NVE

EKSTERN RAPPORT NR. 24 / 2024

Regulering av IT/OT-sikkerhet hos leverandører og leverandørkjeder i kraftforsyningen

SKREVET AV DNV

NVE Ekstern rapport nr 24/2024

Regulering av IT/OT-sikkerhet hos leverandører og leverandørkjeder i kraftforsyningen

Utgitt av:	Norges vassdrags- og energidirektorat
Redaktør:	Linn Barstad
Forfattere:	Alexander Iversen, Rune Moen, Arve Johan Kalleklev, Jean-Raphaël Vielle, Tore Helge Kristiansen og Mai H. Tran / DNV
Omslagsbilde:	Kraftledninger, Kuhtai
Foto:	Pål Mellquist/ NVE
ISBN:	978-82-410-2428-3
ISSN:	2535-8235
Saksnummer:	202420468

Sammendrag: Virksomheter i kraftforsyningen bruker digitale tjenester, programvare og styringssystemer fra nasjonale og internasjonale leverandører. Den sterke avhengigheten av digitale tjenester og et stadig mer krevende trusselbilde styrker behovet for å styre risiko i anskaffelser, og å ha god oppfølging av IT/OT-sikkerhet i hele leverandørkjeden samtidig som det kommer nye europeiske sikkerhetsregelverk som aktørene må forholde seg til. Rapporten belyser hvilken grad kravene i kraftberedskapsforskriften dekker nye behov for leverandørkjedesikkerhet og hvordan NVE kan følge opp viktige leverandører til virksomhetene som er underlagt kraftberedskapsforskriften.

Emneord: IT/OT-sikkerhet, leverandørkjede, leverandørkjedesikkerhet, leverandøroppfølging, kraftberedskapsforskriften, lov om digital sikkerhet, NIS-direktiv, NIS2-direktiv, Cyber Resilience Act, regulering, veiledning

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

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

November, 2024

Forord

Digitaliseringen av kraftforsyningen har skapt en kompleks avhengighet til digitale tjenester, systemer og leverandørkjedene som støtter disse. Med et stadig mer krevende trusselbilde og økt europeisk regulering gjennom blant annet NIS2-direktivet, er det avgjørende å sikre at kravene til IT- og OT-sikkerhet er tilpasset dagens og fremtidens utfordringer.
Denne rapporten styrker forståelsen av hvordan IT- og OT-sikkerhet kan og bør reguleres i kraftforsyningens leverandørkjeder. Den bygger på tidligere anbefalinger og tilbakemeldinger fra blant annet Riksrevisjonen og bransjeaktører, og vurderer ulike reguleringsalternativer. Samtidig belyser den hvordan NVE kan balansere rollen som veileder og regulator for å sikre en robust og trygg leverandørkjede.

Vi vil takke DNV for deres grundige arbeid med denne utredningen, samt virksomhetene som deltok i intervjuer og bidro med innsikt. Rapporten gir et godt grunnlag for å styrke sikkerheten i kraftforsyningen gjennom bedre oppfølging av leverandører og leverandørkjeder.

Oslo, 14. november 2024

Jon-Martin Storm
fungerende seksjonssjef
Seksjon for digital sikkerhet i kraftforsyningen
Avdeling for tilsyn og beredskap
Norges vassdrags- og energidirektorat

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

Regulering av IT/OT-sikkerhet hos leverandører og leverandørkjeder i kraftforsyningen

Rapport for Norges vassdrags- og energidirektorat

Rapportnr.: 2024-2034, Rev. 0
NVE referansenr.: 58500/713
Dato: 31.10.2024

Rapporttittel:	Regulering av IT/OT-sikkerhet hos leverandører og leverandørkjeder i kraftforsyningen	DNV AS Cyber Security
Oppdragsgiver:	Rapport for Norges vassdrags- og energidirektorat	Tel: +47 67 57 99 00
Kontaktperson:	Linn Barstad	MVA 945 74 89 31
Dato:	31.10.2024	
Prosjektnr.:	10524836	
Org. enhet:	DNV Cyber	
Rapportnr.:	2024-2034, Rev. 0	
NVE referansenr.:	58500/713	

Levering av denne rapporten er underlagt bestemmelsene i kontrakt med saksnummer 202409752

Oppdragsbeskrivelse: NVE ønsker å få kartlagt om eksisterende reguleringer er tilpasset dagens behov i hele leverandørkjeden for energiaktører, og få kvalifiserte innspill og vurdering for hvordan best forme retningslinjer for sikkerhet og beredskap i sektoren.

Utført av:	Verifisert av:	Godkjent av:
Alexander Iversen Sjefskonsulent	Rune Moen Senior Sjefskonsulent	Arve Johan Kalleklev Vice President
Jean-Raphaël Vieille Sjefskonsulent	Tor Helge Kristiansen Senior Sjefskonsulent	
Mai H. Tran Konsulent		

Internt i DNV er informasjonen i dette dokumentet klassifisert som:

☒ Open
☐ DNV Restricted
☐ DNV Confidential
☐ DNV Secret

-- --

Keywords

Cybersikkerhet i leverandørkjeden, krav i kraftberedskapsforskriften (kbf) mot europeiske krav, NIS/NIS2, CRA.

Rev. no.	Date	Reason for issue	Prepared by	Verified by	Approved by
A	22.10.24	Foreløpig rapport for NVE verifikasjon	Alexander Iversen Jean-Raphaël Vieille Mai H. Tran	Tor Helge Kristiansen	Rune Moen
0	31.10.24	Endelig rapport	Alexander Iversen Jean-Raphaël Vieille Mai H. Tran	Rune Moen	Arve Johan Kalleklev

UAVHENGIGHET, UPARTISKHET OG BEGRENSNINGER I RÅDGIVNINGENS UTSTREKNING

Dette dokumentet inneholder innhold levert av DNV. Vær oppmerksom på følgende:

Etiske uavhengighetstiltak

For å opprettholde den nødvendige integritet og upartiskhet som er essensielt for våre tredjepartsroller knyttet til samsvarsvurderinger, utfører DNV innledende interessekonfliktvurderinger før vi påtar oss engasjement i tilknytning til rådgivningstjenester.

Rolleprioritet

Denne rapporten er utarbeidet av DNV i sin rådgivende kapasitet, etter at vi har gjort interessekonfliktvurderinger. Innholdet i rapporten er adskilt fra DNVs ulike roller som uavhengig leverandør av tredjeparts tjenester knyttet til samsvarsvurdering. Hvor overlapp eksisterer mellom disse to typene av tjenester, vil tredjeparts tjenester knyttet til samsvarsvurdering utført av DNV være uavhengige av rådgivning som er gitt på vegne av DNV og de vil ha forrang over de rådgivende tjenestene som ytes.

Fremtidige tredjeparts tjenester knyttet til samsvarsvurdering

Innholdet i dette dokumentet vil ikke forplikte eller påvirke DNVs uavhengige og upartiske dømmekraft eller utfallet i eventuelle fremtidige tredjeparts tjenester knyttet til samsvarsvurdering som utføres av DNV hvor det kan være en viss tilknytning og sammenheng mellom rådgivingen som er gjort og den fremtidige tredjeparts tjenesten knyttet til samsvarsvurdering som skal ytes.

Gjennomgang av overholdelse

DNVs overholdelse av etiske regler og bransjestandarder når det gjelder skille av DNVs ulike roller og tjenester er underlagt periodiske eksterne gjennomganger.

INNHOLDSFORTEGNELSE

1 FORKORTELSER 4

2 SAMMENDRAG 5

3 INNLEDNING 7
3.1 Bakgrunn 7
3.2 Metode 7
3.3 Avgrensinger 9

4 LEVERANDØRKJEDESIKKERHET: REGELVERK, STANDARDER OG RAMMEVERK 10
4.1 Gjeldende regelverk i kraftforsyningen 10
4.2 Relevante standarder, rammeverk og veiledninger 11
4.3 Kommende regulering 13

5 SAMMENLIGNING AV KBF OG NYE EUROPEISKE REGULERINGER OG KONSEVENSER FOR LEVERANDØRER I KRAFTFORSYNINGEN 16
5.1 Leverandørkjedesikkerhet i kbf og i europeiske reguleringer 16
5.2 Vurdering av kraftforsyningens leverandører opp mot NIS/NIS2 17

6 ALTERNATIVE FREMTIDIGE REGULERINGSMETODER 19
6.1 Nullalternativet: Indirekte regulering med dagens veiledningsinnsats 19
6.2 Alternativ A: Indirekte regulering med forsterket leverandøroppfølging 22
6.3 Alternativ B: Direkte regulering av leverandører 25

7 ANBEFALING OG VEIEN VIDERE 28
7.1 Samlet vurdering og anbefalt løsning: Alternativ A 28
7.2 Oppdatering av forskriftskrav versus retningslinjer i veiledning 29
7.3 Bruk av standardisering for leverandørkjedesikkerhet 30
7.4 Innhenting og bruk av opplysninger om leverandører 31
7.5 Opplysning og veiledning om IT/OT-sikkerhet til leverandører i kraftforsyningen 32

8 REFERANSER 33

VEDLEGG A: KBF-KRAV VERSUS EUROPEISKE-KRAV 35

VEDLEGG B: ANONYMISERT UTTREKK AV LEVERANDØRER 42

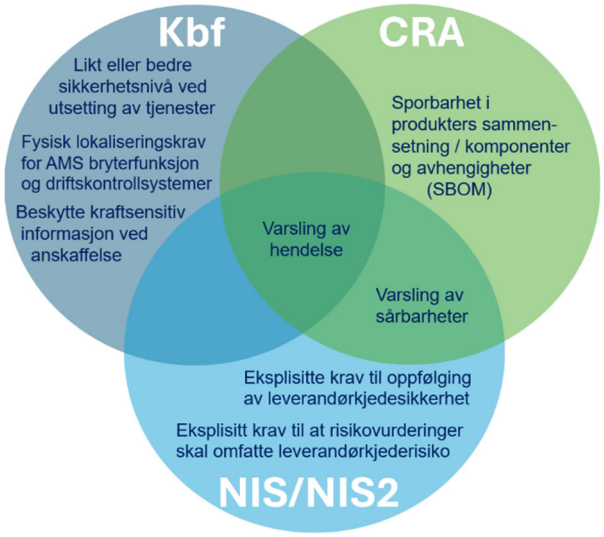
1 FORKORTELSER

Forkortelse	Definisjon
AI	Artificial Intelligence
AICPA	American Institute of Certified Public Accountants
AMS	Avanserte måle- og styringssystemer
CRA	Cyber Resilience Act
CSF	NIST Cybersecurity Framework
CSIRT	Computer Security Incident Response Team
DSP	Digital Service Provider
EU-CyCLONe	European cyber crisis liaison organisation network
FSK	Forum for informasjonssikkerhet i kraftforsyningen
IACS	Industrielle automasjons og kontrollsystemer
IEC 62443	En serie standarder som dekker cybersikkerhet for operasjonell teknologi (OT) i industrielle automasjons- og kontrollsystemer (IACS)
IKT	Informasjons- og kommunikasjonsteknologi
IoT	Internet of Things
ISO/IEC 27001	Standard for informasjonssikkerhet
ISO/IEC 27002	Standard som beskriver beste praksis for informasjonssikkerhetstiltak
ISO/IEC 27036-3	Retningslinjer for sikkerhet i leverandørkjeder for maskinvare, programvare og tjenester
IT	Informasjonsteknologi
Kbf	Kraftberedskapsforskriften
KBO	Kraftforsyningens beredskapsorganisasjon
KBO-enhet	Virksomhet som eier eller driver anlegg, system eller annet, og som er klassifisert etter kbf § 5-2 eller § 5-7
KDS	Kraftforsyningens distriktssjefer
KSL	Kraftforsyningens sentrale ledelse
MSP	Managed Service Provider
MSSP	Managed Security Service Provider
NCCS	Network Code on Cybersecurity
NIS	Direktiv (EU) 2016/1148 om sikkerhet i nettverks- og informasjonssystemer
NIS2	Direktiv (EU) 2022/2555 om sikkerhet i nettverks- og informasjonssystemer (som erstatter NIS)
NIST	National Institute of Standards and Technology
NSM	Nasjonal sikkerhetsmyndighet
NVE	Norges vassdrags- og energidirektorat
OT	Operasjonell teknologi – brukt som begrep for driftskontrollsystemer
SBOM	Software Bill Of Materials
SOC 2	System and Organization Controls 2

2 SAMMENDRAG

Virksomheter i kraftforsyningen bruker digitale tjenester, programvare og styringssystemer fra nasjonale og internasjonale leverandører. Den sterke avhengigheten av digitale tjenester og et stadig mer krevende trusselbilde, styrker behovet for å styre risiko i anskaffelser, og å ha god oppfølging av IT/OT-sikkerhet i hele leverandørkjeden. Samtidig kommer det nye europeiske sikkerhetsregelverk som også aktørene i kraftforsyningen må forholde seg til. Norges vassdrags- og energidirektorat har behov for å forstå i hvilken grad kravene i kraftberedskapsforskriften (kbf) dekker nye behov for leverandørkjedesikkerhet, og hvordan de best kan følge opp viktige leverandører til virksomhetene som er underlagt kbf.

Denne rapporten gir først en oversikt over regelverk, relevante standarder, rammeverk og kommende reguleringer som har relevans for sikkerhet i leverandørkjeden. Kravene til leverandørstyring i kbf vurderes opp mot forventede krav etter lov om digital sikkerhet (som implementerer EUs NIS-direktiv), EUs NIS2-direktiv og Cyber Resilience Act (CRA). Figuren under illustrerer krav til leverandørkjeden.



Det er videre gjort en vurdering av i hvilken grad virksomhetene i kraftforsyningen, og deres leverandører forventes å bli direkte regulert etter de nye EU-regelverkene, basert på et representativt utvalg av leverandører av IT, OT og IT-sikkerhetstjenester fra NVEs leverandøroversikt. Vurderingen viser at både virksomheter som inngår i kraftforsyningens beredskapsorganisasjon (KBO-enheter) og de fleste av deres IT/OT-leverandører ventes å bli underlagt nye sikkerhetskrav. Dette har dermed potensiale til å styrke sikkerheten i leverandørkjedene. Et viktig spørsmål er da hvordan NVE som sektormyndighet, og med utgangspunkt i kravene i kbf, i fremtiden kan regulere og følge opp kritiske leverandører til kraftforsyningen. DNV har utredet tre alternativer:

Nullalternativet – indirekte regulering med dagens veiledningsinnsats: Alternativet innebærer at det ikke gjøres noen endringer i kbf, og at veiledningen knyttet til leverandørkjedesikkerhet videreføres som i dag. Ved iverksettelse av fremtidig regulering som bl.a. lov og digital sikkerhet med tilhørende forskrift, og ny regulering som følge av NIS2, videreføres dagens veiledningspraksis tilsvarende.

Alternativ A – indirekte regulering med forsterket leverandøroppfølging: Alternativet innebærer fortsatt indirekte regulering av leverandører, men med tydeligere regulatoriske krav til KBO-enhetenes oppfølging av sikkerhet i leverandørkjeden, samt at NVE gjør tiltak som sikrer økt oversikt over kraftforsyningens leverandørkjeder og kontroll med leverandørkjederisiko.

Alternativ B – direkte regulering av kritiske leverandører: Alternativet innebærer at det etableres regulatoriske krav i kbf som rettes direkte mot kritiske aktører som inngår i kraftforsyningens leverandørkjede. NVE får da virkemidler for å ha oversikt over, og kunne følge opp sikkerheten til, leverandørene direkte.

DNV har drøftet tilnærmingene, herunder hvilke positive og negative virkninger de har for NVE, for KBO-enhetene og for leverandørene. DNV har også innhentet synspunkter på problemstillingen gjennom intervjuer med tre utvalgte virksomheter i kraftforsyningen innenfor kraftproduksjon og -distribusjon.

Samlet finner DNV at alternativ A gir best måloppnåelse da det imøtekommer både behovet for å styrke den enkelte KBO-enhetenes sikkerhet, og gir grunnlag for å styrke NVEs oversikt og kontroll med sikkerhetstilstanden i leverandørmarkedet. Alternativet bygger også på innarbeidede prinsipper om at KBO-enhetene har ansvaret for egen sikkerhet også ved tjenesteutsetting, og innebærer at NVE ikke trenger å etablere et nytt oppfølgingsregime mot en heterogen gruppe med leverandører av IT, OT og IT-sikkerhetstjenester.

Videre drøfter DNV hvordan alternativ A kan gjennomføres i praksis, og viktige forutsetninger for å lykkes. Følgende tema belyses:

Forskriftskrav versus retningslinjer i veiledning: Først gis det føringer for hvilke kravområder som det er aktuelt å tilføye som nye krav i kbf. Dette inkluderer blant annet eksplisitte krav om at leverandørkjederisiko skal inngå i KBO-enhetenes risikovurderinger, og tydeligere oppfølgingsplikt ved tjenesteutsetting gjennom hele livsløpet til leveransen. Det drøftes også hva som bør presiseres i forskrift og hva som bør inngå i veiledning.

Bruk av standardisering: Selv om det brukes relevante rammeverk og standarder som NSMs grunnprinsipper for IKT-sikkerhet og ISO 27001, er det ingen bransjestandard som virker å ha bred adopsjon blant KBO-enhetene for leverandørkjedesikkerhet. Dette kan føre føre til redusert forutsigbarhet og kostnadseffektivitet. DNV anbefaler at det gjennomføres en nærmere analyse av hvordan kraftbransjen bedre kan utnytte potensialet ved å enes om felles standarder og rammeverk.

Innhenting og bruk av opplysninger om leverandører: Før NVE utarbeider eventuelle krav eller retningslinjer til KBO-enhetene om opplysningsplikt om deres leverandører, bør NVE tydeliggjøre hva leverandøroversikten skal brukes til. Hovedformålet er å avdekke sårbarheter og risiko i leverandørkjedene for hele sektoren, som den enkelte KBO-enhet ikke kan identifisere alene, men som NVE som sektormyndighet har forutsetninger for å oppdage. Dette inkluderer blant annet konsentrasjonsrisiko og geopolitisk risiko/nasjonal kontroll. NVE bør i tillegg utarbeide en plan over konkrete virkemidler og tiltak som kan adressere de avdekkede risikoene.

