EKSTERN RAPPORT

Nr. 17/2022

Risikostyring av IKT-sikkerhet i leverandørkjeder

Ida-Kristin Johnsen og Vilde Lysgaard

NVE Ekstern rapport nr. 17/2022
Risikostyring av IKT-sikkerhet i leverandørkjeder

Utgitt av:	Norges vassdrags- og energidirektorat
Redaktører:	Janne Hagen og Birgitte Kjelsberg
Forfattere:	Ida-Kristin Johnsen og Vilde Lysgaard
Forsidefoto:	Bigstock.com, image ID: 123072218
ISBN (online):	978-82-410-2242-5
ISSN (online):	2535-8235
Saksnummer:	202216228

Sammendrag: Risikostyring av IKT-sikkerhet i leverandørkjeder har de siste årene fått økende oppmerksomhet. Leverandørkjeder blir stadig mer komplekse og tett koblet. Rapporten undersøker praksis og utfordringer i utvalgte virksomheters risikostyring av IKT-sikkerhet i leverandørkjeder.

Emneord: Risiko, risikostyring, IKT-sikkerhet, leverandørkjeder, beredskap, risikovurdering, kraftberedskapsforskriften

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

september 2022

Innhold

Figurliste

Tabelliste

Forord

Leverandørkjedesikkerhet (supply chain security) har fått økt aktualitet de siste årene. Etter tiår med globalisering og digitalisering så spenner nå digitale verdikjeder over mange landegrenser og flere kontinent. Samtidig har nettkriminaliteten økt og blitt mer sofistikert. Kriminelle fra hele verden angriper virksomheter og benytter blant annet skadevare til utpressing og for egen økonomisk vinning. I tillegg til de nettkriminelle er statlige aktører aktive ifølge NSM. Leverandører blir i økende grad rammet, samtidig som kundene til leverandøren også rammes.

NVEs myndighetsområde på sikkerhet og beredskap i kraftforsyningen er regulert av energiloven og kraftberedskapsforskriften. Kravene dekker anskaffelser og IKT-sikkerhet.

I 2021 publiserte Riksrevisjonen sin rapport om NVEs arbeid med IKT-sikkerhet i kraftforsyningen. Riksrevisjonen pekte på NVEs manglende oppfølging og kontroll av leverandørene til kraftforsyningen. NVE forvalter kraftberedskapsforskriften og fører tilsyn med virksomhetene i kraftforsyningens beredskapsorganisasjon (KBO) sin etterlevelse av forskriftskravene. Det er KBO-enheter som må sette krav til sine leverandører og kontrollere at kontrakter KBO-enhetene har inngått med leverandørene og leverandørenes underleverandører er i samsvar med regelverket. Det er KBO-enhetene som selv må drive aktiv risikostyring i leverandørkjedene sine.

NVE har i flere studier satt søkelyset på leverandørkjedesikkerhet. Dette er gjort for å framskaffe et bedre kunnskapsgrunnlag slik at risikostyringen i leverandørkjedene kan bli bedre.

Denne studien inngår i arbeidet med å forbedre kunnskapsgrunnlaget. Det er gjort en kvalitativ analyse av utvalgte virksomheters praktiske risikostyring av leverandørkjeder. Temaet er avgrenset til IKT-sikkerhet. NVE vil takke Forum for sikkerhet i kraftforsyningen for innspill og kommentarer til arbeidet, og også takke informantene som stilte opp på intervju og delte erfaring og kunnskap med NVE. NVE vil bruke rapporten som grunnlag for arbeidet med bedre og mer målrettet veiledning til forskriften for å bedre IKT-sikkerheten i kraftforsyningen.

Kristian Markegård
direktør
Tilsyns- og beredskapsavdelingen

Eldri Holo
seksjonsleder
Tilsyns- og beredskapsavdelingen

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

Sammendrag

Kraftforsyningen er en kritisk samfunnsfunksjon som er nødvendig for ivaretakelse av samfunnets behov for elektrisk kraft. Kraftforsyningens systemer blir i økende grad digitalisert ved bruk av digital teknologi og skytjenester levert av transnasjonale leverandører.

Formålet med rapporten er å bedre kunnskapsgrunnlaget om risikostyring av IKT-sikkerhet i kraftsektoren. Problemstillingen som vi har arbeidet med i rapporten er:

Hvordan praktiserer utvalgte virksomheter risikostyringen av IKT-sikkerhet i leverandørkjeder, og hvilke utfordringer eksisterer?

For å besvare problemstillingen har vi gjennomført en kvalitativ studie med semistrukturert intervju, og dokumentanalyse. Empirien baseres på fire hovedtemaer som er gjennomgående i rapporten; risikovurderinger, beredskap, risikostyring og leverandørkjeder.

Rapporten konkluderer med tjue gode måter å håndtere utfordringene på (praksiser), som er en kombinasjon av praksiser som foregår i virksomhetene i dag, og informantenes refleksjoner om hva virksomhetene burde gjøre for å oppnå en god praksis. Praksisene er forankret i figuren nedenfor, som viser faser i risikostyringsarbeidet i virksomheter. Ledelsesinvolvering påvirker alle fasene i prosessen med risikostyring, og er derfor plassert i midten.

Risikostyring av IKT-sikkerhet i leverandørkjeder vil fortsette å være viktig tema i kraftsektoren i årene fremover. Det er behov for målrettet arbeid med risikostyring, og gode praksiser nevnt i denne rapporten er et bidrag i dette arbeidet.

1 Bakgrunn

Kraftforsyningen er en kritisk samfunnsfunksjon, som er nødvendig for ivaretakelse av samfunnets behov for elektrisk kraft. Kraftforsyningens systemer blir i økende grad digitalisert ved bruk av digital teknologi og skytjenester levert av transnasjonale leverandører. I den forbindelse ble kraftberedskapsforskriften (kbf) revidert av Norges vassdrags- og energidirektorat (NVE), som innlemmet nye krav til IKT-sikkerhet. Digitalisering kan gjøre IKT-systemer i kraftforsyningen mer sårbare og bidrar til flere utfordringer, men samtidig gir det store muligheter for utvikling, innovasjon og produktivitet (NOU 2015:13; NVE, 2021c). Virksomheter i kraftforsyningen må gjøre mange avveininger for å kunne styre risiko som skal balanseres mellom å skape og beskytte verdier (Aven & Thekdi, 2022).

Risikostyring av IKT-sikkerhet i leverandørkjeder har de siste årene fått økende oppmerksomhet, og leverandørkjedene blir stadig mer komplekse og tett koblet. Energiloven stiller krav til å beskytte kraftsensitiv informasjon. Kraftsensitiv informasjon er informasjon som kan brukes til å skade kraftforsyningen (kbf § 6-2). Det er virksomhetene i kraftforsyningens beredskapsorganisasjon (KBO-enheter) som bestemmer hvem som skal ha tilgang til deres kraftsensitive informasjon, og når KBO-enheter inngår kontrakter med leverandører, kan det ofte være slik at leverandørene må ha tilgang til kraftsensitiv informasjon for å kunne levere produktet eller tjenesten. Det betyr også at leverandøren må beskytte kraftsensitiv informasjon som leverandøren er gitt tilgang til. Å beskytte kraftsensitiv informasjon, som blir håndtert av leverandører, kan være utfordrende. Følgende eksempel illustrerer dette: Dagens Næringsliv publiserte i juni 2022 en sak om kraftsensitiv informasjon på avveie. Saken gjaldt en anmeldelse av NORPEC AS, og mulig lovstridig håndtering av kraftsensitiv informasjon og bekymring for informasjonstap i forbindelse med konkursen i Jacobsen Elektro. Jacobsen Elektro var en viktig leverandør av vern og gikk konkurs i 2019. På grunn av den sentrale rollen de hadde som leverandør over lang tid, satt de på mye kraftsensitiv informasjon om vern i kraftsystemet. Dette er kraftsensitiv informasjon som er beskyttet gjennom krav til taushetsplikt i energiloven. Slik type kraftsensitiv informasjon på avveie kan være skadelig for kraftforsyningen (NVE, 2019a).

Internasjonalt finnes det flere store IKT-sikkerhetshendelser hos leverandører som også har kunder i den norske kraftsektoren. Disse hendelsene omtales som leverandørkjedeangrep. De mest kjente sakene om leverandørkjedeangrep er SolarWinds- og Volue-sakene. Disse hendelsene har bidratt til å rette større søkelys på oppfølgningen av leverandørkjeder, og hvilke betydelige konsekvenser slike hendelser kan få (NSM, 2022). Ingen av disse hendelsene har hatt betydning for kraftforsyningen eller leveransen av elektrisitet.

Flere direktorater har i sine rapporter uttrykt bekymring rundt leverandørkjedeangrep, og hvordan kompleks avhengighet mellom leverandører og underleverandører fører til store ringvirkninger for de involverte (DSB, 2020; NSM, 2022; NVE, 2021b; NVE, 2021c). I mange tilfeller vil det være enklere å utnytte leverandører eller underleverandører sine systemer for å få tilgang til sensitiv informasjon om virksomheter (DSB, 2020; NSM, 2022). NVE (2021c) sin tidligere undersøkelse underbygger disse påstandene, og ett av funnene i NVEs studie var at 8% av virksomhetene hadde opplevd uønskede IKT-hendelser i sine administrative IKT-systemer med konsekvenser for virksomhetens drift. En stor andel av de uønskede IKT-

hendelsene hadde sitt opphav hos leverandører (NVE, 2021c). Leverandørkjeder gir flere angrepsflater for datakriminelle, og det er bred variasjon i mål og teknikker som benyttes. Dette gjør arbeidet med IKT-sikkerhet i leverandørkjeder utfordrende. Risikostyring av IKT-sikkerhet i leverandørkjeder i kraftsektoren er viktig, og denne rapporten vil være et bidrag til dette arbeidet.

1.1 Formål og problemstilling

Formålet med rapporten er å bedre kunnskapsgrunnlaget om risikostyring av IKT-sikkerhet i kraftsektoren. Risikostyring av IKT-sikkerhet i leverandørkjedene i kraftsektoren er relativt lite utforsket. Studien drøfter utvalgte virksomheters praksis og utfordringer tilknyttet risikostyring av IKT-sikkerhet i leverandørkjeder. På bakgrunn av dette har vi utarbeidet følgende problemstilling;

Hvordan praktiserer utvalgte virksomheter risikostyringen av IKT-sikkerhet i leverandørkjeder, og hvilke utfordringer eksisterer?

2 Metode

I litteratursøk har vi funnet lite forskning på risikostyring av IKT-sikkerhet i leverandørkjeder i kraftforsyningen. Denne kvalitative studien er et bidrag til fagfeltet, hvor vi undersøker risikostyringen av IKT-sikkerhet i utvalgte virksomheters leverandørkjeder i kraftforsyningen. Studien bruker kvalitativ forskningsmetode, med personlige intervju og dokumentanalyse som metode for innhenting av empiri.

