NVE

EKSTERN RAPPORT NR. 19 / 2024

Leverandørkartlegging av viktige leverandører for kraftforsyningen inkludert metodikk for vedlikehold

SKREVET AV PwC AS

NVE Ekstern rapport nr. 19/2024
Leverandørkartlegging av viktige leverandører for kraftforsyningen inkludert metodikk for vedlikehold

Utgitt av:	Norges vassdrags- og energidirektorat
Redaktør:	Jon-Martin Storm
Forfatter:	PwC AS
Omslagsbilde:	Detalj av utsmykning i vestibylen i NVE-huset, av kunstneren Odd Tandberg. Foto: Stig Storheil/NVE
ISBN:	978-82-410-2395-8
ISSN:	2535-8235
Saksnummer:	202307146

Sammendrag: PwC AS har kartlagt nøkkelleverandører innenfor IT og OT i kraftforsyningen for å forbedre arbeidet med sikkerhet og motstandsevne. Gjennom kvalitative og kvantitative metoder, inkludert workshops og spørreundersøkelser, har de skapt en oversikt for å styrke NVEs veiledning og tilsyn med sikkerhet i kraftforsyningen.

Emneord: Cybersikkerhet, leverandører, leverandørkjedesikkerhet, kraftforsyning

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

Juni 2024

Innhold

Forord

God leverandørkontroll og god sikkerhet i leverandørkjeder er vesentlig for å sikre sine egne digitale systemer. Kraftforsyningen er ikke et unntak, og virksomhetene har over flere år hatt konkrete og strenge krav til sikkerhet i anskaffelser. En del av dette er selskapenes egen oppfølging av leverandørene for egen sikkerhet og for å følge kravene. Dette følger vi opp med veiledning og med kontroll med selskapene i kraftforsyningen.

En annen del av leverandørkjedesikkerhet, er at vi som myndighet har god nok informasjon om de viktige leverandørene til kraftforsyningen. Dette er nødvendig for at vi skal kunne gjøre gode risikovurderinger og prioritere de riktige leverandørene i vår oppfølging. Et første trinn i å følge opp leverandørene er å etablere en oversikt over de viktigste leverandørene, og vedlikeholde denne oversikten over tid. Leverandører av systemer innen OT, kundeadministrasjon, AMS, DMS og nett/infrastrukturoversikt og cybersikkerhet er særlig aktuelle.

PwC AS har utarbeidet en leverandøroversikt og rapport som adresserer flere viktige tema:

- Hvilket ambisjonsnivå bør NVE ha for å holde oversikt over leverandører og deres leveranser til kraftforsyningen, og hvor langt ned i leverandørkjeden bør NVE ha oversikt?
- Nødvendige prosesser og systemer for NVE for å opprettholde denne oversikten.
- Hvorvidt ansvaret for å opprettholde oversikten bør ligge hos NVE eller overføres til andre.

Denne oversikten og tilhørende metode for vedlikehold er et godt grunnlag for NVE sin videre oppfølging av sikkerhet hos leverandører og i leverandørkjeder. Vi vil takke alle virksomhetene som stilte opp i intervjuer og spørreundersøkelser. De har bidratt med uvurderlig kunnskap om utfordringer og mulige løsninger.

Oslo, juni 2024

Eldri Naadland Holo
seksjonssjef
Seksjon for beredskap
Tilsyns- og beredskapsavdelingen

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

Sammendrag

Oversikt over leverandørkjeder og oppfølging av disse er essensielt i arbeidet med sikkerhet og motstandsevne, både for den enkelte virksomhet, men også for sektorer og tilhørende myndigheter.

NVE har gjennom dette arbeidet fått etablert en oversikt over de mest sentrale leverandørene i kraftforsyningen. Oversikten er kommet frem gjennom bruk av kvalitative metoder som workshop og intervjuer, samt kvantitative metoder som spørreundersøkelse og gjennomgang av åpne kilder. Leverandøroversikten danner et godt utgangspunkt for videre arbeid i det som må etableres som en kontinuerlig prosess. Rapporten viser overordnet fra leverandøroversikten, men den komplette leverandøroversikten er regnet som kraftsensitiv og er ikke tilgjengelig offentlig.