Veiledning av leverandører i kraftforsyningen: Det kan være utfordrende å gi nødvendig veiledning om IT/OT-sikkerhet til leverandører når disse ikke regulerer direkte. Opplysning og veiledning bør derfor skje gjennom samarbeid og dialog, med mål om at leverandørene blir kjent med sikkerhetskravene i kraftsektoren. Samarbeidet bør innrettes slik at leverandørene har incentiver til å delta, ved at NVE deler informasjon som har verdi for leverandørene, og at leverandørene får mulighet til å gi innspill til NVE om forhold som kan bedre deres situasjon overfor kundene i kraftsektoren.

3 INNLEDNING

Denne rapporten utreder ulike tilnærminger til hvordan Norges vassdrags- og energidirektorat (NVE) kan regulere IT- og OT-sikkerhet hos leverandører og leverandørkjeder i kraftforsyningen. En nærmere bakgrunn for utredningen og utredningens metode og avgrensninger er beskrevet i kapitlene 3.1 til 3.3.

Rapporten behandler tre hovedtema. Det første er om krav til leverandørkjedesikkerhet i kraftberedskapsforskriften (kbf) er dekkende og tilstrekkelig i forhold krav i nye EU-regelverk (f.eks. NIS2), eller om det er gap. Dette temaet behandles i kapittel 4.

Det andre hovedtemaet er å vurdere i hvilken grad leverandører av IT- og OT-systemer og -tjenester og leverandører av IT-sikkerhetstjenester til kraftforsyningen, vil bli underlagt fremtidige sikkerhetskrav etter nye EU-regelverk. Dette temaet behandles i kapittel 5.

Det siste hovedtemaet, som behandles i kapittel 6, er hvordan NVE kan innrette egen regulering og oppfølging for å ivareta IT/OT-sikkerhet hos leverandører i kraftforsyningen i lys av nye EU-reguleringer.

Kapittel 7 gir en samlet vurdering og anbefalt løsning for videre arbeid med oppfølging av leverandørkjeden.

3.1 Bakgrunn

Virksomheter i kraftforsyningen bruker digitale tjenester og programvare fra tredjeparter. Disse kan være av ulik størrelse og lokalisert i og utenfor Europa. Kostnadseffektivitet, fokus på egen kjernevirksomhet og økt produktivitet er grunner til at virksomhetene benytter seg av underleverandører og slik sett blir siste ledd på toppen av en leverandørkjede. Den sterke avhengigheten av digitale tjenester og et stadig mer krevende trusselbilde, styrker behovet for å styre risiko i anskaffelser og ha god oppfølging av IT/OT-sikkerhet hos leverandører og leverandørkjeder i anskaffelsen og gjennom hele kontraktsperioden.

Kbf inneholder visse krav til virksomhetene i kraftforsyningen om oppfølging av sikkerhet i anskaffelsesfasen, og oppfølging av at leverandører som utfører tjenester på vegne av virksomheten etterlever sikkerhetskrav. Kravene er rettet mot virksomhetene i kraftforsyningen og ikke direkte mot leverandørene.

I 2021 ble NVEs arbeid med oppfølging av IKT-sikkerhet i kraftforsyningen kritisert av Riksrevisjonen /1/. Riksrevisjonen mente blant annet at NVE hadde for lite oversikt over IKT-sikkerheten hos leverandørene til kraftforsyningen og at tilsynet med virksomheter som inngår i kraftforsyningens beredskapsorganisasjon (KBO) og deres oppfølging av egne leverandører var mangelfull. I etterkant har NVE gjennomført flere aktiviteter for å møte utfordringen. Blant annet er veiledningene til kbf oppdatert. NVE har fått utarbeidet en rapport som beskriver sårbarheter, risiko og foreslår et veikart for NVEs oppfølging av IKT-sikkerhet i leverandørkjeden /2/. Det er også gjennomført en leverandørkartlegging av viktige leverandører for kraftforsyningen, inkludert forslag til metodikk for vedlikehold /3/.

For dette oppdraget har NVE behov for å vurdere om dagens krav til leverandørkjedesikkerhet i kbf er dekkende, sett opp mot nye krav som ventes fra europeisk regelverk, spesielt NIS2-direktivet. NIS2-direktivet har en vid utstrekning i typer virksomheter som omfattes, som vil kunne dekker både norske KBO-enheter og leverandører til kraftforsyningen innen IT, OT, og IT-sikkerhetstjenester, når direktivet innføres i norsk rett.

Denne rapporten vurderer nye problemstillinger som følge av et skjerpet europeisk regelverk og økt behov for tettere leverandøroppfølging. gir en vurdering av hvorvidt eksisterende reguleringer er tilpasset disse problemstillingene og beskriver hvordan leverandørene best kan følges opp fra NVE.

3.2 Metode

Datainnsamlingen til denne utredningen er basert på gjennomgang av rapporter, utredninger, høringsdokumenter og lovdokumenter. DNV har også fått tilgang til et tilfeldig og representativt uttrekk av navn på konkrete leverandører til kraftforsyningen fra NVEs leverandøroversikt.

DNV har gjennomført semi-strukturerte intervjuer med tre aktører i kraftforsyningen. Dette er nettselskapet Lnett AS (2. oktober 2024), energi- og infrastrukturkonsernet Hafslund AS (7. oktober 2024), og Nettalliansen AS, som er en samarbeidsorganisasjon for norske nettselskap (8. oktober 2024). Tema for intervjuene var:

- Prosess for kravsettingen mot leverandører om IT/OT-sikkerhet
- Krav og oppfølging for å ivareta IT/OT-sikkerhet i leverandørkjeder
- Bruk av rammeverk og standarder i leverandøravtaler
- NVEs oppfølging og veiledning på området leverandørkjedesikkerhet
- Fordeler/ulemper med strengere myndighetskrav knyttet til leverandøroppfølging
- Fordeler/ulemper med strengere myndighetskrav rettet direkte mot leverandører

På bakgrunn av innsamlede data og DNVs interne kompetanse, har DNV analysert de tre hovedtemaene nevnt i innledningen:

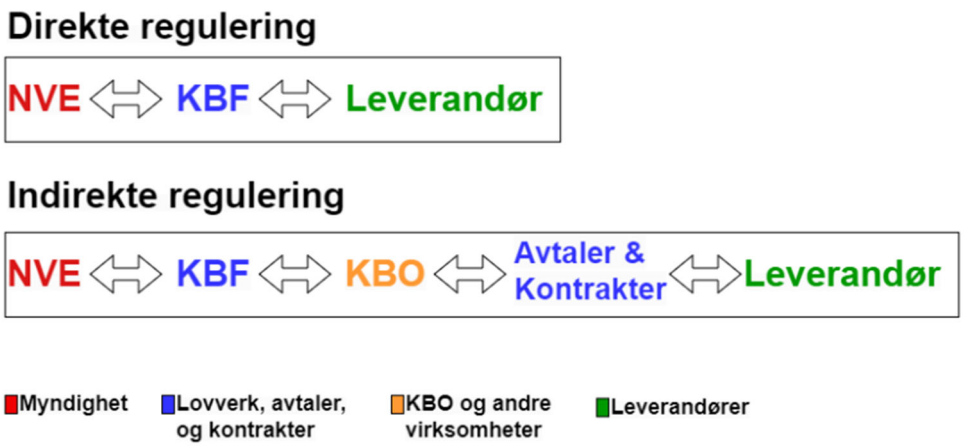
1) Sammenligning av leverandørkjedekrav i kbf, NIS/NIS2-direktivene og CRA
2) Vurdering av hvorvidt leverandører antas å omfattes av NIS2
3) Vurdering av alternative regulatoriske tilnærminger for NVE til å følge opp IT/OT-sikkerhet hos leverandørene.

Når det gjelder det siste hovedtemaet, har DNV definert følgende alternativer:

Nullalternativet: Indirekte regulering med dagens veiledningsinnsats og uten endringer i kbf.

Alternativ A: Indirekte regulering med forsterket leverandøroppfølging med tydeligere regulatoriske krav til KBO-enhetenes oppfølging av sikkerhet i leverandørkjeden.

Alternativ B: Direkte regulering av kritiske leverandører gjennom ny forskriftsbestemmelse i kbf om registreringsplikt for leverandører med sikkerhetskrav.



Figur 1 Struktur for direkte og indirekte regulering av leverandørkjeden

Utredningen av alternativene er bygd opp etter hovedprinsippene i utredningsinstruksen for staten. Det innebærer først en beskrivelse av problemet, og hva som ønskes oppnådd. Deretter defineres og beskrives de alternative tiltakene nærmere, herunder hvilke positive og negative virkninger de har. På bakgrunn av en samlet drøfting gis det en anbefaling om hvilket tiltak som bør gjennomføres. Avslutningsvis peker rapporten på hvordan tiltaket kan gjennomføres og viktige forutsetninger for å lykkes.

3.3 Avgrensinger

Det er gjort følgende avgrensninger i dette arbeidet:

- Utredningen vurderer ikke faktisk sikkerhet og risiko i leverandørkjedene i kraftforsyningen, men fokuserer på hvordan leverandørkjedesikkerhet kan reguleres gjennom en kombinasjon av forskriftskrav og veiledning.
- Regulatoriske forhold knyttet til sikkerhetsloven (f.eks. sikkerhetsgraderte anskaffelser) behandles ikke.
- Intervjuene er begrenset til tre selskaper, som representerer henholdsvis distribusjon/nett, kraftproduksjon og distribusjon, og en samarbeidsorganisasjon for nettselskaper som blant annet jobber med sikkerhet og anskaffelser. Innspillene er brukt for å berike analysen fra ulike perspektiver, men det begrensede antallet intervjuer gjør at innspillene ikke nødvendigvis er representative for bransjen.
- Den sammenlignende analysen av kbf opp mot NIS- og NIS2-direktivene og CRA er overordnet og må vurderes som en foreløpig og innledende analyse. Det samme gjelder vurderingen av hvorvidt leverandører til kraftforsyningen kan ventes å bli omfattet av de nevnte regelverkene. Én utfordring er at prosessene med lovgivning har kommet ulikt og at det derfor er ulik detaljeringsgrad på kravene, noe som skaper til dels stort tolkningsrom.

Vurderingene og anbefalingene i denne rapporten er ikke en juridisk analyse, men er ment å gi NVE innspill til retning for det videre regulatoriske arbeidet med å forbedre leverandørkjedesikkerheten i kraftforsyningen.

4 LEVERANDØRKJEDESIKKERHET: REGELVERK, STANDARDER OG RAMMEVERK

Dette kapittelet beskriver de mest relevante regelverk, standarder og rammeverk som er aktuelle for virksomhetene i kraftforsyningen, og som er generelt anerkjent i industrien for styring av IT/OT-sikkerhet. Herunder beskrives det kort hvordan disse regelverkene, standardene og rammeverkene omtaler leverandørkjedesikkerhet.

4.1 Gjeldende regelverk i kraftforsyningen

Energiloven

Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven) /4/ regulerer hele energisektoren, inkludert elektrisk kraft og fjernvarme. Formålet med loven er å sikre at produksjon, omforming, overføring, omsetning, fordeling og bruk av energi skjer på en samfunnsmessig rasjonell måte. Dette innebærer å ta hensyn til både samfunnsøkonomiske beregninger og andre viktige faktorer som natur og miljø.

Loven legger også til rette for et fritt kraftmarked, hvor elektrisk energi kan kjøpes og selges basert på tilbud og etterspørsel. Den inneholder bestemmelser om leveringsplikt, forbrukerbeskyttelse, og et konsesjonssystem for bygging og drift av kraftanlegg. Loven refererer til informasjonssikkerhet og generelt krav som er relevante for KBO-enheter.

Loven lister opp en rekke relevante forhold som også må ivaretas i leverandørkjeden. Dette inkluderer å sørge for at informasjonssikkerhet ivaretas gjennom kartlegging, avskjerming og beskyttelse av sensitiv informasjon samt vilkår for tilgang til anlegg.

Energilovforskriften

Forskrift om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energilovforskriften) /5/ utfyller energiloven. Forskriften regulerer detaljene rundt hvordan energiproduksjon, -omforming, -overføring, -omsetning, -fordeling og -bruk skal foregå på en samfunnsmessig rasjonell måte.

Forskriften dekker blant annet:

- Krav til konsesjon for bygging og drift av energianlegg.
- Saksbehandlingsregler for konsesjonssøknader.
- Tekniske krav til elektriske anlegg og fjernvarmeanlegg.
- Systemansvar og leveringskvalitet for å sikre stabil og sikker energiforsyning.
- Energiplanlegging for å sikre langsiktig og bærekraftig energiforsyning.

Forskriften bidrar til å sikre at energiforsyningen er pålitelig, effektiv og i tråd med samfunnets behov og miljøhensyn, men har lite krav for sikkerhet utover «å holde anlegget i tilfredsstillende driftssikker stand».

Forskriften lister opp forhold som også må ivaretas i leverandørkjeden. Dette inkluderer å sørge for at personell i virksomheter har kompetanse til å følge opp innhold og utførelse av sine oppgaver dersom disse er satt bort til andre.

Kraftberedskapsforskriften

Forskrift om sikkerhet og beredskap i kraftforsyningen (kbf) /6/ har som mål å sikre at kraftforsyningen opprettholdes og at normal forsyning gjenopprettes på en effektiv og sikker måte under og etter ekstraordinære situasjoner. Målet er å redusere de samfunnsmessige konsekvensene av slike hendelser.

Forskriften gjelder for virksomheter som inngår i kraftforsyningens beredskapsorganisasjon (KBO) og pålegger dem krav og plikter som må oppfylles både i normal drift og i ekstraordinære situasjoner. Dette inkluderer forebyggende sikringstiltak og planlegging av beredskapstiltak.

Forskriften lister opp en rekke relevante forhold som også må ivaretas i leverandørkjeden. Dette inkluderer etterlevelse av bestemmelsene om informasjonssikkerhet og taushetsplikt for kraftsensitiv informasjon i anskaffelse, at

sikkerhetsnivået opprettholdes eller forbedres ved utsetting av tjenester for digitale informasjonssystemer, og lokaliseringskrav for leverandører som har fjerntilgang til bryterfunksjon i avanserte måle- og styringssystemer (AMS), som oppdaterer AMS eller leverer driftskontrollsystemer.

4.2 Relevante standarder, rammeverk og veiledninger

ISO/IEC 27001/2 - Informasjonssikkerhet

ISO/IEC 27001 /7/ er en anerkjent internasjonal standard for informasjonssikkerhet. Standarden beskriver krav for å etablere, gjennomføre, vedlikeholde og kontinuerlig forbedre et ledelsessystem for informasjonssikkerhet. Denne standarden, som setter søkelys på selve ledelsessystemet, utfylles i ISO/IEC 27002 /8/, som beskriver beste praksis for organisatoriske, personellmessige, fysiske og teknologiske sikkerhetstiltak.

ISO/IEC 27002 inkluderer tiltak for å ivareta IKT-sikkerhet i leverandørkjeder. Dette handler om prosesser og prosedyrer for å håndtere leverandørkjederisikoer spesifikt, og å opprettholde nødvendig sikkerhetsnivå gjennom leverandøravtaler både når det gjelder konfidensialitet, integritet og tilgjengelighet.

Standarden lister opp en rekke relevante forhold som må ivaretas gjennom leverandøroppfølgingen. Dette inkluderer å sørge for at sentrale sikkerhetskrav spesifiseres i avtalene og propageres gjennom leverandørkjeden til leverandører og deres kritiske underleverandører. Relevante metoder for å kontrollere leverandørene, inkluderer blant annet rapportering/dokumentasjon, krav om penetrasjonstester, krav om tredjeparts revisjoner, krav om sertifisering osv. Et annet sentralt tema er endringshåndtering og livsløpsvurderinger, herunder tilgang til substitutter og alternativer dersom leverandøren slutter å produsere kritiske produkter og tjenester eller leverandøren selv går konkurs.

ISO/IEC 27002 peker også videre på en rekke andre relevante standarder, for eksempel ISO/IEC 27036-3 som inneholder ytterligere retningslinjer for sikkerhet i leverandørkjeder for maskinvare, programvare og tjenester.

NSM grunnprinsipper for IKT-sikkerhet 2.1

NSMs grunnprinsipper for IKT-sikkerhet 2.1 /9/ omfatter prinsipper og tiltak som skal beskytte IKT-systemer mot uautorisert tilgang, skade eller misbruk. Prinsippene og tiltakene er generelle og tilpasset alle typer virksomheter, og er bygd opp rundt fire pilarer; identifisere og kartlegge, beskytte og opprettholde, oppdage, og håndtere og gjenopprette.

Publikasjonen inneholder et eget kapittel som omhandler tjenesteutsetting, herunder bruk av eksterne skytjenester. Her sier NSM: «*Sikkerhetstiltak er nødvendig, uavhengig av hvem som forvalter tjenestene. NSMs grunnprinsipper for IKT-sikkerhet er like relevante for IKT-tjenester som er tjenesteutsatt som for IKT-tjenester som forvaltes av virksomheten selv. Forskjellen er om man stiller krav til interne eller eksterne tjenesteleverandører.*"

Videre stilles det opp fem forutsetninger som er viktige å ta hensyn til før virksomheter beslutter å tjeneste utsette deler av porteføljen sin: 1) oversikt og kontroll på hele livsløpet, 2) god bestillerkompetanse, 3) gode risikovurderinger for å kunne ta riktig beslutning, 4) riktige og gode krav til IKT-tjenesten og til leverandører, 5) riktig beslutning på riktig nivå.

Et av grunnprinsippene omhandler ivaretakelse av sikkerhet i anskaffelses- og utviklingsprosesser. Blant anbefalte tiltak er å foretrekke IKT-produkter som er sertifiserte og evaluert av en tiltrodd tredjepart, og undersøke sikkerheten hos tjenesteleverandør ved tjenesteutsetting, herunder undersøke om leverandøren har et etablert styringssystem for informasjonssikkerhet og eventuelt sertifisering i henhold til internasjonale standarder, for eksempel ISO/IEC 27001.

Det vises videre til andre relevante nasjonale og internasjonale veiledninger og standarder knyttet til anskaffelser/tjenesteutsetting.

System and Organization Controls 2 (SOC 2)

SOC 2 /10/ er en frivillig rapporteringsstandard fra American Institute of Certified Public Accountants (AICPA) for å vurdere og verifisere sikkerheten hos tjenesteleverandører. Standarden er spesielt relevant for selskaper som håndterer sensitive data for kunder, for eksempel leverandører av skybaserte tjenester, for å dokumentere at de kan håndtere

kundedata på en sikker måte. En SOC 2-rapport kan dekke fem områder; sikkerhet (det overordnede rammeverket), tilgjengelighet, konfidensialitet, personvern og integritet.