2.1 Utvalg av datakilder

Rapporten bygger på svar fra åtte informanter.[1] Intervjuene av informantene i ulike virksomheter gir et syn på hvordan virksomhetene forstår og arbeider med risikostyring av IKT-sikkerhet i leverandørkjeder. Informantene er anonymisert og beskrives kun som virksomhet (kraftproduksjon eller nettselskap) eller organisasjon (gir råd til virksomheter i kraftforsyningen).

2.2 Datainnsamling

Studiets primærdata er innhentet ved hjelp av intervjuer over Teams. I forkant av intervjuene ble det utformet en semistrukturert intervjuguide, med utgangpunkt i studiets hovedtemaer (se vedlegg). Spørsmålene i intervjuguiden er noe tilpasset de ulike informantenes rolle i

[1] Utvalget er basert på et strategisk utvalg (Thagaard, 2013)

kraftforsyningen. På et overordnet nivå er intervjuguidene utformet etter fire hovedtemaer; *risikovurdering*, *beredskap*, *risikostyring* og *leverandørkjeder.*

Intervjuene ble gjennomført i tidsrommet 21. juni – 1. juli 2022. Samtlige intervjuer varte i underkant av én time. Intervjuene ble gjennomført med åpenhet og fleksibilitet, og formålet var å få et innblikk i hvordan risikostyringen av IKT-sikkerhet i leverandørkjeder blir gjennomført. Personidentifiserende opplysninger ble ikke innhentet, og intervjuene ble transkribert underveis i samtalen.

Studiets sekundærdata er dokumentanalyse. Studiets eksterne dokumenter gav oss kunnskap og bakgrunnsinformasjon ved utformingen av intervjuguide, og ble under empiri benyttet for å styrke og underbygge funn fra intervjuene. Vi har benyttet offentlige kilder (rapporter, veiledere og rundskriv) og dokumenter fra NSM, NVE og DSB.

Vurdering av kilder, innsamling og data fra studien beskrives nærmere i vedlegg 7.2.

3 Kunnskapsgrunnlag

3.1 Risiko

Risiko er et begrep som blir brukt i ulike sammenhenger og fagområder. Den brede bruken av begrepet har ført til forskjellige definisjoner og forståelser. Grunnleggende handler risiko om fremtiden, om eventuelle hendelser og konsekvensene hendelsene kan medføre. Dette gjør at usikkerhet stadig blir en viktigere dimensjon ved risiko som begrep (Engen, Gould, Kruke Lindøe, Olsen og Olsen, 2021). I denne studien blir følgende definisjon av risiko benyttet: «Risiko refererer til usikkerhet om og alvorlighetsgraden av hendelser og konsekvenser (eller utfall) av en aktivitet med hensyn til noe som mennesker verdsetter» (egen oversettelse, Aven & Renn, 2010). Definisjonen inkluderer usikkerhet, samtidig om den fanger opp den subjektive dimensjonen. Dette perspektivet avviker fra den tradisjonelle tilnærmingen, og vi ser på risiko som noe annet enn bare *sanne* tall for sannsynlighet og konsekvens for en uønsket hendelse som kan inntreffe.

Digitalisering gir mange muligheter i kraftsektoren, men det fører også til sårbarheter. Ny teknologi, utenlandske leverandører, skytjenester og integrering av ulike systemer øker risikoen for IKT-hendelser i kraftforsyningen. Norge er et digitalisert og åpent demokratisk samfunn, og det er en økende forståelse for at alvorlige IKT-hendelser kan inntreffe. Risikoen er særlig tilknyttet tre forhold (NSM, 2017a):

1. Funksjoner og tjenester består av komplekse systemer samfunnet er avhengig av
2. Stadig flere angrep skjer med ulike angrepsmetoder, og aktørene bak angrepene er ressurssterke
3. Stor avhengighet mellom virksomheter som drifter kritiske infrastrukturer og kritiske samfunnsfunksjoner. Dette gir uoversiktlige verdikjeder

3.2 Risikovurdering

Risikovurderinger er et verktøy for å identifisere uønskede hendelser, forstå risikoen knyttet til aktiviteter, og vurdere betydningen av risikoen. Overordnet består risikovurderinger av en kombinasjon av risikoanalyser og risikoevalueringer. Risikovurderinger er påvirket av verdier, holdninger, egenskaper og erfaringer mennesker har. Arbeidet med risikovurderinger vil danne grunnlaget for risikostyring i virksomheter (Aven & Thekdi, 2022; Engen et al., 2021).

Risikovurderinger kan gjennomføres i henhold til anerkjente standarder for risikovurdering eller -analyse, som for eksempel ISO/IEC 27001, ISO 31000-serien, NS 5814:2021, NS 5832:2014 og IEC 62443.

Tabell 1 Oversikt over utvalgte standarder

Standard	**Beskrivelse**
ISO/IEC 27001	Internasjonal standard som er utarbeidet for å stille krav til etablering, implementering, vedlikehold og kontinuerlig forbedring av et ledelsessystem for informasjonssikkerhet (Standard Norge, 2022a).
ISO 31000	Et åpent prinsippbasert system, som brukes til å veilede organisasjoner i risikobaserte beslutninger i styring, rapportering, planlegging, ledelse, verdier og kultur (Standard Norge, 2022b).
NS 5814:2021	Stiller krav til risikovurderinger i virksomheter, og er et hjelpemiddel for å kunne ta beslutninger om tiltak eller valg av løsninger for å forebygge risiko (Standard Norge, 2021b).
NS 5832:2014	Standarden tar for seg sikringsrisikoanalyse som en del av sikringsrisikostyringen, og skal bidra til å håndtere og analysere risiko tilknyttet tilsiktende uønskede handlinger (Standard Norge, 2021a).
IEC 62443	Internasjonal standard som handler om å etablere et cybersikkerhetsstyringssystem for industrielle automasjons- og kontrollsystemer (NEK, 2020).

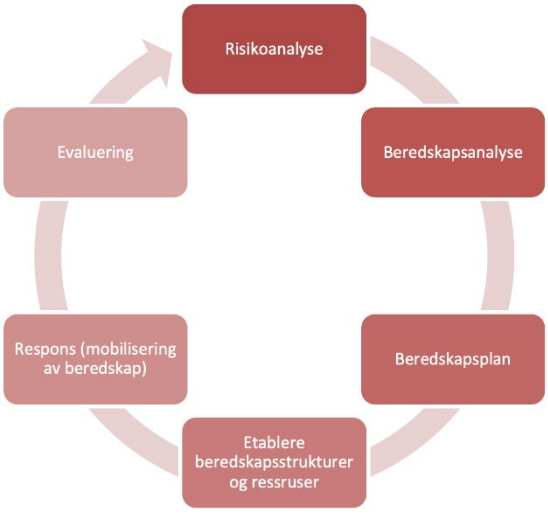
Kbf § 2-3. Risikovurdering
KBO-enheter skal gjennomføre risikovurdering knyttet til ekstraordinære forhold. Vurderingene skal ha et slikt omfang at enheten kan identifisere risiko og sårbarhet ved alle funksjoner, anlegg og tiltak av betydning for å oppfylle kravene i forskriften. Vurderingene skal minimum gjennomgås årlig og oppdateres ved behov.

Etter kbf § 2-3 skal KBO-enheter gjennomføre risikovurderinger knyttet til ekstraordinære forhold. Videre står det skrevet i kbf § 2-4 at; «KBO-enheter skal ha et oppdatert beredskapsplanverk tilpasset virksomhetens art og omfang. Planverket skal bygge på risikovurdering og skal omfatte alle beredskapstiltak etter denne forskriften». Kravene til risikovurdering gjelder også IKT. I tillegg stiller kbf § 6-9 bokstav *b* krav til risikovurdering ved systemendringer, som gjør at de må holdes oppdatert. Detaljert og utfyllende forklaring til forskriften finnes i egen veileder.[2]

3.3 Beredskap

Beredskap handler om å begrense eller håndtere uønskede IKT-hendelser og følgende av konsekvenser som oppstår, til tross for god forebyggende sikring (Engen et.al., 2021). Beredskap er en sentral del av det helhetlige risiko- og sikkerhetsarbeidet i en virksomhet. Selv om virksomhetene har utarbeidet planer betyr ikke det at de er forberedt, eller har en beredskap (Perry & Lindell 2007; Alexander, 2008). Planlegging og beredskapsarbeid bør være en kontinuerlig prosess. Fremtiden omhandler usikkerhet, og det vil være viktig å kontinuerlig planlegge for at noe kan skje eller for å unngå farer. Videre bør virksomhetene kunne håndtere og være fleksible når en hendelse oppstår, eller har skjedd.

Arbeidet med risikovurderinger, som både inkluderer risikoanalyse og risikoevaluering, er en sentral del av beredskapsarbeidet. Figur 1. illustrerer fasene i beredskapsarbeidet. Beredskapsarbeidet er en sirkulær prosess med kontinuerlig arbeid.



Figur 1: Faser i beredskapsarbeidet (Engen et at., 2021)

Etablering av sikkerhetsmål er grunnleggende for arbeidet med beredskap. Etter revidering av NS 5814 ble risikoakseptkriterier erstattet av sikkerhetsmål (Standard Norge, 2021b). Risikoakseptkriterier er «kriterier som legges til grunn ved beslutning om akseptabel risiko» (Olje- og energidepartementet, 2012). Risikoakseptkriterier kan få risiko til å fremstå som en absolutt grense for hva som er akseptabelt i en virksomhet. Ved bruk av sikkerhetsmål kan virksomheter sette søkelys på hva som er *best mulig* praksis, og ikke hva som er *godt nok*.

[2] Veiledning til kraftberedskapsforskriften - NVE

Sikkerhetsmål defineres av Standard Norge (2021b) som; «Fastsatte mål for ivaretakelse av verdier». På bakgrunn av risikovurderingen som utføres, bør virksomhetene kartlegge interne og eksterne krav som stilles til sikkerhet, og definere sikkerhetsbehovene (NSM, 2020d). Kravene gir føringer for hvordan virksomhetene skal oppnå sine sikkerhetsmål, og hva det skal etableres en dimensjonerende beredskap for.

3.4 Risikostyring og sikring

Risikostyring handler om å utvikle og skape verdier, samt ha et forsvarlig sikkerhetsnivå for å unngå ulykker, skader og tap (NSM, 2020b; Aven, 2007). Aven og Thekdi (egen oversettelse, 2022) definerer risikostyring på følgende måte; «Risikostyring refererer til anvendelse av styringsprinsipper for håndtering av risiko, knyttet til aspekter som deltakelse, ansvarlighet, effektivitet, koherens og proporsjonalitet». I denne rapporten ser vi på risikostyring som «koordinerte aktiviteter som styrer og kontrollerer mot virksomhetenes mål, med tanke på risiko».

