens behov.
Trusselvurderingene fra etterretningstjenesten og PST bør vurderes i tillegg til disse indikatorene, da disse sier noe om etterretningstrusselen mot norske interesser i utlandet, og hvilke land som anses som den største trusselen. Mindre virksomheter kan ha kapasitetsmessige utfordringer med å kartlegge og vedlikeholde faktorer som politisk risiko og statlige styringsindikatorer. *En mulig løsning er at KraftCERT drifter en slik oversikt over relevante ikke-styrbare forhold, som virksomhetene kan bruke som et hjelpemiddel i arbeidet med å vurdere risiko ved tjenesteutsetting eller samarbeid med andre land i Europa eller verden.*

NVEs retningslinjer for IKT-sikkerhet i anskaffelser og tjenesteutsetting bør utvides til leverandørkjeden
NVEs retningslinjer IKT-sikkerhet i anskaffelser og tjenesteutsetting i kraftbransjen (2020) er en sjekkliste som fungerer som et verktøy i en forberedende fase, selve anskaffelsesfasen, i implementerings- og forvaltningsfasen og i opphørsfasen. I den forberedende fasen inkluderes risikovurderinger, vurdering av egne ferdigheter/forutsetninger og virksomhetens kontekst, etterlevelse av krav og beslutning om tjenesteutsetting og anskaffelse (NVE, 2020). Informanter har påpekt at en lignende type sjekkliste rettet mot leverandørene bør utarbeides og komme fra NVE, slik at leverandører har samme fokus på sikkerhet når det kommer til bruk av underleverandører.

Bransjen er ikke så langt fremme når det kommer til IKT-sikkerhet da fokus har vært å sikre kraftproduksjonsanlegg fysisk, men nå brukers det digitale løsninger på andre områder enn tidligere. Mange små selskaper har ikke kapasitet og har dermed mindre fokus på IKT-sikkerhet, mens de større selskapene forsterker sin IKT-sikkerhet. Informanter mener at samarbeid på tvers av bransjen må vektlegges. Det gjelder også samarbeidet med leverandører for å løfte sikkerhetsarbeidet hos alle. I tillegg virker det å være ønskelig med veiledning fra NVE som beskriver hvordan selskaper og leverandører skal forholde seg til sikkerhet. Målet er felles sikkerhetsnivå på leveranser. Det er viktig å stille krav i anskaffelsesprosessen. *Ved å lage en sjekkliste med status som veileder eller retningslinje vil NVE involvere seg i forhold som bidrar til leverandørkjedesårbarhet.*

Mer samarbeid mellom virksomheter kan være en løsning
Mer samarbeid og kommunikasjon mellom ulike virksomheter, samt å prioritere IKT-sikkerhet vil gjøre at bransjen kommer lenger. Igjen bunner dette i ressurser og om virksomheter er villige eller har mulighet til å betale mer for bedre IKT-sikkerhet når det for eksempel bygges nye anlegg. Det oppstår et dilemma mellom sikkerhet og pris. Kundene er nødt til å forholde seg til et budsjett, og forvalte pengene på best mulig måte, med hensyn til både sikkerhet, pris, kvalitet og brukervennlighet. Hvis innkjøperen vurderer at kostnaden for mer avanserte sikkerhetssystemer overgår nytteverdien, anses det ikke som hensiktsmessig å kjøpe dyrere sikkerhetsløsninger. Samtidig ønsker leverandører at sikkerhetskravene som stilles til dem er tydeligere. Leverandørene opplever det som vanskelig å selge inn en sikrere løsning når den er dyrere, og dette kan også oppfattes av innkjøperen som et forsøk på mersalg fra leverandørens side. Den norske kraftbransjen, og norske virksomheter generelt, har opplevd få alvorlige cyberhendelser med store konsekvenser for driften, hvilket kan føre til at behovet for sikkerhetsløsninger som går utover minimumskravene ikke anses som nødvendige (Halvorsen & Selnes, 2020).