Det finnes to typer SOC 2-rapporter:

- Type 1 gir et øyeblikksbilde av kontrollene som er på plass på et spesifikt tidspunkt.
- Type 2 er mer omfattende og vurderer både design og effektivitet av kontrollene over en spesifisert periode.

Rapportene utstedes av tredjeparts revisjonsfirmaer. SOC 2-rapporter er vanlig å etterspørre for eksempel ved anskaffelse av skytjenester.

Veiledninger utarbeidet av NVE og Forum for informasjonssikkerhet i kraftforsyningen (FSK)

NVEs veileder til kbf /11/ forklarer mer detaljert hvem som er omfattet av kbf, og gir råd om hvordan de kan etterleve kravene. Veiledningen spesifiserer hvordan KBO-enhetene bør følge opp underleverandørene iht. kbf kravene ved å presisere noen av kravene, gi eksempler, forslå maler (for eksempel mal om informasjonssikkerhetsavtale for håndtering og beskyttelse av kraftsensitiv informasjon), og henvise til relevante standarder og rammeverk.

Veileder for sikkerhet i anskaffelser og leverandørkjeder (august 2023) /12/ er utarbeidet av Forum for informasjonssikkerhet i kraftforsyningen (FSK). Formålet er å hjelpe virksomhetene i kraftforsyningen med å gjennomføre anskaffelser av IKT-relaterte produkter eller tjenester på en måte som gjør at sikkerhetsnivået i virksomhetene, og dermed også potensielt innen kraftforsyningen, ikke påvirkes negativt. Veiledningen gir råd på hvordan innkjøpsprosess av IKT-produkter og tjenester for KBO-enheter best mulig kan ivareta overordnet mål og krav om forsvarlig cybersikkerhet ved utsetting av tjenester eller innkjøp av produkter. Blant annet gir veilederen anbefalinger som gjelder cybersikkerhetskrav i innkjøp og i evaluering av tilbudene, og hvordan kravene følges opp gjennom leveransens livssyklus.

Sikkerhetsveileder for kraftsensitiv informasjon i skytjenester (november 2021) /13/ er også utarbeidet av FSK. Formålet er å hjelpe virksomhetene til å gjøre grundige vurderinger av skyløsninger som skal behandle kraftsensitiv informasjon, slik at informasjonen er tilstrekkelig sikret i henhold til virksomhetens eget behov for informasjonssikkerhet, og i tråd med myndighetskrav for lagring, transport og behandling av kraftsensitiv informasjon. Veilederen vektlegger viktigheten i å følge opp sikkerhetskrav gjennom leveransens livssyklus, og det er utarbeidet et forslag til kravliste til skyleverandørene.

IEC 62443 – Cybersikkerhet i OT

IEC 62443 /14/ er en serie internasjonale standarder som adresserer cybersikkerhet for operasjonell teknologi (OT) i automatiserings- og kontrollsystemer. Disse standardene dekker både tekniske og prosessrelaterte aspekter av cybersikkerhet for industrielle automasjons- og kontrollsystemer (IACS) gjennom hele deres livssyklus.

IEC 62443 er delt inn i fire hoveddeler:

1. Generelle emner: Terminologi, konsepter og modeller.
2. Retningslinjer og prosedyrer: Metoder og prosesser knyttet til IACS-sikkerhet.
3. Systemkrav: Krav på systemnivå, inkludert sikkerhetsteknologier og risikovurdering.
4. Komponent- og produktkrav: Krav til utvikling og sikkerhet for IACS-komponenter.

Disse standardene bidrar til å identifisere, beskytte, oppdage og respondere på cybersikkerhetstrusler samt gjenopprette systemer og funksjoner etter hendelser.

IEC 62443-2-4 stiller noe krav til sikkerhetsstyringssystemer, risikovurdering, og sikkerhetskontroller som tjenesteleverandører må implementere med blant annet kompetanse for personell og verifikasjon av leveransen.

IEC 62443-3-3 dekker tekniske sikkerhetskrav som tilgangskontroll, autentisering, kryptering, og inntrengingsdeteksjon. Disse kravene bør iverksettes av leverandøren for å kunne oppnå bestillerens definerte sikkerhetsmål.

IEC 62443-4-1 beskriver kravene til sikkerhet gjennom hele produktets livssyklus, fra utvikling til avhending. Disse kravene kan bli pålagt av bestilleren eller selv pålagt av leverandøren som interne krav.

IEC 62443-4-2 omfatter sikkerhetskrav for individuelle komponenter i industrielle kontrollsystemer, inkludert sikker design og utvikling. Disse kravene kan bli pålagt av bestilleren eller selv pålagt av leverandøren som interne krav.

NIST Cybersecurity Framework 2.0 (CSF)

NIST Cybersecurity Framework (CSF) /15/ er et rammeverk utviklet av det amerikanske National Institute of Standards and Technology (NIST) for å hjelpe organisasjoner med å redusere og håndtere cybersikkerhetsrisikoer. Rammeverket er anerkjent internasjonalt og iverksatt på tvers av ulike bransjer, inkludert offentlig sektor og privat næringsliv.

Den nyeste versjonen av rammeverket, CSF 2.0, ble publisert i 2024. Den oppdaterte versjonen har en endret struktur blant annet ved å introdusere og vektlegge styring/ledelse («govern») som en egen pilar, i tillegg til de opprinnelige pilarene, som man også kjenner igjen fra NSMs grunnprinsipper for IKT-sikkerhet, nemlig å identifisere, beskytte, oppdage, håndtere og gjenopprette.

Leverandørkjedesikkerhet er også et område som er forsterket i CSF 2.0. Innenfor pilaren styring/ledelse er det etablert en egen hovedkategori som omhandler styring av leverandørkjederisiko. Et viktig mål er at leverandørkjederisiko skal bli en integrert del av virksomhetens øvrige risikostyringssystem, og følges opp gjennom hele livsløpet til leveransen.

NIST definerer følgende krav for å styrke leverandørkjedesikkerhet: retningslinjer for leverandørkjedesikkerhet for virksomheten, integrert leverandørkjedesikkerhet risikohåndtering, krav som muliggjør iverksetting av tiltak for å redusere risikoer i leverandørkjeden er lagt i avtaler, oppfølging og overvåking av leveranser gjennom hele livssyklusen, og plan ved utfasing av produktet eller tjenesten.

4.3 Kommende regulering

NIS-direktivet og norsk implementering gjennom digitalsikkerhetsloven og -forskriften

Lov om digital sikkerhet (digitalsikkerhetsloven) /16/, som innfører NIS-direktivet i norsk rett, ble vedtatt i desember 2023, men har enda ikke trådt i kraft. Loven har som mål å styrke digital sikkerhet for tilbydere av samfunnsviktige tjenester og digitale tjenester. I september 2024 ble forslag til forskrift til digitalsikkerhetsloven (digitalsikkerhetsforskriften) sendt på høring /17/. Forskriften presiserer og konkretiserer kravene i loven, og forslaget er på høring frem til desember 2024.

Leverandørkjedesikkerhet omtales flere steder i høringsforslaget, blant annet er det foreslått en egen bestemmelse om oppfølgingsplikt av leverandører og andre som utfører arbeid på vegne av virksomheten. Det påpekes at leverandørkjederisikoen er økende, og at virksomhetene må forvente å bruke mer ressurser på oppfølging av leverandører.

NIS2-direktivet

NIS2-direktivet /18/ fra 2022 erstatter NIS-direktivet fra 2016 og introduserer flere nye krav og tiltak for å møte dagens økende digitale trusler. NIS2 trådte i kraft 16. januar 2023, og medlemslandene hadde frist til 17. oktober 2024 for å implementere direktivet i nasjonal rett. For Norges del er NIS2-direktivet foreløpig vurdert å være EØS-relevant. NIS2 omtales også i høringen til digitalsikkerhetsforskriften, hvor det påpekes at det blir behov for revisjon av digitalsikkerhetsloven og -forskriften, eller regulering i annen lov, dersom NIS2-direktivet tas inn i EØS-avtalen. Merk at i forslaget til digitalsikkerhetsforskrift

NIS2-direktivet legger stor vekt på å styrke sikkerheten i leverandørkjeder. Leverandørkjederisiko skal inngå i virksomhetenes risikovurderinger, og det skal gjennomføres tiltak for å håndtere denne risikoen. På europeisk nivå legges det opp til tett samarbeid mellom EU-kommisjonen og EUs cybersikkerhetsbyrå (ENISA) i å utføre koordinerte risikovurderinger knyttet til kritiske leverandørkjeder.

EU-kommisjonen har også vedtatt 17. oktober 2024 en første gjennomføringsrettsakt («implementing regulation») knyttet til NIS2 /19/. Denne presiserer spesifikt varslingskrav for sektorer som digital infrastruktur, IT-tjenester, og digitale tjenester. I kapittel 5 i gjennomføringsrettsaktens vedlegg er det imidlertid også oppstilt nærmere spesifikasjoner til NIS2-direktivets artikkel 21 nummer 2 bokstav d, som omhandler leverandørkjedesikkerhet, som gir føringer for hvordan denne bestemmelsen bør iverksettes.

Hvert land står forholdsvis fritt til hvordan de gjennomfører NIS2-direktivet i nasjonalt regelverk, herunder hvordan de iverksetter leverandørkjedekrav. Et overordnet søk per 14. oktober 2024 indikerer følgende (basert på ulike nettbaserte kilder fra hvert enkelt land), og viser at det er stort sprik i tilnærming og generelt forsinkelser når det gjelder operasjonalisering innen fristen:

- Belgia: Ingen utvidede leverandørkjedekrav i gjeldende lovverket, forskrift er under arbeid.
- Finland: Ingen utvidede krav, men presiserer at leverandørkjedesikkerhet innebærer å kartlegge, forstå avhengigheter, sårbarheter, trusler, og konsekvenser om risiko blir til hendelser. Finsk regelverk, presenterer konkrete eksempler på leverandørkjedeangrep samt tar høyde for leverandørkjedesikkerhet i sin kostnadskalkulator som kvantifiserer kostnader knyttet til NIS2 etterlevelse.
- Polen: Ingen utvidede krav relatert til leverandørkjedesikkerhet.
- Tsjekkia: Gjeldende lov setter krav om identifisering og evaluering av avhengigheter til leverandører i vesentlig tjenester leveranser. Det er også nødvendig å innføre tiltak ved for høyt sårbarhetsnivå og krav til rapportering til myndighetene.
- Tyskland: Tyskland definerer tilleggskrav som gjelder leverandørkjedesikkerhet. Blant annet, er det krav om å utarbeide retningslinjer for leverandørkjedesikkerhet, gjennomføre risikovurdering, definere kriteria for evaluering og valg av leverandører. Evne til etterlevelse av sikkerhetskrav skal vurderes i innkjøpsfasen. Avtaler med leverandører bør inkluderer sikkerhetskrav hvorav etterlevelse skal følges opp. Virksomheter bør utarbeide og vedlikeholde oversikt over kontaktpunkter hos leverandører av tjenester.
- Ungarn: Gjeldende lovverket innfører krav om sertifisering. Et ungarsk sertifiseringsregime er innført som legger vekt på –relevant for leverandørkjeden – oppdatert programvare og maskinvare uten kjente sårbarheter, og med muligheter for sikker oppdatering.

Cyber Resilience Act (CRA)

Cyber Resilience Act (CRA) /20/, er en EU-forordning om horisontale cybersikkerhetskrav for digitalt utstyr. Forordningen ble vedtatt av ministerrådet 10. oktober 2024, men er per 22. oktober 2024 enda ikke formelt godkjent og publisert i EU-tidende. Forordningen er heller ikke innlemmet EØS-avtalen. Norges foreløpige vurdering er at forordningen er EØS-relevant, noe som innebærer at den kan forventes innført i Norge.

CRA har som mål å styrke cybersikkerheten ved å sette felles standarder i EU for produkter med digitale elementer som er direkte eller indirekte koblet til en enhet eller et nettverk, inkludert maskinvare, programvare og tilhørende tjenester (typisk IoT-produkter). Produkter spenner alt fra leketøy til brannmurer og nettverksrutere.

Produsenter må implementere cybersikkerhetstiltak som dekker hele livsløpet til produktet, fra design, til utvikling, vedlikehold og oppdateringer. Produkter som overholder CRA vil bære CE-merking, noe som indikerer at de oppfyller cybersikkerhetskravene.

Ettersom CRA er et produktsikkerhetsregelverk, vil det i hovedsak treffe aktører i leverandørkjeden til KBO-enhetene som er omfattet av kraftberedskapsforskriften, og ikke KBO-enhetene selv. Dette i motsetning til NIS2 som omfatter virksomheter som kan være både KBO-enheter og deres IT, OT og IT-sikkerhetsleverandører.

Network Code on Cybersecurity (NCCS)

«The Network Code on Cybersecurity» (NCCS) /21/ er en delegert kommisjonsforordning vedtatt 11. mars 2024 som utfyller forordning (EU) 2019/943 (elektrisitetsforordningen) som etablere sektorspesifikke regler for cybersikkerhetsaspekter for virksomheter som driver med grensekryssende elektrisitetsstrømmer.

Forordningen er relevant for virksomheter i kraftsektoren som har rolle i å utveksle strøm over landegrensene innad i EU. Det er ikke gjort en vurdering av om forordningen er EØS-relevant, og den gjelder derfor foreløpig ikke i Norge, men kan bli brukt for inspirasjon for bransjen.

Formålet med forordningen er å fastsette felles regler for utførelse av cybersikkerhetsrisikovurderinger, fremme et felles rammeverk for cybersikkerhet på tvers av EU, samt etablere informasjonsflyt og rapporteringsmekanismer for sårbarheter og cyberangrep.

NCCS omfatter regler for cyberrisikovurdering, felles minimumskrav, cybersikkerhetssertifisering av produkter og tjenester, samt overvåking, rapportering og krisehåndtering. Flere bestemmelser omhandler leverandørkjedesikkerhet. Dette gjelder blant annet spesifikke leverandørkjedeaspekter som skal inkluderes i risikovurderingene. Det skal defineres cybersikkerhetskrav ved innkjøp, og det skal verifiseres at leveranser innfrir sikkerhetskravene gjennom hele leveransens livssyklus. Kritiske virksomheter kan få tilleggskrav, som sertifisering av leverandørers produkter eller tjenester, for å sikre at de oppfyller nødvendige standarder. Det er også krav rundt diversifisering av leverandører.

5 SAMMENLIGNING AV KBF OG NYE EUROPEISKE REGULERINGER OG KONSEVENSER FOR LEVERANDØRER I KRAFTFORSYNINGEN

Kapittel 5.1 oppsummerer først en overordnet sammenligning av krav relatert til leverandørkjedesikkerhet i kbf opp mot NIS, NIS2 og CRA. Hensikten er å identifisere potensielle gap mellom omfanget av leverandørkjedekrav i kbf opp mot de som forventes å bli implementert i norsk regelverk som følge av de nevnte EU-regelverkene. Videre oppsummerer kapittel 5.2 en overordnet analyse av om dagens leverandører til kraftforsyningen kan ventes å i fremtiden bli omfattet av nasjonale krav etter henholdsvis NIS, NIS2 og CRA, ut fra kriteriene som oppstilles i disse regelverkene.

5.1 Leverandørkjedesikkerhet i kbf og i europeiske reguleringer

Vedlegg A inneholder en nærmere vurdering av egenskaper og krav ved de ulike reguleringene, og hvordan de skiller seg fra hverandre. Dette omfatter blant annet formålet med reguleringen, reguleringens omfang, og ulike kategorier sikkerhetskrav. Vedlegget omhandler derfor mer enn bare leverandørkjedekrav, ettersom DNV anser det som viktig å se selve leverandørkjedekravene i en bredere kontekst. Merk at sammenligningen er overordnet og må vurderes som en foreløpig og innledende analyse. Merk også at regelverkene tjener til dels ulike formål, jf. vedlegg A, og derfor ikke kan sammenlignes direkte. CRA er et produktsikkerhetsregelverk, NIS2 er sektorovergripende regelverk for nettverks- og informasjonssikkerhet, mens kbf er en sektorspesifikk sikkerhets- og beredskapsregulering.

Ut fra sammenstillingen av de gjeldende kravene i kbf opp mot NIS/NIS2-direktivene og CRA, har DNV identifisert følgende områder hvor kbf vurderes å ikke ha krav eller ha mindre omfattende krav mot leverandør eller leverandørkjeden enn det som ventes å komme i nasjonalt regelverk som følge av NIS/NIS2-direktivene og CRA.

Varslingskrav:

- NIS2/CRA krever varsling ved oppdagelse av sårbarheter i egen virksomhet eller i virksomhetens leverandørkjede, i tillegg til ved hendelser.
- Kbf krever at KBO-enheter varsler ved ekstraordinære hendelser. Det er uklart om varslingskrav gjelder for andre virksomheter omfattet av kbf, og forholdet til varsling fra virksomhetens leverandørkjeder. Varsling ved avdekkede sårbarheter omhandles ikke.

