Proactima Stavanger
Postboks 8034
4068 Stavanger

Proactima Oslo
Grubbegata 4
0155 Oslo

Proactima Bergen
St. Jakobsplass 9
5008 Bergen

Proactima Trondheim
Innherredsveien 7
7014 Trondheim

T: 40 00 19 33 - org. nr. 915 641 938 - Post@proactima.com - www.proactima.com

RAPPORT

Norges vassdrags- og energidirektorat (NVE)

Veikart for NVEs oppfølging av IKT-sikkerhet i leverandørkjeden

Kunde:	**Kontaktperson:**
Norges vassdrags- og energidirektorat (NVE)	Janne Hagen

Oppsummering:

Proactima har, på oppdrag for Norges vassdrags- og energidirektorat (NVE), utarbeidet et veikart for NVEs oppfølging av IKT-sikkerhet i leverandørkjeden. Som del av oppdraget er det gjennomført en kartlegging av digitale sårbarheter i leverandørkjeden til norsk kraftforsyning.

Nøkkelord	IKT-sikkerhet, digital sårbarhet, leverandørkjeder, kraftforsyning
Rapportnr.	1074197-RE-01
Forfatter(e)	Karianne Haver, Anne-Kari Valdal, Terje Vernholt (Netsecurity), Hermann S. Wiencke
Konfidensialitet	Intern
Revisjonsnr.	02
Revidert dato	15.12.2021
Antall sider	52

Rev.nr.	**Dato**	**Årsak til revisjon**
00	19.11.2021	Første utkast til rapport
01	26.11.2021	Oppdatert utkast til rapport
02	15.12.2021	Endelig rapport

Utarbeidet av	**Verifisert av**	**For Proactima AS**
Karianne Haver, Hermann S. Wiencke	Anne-Kari Valdal	Rune Winther

Innhold

1 Sammendrag

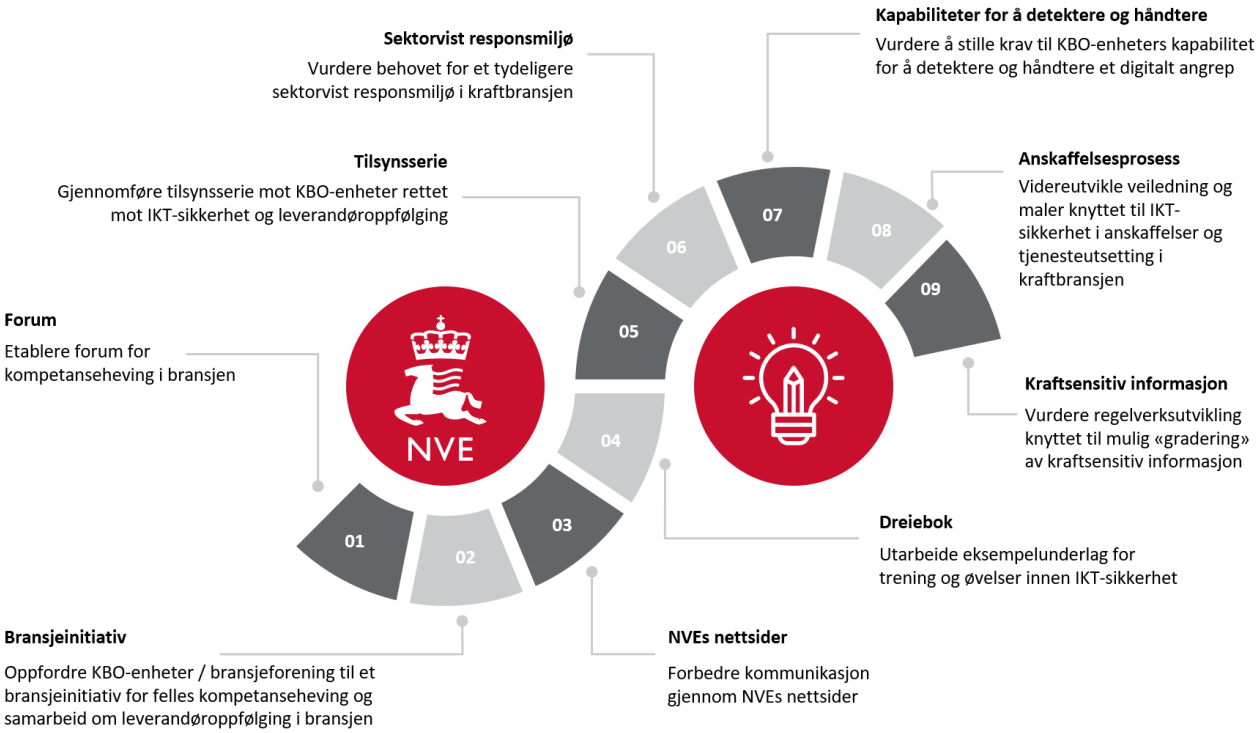
Kraftbransjen moderniseres og opplever økt digitalisering, kritiske systemer tilknyttes i større grad til internett og flere oppdrag utføres i større grad enn før gjennom fjerntilkobling av en tredjepart. Sikkerhetsbrister og cyberangrep mot selskaper via digitale verdikjeder er en reell trussel. Trusselen er tydelig demonstrert med angrepene mot Volue og Solarwinds, samt sikkerhetsvarsler som sendes ut fra KraftCERT. Riksrevisjonen, som avga en rapport om NVEs arbeid med IKT-sikkerhet i kraftforsyningen i 2021, har også pekt på bransjens avhengighet av leverandører, mangelfull oppfølging av disse og det at NVE ikke lenger fører tilsyn med leverandørene.

Proactima har, på oppdrag for Norges vassdrags- og energidirektorat (NVE), utarbeidet et veikart for NVEs oppfølging av IKT-sikkerhet i leverandørkjeden. Som del av oppdraget er det gjennomført en kartlegging av digitale sårbarheter i leverandørkjeden til norsk kraftforsyning. Formålet med oppdraget har vært å beskrive digitale sårbarheter i verdikjeden, anbefale tiltak og lage en plan for videre arbeid med oppfølging av IKT-sikkerhet i leverandørkjeden i kraftsektoren.

Kartleggingen viser at det er stor variasjon i relevante og fremtredende sårbarheter hos KBO-enhetene og leverandørene. Problemstilling er sammensatt der ulike varianter og nyanser av sårbarhetene er gjeldende for de ulike aktørene. Dette gjør at det er ikke ett enhetlig bilde på hva som er digitale sårbarheter i leverandørkjeden. Det er likevel noen sårbarheter som er mer gjennomgående og fremtredende enn andre knyttet til:

1) Manglende risiko- og trusselforståelse hos aktørene i leverandørkjeden
2) Manglende forståelse og etterlevelse av regelverkskrav hos KBO-enhetene
3) Manglende kompetanse og/eller kapasitet / evne til å stille tilstrekkelige krav til leverandører
4) Manglende kompetanse og/eller kapasitet / evne til å følge opp krav som stilles i leverandørkjeden
5) Manglende identifisering av, informasjonsdeling om, og lukking av digitale sårbarheter i utstyr og systemer hos aktørene i leverandørkjeden
6) Manglende kompetanse og/eller kapasitet / evne til å detektere og håndtere IKT-sikkerhetshendelser hos aktørene i leverandørkjeden

Med utgangspunkt i disse sårbarhetene er det vurdert og anbefalt tiltak. I lys av økt digitalisering og et endret trusselbilde, vil det være behov for å styrke både kompetanse og kapasitet hos NVE for å gjennomføre tiltakene. I Figur 1 presenteres et forslag til hvordan de anbefalte tiltakene bør innføres i form av et veikart for NVEs oppfølging av IKT-sikkerhet i leverandørkjeden. Tiltakene er delt i tre kategorier ut fra hvilken rekkefølge tiltakene bør iverksettes og hvor raskt man kan få effekt av tiltakene. Se Tabell 1.



Figur 1: Forslag til veikart for NVEs oppfølging med IKT-sikkerhet i leverandørkjeden

Tabell 1: Forslag til kategorisering av tiltak for NVEs oppfølging av IKT-sikkerhet i leverandørkjeden

Kategori	Tiltak
Tiltak som bør iverksettes snarlig og som er vurdert å kunne gi rask effekt	1) Etablere forum for kompetanseheving i bransjen 2) Ta et bransjeinitiativ mot KBO-enheter / bransjeforening for kompetanseheving og samarbeid om leverandøroppfølging i bransjen 3) Forbedre kommunikasjon gjennom NVEs nettsider 4) Utarbeide eksempelunderlag for trening og øvelser innen IKT-sikkerhet 5) Gjennomføre tilsynsserie mot KBO-enheter rettet mot IKT-sikkerhet og leverandøroppfølging
Tiltak som bør påbegynnes snarlig og som er vurdert å kunne gi effekt på lengre sikt	6) Vurdere behovet for et tydeligere sektorvist responsmiljø i kraftbransjen 7) Vurdere å presisere forventninger til KBO-enheters kapabilitet for å detektere og håndtere et digitalt angrep
Tiltak som bør gjennomføres på litt lengre sikt	8) Videreutvikle veiledning knyttet til IKT-sikkerhet i anskaffelser og tjenesteutsetting i kraftbransjen 9) Vurdere regelverksutvikling knyttet til mulig gradering av kraftsensitiv informasjon

2 Bakgrunn

2.1 Et endret trusselbilde og nye digitale sårbarheter via digitale verdikjeder

Kraftforsyning er en kritisk samfunnsfunksjon, og er en av funksjonene som er nødvendige for å ivareta befolkningens og samfunnets grunnleggende behov og befolkningens trygghetsfølelse. Kraftbransjen moderniseres og opplever økt digitalisering, kritiske systemer knyttes i større grad til internett og flere oppdrag utføres i større grad enn før gjennom fjerntilkobling av en tredjepart. Dette medfører behov for nye og strengere krav og et bevisst forhold til IKT-sikkerhet. I begynnelsen av 2019 kom det derfor en oppdatering av kraftberedskapsforskriften (2018) der det stilles strengere krav til IKT-sikkerhet. Samtidig med endringen av kraftberedskapsforskriften kom det også en ny sikkerhetslov (2018). NVE har harmonisert bestemmelsene i kraftberedskapsforskriften med sikkerhetsloven.

NSM vurderer i «Risiko 2021» at virksomheter innenfor kraftsektoren fortsatt er risikoutsatt (NSM, 2021). Blant annet peker NSMs «Risiko 2021» på et skjerpet digitalt risikobilde, sårbarheter i lange digitale verdikjeder, tydeligere avhengigheter, og vier et spesifikt fokus på sikkerhet (og sårbarheter) i anskaffelser.

Sikkerhetsbrister og cyberangrep mot selskaper via digitale verdikjeder er en reell trussel. Trusselen er tydelig demonstrert med angrepene mot Volue og Solarwinds, samt sikkerhetsvarsler fra KraftCERT. Også løsepengeangrepet mot Colonial Pipeline er en påminnelse om at kritisk infrastruktur kan bli berørt. Lange digitale verdikjeder, komplekse systemer, økende grad av autonomi, betydelig gjensidige avhengigheter mot leverandører både nasjonalt og internasjonalt, samt nye og stadig økende antall trusselaktører, gjør det utfordrende både for virksomheter og myndigheter å styre sin risiko og sine sårbarheter.

Det viser seg at KBO-enhetenes[1] innsyn i IKT-sikkerhet knyttet til leveransene, i praksis bare omfatter det første leddet i verdikjeden, kun enkelte ganger også underleverandørene. En NVE-rapport fra 2018 drøfter denne problematikken og oppfordrer blant annet til videre bransjesamarbeid for å utvikle felles krav (NVE, 2018).

For at bransjen skal ha en god beredskap for uønskede IKT-hendelser er det nødvendig med et godt samarbeid med leverandørene. IKT-sikkerhet må tas hensyn til allerede i en tidlig fase i en anskaffelse eller tjenesteutsetting. Samtidig må IKT-sikkerhet være et tema gjennom hele levetiden til produktet eller tjenesten som er anskaffet, inkludert avhending eller skifte av leverandør. Som en oppfølging av studien fra 2018, fikk NVE utarbeidet en sjekkliste for IKT-sikkerhet i anskaffelser som dekker hele livssyklusen til anskaffelsen (NVE, 2020).

NVE har tidligere hatt en godkjenningsordning for leverandører til kraftbransjen der NVE inngikk sikkerhetsavtale med utvalgte leverandører. Denne ordningen er opphevet. I dag leverer både små nasjonale leverandører og store globale selskap sine tjenester og produkter til KBO-enheter uten at NVE gjør noen godkjenning. Det er opp til selskapene selv å vurdere risiko og innføre risikoreduserende tiltak. Sikkerhet er regulert i privatrettslige kontrakter mellom leverandør og kunde, og mellom leverandør og underleverandør.

Våren 2021 leverte Riksrevisjonen en rapport om NVEs arbeid med IKT-sikkerhet i kraftforsyningen. Riksrevisjonen har også pekt på bransjens avhengighet av leverandører, mangelfull oppfølging av disse og det at NVE ikke lenger fører tilsyn med leverandørene (Riksrevisjonen, 2021). De har anbefalt at NVE *«Vurderer tiltak for å håndtere utfordringen med å følge opp leverandørenes IKT-sikkerhet»*.

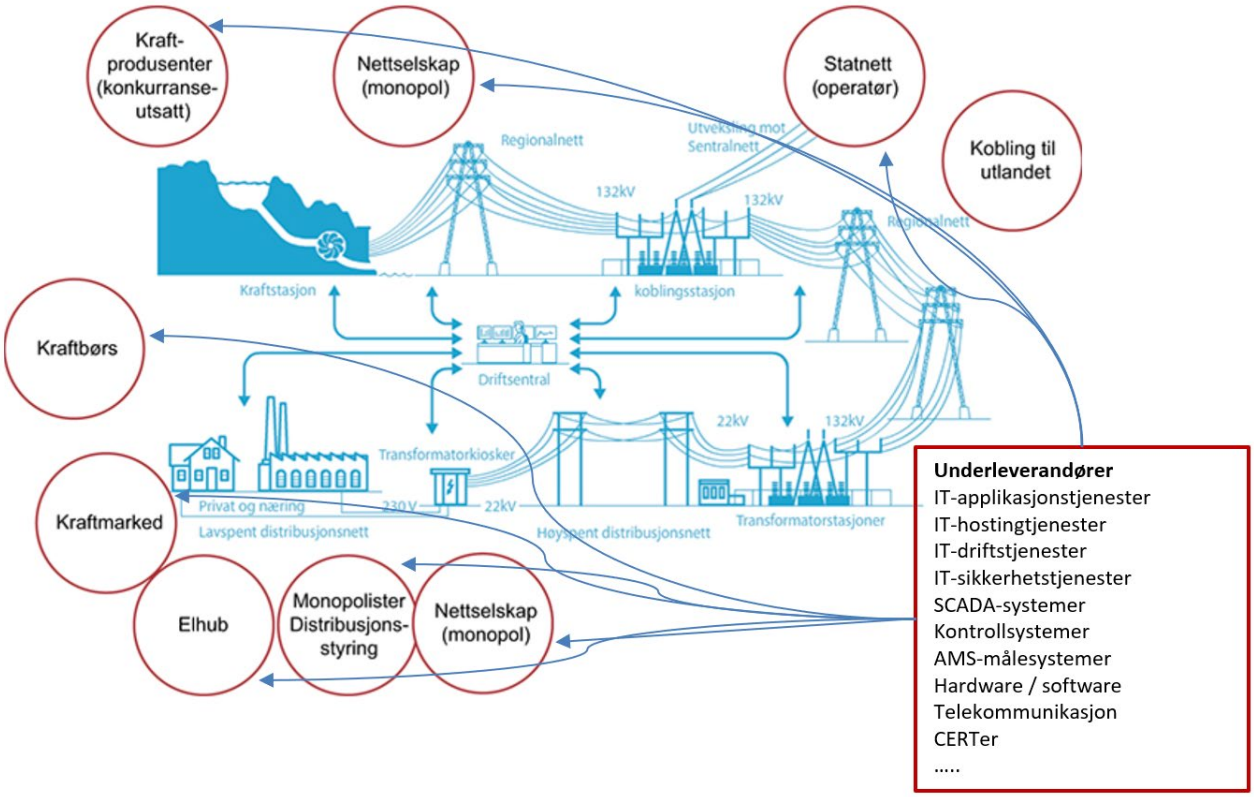
[1] Kraftforsyningens beredskapsorganisasjon https://www.nve.no/energi/tilsyn/kraftforsyningsberedskap/organisering-av-kraftforsyningsberedskap/kraftforsyningens-beredskapsorganisasjon-kbo/

Som en oppfølging til Riksrevisjonens rapport, har NVE sommeren 2021 gjennomført en studie av leverandørkjedesårbarhet og sikkerhet (NVE, 2021).

Med dette som bakgrunn har Proactima, på oppdrag for Norges vassdrags- og energidirektorat (NVE), gjennomført en kartlegging av digitale sårbarheter i leverandørkjeden til norsk kraftforsyning og utarbeidet et veikart for NVEs oppfølging av IKT-sikkerhet i leverandørkjeden.

Et endret trusselbilde – og ikke minst nye digitale sårbarheter, gir økende utfordringer. På den ene siden gir kompleksiteten behov for spesifikasjoner, standardisering og tett kontroll for å ivareta samfunnets og den enkeltes sikkerhetsbehov. Dette også fordi det stadig kreves mer kapasitet og kompetanse på flere felter for å forstå og håndtere nye sårbarheter. Samtidig fordrer en rivende teknologisk utvikling, innovasjon og lange digitale verdikjeder både dynamiske krav og nærhet til risikoen for å nyttiggjøre seg utviklingen. Ikke minst for å forbedre sikkerheten over tid. Dette gir en utfordring med tanke på hvordan IKT-sikkerhet i samfunnets viktige infrastruktur best ivaretas. Tettere myndighetskontroll med de digitale verdikjedene kan sikre tilgang til kompetanse, forståelse for trusler og regelverk og konsekvent oppfølging av krav. Samtidig vil det være svært kapasitetskrevende, gi rom for «frisoner» der myndighetene ikke når, og medføre fare for avstand, mindre kunnskap og fravær av ansvar for de som eier, kjenner og skal operere systemene. Dersom styring av sikkerhet også i leverandørkjeden i større grad legges på virksomhetene, kan en oppnå større eierskap, ansvar og nærhet til utfordringene. Da kan man potensielt også oppnå en mye tettere og frekvent oppfølging ved at alle aktører bidrar i arbeidet. Samtidig er en slik løsning krevende for spesielt mindre virksomheter som har begrenset tilgang til kompetanse og kapasitet til oppfølging. Løsningen vil også kreve tydelig kravstilling / regelverk fra myndigheten mot de ansvarlige virksomhetene, og ikke minst kontroll med at kravet følges opp.

Figur 2 under er hentet fra NOU 2015:13 og illustrerer kraftsystemet i Norge med de ulike aktørene. Dette er et bilde som stadig endrer seg etter hvert som nye aktører kommer inn som kraftprodusenter (vannkraft, vindkraft, solenergi, husholdninger osv.), og kraftbransjen og samfunnet generelt digitaliseres. I dette bildet er underleverandører, knyttet opp mot aktørene i kraftbransjen, kritiske aktører i verdikjeden for å sikre kraftleveransene til samfunnet. Dette kan være leverandører av applikasjons-tjenester, hostingtjenester, SCADA-systemer, kontrollsystemer, AMS-målesystemer, driftstjenester, sikkerhetstjenester, telekommunikasjon osv.



Figur 2: Illustrasjon av kraftsystemet i Norge (Kilde: NOU 2015:13)

2.2 Formål

Formålet med oppdraget har vært å kartlegge og beskrive digitale sårbarheter i verdikjeden, anbefale tiltak og lage et veikart for videre arbeid.

I tråd med oppdraget har følgende forhold blitt belyst:

a) Hvilke sikkerhetsutfordringene det er i leverandørkjeden, samt i hvilken grad IKT-sikkerhet er regulert i kontraktregimene nedover i en leverandørkjede
b) I hvilken grad leverandører bygger inn IKT-sikkerhet i egne pilotprosjekter som testes i kraftbransjen
c) I hvilken grad leverandørene lukker digitale sårbarheter i egne produkter, varsler sine kunder og samarbeider med KraftCERT eller andre CSIRT-miljøer
d) Hvordan leverandører som ikke er sertifisert allerede, stiller seg til mulig krav til sertifisering i henhold til internasjonale sikkerhetsstandarder
e) Hvordan leverandørene er bevisste på sikkerhetsutfordringer og ser at de selv kan bidra for å beskytte norsk kraftforsyning mot cyberangrep
f) Hvordan myndigheter i andre land arbeider for å ivareta sikkerhet i leverandørkjeden til energiforsyningen
g) Om viktige leverandører bør bli KBO-enhet og underlagt deler av kraftberedskapsforskriften.

Basert på funnene er det pekt på aktuelle tiltak og skissert et veikart for NVEs videre arbeid med sikkerhet i leverandørkjeden.