Kraftberedskapsforskriften § 6-5 omhandler anskaffelser og sier at KBO-enheter har ansvaret for at bestemmelsene om informasjonssikkerhet og taushetsplikt for kraftsensitiv informasjon ivaretas i anskaffelser. Helhetlige risiko- og sårbarhetsanalyser, som inkluderer ulike deler av organisasjonen kan være viktige verktøy i samarbeidet. DSB gir klare råd til å bruke tenkningen i NS-ISO 31000 når

utvalget presenterer sin modell for risikostyring knyttet til digitale verdikjeder. Modellen vil være nyttig i anskaffelser, så vel som under drift og vedlikehold av virksomhetenes systemer (DSB, 2020). I anskaffelsesprosesser er det viktig at innkjøp blir involvert tidlig, og at de som jobber med IKT blir inkludert av innkjøp når det gjøres anskaffelser på dette området. Noen informanter mener at innkjøpsavdelingen selv må ta ansvar for å inkludere de relevante fagmiljøene internt i virksomheten, men dette kan ikke gjøres uten solid forankring i ledelsen, og flere argumenterer for at forankring i ledelsen derfor er den aller viktigste faktoren for at samarbeid mellom fagfelt skal fungere. Å bake dette inn i arbeidspraksisene i virksomhetene er viktig, slik at ansatte har større forståelse av hverandres oppgaver og forstår helheten de er en del av. Risiko- og sårbarhetsvurderinger vil i tillegg til å være et beslutningsstøtteverktøy også være en arena for samarbeid og læring.

Systemtenkning vil sikre kontinuitet i arbeidet med leverandørkjedesårbarhet
Når det kommer til leverandørkjedesikkerhet må det gjøres mer forskning på hvilke prosesser som er mulig å kontrollere og hva som ligger utenfor virksomhetens kontroll. Informanter etterlyser mer samarbeid mellom IKT-avdeling og innkjøpsavdeling for å få et helhetlig bilde på hva som faktisk skal kjøpes og hva anskaffelsen krever av sikkerhetstiltak. Informantene vi har snakket med er delte i meningene rundt graden av kommunikasjon mellom disse avdelingene, og hvor godt de utnytter kunnskapen som finnes i de ulike fagmiljøene internt i virksomheten. Om de greier å inkludere sikkerhet hver gang det gjøres anskaffelser kan de sikre seg bedre. Det understrekes at det er en voksende oppmerksomhet rundt sikkerhet i anskaffelser, men at det ikke kan forventes at alle i bransjen har søkelyset på digital sikkerhet til enhver tid. Dette handler igjen om å bidra til en sikkerhetskultur hvor alle ansatte i virksomheten er inkludert.

I tillegg nevnes det at det ikke er realistisk å følge detaljert opp leveranser og produksjon av maskinvare. Løsningen er heller å gjennomføre hyppigere stikkprøver av produktene som blir levert. Informanter sier at det er viktig å skille mellom det som er en ren sikkerhetsanskaffelse og andre anskaffelser. Ofte er sikkerhet en del av en større anskaffelse og da må flere være med å finne de beste løsningene. Vi anbefaler at NVE bidrar til en veileder for å identifisere kritiske prosesser i anskaffelser, så vel som i ordinær drift. Disse prosessene må kontrolleres ved hjelp av funksjoner som vil identifisere utfordringer i god tid før det blir reelle problemer, slik at dette kan korrigeres på en god måte.

7.3 Kritisk blikk på risikostyringen

Tjenesteutsetting skal ikke redusere sikkerheten. Dette er krav i kraftberedskapsforskriftens § 6-9 bokstav e. Tillit til leverandører innebærer at kjøperen kan stole på at produkter og tjenester ikke kan utnyttes i fremtiden (Lysne, 2018). Programvare vil komme med en rekke sikkerhetsoppdateringer i løpet av levetiden. Oppdateringer kan utnyttes og endre operasjonaliseringen til noe uønsket. Behovet for sikkerhetsoppdateringer medfører at virksomheten må stole på leverandøren i hele levetiden til produktet eller tjenesten.