Virksomheter kartlegger og styrer risiko ved å benytte ulike strategier, metoder og prosesser. Ifølge kbf § 6-9 skal virksomheter har en grunnsikring for digitale informasjonssystemer i henhold til anerkjente standarder og normer. NSM sine grunnprinsipper for IKT-sikkerhet og internasjonale standarder, med utspring i ISO/IEC 27000-serien, er viktige rammeverk for virksomheters arbeid med systematisk risikostyring.

3.4.1 Kbf§ 6-9

§ 6-9 Digitale informasjonssystemer
Virksomheter skal sikre digitale informasjonssystemer slik at konfidensialitet, integritet og tilgjengelighet ivaretas. Det er den enkelte virksomhets ansvar å planlegge, gjennomføre og vedlikeholde sikringstiltak etter det digitale informasjonssystemets type, oppbygning og funksjon. Virksomheter skal ha en grunnsikring for digitale informasjonssystemer i henhold til anerkjente standarder og normer (…).

Kbf § 6-9 bygger på NSM sine grunnprinsipper. § 6-9 bokstav *a*, *c* og *d* vil særlig være relevant i denne rapporten. Bokstav *a* omhandler å *identifisere og dokumentere*. Det er viktig å ha oversikt over systemer, programvare, tjenester mv. for å kunne følge opp de øvrige sikringskravene i NSMs grunnprinsipper, og sikkerhets- og risikostyringen. Det handler om å opparbeide en forståelse av virksomhetens IKT-systemer, styringsstrukturer, leveranser og funksjoner. I tillegg er det relevant å vurdere iverksatte sikringstiltak opp mot virksomhetenes sikkerhetsmål og tiltak. Bokstav *c* handler om å *sikre og oppdage*. Det innebærer at uønskede og sikkerhetstruende hendelser blir oppdaget, og sårbarheter og trusler blir minimert eller fjernet. Punktet er nært koblet til kraftsensitiv informasjon, personopplysninger eller gradert informasjon. Bokstav *d* innebærer å *håndtere* uønskede hendelser som oppstår, og *gjenopprette* funksjonaliteten til en normaltilstand. Med andre ord beskriver bokstav *d* digital beredskap, og grunnprinsipper som blir inkludert er blant annet vurdering, kontrollering og evaluering av hendelser.

3.5 Leverandørkjeder

Tidligere studier har vist at sikkerheten i leverandørkjeder har blitt en stor utfordring (NVE, 2021b; Ponemon Institute, 2019; Riksrevisjonen, 2021). I forskningsrapporten til Ponemon Institute (2019) var leverandørene inngangsporten for angriper til over 63% av dataangrepene. KraftCERT ser en økende trend i angrep mot leverandører, partnere og kunder. Lange digitale verdikjeder med sammensatte avhengighetsforhold og komplekse samhandlingsmønstre har også ført til større angrepsflate mot kraftsektoren. Digital verdikjede defineres som «en struktur av leveranser mellom virksomheter, hvor hver leveranse enten er en digital tjeneste, software eller hardware» (DSB, 2020). Sårbarhet kan oppstå i alle ledd, og forplante seg videre i verdikjeden, noe som kan føre til at virksomhetene blir mer utsatt for IKT-trusler (NOU 2015:13). Sårbarheter i leverandørkjeder kan oppstå ved uønskede hendelser fra både eksterne aktører med tilsiktede intensjoner, eller ved teknisk eller menneskelig svikt. I sammenkoblede IKT-systemer kan sårbarheten enklest utnyttes gjennom det svakeste leddet. Det er derfor grunnleggende å tenke helhetlig og inkludere alle deler av systemene når aktører gjennomfører risikovurderinger i verdikjeder og leverandørkjeder (NVE, 2017).

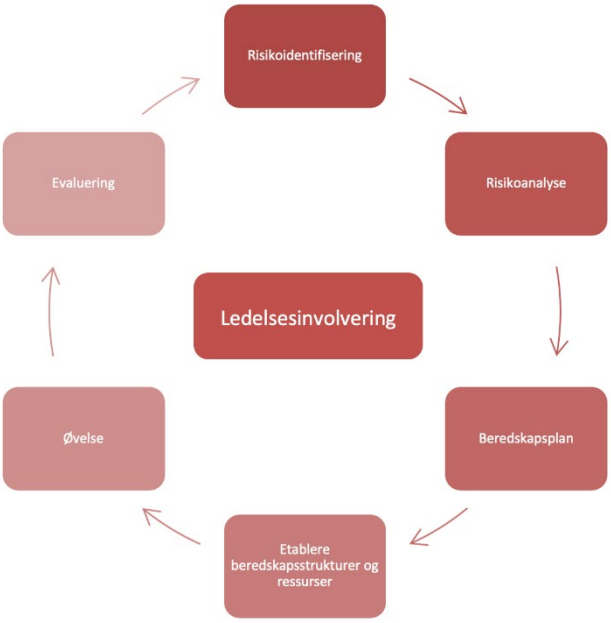
Leverandørkjeder er komplekse og uoversiktlige. Det gjør at sårbarheter og utfordringer i kjedene er vanskeligere å oppdage. NVE (2021b) har i en tidligere rapport beskrevet at risikostyring i leverandørkjedene er utfordrende. Risikostyring av leverandørkjeder handler f.eks. om evnen til å identifisere leverandører eller underleverandører som har størst potensial for å bli utsatt for et angrep eller en uønsket hendelse. Etter å ha identifisert svakhetene i systemet, blir neste skritt å håndtere hyppigheten eller påvirkningen av de uønskede hendelsene i leverandørkjeder (Trkman & McCormack, 2009). Styring av risiko i leverandørkjeder blir påvirket av svært forskjellige faktorer, og det kreves dermed ulike tilnærminger for ulike leverandørkjeder. Leverandører og underleverandører kan operere i ulike markeder, miljøer og transnasjonalt. Styring av risiko i én del av leverandørkjeden, trenger ikke å være lik i en annen del av leverandørkjeden. Faktorene kan ha ulik vekt og betydning hos ulike leverandører.

4 Risikostyring av IKT-sikkerhet i leverandørkjeder

Kapittel fire vil forklare det teoretiske rammeverket opp mot empiriske funn og analyse. Empirien tar utgangspunkt i temaene; *risikovurdering, beredskap, risikostyring og leverandørkjeder*. Datagrunnlaget er hentet fra intervju og dokumentanalyser. Ved å se sammenhenger mellom teori, eksterne dokumenter, lovverk og informantenes utsagn, vil vi få et overblikk over hvilke praksiser virksomhetene benytter og hvilke utfordringer virksomhetene står overfor tilknyttet risikostyring og leverandørkjeder.

Vi har utarbeidet Figur 2: *Risikostyring i virksomheter*, som viser hvordan risikostyring foregår som en kontinuerlig prosess i virksomhetene. Fasene innehar ulike egenskaper, men det er

viktig å se alle fasene i sammenheng, da de har noe overlapp og er en sammensatt prosess. Funnene i rapporten blir sett i lys av fasene presentert i Figur 2.



Figur 2: Risikostyring i virksomheter

Første fase i prosessen er *risikoidentifisering* (øverste boks i figur 2). Det innebærer bl.a. å innhente kunnskap om risikobildet, og identifisere trusler og farer. Den andre fasen er *risikoanalyse* (høyre boks øverst i figur 2), hvor det gjennomføres en systematisk beskrivelse og gjennomgang av identifiserte risikoer. Risikoer blir vurdert ut ifra sårbarhet, sannsynlighet, konsekvenser og usikkerhet (Aven & Renn, 2010). Den tredje fasen er utarbeidelse av *beredskapsplan* (høyre boks nederst i figur 2). Planen beskriver hvordan og hvem (funksjoner eller personer) som skal håndtere en uønsket hendelse, samt dimensjonering av beredskapen. Den fjerde fasen er *beredskapsstrukturer og ressurser* (nederste boks i figur 2). Fasen beskriver hvilke beredskapsstrukturer som må etableres, samt kartlaglegging av interne og eksterne tilgjengelige ressurser (Engen et.al., 2020). Den femte fasen er *øvelser* (nederste boks til venstre i figur 2). Trening og øvelser bidrar til å teste og videreutvikle systemer, kompetanse, funksjoner, og for å effektivt gjennomføre tiltak og endringer i virksomheten (DSB, 2018). Siste fasen i figuren er *evaluering* (øverste boks til venstre i figur 2). Når uønskede hendelser er håndtert, eller man har gjennomført øvelser, er det viktig at virksomhetene lærer av hendelsene. Lærdommen fremskaffes best gjennom evaluering for å identifisere nye risikoer og oppdatere eksisterende planverk. Fasen med *ledelsesinvolvering* er plassert i midten av figur 2 fordi ledelsen må være involvert i alle fasene i risikostyringsarbeidet for å ha kontroll med virksomheten. Det er avgjørende at ledelsen tar eierskap til og involverer seg i sikkerhetsarbeidet i egen virksomhet, ifølge NSM (2020).

4.1 Risikovurdering

Den overordnede digitale risikoen blir vurdert av samtlige informanter til å stamme fra trusler som kan påvirke kraftforsyningen og virksomheter sin manglende evne til å levere strøm. Mer spesifikt trekker to av virksomhetene frem skadevare, nettverksoperasjoner og informasjonslekkasje som digitale risikoer virksomhetene er særlig bekymret for. En av organisasjonene nevner i tillegg leverandørkjeder, som henger nøye sammen med den digitale risikoen

Risikovurderingene blir av tre virksomheter gjennomført med bakgrunn i bl.a. tjenesteutsetting, anskaffelser, eller nyetableringer og større endringer. Tre av virksomhetene tar utgangpunkt i veiledere og standarder. Veiledere fra FSK og NVE, samt sårbarhetsvarsler fra KraftCERT, trusselvurderinger fra NSM, E-tjenesten og PST, bidrar til et rammeverk for virksomhetenes egne risikovurderinger. Kraftberedskapsforskriften, ISO 27005 og NSM sine grunnprinsipper blir nevnt som sentrale hjelpemidler. En virksomhet benytter i stor grad interne krav og metodikk, samt relevant lovverk. Samtlige av studiets virksomheter benytter dermed relevante lover og regelverk ved gjennomføring av risikovurderinger.