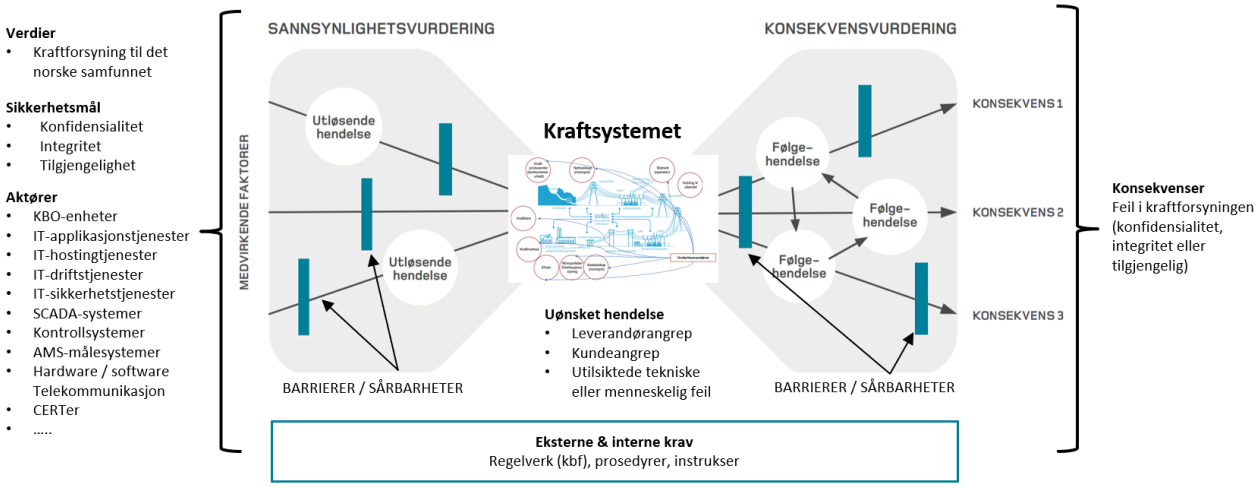
2.3 Metode, arbeidsomfang og avgrensninger

Oppdraget har blitt gjennomført i henhold til hovedtrinnene i en risikoevalueringsprosess der tiltak og veikart for videre arbeid etableres basert på en forståelse av risiko og sårbarheter knyttet til bruken av leverandører og underleverandører i de digitale verdikjedene:

1) Bakgrunn og planlegging: Definere bakgrunn, rammer og formål med oppdraget, inkludert avgrense arbeidsomfang, avklare metode og identifisere aktører som skal inngå i kartleggingen.
2) Kartlegging og vurdering av sårbarheter: Kartlegge og beskrive digitale sårbarheter knyttet til leverandørkjedene, samt vurdere hva som er de viktigste sårbarhetene for kraftsystemet.
3) Anbefalinger: Basert på dette foreslå prioriterte tiltak, i form av et veikart for videre arbeid.

I Figur 3 under er problemstillingen synliggjort gjennom en sløyfemodell, der en uønsket hendelse i kraftsystemet som følge av angrep gjennom digitale verdikjeder, utgjør midtpunktet i sløyfen. Spørsmålet blir da hvilke sårbarheter som eksisterer i disse verdikjedene – sårbarheter som åpner for uønskede hendelser og/eller påvirker håndteringen av hendelser. Digitale sårbarheter kan være sårbarheter som knyttes direkte til IKT-systemer eller sårbarheter i selve kraftforsyningen som er forårsaket av svikt i IKT-systemer, og ved at svakheter arves av feil i IKT-systemer (NOU 2015:13).

Flere av spørsmålene NVE stiller knytter seg til å kartlegge i hvilken grad leverandørene gjør tilstrekkelig forebyggende arbeid og planlegger for å håndtere eventuelle konsekvenser av en hendelse, samt hvilken oppfølging som aktørene i verdikjeden gjør eller bør gjøre. Noen av spørsmålene er rettet mot ramme-betingelser og regelverk, og om det er læring å hente fra hvordan dette utøves i andre land. Som illustrert i figuren, er også rammene og konteksten viktig for å gjøre gode vurderinger og kunne peke på den riktige veien videre. I dette ligger at en grunnleggende forståelse for trender og utvikling i bransjen, utviklingen i det generelle trusselbildet og endringer i rammebetingelser og regelverk er avgjørende for å forstå dagens og fremtidens sårbarheter. Det er viktig å ha hele dette perspektivet for å identifisere tiltak og barrierer som er effektive og hensiktsmessige for å oppnå den sikkerheten man ønsker og trenger i kraftsystemet.



Figur 3: Risikoevaluering i kontekst

Problemstillingen som belyses i denne kartleggingen er i utgangspunktet omfattende og bred, mens studien er relativt begrenset i tid og omfang. Det er derfor gjort følgende valg og prioriteringer med tanke på metode, arbeidsomfang og avgrensninger i samråd med NVE:

- Det ble benyttet en kvalitativ forskningsmetode med fokus på gjennomføring av (dybde)intervjuer med et lite utvalg KBO-enheter, leverandører, bransjeorganisasjoner, KraftCERT og myndigheter.

- Det ble gjennomført semistrukturerte intervjuer. Det vil si at intervjuene er basert på en fastlagt intervjuguide, men at spørsmålene er forholdsvis åpent formulert og at det samtidig er rom for improvisasjon underveis i intervjuene dersom relevante tema det ikke er planlagt for, dukker opp.
- I for- og etterkant av intervjuene ble relevant dokumentasjon som ble gjort tilgjengelig, gjennomgått, i tillegg til nettsøk osv.

2.4 Datagrunnlag og avgrensninger

I kraftbransjen inngår en rekke ulike aktører. Det finnes nær 200 enheter i kraftforsyningens beredskaps-organisasjon (KBO-enheter), det vil si alle nettselskaper, alle store produksjonsselskap inklusive vindkraft, store fjernvarmevirksomheter, samt vassdragsregulanter. I tillegg kommer de mange aktørene som leverer produkter, systemer, applikasjoner og tjenester til kraftbransjen. Med den raske utviklingen av nye og digitale teknologiske løsninger ser man også en økning i antall nye leverandører som tilbyr tjenester eller produkter til denne sektoren. I denne begrensede kartleggingen har det ikke vært mulig å innhente informasjon som er dekkende for hele nedslagsfeltet. Det ble derimot valgt å gjøre et utvalg av enkelte informanter som ble antatt å kunne belyse flest mulig av elementene som ble undersøkt – på et overordnet nivå.

I samråd med NVE ble det bestemt å gjennomføre intervjuer av et lite utvalg av KBO-enheter, leverandører, bransjeorganisasjoner, KraftCERT og myndigheter. Gjennom utvelgelsen av intervjuobjekter ble det forsøkt å sikre god dekning over verdikjeden og å fange opp om det er vesentlige forskjeller mellom forskjellige aktører. Utvalget forventes ikke å være representativt for hele bransjen. Ulike intervjuguider ble utarbeidet for KBO-enheter, leverandører, KraftCERT og myndigheter (se Vedlegg I). Disse ble hovedsakelig benyttet som sjekklister under intervjuene for å sikre at alle problemstillingene ble belyst.

Fem KBO-enheter som er nettselskap og/eller produksjonsselskap, inkludert vindkraft, ble valgt ut. Dette inkluderer både større og mindre selskaper. Alle KBO-enhetene som ble kontaktet, var villige til å delta i kartleggingen. Kompetansebakgrunnen og rollene informantene innehar i sine respektive selskaper inkluderte både IKT-sikkerhetskoordinator / IKT-leder / CISO, beredskapskoordinator, fagledere og senior-rådgivere innen IT / cybersikkerhet og anskaffelser/ kontrakt, samt prosjektledere.

Når det gjelder leverandører, er det stor variasjon i aktørbildet mellom de større og mindre KBO-enhetene både knyttet til leverandører på SCADA- og kontrollsystemer, samt leverandører innenfor drifts-, applikasjons- og sikkerhetstjenester. Basert på innspill fra KBO-enhetene ble åtte leverandører valgt ut og kontaktet, hvorav syv leverandører ga tilbakemelding at de hadde anledning til å delta i kartleggingen. Også her ble det forsøkt å dekke spekteret i leverandører, både større og mindre leverandører, leverandører til større og mindre KBO-enheter, samt leverandører av ulike systemer og tjenester til kraftbransjen, herunder leverandører av SCADA-systemer, kontrollsystemer, AMS-målesystemer, IT-applikasjonstjenester, sikkerhetstjenester, IT-driftstjenester og sensortjenester.

I tillegg ble det gjennomført intervjuer med KraftCERT, samt med Energimyndigheten i Sverige og Reguleringsmyndigheten for energi (RME) for å få en forståelse av hvordan KraftCERT og myndigheter i andre land arbeider for å ivareta sikkerhet i leverandørkjeden til energiforsyningen.

Intervjuene ble gjennomført som individuelle samtaler med hver aktør der aktøren stilte med en eller flere informanter. Hver av intervjuene hadde en varighet på 1-1,5 timer. Helhetsinntrykket er at intervju-objektene har delt åpent omkring både egne styrker og sårbarheter og generelle styrker og sårbarheter i bransjen. Det er ingenting som tilsier at ikke de mest vesentlige forholdene har blitt belyst, selv om det ikke har blitt gitt anledning til å ettergå og verifisere den informasjonen som er blitt gitt.

Det viste seg utfordrende å få tilgang til kontraktdokumentasjon fra aktørene og dette er derfor ikke brukt som datagrunnlag.

Ut over informasjon tilgjengeliggjort gjennom intervjuene og informasjon åpent tilgjengelig på internett, har det vært begrenset mulighet for å gå inn i andre nasjoners tilsynsregimer.

2.5 Forkortelser

ACER	The Agency for the Cooperation of Energy Regulators
AMS	Avanserte måle- og styringssystemer
CERT	Computer emergency response team
CISO	Chief information security officer
CSIRT	Computer security incident response team
DSO	Operatør av distribusjonssystem
ENISA	The European Union Agency for Cybersecurity
ERP	Enterprise resource planning
EU	Den europeiske union
EØS	Det europeiske økonomiske samarbeidsområde
GDPR	General data protection regulation (personvernforordningen)
IKT	Informasjon, kommunikasjon, teknologi
ISO	International organization for standardization
IT	Informasjonsteknologi
kbf	Kraftberedskapsforskriften
KBO	Kraftforsyningens beredskapsorganisasjon
MSSP	Managed security service provider
NCSC	Nasjonalt cybersikkerhetssenter
NIS	Network and information systems
NOU	Norsk offentlig utredning
NSM	Nasjonal sikkerhetsmyndighet
NVE	Noregs vassdrags- og energidirektorat
OT	Operasjonell teknologi
RME	Reguleringsmyndigheten for energi

SaaS	Software as a Service
SCADA	Supervisory control and data acquisition
SDLC	Software Development LifeCycle
SOC	Security operations centre
TSO	Operatør av transmisjonssystem

3 Kartlegging og vurdering av sårbarheter

Det er ulike trusselaktører som kan utnytte digitale sårbarheter i leverandørkjeden, og det er ulike uønskede hendelser som kan ramme kjeden. Dette kan enten være i form av tilsiktede angrep som leverandørkjedeangrep eller kundeangrep, eller det kan knytte seg til tekniske eller menneskelige feil.

- Et leverandørkjedeangrep er en kombinasjon av to angrep (ENISA, 2021). Først er det 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 interne IKT-sikkerhet er god, fordi inngangen kan være gjennom andre aktører i leverandørkjeden. Angrepsteknikker inkluderer blant annet skadelig programvare, utnyttelse av programvaresårbarhet eller konfigurasjonssårbarhet, sosial manipulasjon som for eksempel nettfiske («phishing") eller direktørsvindel, og fysiske angrep eller modifikasjon. Verdiene som er mål for angrepet kan være programvare, programvarebibliotek, kode, konfigureringer, data, prosesser, hardware / maskinutstyr eller mennesker.
- Et kundeangrep er i denne sammenheng et angrep direkte mot KBO-enheten. Relevante angrepsteknikker sammenfaller i stor grad med angrepsteknikkene ved et leverandørkjedeangrep. Verdiene som er mål for angrepet kan være programvare, data, prosesser, båndbredde, finans eller mennesker.
- Utilsiktede tekniske eller menneskelige feil kan for eksempel knytte seg til feil i konfigurering eller dataflyt.

Det mulige utfallsrommet fra slike hendelser er stort. Det norske kraftsystemet og strømforsyningen er kritisk for å opprettholde svært mange samfunnsfunksjoner. Om uvedkommende får tilgang til sensitiv informasjon om kraftsystemet (brudd på konfidensialitet), kan informasjonen potensielt utnyttes til å ramme systemet og samfunnet på et senere tidspunkt. I andre tilfeller kan sårbarheter enten utnyttes eller «realiseres» umiddelbart ved at systemer gjøres utilgjengelige (brudd på tilgjengelighet) eller feiler (brudd på integritet).

Gjennom kartleggingen har informantene belyst flere konkrete sikkerhetsutfordringer som kan oppstå i leverandørkjeden. Disse utfordringene er beskrevet i kapittel 3.1. Med bakgrunn i kartleggingen er deretter spørsmålene som NVE har stilt, besvart i kapittel 3.2 til kapittel 3.8.

3.1 Sikkerhetsutfordringer identifisert i leverandørkjeden

3.1.1 Sårbarheter i gammel teknologi og softwareløsninger

Flere av informantene fremhever at kraftbransjen er kritisk infrastruktur med lang levetid (10, 20 og 30 år) på utstyr og systemer. Dette kan medføre sårbarheter i gammelt utstyr og systemer som ikke er utviklet med tanke på dagens og fremtidens trusselbilde, og med den sikkerheten som ny teknologi og softwareløsninger har. Eksempler på dette kan være krypteringsalgoritmer som ikke møter dagens beste praksis, at det mangler reservedeler eller at leverandørene av systemene ikke lengre støtter oppgraderinger eller sikkerhetspatching («end of support»).

SCADA- og kontrollsystemer oppgraderes hardwaremessig normalt sett rundt hvert 5. år, og underveis legges det til rette for sikkerhetspatching fra leverandør. Det beskrives at det er tilfeller der KBO-enheter benytter gammelt utstyr uten å oppgradere eller gjøre sikkerhetspatchinger. Dette kan skyldes flere forhold som manglende bevissthet og kompetanse hos KBO-enhetene, manglende kravstilling i kontrakter, økonomiske forhold, eller at det ikke er noen som pålegger eller følger opp at verken KBO-enheten eller leverandøren gjør dette. Det er en tiltro til at beskyttelse mot uønskede hendelser er håndtert av segregering av nettverk, fjerntilgangsløsninger, brannmur og andre former for

sikkerhetstiltak. Dette kan imidlertid gi digitale sårbarheter, spesielt der SCADA-systemet er basert på IP-kommunikasjon. Informanter fra leverandører erfarer at denne typen sårbarhet er mest relevant for de mindre KBO-enhetene. Leverandørinformanter uttrykker også at det er ulik tilnærming og bevissthet blant KBO-enhetene knyttet til den sentrale driftskontrollfunksjonen og lokalkontrollfunksjonen på ute på anleggene.

For anlegg hvor det foreligger planer om å oppgradere hele eller større deler av anlegget så kan det være at KBO-enheten ikke ønsker å investere i oppgradering av kontrollsystemet. Erfaringsmessig kan en slik anleggsoppgradering trekke ut i tid. Da kan det være sårbarheter i systemet som man er eksponert for i en lengre periode enn strengt tatt nødvendig – dette gjelder både digitale sårbarheter, men også dersom systemet blir ødelagt. En informant uttalte at *«man må ikke dra strikken for langt, og så bli overrasket»*.

En informant fra KBO-enhetene ga en annen vinkling av problemstillingen knyttet til gammelt utstyr og systemer som ikke lengre støttes av leverandørene («end of support»). Selv om en enkeltstående komponent i utgangspunktet har en lav innkjøpskost, så kan det medføre behov for en større investering og mer omfattende bytte av utstyr for å bytte denne komponenten. Dette kan bli veldig kostbart og kan også medføre at komponenter med kjente digitale sårbarheter blir stående i anlegget for en lengre periode frem til det er besluttet å oppgradere hele eller større deler av anlegget.

En annen problemstilling som er blitt løftet frem av et nettselskap, er at det er vanskelig å ha full kontroll over alt utstyr som står i eget nett når man går langt ut i nettet og flere generasjoner tilbake i tid. Selv om man har kontroll på det som står i framkant i nettet, kan det være gammelt utstyr langt ut i nettet som har blitt digitalisert. Dette kan gjøre at varslinger om sikkerhetshull i en slik komponent ikke fanges opp fordi verken selskapet eller leverandøren har oversikt og kunnskap om at komponenten finnes i nettet.

3.1.2 Sårbarheter som innføres ved ny teknologi og softwareløsninger

Innføring av ny teknologi og softwareløsninger kan medføre nye digitale sårbarheter. Informantene omtaler kraftbransjen som en konservativ bransje der det tar tid før ny teknologi og systemer tas i bruk. Når ny teknologi, systemer og utstyr tas i bruk, så gjøres det med høy kvalitet. Også kraftbransjen moderniseres gjennom økt digitalisering, kritiske systemer tilknyttes i større grad til internett og flere oppdrag utføres i større grad enn før gjennom fjerntilkobling av en tredjepart. De fleste intervjuobjektene, både selskapene og leverandørene, sier at de har tatt i bruk skytjenester (SaaS-tjenester) blant annet på virksomhetsstyringssystem (ERP-system), fagapplikasjoner og andre administrative systemer, mens SCADA-systemer ikke er løftet til sky på grunn av forskriftskrav.

Aktørene som bruker skyløsninger er klar over at det å legge kritisk infrastruktur i sky, der man er avhengig av internett, utgjør en risiko. De anser det likevel som en sikrere løsning enn å ha det lokalt. Dette fordi skyleverandørene er avhengig av å levere ekstremt høy sikkerhet i sine tjenester. Noen få av KBO-enhetene har jobbet tett med større leverandører som tilbyr skytjenester, og også deres erfaring er at store leverandørene gir en bedre sikkerhet enn det de klarer å etablere i egne datasentre på bakken med de ressurser og midler man har tilgjengelig. Både KBO-enhetene og leverandører som tilbyr SaaS-tjenester, fremhever at skyløsninger gir nye muligheter blant annet i form av overvåkning, varsling, kryptering, samt andre verktøy og produkter for sikkerhet enn det man vil ha i et datasenter på bakken eller i en privat sky. En informant påpekte også at selv om det blir bedre, er det fortsatt sikkerhetsutfordringer i de store skytjenestene som det er viktig å være klar over. Andre utfyllende kommenterer fra informantene i denne sammenheng var at:

- Jo mer man outsourcer og legger i sky, jo mindre kontroll har man og jo mer må man stole på leverandørene. Solarwinds-hendelsen er en påminnelse om at en overvåkningsløsning og leverandør man stoler på, kan være kompromittert.

- I en del sammenhenger er det gamle løsninger og teknologi som har fått en ny innpakning og blitt løftet skyen. Selv om autentiseringen har fått bedre, innebygget sikkerhet, kan det være det gamle innholdet og teknologien (uten god sikkerhet) på innsiden. Dette er en problemstilling det er viktig å være klar over i forbindelse med innkjøp av nye løsninger.
- Ikke alle leverandørene tilbyr sikkerhet på beste nivå som del av sin standardleveranse, men krever at selskapene må betale mer for å få det beste sikkerhetsnivået. Informanten mente at det ikke burde være noen grunn til å ikke velge det beste krypteringen, og problematiserte hvorfor leverandører tilbyr dårlig kryptering som standard. Kun en av KBO-enhetene nevnte at de har valgt det aller høyeste sikkerhetsnivået hos Microsoft (Enterprise 5) hvor selskapet har egen krypteringsnøkkel og Microsoft ikke har tilgang til dataene deres. Selv om kun ett av selskapene har fremhevet dette som et viktig sikkerhetstiltak de har gjennomført i grenseskillet mot egne leverandører, så kan det ikke utelukkes at også andre av aktørene som har inngått i denne kartleggingen også har dette sikkerhetstiltaket.
- Ingen av informantene blant leverandørene kjente seg igjen i denne problemstillingen, men uttrykte at de bygger løsninger med sikkerhet fra bunnen av. Flere av leverandørene problematiserte imidlertid at de ikke har kontroll på hvordan kunden ivaretar sin egen sikkerhet og at de er avhengig av at kunden gjør det de skal.
- Flere av informantene fremhevet at feilkonfigurering er en viktig sårbarhet uavhengig av hvor godt eller sikkert systemet eller applikasjonen er, og at det kan oppstå feilkonfigurering uavhengig av om det er i sky eller på bakken («on-premise»). Dette gjør det viktig med gode rutiner uavhengig av plattform.

3.1.3 Sårbarheter som oppstår i grensesnitt mellom ny og gammel teknologi og softwareløsninger

Digitalisering medfører at informasjon fra de industrielle IKT-systemer i stadig større grad blir tilgjengelige i kontorsystemer og skillet mellom industrielle IKT-systemer og administrative IT-systemer utfordres. Dette medfører at sårbarheter som eksisterer i de industrielle IKT-systemene blir eksponert mot nye trusler der et angrep på administrative IT-systemer i kontornette kan være et springbrett inn mot de industrielle IKT-systemene.