NSM påpeker at virksomhetene selv må ta ansvar for virksomhetens sikkerhet ved tjenesteutsetting. Deres ansvar for sikkerheten forsvinner ikke ved tjenesteutsetting, og de har et ansvar uavhengig av hvem som utfører de ulike oppgavene. Å ta dette ansvaret innebærer følgende:

- Å ha oversikt og kontroll på hele livsløpet til tjenesten(e) som skal settes ut.
- Å ivareta behovet for bestillerkompetanse gjennom hele livsløpet til tjenesteutsettingen.
- Gjennomføre gode risikovurderinger som inkluderer IKT og hensyntar hele livsløpet.
- Utarbeide et kravdokument for alle faser av tjenesteutsettingen hvor krav kan verifiseres.

- Avtaler om tjenesteutsetting av IKT-tjenester og endringer i slike avtaler skal behandles i henhold til virksomhetens fullmaktsstruktur.
- Det bør sjekkes at leverandøren har utviklingsplaner for fremtidig sikkerhetsfunksjonalitet i tjenestene i tråd med utvikling i teknologi og trusselbildet over tid (NSM, 2020)

Lysneutvalget gir generelle anbefalinger til risikostyring i digitale verdikjeder (DSB, 2020). Det ligger mange interessante og viktige råd til hvordan leverandørkjedesårbarhet kan møtes. Det utgis mange veiledninger som dekker risikoanalyse og risikostyring, som alle har gode intensjoner. Kunnskapen om hvordan risikoanalysene brukes og hvordan risikostyringen foregår i bransjen er imidlertid ikke like god. Her mangler vi forskningsbasert kunnskap. En hypotese er at virksomhetene i sektoren er opptatt av å tilfredsstille regelverk og at risikoanalysene er påkrevd dokumentasjon med begrenset effekt. Analysenes effekt som beslutningsstøtte handler i et slik perspektiv om anbefalte tiltak og at risiko presenteres som akseptabel. Analysene kan også være outsourcet og vil dermed ha liten læringseffekt i virksomheten. *Det bør etableres forskningsbasert kunnskap om risikostyring med hensikt å utvikle bruken av risikoanalyser i risikostyringen av sektoren.*

7.4 Kompleksitet krever sterkere systemorientering

Vi tror at alle i kraftforsyningen er enig i punktlisten over, men at dette er vanskelig å gjennomføre i praksis:

- Virksomhetene må kjenne til og ta ansvar for egne systemer.
- Virksomhetene må vite grensene til omgivelsene.
- Virksomhetene må være i stand til å kontrollere og korrigere viktige prosesser.
- Avhengighetene til leverandørkjedene må avklares.

Risikostyring gir i mange tilfeller en mekanistisk tilnærming til sikkerhetsarbeidet hvor hensikten er å oppnå risikoaksept. Sikkerhetsarbeidet er redusert til overflatiske vurderinger som ikke erkjenner kompleksiteten, som vi beskrev i kapittel 2.3. Vi behøver en helhetlig jobbing med IKT-sikkerhet – mer systemorientert tenkning (Leveson, 2011).

Systemteori er utviklet for systemer med organisert kompleksitet. Organisert kompleksitet viser til systemer som er for kompliserte for fullstendige analyser og for organiserte for statistiske vurderinger. Systemene må dermed forstås ut fra underliggende strukturer og gjelder eksempelvis samfunnsviktige funksjoner, som kraftforsyningen, samt systemer som bygger på IKT-systemer, programvare og applikasjoner. Dette krever at helheten skal være med. Visse egenskaper kan kun håndteres ved å se systemet som helhet og ta hensyn til alle sosiale og tekniske momenter. Utvikling av systemer er noe mer enn å sette sammen enkeltkomponenter. Selv om det har vært få cybersikkerhetshendelser knyttet til leverandørkjeder i samfunnsviktige funksjoner i Norge så langt, er det ikke sikkert at dette bildet vil vedvare over tid med økt digitalisering. Rammeverket i kap. 2.3 kan gjerne være et utgangspunkt for å avdekke graden av organisert kompleksitet, og dermed gi innspill til utforming av begrensninger (constraints). Kraftforsyningen trenger et rammeverk for å identifisere sårbarheter og jobbe med sikkerheten i leverandørkjedesystemet.