Virksomhetene involverer både interne og eksterne ressurser ved utarbeidelse av risikovurderinger. Interne ressurser blir hentet fra ulike avdelinger i virksomhetene, som IKT-personell, teknisk personell, informasjonseiere og beredskapskoordinatorer. Eksterne ressurser er leverandører og samarbeidspartnere, og de blir involvert ved spesielle hendelser. For en av organisasjonene er den største påvirkningen på virksomhetenes risikovurderinger å løfte tematikken høyt på agendaen internt og hos ledelsen. To av organisasjonene bistår virksomheter med risikovurderinger etter ønske, og dirigerer i riktig retning.

Én av de store bekymringene for en av organisasjonene er manglende kompetanse blant virksomhetene til å vurdere dagens risikobilde. Manglende kompetanse er påpekt av både NVE (2021c) og Riksrevisjonen (2021). Virksomhetene er avhengige av å gjennomføre risikovurderinger for å identifisere og forstå risikoer til aktiviteter, og vurdere betydningen av risikoene. Manglende relevant kompetanse om forebyggende sikkerhet utgjør en sårbarhet i virksomhetene (NSM, 2021). Basert på to av organisasjonene sine erfaringer, har de mindre virksomhetene bedre oversikt og kontroll over egne IKT-systemer enn de større virksomhetene, og de evner i stor grad å sikre IKT-systemene mot inntrengning. Dette kan tolkes som at større virksomheter har mer omfattende og komplekse IKT-systemer der grensesnittene særlig kan være uklare. Det kan også tolkes som at tilgangen er begrenset til en liten gruppe personer som kjenner hverandre. Sikkerhetsbrudd gjennom personer kan dermed i større grad begrenses.

En av organisasjonene opplever det motsatte, og hevder at mindre virksomheter ikke har like god kompetanse og kontroll på IKT-systemene som de store virksomhetene. Organisasjonen mener at de mindre virksomhetene har færre ressurser og større utfordringer knyttet til prioriteringer. Ved å være få ansatte i en virksomhet, vil ansatte ofte ha flere roller i virksomheten. Dette kan gå på bekostning av kompetansen.

Virksomheter med få ansatte har vanligvis god breddekompetanse, men lite spesialistkompetanse på utvalgte deler av IKT-systemet. I større virksomheter kan forholdet derimot være motsatt, dvs. at de har god spesialkompetanse, men få med god

generalistkompetanse. Å få gode generalister forutsetter at virksomheter har gode indre prosesser for kompetansedeling på spesialistområdene. Gode indre prosesser for kompetansedeling vil gjøre virksomheter mindre sårbare når ansatte med spesialistkompetanse slutter i sin stilling.

Risikoen for at virksomheter ikke er i stand til å beskytte viktige verdier øker i takt med det komplekse risikobildet i kraftforsyningen (NSM, 2022). Statlige aktører er villige til å angripe og skade virksomhetene, og det er viktig at dette blir tatt med i betraktningene om risiko. Det er i dag stor usikkerhet knyttet til krigen i Ukraina, og videre utvikling i den geopolitiske situasjonen og sikkerhetssituasjonen i Europa. IKT-hendelser kan ramme deler av kraftsektoren i Europa, Norge er intet unntak. Det dagsaktuelle trussel- og risikobildet er ifølge en virksomhet viktig å se i sammenheng med virksomhetens verdier. NSM (2022) skriver at «statlige trusselaktører viser en økende vilje til å utnytte sårbarheter (…)». Det er én av grunnene til at samme virksomhet også nevner viktigheten av å sikre kommunikasjonsveier, passord og utstyr. Det er viktig å hindre at uvedkommende får til tilgang til dokumenter og sensitiv informasjon. Å gjennomføre detaljerte risikovurderinger internt i virksomheten kan motvirke de nevnte truslene. To av virksomhetene mener risikovurderinger også vil være aktuelt ved større endringer, nyetableringer og anskaffelser, slikt at vurderingene er tilpasset de raske endringene i dagens samfunn.

Det er viktig å understreke at det å *evaluere* risikoen er vel så viktig som det å identifisere og analysere risiko. Det er en del av risikovurderingen.

4.2 Beredskap

Ifølge kbf §§ 1-5 og 2-4 er det lovfestet at virksomheter skal ha en oppdatert beredskapsplan som bygger på risikovurderinger. Beredskapsplanen skal bidra til å «forebygge, håndtere og begrense virkningene av ekstraordinære situasjoner (…)» kbf § 1-5. Alle virksomhetene påpeker at det er en direkte og tett kobling mellom risikovurderinger og digital beredskap. Tre av virksomhetene mener at beredskapsplanen blir oppdatert kontinuerlig, og at den er et dynamisk dokument (se Figur 2). Beredskapsplanen bygger på sjekklister og utvalgte risikoer som er identifisert. En virksomhet forteller i tillegg at IT-avdelingen har en egen innsatsplan som baseres på identifiserte risikoer, og denne innsatsplanen er knyttet til den sentrale beredskapsplanen for virksomheten. To av virksomhetene mener bruk av innsatsplaner knyttet til konkrete hendelser er viktig.

Det eksisterer et komplekst og dynamisk risikobilde, og informantene mener virksomhetene har en beredskapsplan som er dimensjonert for kompleksiteten. To av virksomhetene nevner at de har standardiserte, generelle lister og prosedyrer, men at de kontinuerlig oppdateres med spesifikke risikovurderinger. For å innhente oppdatert kunnskap og informasjon, benytter virksomhetene både interne og eksterne kilder. Det nevnes f.eks. KraftCERT, PST, NSM og andre aktuelle fagforum. Interne prosesser som blir benyttet er bl.a. evalueringer og erfaringsmøter etter øvelser og hendelser (se Figur 2), egne overvåkningssystemer, og møter med leverandører og underleverandører. Videre tilrettelegger og deler alle organisasjonene kunnskap med virksomhetene. En av organisasjonene mener det er viktig å stille kritiske spørsmål til virksomhetene om hva de gjør, hva de har gjort, og hva de har lært. Repetisjon, og det å sette beredskapsarbeidet høyt på agendaen, er også nødvendig. En annen organisasjon

mener innsatsplaner har stor verdi for virksomheter. Innsatsplaner dekker de hendelsene som er mest vanlige i dagens komplekse risikobilde.

Beredskap henger nøye sammen med sikkerhetsmål som blir satt mellom virksomhet og leverandør. Samtlige av virksomhetene har etablert enten risikoakseptkriterier eller sikkerhetsmål for leverandørene. Hvordan kriteriene er utformet og kategorisert er derimot forskjellig. En av virksomhetene benytter en matrise for å kategorisere lav, middels og høy risiko, som er en beskrivelse av risikoakseptkriterier. Å benytte en matrise er fortsatt gjeldende i virksomheten. Virksomheten gir som et eksempel på risikoakseptkriterier utarbeidelse av policy for informasjonssikkerhet. Der stilles det krav til kryptering, lagring, overføring, krav til sikker utvikling osv. Virksomheten følger opp risikoakseptkriteriene gjennom skjema som leverandører må underskrive. Deretter utformes det en kontrakt som risikoakseptkriteriene er en sentral del av. Etablering og oppfølging av risikoakseptkriterier foregår på liknende måte i en av de andre virksomhetene. De har utarbeidet et internt rammeverk hvor det stilles kriterier til IKT-systemer. Kriteriene vil variere ut ifra hvilket system det gjelder, men det finnes flere kriterier som er standard. Oppfølging av risikoakseptkriteriene skjer allerede når leverandører responderer på anbud og forespørsler. Da vil virksomheten ha en gjennomgang med leverandøren for å etablere forståelse rundt eventuelle spørsmål, og leverandøren må dokumentere at de forstår. Kartlegging av kriterier etablerer en forståelse for risikoer og verdier, og det hjelper virksomheter med å bygge og opprettholde en beredskap. Etter at avtale er inngått, er det ideelle å gjennomføre revisjoner, men i praksis er det et arbeid som blir nedprioritert. Oppsummert tyder funnene på at flere virksomheter fortsatt benytter risikoakseptkriterier som ny standard fra Standard Norge anbefaler å gå bort fra.

Som en del av beredskapsarbeidet gjennomføres det øvelser i virksomhetene (se Figur 2). Øvelser bør ha som formål å sette søkelys på og teste beredskapsplanen, ansatte, prosedyrer, utstyr og ressurser (NSM, 2020a). Kbf § 2-7 stiller krav til at det øves på ekstraordinære situasjoner. Det er et bredt spekter av ekstraordinære hendelser som kan ramme virksomhetene, bl.a. IKT-hendelser og teknisk svikt. Informantene vektlegger at det bør gjennomføres ulike typer øvelser. En av virksomhetene holder diskusjonsbaserte øvelser (skrivebordsøvelser) med relevante personer fra leverandører og virksomheten. En diskusjonsbasert øvelse gir mulighet til å teste den teoretiske evnen til en gruppe, som skal reagere på en gitt situasjon og arbeide med problemstillinger etter innspill fra øvingsleder. Det kan øves på blant annet grensesnitt, planverk og rutiner (Statsforvalteren, 2014). Denne formen for øvelse er en indikator for virksomheten for å vurdere om resultatet av øvelsen er i tråd med forventningene. Hvis øvelsen ikke er i tråd med forventningene, gir det virksomheten mulighet til å redusere avviket mellom resultatet av øvelsen og øvingsmålene.

En av virksomhetene gjennomfører spilløvelser og funksjonsbaserte øvelser av IKT-systemene i samarbeid med sine leverandører. Øvelsene omhandler håndtering av uønskede hendelser, hvor målet er å sjekke at kompleksiteten faktisk kan overleve en hendelse med bidrag fra en tredjepart. Øvelser blir av informantene generelt beskrevet som svært relevant for å tilpasse beredskapsplanen til dagens komplekse risikobilde, og som et verktøy for å innhente og dele oppdatert kunnskap. Selv om øvelser varierer i omfang og ressursbruk, anses det som en viktig del av beredskapen som må bli prioritert i virksomhetene. Ledelsen må sikre tilstrekkelig risiko- og sikkerhetsforståelse i hele virksomheten. Dette gjøres gjennom opplæring av egne ansatte,

samt sørge for at leverandører, underleverandører og andre oppdragstakere har en god risiko- og sikkerhetsforståelse (NSM, 2020c). Øvelser en viktig fase i Figur 2. Virksomhetene må prioritere øvelser tilknyttet IKT-systemer i større grad, for å bli bedre rustet til å håndtere reelle hendelser som kan oppstå i fremtiden.