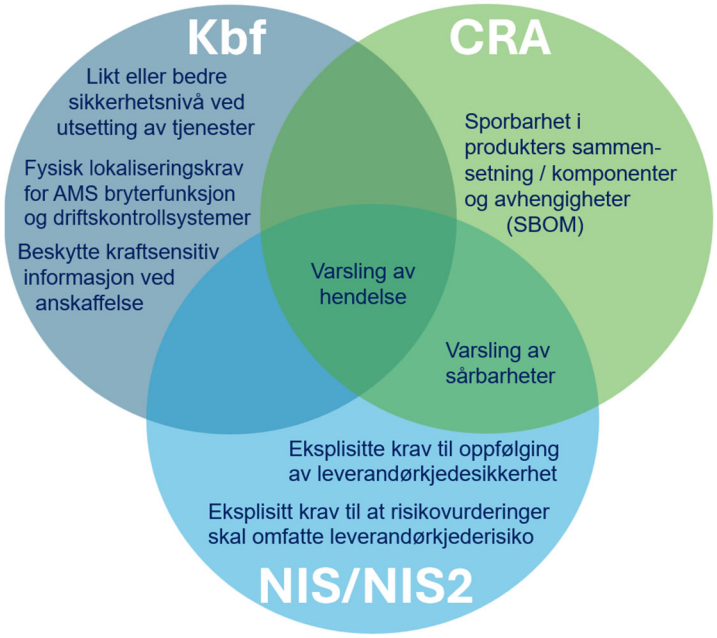
Leverandørkjedesikkerhet:

- NIS/NIS2 har eksplisitte krav til at risikovurderinger skal omfatte risiko knyttet til leverandørkjeder. Se for eksempel NIS2 artikkel 21 punkt 3. Virksomhetene er her pliktige til å ta hensyn til sårbarheter spesifikt for sine direkte leverandører, og deres underleverandører. Det er også krav om at koordinerte risikovurderinger av leverandørkjeder som er gjennomført av «NIS Cooperation Group» skal hensyntas når de finnes (jf. NIS2 artikkel 22). Ut fra dette må virksomhetene treffe tiltak spesifikt for å ivareta leverandørkjedesikkerhet (jf. NIS2 artikkel 21 punkt 2 bokstav d).
- I kbf er leverandørkjedesikkerhet i hovedsak et implisitt hensyn i sikkerhetskravene. Det omtales også spesifikt i noen tilfeller: Dette er plikt om landtilhørighet for leverandører til AMS (jf. § 6-10) og driftskontrollssystemer (jf. § 7-14 bokstav k), plikt til å ivareta informasjonssikkerhet og taushetsplikt for kraftsensitiv informasjon i anskaffelser (jf. § 6-5), og presisering at sikkerhetsnivået i digitale informasjonssystemer skal opprettholdes eller forbedres ved utsetting av tjenester (§ 6-9 tredje ledd bokstav e).[1]

Sporbarhet i leverandørkjeden:

- CRA krever sporbarhet i produkters sammensetning/komponenter og avhengigheter. Blant annet stilles det krav om at leverandøren skal dokumentere digitale komponenter i produktet gjennom en «Software Bill of Materials» (SBOM), som er en detaljert oversikt over programvarekomponenter inkludert avhengigheter til tredjepartskomponenter.
- Kbf eller NIS/NIS2-direktivene har ikke sporbarhetskrav av komponenter på samme nivå som CRA.

[1] NVE gav i oktober 2024 innspill til Energidepartementet om forvaltningsregime for kraftforsyningssikkerhet til havs (havvind) /22/. Der peker de blant annet på at mange vindkraftselskaper i Norge har utenlandske driftssentraler, og at dette kan utgjøre en sårbarhet som må utredes også i forhold til krav til kraftforsyningssikkerhet til havs.



Figur 2 Illustrasjon av krav til leverandørkjedesikkerhet fra tre regelverk

Figur 2 illustrerer likhetene og forskjellene mellom de nevnte regelverkene. Som vist inneholder NIS2-direktivet og CRA krav knyttet til leverandørkjedesikkerhet som er mer utfyllende enn kbf. Blant annet setter NIS2-direktivet opp mer spesifikke krav til at leverandørkjederisiko skal inngå i risikovurderingene til virksomheten. På samme måte har kbf sektorspesifikke krav til leverandørkjedesikkerhet som ikke finnes i de andre regelverkene, f.eks. leverandørers håndtering av kraftsensitiv informasjon og lokaliseringskrav for leverandører av AMS.

I den grad aktørene i leverandørene til kraftforsyningen i fremtiden blir direkte underlagt sikkerhetskrav etter NIS2-direktivet og eventuelt CRA (typisk vil også produktleverandørene til kraftforsyningens leverandører bli underlagt CRA), så vil dette generelt styrke sikkerheten i leverandørkjedene og kunne bidra til å forenkle/standardisere KBO-enhetenes egen oppfølging av leverandørkjedesikkerhet.

5.2 Vurdering av kraftforsyningens leverandører opp mot NIS/NIS2

DNV har gjort en overordnet analyse av om dagens leverandører til kraftforsyningen kan ventes å i fremtiden bli omfattet av nasjonale krav etter henholdsvis NIS-direktivet (med utgangspunkt i høringsforslaget til digitalsikkerhetsforskriften) og NIS2-direktivet, ut fra kriteriene som oppstilles i disse regelverkene. CRA er ikke omfattet av vurderingen.

Det finnes fire alternativer for at en aktør i verdikjeden til kraftforsyningen i Norge kan bli underlagt sikkerhetskrav i norsk regulering som implementerer NIS/NIS2-direktivene:

- Sektortilhørighet og størrelse: Virksomheten opererer innenfor en av de sektorene som er definert som kritiske under NIS- og NIS2-direktivene. Dette inkluderer blant annet energi og digital infrastruktur.
- Type tjeneste: Tjenestene som leveres er essensielle for samfunnet.
- Utvidet nasjonal regulering: Nasjonalt regelverk som gjennomfører NIS- og NIS2-direktivene i Norge kan pålegge ytterligere sektorer eller navngitte virksomheter å bli omfattet av kravene i regelverket.
- Leverandørkjedetilhørighet: Leverandør til en virksomhet som er underlagt NIS og NIS2, kan indirekte bli påvirket av kravene gjennom avtaler, dersom leverandøren eller underleverandøren leverer tjenester eller produkter som er kritiske for å opprettholde kritiske samfunnsmessige eller økonomiske aktiviteter.

Med utgangspunkt i et representativt uttrekk av leverandørnavn fra NVEs leverandøroversikt til kraftforsyningen, har DNV gjort vurdert virksomhetene opp mot vilkårene for å bli underlagt digitalsikkerhetsloven/-forskriften (NIS-direktivet) og NIS2-direktivet. Merk at denne vurderingen er basert på en overordnet vurdering og offentlige opplysninger om virksomheten som størrelse og omsetning, og angir på ingen måte noe fasit. Det er enten virksomhetene selv som skal vurdere om de tilfredsstiller vilkårene for å bli underlagt lovverkene, eller de pekes ut av myndighetene. Vurderingen gir likevel en pekepinn på antatt omfang av leverandører som underlegges nye krav. En anonymisert oversikt over leverandørvurderingene finnes i vedlegg B, og omfatter leverandører av IT, OT og IT-sikkerhetstjenester («managed service providers»).

Omfang

Basert på vurdering av et tilfeldig og representativt utvalg av leverandører til KBO-enheter, er det grunn til å anta at de fleste leverandører blir underlagt NIS2-direktivet, enten som vesentlige eller viktige virksomheter. Merk at flere leverandører blir underlagt NIS2-direktivet enn NIS-direktivet, som har et snevrere omfang. Kun de minste virksomhetene (mindre enn 50 ansatte eller 100 MNOK i omsetning) blir ikke regulert av NIS2-direktivet.

Merk at noen leverandører av digitale tjenester sammen med produsenter innenfor definisjon i NIS2-direktivet kan samtidig ha en dobbeltrolle som både vesentlig/viktig enhet og produkt-/tjenesteleverandør. Et eksempel er kontrollsystemleverandører som leverer maskinvarer, programvarer og tjenester.

Problemstillinger

Under listes noen aktuelle problemstillinger som kan oppstå i utpeking og regulering av leverandører og forholdet til overlappende regelverk.

- Hvem fører tilsyn? Hvem er sektormyndighet? Hvem skal varsles og koordinere ved hendelse? For eksempel fremkommer det i høring til digitalsikkerhetsforskriften: «Departementet foreslår at KBO-enheter, jf. kbf § 2-1 andre ledd og virksomheter som helt eller delvis er underlagt kbf etter samme forskrift § 1-3 andre ledd, blir underlagt digitalsikkerhetsloven gjennom forslag til forskriften § 1 første ledd nr. 1 og nr. 2.».
- Når en leverandør tilbyr både ren programvare og skytjenester, kan det oppstå usikkerhet om hvilke deler av virksomheten som må overholde krav etter NIS2. Dette kan føre til inkonsistent implementering av sikkerhetstiltak og varierende grad av samsvar.
- Når en leverandør tilbyr både ren programvare og skytjenester, kan det oppstå forvirring om hvilke deler av virksomheten som må overholde kravene i NIS2. For eksempel, hvordan vil Microsoft klassifiseres om KBO-enheter kun bruker programvare som Office, versus i form av integrerte løsninger basert på skyplattformen Azure? Er det mulig å klassifisere leverandører som bare delvis faller innenfor definisjonene, uten å vite hvilke tjenester eller produkter KBO-enheter faktisk har i bruk?
- Samme problemstilling oppstår når størrelsen avgjør om virksomheten er «vesentlig» eller «viktig», hvilken deler av virksomheten teller?

6 ALTERNATIVE FREMTIDIGE REGULERINGSMETODER

Dette kapittelet definerer og drøfter tilnærminger for hvordan NVE kan stille regulatoriske krav og følge opp sikkerheten i IT/OT-leverandørkjeder i kraftforsyningen.

Målsetningen er å;

1) styrke KBO-enhetenes sikkerhet ved hjelp av krav og oppfølging av egne leverandørkjeder, og
2) styrke NVEs oversikt og kontroll med sikkerhetstilstand og risiko i leverandørmarkedet for kraftforsyningen.

Én hovedtilnærming er, som i dagens regulatoriske regime, at sikkerhetskrav rettes utelukkende mot KBO-enhetene i kbf, som da selv må sikre å ivareta disse kravene gjennom avtaler med sine underleverandører. Leverandørleddet reguleres da indirekte gjennom disse avtalene. En annen hovedtilnærming er at NVE, gjennom kbf eller annet relevant regelverk, (også) kan stille direkte krav til leverandører i kraftforsyningen, og dermed følge opp sikkerhet i leverandørleddet direkte.

Med utgangspunkt i disse tilnærmingene har DNV oppstilt tre aktuelle alternativer som defineres ut og drøftes i det videre:

- **Nullalternativet – indirekte regulering med dagens veiledningsinnsats**. Alternativet innebærer at det ikke gjøres noen endringer i kbf, og at veiledningen knyttet til leverandørkjedesikkerhet videreføres som i dag. Ved iverksettelse av fremtidig regulering som bl.a. lov og digital sikkerhet med tilhørende forskrift, og ny regulering som følge av NIS2, videreføres dagens veiledningspraksis tilsvarende.
- **Alternativ A – indirekte regulering med forsterket leverandøroppfølging**. Alternativet innebærer fortsatt indirekte regulering av leverandører, men med tydeligere regulatoriske krav til KBO-enhetenes oppfølging av sikkerhet i leverandørkjeden, samt at NVE gjør tiltak som sikrer økt oversikt over kraftforsyningens leverandørkjeder og kontroll med leverandørkjederisiko.
- **Alternativ B – direkte regulering av kritiske leverandører.** Alternativet innebærer at det etableres regulatoriske krav i kbf som rettes direkte mot kritiske aktører som inngår i kraftforsyningens leverandørkjede. NVE får da virkemidler for å ha oversikt over, og kunne følge opp sikkerheten til, leverandørene direkte.

Merk at selv om vi har valgt å drøfte alternativene individuelt, så betyr ikke det at for eksempel alternativ A og B er gjensidig utelukkende. Selv om det kommer på plass krav rettet direkte mot leverandørleddet, så kan det fortsatt være relevant å styrke KBO-enhetenes krav til å følge opp egne underleverandører.

Drøftingen av alternativene tar utgangspunkt i følgende struktur:

- En nærmere beskrivelse av alternativet i form av aktuelle regulatoriske krav og relevant oppfølgingsmodell (tilsyn og veiledning).
- En vurdering av hvor fremtidssikkert/tilpasset alternativet er i forhold til kommende reguleringer, som NIS/NIS2.
- En overordnet drøfting av nyttevirkninger/formålseffektivitet opp mot kostnader for NVE, KBO-enhetene og leverandørene.
- Avslutningsvis oppsummeres alternativet, opp mot effekter og prinsipielle spørsmål.

6.1 Nullalternativet: Indirekte regulering med dagens veiledningsinnsats

Beskrivelse

Nullalternativet innebærer en videreføring av dagens praksis, som i hovedsak består av veiledning om leverandøroppfølging med utgangspunkt i de gjeldende kravene i kbf.

De relevante kravene knyttet til leverandørkjeder er i hovedsak begrenset til kbfs kapittel 6 om informasjonssikkerhet. Bestemmelsene §§ 6-5 og 6-6 omhandler konfidensialitet og håndtering av kraftsensitiv og sikkerhetsgradert

informasjon ved anskaffelser. Bestemmelsen § 6-9 setter krav til både konfidensialitet, integritet og tilgjengelighet i virksomhetenes digitale informasjonssystemer. Her er det § 6-9 tredje ledd bokstav e, som er særlig relevant for leverandøroppfølging da det presiseres at sikkerhetsnivået skal opprettholdes eller forbedres ved utsetting av tjenester. I § 6-10 stilles det krav til nettselskap om begrensninger av funksjonalitet for leverandører av AMS, og i § 7-14 stilles det krav vil virksomheter om at utenlandske leverandører av driftskontrollsystem klasse 2 må være EFTA-, EU- eller NATO-land.

De gjeldene kravene i §§ 6-5 og 6-6 er rettet mot KBO-enheter, mens § 6-9 gjelder virksomheter (det vil si KBO-enheter og eventuelt andre som er underlagt forskriftens krav etter vedtak). Underleverandørene reguleres derfor indirekte gjennom avtalene med virksomhetene.

Gjeldende veiledning til de aktuelle bestemmelsene i kbf spesifiserer hvordan KBO-enhetene bør følge opp underleverandørene. Veiledningen inneholder presiseringer av kravene, eksempler, maler (for eksempel mal om informasjonssikkerhetsavtale for håndtering og beskyttelse av kraftsensitiv informasjon), og henvisning til relevante standarder og rammeverk. I tillegg har NVE fått utarbeidet og publisert flere rapporter om leverandørkjedesikkerhet som gir ytterligere underlag (se også /2/ og /3/).

Innenfor nullalternativet vil NVE fortløpende kunne videreutvikle og forbedre veiledningsmaterialet overfor KBO-enhetene. Dette kan være spesifikk veiledning som gir KBO-enhetene en rettesnor for hvordan de skal oppfylle de spesifikke kravene knyttet til leverandøroppfølging. Denne veiledningen vil da også være retningsgivende for NVEs vurderinger av etterlevelse når de gjennomfører tilsyn.

Veiledningen kan også være mer generell og peke på beste praksis for sikkerhet i leverandørkjeder, for eksempel gjennom temarapporter eller henvisning til rammeverk og standarder, uten at dette er konkret knyttet til oppfyllelse av spesifikke bestemmelser. Slik generell veiledning vil være nyttig for bevisstgjøring og kompetanseheving hos KBO-enhetene, men mindre egnet som direkte rettesnor for etterlevelse og grunnlag for tilsyn.

Forholdet til fremtidig regulering

Prinsippet om at spesielle lover går foran generelle lover («lex specialis»), gjør at sektorkravene i kbf vil ha forrang fremfor digitalsikkerhetsloven og digitalsikkerhetsforskriften, når disse trer i kraft, dersom de regulerer det samme. Det samme vil gjelde for fremtidige regulering etter NIS2-direktivet, dersom direktivets krav implementeres i norsk rett etter samme prinsipp som digitalsikkerhetsloven.

Imidlertid viser gjennomgangen i kapittel 5.1. at enkelte krav i NIS/NIS2 knyttet til leverandørkjedesikkerhet, kan tolkes som strengere enn kravene i kbf. I den grad de nye kravene blir gjeldende for KBO-enheter, så kan det innebære at de må etterleve krav om leverandørkjedesikkerhet i flere regelverk samtidig. Dette trenger ikke å innebære noen konflikt. Regelverkene kan leve side om side. Samtidig vil det kunne være mer kompliserende enn om alle relevante sikkerhetskrav var samlet i kbf.

Likevel kan det oppstå potensielle konflikter. For eksempel er formålet med de ulike regelverkene forskjellige. Mens kbfs formål først og fremst er å opprettholde kraftforsyningen i enhver situasjon, er digitalsikkerhetslovens formål å forebygge, avdekke og motvirke uønskede hendelser i nettverks- og informasjonssystemer. Kbfs formål vektlegger derfor tilgjengeligheten til kraftforsyningen tydelig, mens digitalsikkerhetsforskriftens formål dekker både tilgjengelighet, autentisitet, integritet og tillit til data og tjenester. Dette kan gjøre at KBO-enhetenes risikovurderinger og egnede sikkerhetstiltak kan komme i konflikt, ut fra hvilket regelverk de skal sikre etterlevelse etter.

Fra oversikten i kapittel 8 Vedlegg A kan det tyde på at regulatoriske krav etter NIS, NIS2 eller CRA vil treffe mange av leverandørene i kraftforsyningen direkte. Disse kravene vil kunne leve side om side med gjeldende krav til KBO-enhetene i kbf. Et sentralt spørsmål er da hvilke myndigheter som vil få tilsynsansvar for å følge opp kravene overfor leverandørene. Dersom det er snakk om leverandører som leverer generiske IT-, OT eller IT-sikkerhetstjenester innenfor mange ulike sektorer, kan det være mer naturlig at tilsynsansvaret legges til en nasjonal myndighet som NSM, heller enn sektormyndighet som NVE. Selv om leverandørenes sikkerhet da blir fulgt direkte opp av en nasjonal

myndighet, gir det nødvendigvis ikke NVE en større innflytelse og evne enn i dag til å følge opp leverandørmarkedet opp mot særegenhetene i kraftforsyningen spesifikt.