Systemtenkning handler om kommunikasjon og kontroll. Det er evnen til å utforme kontrollfunksjoner i kraftforsyningen som er i stand til å utøve kontroll og korrigere ved behov. Kontroll er knyttet til begrensninger som skal styre atferd eller prosessene som utøves i de ulike nivåene. Et komplekst system kan forstås som et hierarki av organiserte nivåer. Lunde og Njå (2021) har analysert norsk

snøskredberedskap, som kan tjene som et eksempel, se også (Njå, Sommer, Rake, & Braut, 2020). *Vi anbefaler at NVE tar initiativ til å utvikle rammeverket for systemtenkning sammen med virksomhetene i kraftforsyningen og øvrige enheter med ansvar for IKT-sikkerheten. Leverandørkjedesikkerhet kan på denne måten bli del av daglig arbeidspraksis og bidra til læringsprosesser som utvikler virksomhetene.*

8 Konklusjon

I denne rapporten er utfordringer og sårbarheter knyttet til leverandørkjedene i norsk kraftforsyning belyst. Vi har konsentrert rapporten om hva som er de digitale sårbarhetene i leverandørkjedene. Vi har benyttet oss av to modeller som illustrerer ulike leverandørkjeder. Den ene modellen viser en leverandørkjede med en sterk hovedleverandør, og den andre viser en mer distribuert leverandørkjede. Vi har forklart relasjonene mellom de ulike leddene i kjeden, hvilke sårbarheter og trusler som kan muliggjøre et cyberangrep eller en uønsket digital hendelse, og hvor i leverandørkjeden de ulike sårbarhetene og truslene kan ramme. Et viktig poeng å ta med seg er at sårbarheter kan finnes hvor som helst i en leverandørkjede, og at man må se leverandørkjeden som en helhet og ikke som en rekke komponenter eller tjenester som er adskilt fra hverandre.

De aller fleste virksomhetene oppgir at de har stor tillit til leverandører. I lange leverandørkjeder med flere underleverandører er man avhengig av å kunne ha tillit leverandørene, ettersom det er svært vanskelig, ressurskrevende og kostbart å holde kontroll på alle ledd i leverandørkjeden. Flere argumenterer for at det ikke er mulig. Leverandører understreker at selv om de leverer produkter og tjenester som er trygge og sikre, så er det opp til kunden å bruke produktene riktig. Her etterlyses bevissthet og ansvar fra kunden, hvor de aktivt setter seg inn i hvordan systemene fungerer og hvordan de kan driftes på sikrest mulig måte. Målet er å unngå at høy tillit til leverandører ender opp med å bli en sårbarhet. Samtidig mener kunder at de må kunne stole på at produktene de kjøper er trygge fra leverandørens side. Uavhengig av tillitsnivå må man være klar over at sikkerheten i leverandørkjeden også vil påvirke sluttbruker, altså virksomhetene selv. Informasjonen som er innhentet i forbindelse med dette prosjektet viser at det er delte meninger i bransjen om hvor sannsynlig det er at kraftbransjen vil bli utsatt for et målrettet cyberangrep, og ulik grad av bekymring knyttet til kompleksiteten i leverandørkjedene og usikkerheten som følger med mangelen på oversikt.

Informantene fremhever viktigheten av rask gjenoppretting, da det vil være utfordrende å sikre seg 100% mot hendelser. Også KraftCERT deler dette synet, da de har sett en økning i antall hendelser og en større variasjon av angrepstyper. Kraftbransjen må være forberedt på at hendelser vil ramme dem, og sikre at de er i stand til å håndtere dem. Dette er også i tråd med intensjonen i kraftberedskapsforskriften. Det blir stadig viktigere å sette inn tiltak der hvor behovet er størst, ettersom det ikke kan settes inn tiltak overalt. Det innebærer å ha en oversikt over hvilke deler av systemet som er sårbart, og som har stort behov for sikkerhetstiltak. Det er også viktig å ha redundante og resiliente løsninger og systemer som er i stand til å opprettholde en viss funksjon under påkjenninger. Når oppfatningen er at det ikke er mulig å sikre seg hundre prosent mot hendelser er det viktig å ha gode beredskapsplaner og gjenopprettingsplaner for den dagen det skjer, og øve på disse hendelsene. Volue hendelsen er et eksempel på hvordan gode planer og forberedelser hindret et angrep i å spre seg og i å påvirke andre deler av leverandørkjeden. Det er ikke lenger snakk om hvis et angrep skjer, men når det skjer. Med dagens teknologi og tilgang til ressurser, spesielt i utvalgte land eller grupper, vil det være svært vanskelig å sikre seg fullstendig mot digitale angrep, uansett hvor mye sikkerhet som bygges inn.