- Det har blitt påpekt at det kan oppstå digitale sårbarheter i utviklingen av nye løsninger og ny funksjonalitet når disse skal fungere både mot nytt og gammel grensesnitt. Ny kode må utvikles og testes mot alle grensesnitt og konfigureres riktig opp mot de andre systemene – her er det mange nivå det kan oppstå feil i. Sikker kode i hele livsløpet er leverandørens ansvar («Software Development LifeCycle», SDLC). Enkelte av leverandørene har uttrykt at det er stort fokus på dette og at de har referansesystemer som går mange år tilbake i tid som de bruker til å teste ny kode mot.
- En av informantene blant KBO-enhetene nevnte at digitalisering og optimalisering av produksjons- og vedlikeholdsprosesser gir økende muligheter, men legger også press på å hente ut data og koble ulike systemer sammen med kontrollanlegget. Kontrollanlegget har tradisjonelt sett vært i et eget, avgrenset nettverk og miljø. Når kontrollanlegget kobles mot andre systemer i mindre sikre nettverk, medfører dette eksponering av sårbarheter mot nye trusler. Per i dag er flere dataanalyseløsninger satt opp slik at måledata konsumeres i ett system og at dette inkluderes manuelt ved drift av SCADA-systemet. Det kan forventes at det fremover blir stadig flere sammenkoblinger, enten direkte mot SCADA-systemet eller gjennom at selskapene bygger egne IT-plattformer hvor man setter sammen ulike datakilder slik at IT og OT smelter mer og mer sammen.

3.1.4 Manglende styring av IKT-sikkerhet i pilotprosjekter

Gjennom samtalene med aktørene fremkommer det at det er ulik erfaring knyttet til KBO-enhetenes og leverandørers bevissthet og fokus på sikkerhet i pilotprosjekter som gjennomføres i kraftbransjen, og som innebærer tester i / mot kraftsystemer. Flere KBO-enheter har ikke tilstrekkelig regulering av og krav til IKT-sikkerhet i forbindelse med gjennomføring av pilotprosjekter. Det er blitt påpekt at det i en god del tilfeller ikke er hovedfokus på sikkerhet, men at det nok finnes prosjekter hvor dette har stort fokus. Nedenfor gis det noen eksempler på de tilbakemeldingene informantene har gitt knyttet til dette:

- Noen av informantene både blant KBO-enhetene og leverandørene har erfart at det i pilotprosjektene i hovedsak er fokus på å teste funksjonalitet ut i fra effektiviserings- og produksjonshensyn, og at sikkerhet blir nedprioritert, men at det finnes unntak.
- En informant gir uttrykk for at sikkerhetsfokuset varierer med hvilken type prosess eller del av virksomheten pilotprosjektet berører. I pilotprosjekter mot infrastrukturen så er det bevissthet og fokus på sikkerhet, mens i andre prosesser eller deler av virksomheten som ikke direkte berører infrastrukturen, for eksempel et prosjektverktøy, er det ikke slik.
- Noen av KBO-enhetene uttrykker at de har stort fokus både på personvern og informasjonssikkerhet i pilotprosjekter som gjennomføres og testes i kraftbransjen. Det inngås avtaler med leverandørene og ved behov også med sluttkundene, og leverandørene er bevisste på dette.

Det synes som om mange leverandører i all hovedsak har fokus på utvikling av funksjonalitet, og forutsetter at KBO-enheten setter klare krav for å ivareta sikkerhet i pilotprosjekter som testes i kraftbransjen. Uavhengig av om KBO-enhet stiller funksjonelle krav om sikkerhet, vil sikker kode i hele livsløpet (SDLC) være leverandørens ansvar.

3.1.5 Manglende styring av tilgangskontroll mellom KBO-enhet og leverandører

Kraftberedskapsforskriften stiller krav til brukere både i digitale informasjonssystemer generelt og til tilgang til driftskontrollsystemet spesielt. Kartleggingen viser imidlertid at det er varierende bevissthet og rutiner knyttet til dette blant både KBO-enhetene og leverandørene. Det gis imidlertid inntrykk av at det har skjedd en forbedring av bevissthet og rutiner knyttet til tilgangskontroll mellom KBO-enhetene og leverandørene de siste årene. I det følgende gis det noen eksempler på de tilbakemeldingene informantene har gitt knyttet til dette:

- De fleste KBO-enhetene har strenge rutiner for fjerntilkobling for leverandører, hvor KBO-enheten har mulighet til å åpne opp for leverandør ved behov, der KBO-enheten styrer minst en faktor selv og har full oversikt over hva leverandøren gjør etter at leverandøren har blitt sluppet inn. Selv om det er fokus på kontroll med hvem som har tilgang, kan det være sikkerhets-utfordringer knyttet til at datautstyret som benyttes, ikke er under KBO-enhetens kontroll.
- Informantene gir uttrykk for at det finnes KBO-enheter som tildeler permanente tilganger til leverandører med fellesbrukere. Det finnes også eksempel på at leverandør selv kan invitere inn nye brukere til SCADA-system uten at KBO-enhet har kontroll med dette.
- Flere av informantene har nevnt at de små KBO-enhetene kan ha full kontroll på egne løsninger og har stort fokus og bevissthet på styring av tilgangskontroll mellom KBO-enhet og leverandører – gjerne vel så mye som de store KBO-enhetene har, og at kompleksiteten hos de store kan gjøre det mer krevende å etterleve enn for de små.
- Flere av KBO-enhetene har opplevd at leverandører ønsker enklest mulig oppkobling for å komme seg inn i systemer og at leverandørene har liten bevissthet knyttet til hvilken sårbarhet dette medfører.

- Noen av leverandørene opplever at kundene har dårlige rutiner for brukertilganger både for kundenes egne ansatte (for eksempel kunder som ikke benytter tofaktorautentisering), men også for hvordan brukerinformasjon meddeles leverandøren (her ble det nevnt et eksempel der brukernavn og passord meddeles leverandør i samme e-post).

Det synes som om mange leverandører ønsker enklest mulig tilgang til KBO-enheters systemer, og at det forutsetter at KBO-enheten selv må sette klare krav for å ivareta sikkerhet i styring av tilgangskontroll for leverandør.

3.1.6 Sårbarheter som kan oppstå i lange leverandørkjeder av hardware- og softwarekomponenter

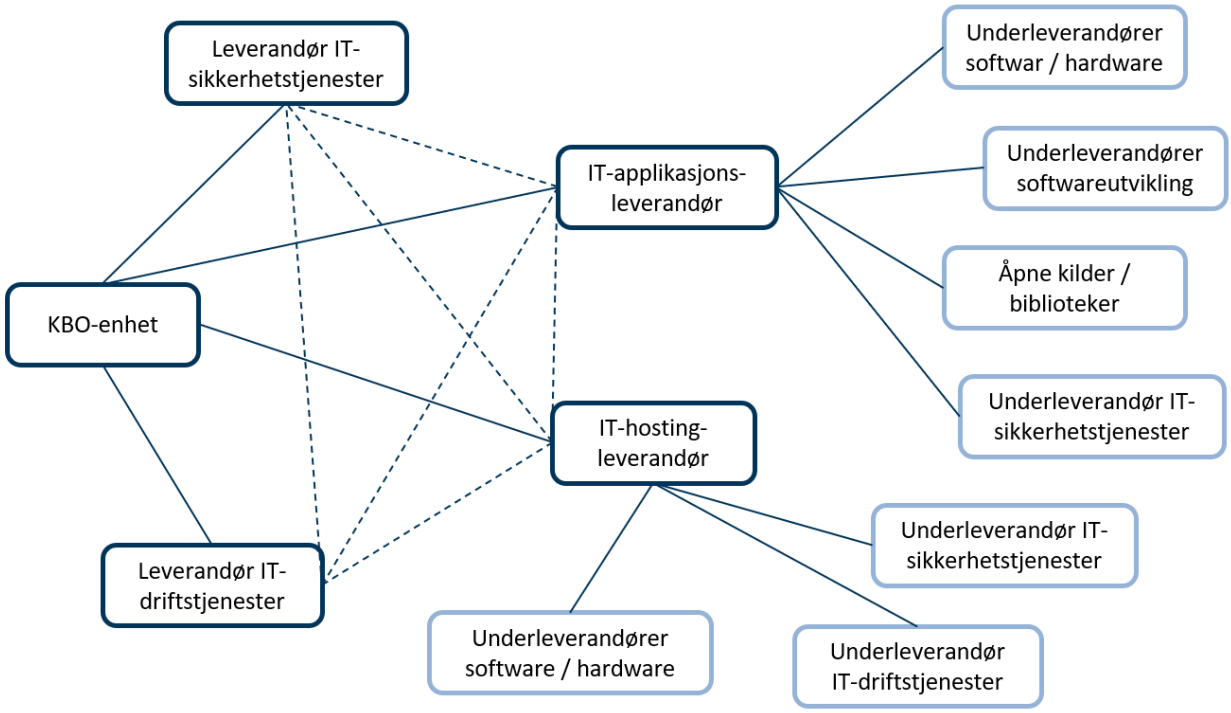
Flere av informantene nevnte sårbarheter knyttet til lange leverandørkjeder av hardware- og softwarekomponenter som inngår i leveransen av et system eller produkt. Dette er basert på tillit til leverandørene og det er vanskelig både for KBO-enhetene og for leverandørene å ha kontroll med hele kjeden og alle leddene som inngår. Frem til et produkt selges og tas i bruk i kraftforsyningen i Norge, er det et stort apparat bak fremstillingen av produktet med mange ledd av underleverandører, diverse hardware-, firmware- og softwarekomponenter, samt individer som designere, utviklere, testere, teknikere og ingeniører med spisskompetanse i hvert ledd av prosessen. Alt fra design og utvikling av en enkelt chip, design og implementering av større system hvor chipene inngår sammen med annen hardware, firmware og software, til design og utvikling av endelig produkt. Det ble nevnt eksempler som at dersom en underleverandør har installert ondsinnet programvare eller byttet ut et sertifikat i hardwaren som inngår i produktet, så klarer man ikke kontrollere dette. Dette reguleres i liten eller ingen grad av myndigheter, selskaper eller leverandører, og det er heller ikke utviklet god nok metodikk for å klare å detektere slik maskinvareproblematikk.

Figur 4: Eksemplifisering av lange verdikjeder for hardware- og softwarekomponenter frem til ferdig produkt [2] (True et. al, 2021)

[2] Global semiconductor market as of 2016, published in 2018 by SIA adapted from semiconductors.org. Source: UN Comtrade and Taiwan Customs Administration, Ministry of Finance; Year of 2014.

3.1.7 Kompleks og uavklart organisering og ansvarsforhold mellom KBO-enhet og leverandører

I kraftbransjen er det flere ulike konstellasjoner mellom KBO-enhet og leverandører. Det er mange ulike leverandører som KBO-enheten enten har et direkte kundeforhold til, eller et indirekte kundeforhold som underleverandør til en av leverandørene. I alle tilfeller er det flere parter inne i bildet, hver med sitt ansvar for å ivareta sikkerheten i løsningen. Ett eksempel kan være en KBO-enhet som har kjøpt en applikasjon fra en applikasjonsleverandør. Applikasjonen er installert i et norsk datasenter forvaltet av en hostingleverandør, og KBO-enheten har outsourcet drift til en IT-driftstjenesteleverandør. I tillegg har datasenteret også egen IT-driftstjeneste. I et slikt oppsett kan det være uklarheter knyttet til hvem som har ansvar for å overvåke applikasjonen. KBO-enheten vil stille noen krav til applikasjonen, men applikasjonsleverandøren har ikke oversikt over hvilke sikkerhetskrav KBO-enheten har stilt til hosting-leverandøren eller til IT-driftsleverandøren. Det finnes også eksempler på andre konstellasjoner der IT-driftsleverandører tar et større, mer komplett / integrert plattformansvar, inkludert ansvar for leveranse og sikkerhet i hostingtjenester, skytjenester, applikasjonstjenester, sikkerhetstjenester osv. I alle tilfeller gir flere av informantene inntrykk av at det er behov for å tenke mer helhetlig når det kommer til sikkerhet.



Figur 5: Eksemplifisering av nettverk av leverandører og underleverandører som KBO-enheten er avhengig av

3.1.8 Manglende identifisering og lukking av digitale sårbarheter

Det fremkom flere årsaker til at digitale sårbarheter ikke identifiseres og lukkes. Dette inkluderer blant annet:

- Manglende rutiner og prioritering hos leverandørene
- Økonomiske forhold
- Uklar ansvarsfordeling mellom KBO-enhet og leverandører, samt lange leverandørkjeder
- Manglende kompetanse og kapasitet hos KBO-enhetene
- Manglende systemoppfølging fra KBO-enhetene
- Teknisk gjeld i gammel teknologi og software
- KBO-enheters manglende kontrollmulighet ved bruk av store underleverandører

Alle leverandørene sier de har fokus på å identifisere og lukke digitale sårbarheter i egne produkter. Leverandørene nevnte blant annet rutiner for gjennomgang og sikkerhetstesting av ny kode, samt regelmessige trusselmodelleringer, penetrasjonstester og sårbarhetsanalyser for å identifisere og håndtere sårbarheter i egne løsninger. Noe gjøres internt og noe gjøres av eksterne, uavhengige sikkerhetstjenesteleverandører.

Leverandørene legger også softwarebidrag fra andre underleverandører inn i utvikling av egne løsninger. Dette er både fra store underleverandører som for eksempel Oracle, Microsoft og Esri, men også fra åpne kildekoder («open source»). En av leverandørene nevnte eksplisitt at det også her gjøres regelmessige sikkerhetssjekker av slike tredjepartskomponenter, men at leverandørene har liten påvirkningsmulighet og må stole på sikkerheten til de store underleverandørene som for eksempel Microsoft Azure. Det ble også nevnt at det er utfordrende for leverandører å ha oversikt over alle åpne kildekoder i egne produkter og eventuelle identifiserte sårbarheter i disse.

Leverandørene ga inntrykk av at kundene varsles ved funn av (alvorlige) sårbarheter.

En utfordring som ble nevnt av en av leverandørene var viktigheten av å prioritere tid og ressurser internt til å få lukke sårbarhetene, og at leverandøren jobbet aktivt opp mot ledergruppen i eget selskap for å sikre prioritet. Selv om leverandørene tenker sikkerhet i forbindelse med utvikling, så er det likevel en usikkerhet om alle leverandørene har tilstrekkelig rutiner, kapasitet og et anerkjent ansvarsforhold for å følge opp sikkerheten i alle egne systemer i drift hos kunder.

Informantene fra de store KBO-enhetene sier at de også gjør regelmessige tiltak for å identifisere og håndtere sårbarheter i leverandørenes produkter som er i bruk hos dem selv. Selv om dette kun ble nevnt av de store KBO-enhetene, er ikke det ensbetydende med at lignende ikke gjøres også av de andre KBO-enhetene. Tiltak som ble nevnt var blant annet regelmessige IT-revisjoner, sårbarhetsanalyser og penetrasjonstester. KBO-enhetene mener at kvaliteten til leverandørene varierer. For en del av testene KBO-enhetene gjennomfører selv oppdages det for mange feil som er enkle å finne og burde vært avdekket av leverandørene selv på et tidligere tidspunkt. Andre problemstillinger som ble nevnt er funn som gjentas fra det ene året til neste, og at for noen løsninger er det teknisk gjeld som ikke er så lett å lukke for leverandørene. Da må man som kunde leve med systemet selv med kjente sårbarheter. Dette underbygger usikkerheten knyttet til om alle leverandørene har tilstrekkelig rutiner, kapasitet og et anerkjent ansvarsforhold for å følge opp sikkerheten i egne systemer i drift hos kunder.

Leverandørene påpekte at selv om de lukker sårbarheter i egne produkter, så er man også avhengig av at kunden jevnlig oppdaterer og patcher sine systemer, slik at de kontinuerlig er oppdatert til siste versjon. En informant blant leverandørene mente at de største sårbarhetene kommer via operativsystemer som Windows og Linux, og at det viktigste er at kundene jevnlig oppdaterer operativsystemet sitt. Leverandørene uttrykte at ikke alle KBO-enhetene hadde satt av tilstrekkelig med ressurser til drift av egne systemer, verken ved outsourcing eller internt.

KraftCERT[3] nevnes av flere informanter å være en viktig arena og funksjon i kraftbransjen for blant annet utveksling av informasjon om nye trusler, sårbarheter og angrep. Det er NVE som er sektorvist respons-miljø for IKT-sikkerhetshendelser i kraftforsyningen, der NVE har delegert noen oppgaver til KraftCERT. KraftCERT er KBO-enhet og ivaretar en responsfunksjon for energisektoren der medlemskap er frivillig. Av informantene blant KBO-enhetene er alle med unntak av en medlem av KraftCERT. De KBO-enhetene som er del av Nettalliansen inngår i et felles KraftCERT-medlemskap som forvaltes av alliansen. Flere av leverandørene er medlem av KraftCERT for å utveksle informasjon om sårbarheter, mens enkelte leverandører har påbegynt en dialog med KraftCERT uten enda å ha formalisert dette i form av medlemskap.

En av leverandørene som var medlem i KraftCERT informerte at de varsler KraftCERT om alle sårbarheter som avdekkes i egne produkter og motsatt. Denne prosessen fungerer, men mye av den informasjonen som kommer fra KraftCERT til leverandøren mente leverandøren var kjent fra andre kilder. Leverandøren mente at dialogen med KraftCERT var enda viktigere for KBO-enhetene. KBO-enhetene får også informasjon om at det er avdekket sårbarheter i en viss type utstyrskomponent. Da kan KBO-enheten forsikre seg hos sine leverandører at deres systemer ikke inneholder denne utstyrskomponenten. Alternativt kan det avklares hvilke tiltak som må gjøres for å kompensere for sårbarheten dersom denne utstyrskomponenten inngår i egne systemer.

3.1.9 Manglende kapasitet, kunnskap og kompetanse hos både KBO-enheter og leverandører

Flere informanter sier det har skjedd en endring i bransjen med tanke på IKT- og cybersikkerhet de siste årene og at temaet nå blir løftet oppover i organisasjonene og inn på leder- og styrenivå. Både større sikkerhetshendelser som har inntruffet de siste årene (eksempler som er blitt nevnt er dataangrepene på både Hydro, Volue, Solarwinds og Østre Toten kommune), og den nye kraftberedskapsforskriften som stiller strengere krav til både informasjonssikkerhet og driftskontrollfunksjonen, nevnes som årsaker til dette. Informantene blant leverandørene sier likevel at det er ulik grad av modenhet knyttet til informasjonssikkerhet og ulik tilgang på ressurser hos kundene, selv om det generelt er en økende bevissthet i bransjen.

Gjennom samtalene dannes det et inntrykk av at det er forskjell på KBO-enhetene. Flere av informantene fremhever at det ikke nødvendigvis er slik at alle de store er gode, og alle de små dårlige. En informant sa at *«man kan ha små selskap som er veldig kompetente og interesserte, og så kan man ha halvstore selskap som tar litt lett på det»*. Nedenfor gis det noen eksempler på momenter som fremkom gjennom samtalene.

- Flere informanter sier at det kan være en utfordring for de små og mellomstore KBO-enhetene at de har få ressurser, der enkeltindivider må ivareta flere roller i organisasjonen (for eksempel ikke dedikert ressurs på IT og/eller sikkerhet). Det beskrives imidlertid også at de små og mellomstore KBO-enhetene har en mer oversiktlig organisasjon og systempark der det er lettere å ha kontroll over utstyr, systemer og tilganger. I tillegg kan det være enklere å nå ut til hele organisasjonen for å forankre og få til etterlevelse av interne prosesser, rutiner og systemer.
- Flere sier at mange av de små KBO-enhetene er helt avhengige av IT-leverandører for å ivareta sikkerheten, og at flere benytter den lokale IT-leverandøren som i utgangspunktet ikke har noe bevissthet til eller kompetanse på kraftberedskapsforskriften og muligens også mindre kompetanse på IT-sikkerhet. I denne sammenheng nevnes Nettalliansen å være en aktør som bidrar med arenaer, brukerforum og prosjekter hvor medlemmene kan delta og dele erfaringer med hverandre. Dette oppleves som et bidrag til å heve kompetansenivået og bevisstheten og derigjennom bidrar til bedre sikkerhet blant de små og mellomstore aktørene. En aktør mente

[3] KraftCERT https://www.kraftcert.no/

imidlertid det var farlig dersom KBO-enhetene overlater ansvaret til Nettalliansen. En annen problemstilling kan være at mange KBO-enheter blir avhengige av de samme leverandørene gjennom felles fremforhandlede innkjøpsavtaler gjennom Nettalliansen.

- De store KBO-enhetene gir inntrykk av at de har systemer, rutiner og prosesser på plass for å ivareta sikkerheten i egne leveranser. Det er imidlertid flere informanter som opplever at det ikke er satt av tilstrekkelig ressurser til å operasjonalisere de kravene som er satt. Som tidligere nevnt, er det flere leverandører som oppfordrer sine kunder til å oppgradere systemene sine straks det foreligger en sikkerhetsoppdatering, men at dette ikke alltid gjøres av alle da det ikke er satt av tilstrekkelig ressurser til drift av systemene, verken ved outsourcing eller internt. Det kan dermed være en utfordring at det ikke er samsvar mellom det som vedtas skal gjøres, og ressurser avsatt til å levere på det som er vedtatt. Noen stiller også spørsmål ved om det å ha gode systemer, rutiner og prosesser fullt ut kompenserer for den økte kompleksiteten det er å være stor sammenlignet med mindre enheter.
- En av informantene blant leverandørene som tilbyr applikasjonstjenester i skyen, mente at det generelt var lite kompetanse blant KBO-enhetene knyttet til hva skyleverandører som for eksempel Microsoft Azure, kan tilby av ulike sikkerhetsløsninger. Informanten mente at enkelte av KBO-enhetene pekte seg ut, men at dette ikke nødvendigvis hadde sammenheng med størrelsen på KBO-enheten: Flere av de mindre KBO-enhetene kan ha vel så mye kompetanse som de større og dette henger først og fremst sammen med hvor fremoverlente KBO-enhetene er på digitalisering.