Tabell 1 Kost- og nyttevurdering for Nullalternativet

NVE	
+	Alternativet innebærer i utgangspunktet ikke nye tiltak eller økonomiske/administrative kostnader for NVE. NVE viderefører veiledningspraksis på dagens nivå. Når nye reguleringer kommer på plass, for eksempel digitalsikkerhetsloven, så tilpasser NVE veiledningen tilsvarende.
+	Ansvarsplassering angående underleverandører er tydelig. Ansvaret ligger hos KBO-enheten, også der dette er satt ut til underleverandører.
-	Det identifiserte behovet for å gjennomføre tiltak for å styrke leverandøroppfølgingen blir bare i begrenset grad fulgt opp, da det gjennomføres innenfor dagens regulering og veiledningsrammer. NVE må vente til oppdaterte krav til KBO-enheter og ev. underleverandører kommer på plass i NIS og NIS2-reguleringen. Særlig iverksetting av NIS2 kan fortsatt ta flere år.
-	Når nytt regelverk er på plass er det sannsynlig at NVE må utarbeide veiledning og drive tilsyn etter flere regelverk (kbf og lover som iverksetter NIS/NIS2). Dette kan gjøre veiledningsprosessen mer krevende, særlig dersom det oppstår usikkerhet rundt hvilke bestemmelser som skal gjelde i hvilket regelverk, og hvordan de skal tolkes dersom det oppstår motstrid.
-	For NVE vil det fortsatt forbli ressurskrevende å holde ved like oversikt over leverandørmarkedet, og risikobildet knyttet til leverandørkjeder.
KBO-enhetene	
+	Ansvarsplassering er tydelig. Ansvaret for etterlevelse av kravene i kbf ligger hos KBO-enheten, og det er KBO-enhetenes ansvar å ivareta disse også ved tjenesteutsetting.
+	Gjeldende krav til leverandøroppfølging er overordnet, noe som bidrar til fleksibilitet for KBO-enhetene om hvordan de vil iverksette kravene.
-	Når ny regulering kommer på plass vil KBO-enhetene sannsynligvis måtte forholde seg til flere regelverk når det gjelder leverandørkjedesikkerhet. Dette kan skape usikkerhet om hvilke regler som gjelder i hvilken situasjon.
-	Mens de gjeldende overordnede funksjonelle kravene på den ene siden gir fleksibilitet, vil de på en annen side også opprettholde usikkerhet rundt hvorvidt valgte løsninger for leverandøroppfølging er i tråd med kravene.
Leverandørene	
+	Leverandørene, som i stor grad leverer produkter og tjenester på tvers av sektorer, trenger ikke forholde seg til spesifikk regulering i kraftsektoren i Norge, eller til NVE som sektormyndighet. Kravene blir heller spesifisert og fulgt opp gjennom de kommersielle avtalene mellom KBO-enhetene og leverandørene. Leverandørene kan dermed fokusere på sektorovergripende og harmoniserte krav som kommer i NIS/NIS2-reguleringen.
-	For leverandører som leverer produkter og tjenester til mange KBO-enheter, kan det oppstå variasjon i kravene gjennom avtaler, basert på at ulike KBO-enheter tolker myndighetskrav og veiledning ulikt. At leverandørene må gjøre individuelle tilpasninger, kan skape uforutsigbarhet og økte kostnader for leverandørene (som igjen kan belastes KBO-enhetene).

Drøfting

En fordel med gjeldende regulering og «Nullalternativet» er at det gir nettselskapene en god del fleksibilitet i måten de kan følge opp leverandørene. Tilbakemelding fra nettselskaper har vært at veiledningen i utgangspunktet er god, særlig der veiledningen er konkret - for eksempel i form av sjekklister. Konkret veiledning om hvordan krav i kbf skal etterleves («skal-krav»), kan tas rett inn i virksomhetens styringsdokumenter, for eksempel som kravlister i anskaffelser.

Når det gjelder veiledning og anbefalinger som er mindre konkret, eller ikke er direkte knyttet til oppfyllelse av et forskriftskrav («bør-krav»), så er incentivene til å gjennomføre sikkerhetstiltak mindre. Særlig for nettselskaper kan en

medvirkende årsak være inntektsrammemodellen. Dette systemet sikrer at nettselskaper som opererer kostnadseffektivt kan oppnå høyere inntekter, mens de som er mindre effektive vil få lavere inntektsrammer. Som alle sikkerhetstiltak, vil også tiltak for å følge opp sikkerhet i leverandørkjeden, ha en administrativ kostnad. Det kan derfor være vanskelig å prioritere tiltak som vurderes som «bør-krav», og det heller ikke kan sannsynliggjøres at tiltaket gir en påviselig gevinst (f.eks. i form av reduserte KILE-kostnader).

Med nullalternativet kan det diskuteres hvor langt NVE har anledning til å utvide veiledningen med ytterligere «må-krav», uten at man også må gjennomføre endringer i kbf som tydeliggjør skjerpede krav. Det kan derfor være begrenset hvor mye økt leverandørkjedesikkerhet som i praksis vil oppnås for KBO-enhetene i gjeldende kraftberedskapsforskrift. Når skjerpede krav som følger av NIS- og NIS2-direktivene blir implementert, vil dette kunne endre seg. NVE vil da kunne utvikle tilpasset veiledning, men da med utgangspunkt i forskjellige lovverk.

Når det gjelder NVEs oversikt over leverandørmarkedet og leverandørkjederisiko i kraftforsyningen, så vil en slik oversikt måtte opparbeides og vedlikeholdes jevnlig. NVE-rapporten om leverandørkartlegging /3/ pekte på ulike løsninger, fra manuell innhenting og vedlikehold, til mer automatiserte løsninger ved hjelp av tredjepartsløsninger. Rapporten pekte på at alle løsningene ville være ressurskrevende på sine måter.

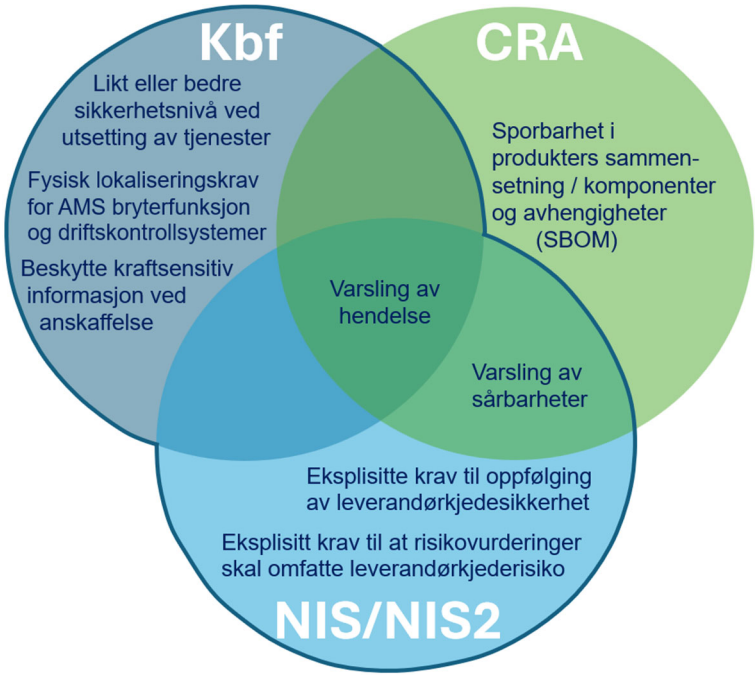
Det rapporten ikke pekte på, var hvilket hjemmelsgrunnlag NVE har for å hente inn disse opplysningene. Kbf § 8-1 sier at KBO-enhetene må fremskaffe dokumentasjon og opplysninger som er nødvendige for å gjennomføre kontroll med at kravene i forskriften overholdes. Det kan stilles spørsmål til om denne bestemmelsen gir NVE hjemmel til å kreve opplysninger fra KBO-enhetene om leverandører og leverandørkjeder, dersom formålet ikke er en kontroll, men at NVE skal få en generell oversikt over leverandørmarkedet. Dersom hjemmelsgrunnlaget mangler, står NVE igjen med frivillig innrapportering.

6.2 Alternativ A: Indirekte regulering med forsterket leverandøroppfølging

Beskrivelse

Alternativ A innebærer fortsatt indirekte regulering av leverandører, men med tydeligere regulatoriske krav til KBO-enhetenes oppfølging av sikkerhet i leverandørkjeden. I tillegg innebærer alternativet at NVE gjør regulatoriske tiltak som sikrer økt oversikt over kraftforsynings leverandørkjeder og dermed kontroll med leverandørkjederisiko.

Den første delen av alternativ A vil være at NVE gjennomfører forskriftsendringer som tetter gapet mellom kravene til leverandørkjedesikkerhet i kbf og krav til leverandørkjedesikkerhet i NIS/NIS2-direktivene (som vil være relevant for KBO-enheter). Hensikten vil da være at KBO-enhetene kan forholde seg utelukkende til kbfs krav til leverandørkjedesikkerhet, også etter at nasjonalt lovverk som implementerer NIS/NIS2-direktivene har kommet på plass (se Figur 3).



Figur 3 Alternativ A innebærer å proaktivt forsterke krav til leverandørkjedesikkerhet i Kbf slik at de også dekker fremtidige relevante krav i NIS2-direktivet

Den andre delen av alternativ A vil være å gjennomføre nødvendige forskriftsendring som gir NVE hjemmel til å innhente opplysninger fra KBO-enheter, herunder leverandøroversikter, som går utover rene kontrollformål overfor den enkelte KBO-enhet. Rasjonale er at NVE skal gjøres bedre i stand til å kunne ivareta forskriftens formål i møte med leverandørkjede-hendelser. Dette kan for eksempel være en ekstraordinær situasjon hvor mange KBO-enheter rammes samtidig av en hendelse hos én felles underleverandør, og som dermed rammer betydelige deler av kraftforsyningen. Ved at NVE får bedre oversikt over konsentrasjonsrisiko i leverandørkjedene, kan de motvirke slike hendelser ved å iverksette skadeforebyggende og skadereduserende tiltak i sektoren.

Innenfor alternativ A vil NVE ha utvidet handlingsrom til å utvikle mer spesifikke veiledninger («må-krav») overfor KBO-enhetene.

Forholdet til fremtidig regulering

Dersom alternativ A innrettes slik at kbfs krav til leverandørkjedesikkerhet blir minst like god, eller bedre enn det nasjonale lovverket som implementerer NIS/NIS2-direktivene, vil KBO-enhetene bare trenge å forholde seg til kravene i kbf. Man unngår dermed mulige uklarheter eller konflikter som nevnt om nullalternativet i kapittel 6.1.

Nye krav i kbf om opplysningsplikt for KBO-enheter om leverandører, vurderes ikke å ha noe betydning for, eller komme i konflikt, med fremtidig regulering.

Tilsvarende som nullalternativet, vil nye regulatoriske krav etter NIS, NIS2 eller CRA som treffer leverandørene i kraftforsyningen direkte, kunne leve side om side med gjeldende krav i kbf. Men som i nullalternativet, vil NVE sannsynligvis ikke være tilsynsmyndighet etter disse kravene, og dermed ikke få en større innflytelse over leverandørmarkedet enn i dag.

Tabell 2 Kost- og nyttevurdering for alternativ A

NVE	
+	Å oppdatere kbf med leverandørkjedekrav som er minst like god som i NIS/NIS2 gjør at krav bedre kan tilpasses og harmoneres med de øvrige sikkerhetskravene i forskriften, slik at de blir mest mulig hensiktsmessig for kraftsektoren og kbfs formål.
+	Å samle alle leverandørkjedekrav i én forskrift gjør regelverket mer oversiktlig, og gjør det enklere for NVE å lage veiledninger og å føre tilsyn. Dette vil være ressursbesparende.
+	Ansvarsplassering angående underleverandører er tydelig. Ansvaret ligger hos KBO-enheten, også der dette er satt ut til underleverandører.
+	Tydeligere plikt til KBO-enhetene om å rapportere oversikt over leverandører kan bidra til at det blir mer ressursbesparende for NVE å vedlikeholde en slik oversikt (f.eks. årlig rapporteringsplikt, rapportering ved endring).
-	Forskriftsendring er en administrativ prosess som krever tid og ressurser, gjennom utredning, høring og fastsettelse. I tillegg må det revideres og utarbeides nytt veiledningsmateriell med veiledningsaktiviteter.
KBO-enhetene	
+	Det er forenklende, og ressursbesparende for KBO-enhetene om de har ett sett med regelverk å forholde seg til.
+	Ansvarsplassering angående underleverandører er tydelig. Ansvaret ligger hos KBO-enheten, også der dette er satt ut til underleverandører.
+	Mer eksplisitte krav i forskrift gjør at kravene blir tydeligere og KBO-enheten vet hva den har å forholde seg til.
-	Mer eksplisitte krav i forskrift, i forhold til veiledning, kan gjøre at man mister noe av fleksibiliteten og muligheten til å finne egne de mest effektive metodene for å innfri kravene på. Dette kan være særlig utfordrende for små KBO-enheter.
-	Økte krav til leverandøroppfølging vil medføre økte administrative kostnader for KBO-enhetene. Forsterkede krav til leverandøroppfølging vil innebære å omsette disse i avtaler med underleverandørene. Noen krav kan være utfordrende å innfri for leverandør, eventuelt øke kostnaden i avtalene. Også dette kan være særlig utfordrende for små KBO-enheter, som også kan ha utfordringer med tanke på nødvendig kompetanse.
Leverandørene	
+	Leverandørene, som i stor grad leverer produkter og tjenester på tvers av sektorer, trenger ikke forholde seg til spesifikk regulering i kraftsektoren i Norge, eller til NVE som sektormyndighet. Kravene blir heller spesifisert og fulgt opp gjennom de kommersielle avtalene mellom KBO-enhetene og leverandørene. Leverandørene kan dermed fokusere på sektorovergripende og harmoniserte krav som kommer i NIS/NIS2-reguleringen
+	For leverandører som leverer produkter og tjenester til mange KBO-enheter, så kan mer entydige krav og økt forutsigbarhet fra KBO-enhetene være kostnadsbesparende.
-	Økte kundekrav fører til økte kostnader for leverandør, som må reflekteres i prisen som kundene betaler. Dette kan for eksempel påvirke mindre leverandører negativt, som blir mindre konkurransedyktige enn de store leverandører som kan dra nytte av stordriftsfordeler.

Drøfting

Alternativ A medfører at KBO-enhetenes krav til leverandørkjedesikkerhet i kbf styrkes. Når kravene iverksettes i denne forskriften kan de også tydeligere tilpasses denne forskriftens formål, enn om de er spredt på ulike lovverk. Dette gir NVE et godt grunnlag for å utarbeide en helhetlig og konkret veiledning overfor KBO-enhetene, og tydeliggjør hva KBO-enhetene må gjøre for å sikre etterlevelse.

Styrkede og mer konkrete krav har også en nedside, ved at de kan øke driftskostnadene og redusere fleksibiliteten som KBO-enhetene har til å tilpasse tiltak mest mulig optimalt til egen organisasjon. Her kan det være store forskjeller mellom KBO-enhetene basert på selskapstype, størrelse, og hvordan de har innrettet driften med tanke på tjenesteutsetting. Det er derfor viktig at NVE finner en god balanse mellom konkrete krav (preskriptive krav) og mål/resultat-krav (funksjonelle krav).

Alternativ A innebærer også lov-/forskriftsendring for å tydeliggjøre NVEs hjemmel til å innhente opplysninger fra KBO-enhetene om deres leverandørforhold. Når en slik opplysningsplikt er spesifisert i lov eller forskrift, har NVE også større handlingsrom til å spesifisere, for eksempel i veiledning, hvilke type opplysninger som er aktuelle og hvordan KBO-enhetene skal rapportere. NVE bør vurdere om opplysningsplikten også kan/bør utvides til en rapporteringsplikt, f.eks. årlig eller ved endringer. En ulempe med rapporteringsplikt er at det kan skape unødvendig ressursbruk både hos KBO-enhetene og i NVEs oppfølging av plikten.

Omfanget av opplysningsplikten må i alle tilfeller være begrunnet med å oppfylle kbfs formål, som blant annet vil være å identifisere og treffe tiltak for å håndtere konsentrasjonsrisiko i leverandørkjedene i kraftforsyningen. Det vil si, risikoen ved at et fåtall leverandører leverer til mange virksomheter i kraftforsyningen, og en hendelse hos leverandøren kan påvirke mange virksomheter samtidig. Hvordan opplysningsplikten innrettes vil avhenge av hvilken metode NVE vil bruke for å vedlikeholde oversikten over leverandørkjedene i kraftforsyningen. Dette kan da spenne fra å kreve opplysninger ved behov (ad-hoc), til å kreve rapportering jevnlig, ved betydelig endringer, eller at det etableres automatiserte løsninger, jf. /3/.

6.3 Alternativ B: Direkte regulering av leverandører

Beskrivelse

Alternativ B innebærer at det etableres regulatoriske krav i kbf som rettes direkte mot kritiske leverandører som inngår i kraftforsyningens leverandørkjede. NVE får da virkemidler for å ha oversikt over, og kunne følge opp sikkerheten til, leverandørene direkte.

Oversikten i kapittel 8 Vedlegg A viser at mange av leverandørene som leverer til kraftforsyningen sannsynligvis vil bli direkte underlagt sikkerhetskrav gjennom NIS2 og CRA. Det er derfor lite hensiktsmessig å etablere generiske sikkerhetskrav i kbf, som skal rettes mot leverandører som leverer IT/OT- og IT-sikkerhetstjenester innenfor en rekke sektorer. Tilnærmingen i alternativ B er derfor at leverandører som leverer systemer eller tjenester som har kritisk betydning for kraftforsyningen, blir pålagt nødvendige plikter for å ivareta særskilte behov i kraftforsyningen.

Først må de kritiske leverandørene identifiseres og underlegges kbf. Vilkårene for å bli underlagt må være knyttet til hvorvidt man leverer IT-/OT- eller IT-sikkerhetstjenester som vurderes å ha vesentlig betydning for kraftforsyningen.

NVE har allerede i dag hjemmel til å underlegge virksomheter deler av kbf gjennom vedtak etter § 1-3, dersom de har «vesentlig betydning for produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme». Dette krever at NVE selv identifiserer og treffer vedtak overfor virksomhetene.

Alternativ B forutsetter imidlertid at etableres en registreringsplikt, der leverandøren selv plikter å registrere seg hos NVE dersom de oppfyller nærmere definerte vilkår. Denne rapporten går ikke nærmere inn på å definere disse vilkårene i detalj, men vilkårene kan for eksempel være basert på type tjeneste som leveres (IT-/OT- eller IT-sikkerhetstjeneste) og til hvilket system i kraftforsyningen (f.eks. driftskontrollsystemer). Videre kan leverandørens markedsandel/omsetning gi indikasjoner på kritikalitet. Det at leverandøren har tilgang på kraftsensitiv informasjon kan også være et vilkår, eller om tjenesten leveres fra Norge eller utlandet, osv. Det som er avgjørende, er at vilkårene defineres i forskriften på en slik måte at leverandørene enkelt kan vurdere om de plikter å registrere seg eller ikke.