4.3 Virksomhetenes praksiser

4.3.1 Risikostyring

Det er konsensus blant informantene at begrepet risikostyring handler om å ha et styringssystem, som gir kontroll og oversikt over risikoer, trusler og sårbarheter. Risikostyring blir beskrevet som et kontinuerlig arbeid, og en del av den daglige aktiviteten i virksomhetene. En av virksomhetene nevner viktigheten ved å ha oversikt over krav til risikostyring, og kontrollere etterlevelse og oppfyllelse av kravene. En annen virksomhet mener det er viktig å huske at all risiko ikke kan elimineres, og det vil derfor være sentralt for virksomhetene å jobbe med å finne en risikoaksept som de er komfortable med å håndtere. Organisasjonene vektlegger betydningen av at virksomhetene har oversikt og forstår egen IKT-situasjon og utfordringsbilde. På denne måten kan virksomhetene sette opp og gjennomføre tiltak. To av organisasjonene arbeider med å påvirke virksomhetenes risikostyring med å avmystifisere IKT-arbeidet, slik at de ansatte er i stand til å forstå det helhetlige arbeidet med risikostyring av IKT-sikkerhet.

Informantene nevner flere faktorer som sikrer god risikostyring i virksomhetene. En av organisasjonene mener bevisstgjøring av alle ansatte er én faktor som er grunnleggende praksis for risikostyring av IKT-sikkerhet. Ved å ha god bevissthet innebygget i den daglige risikostyringen, vil det ifølge en av de andre organisasjonene forplante seg videre til andre områder av virksomheten. Risikovurderings- og beredskapsarbeidet nevnes eksplisitt i denne sammenheng. Samtlige av virksomhetene mener de har en bevissthet og god kultur rundt risikostyring av IKT-sikkerhet. Det innebærer at alle de intervjuede virksomhetene styrer etter risikoakseptkriteriene som virksomhetene selv har satt. En annen faktor som sikrer god praksis for risikostyring er utarbeidelse av rammeverk med tilhørende sjekkpunkter, rutiner, prosedyrer og metoder. For å utarbeide rammeverk er det avgjørende med lederforankring av IKT-sikkerhet, hvor det er definert hva som er risikoaksepten for virksomheten, mener en av virksomhetene.

Samtlige organisasjoner synes å ha et noe mer pessimistisk syn på praktisk risikostyring i virksomhetene. En av organisasjonene mener mange virksomheter har en lang vei å gå når det gjelder bevisstgjøring av risikostyring av IKT-sikkerhet, men nevner det skal lite til for å forbedre praksisen. Selv om virksomhetene har stort forbedringspotensial når det gjelder risikostyring, mener to av organisasjonene at virksomhetene har en god oversikt over egne systemer. I tillegg sier de samme organisasjonene at det ikke er så stor forskjell mellom små og store virksomheter. Små virksomheter har mindre komplekse IKT-systemer, som vil si at oversikten og kompetansen er tilpasset virksomhetens systemer. Store virksomheter har mer komplekse IKT-systemer, men har flere ressurser og mer kompetanse tilgjengelig.

Alle informantene uttrykker at risikostyring i virksomhetene er forankret i ledelsen. Det er i samsvar med Figur 2, hvor ledelsesinvolvering påvirker alle fasene i risikostyringsprosessen. Informantene har derimot ulike oppfatninger av hvilket ledernivå arbeidet bør foregå på. Kbf § 1-4 viser til at; «Leder for virksomheten som er omfattet av denne forskrift, har ansvar for at virksomheten er organisert og har funksjoner og ressurser slik at virksomheten er innrettet for å oppfylle kravene i energiloven kap. 9 (…)». Ledere er viktige for arbeidet med risikostyring. Ifølge NSM (2020) bør toppledelsen fokusere på organisatorisk risiko i virksomheten. Det vil være avgjørende at de tar eierskap til og involverer seg i sikkerhetsarbeidet i egen virksomhet. Dette arbeidet kan ta utgangpunkt i NSM sine grunnprinsipper. På denne måten kan virksomheten beskytte informasjonssystemer mot uautorisert tilgang, misbruk og skade (Kbf; NSM, 2020).

Tre av virksomhetene mener de involverer riktig ledernivå i arbeidet. De argumenterer for at risikostyring er forankret på et ledernivå med bakgrunn i hvilken type trussel eller risiko virksomheten står overfor. Hvis det gjelder trusselbildet på et generelt nivå, viser en av dem til CISO (chief information security officer) og konserndirektøren som aktuelt ledernivå. Ledere med ansvar for IT-tekniske løsninger har ansvar for den daglige risikostyringen på et lavere ledernivå. Det inkluderer bl.a. prosjekteiere, prosjektledere, risk-avdeling, beredskapskoordinator/-leder, og driftssentral.

Samtlige av informantene mener risikostyring og endringsledelse henger nøye sammen. Ifølge kbf § 6-9 bokstav *b* skal virksomheter «gjennomføre risikovurdering ved systemendringer. Risikovurderingen skal holdes oppdatert». Det innebærer at endringer i IKT-systemer krever risikostyring, som igjen forutsetter endringsledelse. En av organisasjonene beskriver risikostyring som en grunnleggende arbeidsoppgave i virksomheten, fordi en til enhver tid må se fremover mot mulige nye risikoer. Dette er i tråd med kbf § 6-9. Endringsledelse vil være en sentral del av denne prosessen, og det er essensielt for å endre tankesett og handlingsmønster i virksomheter. Likevel er det ikke like enkelt i praksis. Organisasjonen mener også at den største svakheten i virksomheter på dette området er at ledere har kunnskap, men ikke evne til handling. Det er også i tråd med en av de andre organisasjonene sine utsagn om utfordringer med å utøve teori i praksis. NVE (2021b) sin tidligere rapport underbygger denne påstanden.

4.3.2 Leverandører

Det er ulik praksis i virksomhetene når det gjelder risikostyring av IKT-sikkerhet i leverandørkjeder. En virksomhet informerer om at de ikke har et register over leverandører, men at det er under utarbeidelse. En annen av virksomhetene har derimot allerede utviklet et register hvor det er god oversikt over både leverandører og underleverandører. Virksomhetene trenger en form for godkjenning, sikkerhetsklaring, sertifisering eller loggføring av leverandører for å etablere oversikt ifølge en av organisasjonene. Det kan være aktuelt å regulere antall underleverandører i kontraktene som blir inngått. Disse løsningene kan bidra til å etablere den etterspurte oversikten for virksomhetene, og det kan være sentralt for virksomhetenes mulighet for praktisk risikostyring i leverandørkjeder.

Under intervjuene kommer det frem at det optimale er å gjøre risikovurderinger av IKT-systemene til leverandørene, som gir virksomhetene bedre mulighet til å følge opp risikostyring av IKT-sikkerhet i leverandørkjeder. To av virksomhetene nevner eksplisitt at det

gjøres risikovurderinger av skytjenester. Bruk av skytjenester er utbredt blant norske virksomheter, hvor gamle IKT-systemer ofte blir erstattet av skytjenester (NSM, 2021). Skytjenester bidrar til mer komplekse og, som følge av kompleksiteten, også sårbare leverandørkjeder. Skytjenester bidrar samtidig til økt robusthet ved at data lagres på ulike servere og geografiske steder. Dette gjør det relevant for virksomhetene å gjennomføre risikovurderinger av skytjenester. Virksomhetene benytter veiledere fra FSK (2021) og NVE (2020), samt oppdatert varsling, informasjon og kunnskap fra KraftCERT, NSM, E-tjenesten og PST i arbeidet med risikovurderinger. ISO-standarder, krav i kbf og NSM sine grunnprinsipper er også sentrale hjelpemidler.

Praksis for kunnskaps- og erfaringsdeling varierer blant virksomhetene. To av virksomhetene deler informasjon og erfaringer på tvers av virksomhetene med leverandører. En av de andre virksomhetene driver ikke med kunnskapsdeling om IKT-sikkerhet med sine leverandører. Informanten forteller at virksomheten burde vært mer aktiv ut mot leverandørene sine. Samtlige informanter utveksler informasjon gjennom KraftCERT. KraftCERT anerkjennes som en god arena for utveksling av informasjon på tvers, og en av virksomhetene sier det er avgjørende å være aktiv i fagmiljøer hvor det diskuteres og informasjon deles. Alle organisasjonene understreker dette poenget ved å uttrykke at virksomheter i kraftsektoren er noe fragmentert, og de har et ønske om at sektoren i større grad samles til en felles praksis. Det kan gjøre virksomheter og leverandører mer opplyst og bevisst på rammebetingelser, sikkerhetsmål og tiltak for risikostyring av IKT-sikkerhet i leverandørkjeder.

En av organisasjonene mener det burde være større søkelys på samarbeid om felles sikkerhetsrevisjoner i kraftsektoren, når det gjelder leverandørkjeder. Det blir eksemplifisert med at mange virksomheter har samme underleverandører, men det er ikke felles samarbeid om sikkerhetsrevisjoner. Det er mange virksomheter som fortsatt står alene.

4.4 Utfordringer tilknyttet risikostyring

4.4.1 Ressursmangel

Virksomhetene trekker frem flere utfordringer knyttet til risikostyring av IKT-sikkerhet. Fire av informantene opplever å få bevilget nok økonomiske midler til arbeidet med risikostyring, men en vesentlig utfordring er mangel på menneskelige ressurser med kunnskap og praktiske ferdigheter. Tre av de samme virksomhetene synes det er vanskelig å følge opp risikoanalyser og tiltak i praksis, og det med bakgrunn i at både tid og menneskelige ressurser ikke strekker til. Risikostyring av IKT-sikkerhet må ikke bli et *venstrehåndsarbeid*, men når det er en kamp om de menneskelige ressursene hjelper det ikke om viljen og evnen er til stede, uttrykker en av dem.

Ved mangel på menneskelige ressurser, mener en av virksomhetene at det er utfordrende med regelverk og informasjonssikkerhetsavtaler som dekker bredt nok og ikke er tydelig definert. Det vil dermed være utfordrende å forholde seg til f.eks. innkjøpsprosesser, hvor virksomheten bruker mye tid på å gå bredt ut. Virksomheten har et ønske om mer konkrete regelverk og avtaler, slik at det er lettere å unngå unødvendig arbeid for ansatte.

I mange studier er ressursmangel en gjentakende utfordring for arbeidet med risikostyring (Riksrevisjonen, 2021; NVE, 2021b). Som illustrert i Figur 2, er kartlegging av tilgjengelige ressurser en del av prosessen med risikostyring i virksomheter. Det gjelder kartlegging av både interne og eksterne ressurser. For virksomhetene er det viktig å forstå at risikostyring handler om å bruke de ressursene som er tilgjengelig på en mest mulig effektiv måte. Virksomhetene vil *aldri få nok* ressurser, og arbeidet må derfor tilpasset deretter.