Flere KBO-enheter gir tilbakemelding om at det er varierende grad av bevissthet knyttet til sikkerhet hos leverandørene og at det er usikkert om alle leverandørene innser at de selv er en mulig angrepsvektor («stepping stone») inn mot kritisk infrastruktur. En informant uttalte at *«noen leverandører har ikke kommet videre fra sikkerhetsarbeidet tidlig på 2000-tallet»*. En annen informant uttalte at de *«har erfart at leverandører ikke følger rutinene sine – kanskje ikke en gang snakker sant»*. Alle leverandør-informantene sier på sin side at de selv har sterk bevissthet på sikkerhetsutfordringer og at de er bevisste på at de selv er en mulig angrepsvektor inn mot kritisk infrastruktur. Samtalene med leverandørene gir imidlertid ikke et grunnlag til å si noe om denne bevisstheten gjennomsyrer organisasjonen eller ikke. Leverandørinformantene pekte videre på at andre, gjerne mindre eller nye leverandører til kraftbransjen kan ha lavere kompetanse og bevissthet knyttet til sikkerhet.

De fleste av leverandørene som har deltatt i kartleggingen, er enten ISO 27001 sertifisert, har påbegynt arbeid med å bli ISO 27001 sertifisert eller sier at de har interne systemer, rutiner og prosesser i henhold til kontrollelementene i ISO 27001. Mindre leverandører sier at de jobber mot ISO 27001 sertifisering for å heve egen kompetanse og intern sikkerhet. De større leverandørene uttrykker at sertifisering i henhold til internasjonale standarder legger gode føringer for hvordan bygge informasjonssikkerhet med en risiko-basert tilnærming i bunn, og at det vitner om at virksomheten har lagt et formalisert og strukturert virksomhetsstyringssystem i bunn for informasjonssikkerhet. De fleste aktørene, både leverandører og KBO-enheter, uttrykker imidlertid at sertifisering i seg selv ikke sier noe om godheten og effektiviteten av kontrollmekanismene som er satt opp. Flere leverandører var også opptatt av at krav til sertifisering kan hemme innovasjon i bransjen da det vil sette strengere krav til nye aktører. Det ble også påpekt at en virksomhet kan ha gode og effektive kontrollmekanismer selv om man ikke er sertifisert.

3.1.10 Manglende regulering av IKT-sikkerhet i anbudsdokumenter og kontrakter, og manglende oppfølging av leverandør

Krav til IKT-sikkerhet

Informantene fra de store KBO-enhetene sier at de har systemer, rutiner og prosesser for regulering av og krav til IKT-sikkerhet i anbudsdokumenter og kontrakter. Også her har det vært en endring de siste årene og noen av kravene som stilles av KBO-enhetene i anbud og kontrakter er ganske nye. Noen av KBO-enhetene sier imidlertid at de ikke stiller eksplisitte IKT-sikkerhetskrav i kontraktene, men at IKT-sikkerhet bygges på tillit til de store leverandørene og samarbeidspartnere.

Erfaring fra KBO-enheter som stiller krav til IKT-sikkerhet i anbudsdokumenter og kontrakter mot leverandører:

- Flere tar utgangspunkt i statens standardavtaler, samt NVEs mal for informasjonssikkerhetsavtale.
- Ingen av KBO-enhetene har stilt krav til sertifisering i henhold til ISO 27001 eller andre internasjonale standarder.
- Flere KBO-enheter stiller spesifikke krav til leverandørene, for eksempel krav i henhold til kraftberedskapsforskriften og NSMs grunnprinsipper, til at leverandør har styringssystem i henhold til ISO eller andre anerkjente standarder, krav og forventninger til softwareutviklings-metodikk, varsling og responstid, samt kontraktsfestet rett til å gjennomføre revisjon av leverandør.
- Flere av KBO-enhetene stiller krav om at leverandørene må gjøre en vurdering, samt dokumentere hvordan de etterlever kontraktskravene, for eksempel hvordan grunnprinsippene håndteres eller hvordan informasjonssikkerhetsavtalen etterleves.
- Noen KBO-enheter gjør IT-risikoanalyser, inkludert landrisikoanalyser, som underlag for anskaffelse av IT-systemer. Det er spesielt fokus på dette ved anskaffelse av ny teknologi eller software.
- Både Nettalliansen og Valider nevnes som innkjøpsallianser som har hjulpet bransjen på dette området. Avtalene som inngås i alliansen stiller krav til revisjon av leverandør og under-leverandør, der alliansen gjennomfører revisjoner på vegne av selskapene.
- Flere KBO-enheter har erfart at leverandører har vanskeligheter med å dokumentere hvordan de skal håndtere og etterleve kontraktskravene. Leverandører har også gitt tilbakemelding om at *«det er første gang noen spør»* om dette.

Erfaring fra leverandører:

- En leverandør sier det er stor forskjell på kontraktene de mottar fra KBO-enhetene. Noen bruker statens standardavtale, mens andre bekrefter bestilling i henhold til leverandørens tilbud på e-post.
- Flere leverandører bekrefter at de vanligvis i en anbudskonkurranse må gjøre en egenvurdering og dokumentere etterlevelse av kundens krav selv om de er sertifisert i henhold til internasjonale standarder.
- En leverandør sier at enkelte kunder ikke stiller krav til sikkerhetsavtale, og at det da blir opp til leverandør å ta initiativ til dette. Det er imidlertid uklart om dette eksempelet gjaldt KBO-enheter eller leverandørens kunder generelt.
- En av SaaS-applikasjonstjenesteleverandørene mente at kravspesifikasjonene som de mottar fra KBO-enhetene, ikke er tilpasset den type teknologi, leveranse- og driftsmodell som de tilbyr. Deres erfaring var at kundene stiller sikkerhetskrav i henhold til tidligere, mer tradisjonelle, systemer de har fått levert, med standard krav som om løsningen skulle vært installert fysisk («on-premise»).

- En leverandør sier at bestillerne fra KBO-enhetene muligens stiller strenge krav til IT-sikkerhet, men det er blitt mer forretningsfokuserte beslutningstakere og da mister man fokuset på å faktisk ivareta sikkerheten.

Intervjuobjektene nevner flere dilemmaer og problemstillinger knyttet til regulering av og krav til IKT-sikkerhet i anbudsdokumenter og kontrakter:

- En informant uttalte at det var viktig med gode kontrakter og avtaler, men at det må være en praktisk komponent i dette da mer sikring og flere revisjoner medfører økte kostnader. Det er viktig å sikre grunnsikkerheten, men det er urimelig å tro at selskapene ber om mer enn det som er påkrevd.
- En informant mente at det er utfordrende for leverandørene dersom alle KBO-enhetene skal ha ulike informasjonssikkerhetsavtaler.
- En informant mente det var utfordrende for KBO-enhet å få leverandør til å underskrive informasjonssikkerhetsavtale basert på NVEs mal. Dette gjaldt både for store og mellomstore leverandører, mens små leverandører signerte uten å reflektere over og forstå hva man signerte på. Punktene som oftest blir utfordret er knyttet til adgang til å gjennomføre revisjon av leverandører og det at kunden kan motsette seg at leverandør bytter underleverandør (transparens i leverandørkjeden). En annen informant mente imidlertid at NVEs mal for sikkerhetsavtale ikke var tilstrekkelig.
- Det er utfordrende å få endret kontraktene etter at de er inngått.
- Alle avtalene skal i utgangspunktet følge alle lover og forskrifter, der lovpålagte endringer må gjennomføres av leverandør og kunden betaler. Ved lange levetid på utstyr (og kontrakter) er det imidlertid ikke alltid praktisk gjennomførbart å oppgradere alle gamle system til gjeldende praksis.
- Noen av de store leverandørene krever å bruke egne standardkontrakter. Norske KBO-enheter har liten innflytelse og det blir et ultimatum, *«take it, or leave it»*. Det er kun de største KBO-enhetene som kan ha kapasitet og ressurser og er store nok til å få gjennomslag for andre krav. Selv de store KBO-enhetene sier de har liten innflytelse på blant annet de internasjonale skytjenesteleverandørene.
- For å få robuste og gode kontrakter kreves det spesialkompetanse på det juridiske og på IT-sikkerhet, spesielt ved anskaffelse av skytjenester. I enkelte tilfeller har KBO-enhetene kjøpt juridiske tjenester fra advokatfirma som er spesialiserte på dette området for å kunne forhandle og få gjennomslag for egne krav.
- Spesielt utenlandske leverandører kjenner ikke kravene i kraftberedskapsforskriften. Kravene i kraftberedskapsforskriften er særnorske og kraftberedskapsforskriften med veileder finnes kun på norsk. Det gjør det utfordrende for utenlandske leverandører å forstå innholdet og kravene som stilles.
- Det oppleves som spesielt utfordrende å fremforhandle særnorske krav mot utenlandske leverandører der KBO-enhet forhandler med en norsk salgsrepresentant og der systemansvarlig er lokalisert i utlandet. Enkelte leverandører har ikke engang norsk salgsrepresentant og da forhandler KBO-enheten direkte med utlandet.
- Dersom leverandøren har lovet den samme respons- og feilrettingstiden til mange kunder, vil det være en utfordring med mangel på ressurser fra leverandøren i en reell hendelse.

Oppfølging av IKT-sikkerhet

Et økende fokus og mer strukturerte prosesser fra KBO-enhetene på regulering av og krav til IKT-sikkerhet i anbudsdokumenter og kontrakter, medfører at også leverandørene blir bedre på dette området. Selv om KBO-enhetene har mer fokus på regulering av og krav til IKT-sikkerhet, så er det varierende, og for enkelte til dels mangelfull, oppfølging og verifisering av etterlevelse og håndtering av de kravene som er stilt til leverandørene:

- En av KBO-enhetene sier at leverandørene rangeres ut i fra kritikalitet og det etableres informasjonssikkerhetsplan for hver leveranse. Denne planen følges opp med regelmessige møter med og revisjoner av leverandørene avhengig av kritikalitet.
- En av KBO-enhetene sier de har gjennomført noen revisjoner av leverandører og at de er i ferd med å etablere en rutine der leverandørene skal gjøre en årlig egenevaluering med grundigere oppfølging av noen av leverandørene.
- Andre KBO-enheter sier de ikke har gjennomført egne revisjoner, mens noen har fått 3. part til å gjennomføre revisjoner av kritiske leverandører, samt fått tilsendt revisjonsrapporter fra leverandør.
- Ingen KBO-enheter eller leverandører har nevnt at de har gjennomført eller deltatt i øvelser som involverer både kunde og leverandører.

Intervjuobjektene nevner også flere dilemmaer og problemstillinger knyttet til oppfølging av leverandører gjennom revisjoner:

- De små KBO-enhetene har begrenset med ressurser og prioriterer ikke nødvendigvis å gjennomføre revisjoner av leverandører.
- Uavhengig av størrelse stiller det krav til kompetanse å gjennomføre revisjoner der man skal ettergå tekniske løsninger.
- Dersom KBO-enhetene skal bruke 3. part til å gjennomføre revisjoner av leverandører, medfører dette kostnader.
- Det kan også være en utfordring å få tilgang til systemer, rutiner og prosesser som underlag for revisjon hos leverandør.
- Erfaring fra revisjoner viser at det kan være krevende for KBO-enhetene å få de riktige personene i tale hos leverandør. KBO-enhetene uttrykker at dersom man snakker med de riktige personene hos leverandør, får man en god forståelse av hvordan situasjonen er.
- For de store globale leverandørene er det utfordrende for KBO-enhetene å få tilgang til informasjon. Disse leverandørene har ofte gjennomført egne 3. partsverifikasjoner som de deler med sine kunder.
- Nå er det lagt opp til at hver KBO-enhet skal sjekke egne leverandører. Da kan det komme flere etter hverandre til samme leverandør og spørre om det samme. Det er lite samkjøring av revisjoner av leverandører.

3.1.11 Usikkerhet knyttet til håndtering av kraftsensitiv informasjon

Flere informanter fremhever usikkerhet knyttet til håndtering av kraftsensitiv informasjon i samarbeidet mellom KBO-enhet, leverandører og underleverandører som en digital sårbarhet. På et overordnet nivå er det ikke en felles forståelse av hva som er kraftsensitiv informasjon blant KBO-enheter, leverandører og underleverandører til kraftbransjen. I samtalene kom det frem noen eksempler som er beskrevet under.

- Både en informant blant KBO-enhetene og en informant fra leverandørene nevnte utveksling og håndtering av kraftsensitiv informasjon i forbindelse med anbudsprosesser som mulig digital sårbarhet i leverandørkjeden. I forbindelse med anbudsprosesser har KBO-enhetene behov for å dokumentere hva man ønsker å bestille fra leverandør. Dette kan for eksempel være i form av tegninger av en kraftstasjon som kategoriseres som kraftsensitiv informasjon. Mange av de store leverandørene er internasjonale og har et stort nettverk av underleverandører som også er internasjonale. Selv om kraftberedskapsforskriften stiller krav til at den som har fått tilgang til kraftsensitiv informasjon av en KBO-enhet ikke kan videreformidle den kraftsensitive informasjonen til andre, har KBO-enheten liten kontroll med hvordan leverandør håndterer slik kraftsensitiv informasjon, samt i hvilke land eller hos hvilke underleverandører slik informasjon

ender opp. Leverandørene på sin side skal dokumentere sitt løsningsforslag ovenfor kunden og i den forbindelse er det ofte behov for å gi detaljert informasjon om egne systemer og løsninger til kunden. Leverandøren har liten kontroll med hvordan KBO-enheten håndterer denne informasjonen. Dersom informasjonen kommer på avveie, kan dette sette andre av leverandørens kunder i en sårbar posisjon.

- Kraftbransjen har allerede tatt i bruk digitale tvillinger. Dette gjelder spesielt for vannkraftverk der en av hensiktene er å optimalisere drifts- og vedlikeholdsprosessene. En informant nevnte at det er usikkerhet knyttet til om KBO-enheter og leverandører har forståelse for hva som er kraftsensitiv informasjon med tanke digitale tvillinger, at digitale tvillinger også kan utsettes for digitale angrep enten de er lagret hos selskapene selv eller hos leverandørene, og at digitale tvillinger må sikres i henhold til dette.
- En informant nevnte et annet eksempel på usikkerhet knyttet til kategorisering av data i henhold til kraftberedskapsforskriften. Kraftbransjen moderniseres med mer utstrakt bruk av sensorer og IT-teknologi til innsamling av data. Hvert enkelt datasett er i seg selv ikke kraftsensitiv informasjon, men det ble uttrykt som en usikkerhet om dette kunne bli kategorisert som kraftsensitiv informasjon dersom man samlet store nok mengder av slike datasett.
- Flere informanter nevnte at det ikke er samsvar mellom hva som defineres som kraftsensitiv informasjon og informasjon som allerede finnes på internett (for eksempel på Google Maps eller NVEs Atlas).

Informantene ga også inntrykk av at det er for mye som kategoriseres som kraftsensitivt. Dersom *«alt»* defineres som kraftsensitiv informasjon, vil man kunne miste fokus på å sikre det som faktisk er relevant kraftsensitiv informasjon.

3.1.12 Manglende sikkerhetskultur og bevissthet på informasjonssikkerhet

Kraftbransjen omtales som en bransje med høy sikkerhetskultur og beredskap sammenlignet med andre bransjer. Flere informanter nevnte likevel organisasjonens sikkerhetskultur og i hvilken grad de ansatte er utrustet og bevisst på informasjonssikkerhet som en mulig sårbarhet. En dårlig sikkerhetskultur eller manglende bevissthet kan medføre menneskelig feilhandling enten i form av en utilsiktet handling eller mangel av handling av ansatte og brukere. Dette kan resultere i redusert sikkerhet eller generere en hendelse. Eksempler på menneskelige feil som ble nevnt i samtalene var:

- Dårlige passord
- Dårlig håndtering av passord (for eksempel gjennom å dele brukernavn og passord i samme e-post eller å lagre passord i nettleseren eller tilgjengelige tekstfiler)
- Bruk av PC til jobb og private applikasjoner
- Bruk av USB minnepinner
- Mangelfull fysisk sikring av enheter
- Mangel på programvare- og operativsystemoppdateringer

En ondsinnet aktør kan også bruke de ansatte som angrepsvektor i et målrettet angrep. Dette kan for eksempel være i form av nettfiske («phishing») eller direktørsvindel. Cyberkriminelle prøver seg ofte på enkleste vei inn gjennom menneskene – det er viktig som selskap å være bevisst på dette trusselbildet.

Flere av informantene, både KBO-enheter og leverandører, uttrykker at de jobber aktivt med sikkerhetskultur og bevissthet i egen organisasjon. Dette inkluderer både regelmessig opplæring og oppfølging av alle ansatte, inkludert praktiske øvelser, samt å systematisk og aktivt jobbe med leder-gruppene på dette området. Det er likevel flere informanter som sier at det er store forskjeller i hvor stort fokus dette har hos leverandørene, også de som er mer spesifikt rettet mot kraftbransjen. Noen

leverandører sies å ha det meste av sikkerhetsarbeidet på plass og jobber systematisk med dette, mens andre leverandører sies å være mindre modne og mindre bevisste på sikkerhetsarbeidet. Dette gjelder alle typer leverandører, både av SCADA-systemer, nettinformasjonssystemer (NIS), kundeinformasjons-systemer (KIS), analysesystemer osv. Det vil si systemer som behandler kraftsensitiv informasjon og/eller er viktig for analyse og styring inn mot bransjen. For nystartede selskap og nye leverandører til kraftbransjen kan det være manglende forståelse for hvilken risiko man utsetter kraftforsyningen for.

3.1.13 Manglende bakgrunnssjekk i forbindelse med ansettelse og kontraktsinngåelse

Ansatte hos både KBO-enheter og leverandører kan være utsatt for eksternt press eller ha en motivasjon til å ta imot penger for å gi fra seg opplysninger eller gjøre andre skadelige handlinger mot digitale systemer som påvirker integritet og/eller tilgjengelighet. En informant blant KBO-enhetene uttrykker at det gjøres bakgrunnssjekker på ulike nivå, inkludert for leverandører som har kritiske roller. KBO-enheten bruker de strengeste og mest omfattende mekanismene de har tilgang til, inkludert krav til politiattest for anlegg som er klassifisert høyt. Det er imidlertid ikke praktisk mulig å gjøre bakgrunnssjekk på alle som skal inn i en kraftstasjon for å gjøre en jobb – dette håndteres med adgangskontroll og ledsagelse under arbeidet. En informant blant leverandørene problematiserer imidlertid at leverandøren kun kan gjennomføre overfladisk bakgrunnssjekk i forbindelse med ansettelser.

3.1.14 Avhengighet til leverandør i forbindelse med håndtering og gjenoppretting

Spesielt ved hendelser er det flere informanter som uttrykker at det er et stort behov for dybdekunnskap om de berørte produktene og systemene for å kunne håndtere situasjonen og gjenopprette. Dette gjelder spesielt for digitaliserte industri- og kontrollsystemer. Her kreves det ofte at leverandørene går inn i systemene for å feilsøke og behovet for dette øker ettersom kraftbransjen digitaliseres mer og mer. Det er et begrenset antall personer som har den nødvendige dybdekompetansen.

De viktigste SCADA- og kontrollsystemleverandørene er internasjonale. De har noe kompetanse i Norge, men inntreffer det kompliserte hendelser er man avhengig av utenlandsk spisskompetanse. Om leverandør gis tilgang til systemet via fysisk tilstedeværelse eller fjerntilgang avhenger av risiko knyttet til å gi tilgang opp mot hvor mye det haster. En informant sa at under covid-19-pandemien ble 3. partstilkobling åpnet opp mot noe som normalt krever fysisk tilstedeværelse da det ble vurdert å medføre lavere risiko enn smitterisiko for kritisk personell.

Avhengigheten til leverandør i forbindelse med håndtering og gjenoppretting har vært der lenge, men det er blitt større bevissthet i bransjen. Det er viktig at KBO-enhetene har beredskapsplan som inkluderer en oversikt over komponenter det er nødvendig å ha kompetanse på, samt hvilken type kompetanse som er nødvendig, for å feilsøke og reetablere systemene igjen – både i egen organisasjon og fra leverandører.

Flere av informantene fremhevet også viktigheten til KraftCERT sin koordinerende rolle mellom kraftbransjen, leverandør og sikkerhetsmyndighetene basert på erfaring fra angrepet mot Volue.

En av informantene nevnte at under covid-19-situasjonen er KBO-enheter med tilhørende personell-grupper definert som sentrale for å opprettholde driften av kraftforsyningen og de har dermed spesielle vilkår. Dette omfatter ikke leverandørene. I en krisesituasjon kan det imidlertid være behov for å inkludere leverandørene.

3.2 I hvilken grad er IKT-sikkerhet regulert i kontraktregimene nedover i en leverandørkjede

Gjennom samtalene fremkommer det at det er variasjon i hvilken grad KBO-enhetene regulerer og stiller krav til IKT-sikkerhet i anbud og kontrakter med leverandørene. Flere KBO-enheter har ikke tilstrekkelig regulering av og krav til IKT-sikkerhet i alle prosesser. Dette gjelder både i anbudsprosesser og kontraktsinngåelse for alle typer IT-anskaffelser og som inkluderer hele livsløpet, samt ved gjennomføring av pilotprosjekter i bransjen. De store KBO-enhetene sier at de har systemer, rutiner og prosesser for regulering av og krav til IKT-sikkerhet i anbudsdokumenter og kontrakter. Det har vært en endring de siste årene og noen av kravene som stilles av KBO-enhetene i anbud og kontrakter er ganske nye. KBO-enhetene opplever det spesielt i møte med store leverandører som vanskelig å stille krav, med liten påvirkningsmulighet. Enkelte KBO-enheter sier imidlertid at de ikke stiller eksplisitte IKT-sikkerhetskrav i kontraktene, men at IKT-sikkerhet bygges på tillit til de store leverandørene og samarbeidspartnere.