Når en leverandør oppfyller vilkårene, vil de ha plikt til å registrere seg hos myndigheten, og de vil da være gjenstand for en rekke krav. Kravene bør fylle ut behovet som ikke dekkes gjennom de mer generelle sikkerhetskravene som leverandørene sannsynligvis blir pålagt gjennom NIS/NIS2/CRA-direktivene, eller kravene som naturlig bør inngå i de privatrettslige avtalene mellom leverandørene og KBO-enhetene. Krav de vil pålegges gjennom kbf vil da typisk kunne være:

- Plikt til å registrere seg hos NVE med organisasjonsnummer, norsk adresse, fysisk lokasjon, kontaktperson, levert tjeneste/produkt og KBO-enhet de leverer til, osv.

- Plikt til å varsle direkte til NVE ved sårbarheter eller hendelser har påvirket eller kan påvirke kraftforsyningen vesentlig.
- Plikt til å ha beredskapsplan for ekstraordinære situasjoner i kraftforsyningen.
- Plikt til å bidra i øvelser i kraftforsyningen når NVE krever det.
- Plikt til å medvirke i kontroll og tilsyn.

Forholdet til fremtidig regulering

Kap. 5.2 viser at det er varierende hvorvidt de undersøkte leverandørene som antas falle inn under NIS/NIS2/CRA tilhører et spesifikt sektorområde, og dermed om de blir underlagt tilsyn fra en sektormyndighet eller f.eks. Nasjonal sikkerhetsmyndighet. I de fleste tilfeller vil aktørene ikke falle inn under NVEs tilsynsområde. Dersom leverandørene blir underlagt kbf gjennom direkte krav, så vil NVE være tilsynsmyndighet for de spesifikke kravene for kraftsektoren, mens de er underlagt tilsyn av en annen myndighet etter NIS/NIS2/CRA. Leverandørene vil da være underlagt sikkerhetskrav fra ulike lovverk.

Som nevnt over, er alternativ B innrettet slik at krav som rettes direkte mot leverandørene i mest mulig grad skal utfylle, og komme i tillegg til, de generelle sikkerhetskravene som de sannsynligvis blir underlagt i henhold til NIS/NIS2/CRA-direktivene. Det vil derfor i utgangspunktet ikke være noe konflikt mellom kravene, selv om det kan være en større byrde å etterleve krav i flere sikkerhetsreguleringer.

Tabell 3 Kost- og nyttevurdering for alternativ B

NVE	
+	Dersom leverandører underlegges registreringsplikt og andre sikkerhetskrav i kbf, vil NVE lettere ha en løpende oversikt over viktige leverandører uten selv å måtte innhente dette fra leverandørmarkedet eller via KBO-enhetene.
+	Leverandørene blir nærmere knyttet til beredskapsmyndigheten. Direkte regulering legger til rette for tettere myndighetsdialog, direkte varsling til myndighetene og direkte oppfølging mellom NVE og leverandørene. Dette kan styrke forsyningssikkerheten i både forebygging og håndteringen av uønskede hendelser.
-	Veilednings- og tilsynsarbeidet kan bli komplekst og ressurskrevende ettersom dette må tilpasses en heterogen gruppe leverandører som dekker både IT-leveranser, OT-leveranser og IT-sikkerhetstjenester. I tillegg skal NVE følge opp KBO-enhetene som vanlig.
-	Kompleksiteten i tilsyn og regelverkstolkning kan øke når det samme regelverket og samme tilsynsmyndighet skal følge opp KBO-enheter og kravene knyttet til deres oppfølging av underleverandører, og de samme underleverandørene direkte. Det kan oppstå konflikt eller usikkerhet om ansvarsplassering. For eksempel, vil et avvik skyldes KBO-enhetens manglende oppfølging av leverandøren, eller leverandørens brudd på krav i kbf?
KBO-enhetene	
+	KBO-enheter som har leverandører underlagt kbf direkte, vil kjenne til hvilke krav disse underleverandørene er underlagt. Dette gir en forsikring om at de blir fulgt opp og kontrollert av myndighetene under samme regulatoriske regime som de selv har.
+	At leverandørene er underlagt direkte regulatoriske krav kan muligens avlaste KBO-enhetene for enkelte oppfølgingskrav, for eksempel ved varsling. Her vil KBO-enhetene kunne varsle myndighetene, men med forvissning om at deres involverte leverandører også har direkte varslingsplikt.
-	Det kan oppstå en forventning blant KBO-enhetene om at når leverandørene er underlagt krav fra NVE direkte, så blir deres behov for leverandøroppfølging mindre. Dette kan skape et forventningsgap og gi KBO-enheter incentiver til å spare kostnader ved å redusere oppfølgingen av egne leverandøravtaler.
-	Dersom de nye regulatoriske kravene rettet mot leverandørene øker deres kostnader med å levere tjenestene til KBO-enhetene, så kan disse kostnadene bli belastet KBO-enheten. Dette kan ytterligere forsterke incentivet over.

Leverandørene
- Leverandører som leverer IT/OT-tjenester eller IT-sikkerhetstjenester innenfor flere sektorområder vil måtte forholde seg til ny sektorspesifikk regulering. Dette vil kunne skape utfordringer med at de underlegges ulike sikkerhetsreguleringer som enten overlapper eller ikke er harmonerer, og øke kompleksiteten og kostnadene for etterlevelse for underleverandørene. - Dersom det følger med særskilte og byrdefulle regulatoriske krav ved å levere tjenester til den norske kraftforsyningen, kan dette medføre at leverandørene finner det forretningsmessig uhensiktsmessig å levere disse tjenestene. Dette kan medføre nedkjølingseffekt i markedet.

Drøfting

NVE har tidligere hatt en godkjenningsordning for leverandører til kraftforsyningen, der det ble inngått sikkerhetsavtale med utvalgte leverandører. Denne ordningen ble opphevet for flere år siden. Det er nå KBO-enhetene selv som må vurdere risiko og innføre risikoreduserende tiltak.

Det er gode grunner for å gå bort fra en slik løsning. For det første er det ressurskrevende for myndigheten å opprettholde en slik ordning gitt den raske teknologiske utviklingstakten og dynamikken i markedet. For det andre kan en slik ordning bidra til at KBO-enhetene i mindre grad har incentiver til å vurdere egen risiko og selv følge opp leverandørene, og dermed kunne skape en falsk trygghet.

Alternativ B innfører en variant av en slik ordning. Imidlertid innebærer ikke alternativ B en godkjenningsordning, men at viktige leverandører pålegges visse regulatoriske plikter. I så måte er løsningen mindre ressurskrevende for myndigheten, og medfører også mindre risiko for at det skal oppstå en falsk trygghet for KBO-enhetene. NVE vil også få god oversikt over leverandørmarkedet, få tilgang til nødvendig informasjon fra leverandørene, og kunne gi direkte pålegg for å ivareta kbfs formål.

Alternativet medfører imidlertid også noen utfordringer. En sentral utfordring kan være å definere vilkårene for registreringsplikt treffsikkert nok, og tydelig nok for de potensielt registreringspliktige leverandørene. Hvis vilkårene er for strenge, kan NVE risikere å overse aktører i leverandørkjeden som kan ha betydning for kraftforsyningen. På en annen side, hvis vilkårene utformes slik at svært mange leverandører må registrere seg og oppfylle tilleggskrav i kbf, kan dette være uforholdsmessig byrde for leverandørene, og unødvendig ressursbruk for NVEs oppfølgingsarbeid. Ressursbruken for NVEs nødvendige veiledningsarbeid overfor en heterogen gruppe IT-, OT- og IT-sikkerhetsleverandører skal heller ikke undervurderes.

En annen utfordring kan oppstå dersom det stilles krav om direkte varsling til NVE ved sårbarheter eller hendelser. Dersom leverandørene pålegges varslingsplikt til f.eks. NSM etter fremtidige lover som implementerer NIS/NIS2/CRA-direktivene, og sektorvis varslingsplikt til NVE etter kbf (og gjerne med ulike terskler), så kan dette skape utfordringer både for leverandøren og for myndighetskoordineringen. En mer effektiv løsning vil være at myndighetene etablerer ett koordinert varslingsmottak for «tverrsektorielle» leverandører, og at myndighetene innad utveksler varslingsinformasjon seg imellom, f.eks. gjennom det sektorvis responsmiljøet (SRM).

7 ANBEFALING OG VEIEN VIDERE

Kapittel 6 presenterer og drøfter hvordan NVE kan stille regulatoriske krav og følge opp sikkerheten i IT- og OT-leverandørkjeder i kraftforsyningen. Målet er todelt:

1) Å styrke den enkelte KBO-enhetenes sikkerhet
2) Å styrke NVEs oversikt og kontroll med sikkerhetstilstanden i leverandørmarkedet.

Tre alternativer nærminger er vurdert og drøftet:

- Nullalternativet – videreføring av dagens veiledningsinnsats uten endringer i regelverket.
- Alternativ A – indirekte regulering med forsterket oppfølging av leverandørkjeder.
- Alternativ B – direkte regulering av kritiske leverandører.

I kapittel 7.1 gjøres det en samlet vurdering av alternativanalysene og anbefaling. I kapittel 7.2. drøftes innretningen av det anbefalte alternativet og oppfølgningen.

7.1 Samlet vurdering og anbefalt løsning: Alternativ A

Først oppsummeres drøftingen av de enkelte alternativene. Deretter følger en samlet vurdering og den anbefalte løsning.

Oppsummering av alternativene

Nullalternativet gir nettselskapene betydelig fleksibilitet i oppfølgingen av leverandører. Incentivene for å iverksette anbefalte «bør-krav» er i dag imidlertid svake. NVE kan gi tydeligere krav i veiledning («må-krav») men da må det være reelt grunnlag for å fortolke de eksisterende forskriftskravene strengere enn i dag. Når det gjelder NVEs behov for oversikt over leverandørmarkedet, er det usikkert om eksisterende kontrollhjemmel kan brukes til å innhente leverandøroversikter med formål å få generell oversikt. Dette kan resultere i at NVE må basere slik informasjonsinnhenting på frivillighet. Fremtidige regulatoriske krav fra NIS, NIS2 og CRA vil sannsynligvis treffe mange leverandører i kraftforsyningen direkte. Imidlertid er det mindre sannsynlig at NVE som sektormyndighet får tilsynsansvaret overfor leverandører som tilbyr generiske IT-, OT- eller IT-sikkerhetstjenester på tvers av sektorer. NVE får i så tilfelle ikke noe direkte innflytelse over leverandørmarkedet i kraftforsyningen.

Alternativ A innebærer å styrke kravene til KBO-enhetene oppfølging av leverandørkjeder i kbf. Kravene bør da utformes slik at de dekker gapet mellom dagens krav og antatt fremtidige krav til leverandørkjedesikkerhet som KBO-enhetene vil pålegges som følge av NIS/NIS2-direktivene. KBO-enhetene får da ett regelverk å forholde seg til, som tar høyde for fremtidige lovendringer etter NIS/NIS2. Styrkede krav vil på en annen side kunne øke driftskostnadene og redusere fleksibiliteten for KBO-enhetene. Alternativ A innebærer også lov- eller forskriftsendringer for å tydeliggjøre NVEs hjemmel til å innhente opplysninger fra KBO-enhetene om deres leverandørforhold. Dette legger til rette for at NVE lettere kan fremskaffe oversikt over leverandørkjederisiko som kan ha betydning for kraftforsyningen, og dermed kunne treffe egnede tiltak.

Alternativ B innebærer endringer i kbf som gjør at leverandørene pålegges plikter direkte, herunder en plikt til å registrere seg hos NVE dersom de oppfyller visse vilkår. Denne løsningen er mindre ressurskrevende enn den tidligere godkjenningsordningen som er avviklet, og reduserer også den gamle ordningens risiko for falsk trygghet, ved at KBO-enhetene fortsatt må vurdere risiko og innføre risikoreduserende tiltak som i dag. En sentral utfordring med alternativ B er å kunne definere vilkårene for registreringsplikt presist nok i forskriften, slik at NVE får oversikt over de reelt viktigste leverandørene. En annen utfordring er ressursene som vil kreves for veiledning og oppfølging av en heterogen gruppe med IT-, OT-, og IT-sikkerhetsleverandører. En tredje er at leverandørene vil kunne få overlappende/doble plikter, for eksempel å måtte registrere seg hos flere myndigheter, og varsle flere myndigheter i parallell.

Samlet vurdering

Både nullalternativet og alternativ A tydeliggjør gjeldende prinsipper om at KBO-enhetene er ansvarlige for sikkerheten, uavhengig av hvordan de innretter virksomheten gjennom bruk av leverandører. I begge alternativene så vil også potensielt styrkede krav til leverandørkjedesikkerhet treffe KBO-enhetene når NIS- og NIS2-dirketivene blir implementert i norsk rett. En hovedforskjell er at alternativ A innebærer aktive grep for å oppdatere kbf slik at KBO-enhetene kan forholde seg kun til kravene i kbf, og at kravene kan innføres på det tidspunkt NVE bestemmer.

Når det gjelder NVEs evne til å få oversikt over leverandørmarkedet, og kunne identifisere leverandørkjederisiko for kraftforsyningen på tvers av enkeltselskaper, så vil forskriftsendringene i alternativ A gi tydeligere hjemmel for NVE til å innhente opplysninger fra KBO-enhetene til dette formålet. Også alternativ B vil muliggjøre dette, ved at leverandørene selv får plikt til å registrere seg hos NVE, noe som avlaster KBO-enhetene. Men alternativ B har også flere ulemper ved seg, som nevnt i drøftingene over.

En sentral forskjell mellom alternativ A og B er at førstnevnte kan bidra til en mer presis informasjonstilgang. Dersom KBO-enhetene blir pålagt å gi opplysninger om sine kritiske leverandører, så vil NVE få rapportert inn leverandører og deres tjenester som har reell kritikalitet for kraftforsyningen. Leverandørene på sin side sitter gjerne ikke på nøyaktig informasjon om hvor kritisk deres produkter og tjenester er for den enkelte kunde. For eksempel kan KBO-enhetene utnytte en leveranse til både kritiske og ikke-kritiske funksjoner, ha iverksatt beredskapsløsninger som reduserer kritikaliteten på produktet eller tjenesten, eller ha innført en diversifiseringsstrategi med redundante løsninger fra flere leverandører.

Anbefalt løsning: Alternativ A - indirekte regulering med forsterket oppfølging av leverandørkjeder

Samlet finner DNV at alternativ A gir best måloppnåelse da det imøtekommer både behovet for å styrke den enkelte KBO-enhetens sikkerhet, og gir grunnlag for å styrke NVEs oversikt og kontroll med sikkerhetstilstanden i leverandørmarkedet. Alternativet bygger også på å innarbeide prinsipper om at KBO-enhetene har ansvaret for egen sikkerhet også ved tjenesteutsetting, og innebærer ikke at NVE må etablere et nytt oppfølgingsregime mot en heterogen gruppe med IT-/OT- og IT-sikkerhetstjenesteleverandører.

7.2 Oppdatering av forskriftskrav versus retningslinjer i veiledning

Alternativ A innebærer forskriftsendringer i kbf som skal ivareta to forhold: Det ene er å styrke KBO-enhetenes krav til leverandørkjedesikkerhet, ved å lukke gapet mellom pliktene i dagens kraftberedskapsforskrift, og forventede krav som følger av innføring av NIS, NIS2 og CRA direktivene i norsk rett. Det andre er å forsterke og tydeliggjøre hjemmelen for å innhente opplysninger fra KBO-enhetene om leverandørforhold, for å sikre at NVE kan gjøres bedre i stand til å analysere leverandørkjederisiko for hele kraftforsyningen, og på tvers av den enkelte KBO-enhet.

Denne rapporten foreslår ikke et konkret forslag til oppdaterte forskriftsbestemmelser om leverandørkjedesikkerhet, da dette vil forutsette en nærmere juridisk analyse. Den overordnede analysen i kapittel 7.1 gir likevel noen føring på hvilke kravområder som det er aktuelt å tilføye som krav i kbf. Dette omfatter:

- Krav til at leverandørkjederisiko skal inngå i KBO-enhetenes risikovurdering. Herunder må det tydeliggjøres at ved endringer som innebærer tjenesteutsetting, så skal risikoer i de nye verdikjedene identifiseres.
- Forsterket krav til aktiv oppfølgingsplikt/påse-plikt ved tjenesteutsetting, og tydeliggjøring av at denne plikten gjelder gjennom hele livsløpet til leveransen.
- Krav til at leverandører også varsler om avdekkede sårbarheter, og ikke bare hendelser.
- Tydeligere tidsfrister for sårbarhets- og hendelsesrapportering gjennom leverandørkjeden.
- Krav om at KBO-enhetene plikter å gi opplysninger til NVE om leverandører og leverandørforhold som er nødvendig for å ivareta kbfs formål, herunder konsentrasjonsrisiko.

Det er også relevant å se hen til hvordan leverandørkjedekrav er utformet i EU-forordning for cybersikkerhet i kraftsektoren (NCCS), selv om hovedfokuset i forordningen er grensekryssende elektrisitetsflyt.

Videre vil det være viktig å avklare hva som bør defineres i forskrift og hva som bør presiseres i veiledning. Intervjuene som DNV har gjennomført indikerer at KBO-enhetene gjerne ønsker tydelige tydeligere krav og veiledning som gir mindre tolkningsrom. Det vil si, preskriptive beskrivelser og fremgangsmåter for å sikre etterlevelse. Dette må imidlertid avveies mot den fleksibiliteten som mer funksjonelle krav gir, som angir resultatet som ønskes oppnådd, men hvor hver KBO-enhet står friere til å implementere løsninger som passer for egen virksomhet. DNV vil peke på noen viktige spørsmål som NVE må ta stilling til:

Hvilke krav til leverandørkjedesikkerhet bør presiseres i forskrift?

Ved revisjon av kbf som skal innføre forsterkede krav til leverandørkjedesikkerhet, må detaljeringsnivået på forskriftskravene harmoniseres med det nivået som ventes å komme i lovverket som skal innføre NIS2-direktivet. Dette for å sikre tydelige og rettslig bindende krav i kbf som vil være minst like god som forventede krav i lov og forskrift som innfører NIS2-direktivet. Høringen til digitalsikkerhetsforskriften, som innfører NIS-direktivet i norsk rett, vil også kunne gi en pekepinn på hvordan lovverket som innfører NIS2 vil utformes.

Hvilke krav i kbf bør være preskriptive og hvilke bør være funksjonelle?