4.4.2 Eierskap til risikoer

En av virksomhetene synes det er utfordrende å få avdelinger i virksomheten til å forstå at de må ta eierskap til risiko. Informanten uttrykker at kraftsektoren er i endring når det gjelder å eie risiko, og at kraftsektoren har mye å lære av andre sektorer – f.eks. finans- eller forsvarssektoren. I disse sektorene har digitalisering vært en sentral del i mange år, og digitaliseringsløpet generelt har kommet mye lenger enn i kraftsektoren. Kraftsektoren er i utvikling, og det innebærer at avdelinger må eie risikoen for informasjon og tjenester de benytter. Virksomheten uttrykker videre hvor lett det er for ulike avdelinger hos dem å tenke på IT-avdelingen som ansvarlig for risiko, men dette er ikke tilfellet. Eiere av systemer må være bevisst på risikostyring, og hvordan systemene skal beskyttes med rådgivning fra sikkerhetspersonell.

4.4.3 Mangel på transparens i programvare-leverandørkjeder

Risiko i programvare er lite transparent for brukere av applikasjonene. Programvare og kode er utviklet av ulike personer og programvareleverandører og senere bygget inn i applikasjoner som benyttes av virksomheter. Dette gjør at sårbarheter som eksisterer i kode utviklet i en tidsperiode til ett formål, kan bli del av applikasjoner som utvikles senere og brukes av mange brukere til annet formål. Mange «kokker» og mangel på transparens øker risikoen. Log4J hendelsen illustrerer risiko knyttet til denne måten å utvikle applikasjoner på. 9. desember 2021 ble det publisert informasjon om en kritisk sårbarhet i loggverktøyet Apache Log4j. Sårbarheten var under aktiv utnyttelse også i Norge av kryptoutvinnings- og andre avanserte aktører. Det var viktig å iverksette tiltak for å hindre at flere virksomheter ble kompromittert, og NSM ga ut veiledning om hvordan virksomhetene kunne rette feil og redusere risikoen (NSM, 2021).

4.4.4 Situasjonsforståelse

To av organisasjonene mener en utfordring med risikostyring er hvorvidt virksomheter faktisk har en forståelse av hva som kreves, og hvor alvorlig trusselsituasjonen faktisk er. De opplever at virksomheter har en generell forståelse av hvor utsatt kraftsektoren er, men virksomheter har utfordringer med å forankre risikobildet i deres egen virksomhet. Denne forankringen må skje på ledernivå, og ledere må gå foran som gode eksempler. En viktig faktor for at ledere skal kunne oppnå dette, er at ansatte i virksomhetene involveres i risikostyringsarbeidet, ifølge tre av virksomhetene. I tillegg må øverste leder ta eierskap til IKT-sikkerhet, ifølge en av organisasjonene. Dette vil gjøre at ledere overfører en god forståelse og kultur til ansatte om risiko- og trusselbildet. Det vil videre ha betydning for terskelen ansatte har til å rapportere om sårbarheter og avvik i virksomheten (NSM, 2020a). Selv om ledelsen må gå foran som gode eksempler, er det et felles ansvar for samtlige ansatte i virksomheten å sikre en god sikkerhetskultur.

For å oppnå er god situasjonsforståelse bør virksomhetene oppfordres til å delta på arenaer hvor det er mulig å utveksle informasjon mellom virksomhetene, og på denne måten bidra til læring. Det er viktig at ledelsen i virksomheten ikke delegerer slik deltakelse til kun IT-ansatte. Deltakelse på arenaer med informasjonsutveksling er like relevant for andre avdelinger og ansatte i virksomhetene.

4.4.5 Leverandører

Leverandører i seg selv er en stor utfordring for risikostyring av IKT-sikkerhet. Leverandører blir beskrevet av en av virksomhetene som en *kjempeprosess*. Det er et komplekst og stort område, og det er utfordrende for virksomheter å styre risikoer på ønskelig måte. Ved flere anledninger nevnes det at virksomheter må stille tydelige krav til leverandører på hva som er sikkerhetsmålene. Det bidrar til å veilede leverandørene i riktig retning, og løfte deres arbeid med risikostyring. Virksomhetene er ikke sterkere enn det svakeste ledd, og noen virksomheter peker på at leverandører og underleverandører kan være det svakeste ledd. Leverandører kan trenge oppmuntring til å øke egen bevissthet, og danne et risikobilde av den aktuelle situasjonen. Virksomhetene er avhengig av at leverandører beskytter seg selv. IKT-sikkerhet krever et gjensidig arbeid mellom virksomhet og leverandør.

4.5 Utfordringer tilknyttet leverandørkjeder

4.5.1 Oversikt og ressursmangel

Under intervjuene blir det påpekt flere utfordringer tilknyttet risikostyring i leverandørkjeder. Virksomhetene og organisasjonene sier de ikke har god nok oversikt over leverandørkjedene. Transparens gjennom leverandørkjedene, ved bruk av mange underleverandører, er krevende. Dette funnet samsvarer med NVE (2021b) sin rapport om kraftbransjens leverandørkjeder. Samtidig eksisterer det ulike nivåer av oversikt. En av virksomhetene mener de har oversikt over leverandører og underleverandør på deres avdeling, men i virksomheten som helhet er det ikke fullstendig oversikt over leverandørkjeder. Resten av virksomhetene mener de har oversikt over leverandører, men det gjelder ikke underleverandører. Jo lenger ut i kjeden, jo mindre oversikt har virksomhetene. Ifølge en av organisasjonene bør det vært et mål for alle virksomheter å etablere full oversikt over leverdørkjeden. Det innebærer også at leverandører må bli flinkere til å dokumentere og finne prosedyrer for deres egne underleverandører.

Selv om virksomhetene har noe oversikt, problematiserer en av virksomhetene hvor utfordrende det er å kontrollere og følge opp leverandører. Det skyldes i stor grad begrenset kompetanse og kapasitet til å revidere leverandører, ressursmangel, og omfattende og tidskrevende arbeid. Samme virksomhet opplever i tillegg at økonomiske midler ikke alltid blir bevilget. Informanten anser det som grunnleggende at ledelsen bevilger ressurser til å følge opp leverandører og underleverandører. Selv om det å ha god nok oversikt og tilstrekkelige ressurser er svært utforende, påpeker en av de andre virksomhetene nødvendigheten av å prioritere arbeidet. Prioriteringer av arbeidet kan skje ved å legge større innsats og ressurser i risikostyring av leverandører med høyest risiko.

4.5.2 Kraftsensitiv informasjon

Kraftsensitiv informasjon blir også ansett som en utfordring ifølge en av virksomhetene. Kbf § 6-2 definerer kraftsensitiv informasjon som «spesifikk og inngående opplysninger om kraftforsyningen som kan brukes til å skade anlegg, system eller annet eller påvirke funksjoner som har betydning for kraftforsyningen (...)». Videre listes det opp 10 underpunkter som konkretiserer kravet ytterligere. Kraftsensitiv informasjon beskrives av en av organisasjonene som en IKT-verdi som må beskyttes. Det er mange krav som stilles til identifisering av kraftsensitiv informasjon, og hvordan informasjonen skal oppbevares. To av virksomhetene forteller hvordan små virksomheter med få ansatte vil slite med ressurser for å innfri alle kravene som blir stilt. Hvis sensitiv informasjon kommer på avveie, kan det få negative følger for andre i samme sektor.

Håndtering av kraftsensitiv informasjon kan også være utfordrende for virksomheter, ifølge en virksomhet og en organisasjon. Problemstillinger rundt tilgangskontroll er de begge spesielt bekymret for. Hva betyr det egentlig å ha tilgang, og hvordan minimere risikoen for at kraftsensitiv informasjon i virksomheter kommer på avveie? Det kan argumenteres for at leverandører ønsker å ha god tilgang og funksjonalitet for den jobben de skal gjøre, som gjør at leverandørene gir seg selv flere administrative rettigheter enn strengt nødvendig. Hvis leverandørene ikke har god nok oversikt over tilgangskontroll for kraftsensitiv informasjon samsvarer praksisen ikke i henhold til kapittel 6 i kbf. Denne problematikken ble også beskrevet i NVEs rapport om IKT-sikkerhetstiltastanden i kraftforsyningen (2021c).

En av virksomhetene mener det er viktig å stille spørsmål om hva man gjør når kraftsensitiv informasjon ikke lenger er relevant for leverandør å oppbevare. Hva som anses som relevant er i stor grad subjektivt og kontekstavhengig, og det kan være ulike synspunkter mellom virksomhetene. Når ansvarlige i en virksomhet skal vurdere kraftsensitiv informasjon og dens relevans, må de forholde seg til usikkerhet og ta høyde for sorte svaner (Taleb, 2010). For tidlig sletting, eller feil vurderingsgrunnlag for sletting av kraftsensitiv informasjon, kan ha negativ betydning på beredskapssituasjonen ifølge en av virksomhetene. Leverandører har ikke alltid tilstrekkelige tilganger på kort varsel, noe som kunne vært avgjørende for å stille opp med relevant kompetanse i en ekstraordinær situasjon og bidra i gjenoppretting av IKT-systemer. Tilgangsstyringen gjør at informasjonssikkerheten tilfredsstilles, men på bekostning av gjenopprettingstid. Det kan samtidig argumenteres for at virksomhetene blir mer sårbare hvis de lar leverandører ha konstant tilgang til sine systemer, enn kun når de må inn i systemene for å rette/oppgradere. En mulig løsning på denne problematikken er bruk av tredjepart, med konstant overvåking av tilgangen leverandøren har til systemet og den kraftsensitive informasjonen. En tredjepart kan gjøre leverandørkjedene mer komplekse, men det er en avveining virksomheter må ta.

4.5.3 Leverandøravhengighet

Avhengigheter mellom virksomheter og leverandører er en stor utfordring og risiko (NVE, 2021b). Det understreker en av organisasjonene basert på egne erfaringer. Tjenesteutsetting er et område i kraftsektoren hvor avhengigheter er fremtredende. Etter kbf 6-9 bokstav *e* skal virksomheter «sørge for at sikkerhetsnivået opprettholdes eller forbedres ved utsetting av tjenester». Tjenesteutsetting bidrar til å øke kompleksitet og avhengighet mellom

virksomheter, leverandører og underleverandører (NSM, 2017b). Kompleksiteten i tjenesteutsetting øker sårbarheten i virksomhetene når ansvaret for IKT-sikkerheten blir fordelt på flere aktører. I tillegg er oversikt over leverandørkjeder en stor utfordring for informantene. Disse utfordringene overføres dermed til andre områder, som i dette tilfellet er tjenesteutsetting.