KBO-enhetene erfarer at et økende fokus og mer strukturerte prosesser fra KBO-enhetene på regulering av og krav til IKT-sikkerhet i anbudsdokumenter og kontrakter, medfører at også leverandørene blir bedre på dette området. Det er påpekt utfordringer med å få aksept for krav knyttet til for eksempel retten til å revidere leverandørene, og til å kunne motsette seg skifte av underleverandører. Selv om KBO-enhetene har mer fokus på regulering av og krav til IKT-sikkerhet, så er det varierende, og for enkelte gjøres det ingen oppfølging og verifisering av etterlevelse og håndtering av de kravene som er stilt til leverandørene.

Leverandørene bekrefter inntrykket av at det varierer i hvilken grad KBO-enhetene stiller krav til IKT-sikkerhet. Enkelte leverandører stiller imidlertid spørsmål ved om kundene har kompetanse og modenhet til å stille de riktige kravene i henhold til kraftberedskapsforskriften, inkludert det å stille krav til livsløpsleveranser.

Flere informanter fremhever usikkerhet knyttet til håndtering av kraftsensitiv informasjon i samarbeidet mellom KBO-enhet, leverandører og underleverandører som en digital sårbarhet. På et overordnet nivå er det ikke en felles forståelse av hva som er kraftsensitiv informasjon blant KBO-enheter, leverandører og underleverandører til kraftbransjen.

3.3 I hvilken grad bygger leverandører IKT-sikkerhet inn i egne pilotprosjekter som testes i kraftbransjen

Flere KBO-enheter har ikke tilstrekkelig regulering av og krav til IKT-sikkerhet i forbindelse med gjennomføring av pilotprosjekter. Leverandørene sier de har fokus på IKT-sikkerhet *«by design»* i produktutviklingen, men flere aktører har nevnt at det ikke nødvendigvis er god nok bevissthet og fokus på IKT-sikkerhet i oppsettet og konfigurering opp mot andre systemer i forbindelse med uttesting av pilotprosjektene.

Flere aktører har erfart at det i pilotprosjekter i hovedsak er fokus på å teste funksjonalitet ut i fra effektiviserings- og produksjonshensyn, og at sikkerhet blir nedprioritert. Det kan virke som om sikkerhetsfokuset varierer med hvilken type prosess eller del av virksomheten et pilotprosjekt berører. I pilotprosjekter mot infrastrukturen er det mer bevissthet og fokus på IKT-sikkerhet enn i andre prosesser eller deler av virksomheten som ikke direkte berører infrastrukturen.

Det synes som om mange leverandører i all hovedsak har fokus på utvikling av funksjonalitet, og at det forutsetter at det er en KBO-enhet som setter klare krav for å ivareta sikkerhet i pilotprosjekter som testes i kraftbransjen. Det synes også som om mange leverandører ønsker enklest mulig tilgang til KBO-enheters systemer i forbindelse med testing i et operativt miljø, og at det forutsetter at det er en KBO-enhet som setter klare krav for å ivareta sikkerhet i styring av tilgangskontroll for leverandør.

3.4 I hvilken grad lukker leverandører digitale sårbarheter i egne produkter, varsler sine kunder og samarbeider med KraftCERT eller andre CSIRT-miljøer

Det kan være flere årsaker til at digitale sårbarheter ikke identifiseres og lukkes. Dette inkluderer blant annet:

- Manglende rutiner og prioritering hos leverandørene
- Økonomiske forhold
- Uklar ansvarsfordeling mellom KBO-enhet og leverandører, samt lange leverandørkjeder
- Manglende kompetanse og kapasitet hos KBO-enhetene
- Manglende systemoppfølging fra KBO-enhetene
- Teknisk gjeld i gammel teknologi og software
- KBO-enheters manglende kontrollmulighet ved bruk av store underleverandører

Alle leverandørene sier de har fokus på å identifisere og lukke digitale sårbarheter i egne produkter. Det kan imidlertid være utfordringer med prioritering av ressurser hos leverandør til å få lukket sårbarhetene.

Videre gir leverandørene inntrykk av at kundene varsles ved funn av (alvorlige) sårbarheter.

De store KBO-enhetene sier at de også gjør regelmessige tiltak for å identifisere og håndtere sårbarheter i leverandørenes produkter som er i bruk hos dem selv. KBO-enhetene mener at kvaliteten til leverandørene varierer. For en del av testene de gjennomfører selv, oppdages det imidlertid for mange feil som er enkle å finne og burde vært avdekket av leverandørene selv på et tidligere tidspunkt.

Leverandørene påpekte at selv om de lukker sårbarheter i egne produkter, er man også avhengig av at kunden jevnlig oppdaterer og patcher sine systemer slik at de kontinuerlig er oppdatert til siste versjon, for å ivareta sikkerheten.

KraftCERT nevnes av flere av informantene å være en viktig arena og funksjon i kraftbransjen for blant annet utveksling av informasjon om nye trusler, sårbarheter og angrep. Alle KBO-enhetene med unntak av en er medlem av KraftCERT. De KBO-enhetene som er del av Nettalliansen inngår i et felles KraftCERT-medlemskap som forvaltes av alliansen. Flere av leverandørene er medlem av KraftCERT for å utveksle informasjon om sårbarheter, mens enkelte leverandører har påbegynt en dialog med KraftCERT uten enda å ha formalisert dette i form av medlemskap.

En av leverandørene som var medlem i KraftCERT informerte at de varsler KraftCERT om alle sårbarheter som avdekkes i egne produkter og motsatt. Denne prosessen fungerer, men mye av den informasjonen som kommer fra KraftCERT til leverandøren mente leverandøren var kjent fra andre kilder.

3.5 Hvordan stiller leverandører som ikke er sertifisert allerede seg til mulig krav til sertifisering i henhold til internasjonale sikkerhetsstandarder

De fleste av leverandørene som har deltatt i kartleggingen, er enten ISO 27001 sertifisert, har påbegynt arbeid med å bli ISO 27001 sertifisert eller sier at de har interne systemer, rutiner og prosesser i henhold til kontrollelementene i ISO 27001. Mindre leverandører sier at de jobber mot ISO 27001 sertifisering for å heve egen kompetanse og intern sikkerhet. De større leverandørene uttrykker at sertifisering i henhold til internasjonale standarder legger gode føringer for hvordan bygge informasjonssikkerhet med en risikobasert tilnærming i bunn, og at det vitner om at virksomheten har lagt et formalisert og strukturert virksomhetsstyringssystem i bunn for informasjonssikkerhet. De fleste aktørene, både leverandører og

KBO-enheter, uttrykker imidlertid at sertifisering i seg selv ikke sier noe om godheten og effektiviteten av kontrollmekanismene som er satt opp. Flere leverandører var også opptatt av at krav til sertifisering kan hemme innovasjon i bransjen da det vil sette strengere krav til nye aktører. Det ble også påpekt at en virksomhet kan ha gode og effektive kontrollmekanismer selv om man ikke er sertifisert.

Flere aktører uttrykker at det er en forventning at store, etablerte leverandører er sertifisert i henhold til internasjonale sikkerhetsstandarder. Verken KBO-enhetene eller leverandørene anså det som nyttig å stille krav til sertifisering.

Gjennom samtalene fremkom det at enkelte land som Tyskland og Tyrkia stiller krav til om at nettselskaper og leverandører til kraftbransjen er sertifisert i henhold til internasjonale standarder som ISO 27001 og ISO 27002 om ledelsessystem for informasjonssikkerhet eller tilsvarende. Vi har imidlertid ikke fulgt opp denne informasjonen videre.

3.6 Hvordan er leverandørene bevisste på sikkerhetsutfordringer og ser at de selv kan bidra for å beskytte norsk kraftforsyning mot cyberangrep

Flere informanter sier det har skjedd en endring i bransjen med tanke på IKT- og cybersikkerhet de siste årene, der slike tema også blir løftet oppover i organisasjonene og inn på leder- og styrenivå. Både større sikkerhetshendelser som har inntruffet de siste årene (eksempler som er blitt nevnt er dataangrepene på både Hydro, Volue, Solarwinds og Østre Toten kommune) og den nye kraftberedskapsforskriften som stiller strengere krav til både informasjonssikkerhet og driftskontrollfunksjonen, nevnes som årsaker til dette.

Alle leverandørene sier at de har sterk bevissthet på sikkerhetsutfordringer og at de er bevisste på at de er en mulig angrepsvektor inn mot kritisk infrastruktur. Samtalene med leverandørene gir imidlertid ikke et grunnlag til å si noe om denne bevisstheten gjennomsyrer organisasjonen hos alle leverandørene. Leverandørene pekte videre på at andre, gjerne mindre eller nye leverandører til kraftbransjen, kan ha lavere kompetanse og bevissthet knyttet til sikkerhet.

Leverandørene sier de har fokus på IKT-sikkerhet *«by design»* i produktutviklingen, men flere aktører har nevnt at det ikke nødvendigvis er god nok bevissthet og fokus på IKT-sikkerhet i oppsett og konfigurering opp mot andre systemer. Flere av informantene nevnte også sårbarheter knyttet til lange leverandør-kjeder av hardware- og softwarekomponenter som inngår i leveransen av et system eller produkt, at dette er basert på tillit til leverandørene og at det er vanskelig både for KBO-enhetene og for leverandørene å ha kontroll med hele kjeden og alle leddene som inngår. Også kompleks og uavklart organisering og ansvarsforhold mellom KBO-enhet og leverandører kan medføre sårbarheter hvor flere av informantene har gitt inntrykk av at det er behov for å tenke mer helhetlig når det kommer til sikkerhet.

Flere KBO-enheter gir tilbakemelding om at det er varierende grad av bevissthet knyttet til sikkerhet hos leverandørene og at det er usikkert om alle leverandørene innser at de selv er en mulig angrepsvektor («stepping stone») inn mot kritisk infrastruktur.

3.7 Hvordan arbeider myndigheter i andre land for å ivareta sikkerhet i leverandørkjeden til energiforsyningen

I et nasjonalt perspektiv har ulike tilsynsmyndigheter valgt ulike virkemidler for å følge opp sikkerhet i leverandørkjeder. Flere tilsynsmyndigheter (eksempelvis innen jernbane og petroleum) legger svært stor vekt på virksomhetenes ansvar for å følge opp sikkerhet hos leverandørene på lik linje med aktiviteter de

selv utfører. Den nasjonale sikkerhetsmyndigheten (NSM) har på den andre siden gjennom ny sikkerhetslov fått et utvidet tilsynsansvar med leverandører i sikkerhetsgraderte anskaffelser (som tidligere lå hos anskaffelsesmyndigheten). Selv om denne studien, med utgangspunkt i NVEs spørsmål, ikke fokuserer på andre norske tilsynsmyndigheter, vil også erfaringer med ulike tilnærminger hos disse være nyttige i vurderinger og anbefalinger avslutningsvis.

I det følgende beskrives hvordan enkelte myndigheter utenfor Norge arbeider for å ivareta sikkerhet i leverandørkjeden til energiforsyningen. Beskrivelsen er basert på søk og gjennomgang av åpne kilder, samt samtaler med Reguleringsmyndigheten for energi (RME) og Energimyndigheten i Sverige, samt leverandører som leverer systemer og tjenester til andre nordiske land.

EUs styring av digital sikkerhet: personvernforordningen, NIS-direktivet og cybersikkerhetsforordningen[4, 5, 6, 7, 8]

EU tar en stadig større pådriverrolle i det digitale sikkerhetsarbeidet og har en aktiv rolle på den lovgivende siden med innføring av nytt harmonisert regelverk innenfor digital sikkerhet. Innføringen av personvernforordningen (GDPR) trådte i kraft i Norge og EU i 2018. Innføringen førte til økt oppmerksomhet rundt personvern og hvordan virksomheter må arbeide for å sikre de person-opplysningene de behandler. Dette har også ført til styrket fokus på digital sikkerhet generelt. EU har også vedtatt NIS-direktivet («Directive on Security of network and information systems») og cybersikkerhetsforordningen («EU Cybersecurity Act»).

Direktivet om tiltak for et høyt felles sikkerhetsnivå i nettverk og informasjonssystemer i EU (NIS-direktivet) ble vedtatt i EU i 2016. Formålet med direktivet er å forbedre det indre markeds funksjon gjennom etableringen av et høyt felles sikkerhetsnivå i viktige nettverks- og informasjonssystemer. Direktivet pålegger medlemsstatene å sørge for et visst nivå for landets IKT-sikkerhet ved å lage en strategi for sikkerhetsarbeidet, etablere en IKT-sikkerhetsberedskapsenhet (CSIRT) og pålegge operatører og leverandører av samfunnsviktige tjenester IKT-sikkerhetskrav og varslingsplikt ved alvorlige IKT-sikkerhetshendelser. Flere sektorer, inkludert energisektoren og herunder elektrisitet, er omfattet av direktivet. Dette betyr i praksis at de fleste energioperatørene i medlemsstatene, spesielt mange nettselskap og operatører av distribusjonssystem (DSOer), samt alle operatører av transmisjonssystem (TSOer), er underlagt cybersikkerhets- og varslingskravene.

NIS-direktivet er det første EU-direktivet som regulerer cybersikkerhet i Europa. Direktivet har som formål å styrke IKT-sikkerheten i EU og er ett av flere tiltak for å nå målene i EUs strategi for cybersikkerhet. Direktivet er et minimumsdirektiv og setter dermed minimumskrav til medlemsstatene både når det gjelder direktivets virkeområde og krav til sikkerhet. Dette medfører at medlemsstatene kan velge å innføre strengere regler enn det som fremgår av direktivet. Det bemerkes at NIS-direktivet har kun et markedsperspektiv, ikke et nasjonalt samfunnssikkerhetsperspektiv.

NIS-direktivet trådte i kraft i EU i 2018 og i løpet av 2020 hadde alle medlemslandene inkludert direktivet i nasjonal lovgivning. Regjeringen har gitt følgende oppsummering av EU-landenes erfaring med direktivet:

- Virkeområdet er snevert og ikke klart angitt i direktivet. Det medfører en krevende utpekingsprosess. Denne prosessen har medført et stort sprik i hvordan EU-landene har definert

[4] https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2014/sep/nis-direktivet/id2483374/
[5] https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2021/feb/nis2-direktivet/id2846097/
[6] https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2017/nov/cybersecurity-act/id2590048/
[7] https://nsm.no/regelverk-og-hjelp/rapporter/helhetlig-digitalt-risikobilde-2020/digitalisering-krever-styring-og-gode-prosesser/samarbeid-tiltak-og-regelverk-over-landegrenser/ (NSM, 2020)
[8] https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

virkeområdet nærmere og medført at enkelte grenseoverskridende virksomheter ikke har blitt identifisert.
- Uklare regler knyttet til varsling har medført stor forskjell mellom medlemsstatenes implementering. Dette har skapt en ekstra byrde for virksomhetene, særlig for virksomheter som opererer i flere land.
- Tilsyn etter gjeldende direktiv og håndheving av kravene som oppstilles har blitt gjennomført svært forskjellig innad i unionen. Ifølge evalueringen av direktivet skal dette ha medført at det er stor forskjell på medlemsstatenes evne til å håndtere og vurdere risiko.

I 2020 ble det lagt frem ny EU-strategi for cybersikkerhet og et forslag til nytt direktiv om tiltak for å sikre et høyt felles nivå for sikkerhet i nett- og informasjonssystemer i hele Unionen (NIS 2-direktivet). Forslaget til NIS 2-direktiv er til behandling hos Europaparlamentet og Rådet og vil erstatte det nåværende direktivet. NIS 2-direktivet inkluderer følgende momenter:

- Virkeområdet utvides ved å innlemme flere sektorer som anses som kritisk for både økonomien og samfunnet, totalt 15 definerte sektorer. Det vil skilles mellom mer og mindre samfunnsviktige tjenester. Foreløpig benyttes «vesentlige» og «viktige» på norsk, der «vesentlige» omfatter virksomheter i energisektoren. I utgangspunktet vil det kun være større virksomheter som underlegges NIS 2 fordi det innføres et størrelsestak som avgrenser virkeområdet mot små og mellomstore virksomheter.
- Sikkerhetskravene som stilles til tilbydere, styrkes ved å innføre krav om en risikostyringsmetode som skal gi en minimumsliste over grunnleggende sikkerhetselementer som må legges til grunn for sikkerhetsarbeidet.
- Medlemsstatene pålegges å sikre at tilbydere iverksetter hensiktsmessige og proporsjonale tekniske og organisatoriske tiltak for å håndtere risiko i nettverk og informasjonssystemer (som er en videreføring av gjeldende direktiv). Det foreslås imidlertid noen minimumskrav, blant annet krav om at tilbydere håndterer cybersikkerhetsrisiko i forsyningskjeder og hos leverandører, planer for vedlikehold, overvåkning og testing, samt bruk av krypto.
- Det innføres mer presise bestemmelser om prosessen for varsling av hendelser, hva det skal varsles om og når.
- På europeisk nivå skal forslaget styrke sikkerhet i forsyningskjeden for viktige informasjons- og kommunikasjonsteknologier. Det legges opp til et tettere samarbeid med Kommisjonen og ENISA for å utføre koordinerte risikovurderinger av kritiske forsyningskjeder. Forslaget innfører strengere tilsynsmessige tiltak for nasjonale myndigheter, strengere håndhevingskrav og tar sikte på å harmonisere sanksjonsregimer i alle medlemsstater. Direktivet forplikter medlemsstatene til å sikre at myndighetene har anledning til å pålegge bøter, av en nærmere angitt maksimalsats.

Cybersikkerhetsforordningen styrker EUs byrå for cybersikkerhet, ENISA[9], sitt mandat og danner grunnlaget for et felles marked for sertifisering av produkter, tjenester og prosesser for cybersikkerhet. Forordningen ble vedtatt i EU i 2019.

Det gjeldende NIS-direktivet og cybersikkerhetsforordningen er ikke en del av EØS-avtalen og heller ikke innført i norsk rett. Det er imidlertid utarbeidet et forslag til en lov som gjennomfører det gjeldende NIS-direktivet i norsk rett. Dersom loven vedtas, vil den bli gjenstand for revisjon når NIS 2-direktivet eventuelt blir en del av EØS-avtalen.

[9] The European Union Agency for Cybersecurity (ENISA) https://www.enisa.europa.eu/

EUs styring av cybersikkerhet i elektrisitetssektoren: Elektrisitetsforordningen og EUs nettkode for cybersikkerhet for grensekryssende elektrisitetsflyt [10, 11, 12]

EUs energibyrå, ACER[13], har i 2021 utarbeidet rammeretningslinjer for en nettkode på cybersikkerhet på forespørsel fra EU-Kommisjonen. Dette er forankret og beskrevet i elektrisitetsforordningen. Rammeretningslinjene gir forslag til sektorspesifikke krav for cybersikkerhet for grensekryssende elektrisitetsflyt. Fremtredende punkter i rammeretningslinjene er:

- De fleste virksomheter som kan ha betydning for grensekryssende elektrisitetsflyt, skal omfattes av nettkoden. Dette inkluderer tjenesteleverandører både innenfor og utenfor EU.
- Nettkoden skal etablere et rammeverk for cybersikkerhet som alle virksomheter som er viktige eller kritiske for grensekryssende elektrisitetsflyt i EU, skal implementere. Dette inkluderer å gjennomføre risikovurdering, drifte sikkerhetssentre for hendelseshåndtering og informasjonsdeling, samt gjennomføre cybersikkerhetsøvelser.
- Alle virksomheter som er kritiske for grensekryssende elektrisitetsflyt, skal være gjenstand for verifisering av sitt rammeverk for cybersikkerhet i form av sertifisering, «peer review» eller tilsyn av myndigheter.

Rammeretningslinjene stiller også flere andre krav som er vurdert å være relevant i lys av sårbarhetene som er kartlagt i dette oppdraget, jf. kapittel 3.1, og spørsmålene som NVE har stilt, jf. kapittel 2.2. Retningslinjene stiller krav til at dette skal gjøres, men beskriver ikke hvordan kravene skal være:

- Det skal gjøres risikovurdering som inkluderer leveransekjeder, samt prioritering av tiltak for å ivareta leveransekjedesikkerhet, inkludert kontraktskrav i leveransekjeder.
- Kritiske / større virksomheter skal etablere «security operations centre» (SOC) eller anskaffe SOC-tjenester gjennom en «managed security service provider» (MSSP). Dette skal komplementere det eksisterende CSIRT-nettverket etablert gjennom NIS-direktivet.
- Alle nye systemer, prosesser og prosedyrer skal anskaffes, designes, konfigureres og opprettholde integrerte prinsipper som «security in-depth» og «security by design».
- Både kunde og leverandør kan holdes ansvarlig for å ivareta cybersikkerhet (for eksempel et nettselskap kan holdes ansvarlig fordi de ikke har fulgt opp leverandør tilstrekkelig, mens leverandør kan holdes ansvarlig fordi de ikke har fulgt opp sikkerhet godt nok).
- Alle virksomheter som ikke defineres som kritiske / større virksomheter, skal implementere grunnleggende «cyber hygiene» i tråd med krav fra ENISA. Dette tilsvarer omtrent NSMs grunnprinsipper for IKT-sikkerhet[14].