I tråd med et helhetlig syn på sikkerhet i leverandørkjeder, som inkluderer hele verdikjeden, er det viktig å ha et bevisst forhold til sikkerhet i anskaffelsesprosesser. Flere leverandører etterspør høyere krav til sikkerhet fra kjøper, og ønsker at de skal ta med ansvar i anskaffelsesprosessen. Dette innebærer blant annet god bestillerkompetanse på IKT-anskaffelser. Utfordringer ligger i å involvere de rette fagmiljøene dersom man ikke innehar kompetanse på sikkerhet eller IT-tjenester selv, å tenke sikkerhet hele veien, og å stille de rette spørsmålene. Leverandører og kunder har ulik oppfatning av i

hvilken grad bestillere samarbeider med IT-avdelingen, og det er også ulik praksis rundt dette. NVEs sjekkliste for tjenesteutsetting spesifiserer at teamet som er involvert i anskaffelsen skal ha nødvendig kompetanse innen sikkerhet, men det skilles ikke mellom tradisjonell sikkerhet og IKT-sikkerhet. Det kunne vært hensiktsmessig ettersom kraftforsyningen i lang tid har forholdt seg til tradisjonell sikkerhet, og bare de siste årene har hatt økt digitalisering og bruk av IKT-tjenester.

Leverandørkjedene er og vil fortsette å være en svært viktige for virksomheter i kraftforsyningen. Den kritiske samfunnsfunksjonen «kraftforsyning» trenger at det arbeides med sikkerhet i leverandørkjeder i tiden som kommer, og at utviklingen i risiko- og trusselbildet krever målrettede tiltak for god digital sikkerhet.

9 Referanser

ACER. (2021). *ACER and Cybersecurity*. Hentet fra nra.acer.europa.eu: https://nra.acer.europa.eu/en/Electricity/CLEAN_ENERGY_PACKAGE/Pages/ACER-and-cybersecurity.aspx

ACER. (2021). *Framework Guideline on sector-spesific rules for the cyber security aspects of cross-border electricity flows.* Ljubljana: European Union Agency for the Cooperation of Energy Regulators.

Claes, D. H., & Førland, T. E. (2015). *EU: mellomstatlig samarbeid og statlig system.* Oslo: Gyldendal Akademisk.

CyberSec4Europe. (2021). Aiming to safeguard values through excellence in cybersecurity. *ifip SEC2021.* Oslo: CyberSec4Europe.

DSB. (2016). *Samfunnets kritiske funksjoner.* Direktoratet for samfunnssikkerhet og beredskap.

DSB. (2020). *Risikostyring i digiale verdikjeder* . Direktoratet for samfunnssikkerhet og beredskap.

ENISA. (2021). *ENISA Threat Landscape for Supply Chain Attacks.* European Union Agency for Cybersecurity.

EPRI. (2021). *Preparing for the 2030 Energy System. Why We Need a New Cyber Security Vision.* Electric Power Research Institute.

Etikkinformasjonsutvalget. (2019). *Åpenhet om leverandørkjeder.* Oslo : Regjeringen.

European Commission. (2020). *Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union.* Brussel: European Commission.

Hagen, J. (2018). Standarder for IKT-sikkerhet - nytte i regelutvikling og tilsyn i norsk kraftforsyning. I P. Lindøe, J. Kringen, & G. S. Braut, *Regulering og standardisering: perspektiver og praksis* (ss. 231-251). Oslo: Universitetsforlaget.