Kbf inneholder i dag en blanding av funksjonelle krav og preskriptive krav. En rettesnor er at dersom måten å sikre etterlevelse på vil kunne variere betydelig fra virksomhet til virksomhet, og også kan endre seg betydelig med teknologiendringer og endringer i trusselbildet, så taler det for å bruke funksjonelle krav. Bestemmelsene knyttet til leverandørkjedesikkerhet (§ 6-5 om anskaffelser og § 6-9 tredje ledd bokstav e om tjenesteutsetting) er i hovedsak funksjonelle, noe som gjør at nær all presisering skjer i veilednings form. Særlig når det gjelder § 6-9 bør NVE vurdere om kravene rundt tjenesteutsetting bør utvides med preskriptive beskrivelser, f.eks. om aktiv oppfølgingsplikt. Videre kan allerede preskriptive krav knyttet til risikovurdering (§ 2-3), varsling (§ 2-5) og rapportering (§ 2-6) – også utvides med presiseringer som rettslig binder KBO-enhetene til styrket leverandørkjedesikkerhet.

Hvilke veiledningskrav bør være «må-krav» og hvilke bør være «bør-krav»?

Veiledninger vil inneholde ytterligere preskriptive beskrivelser, gjerne med henvisning til standarder og rammeverk, som kan tilpasses i takt med endringer i teknologi og trusselbildet. For nye forskriftskrav knyttet til leverandørkjedesikkerhet, er det mulighet å tilpasse veiledningen til ulike typer KBO-enheter, og om det er snakk om leverandørkjedesikkerhet i IT- eller OT-domenet, eller for IT-sikkerhetstjenester. Det bør forventes at veiledningens «må-krav» gjennomføres av alle KBO-enheter. Ut fra en risikobetraktning bør det også uttrykkes en forventning fra myndighetenes side om at større/kritiske KBO-enheter gjennomfører flere «bør-krav», mens for mindre KBO-enheter med begrensede ressurser må man erkjenne at «bør-krav» i praksis være vanskelig å prioritere.

7.3 Bruk av standardisering for leverandørkjedesikkerhet

NVE har i sitt veiledningsmateriale allerede utarbeidet flere skjema, sjekklister og henvisninger til standarder og rammeverk. Nettselskapene gav i intervjuene inntrykk av at konkrete hjelpemidler, for eksempel i form av sjekklister, var svært nyttige. For det første kan de lett innarbeides (eventuelt med tilpasning) i egne styringssystemer for sikkerhet, for å sikre etterlevelse. For det andre kan de bidra til en standardisering i kravstillingen mot underleverandørene. Ettersom KBO-enhetene i mange tilfeller bruker de samme underleverandørene, kan dette øke forutsigbarhet og redusere kostnader for både leverandørene og for KBO-enhetene.

DNV har spurt intervjuobjektene om hvorvidt standarder og rammeverk er benyttet for leverandørkjedesikkerhet og -oppfølging. NSMs grunnprinsipper for IKT-sikkerhet og SOC 2 ble nevnt. Det samme ble veiledningene om leverandørkjeder og skytjenester utarbeidet i regi av FSK. Den generelle oppfatningen er at det ikke finnes noen de-facto bransjestandard eller rammeverk som har bred adopsjon blant KBO-enhetene. Når det gjelder å stille krav i avtaler med leverandører om at de skal etterleve visse sikkerhetsstandarder, ble ISO 27001 nevnt. Ettersom bare tre aktører har blitt intervjuet, har DNV ikke grunnlag for å si at dette synet er representativt for bransjen som helhet. Imidlertid er dette en oppfatning som DNV har fra erfaringer fra arbeid mot kraftsektoren. Man kan også anta, ut fra gjeldende

veiledning til kbf, at dette er tilfelle. I veiledningen listes de fleste relevante standarder opp, uten at det vises til at noen foretrekkes fremfor andre.

Utfordringen er derfor ikke tilgjengeligheten til aktuelle standarder og rammeverk, men at bransjen som helhet ikke er omforent om noen få, de-facto bransjestandarder for å ivareta leverandørkjedesikkerhet. I mangel på dette, så blir heller ikke den fulle gevinsten i form av forutsigbarhet og kostnadseffektivitet for KBO-enhetene og for leverandørkjeden utløst.

DNV vil anbefale at det gjennomføres en nærmere analyse av hvordan kraftbransjen bedre kan utnytte potensialet i standarder og rammeverk med mål å sikre bedre forutsigbarhet, kostnadseffektivitet og standardiserte prosesser for leverandørkjedesikkerhet i fremtiden. Her vil det være nyttig å se på følgende momenter:

- Fordeler/ulemper med bruk av ulike typer innretninger av retningslinjer, rammeverk og standarder for leverandørkjedesikkerhet: Kraftbransjen har egne retningslinjer, for eksempel fra FSK. NSM utvikler nasjonale retningslinjer i grunnprinsipper for IKT-sikkerhet som trekker ut de overordnede prinsippene fra en rekke internasjonalt anerkjente rammeverk og standarder. Så fins det enkeltvis anerkjente rammeverk som NIST CSF, og deretter standarder fra europeiske standardiseringsorganisasjoner som CEN, CENELEC eller ETSI – herunder harmoniserte standarder (bestilt av EU). Til sist internasjonale standarder fra ISO/IEC.
- I NIS2-direktivet nevnes bruk av europeiske og internasjonale standarder som en foretrukket tilnærming for å sikre etterlevelse av kravene i direktivet. ISO 27000-serien nevnes eksplisitt i direktivet, og for eksempel DNV har tatt til orde for at IEC 62443 kan utnyttes for å sikre etterlevelse i OT-domenet /23/. Ettersom mange av IT-, OT-, og IT-sikkerhetsleverandørene som leverer til kraftforsyningen sannsynligvis vil bli underlagt NIS2-direktivet, bør KBO-enhetenes kravstilling til leverandørene om standarder, harmoniseres med utviklingen som skjer i NIS2-sporet.

7.4 Innhenting og bruk av opplysninger om leverandører

Alternativ A innebærer en tydeligere hjemmel for NVE til å innhente opplysninger fra KBO-enhetene om kritiske leverandører. Dette vil da være viktig for å skaffe til veie en leverandøroversikt, som har blitt utredet nærmere i /3/.

Før NVE utarbeider krav og retningslinjer til KBO-enhetenes opplysningsplikt, bør det avklares hva en slik leverandøroversikt skal brukes til og hvordan den skal brukes. Slik DNV vurderer det vil hovedformålet med leverandøroversikten være å kunne avdekke sårbarheter og risiko i leverandørkjedene for sektoren som helhet, utover det som den enkelte KBO-enhet har forutsetninger til å identifisere. Med andre ord, sårbarheter og risiko som bare NVE som sektormyndighet har forutsetninger for å identifisere. Et utvalg av aktuelle områder vil være:

- Konsentrasjonsrisiko: Kartlegge leverandører som benyttes av svært mange KBO-enheter, eventuelt som leverer til kategorier av kritiske KBO-enheter.
- Flaskehalser: En leverandøroversikt kan gi grunnlag for å gjennomføre videre leverandørkjedeanalyser som kan avdekke flaskehalser i leverandørkjeden, slik som «single-points-of-failure», eller manglende dimensjonering av beredskap, som kan få propagerende effekter som påvirker kraftforsyningen.
- Geopolitisk risiko og nasjonal kontroll: Analyser av eierskap av leverandører og grad av nasjonal kontroll av kritiske leveranser i leverandørkjedene, for å avdekke sårbarheter dersom det oppstår geopolitiske endringer, sikkerhetspolitiske kriser og krig. Herunder vurdering av aktuelle substitutter dersom uønskede scenarioer oppstår.
- Sikkerhetsgraderte trussel- og risikovurderinger: NVEs tilgang til sikkerhetsgradert informasjon fra, og samhandling med, sikkerhetstjenestene (NSM, PST og E-tjenesten) kan kobles med kunnskapen om kritiske leverandører og leverandørkjeder i kraftforsyningen, og spille inn på områdene nevnt over.

Oversikten kan i tillegg bidra til å identifisere risiko hos enkeltvirksomheter (KBO-enheter), som kan danne grunnlag for tilsyn og oppfølging, selv om dette ikke er hovedformålet med leverandøroversikten.

For å minimere ressursbruk både hos NVE, KBO-enhetene og leverandørene bør NVE først avklare formålet med informasjonsinnhentingen, og deretter avgrense innhentingen til de opplysningene som er nødvendig for å oppnå dette formålet.

Videre bør NVE avklare hvilke virkemidler som kan brukes til å håndtere avdekket sårbarhet og risiko. Det minst inngripende virkemidlet vil være informasjonsdeling, dialog og veiledning opp mot KBO-enhetene. De kan gjøres kjent med avdekkede sårbarheter og risiko, slik at de kan gjøre avbøtende tiltak. Slik innsikt kan deles på mange måter, og spenne fra offentlig tilgjengelige risikorapporter til deling av sikkerhetsgradert informasjon gjennom en-til-en veiledningsmøter med KBO-enheter.

Andre aktuelle tiltak kan være å gjennomføre øvelser på spesifikke scenarioer, treffe enkeltvedtak som å pålegge beredskapstiltak, endre på markedsbaserte incentivordninger, slik som inntektsrammemodellen, for å fremme økt diversifisering av leverandører, eller gjennomføre lov- og forskriftsendringer.

7.5 Opplysning og veiledning om IT/OT-sikkerhet til leverandører i kraftforsyningen

Alternativ A innebærer at NVE ikke får direkte inngripen med leverandørene. Denne tilnærmingen gjør at det kan være utfordrende for NVE å drive nødvendig opplysning og veiledning om IT/OT-sikkerhet til leverandørene om forhold som er viktig for kraftforsyningen. Imidlertid vil NVE gjennom KBO-enhetenes opplysningsplikt om leverandører og leverandørforhold kunne få en god oversikt over hvem de mest kritiske leverandørene er og hvorfor.

Selv om leverandørene underlegges et regulatorisk regime i Norge, f.eks. av NSM, så vil ikke NVE selv ha noen direkte myndighetsrolle over leverandørene. Derfor bør opplysning og veiledning av disse leverandørene, hva angår forhold i kraftsektoren, skje primært i det frivillige sporet gjennom samarbeid og dialog. Målet med slik dialog og samarbeid må være at leverandørene i størst mulig grad blir kjent med sikkerhetsforhold som er viktig for kraftforsyningen, hvilke krav som pålegges KBO-enhetene og dermed reflekteres i leverandøravtalene, og viktigheten av at leverandørene er sitt samfunnsansvar bevisst, og understøtter kundene i kraftforsyningen og myndighetene ved ekstraordinære situasjoner. Det er også viktig at avtaler sikrer sikkerhet, pålitelighet, integritet og konfidensialitet gjennom hele livssyklusen av produkter eller tjenester.

NVE bør legge til rette for gode arenaer og et godt samarbeidsklima mellom myndigheten, KBO-enhetene og leverandørene. Dette skjer gjennom å involvere viktige leverandør i bransjeorganisasjoner, bransjeforum og workshops, og å gjennomføre en-til-en dialogmøter. Samarbeidet bør også innrettes slik at leverandørene har incentiver til å delta. Det kan gjøres gjennom å bidra med informasjon som har verdi for leverandørene, og gi leverandørene mulighet for å gi innspill til NVE om forhold som kan bedre deres situasjon overfor kundene i kraftsektoren. For eksempel kan NVE invitere leverandørene til å gi innspill på hvordan sikkerhetskrav i leverandøravtalene kan forbedres, effektiviseres og standardiseres. Denne innsikten kan NVE da bruke til å forbedre retningslinjer og veiledningen mot KBO-enhetene.

Når leverandørene etter hvert omfattes av nasjonale krav som implementerer NIS2-direktivet, vil de underlegges tilsyn fra en nasjonal myndighet, for eksempel NSM. Det kan da bli aktuelt å koordinere noe av myndighetsdialogen om leverandørkjedesikkerhet med dem, og eventuelt tilsynsmyndigheter i andre sektorer hvor leverandørene spiller en kritisk rolle i verdikjedene.

8 REFERANSER

/1/ Riksrevisjonen. (2021). *Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen.* https://www.riksrevisjonen.no/globalassets/rapporter/no-2020-2021/nves-arbeid-med-ikt-sikkerhet-i-kraftforsyningen.pdf

/2/ Proactima. (2021). *Veikart for NVEs oppfølging av IKT-sikkerhet i leverandørkjeden*. https://www.nve.no/media/13231/1074197-re-01-veikart-for-nves-oppf%C3%B8lging-av-ikt-sikkerhet-i-leverand%C3%B8rkjeden-endelig-rapport.pdf

/3/ PwC. (2024). *Leverandørkartlegging av viktige leverandører for kraftforsyningen inkludert metodikk for vedlikehold*. https://publikasjoner.nve.no/eksternrapport/2024/eksternrapport2024_19.pdf

/4/ *Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m*. LOV-1990-06-29-50 (energiloven). Lovdata: https://lovdata.no/dokument/NL/lov/1990-06-29-50

/5/ *Forskrift om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m.* FOR-1990-12-07-959 (energilovforskriften). Lovdata: https://lovdata.no/dokument/SF/forskrift/1990-12-07-959

/6/ *Forskrift om sikkerhet og beredskap i kraftforsyningen.* FOR-2012-12-07-1157 (kraftberedskapsforskriften). Lovdata: https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157

/7/ ISO. (2022). *Information security, cybersecurity and privacy protection - Information security management systems - Requirements*. NEK ISO/IEC 27001:2022. https://online.standard.no/nb/nek-isoiec-27001-2022

/8/ ISO. (2022). *Information security, cybersecurity and privacy protection - Information security controls*. NEK ISO/IEC 27002:2022. https://online.standard.no/nb/nek-isoiec-27002-2022

/9/ NSM. (2024). *NSMs grunnprinsipper for IKT-sikkerhet – versjon 2.1*. https://nsm.no/getfile.php/1313975-1717589722/NSM/Filer/Dokumenter/Veiledere/NSMs%20Grunnprinsipper%20for%20IKT-sikkerhet%20v2.1.pdf

/10/ AICPA. (2022). *SOC 2 Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*. https://www.aicpa-cima.com/cpe-learning/publication/soc-2-reporting-on-an-examination-of-controls-at-a-service-organization-relevant-to-security-availability-processing-integrity-confidentiality-or-privacy

/11/ NVE. (2024). *Veiledning til kraftberedskapsforskriften.* NVE digital veileder. https://veiledere.nve.no/kraftberedskapsforskriften

/12/ FSK Forum. (2023). *Veileder for sikkerhet i anskaffelser og leverandørkjeder*. https://fsk-forum.no/wp-content/uploads/2023/08/FSK-Veileder-for-sikkerhet-i-anskaffelser-og-leverandorkjeder-Endelig-versjon-august-2023.pdf

/13/ FSK Forum. (2021). *Sikkerhetsveileder for Kraftsensitiv Informasjon i Skytjenester*. https://fsk-forum.no/wp-content/uploads/2021/11/FSK-Veilder-for-skytjenester-Final-PDF.pdf

/14/ IEC. (2024). *ISA/IEC 62443 Series of Standards.* https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

/15/ NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

/16/ *Lov om digital sikkerhet*. LOV-2023-12-20-108 (digitalsikkerhetsloven). Lovdata: https://lovdata.no/dokument/LTI/lov/2023-12-20-108

/17/ Justis- og beredskapsdepartementet (2024). *Høring - Forslag til forskrift til digitalsikkerhetsloven (digitalsikkerhetsforskriften)*. https://www.regjeringen.no/no/dokumenter/horing-forslag-til-forskrift-til-digitalsikkerhetsloven-digitalsikkerhetsforskriften/id3052967/

/18/ Directive (EU) 2022/2555. *On measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*. https://eur-lex.europa.eu/eli/dir/2022/2555

/19/ Regulation (EU) C(2024)7151. *Commission Implementing Regulation (EU) …/… laying down rules for the application of Directive (EU) 2022/2555*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=pi_com:C(2024)7151

/20/ Regulation (EU) 2022/0272. *On horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454

/21/ Commission Delegated Regulation (EU) 2024/1366 (2024). *Supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202401366

/22/ NVE. (2024). *Innspill til forvaltningsregime: Ivaretagelse av kraftforsyningssikkerhet til havs.* https://publikasjoner.nve.no/rapport/2024/rapport2024_19.pdf

/23/ Kreukniet, Gennady. (2024). *Leverage IEC 62443 for EU NIS2 Directive Compliance*. DNV. https://www.dnv.com/cybersecurity/cyber-insights/leverage-iec-62443-for-eu-nis2-directive-compliance/

VEDLEGG A: KBF-KRAV VERSUS EUROPEISKE-KRAV

Tabell 4 Sammenligning av leverandørkjede relaterte krav mellom kbf, digitalsikkerhetsforskriften (NIS) og NIS2 & CRA

Tema	Kbf	Digitalsikkerhetsforskriften	NIS2 & CRA	Kommentar
Formål	Sikre kraftforsyning i Norge.	Sikre grunnleggende krav til digital sikkerhet i virksomheter med særlig betydning for samfunnet ved å forebygge, avdekke og motvirke uønskede hendelser i nettverk og informasjonssystemer som brukes for å levere samfunnsviktige tjenester og digitale tjenester.	NIS2: Forbedre cybersikkerheten i medlemslandene. CRA: Forbedre standard cybersikkerhet i produkter med digitale elementer og muliggjør korrigering av oppdagede sårbarheter.	Kbf fokuserer mest på tilgjengelighet av kraftforsyningen i sin helhet som samfunnstjeneste mens NIS2 fokuserer spesifikt på cybersikkerhet som et ledd i pålitelige samfunnstjenester.
Omfang	KBO-enheter som definert i lovgivning eller designert av myndighetene.	Tilbydere av samfunnsviktige tjenester samt tilbydere av digitale tjenester (nettbaserte markedsplasser, nettbaserte søkemotorer eller skytjenester). Alle KBO-enheter.	Lister sektorer og subsektorer med kriterier som antall ansatte og omsetning. Gjelder virksomheter som opererer (tilbyr tjenester eller produkter) i EU selv om de ikke er basert i EU.	Langt færre virksomheter er underlagt kbf enn Digitalsikkerhetsforskriften eller NIS2 i Norge.
Ekvivalens (lex specialis prinsipp)		Digitalsikkerhetsforskriften tillater at tilsvarende eller strengere lokalt regelverk overstyrer digitalsikkerhetsforskriften.	NIS2 tillater at tilsvarende eller strengere lokalt regelverk overstyrer NIS2.	Om kbf regelverk dekker minst NIS2 regelverk kan ignoreres for KBO-enheter om kbf dekker i det minste alle krav fra NIS2.
Registrering/ innmelding	Ikke innmelding, det er NVE som utpeker og vedlikeholder et register.	Innmeldingsplikt til NSM og tilsynsmyndigheten for samfunnsviktig tjeneste.		
Ansvar for tiltak	Ledelse for virksomheten (KBO-enheter). Nevner ikke leverandørkjedens ledelse.	Ledelse for virksomheten underlagt Digitalsikkerhetsforskriften.	Ledelse for virksomheten underlagt NIS2.	Noen leverandører til kraftsektor i Norge blir underlagt NIS2, men må ikke nødvendigvis være KBO-enheter og dermed underlagt kbf.