Samarbeid og tjenesteutsetting er ikke prinsipielt galt, så lenge virksomhetene evner å holde oversikt over helhetsbildet (NSM, 2022). Setter virksomhetene bort arbeidet til andre kan de spare penger, tid og unngå feil, men da er de avhengig av klare og kontraktsfestede ansvars- og rolleavklaringer (NSM, 2022). Det stiller store krav til virksomhetene, og NVE (2020) har tidligere utarbeidet en sjekkliste for tjenesteutsetting, som bygger på kraftberedskapsforskriftens krav og NSM sine grunnprinsipper for IKT-sikkerhet.

Virksomhetene blir i ulik grad påvirket hvis en av deres leverandører blir utsatt for en skadevare. Avhengighet mellom virksomhet og leverandør varierer, og det har videre betydning på hvor påvirket virksomheter blir hvis leverandører blir utsatt for skadevare. Noen leverandører er de svært avhengige av, og en uønsket IKT-hendelse kan bli meget kritisk. En enkelthendelse i IKT-systemet hos en leverandør kan få alvorlige og utbredte konsekvenser i leverandørkjeden. For å være mindre sårbare og mer motstandsdyktige, stenger tre av virksomhetene eksterntilgang til tjenesteutsatte IKT-systemer, hvis det blir nødvendig. Det gjør virksomhetene mindre utsatt for å bli påvirket av skadevare i leverandørkjeder. Dette er et viktig sikringstiltak for å motstå eller begrense skade i IKT-systemene kbf, § 6-9 bokstav *c*.

5 Konklusjon

Formålet med rapporten har vært å undersøke følgende problemstilling; *Hvordan praktiserer utvalgte virksomheter risikostyringen av IKT-sikkerhet i leverandørkjeder, og hvilke utfordringer eksisterer?* Vi vil først oppsummere hvordan de utvalgte virksomhetene sikrer god praksis, før vi belyser virksomhetenes utfordringer.

Hvordan praktiserer utvalgte virksomheter risikostyringen av IKT-sikkerhet i leverandørkjeder?

På et overordnet nivå er det nokså lik praksis i de utvalgte virksomhetene. Nedenfor er det listet opp funn som er en kombinasjon av god praksis som foregår i virksomhetene i dag, og informantene sine merknader til hva virksomhetene burde gjøre for å oppnå en god praksis. I tillegg kommer våre vurderinger av informantenes svar. Funnene er listet opp tilsvarende risikostyringshjulet presentert i figur 2.

Risikoidentifisering

- → Sette beredskapsarbeid høyt på agendaen i virksomheten.
- → Innhente oppdatert trussel- og sårbarhetsinformasjon fra KraftCERT, PST, NSM og andre fagforum.
- → Etablere oversikt over leverandører.
- → Etablere ordning for loggføring og godkjenning/kvalifisering av leverandører, f.eks. krav til sertifisering.

Risikoanalyse

- → Etablere sikkerhetsmål som evalueres jevnlig i virksomhetene.
- → Etablere sikkerhetsmål som leverandører skal etterleve.
- → Bruke anerkjente oppdaterte metoder til analysearbeidet (f.eks. Norsk Standard).

Beredskapsplan

- → Lage innsatsplaner for de vanligste hendelsene. Innsatsplanene er knyttet til virksomhetenes overordnete beredskapsplan.
- → Oppdatere eksisterende standardiserte og generelle lister, og prosedyrer fortløpende med konkrete risikovurderinger.

Etablere beredskapsstrukturer og ressurser

- → Ledelsen må bevisstgjøre ansatte på sikkerhet og beredskap.
- → Involvere riktig ledernivå.
- → Involvere leverandører og gjennomføre dialogmøter som en del av kontraktsoppfølgingen.
- → Etablere nødvendige strukturer og prosedyrer for sikkerhetsstyring opp mot etablerte sikkerhetsmål.
- → Følge opp at etablerte sikkerhetsmål for leverandører blir ivaretatt i anbudsprosessen.
- → Følge opp at etablerte sikkerhetsmål blir ivaretatt gjennom risikostyring av anskaffelser og i organisasjonsendringer.

Øvelser

- → Gjennomføring av øvelser.
- → Involvere aktuelle interne ressurser fra fagmiljøer og ledelse.
- → Involvere leverandører når det er relevant.

Evaluering

- → Gjennomføre internrevisjoner.
- → Etablere interne prosesser for kunnskapsdeling og innhenting av oppdatert informasjon fra evalueringer, erfaringsmøter etter øvelser og hendelser, egne overvåkningssystemer, og møter med leverandører og underleverandører.

Hvilke utfordringer eksisterer?

Det er flere utfordringer tilknyttet risikostyring av IKT-sikkerhet. Informantene nevner mangel på menneskelige ressurser. De nevner utfordringer med å sette av nok tid til risikostyringsarbeidet, og å prioritere og følge opp risikoanalyser og tiltak i praksis. Det finnes ingen standardisert prosedyre for risikostyring av IKT-sikkerhet i leverandørkjeder. Dette gjør

at virksomhetene selv er ansvarlig for å prioritere risikostyringsarbeidet på rett nivå. Selv om tid og menneskelige ressurser nevnes som utfordringer, må arbeidet med risikostyring tilpasses innenfor virksomhetenes rammer og forankres hos rett ledernivå.

Det er utfordrende å få avdelinger i virksomheter til å ta tilstrekkelig eierskap til risiko. IKT-sikkerhet er noe som er relevant for alle ansatte i virksomheten, ikke bare IT-avdelingen. Det er også utfordrende å danne en felles situasjonsforståelse i egen virksomhet for å forstå risikobildet. Videre er det uklare krav fra virksomheter til leverandører på hva som er nødvendige sikkerhetsmål.

Virksomhetene påpeker i tillegg utfordringer tilknyttet leverandørkjeder. Informantene er enige om at risikostyring i leverandørkjeder er krevende, og at det er en omfattende prosess å få oversikt over leverandører og underleverandører. Det skyldes bl.a. begrenset kompetanse og kapasitet til å følge opp leverandører, ressursmangler internt, og omfattende og tidkrevende arbeid i virksomheten. Det burde være mulig på sikt å opparbeide bedre oversikt ved å systematisere inngåtte kontrakter. I framtidige kontrakter bør hvem som er underleverandører til leverandørens tjeneste som de selger til virksomheten alltid oppgis.

Kraftsensitiv informasjon er utfordrende å håndtere i leverandørkjeder i kraftsektoren. Informantene i denne studien trekker fram uklarheter rundt definering, håndtering, tilgangskontroll og oppbevaring av kraftsensitiv informasjon.

Virksomheter er svært avhengig av flere av deres leverandører. Det gjelder bl.a. avdekking av skadevare og tjenesteutsetting, som begge bidrar til å øke sårbarheten i virksomhetenes IKT-systemer.

5.1 Avslutning

Risikostyring av IKT-sikkerhet i leverandørkjeder blir stadig viktigere fordi virksomhetene stadig møter nye og hyppigere digitale trusler. Det kommer tydelig frem at risikostyring av IKT-sikkerhet i kraftsektoren bygger på svak teoretisk og empirisk grunnlag. Det er lite kunnskap om beste praksis som virksomhetene kan benytte. Det er behov for å utvikle gode veiledere og spesifikke anbefalinger for praktisk risikostyring gjerne i kombinasjon av kurs.

Ved videre arbeid vil det være interessant å se nærmere på hvordan felles sikkerhetsrevisjoner i kraftsektoren kan bidra til økt risikostyring av IKT-sikkert. Det kan også være relevant å undersøke hvilken type kunnskapsformidling som gir best utbytte for aktørene i kraftforsyningen Resultatet av undersøkelsen vil gi svar på hvordan NVE kan bidra til bedre kompetanseheving, kurs og veiledning for IKT-sikkerhet blant ansatte i kraftforsyningen i møte med fremtidige digitale trusler. Et annet tema innen kompetanseheving, er i hvilken grad kraftsektoren oppnår læring og økt kunnskap på tvers av virksomheter etter evalueringer fra beredskapsøvelser og reelle hendelser.

6 Referanser

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

Aven, T. (2007). *Risikostyring: Grunnleggende prinsipper og ideer*. Oslo: Universitetsforlaget.

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

Aven, T. & Thekdi, S. (2022). *Risk Science: An Introduction*. Taylor & Francis Group.

Engen, O. A., Pettersen, K. A., Kruke, B. I., Lindøe, P., Olsen, K. H. & Olsen, O. E. (2021). *Perspektiver på samfunnssikkerhet*. Oslo: Cappelen Damm AS.

Direktoratet for samfunnssikkerhet og beredskap [DSB]. (2016). *Samfunnets kritiske funksjoner*. Versjon 1.0.

DSB. (2018). Veileder i planlegging, gjennomføring og evaluering av øvelser. *Metodehefte: Evaluering av øvelser*. https://www.statsforvalteren.no/siteassets/fm-innlandet/10-samfunnssikkerhet-og-beredskap/forebyggende-samfunnssikkerhet/ovelsesplanlegging/metodehefte_evaluering_av_ovelser22.pdf

DSB. (2020). *Risikostyring i digitale verdikjeder*. https://www.dsb.no/globalassets/dokumenter/rapporter/risikostyring-i-digitale-verdikjeder.pdf

Forum for informasjonssikkerhet i kraftforsyningen. (2021). *Sikkerhetsveileder for kraftsensitiv informasjon*. https://fsk-forum.no/wp-content/uploads/2021/11/FSK-Veilder-for-skytjenester-Final-PDF.pdf

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

Kraftberedskapsforskriften (2019). *Forskrift om sikkerhet og beredskap i kraftforsyningen* (FOR-2019-12-07-1157). Lovdata. https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157

KraftCERT. (2020). *Om KraftCERT*. https://www.kraftcert.no/om.html

Nasjonal sikkerhetsmyndighet [NSM]. (2017a). *Rammeverk for håndtering av IKT-sikkerhetshendelser*.

Norsk Elektriske komite [NEK]. (2020). *NEK IEC 62443 – en bærebjelke for cybersikkerhet*. https://www.nek.no/nek-iec-62443-en-baerebjelke-for-cybersikkerhet/

NSM. (2017b). *Sikkerhetsfaglige anbefalinger ved bruk av tjenesteutsetting og skytjenester*. https://nsm.no/getfile.php/133998-1593590999/Filer/Dokumenter/Rapporter/2020-07-01%20-%20Temarapport%20-%20Tjenesteutsetting.pdf

NSM. (2020a). *Grunnprinsipper for sikkerhetsstyring*. https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-sikkerhetsstyring/introduksjon/

NSM. (2020b). *Veileder i sikkerhetsstyring*. https://nsm.no/getfile.php/132933-1591350417/Filer/Dokumenter/Veiledere/veileder-i-sikkerhetsstyring.pdf

NSM. (2020c). *NSMs grunnprinsipper for IKT-sikkerhet*. Vol 2.0. Oslo. Nasjonal sikkerhetsmyndighet

NSM. (2020d). *Grunnprinsipper for fysisk sikkerhet*. Nasjonal sikkerhetsmyndighet.