Halvorsen, M., & Selnes, S. H. (2020). *Fra vær og vind til bits and bytes. En kvalitativ studie av hvordan akøtrer i den norske kraftforsyningen forstår og håndterer cyberrisiko som følge av sektorens digitale utvikling.* Stavanger: Universitetet i Stavanger.

Hollnagel, E. (2017). Å bli resilient: organisasjoner, sikkerhet og resiliens. I T. Hafting, *Krisehåndtering - planlegging og handling* (ss. 401-411). Bergen: Fagbokforlaget.

Infront TDN Direkt. (2021, juli 15). Hentet fra E24.no: https://e24.no/boers-og-finans/i/M1ozaK/volue-venter-tap-paa-inntil-40-millioner-etter-dataangrep

ITU. (2020). *Global Cybersecurity Index* . International Telecommunication Union.

Jibilian, I., & Canales, K. (2021, april 15). Hentet fra businessinsider.com: https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?r=US&IR=T

Knutsen, H. M., & Haugen, H. Ø. (2017). Utvikling i globale verdikjeder og produksjonsnettverk. I D. Jordhus-Lier, & K. Stokke, *Samfunnsgeofrai. En innføring* (ss. 95-107). Oslo: Cappelen Damm Akademisk.

Kraftberedskapsforskriften. (2012). *Forskrift om sikkerhet og beredskap i kraftforsyningen (FOR-2012-12-07-1157.*

KraftCERT. (2021). *Trusselvurdering 2021.* Oslo: KraftCERT.

Leveson, N. G. (2016). *Engineering for a safer world.* Cambridge: MIT Press Ltd.

Lysne, O. (2018). *The Huawei and Snowden Questions. Can Electronic Equipment from Untrusted Vendors be Verified? Can an Untrusted Vendor Built Trust Into Electronic Equipment?* Springer Open.

MITRE ATT&CK. (2021, August 15). *ATT&CK Matrix for Enterprise*. Hentet fra MITRE ATT&CK: https://attack.mitre.org

Mjøset, L., & Skarstein, R. (2016). Kina gjennom to globaliseringsperioder. *Agora*, 85-134.

Naume, C. (2015). *Praktiske utfordringer ved modulær produktutvikling. Erfaringer hentet fra modulbasert utvikling av et mikroavfallsforbrenningsanlegg.* . Kristiansand: Universitetet i Agder.

Njå, O., Braut, G., Rake, E., & Aanestad , R. (2012). Risk images as basis for two categories of decisions. *Risk Management: An International Journal*, 60-76.

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

Norsk Fjernvarme. (2021). *Norsk Fjernvarme*. Hentet fra https://www.fjernvarme.no/fakta/fjernvarme

NOU 2000:24. (2000). *Et sårbart samfunn - utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet.* Norges offentlige utredninger.

NOU 2015:13. (2015). *Digital sårbarhet - sikkert samfunn - beskytte enkeltmennesker og samfunn i en digitalisert verden.* Oslo: Norges offentlige utredninger.

NOU 2018:14. (2014). *IKT-sikkerhet i alle ledd - organisering og regulering av nasjonal IKT-sikkerhet.* Oslo : Norges offentlige utredninger.

NSM. (2019, september 16). *nsm.no.* Hentet fra Landvurderinger ved tjenesteutsetting av IKT-tjenester: https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/landvurdering-ved-tjenesteutsetting-av-ikt-tjenester

NSM. (2020). *Grunnprinsipper for personellsikkerhet.* Sandvika: Nasjonal sikkerhetsmyndighet.

NSM. (2020). *NSMs grunnprinsipper for IKT-sikkerhet* . Nasjonal sikkerhetsmyndighet.

NSM. (2021). *Risiko 2021 - helhetlig sikring mot sammensatte trusler.* Nasjonal sikkerhetsmyndighet.

NVE. (2017). *Regulering av IKT-sikkerhet.* Oslo : Norges vassdrags- og energidirektorat.