Tema	Kbf	Digitalsikkerhetsforskriften	NIS2 & CRA	Kommentar
Organisasjon	KBO består av: • KBO-enhetene • KDS og beredskaps-myndigheten • KSL Kbf krever visse funksjoner innad KBO-enheter som: • Beredskapsleder • Beredskapskoordinator • IKT-sikkerhetskoordinator	**Hendelser bistand**: Ansvarlig departement kan utpeke responsmiljøer. **Varsling**: Varsel skal gis til tilsynsmyndighet med kopi til NSM. **Deling** av taushetsbelagt informasjon: dele med andre aktører der nødvendig. **Nasjonal kontakt punkt**: NSM er nasjonalt kontaktpunkt for sikkerhet i nettverk og informasjonssystemer. **Tilsyn**: Ansvarlig departement utpeker myndighet som skal føre tilsyn med virksomheter innenfor egen sektor.	NIS2 krever sektorvis eller nasjonalt at det utnevnes og etableres en CSIRT og en kompetent myndighet.	Kbf pålegger ytterligere krav på virksomhetsnivå ift organisasjon. Digitalsikkerhetsforskriften og NIS2 setter kun organisasjons krav på nasjonalt eller sektor nivå. CSIRT for NIS = KraftCERT for Kbf. Myndighet for NIS = NVE for Kbf. NIS har intet spesifikt krav for beredskap. NIS2 utnevner EU-CyCLONe som ansvarlig for krisehåndtering ved alvorlig cyber hendelser. NVE har overordnet beredskapsansvar ifølge Kbf.
Delegering	Beredskapsmyndigheten kan delegere oppgaver innenfor varsling, informasjonsdeling og analyse for IKT-sikkerhetshendelser i kraftforsyningen til en eller flere KBO-enheter.	Kompetansen til ansvarlig departement om å utpeke enkeltvirksomheter etter bestemmelsen kan delegeres i tråd med gjeldende prinsipper for delegasjon. Tilsynsmyndigheten kan benytte bistand fra andre ved utførelsen av tilsynet.	Kompetent myndighet kan prioritere tilsynsaktiviteter.	Kbf: Uklart om Beredskapsmyndigheten kan delegere tilsyn (for eksempel om NVE kan delegere tilsyn til KBO-enheter av sine leverandører. NIS: Uklart om «competent authorities» kan delegere tilsyn, men de kan prioritere ved å bruke risiko-basert tilnærming.
Sårbarheter varsling	Ikke rapporteringskrav for sårbarheter, kun hendelser eller umiddelbar risiko for driftskontrollsystemets funksjon.	Det er ikke krav til sårbarheters varsling i Digitalsikkerhetsforskriften.	Krav ved CRA (mulig krav for NIS2) om varsling ved funn av aktiv utnyttelse av sårbarheter (både som kunde og som leverandør) med beskrivelse av sårbarhet, berørte produkter eller tjenester, sikkerhetsoppdateringer eller andre tiltak. Varselet skal gjøres innen 24 timer. Bør peke ut en CSIRT for å koordinere sårbarhets eller trussels varsling.	For NIS2, det kan tolkes som frivillig (Article 7 c). Trussels varslings krav uklar.

Tema	Kbf	Digitalsikkerhetsforskriften	NIS2 & CRA	Kommentar
Hendelse varsling	Ja med beskrivelse av hendelsen, forventet gjenoppretting og kontaktperson.	Ja med info om tilbyders navn og kontaktinformasjon, berørt tjeneste, hendelsen, herunder mulige årsaker og konsekvenser, antall berørte brukere, hendelsens virkninger i andre land. Informasjonen i varselet skal oppdateres innen 72 timer.	Krav om varsling ved hendelse (både som kunde og som leverandør). Bør peke ut en CSIRT for å koordinere hendelses varsling.	Ikke eksplisitt krav fra kbf å varsle KraftCERT, NSM, NVE, KDS eller KSL men muligens står et annet sted. Som standard, er det NVE som varsles.
Informasjons-deling	Ikke direkte krav for samarbeid i kbf utenom beredskap og ekstraordinære situasjoner.	Kan dele taushetsbelagt informasjon med andre aktører der nødvendig og hensiktsmessig.	NIS2 krever informasjonsdeling mellom virksomheter av kategori «vesentlig» og «viktig», men også dens leverandører og tjenestetilbyder.	Kbf og Digitalsikkerhetsforskriften åpner for deling. NIS2 krever deling av informasjon mellom «peers». CRA krever ikke deling.

Tema	Kbf	Digitalsikkerhetsforskriften	NIS2 & CRA	Kommentar
Sikkerhetskrav	Gradert ulike sikringskrav per anleggsklasse. Spesifikke krav for brytefunksjonalitet i avanserte måle- og styringssystem (AMS).	**For samfunnsviktige tjenester:** • Etablere og vedlikeholde et styringssystem for sikkerhet som omfatter digital sikkerhet. • Risikovurdering inkl. i hvilken grad virksomheten er avhengig av andre virksomheter for å fungere som de skal. • Plan for å håndtere risiko. • Utarbeide skriftlige instrukser for rutiner og prosedyrer innenfor sikkerhet. • Iverksette teknologiske sikkerhetstiltak som er tilpasset omfang, kompleksitet, driftsmiljø, brukermiljø, funksjon og risiko ved virksomhetens nettverk og informasjonssystemer (se listen av minste krav). • Fysisk sikkerhet (se listen av minste krav). • Sikkerhetstiltak for personell (inkl. leverandører) av minste krav. • Beredskapsplan for håndtering av hendelser og varsling. • Oppfølgingsplikt av leverandører. **For tilbydere av digitale tjenester:** • Varslingsplikt. • Deling av taushetsbelagt informasjon • Opplysningsplikt og tilgang til lokaler.	Skal sikre et nivå av sikkerhet for nettverk og informasjonssystemer som er tilpasset den risikoen som foreligger. Nevner ulike sikkerhetskrav per type enheter «vesentlig», «viktig» som cyber hygiene, trening, hendelse og sårbarhets håndtering, business continuity, personell sikkerhet, tilgangskontroll og forvaltning av IKT-ressurser.	Alle har ulike og graderte krav i forhold til viktigheten av virksomhet.

Tema	Kbf	Digitalsikkerhetsforskriften	NIS2 & CRA	Kommentar
Sikkerhetskrav (krise)	Virksomheter plikter å sikre anlegg, system eller annet som er eller kan bli av vesentlig betydning for virksomhetens ledelse, drift eller gjenoppretting i ekstraordinære situasjoner mot uønskede hendelser og handlinger, herunder adgang for uvedkommende.	Varslingsplikt for virksomheter hvor en hendelse berører en tredjepart som tilbyr en digital tjeneste virksomheten er avhengig av.	NIS2 og CRA krever krisehåndteringsplan.	Kbf skiller mellom ekstraordinære forhold (med vekt på beredskap og gjenoppretting av funksjoner) og ordinær drift (generelle krav) men ikke NIS2 og CRA som kun krever krisehåndteringsplan eller varslingsplikt.
Leverandørkjede sikkerhet	Krav mot leverandører i spesifikke område: • Krav om informasjonssikkerhet og taushetsplikt for kraftsensitiv informasjon i anskaffelse, • AMS leverandører med brytefunksjonalitet har tilleggskrav (lokalisering), • For klasse 2 og 3, driftskontrollsystemer leverandører har tilleggskrav (lokalisering). Ellers, ikke direkte krav utenom selve KBO-enheter.	Formålet med bestemmelsen er å tydeliggjøre at kravene til forsvarlig sikkerhetsnivå også gjelder ved bruk av leverandører med blant annet oppfølgingsplikt av leverandører.	CRA legger direkte krav til sikkerhet for produkter (software og hardware) og data prosessering løsninger. Fri fra kjente sårbarheter, topp-nivå SBOM, varsling ved oppdagelse av feil og foreslå tiltak eller korreksjon. NIS2 legger eksplisitt krav til leverandørkjedesikkerhet.	Kravene fra CRA er i stor grad rettet mot leverandører av produkter i kraftforsyning industrien.

Tabell 5 Sammenligning av eksplisitt cybersikkert tiltak mellom NIS2 og kbf

NIS2 (Artikkel 21)	Kommentar ift. kbf
Tiltakene nevnt skal være basert på en «alle-trussel» tilnærming som tar sikte på å beskytte nettverks- og informasjonssystemer og det fysiske miljøet til disse systemene mot hendelser.	Tilsvarende §2-3, men kbf er ikke like eksplisitt om nettverk og adresserer mest ekstraordinære situasjoner og beredskap. Kbf er utformet slik at den tar høyde for en slags kritikalitetsvurdering der noen anlegg (se klasse), AMS, driftskontrollsystem, kraftsensitiv informasjon og mobile radionett – driftsradio får spesifikke tiltak.
Retningslinjer for risikokartlegging og informasjonssystemer sikkerhet.	Tilsvarende §6-9 men kbf har hovedfokus på informasjonssikkerhet mer enn på systemsikkerhet.
Håndtering av hendelser.	Tilsvarende §7-7 der kbf har fokus på driftskontrollsystem.
Forretningskontinuitet som backup-håndtering og katastrofegjenoppretting, og krisehåndtering.	Tilsvarende §2-4.
Leverandørkjedesikkerhet, inkludert sikkerhetsrelaterte aspekter som gjelder forholdet mellom hver virksomhet og dens direkte leverandører eller tjenesteleverandører. • Retningslinjer for leverandørkjede sikkerhet. • Spesifikk kriterier for vurdering og valg av leverandører som må ta høyde for leverandørers sikker utviklings prosedyrer, tilfredstillelse av sikkerhetskrav, kvalitet og motstandsdyktighet samt fare for avhengighet for bestilleren. • Virksomheter tar høyde for eksiterende risikovurderinger. • Avtaler med leverandører må sørge for etterlevelse av: sikkerhetskrav, trening og bevissthet innen sikkerhet, bakgrunnssjekk, varslingsplikt, rett til audit, plikt til å håndtere sårbarheter, bruk av underleverandør og sluttfase av avtalen. • Kontrollere etterlevelse av plikter i avtaler. • Implementere og vedlikeholde en leverandør register.	Tilsvarende §6-9 e) der virksomheter skal sørge for at sikkerhetsnivået opprettholdes eller forbedres ved utsetting av tjenester, men ikke like eksplisitt om leverandørkjedesikkerhet.
Sikkerhet ved anskaffelse, utvikling og vedlikehold av nettverks- og informasjonssystemer, inkludert håndtering og varsling av sårbarheter.	Tilsvarende § 6-5 men kbf setter søkelys på kraftsensitiv informasjonssikkerhet og nevner ikke håndtering og varsling av sårbarheter (med unntak for driftskontrollsystem i §7-7).
Retningslinjer og prosedyrer for å vurdere effektiviteten av cybersikkerhetsrisikostyringstiltak.	Tilsvarende §2-9 og 2-10 men kbf nevner ikke spesifikt cybersikkerhet.
Grunnleggende cyberhygienepraksis og cybersikkerhetstrening.	Ikke eksplisitt i kbf.
Retningslinjer og prosedyrer angående bruk av kryptografi og, der det er hensiktsmessig, kryptering.	Ikke eksplisitt i kbf.

NIS2 (Artikkel 21)	Kommentar ift. kbf
Menneskelige ressurser, tilgangskontroll og eiendelshåndtering.	Tilsvarende §2-7 men kbf har fokus på øvelser til å håndtere ekstraordinære situasjoner. Tilsvarende §6-7 men kbf har fokus på bakgrunn og eventuelt kredittsjekk og sikkerhetsklarering. Tilsvarende § 6-1, 6-10, 7-4, 7-10, 7-14 og 7-17 men kbf har fokus på tilgang til kraftsensitiv informasjon, AMS, driftskontrollsystem og mobile radionett – driftsradio. Tilsvarende §4-4 men kbf nevner kun reservedeler.
Bruk av flerfaktorautentisering eller kontinuerlige autentiseringsløsninger, sikrede tale-, video- og tekstkommunikasjoner og sikrede nødkommunikasjonssystemer innen enheten, der det er hensiktsmessig.	Ikke eksplisitt i kbf.

VEDLEGG B: ANONYMISERT UTTREKK AV LEVERANDØRER

Et representativt uttrekk av leverandører til kraftsektoren i Norge er listet under med farge kategorier hvorav mørkeblå viser «vesentlig», lyseblå viser «viktig» virksomheter. Leverandører uten farge er mest sannsynlig ikke underlagt NIS2 direktivet. De er videre delt i størrelse, S >=250 ansatte eller mer enn 500 MNOK omsetning, M 50 til 250 ansatte eller mer enn 100 MNOK omsetning.

Tabell 6 Representativt uttrekk av leverandører i kraftforsyningen og hvorvidt de er regulert av NIS2

Størrelse	Kontor i Norge	Kjerneområde	Digitalsikkerhetsforskriften	Direkte regulert av NIS2 (E for vesentlig, I for viktig)
S	Ja	IT, skytjenester, IT-sikkerhet, AI-tjenester, programvare, maskinvare, rådgivning og konsulenttjenester	DSP	E: Annex I, Sector 8, Data centre service provider, Cloud computing service providers E: Annex I, Sector 9, MSP, MSSP
S	Ja	Elektromekanisk utstyr og tjenester	Nei	I: Annex II, Sector 5 I, (d)
S	Ja	IT, skytjenester, rådgivning og konsulenttjenester	DSP	E: Annex I, Sector 8, Cloud computing service providers
S	Ja	IT-drift, AI-tjenester, skytjenester	DSP	E: Annex I, Sector 9, MSP
M	Ja	Programvare for kraft- og telekomselskaper	Mulig men ikke sannsynlig DSP.	I: Annex I, Sector 8, Cloud computing service providers
M	Ja	Utvikle, drifte og forvalte den digitale infrastrukturen til nettselskapene	DSP	I: Annex I, Sector 8, Cloud computing service providers I: Annex I, Sector 9, MSP
M	Ja	IT-system for distribusjon av strømmåleverdier	DSP	I: Annex I, Sector 8, Cloud computing service providers
S	Ja	Tjenester og utstyr til kraftindustrien	Mest sannsynlig ikke	I: Annex II, Sector 5 I, (d)
S	Ja	Spesialiserer på bærekraft og fornybar energi. Leverer utstyr, programvare, automatisering og integrasjon	Mulig DSP	I: Annex II, Sector 5 I, (d)
S	Ja	Fiberbredbånd	DSP	E: Annex I, Sector 8, Providers of public electronic communications networks
S	Nei	Elektronikk (til AMS-målere)	Nei	I: Annex II, Sector 5 I

S	Ja	Elektronikkutstyr, telekomutstyr og annen maskinvare (bl.a. strømmålere) samt programvare relatert til dette.	Mest sannsynlig ikke	E: Annex I, Sector 9, MSP, Cloud computing service providers I: Annex II, Sector 5 I,
	Ja	Telekomtjenester, IoT, testing og sikkerhetsløsninger for OT-miljøer	Mest sannsynlig ikke	Ikke E eller I pga. størrelse. På grense i omsetning. E: Annex I, Sector 9, MSP, MSSP
S	Ja	IT, skytjenester, AI og annen programvare	DSP	E: Annex I, Sector 8, Cloud computing service providers, Data centre service provider E: Annex I, Sector 9, MSP, MSSP
S	Ja	IT-sikkerhet	DSP	E: Annex I, Sector 9, MSSP
	Ja	Rådgivning, drift og tjenester innen nettverk og cybersikkerhet	Mest sannsynlig ikke	Ikke E eller I pga. størrelse eller omsetning. Annex I, Sector 9, MSSP
S	Ja	Digitalisering, kompetanse og ressursdeling på tvers av nettselskapene	Mulig DSP	E: Annex I, Sector 9, MSP
S	Nei	Elektronikk og telekomutstyr, IT-løsninger og OT-sikkerhet	DSP	E: Annex I, Sector 9, MSSP I: Annex II, Sector 5 (b), (c)
S	Ja	IT-løsninger, IT-infrastruktur, skytjenester	DSP	E: Annex I, Sector 8, Cloud computing service providers, Data centre service providers E: Annex I, Sector 9, MSP
S	Ja	Elektronikk og utstyr for kraftverk, telekom, IKT, elektromedisin, automatisering og transportsystemer	Mulig DSP	E: Annex I, Sector 9, MSP I: Annex II, Sector 5 (b), (c), (d)
S	Nei	Programvare innen nettverk, IT og sikkerhet	Mulig DSP	E: Annex I, Sector 8, Cloud computing service providers
S	Ja	Telekomtjenester	DSP	E: Annex I, Sector 8, Providers of public electronic communications networks
S	Nei	Programvare for virtualisering, skytjenester og nettverk	Mulig DSP	E: Annex I, Sector 8, Cloud computing service providers

Om DNV

Vi er et globalt selskap innen kvalitetssikring og risikohåndtering med tilstedeværelse i over 100 land. Vårt formål er å sikre liv, verdier og miljøet. Med vår unike tekniske ekspertise og uavhengighet bistår vi våre kunder med å forbedre sikkerhet, effektivitet og bærekraft.

Enten vi godkjenner et nytt skipsdesign, optimerer energiproduksjonen fra en vindmøllepark, analyserer sensordata fra en gassrørledning eller sertifiserer verdikjeden til en matprodusent, hjelper vi våre kunder med å ta gode og riktige beslutninger og øke tilliten til virksomheten, produktene og tjenestene deres. Verden er i endring. Vi kan påvirke utviklingen. Sammen skal vi takle de globale utfordringene og omstillingene vi vil møte.

NVE

Norges vassdrags- og energidirektorat

Middelthuns gate 29
Postboks 5091 Majorstuen
0301 Oslo
Telefon: (+47) 22 95 95 95