NSM. (2021). *Risiko 2021 – helhetlig sikring mot sammensatte trusler.* https://nsm.no/getfile.php/136419-1616673370/Filer/Dokumenter/Rapporter/NSM_Risiko_2021_web_enkeltside_1203.pdf

NSM. (2022). *Risiko 2022: Økt risiko krever økt årvåkenhet.* https://nsm.no/getfile.php/137798-1644424185/Filer/Dokumenter/Rapporter/NSM_rapport_final_online_enekeltsider.pdf

Norges vassdrags- og energidirektorat [NVE]. (2017). *Regulering av IKT- sikkerhet*. Rapport 26/2017. https://publikasjoner.nve.no/rapport/2017/rapport2017_26.pdf

NVE. (2019a). *Metode for å finne kraftsensitiv informasjon på Internett*. Faktaark nr. 11 09/2019

NVE. (2019b). *Veiledning til forskrift om sikkerhet og beredskap i kraftforsyningen* (Kraftberedskapsforskriften). https://webfileservice.nve.no/API/PublishedFiles/Download/dc13cfde-99c7-46b8-8fbe-dbd3ccdf80bb/202119965/3425781

NVE. (2020). *IKT-sikkerhet i anskaffelser og tjenesteutsetting i kraftsektoren*. Rapport nr. 1/2020.

NVE. (2021a). *Informasjonssikkerhetsledelse i kraftforsyningen*. Faktaark nr. 2/2021.

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

NVE. (2021c*). IKT-sikkerhetstilstanden i kraftforsyningen 2021*. Ekstern rapport nr. 19/2021.

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

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

Olje- og energidepartementet. (2012). *Hvordan leve med farene- om flom og skred* (Meld. St. 15 (2011- 2012). https://www.regjeringen.no/no/dokumenter/meld-st-15-20112012/id676526/?ch=5

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

Riksrevisjonen. (2021). *Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen*. Dokument 3:7 (2020-2021). Oslo: Riksrevisjonen.

Ponemon Institute. (2019). *The Cost of Third-Party Cybersecurity Risk Management*.

Salater, T. (2021). *NEK IEC 62443 – en bærebjelke for cybersikkerhet*. https://www.nek.no/nek-iec-62443-en-baerebjelke-for-cybersikkerhet/

Silverman, D. (2005). *Doing qualitative research: a practical handbook* (2nd ed.). London; Thousand Oaks, Calif: Sage Publications.

Standard Norge. (2021a). *Beskyttelse mot tilsiktede uønskede handlinger*. https://www.standard.no/fagomrader/kvalitet-og-/samfunnssikkerhet/beskyttelse-mot-tilsiktede-uonskede-handlinger/

Standard Norge. (2021b). Krav til risikovurdering. *NS 5814:2021*.

Standard Norge. (2022a). *Ledelsessystemer for informasjonssikkerhet - Krav – NS-EN ISO/IEC 27001*. https://www.standard.no/fagomrader/ikt/it-sikkerhet/isoiec-27001/

Standard Norge. (2022b). *Risikostyring – ISO 31000*. https://www.standard.no/fagomrader/kvalitet-og-/risikostyring/iso-31000-risikostyring--retningslinjer/?gclid=CjwKCAjwwo-WBhAMEiwAV4dybdn_Z6XrRzqfqMI9EAiw3PIp2eL1nuaMhYhsBGUaFfe_ygdMDiqbexoCMvkQAvD_BwE

Statsforvalteren. (2014). Håndbok i øvelsesplanlegging. https://www.statsforvalteren.no/siteassets/fm-rogaland/dokument-fmro/forvaltning/brosjyrer-og-rettleiarar/handbok-i-ovelsesplanlegging-2014.pdf

Taleb, N.N. (2010). The black swan*: the impact of the highly improbable* (2.utg). New York: Random House Trade Paperbacks

Thagaard, T. (2013). *Systematikk og innlevelse* (4 utg.). Bergen: Fagbokforlaget.

Trkman, P. & McCormack, K. (2009). *Supply chain risk in turbulent environments—A conceptual model for managing supply chain network risk*. *International Journal of Production Economics*, 119(2), 247–258. https://doi.org/10.1016/j.ijpe.2009.03.002

7 Vedlegg

7.1 Intervjuguide

Vedlagt er en overordnet intervjuguide utarbeidet til produsent/nettselskap.
Intervjuguiden til organisasjonene ble utarbeidet på bakgrunn av de samme temaene, men tilpasset til deres praksis.

Innledning
Kort presentasjonsrunde og fortelle litt om prosjektet.

Risikovurderinger
Kan du fortelle kort om hvilke digitale risikoer din virksomhet er mest bekymret for?

- Er disse identifisert gjennom risikovurderinger?

Hvordan gjennomføres risikovurderinger av IKT-systemer som allerede eksisterer?
Hva tar dere utgangspunkt i når dere skal gjennomføre risikovurderinger av IKT-systemer?

- Hvilke standarder, veiledere, sjekklister osv. benytter dere?

Hvordan identifiserer dere IKT-verdier som er spesielt viktig for dere?

- Hvordan beskytter og sikrer dere IKT-verdier?

Hvem blir involvert i risikovurderingsarbeidet?

- I hvilken grad blir ledelsen involvert i arbeidet med risikovurderinger?

I etterkant av gjennomføringen av risikovurderinger – hvordan blir ledelsen orientert om funn?

- Opplever du/dere at ledelsen prioriterer resultatene?

Risikostyring av IKT-sikkerhet
Hva legger deres virksomhet i begrepet risikostyring i forbindelse med IKT-sikkerhet?
Kan du fortelle litt om hvordan din virksomhet sikrer god risikostyring?
Hvordan gjøres risikostyring i praksis?
Hva tenker du virksomheten deres gjør bra når det kommer til risikostyring av IKT-sikkerhet?
Opplever dere noen utfordringer knyttet til risikostyring av IKT-sikkerhet?

- Hvis ja: Hvilke?

Hvilke funksjoner er involvert i den daglige risikostyringen?

- Hvilket ledernivå er involvert?
- Hva med eksterne leverandører?

Hvordan henger risikostyring sammen med endringsledelse?
Gjennomfører dere jevnlig evalueringer av iverksatte sikringstiltak for IKT-systemer?
Hvilken opplæring får nyansatte når de starter i virksomheten?

- Hvem gjennomfører opplæringen?

Leverandørkjeder
Har dere oversikt over deres leverandører og underleverandører?

- Kan du fortelle litt om det?
- Hvordan sikrer dere nok oversikt over leverandører lenger ned i kjeden?

Gjøres det risikovurderinger av IKT-systemene i forbindelse med deres leverandørkjeder?
Har dere noen sikkerhetsmål for IKT-sikkerheten til underleverandørene?

- Hvis ja: Hvilke?
    - Hvordan har dere kommet frem til disse sikkerhetsmålene?
    - Hva gjør dere for å følge opp at disse sikkerhetsmålene blir fulgt?
    - Hvordan blir sikkerhetsmålene kommunisert videre?
- Hvis nei: Hvorfor ikke?

Hva tenker dere er utfordringer i leverandørkjeder når det gjelder IKT-sikkerhet?

- Har du noen tanker om hvordan utfordringene kan løses?

I hvor stor grad vil en skadevare på en av deres underleverandører påvirke dere?
Hvordan foregår kunnskaps- og erfaringsdeling på tvers av dere og leverandørkjedene?

Beredskap

Hvilken kobling er det mellom risikovurderingene og arbeidet med digital beredskap?

- Blir funnene i analysen fulgt opp i form av forslag til tiltak i beredskapsarbeidet?

Har dere en beredskapsplan som er tilpasset dagens komplekse risikobilde når det kommer til IKT-sikkerhet?

- Hvordan innhenter dere oppdatert kunnskap og informasjon?

Avsluttende kommentarer

Er det noe du vil legge til?

7.2 Utfordringer og svakheter med studien

Det er tatt høyde for ulike etiske utfordringer tilknyttet studiets gang. Det er behandlet personopplysninger, og samtlige informanter har gitt sitt informerte samtykke før deltagelse. Informantene ble opplyst om deres rett til å avbryte deltagelsen uten negative konsekvenser, og informasjonen som kom frem under intervjuet ikke vil være mulig å spore tilbake til informanten i rapporten.

7.2.1 Reliabilitet

Reliabilitet i forskning handler om hvordan en annen forsker kan komme fram til de samme resultatene ved å bruke samme metodikk (Silvermann, 2005). I denne rapporten er det benyttet kvalitativ forskningsmetode, og det gjør det utfordrende å etterprøve reliabiliteten. Rapportens reliabilitet er styrket på bakgrunn av vedlagt intervjuguide, og i tillegg ble intervjuguiden utformet uten ledende spørsmål. Vi har forsøkt å stille spørsmål som oppfordret til refleksjon, og vi har anonymisert personidentifiserbare opplysninger.

Reliabiliteten er også styrket i denne studien ved at dataen er samlet på en konsistent måte (Thagaard, 2013). Forskningsprosessen er transparent, som innebærer at vi har gjort en detaljert beskrivelse av forskningsstrategi og analysemetoder. På denne måten kan forskningsprosessen vurderes trinn for trinn, og forskingsprosjektet kan blir gjennomført av andre forskere (Thagaard, 2013). Samtlige informanter har hatt stor betydning for studiens resultat. Dette trekkes fram som utelukkende positivt, da det har ført til verdifull empirisk data fra relevante og viktige informanter. Vi vil derfor argumentere for at denne studien er troverdig.

7.2.2 Validitet

Validitet handler om gyldighet, og sier noe om hvordan funn fra dette studiet kan overføres til andre sammenhenger (Thagaard, 2013). Funnene i denne studien kan ikke sies å være gyldig ovenfor andre virksomheter i kraftsektoren. Utvalget er verken bredt eller stort nok. I kvalitative studier er det mer relevant å se på analytisk generalisering; om hvordan data fra et mindre utvalg generaliseres og kobles opp mot teori, med søkelys på å finne sammenhenger, og utdype fenomener og begreper (Jacobsen, 2005). Det fremkommer flere lignende beskrivelser og opplevelser hos informantene, som fører til at våre resultater kan vise til flere fellestrekk ved risikostyring i leverandørkjeder (Thagaard, 2013). Dette styrker studiens validitet. Selv om studiet er skrevet med utgangspunkt i utvalgte virksomheter i kraftsektoren, kan det tenkes at funnene kan generaliseres til andre lignende virksomheter i landet.

NVE

Norges vassdrags- og energidirektorat

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

www.nve.no