Basert på rammeretningslinjene skal systemoperatørene (ENTSO-E[15]) og nettselskaper (EU-DSO enheten[16]) i 2022 levere et forslag til en nettkode på cybersikkerhet til ACER. Deretter vil forslaget til nettkoden med eventuelle oppdateringer sendes til EU-Kommisjonen som vil starte den politiske prosessen for å vedta nettkoden. Vurdering av om koden er EØS-relevant og om og hvordan den skal gjennomføres i norsk rett følger vanlige prosedyrer og er politiske myndigheters ansvar.

[10] https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2017/jan/forslag-til-revidert-elektrisitetsforordning-/id2540021/
[11] https://www.nve.no/reguleringsmyndigheten/nytt-fra-rme/nyheter-reguleringsmyndigheten-for-energi/acer-har-publisert-en-rammeretningslinje-for-en-nettkode-pa-cybersikkerhet/
[12] https://www.acer.europa.eu/events-and-engagement/news/acer-publishes-its-framework-guideline-establish-network-code
[13] The European Union Agency for the Cooperation of Energy Regulators (ACER) https://www.acer.europa.eu/
[14] https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/grunnprinsipper-ikt
[15] The European Network of Transmission System Operators for Electricity (ENTSO-E) https://www.entsoe.eu/
[16] The Association for the European Distribution System Operators (EU-DSO entity) https://www.eudsoentity.eu/

Styring av cybersikkerhet i energisektoren i Sverige [17, 18]

Sverige er medlem av EU og således underlagt EUs rettsakter, inkludert NIS-direktivet. NIS-direktivet trådte i kraft i Sverige i 2018 gjennom loven om informasjonssikkerhet for leverandører av samfunnsviktige og digitale tjenester med tilhørende forskrifter. Sverige har etablert en nasjonal strategi for samfunnets informasjons- og cybersikkerhet[19]. Videre stiller NIS-regelverket blant annet krav til at aktørene skal bedrive systematisk og risikobasert informasjonssikkerhetsarbeid med støtte fra ISO 27001:2017 og ISO 27002:2017 om ledelsessystem for informasjonssikkerhet eller tilsvarende, samt krav til rapportering av hendelser som har betydning for kontinuiteten for samfunnsviktige tjenester. I Sverige er aktørene innenfor de utvalgte sektorene selv ansvarlige for å identifisere om de treffes av lovgivningen eller ikke. Videre har Energimyndigheten i 2021 etablert en forskrift og allmenne råd om sikkerhetstiltak for nettverk og informasjonssystemer innen energisektoren. Denne stiller ytterligere krav til risikoanalyse, informasjonssikkerhet og sikkerhetstiltak.

Den svenske Sikkerhetsbeskyttelsesloven (som er en parallell til den norske Sikkerhetsloven) gjelder beskyttelse av virksomheter eller informasjon som kan ha betydning for Sveriges sikkerhet. Sikkerhets-beskyttelse handler om å ha forebyggende tiltak mot spionasje, sabotasje, terrorisme og annen kriminalitet som kan true Sveriges sikkerhet og i andre tilfeller beskytte sikkerhetsgradert informasjon. Alle som driver sikkerhetssensitiv virksomhet har krav om å gjennomføre en sikkerhetsbeskyttelses-analyse for å identifisere verneverdier innenfor egen virksomhet. Sikkerhetsbeskyttelsen skal opprettes gjennom sikkerhetstiltak, fysisk sikkerhet og personellsikkerhet. Flere virksomheter kan berøres av både sikkerhetsbeskyttelsesloven og NIS-regelverket, men de delene som omfattes av sikkerhetsbeskyttelses-loven er unntatt NIS-regelverket.

Energimyndigheten i Sverige (som i praksis tilsvarer NVE i Norge) har siden 2018 vært tilsynsmyndighet for virksomheter som har identifisert seg som leverandør av samfunnsviktige tjenester innen energisektoren i henhold til NIS-regelverket. Fra 1. desember 2021 har Energimyndigheten i Sverige fått nytt tilsynsansvar for enkeltaktører i energisektoren som driver sikkerhetssensitiv virksomhet innen områdene fjernvarme, naturgass og oljebrensel i henhold til sikkerhetsbeskyttelsesloven.

Sverige har etablert CERT-SE[20] som er Sveriges nasjonale «Computer Security Incident Response Team» med oppgave å støtte samfunnet i arbeidet med å håndtere og forebygge IT-hendelser. Sverige har ikke etablert sektor CSIRT for energisektoren. Videre er sentrale myndigheter i Sverige i ferd med å opprette et nasjonalt senter for cybersikkerhet[21].

Gjennom samtale med Energimyndigheten uttrykkes det at det er liten grad er formalisert ansvar for cybersikkerhet i Sverige. NIS-direktivet beskriver kun svakt hvordan cybersikkerhet i energisektoren skal følges opp og Energimyndigheten har ikke hatt tilsynsansvar på dette området før i 2018. Det antydes at allmennheten ikke har en gjengs oppfatning av at energisektoren har vært utsatt for digitale angrep – fokus har heller vært mot finans og andre bransjer. Det finnes imidlertid en voksende forståelse både blant politikere og allmennheten at trusselen øker og at man blir mer sårbar med digitalisering. NIS-regelverket anses også å ha stor effekt da cybersikkerhet er et mye viktigere spørsmål for ledelsen i selskapene nå enn før, selv om mange ting fortsatt ikke er på plass.

Energimyndigheten bidrar til samordning og samvirke med aktører i markedet og har hatt en jevn dialog og nært samarbeid med selskapene og bransjeorganisasjonene om cybersikkerhet over tid. Erfaring viser at det er varierende tilstand på cybersikkerhet i bransjen. Flere av de store selskapene har jobbet

[17] https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/
[18] https://www.energimyndigheten.se/trygg-energiforsorjning/informationssakerhet/
[19] https://www.regeringen.se/regeringens-politik/krisberedskap/nationell-strategi-for-samhallets-informations--och-cybersakerhet/
[20] https://www.cert.se/
[21] https://www.cfcs.se/

systematisk med cybersikkerhet i flere år, mens de mindre selskapene ofte ikke har kompetanse eller kapasitet. Energimyndigheten deltar i forum og bransjeorganisasjoner sammen med de små selskapene for å prøve å løfte disse gjennom å overføre erfaring fra de store selskapene. Energimyndigheten har samarbeidet med selskapene for å bevisstgjøre standardisering og sertifisering innen cybersikkerhet, herunder bevisstgjøring i innkjøpsprosesser og hvilke krav som bør stilles. Energimyndigheten har begrenset dialog med leverandørene med unntak av noen av de store. Fremover vil Energimyndigheten se på muligheter for i større grad følge opp bransjen med tilsyn (først og fremst de store aktørene gjennom risikobasert tilsyn), vurdere sanksjonsavgifter og oppdatere regelverket slik at selskapene får tydeligere regler å forholde seg til på cybersikkerhet.

Gjennom samtaler med leverandører som leverer til samtlige av de nordiske landene gis det inntrykk av at svensk lovgivning oppleves som strengere enn norsk lovgivning på krav som stilles på cybersikkerhet, men at de har kommet kortere med tanke på nasjonal og sektovervise CERTer. Det bemerkes at leverandørene forholder seg til sine kunder og ikke direkte til myndighetene. Vi har ikke grunnlag for å si om dette inntrykket skyldes ulik kultur, om selskapene faktisk stiller strengere krav og forventninger til IKT-sikkerhet eller om det skyldes andre forhold.

Om krav til sertifisering av leverandører i andre land

Gjennom samtalene fremkom det at enkelte land som Tyskland og Tyrkia stiller krav til om at nettselskaper og leverandører til kraftbransjen er sertifisert i henhold til internasjonale standarder som ISO 27001 og ISO 27002 om ledelsessystem for informasjonssikkerhet eller tilsvarende. Vi har imidlertid ikke fulgt opp denne informasjonen videre.

3.8 Bør viktige leverandører bli KBO-enhet og underlagt deler av kraftberedskapsforskriften

Noen av aktørene ga uttrykk for at det kan være hensiktsmessig å gjøre enkelte viktige leverandører til KBO-enheter underlagt deler av kraftberedskapsforskriften. Følgende mulige fordeler ble nevnt:

- Mulighet for å styre hvilke krav som stilles til viktige leverandører i norsk kraftforsyning (for eksempel kraftberedskapsforskriften §§6 og 7)
- Mulighet for NVE til å avkreve viktige leverandører dokumentasjon og revisjon opp mot kraftberedskapsforskriften for å bedre ivareta IKT-sikkerhet i norsk kraftforsyning
- Mulighet for leverandør til å gjøre bakgrunnssjekker på høyere nivå av eget personell ved ansettelser
- Mulighet for leverandører til å bli definert som virksomheter med kritisk samfunnsfunksjon og nøkkelpersonell i forbindelse med pandemi

Det ble samtidig uttrykt sterk usikkerhet knyttet til den praktiske gjennomføringen av en slik endring. Flere problemstillinger og utfordringer ble nevnt:

- Hvem skal bestemme og hvordan skal man avgjøre hvilke leverandører som er 'viktige'?
- Hvilke deler av en leverandør skal bli KBO-enhet og underlagt kraftberedskapsforskriften – bare den 'norske' delen eller også den 'internasjonale' delen? Hvilken nytte vil man ha av å gjøre kun den 'norske' delen til KBO-enhet uten å sette restriksjoner på de ressursene man egentlig trenger å få tak i?
- Hva gjør man dersom leverandøren ikke ønsker å bli KBO-enhet og underlagt kraftberedskaps-forskriften – må KBO-enheten da si opp avtalen?
- Kan dette gjelde kun norske og ikke internasjonale leverandører?

- Hvilke funksjoner skal eventuelt leverandørene ha og hvilke deler av kraftberedskapsforskriften skal de bli underlagt, eventuelt hvilke unntak skal gjøres?
- Hva tenker man rundt en mulig rolleblanding?
- Hvem skal betale leverandørene for utførelsen av KBO-oppgaver (for eksempel beredskap og øvelser)?
- Hvilken kapasitet har NVE til å følge opp leverandører i tillegg til dagens KBO-enheter?

Den gjengse oppfatning var at det er kraftselskapene, det vil si dagens KBO-enheter, som fortsatt bør ha det helhetlige sikkerhetsansvaret. Videre bør leverandørene ha like krav og forutsetninger og det vil ikke være hensiktsmessig å gjøre utvalgte leverandører til KBO-enheter underlagt deler av kraftberedskaps-forskriften.

Som beskrevet i kapittel 3.7, vil det på sikt trolig komme nye eller endrede krav til IKT-sikkerhet i norsk kraftforsyning gjennom europeiske initiativer som NIS og EUs Cyber Security Network Code. Dette vil kunne bidra til å harmonisere krav på tvers av EU og EØS land og således gjøre et ønske om at viktige leverandører bør bli KBO-enheter underlagt deler av kraftberedskapsforskriften, overflødig.

4 Viktigste sårbarheter og anbefalte tiltak

Kraftbransjen moderniseres og opplever økt digitalisering, kritiske systemer tilknyttes i større grad til internett og flere oppdrag utføres i større grad enn før gjennom fjerntilkobling av en tredjepart. Digitalisering og innovasjon, sammen med lange digitale verdikjeder, komplekse systemer, betydelig gjensidige avhengigheter mot leverandører både nasjonalt og internasjonalt, samt nye og stadig økende antall trusselaktører, gjør det utfordrende både for virksomheter og myndigheter å styre sin risiko og sine sårbarheter.

Tidligere hadde NVE en godkjenningsordning for leverandører til kraftbransjen der NVE inngikk sikkerhetsavtale med utvalgte leverandører. Denne ordningen er opphevet. I dag leverer alle leverandører sine tjenester og produkter til KBO-enheter uten at NVE gjør noen godkjenning og det er opp til selskapene selv å vurdere risiko og innføre risikoreduserende tiltak. Riksrevisjonen har i sin rapport påpekt bransjens avhengighet av leverandører, mangelfull oppfølging av disse og det at NVE ikke lenger fører tilsyn med leverandørene (Riksrevisjonen, 2021).

Kartleggingen og vurderingen av sårbarheter i kapittel 3 viser at det er stor variasjon blant både KBO-enhetene og leverandørene opp mot hvilke sårbarheter som er relevante og fremtredende for de ulike aktørene. Det er også en sammensatt problemstilling der ulike varianter og nyanser av sårbarhetene er gjeldende for de ulike aktørene. Dette gjør at det er ikke ett enhetlig bilde på hva som er digitale sårbarheter i leverandørkjeden. Det fremkommer likevel at det er noen sårbarheter som er gjennomgående og mer fremtredende enn andre. Dette anses å være de viktigste sårbarhetene:

1) Manglende risiko- og trusselforståelse hos aktørene i leverandørkjeden
2) Manglende forståelse og etterlevelse av regelverkskrav hos KBO-enhetene
3) Manglende kompetanse og/eller kapasitet / evne til å stille tilstrekkelige krav til leverandører
4) Manglende kompetanse og/eller kapasitet / evne til å følge opp krav som stilles i leverandørkjeden
5) Manglende identifisering av, informasjonsdeling om, og lukking av digitale sårbarheter i utstyr og systemer hos aktørene i leverandørkjeden
6) Manglende kompetanse og/eller kapasitet / evne til å detektere og håndtere IKT-sikkerhetshendelser hos aktørene i leverandørkjeden

Det kreves en felles, koordinert innsats fra både myndigheter, KBO-enheter og leverandører for å redusere de digitale sårbarhetene i leverandørkjeden. I det følgende drøftes disse sårbarhetene kort, samt at det gjøres en vurdering og anbefaling av tiltak for å redusere sårbarhetene i lys av NVEs virkemiddelapparat. I kapittel 5 presenteres så et forslag til NVEs videre arbeid med oppfølging av digitale sårbarheter i leverandørkjeden i norsk kraftforsyning.

4.1 Viktige sårbarheter

1) Manglende risiko- og trusselforståelse hos aktørene i leverandørkjeden

En god risiko- og trusselforståelse er en nødvendig forutsetning for bevissthet og etterlevelse av krav knyttet til IKT-sikkerhet i leverandørkjeden. Det er vanskelig å være bevisst og følge sikkerhetskrav dersom man ikke har god nok forståelse av hvorfor det er et problem; at det faktisk er en trussel og har et skadepotensiale. Manglende risiko- og trusselforståelse er et element i de fleste av sårbarhetene

beskrevet i kartleggingen. Generelt er informasjonsbehovet blant aktørene stort både fra NVE og fra KBO-enhetene:

- NVE har en viktig rolle i å informere og bidra til forståelse for reell trussel mot og risiko relatert til bransjen generelt.
- KBO-enhetene har (også basert på læring fra NVE) et ansvar for å informere leverandørene sine om både dette – og om risiko som er viktig for akkurat dem å håndtere.

På dette området er det relevant å gjøre tiltak for å heve den generelle kompetansen i bransjen knyttet til å forstå risiko og trusler. Det kan være tiltak som er initiert både av NVE gjennom for eksempel en webinarserie eller regelmessige forum for aktører i bransjen, og gjennom bransjeinitiativer fra KBO-enhetene eller gjennom bransjeforeningene. Et annet relevant tiltak for å heve kompetansen er for KBO-enhetene å gjennomføre trening og øvelser innen IKT-sikkerhet for egen virksomhet, inkludert samarbeid og samvirke med leverandørene. Et mulig tiltak for NVE kan være å etablere ulike «komplette» trenings- og øvelsessenarioer innen IKT-sikkerhet for industrielle IKT-systemer i kraftbransjen. Dette vil kunne gi aktørene i bransjen et godt utgangspunkt for relevant trening og øvelser – og for læring fra disse. I denne sammenheng kan det også være relevant for NVE å forbedre kommunikasjonen og tilgjengeliggjøre relevant og oppdatert informasjon om risiko- / trusselbildet som kraftbransjen står ovenfor gjennom NVEs nettsider (i tillegg til andre kanaler). Dette kan også inkludere forslag til og veiledning i bruk av rammeverk for risikovurdering og risikostyring.

2) Manglende forståelse og etterlevelse av regelverkskrav hos KBO-enhetene

Kartleggingen viser at det er varierende bevissthet og forståelse av IKT-sikkerhet og regelverkskrav både blant KBO-enhetene og leverandørene. Manglende kompetanse kommer opp som tema for de fleste av sårbarhetene beskrevet i kartleggingen. God og relevant sikkerhetskompetanse og forståelse av regelverk, er grunnleggende for å kunne ivareta sikkerhet og etterleve regelverkskravene. Eksempler som er blitt nevnt knytter seg til:

- Det er ikke alle KBO-enhetene som har tilstrekkelig kompetanse om og forståelse for kravene som stilles i kraftberedskapsforskriften med veileder.
- Nye, eventuelt mindre, leverandører til kraftbransjen kjenner ikke kraftbransjen og regelverket.
- Utenlandske leverandører kjenner ikke kravene i kraftberedskapsforskriften med veileder.
- Det er manglende styring av tilgangskontroll mellom KBO-enheter og leverandør, noe som ikke er i tråd med kraftberedskapsforskriften
- Både KBO-enheter og leverandører uttrykker usikkerhet knyttet til håndtering av kraftsensitiv informasjon.

Dersom det ses bort fra alternativet der NVE overtar ansvaret for all kravstilling og oppfølging av leverandørene direkte (som i praksis er lite gjennomførbart), er det to hovedstrategier som kan bidra til å redusere denne sårbarheten. Enten å heve kompetansen i bransjen og/eller å senke kompetansebehovet gjennom bedre og mer tilrettelagt veiledninger, maler og annet støttemateriell.

Flere av informantene har gitt uttrykk for at de ønsker tydeligere, mer detaljerte og spesifikke krav, veiledninger og støtte. NVEs regelverk er et funksjonelt regelverk med krav til hva som skal oppnås, men ikke til hvordan dette gjøres. De som skal etterleve et funksjonelt regelverk, står dermed friere til å finne løsninger som passer for egen virksomhet, og som samtidig svarer ut regelverkskravene. På generell basis foreslås det derfor ikke at myndighetene skal ta inn mer deskriptive krav i regelverket, men beholde regelverket på et mest mulig funksjonelt nivå. Derimot fremstår det som svært relevant for bransjen å ta et initiativ til å etablere arenaer hvor god praksis for ulike tekniske løsninger kan diskuteres. Å kunne lære av hverandres erfaringer og utviklede løsninger kan øke effektiviteten og redusere ressursbehovet for den

enkelte virksomhet betydelig. Et tiltak fra NVE sin side kan imidlertid være å vurdere regelverksutvikling knyttet til mulig gradering av kraftsensitiv informasjon.

For kompetanseheving og veiledning er flere mulige tiltak nevnt i punkt 1 over. Disse tiltakene er også relevante for denne sårbarheten. Både generell sikkerhetskompetanse og mer spesifikk veiledning kan gis i nevnte webinarserie eller regelmessige forum for aktører i bransjen initiert av NVE. Det er også identifisert et betydelig potensiale for NVE i å forbedre kommunikasjonen, og digitalisere og tilgjengeliggjøre relevant informasjon, gjennom sine nettsider. I dette ligger også kraftberedskapsforskriften og veiledningen til denne. Det bør også gjøres en gjennomgang av informasjon som tilgjengeliggjøres på nettsidene, med tanke på kraftsensitivitet / eksponering.

Gjennomføring av trening og øvelser kan også bidra til å heve den generelle sikkerhetskompetansen. Trenings- og øvelsesscenarioene som nevnes i punkt 1 over, kan og bør også inkludere slike elementer.

Mer frekvent oppfølging og kontroll av etterlevelse av krav både mot KBO-enheter og leverandører vil også kunne bidra til økt bevissthet og forståelse av kravene.

3) Manglende kompetanse og/eller kapasitet / evne til å stille tilstrekkelige krav til leverandører

Som nevnt, hadde NVE tidligere en godkjenningsordning for leverandører til kraftbransjen der NVE inngikk sikkerhetsavtale med utvalgte leverandører. Denne ordningen er opphevet. I dag leverer alle leverandører sine tjenester og produkter til KBO-enheter uten at NVE gjør noen godkjenning og det er opp til selskapene selv å vurdere risiko og innføre risikoreduserende tiltak. I leverandørkjederisiko kan det gjennomføres risikoreduksjon både hos leverandør og hos KBO-enheten. I den grad det er KBO-enhetene som er underlagt forskrift (og er utsatt for avanserte trusler), vil det uansett hvile et ansvar på dem om å sikre at sikkerhetskrav er stilt til leverandør og at tiltak er gjennomført.

Gjennom kartleggingen fremkommer det at flere KBO-enheter ikke har tilstrekkelig regulering av og krav til IKT-sikkerhet i alle prosesser. Dette gjelder både i anbudsprosesser og kontraktsinngåelse for alle typer IT-anskaffelser og som inkluderer hele livsløpet, inkludert ved gjennomføring av pilotprosjekter i bransjen. Det fremkommer også at de fleste KBO-enhetene i liten grad gjør risikovurderinger som utgangspunkt for krav som stilles til leverandørene. Flere har også påpekt at det er en ujevn maktbalanse mellom store leverandører og små og mellomstore KBO-enheter, der KBO-enhetene i enkelte situasjoner har mangelfull gjennomslagskraft mot leverandører. I mange tilfeller blir IKT-sikkerhet basert på tillit til de store leverandørene og samarbeidspartnere. Det oppleves ikke at NVE har satt fokus på dette området gjennom å føre tilsyn mot KBO-enhetenes kravstilling til og oppfølging av IKT-sikkerhet i leverandør-kjeden.