NVE. (2018). *IKT-sikkerhet ved anskaffelser og tjenesteutsetting i kraftbransjen.* Norges vassdrags- og energidirektorat.

NVE. (2020). *IKT-sikkerhet i anskaffelser og tjenesteutsetting i kraftbransjen - sjekkliste.* Norges vassdrags- og energidirektorat.

NVE. (2021). *IKT-sikkerhetstilstanden i kraftforsyningen 2021.* Norges vassdrags- og energidirektorat .

Nystuen, K. O. (2021). Kompleksitet i infrastruktur. *Universitetet i Stavanger.* Stavanger .

Oladimeji, S., & Kerner, S. M. (2021, april 15). Hentet fra whatis.techtarget.com: https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know

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

Reason, J. (2016). *Managing the risks of Organizational accidents.* New York: Routledge.

Riksrevisjonen. (2021). *Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen.* Riksrevisjonen.

Sæther, B. (2017). Økonomisk globalisering. I D. Jordhus-Lier, & K. Stokke, *Samfunnsgeografi. En innføring* (ss. 73-83). Oslo : Cappelen Damm Akademisk.

t'Hart, P., & Sundelius, B. (2013). Crisis Management revisited: A new agenda for research, training and capacity building within Europe. *Cooperation and Conflict*, 444-461.

Ubelhör, M. (2021, juni 24). EU cybersecurity Strategy and Capacity-building. European Comission.

Volue. (2021). *Postmorten - A Rewiev of the Cyberattack on Volue.* Volue.

10 Vedlegg

Vedlegg 1: Oversikt over hvilke temaer som er dekket i intervjuene

Informanter	Tema
Informant 1	Leverandørsikkerhet, risikobildet, komplekse produkter, ansvarsfordeling, NSMs grunnprinsipper, oversikt, sikkerhetskultur, leverandørkjeder
Informant 2	CERTs, verdikjeder, avhengigheter, kompleksitet, cybersikkerhet i digitale verdikjeder, NSMs grunnprinsipper, rapportering, anbefalinger, bestillerkompetanse, redundans, industriell teknologi, KBF
Informant 3	Leverandører, KBF, leverandørkjeder, komplekse systemer, utfordringer, sårbarheter, NSMs grunnprinsipper, bestillerkompetanse, sikkerhetskultur, resiliens
Informant 4	Leverandører, KBF, leverandørkjeder, komplekse systemer, utfordringer, sårbarheter, NSMs grunnprinsipper, bestillerkompetanse, sikkerhetskultur, resiliens
Informant 5	Leverandører som trusselaktør, oversikt og kontroll på leverandørkjeder, rapportering, ansvar, resiliens, sikkerhetskultur, risiko- og sårbarhetsanalyser
Informant 6	Leverandørkjedesikkerhet, KBF, ACER, ressurser, sikkerhetskultur, samarbeid i bransjen og med leverandører, veiledning
Informant 7	Komponenter, sikkerhetsnivå, sikkerhetskultur, kapasitet, bestillerkompetanse, IT-kompetanse, ansvarsfordeling, menneskelige feil, ressurser
Informant 8	KBF, ISO, leverandørkjeder, sikkerhetskultur, utfordringer, ansvar, IT i systemene, kompleksitet, krav, tilsyn
Informant 9	Anskaffelser, krav, trusselvurderinger, hendelser, kost-nytte-vurderinger, rapportering, ISO, NSMs grunnprinsipper, kompleksitet, transparens, usikkerhet, sikkerhetskultur, tilsyn hos leverandører
Informant 10	Bestillerkompetanse, krav, anskaffelser, kommunikasjon, IoT, rolleforståelse, ressurser, underleverandører
Informant 11	Leverandørkjedesikkerhet, sikkerhetskultur, kompleksitet, bestillerkompetanse, IT-sikkerhet, OT-sikkerhet, avhengighet

NVE

Norges vassdrags- og energidirektorat

MIDDELTHUNS GATE 29
POSTBOKS 5091 MAJORSTUEN
0301 OSLO
TELEFON: (+47) 22 95 95 95

www.nve.no