Denne sårbarheten henger også sammen med bransjens manglende grunnleggende risiko- og trussel-forståelse (punkt 1), samt sikkerhetskompetanse og regelverkskrav (punkt 2). Det er vanskelig å stille relevante krav til IKT-sikkerhet dersom man ikke har en god nok forståelse av hvorfor det er et problem. Tidligere nevnte tiltak knyttet til kompetanseheving, samt forbedret kommunikasjon og tilgjengeliggjort informasjon på nettsiden vil være relevant også her.

I tillegg ses et stort potensiale for NVE i å bedre utnytte digitalisering og interaksjon for å styrke tilrettelegging for virksomhetene. Eksempelvis har NVE utarbeidet en sjekkliste for IKT-sikkerhet i anskaffelser som dekker hele livssyklusen til anskaffelsen (NVE, 2020), og mal for informasjonssikkerhets-avtale som KBO-enhet kan bruke mot leverandør. Dersom disse, i stedet for å være statiske dokumenter som KBO-enhetene ikke nødvendigvis kjenner seg igjen i, kunne bygges opp som interaktive sider, ville verdien og effekten kunne økes betydelig. Da kan KBO-enhetene eksempelvis bruke et interaktivt anskaffelsesskjema der de gjennom spørsmål må ta stilling til egen risiko og få relevante forslag til

oppfølging og aksjoner basert på dette. Her kan ulike former for veiledning (tekst, tale, video, krav osv.) være tilgjengelig, der spørsmålene kommer opp. Basert på arbeidet i denne prosessflyten kan det genereres tilpassede kontraktskrav som kan hentes ut av KBO-enheten. Det vil da også være enkelt å tilknytte sjekklister som kan benyttes i oppfølging og kontroll, som leverandørrevisjoner.

4) Manglende kompetanse og/eller kapasitet / evne til å følge opp krav som stilles i leverandørkjeden

Da NVEs godkjenningsordning for leverandører ble opphevet, ble hele ansvaret for oppfølging i leverandørkjeden overført til KBO-enhetene. Gjennom kartleggingen fremkommer det at flere KBO-enheter mangler kompetanse og kapasitet til å følge opp de kravene som må stilles mot egne leverandører. NVE har heller ikke satt betydelig fokus på dette området gjennom å føre tilsyn mot KBO-enhetenes kravstilling til og oppfølging av IKT-sikkerhet i leverandørkjeden.

Tiltak rettet mot kompetanseheving og tilrettelegging med informasjon, veiledning og maler som nevnt i punkt 1, 2 og 3, vil være viktig også for å gjøre KBO-enhetene bedre i stand til å følge opp krav.

Dersom det ses bort fra alternativet der NVE overtar ansvaret for all kravstilling og oppfølging av leverandørene direkte (som i praksis er lite gjennomførbart), vil et viktig virkemiddel være at NVE intensiverer sine tilsyn mot KBO-enhetene. Et relevant tiltak for NVE er å gjennomføre en målrettet tilsynsserie mot KBO-enheter og deres oppfølging av leverandører.

Et annet hensiktsmessig tiltak kan være at KBO-enhetene eller bransjeforeningene iverksetter et samarbeid for oppfølging av leverandørene. Det fremkommer at det er utfordrende, spesielt for mindre KBO-enheter, å ha tilstrekkelig kompetanse og kapasitet til å føre tilsyn i det hele tatt. Det er tidligere påpekt at de mindre KBO-enhetene også opplever å ha lite «makt» i forhold til de store leverandørene, og ikke får mulighet til å føre tilsyn om de ønsker det. På den andre siden påpeker også leverandørene at enkelttilsyn fra alle de ulike KBO-enheten krever mye kapasitet fra dem. Dersom KBO-enhetene sammen kan, enten selv eller ved innkjøp av revisjonstjenester, ivareta grunnleggende sikkerhetskontroll med sine felles leverandører, ville det i seg selv heve grunnsikkerheten betydelig. Hver KBO-enhet ville da bare måtte følge opp sine egne «spesialbehov», om noen, og dermed spares ressurser for både dem og leverandørene. Maktbalansen i forhold til store leverandører endres også. Det eksisterer ulike ordninger for dette i andre bransjer og det kan blant annet involvere felles løsninger for sikkerhetskrav som stilles til leverandører, for revisjon og oppfølging av leverandører og for deling av revisjonsrapporter. Dersom bransjen velger å samordne og samarbeide på dette området, er det uansett viktig at den enkelte KBO-enhet gjør en egen vurdering av at krav og informasjon som fremkommer gjennom samordning og samarbeid er relevant for den enkelte KBO-enhets kontraktsforhold.

Også for denne sårbarheten er tiltaket som tidligere er blitt foreslått knyttet til å forbedre NVEs sjekkliste for IKT-sikkerhet i anskaffelser som dekker hele livssyklusen til anskaffelsen (NVE, 2020), relevant.

5) Manglende identifisering av, informasjonsdeling om, og lukking av digitale sårbarheter i utstyr og systemer hos aktørene i leverandørkjeden

Det fremkom flere årsaker til at digitale sårbarheter ikke identifiseres og lukkes. Dette inkluderer blant annet:

- Manglende rutiner og prioritering hos leverandørene
- Økonomiske forhold
- Uklar ansvarsfordeling mellom KBO-enhet og leverandører, samt lange leverandørkjeder
- Manglende kompetanse og kapasitet hos KBO-enhetene
- Manglende systemoppfølging fra KBO-enhetene
- Teknisk gjeld i gammel teknologi og software
- KBO-enheters manglende kontrollmulighet ved bruk av store underleverandører

For kraftbransjen som helhet er informasjonsdeling avgjørende for å detektere og håndtere digitale angrep effektivt. Den totale ressursbruken og risikoen for kraftsektoren blir svært høy dersom sårbarheter som er kjente lukkes bare enkelte steder, og så i det videre kan utnyttes gang på gang.

KraftCERT nevnes av flere av informantene å være en viktig arena og funksjon i kraftbransjen for blant annet utveksling av informasjon om nye trusler, sårbarheter og angrep. KraftCERT er KBO-enhet og ivaretar en responsfunksjon for energisektoren der medlemskap er frivillig.

Det fremkommer et klart behov for å øke samarbeidet og informasjonsflyten generelt knyttet til identifiserte sårbarheter i bransjen. I denne sammenheng bør NVE vurdere å etablere et sektorvist responsmiljø eller gi KraftCERT et tydeligere mandat og oppdragsbeskrivelse for dette, samt presisere krav til varsling og informasjonsdeling blant aktørene i bransjen. Formålet med de sektorvise responsmiljøene er at disse skal kunne bistå sin sektor med kompetanse og være knutepunkt for informasjon og informasjonsflyt mellom virksomheter i sektoren, mellom sektorer og mellom sektor og nasjonalt nivå (NorCERT).

Flere av tiltakene som allerede er nevnt, vil også være svært relevante i denne sammenheng. Dette gjelder både til tiltakene knyttet til kompetanseheving, tilgjengeliggjøring av informasjon og fokus fra myndighetene gjennom tilsyn.

6) Manglende kompetanse og/eller kapasitet / evne til å detektere og håndtere IKT-sikkerhetshendelser hos aktørene i leverandørkjeden

Kartleggingen viser at det er manglende kunnskap, kompetanse eller kapasitet til å detektere og håndtere IKT-sikkerhetshendelser. Det er ulik forståelse i bransjen knyttet til hva som er gode nok løsninger for å kunne detektere en sikkerhetshendelse. KBO-enhetene er ofte også avhengig av dybdekunnskap hos leverandører for å kunne håndtere en feilsituasjon i viktige systemer.

Informasjonsdeling er avgjørende for å detektere og håndtere digitale angrep. Viktigheten til KraftCERT sin koordinerende rolle mellom kraftbransjen, leverandør og sikkerhetsmyndighetene i en alvorlig hendelse ble fremhevet i kartleggingen. Også i denne sammenheng er tiltaket knyttet til å vurdere å etablere et sektorvist responsmiljø eller gi KraftCERT et tydeligere mandat og oppdragsbeskrivelse for dette, svært relevant.

Det bør vurderes å presisere forventninger til KBO-enheters kapabilitet for å detektere og håndtere et digitalt angrep, for eksempel gjennom å presisere forventning eller krav til KBO-enheter om å etablere «security operations centre» (SOC) eller anskaffe SOC-tjenester fra en «managed security service

provider» (MSSP). Dette tiltaket må også vurderes i lys av den nye nettkoden som er under utarbeidelse i EU og som på sikt kan bli gjeldende også for Norge. Der beskriver utkastet til rammeretningslinje for nettkoden dette som et krav til at kritiske / større virksomheter for grensekryssende elektrisitetsflyt. Her kan det også være relevant å hente læring og erfaring fra det nasjonale cybersikkerhetssenteret (NCSC).

Også flere av de andre tiltakene som allerede er nevnt, vil være svært relevante i denne sammenheng. Dette gjelder både tiltakene knyttet til kompetanseheving, tilgjengeliggjøring av informasjon og fokus fra myndighetene gjennom tilsyn.

4.2 Anbefalte tiltak for NVE

Riksrevisjonen har i sin rapport påpekt bransjens avhengighet av leverandører, mangelfull oppfølging av disse og det at NVE ikke lenger fører tilsyn med leverandørene. Et mulig virkemiddel er å gjøre viktige leverandører KBO-enheter underlagt deler av kraftberedskapsforskriften, eller med andre ord at NVE i går tilbake til å føre tilsyn med leverandørene selv i større eller mindre omfang. Alternativet er at NVE styrker tilsyn og oppfølging av dagens KBO-enheter slik at deres oppfølging av leverandørkjeden forbedres.

Noen av aktørene ga uttrykk for at det kan være hensiktsmessig å gjøre enkelte viktige leverandører til KBO-enheter underlagt deler av kraftberedskapsforskriften. Det ble samtidig uttrykt sterk usikkerhet knyttet til den praktiske gjennomføringen av en slik endring og flere problemstillinger og utfordringer ble nevnt.

Basert på en helhetlig vurdering er anbefalingen at dagens KBO-enheter fortsatt bør ha det helhetlige sikkerhetsansvaret, og at ingen av leverandørene underlegges beredskapsforskriften direkte. En eventuell differensiering mellom ulike typer, nasjonaliteter eller størrelse på leverandører, som er nevnt i kartleggingen, fremstår som svært problematisk å gjennomføre.

Basert på denne forutsetningen og med basis i NVEs virkemiddelapparat, gis det i Tabell 2 en oversikt over hvilke av de anbefalte tiltakene som er vurdert å ha effekt på hver av de viktigste sårbarhetene.

I ulik grad vil alle tiltakene kreve ressursbruk fra NVE, og det vil være behov for å styrke både kompetanse og kapasitet hos NVE for å ivareta dagens og fremtidige IKT-sikkerhetsutfordringer i kraftbransjen.

Som beskrevet i kartleggingen, vil det på sikt trolig komme nye eller endrede krav til IKT-sikkerhet i norsk kraftforsyning gjennom europeiske initiativer som NIS og EUs Cyber Security Network Code. Dette vil kunne bidra til å harmonisere krav på tvers av EU og EØS land, og således understøtte anbefalingen om å ikke la viktige leverandører bli KBO-enheter underlagt deler av kraftberedskapsforskriften. Det er imidlertid viktig at IKT-sikkerhet ikke settes på vent for slike internasjonale krav som både kan bli forsinket og ikke nødvendigvis ivaretar norske behov alene. NVEs langsiktige initiativer bør også ligge i forkant av den eksterne regelverksutformingen både for å påvirke denne med tanke på nasjonale behov, og for å gjøre den norske kraftsektoren godt forberedt på å imøtegå internasjonale krav når de stilles.

Tabell 2: Anbefalte tiltak opp mot hver av de viktigste sårbarhetene

Tiltak	Sårbarheter					
	Manglende risiko- og trussel-forståelse hos aktørene i leverandørkjeden	Manglende forståelse og etterlevelse av regelverkskrav hos KBO-enhetene	Manglende kompetanse og/eller kapasitet / evne til å stille tilstrekkelige krav til leverandører	Manglende kompetanse og/eller kapasitet / evne til å følge opp krav som stilles i leverandørkjeden	Manglende identifisering av, informasjonsdeling om, og lukking av digitale sårbarheter i utstyr og systemer hos aktørene i leverandørkjeden	Manglende kompetanse og/eller kapasitet / evne til å detektere og håndtere IKT-sikkerhetshendelser hos aktørene i leverandørkjeden
Etablere forum for kompetanseheving i bransjen	X	X	X	X	X	X
Oppfordre KBO-enheter / bransjeforening til et bransjeinitiativ for felles kompetanseheving og samarbeid om leverandøroppfølging i bransjen	X	X	X	X	X	X
Utarbeide eksempelunderlag for trening og øvelser innen IKT-sikkerhet	X	X		X	X	X
Forbedre kommunikasjon gjennom NVEs nettsider	X	X	X	X	X	X
Gjennomføre tilsynsserie mot KBO-enheter rettet mot IKT-sikkerhet og leverandøroppfølging		X	X	X	X	X
Videreutvikle veiledning og maler knyttet til IKT-sikkerhet i anskaffelser og tjenesteutsetting i kraftbransjen			X	X		

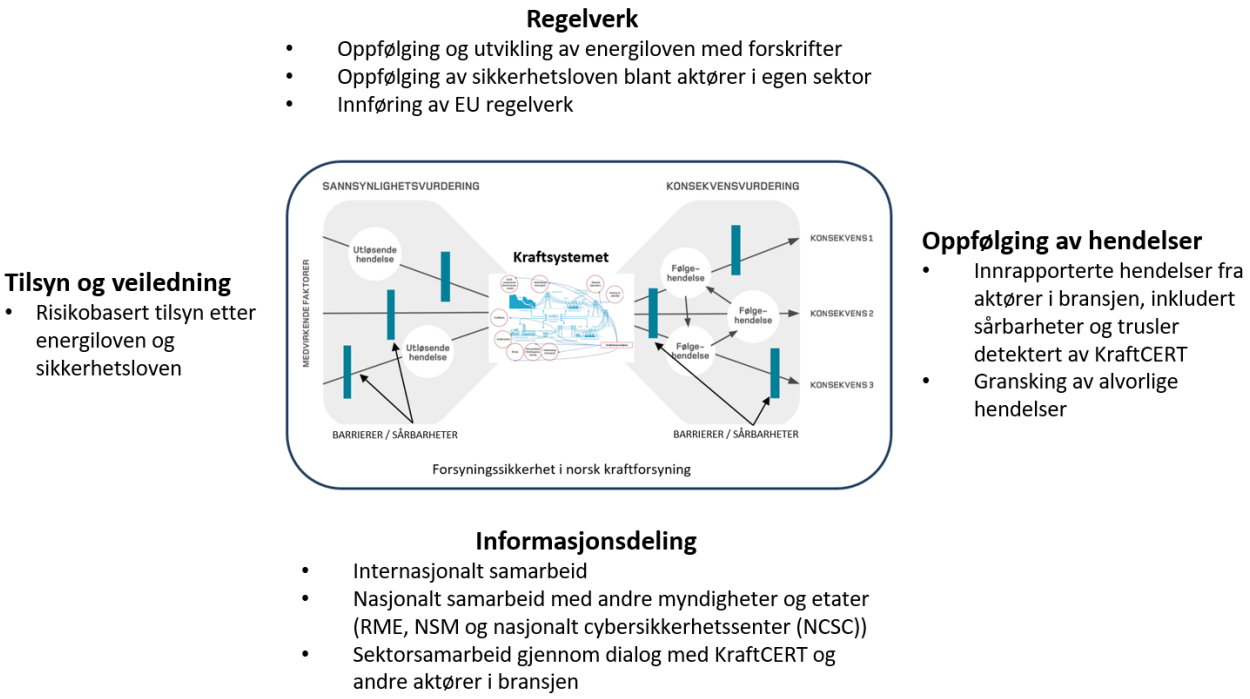
Tiltak	Sårbarheter					
	Manglende risiko- og trussel-forståelse hos aktørene i leverandørkjeden	Manglende forståelse og etterlevelse av regelverkskrav hos KBO-enhetene	Manglende kompetanse og/eller kapasitet / evne til å stille tilstrekkelige krav til leverandører	Manglende kompetanse og/eller kapasitet / evne til å følge opp krav som stilles i leverandørkjeden	Manglende identifisering av, informasjonsdeling om, og lukking av digitale sårbarheter i utstyr og systemer hos aktørene i leverandørkjeden	Manglende kompetanse og/eller kapasitet / evne til å detektere og håndtere IKT-sikkerhetshendelser hos aktørene i leverandørkjeden
Vurdere regelverksutvikling knyttet til mulig «gradering» av kraftsensitiv informasjon			X	X		
Vurdere behovet for et tydeligere sektorvist responsmiljø i kraftbransjen					X	X
Vurdere å stille krav til KBO-enheters kapabilitet for å detektere og håndtere et digitalt angrep						X

5 Forslag til veikart

Kartleggingen viser at det er flere digitale sårbarheter knyttet til IKT-sikkerhet i leverandørkjeden. Gitt trusselbildet kraftsektoren eksponeres for i dag, de lange digitale verdikjedene og den store leverandør-avhengigheten som sektoren i økende grad har, er det en forutsetning for robust IKT-sikkerhet i kraftsektorene at:

- Det finnes tilstrekkelige og tydelige krav som enten direkte eller indirekte regulerer alle aktørene i den digitale leverandørkjeden
- Det finnes tilstrekkelig bevissthet og kompetanse om verdier, trusler, sårbarheter, risiko og tiltak på de ulike leddene i de digitale verdikjedene / leverandørkjedene
- Aktørene i leverandørkjeden på en god og effektiv måte evner å håndtere risiko og oppfylle krav
- Aktørene i leverandørkjeden er tilstrekkelig i stand til å detektere og håndtere hendelser
- Kravene som er stilt følges tilstrekkelig opp gjennom hele kjeden

Det kreves en felles, koordinert innsats fra både myndigheter, KBO-enheter og leverandører å redusere de digitale sårbarhetene i leverandørkjeden, og oppfylle disse forutsetningene. I denne anbefalingen er hovedfokus på hva NVE selv må ta initiativ til eller gjennomføre, men aktuelle initiativer for bransjen berøres også. NVE har både en tilsyns-, veilednings- og forvaltningsrolle i sikkerhetsarbeidet i sektoren. Dette er illustrert i Figur 6.



Figur 6: NVEs ulike roller som myndighet

Som figuren viser har NVE flere ulike virkemidler å spille på for å styrke IKT-sikkerheten. Uansett hvilke virkemidler og tiltak som velges og prioriteres, vil det være nødvendig å styrke NVEs kompetanse og kapasitet på det digitale sikkerhetsområdet for å møte både dagens og fremtidens digitale sikkerhets-behov. Kraftsektoren gjennomgår, som de fleste samfunnsområder for øvrig, en rask teknologisk utvikling og stor grad av digitalisering. Det utvikles smarte nett, og elektrifiseringen av samfunnet gjør avhengigheten til det smarte strømnettet stadig større. NVE er også, fra 2020 tilsynsmyndighet i

kraftsektoren etter sikkerhetsloven. I Nasjonal strategi for digital sikkerhet[22] er digital sikkerhet i kritiske samfunnsfunksjoner som strømnettet, prioritert som én av de fem viktigste områdene å sikre. Ett av delmålene for å ivareta dette er: *«Myndighetene stiller krav til sikkerhet i kritisk digital infrastruktur, veileder og fører tilsyn med at sikkerheten er forsvarlig»*. Aktørene i denne undersøkelsen beskriver at de i liten grad opplever fokus eller tilsyn / kontroll fra NVE på IKT-sikkerhet og leverandørstyring, og de etterlyser også informasjon og veiledning. Det vil derfor være urealistisk å forutsette at IKT-sikkerheten kan ivaretas uten å styrke dette området hos NVE.

Teknologi og digitalisering gir imidlertid ikke bare nye utfordringer og økt behov for kompetanse og kapasitet hos tilsynsmyndigheten. Det finnes også gode muligheter for å utnytte den samme teknologien til å forbedre, tilgjengeliggjøre og effektivisere virkemidlene og tiltakene som iverksettes. Det er derfor i anbefalingene lagt vekt på og prioritert tiltak som også gjør bruk av nettopp disse mulighetene. Selv om dette kan gi behov for ekstra innsats og investering på kort sikt, vurderes effektiviseringsgevinsten å være stor over tid.

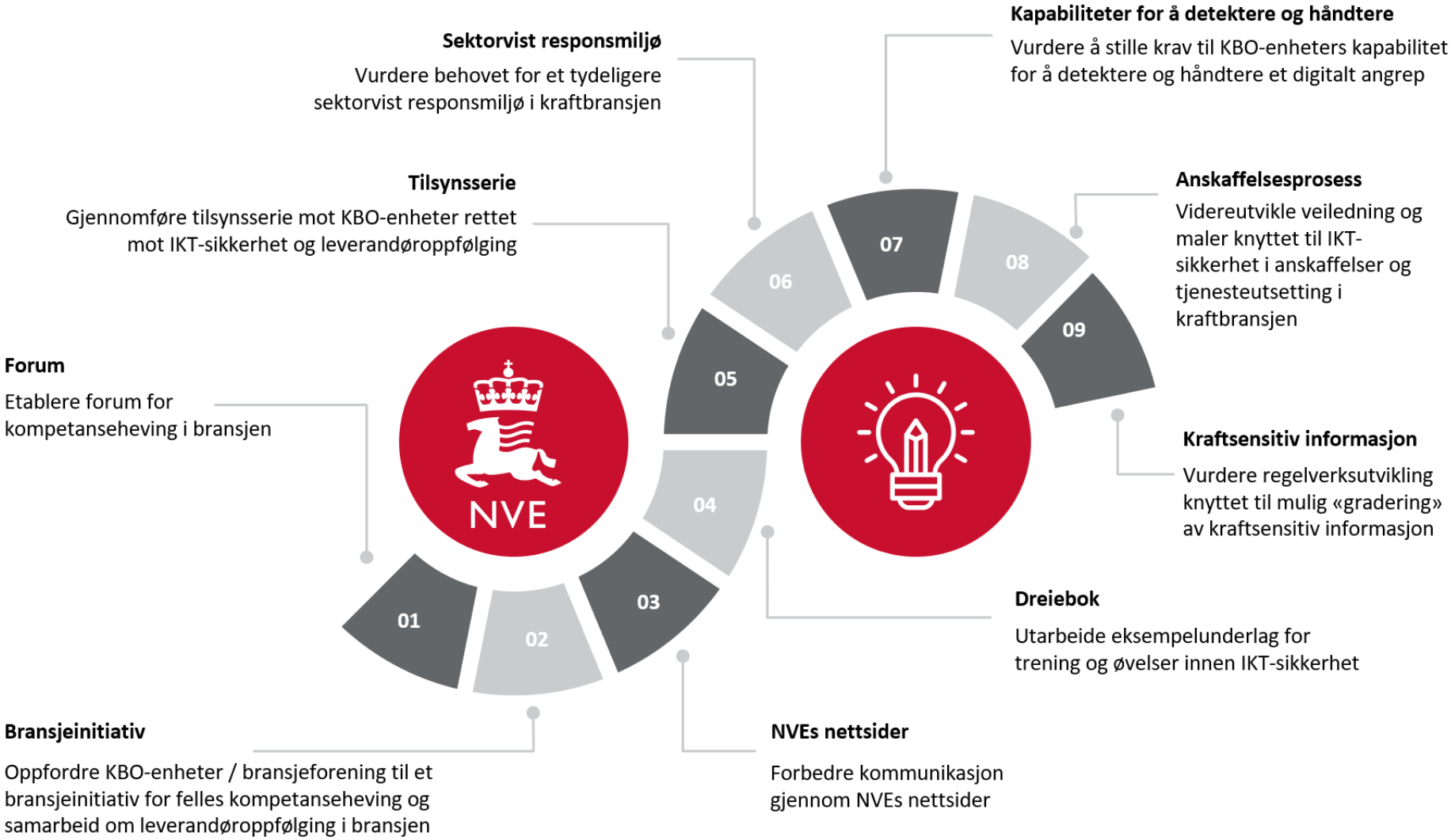
Det er også verdt å merke seg at de gjennomgående og fremtredende sårbarhetene som er avdekket i denne undersøkelsen, for eksempel manglende risikoforståelse, kompetanse og evne til å avdekke og håndtere IKT-sikkerhetshendelser, er helt sammenfallende med tre av de øvrige høyest prioriterte områdene i den nasjonale strategien for digital sikkerhet.

Basert på disse viktigste sårbarhetene og tiltakene som diskuteres i kapittel 4, gis det i Figur 7 en anbefaling til hvordan tiltakene bør innføres, i form av et veikart for NVEs oppfølging av IKT-sikkerhet i leverandørkjeden. Tiltakene er fordelt på tre kategorier ut fra hvilken rekkefølge de bør iverksettes, og hvor raskt man kan forvente effekt av tiltakene. Kategorier og tiltak er oppsummert Tabell 3, mens en kort beskrivelse og forklaring av tiltakene følger til slutt.

Tabell 3: Forslag til kategorisering av tiltak for NVEs oppfølging av IKT-sikkerhet i leverandørkjeden

Kategori	Tiltak
Tiltak som bør iverksettes snarlig og som er vurdert å kunne gi rask effekt	1) Etablere forum for kompetanseheving i bransjen 2) Oppfordre KBO-enheter / bransjeforening til et bransjeinitiativ for felles kompetanseheving og samarbeid om leverandøroppfølging i bransjen 3) Forbedre kommunikasjon gjennom NVEs nettsider 4) Utarbeide eksempelunderlag for trening og øvelser innen IKT-sikkerhet 5) Gjennomføre tilsynsserie mot KBO-enheter rettet mot IKT-sikkerhet og leverandøroppfølging
Tiltak som bør påbegynnes snarlig og som er vurdert å kunne gi effekt på lengre sikt	6) Vurdere behovet for et tydeligere sektorvist responsmiljø i kraftbransjen 7) Vurdere å stille krav til KBO-enheters kapabilitet for å detektere og håndtere et digitalt angrep
Tiltak som bør gjennomføres på litt lengre sikt	8) Videreutvikle veiledning og maler knyttet til IKT-sikkerhet i anskaffelser og tjenesteutsetting i kraftbransjen 9) Vurdere regelverksutvikling knyttet til mulig «gradering» av kraftsensitiv informasjon

[22] https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/nasjonal-strategi-for-digital-sikkerhet.pdf



Figur 7: Forslag til veikart for NVEs oppfølging av IKT-sikkerhet i leverandørkjeden

1) Etablere forum for kompetanseheving i bransjen

For å bidra til å heve sikkerhetskompetansen i bransjen bør NVE etablere et IKT-sikkerhetsforum som er åpent for alle aktører i bransjen, både KBO-enheter og leverandører. Et første steg, gitt både dagens pandemisituasjon og grad av tilgjengelighet for mange aktører, bør være å gjennomføre en serie webinarer med ulike temaer. Forumet bør videreføres som et regelmessig forum med relativt hyppig frekvens, for eksempel månedlig eller annen hver måned. Temaer som bør prioriteres belyst er:

- Hvilket risiko- og trusselbilde kraftbransjen står ovenfor
- Kraftberedskapsforskriften på 1-2-3
- Hva menes med kraftsensitiv informasjon
- Anskaffelsesprosesser: hvordan stille de riktige sikkerhetskravene i alle IT-anskaffelser for hele livsløpet
- Digital sikkerhet i pilotprosjekter

Temaene kan også belyses med erfaringsdeling fra ulike aktører i tillegg til informasjon fra NVE, men eierskap til struktur og innhold bør ligge hos NVE.

2) Oppfordre KBO-enheter / bransjeforening til et bransjeinitiativ for felles kompetanseheving og samarbeid om leverandøroppfølging i bransjen

NVE bør oppfordre KBO-enhetene og bransjeforeningene til at bransjen selv å etablere:

A. Et forum for erfaringsdeling og god praksis som er tilgjengelig for alle aktører i leverandørkjeden. Eksempel på aktuelle temaer kan være:
   - God praksis for ulike tekniske løsninger.
   - God praksis for anskaffelsesprosesser: hvordan stille de riktige sikkerhetskravene i alle IT-anskaffelser for hele livsløpet
   - Fokus på digital sikkerhet i pilotprosjekter

B. Et samarbeid for KBO-enhetene om oppfølging av leverandører. Som beskrevet i kapittel 4.4 opplever bransjen kompetanse- og kapasitetsutfordringer både hos KBO-enheter og blant leverandørene relatert til å følge opp og kontrollere krav i leverandørkjeden. Bransjen bør selv gjøre en vurdering av hva som kan være en god og effektiv måte å samarbeide og samordne oppfølging mot felles leverandører på. Her kan det hentes erfaringer fra en rekke ulike bransjer som har etablert felles løsninger for sikkerhetskrav som stilles til leverandører, for revisjon og oppfølging av leverandører, og for deling av revisjonsrapporter.

3) Forbedre kommunikasjon gjennom NVEs nettsider

Det anbefales å gjøre en helhetlig gjennomgang og revisjon av NVEs nettsider, for å forbedre kommunikasjonen og digitalisere og tilgjengeliggjøre relevant informasjon om IKT-sikkerhet i kraftbransjen. Nettsidene bør omstruktureres og gis forbedret søkbarhet slik at det er enkelt å finne relevant informasjon. Informasjonen som tilgjengeliggjøres kan også gjøres mer interaktiv for enkel digital bruk. Noen viktige elementer som bør inkluderes er:

- Tilgjengeliggjøring av oppdatert, bransjespesifikk informasjon om, og NVEs vurdering av, risiko- / trusselbildet som kraftbransjen står ovenfor. Dette kan også inkludere forslag til og veiledning i bruk av rammeverk for risikovurdering og risikostyring.

- Digitalisering og strukturering av kraftberedskapsforskriften, med tilhørende veiledningstekst, ordforklaringer, funn fra tilsyn og erfaring fra hendelser (og krysskoplinger av informasjonen). Det bør gjøres enklere å se sammenheng mellom forskriftskrav, veiledningstekst og annen relevant informasjon. Denne informasjonen bør foreligge både på norsk og på engelsk.
- Gjennomgang og vurdering av informasjon som er tilgjengeliggjort på nettsidene, med tanke på eksponering av kraftsensitive opplysninger.

4) Utarbeide eksempelunderlag for trening og øvelser innen IKT-sikkerhet

Det foreslås at NVE utarbeider et sett med ulike «komplette» trenings- og øvelsessenarioer (dreiebok) innen IKT-sikkerhet for industrielle IKT-systemer i kraftbransjen. Det bør beskrives hvilke deler av organisasjonen som bør delta i øvelsene, der samspillet mellom KBO-enhet og leverandør inkluderes og fokuseres. Det bør være bredde i øvelsessenarioene slik at ulike aspekter av IKT-sikkerhet blir berørt. Dreieboken bør tilgjengeliggjøres digitalt på NVEs nettsider. Dette vil kunne gi aktørene i bransjen et godt og felles utgangspunkt for relevante trening og øvelser – og for læring fra disse.

5) Gjennomføre tilsynsserie mot KBO-enheter rettet mot IKT-sikkerhet og leverandøroppfølging

KBO-enhetene opplever i liten grad at NVE kontrollerer og følger dem opp med tilsyn som har fokus på IKT-sikkerhet og leverandørstyring. Fokus, oppfølging og kontroll fra tilsynsmyndigheten er essensielt for bransjens oppfatning av temaets viktighet, for prioritering i virksomhetene og ikke minst for lærings-effekten. NVE anbefales å forberede og gjennomføre en tilsynsserie / kampanje mot KBO-enheter rettet mot IKT-sikkerhet og leverandøroppfølging. Dette bør inkludere i hvilken grad KBO-enhetene har en risikobasert tilnærming til sin leverandøroppfølging, og kampanjen bør ha en viss varighet / omfang (eksempelvis ett år og et tilstrekkelig antall tilsynsobjekter). For å nå ut til flere av KBO-enhetene i kampanjeperioden bør det vurderes å supplere stedlige systemtilsyn med tilsynsformer som eksempelvis egenrapportering og ledelsesmøter, med fokus på IKT-sikkerhet og leverandøroppfølging.

6) Vurdere sektorvist responsmiljø for kraftbransjen

Informasjonsdeling er avgjørende for å detektere og håndtere digitale angrep. Det er også behov for å øke samarbeidet og informasjonsflyten generelt knyttet til identifiserte sårbarheter i bransjen. I denne sammenheng bør NVE vurdere å etablere et sektorvist responsmiljø eller gi KraftCERT et tydeligere mandat og oppdragsbeskrivelse for dette, samt presisere krav til varsling og informasjonsdeling blant aktørene i bransjen.

Dette må også ses i sammenheng med nasjonal satsning på det digitale sikkerhetsområdet med tanke på etablering av sektorvise responsmiljøer og styrking av den nasjonale modellen for hendelseshåndtering, der ambisjonen med de sektorvise responsmiljøene er at disse skal kunne bistå sin sektor med kompetanse og være knutepunkt for informasjon og informasjonsflyt mellom virksomheter i sektoren, mellom sektorer og mellom sektor og nasjonalt nivå (NorCERT).

7) Vurdere å stille krav til KBO-enheters kapabilitet for å detektere og håndtere et digitalt angrep

Det bør vurderes å stille krav til KBO-enheters kapabilitet for å detektere og håndtere et digitalt angrep, for eksempel gjennom å kreve at KBO-enheter må etablere «security operations centre» (SOC) selv eller

anskaffe tilstrekkelige SOC-tjenester fra en «managed security service provider» (MSSP). Dette tiltaket må også vurderes i lys av den nye nettkoden som er under utarbeidelse i EU og som på sikt kan bli gjeldende også for Norge der utkastet til rammeretningslinje for nettkoden beskriver dette som et krav til at kritiske / større virksomheter for grensekryssende elektrisitetsflyt. Her kan det også være relevant å hente læring og erfaring fra det nasjonale cybersikkerhetssenteret (NCSC).

8) Videreutvikle veiledning knyttet til IKT-sikkerhet i anskaffelser og tjenesteutsetting i kraftbransjen

NVE bør utnytte digitalisering og interaksjon bedre for å styrke tilrettelegging for virksomhetene. Eksempelvis har NVE utarbeidet en sjekkliste for IKT-sikkerhet i anskaffelser som dekker hele livssyklusen til anskaffelsen (NVE, 2020), og mal for informasjonssikkerhetsavtale som KBO-enhet kan bruke mot leverandør. Dersom disse, i stedet for å være statiske dokumenter som KBO-enhetene ikke nødvendigvis kjenner seg igjen i, kunne bygges opp som interaktive sider, ville verdien og effekten kunne økes betydelig. Da kan KBO-enhetene eksempelvis bruke et interaktivt anskaffelsesskjema der de gjennom spørsmål må ta stilling til egen risiko og få relevante forslag til oppfølging og aksjoner basert på dette. Her kan ulike former for veiledning (tekst, tale, video, krav osv.) være tilgjengelig der spørsmålene kommer opp. Basert på arbeidet i denne prosessflyten kan det genereres tilpassede kontraktskrav som kan hentes ut av KBO-enheten. Det vil da også være enkelt å tilknytte sjekklister som kan benyttes i oppfølging og kontroll, som leverandørrevisjoner. Dette er et eksempel på hvordan digitalisering og ny teknologi kan utnyttes for å effektivisere og tilgjengeliggjøre veiledning (og støttestruktur).

9) Vurdere regelverksutvikling knyttet til mulig «gradering» av kraftsensitiv informasjon

Kartleggingen har avdekket betydelig usikkerhet i bransjen når det gjelder å identifisere, og hensikts-messig håndtere, kraftsensitiv informasjon. Noe av utfordringen synes å ligge i at det ikke finnes noen «gradering» / klassifisering av informasjon innenfor begrepet kraftsensitiv. Dette gir et stort spenn i informasjon som kan synes å ha veldig ulik kritikalitet. Det er pedagogisk utfordrende at informasjon som vurderes som lite sensitiv oppleves å skulle beskyttes like godt som mye mer kritisk informasjon. Det bør vurderes om en form for inndeling etter kritikalitet vil gjøre det enklere for bransjen å se risikopotensialet, og beskytte informasjon hensiktsmessig. Dette kan også bidra til økt bevissthet rundt hvilken informasjon det er viktigst å beskytte, og hvorfor.

6 Referanser

ENISA (2021). ENISA Threat landscape for supply chain attacks. European Union Agency for Cybersecurity.

Kraftberedskapsforskriften (2018). Forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften). FOR-2012-12-07-1157. https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157

NOU 2015:13 (2015). Digital sårbarhet – sikkert samfunn — Beskytte enkeltmennesker og samfunn i en digitalisert verden. https://www.regjeringen.no/no/dokumenter/nou-2015-13/

NSM (2021). Risiko 2021 – helhetlig sikring mot sammensatte trusler. https://nsm.no/regelverk-og-hjelp/rapporter/helhetlig-digitalt-risikobilde-2020/

NSM (2020). Helhetlig digitalt risikobilde 2020. https://nsm.no/getfile.php/134468-1604926904/Demo/Dokumenter/Rapporter/NSM_IKT-risikobilde_2020_enkeltside.pdf

NVE (2021). Kraftbransjens leverandørkjeder – digital sikkerhet og sårbarhet i globaliserings tidsalder. Utkast til rapport. Dato 10. november 2021.

NVE (2020). IKT-sikkerhet i anskaffelser og tjenesteutsetting i kraftbransjen – sjekkliste. NVE rapport nr. 1/2020. http://publikasjoner.nve.no/rapport/2020/rapport2020_01.pdf

NVE (2018). IKT-sikkerhet ved anskaffelser og tjenesteutsetting i energibransjen. NVE rapport nr. 90/2018. https://publikasjoner.nve.no/rapport/2018/rapport2018_90.pdf

Riksrevisjonen (2021). Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen. Dokument 3:7 (2020-2021). https://www.riksrevisjonen.no/rapporter-mappe/no-2020-2021/undersokelse-av-nves-arbeid-med-ikt-sikkerhet-i-kraftforsyningen/

Sikkerhetsloven (2018). Lov om nasjonal sikkerhet (sikkerhetsloven). LOV-2018-06-01-24. https://lovdata.no/dokument/NL/lov/2018-06-01-24

True, John & Xi, Chengjie & Jessurun, Nathan & Ahi, Kiarash & Asadizanjani, Navid. (2021). Review of THz-based semiconductor assurance. Optical Engineering. 60. 10.1117/1.OE.60.6.060901.

Vedlegg I Intervjuguide

KBO-enheter

- Hvilke sikkerhetsutfordringer ser dere i leverandørkjedene?
- Hvordan regulerer dere IKT-sikkerhet gjennom kontrakter nedover i leverandørkjedene – og hvordan følges dette opp?
- Hvordan opplever dere at leverandørene bygger inn IKT-sikkerhet i pilotprosjekter som testes i kraftbransjen?
- I hvilken grad lukker leverandørene digitale sårbarheter i egne produkter, varsler dere som kunde og samarbeider med KraftCERT eller andre CSIRT-miljøer?
- Bør leverandørene avkreves sertifisering i henhold til internasjonale sikkerhetsstandard?
- Er leverandørene bevisste på sikkerhetsutfordringer og ser at (og hvordan) de selv kan bidra for å beskytte norsk kraftforsyning mot cyberangrep?
- Hvordan kan NVE bidra til å ivareta sikkerhet i leverandørkjeden til energiforsyningen?
- Har dere noen synspunkter på om viktige leverandører bør bli KBO-enhet og underlagt deler av kraftberedskapsforskriften?

Leverandører

- Hvilke sikkerhetsutfordringer ser dere i leverandørkjedene til norsk kraftforsyning?
- Hvordan reguleres IKT-sikkerhet gjennom kontrakter nedover i leverandørkjedene – og hvordan følges dette opp?
- Hvordan opplever bygger dere som leverandører inn IKT-sikkerhet i pilotprosjekter som testes i kraftbransjen?
- I hvilken grad lukker dere digitale sårbarheter i egne produkter, varsler kundene deres og samarbeider med KraftCERT eller andre CSIRT-miljøer?
- Bør leverandører som ikke er sertifisert allerede, avkreves sertifisering i henhold til internasjonale sikkerhetsstandarder?
- Er dere som leverandører bevisste på sikkerhetsutfordringer og ser at (og hvordan) dere selv kan bidra for å beskytte norsk kraftforsyning mot cyberangrep?
- Hvordan kan NVE bidra til å ivareta sikkerhet i leverandørkjeden til energiforsyningen?
- Har dere noen synspunkter på om viktige leverandører bør bli KBO-enhet og underlagt deler av kraftberedskapsforskriften?

KraftCERT

- Hvilke sikkerhetsutfordringer ser dere i leverandørkjedene?
- Hvilke erfaringer har dere knyttet til hvordan IKT-sikkerhet reguleres gjennom kontrakter nedover i leverandørkjedene – og hvordan dette følges opp?
- Hvordan opplever dere at leverandørene bygger inn IKT-sikkerhet i pilotprosjekter som testes i kraftbransjen?
- I hvilken grad lukker leverandørene digitale sårbarheter i egne produkter, varsler sine kunder og samarbeider med KraftCERT eller andre CSIRT-miljøer?
- Bør leverandørene avkreves sertifisering i henhold til internasjonale sikkerhetsstandard?
- Er leverandørene bevisste på sikkerhetsutfordringer og ser at (og hvordan) de selv kan bidra for å beskytte norsk kraftforsyning mot cyberangrep?
- Hvordan kan NVE bidra til å ivareta sikkerhet i leverandørkjeden til energiforsyningen?
- Har dere noen synspunkter på om viktige leverandører bør bli KBO-enhet og underlagt deler av kraftberedskapsforskriften?

Myndigheter

- Hvilke sikkerhetsutfordringer ser dere i leverandørkjedene?
- Hvilke erfaringer har dere knyttet til hvordan IKT-sikkerhet reguleres gjennom kontrakter nedover i leverandørkjedene – og hvordan dette følges opp?
- Hvordan opplever dere at leverandørene bygger inn IKT-sikkerhet i pilotprosjekter som testes i kraftbransjen?
- I hvilken grad lukker leverandørene digitale sårbarheter i egne produkter, varsler sine kunder og samarbeider med CSIRT-miljøer?
- Stiller dere krav eller har forventninger om at leverandørene har sertifisering i henhold til internasjonale sikkerhetsstandarder?
- Er leverandørene bevisste på sikkerhetsutfordringer og ser at (og hvordan) de selv kan bidra for å beskytte kraftforsyningen mot cyberangrep?
- Hvordan jobber dere for å følge opp sikkerhet i leverandørkjeden til energiforsyningen?
- Er viktige leverandører direkte underlagt energimyndighetenes regelverkskrav?