Videre beskriver rapporten alternativer for prosess for vedlikehold og videre utvikling av leverandøroversikten, samt fastslår hvem som bør eie denne. Prosessen for vedlikehold og utvikling kan oppsummeres ved at NVE bruker oversikten aktivt i veilednings- og tilsynsarbeidet og oppdaterer leverandøroversikten som del av dette. Det bør også legges til rette for utstrakt samarbeid og informasjonsutveksling på området. Slik kan NVE bygge erfaring med praktisk bruk og samtidig løse oppdraget i påvente av tekniske løsninger. På sikt bør leverandøroversikten flyttes til en mer tilpasset løsning gjennom egen utvikling eller anskaffelse via tredjepart. Eierskapet til leverandøroversikten bør legges hos NVE. Dette med bakgrunn i at de formelt bærer ansvaret, men også fordi oversikten er så tydelig knyttet til deres rolle og oppgaver i kraftberedskapsorganisasjonen.

1 Bakgrunn / beskrivelse

1.1 Kraftforsyningen

Kraftsystemet i Norge kan forstås som et lineært system med produksjon, overføring, distribusjon og forbruk. Kraftsystemet krever høy driftsstabilitet og samfunnet er avhengig av sikker forsyning av kraft. Norges vassdrags- og energidirektorat (NVE) har ansvar for å forvalte landets vann- og energiressurser. Stadig flere systemer og prosesser i kraftforsyningen er digitalisert, og sektoren er avhengig av at informasjonsteknologi (IT)- og operasjonell teknologi (OT)-systemer fungerer stabilt og sikkert. Samtidig er bransjen i endring med nye leveransemodeller og økende bruk av tredjeparter for levering av IT- tjenester. Kraftbransjen er avhengig av at leverandører leverer etter gitte krav og forutsetninger. Dette kan innebære en vesentlig risiko for kraftsektoren. Det er nødvendig å ha oversikt over, kontroll og gode avtaler med leverandørene. Gjennom god internkontroll og oppfølging av leverandører vil kraftbransjen redusere risikoen for at IT-hendelser og cyberangrep skjer som en konsekvens av sårbarheter og risikoer i leverandørkjeden.

Den teknologiske utviklingen har ført til at flere leverandører av OT og IT har kommet på banen. Figuren nedenfor illustrerer kraftforsyningen og hvordan den går fra produksjon til forbruk. Med leverandører menes ikke i denne sammenheng leverandører av strøm, men selskaper som leverer enten IT, OT eller IT-sikkerhet til selskaper i kraftbransjen. Dette kan være leverandører av både hardware, software eller andre tjenester, som for eksempel rådgivning. Disse leverandørene leverer til alle de fire prosessene av kraftforsyningen som er illustrert nedenfor.

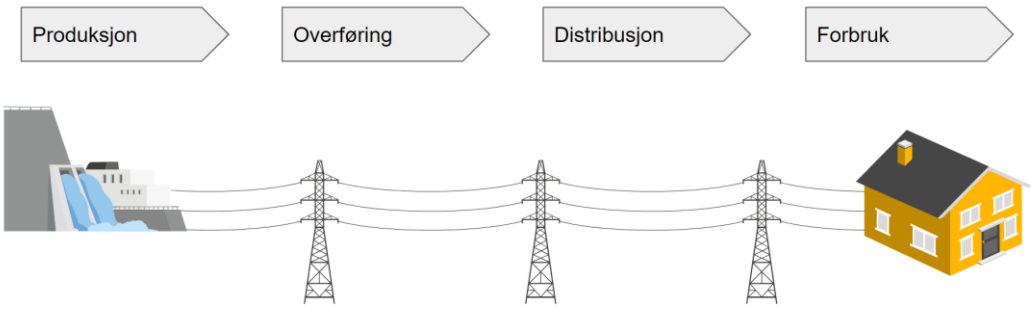

Fig. 1: Illustrasjon av kraftforsyningen.

OT-begrepet brukes om både maskinvare og programvare som administrerer og kontrollerer fysiske prosesser i infrastruktur. I kraftforsyningen omtales dette ofte som driftskontrollsystemer. I moderne industri er OT og IT tett sammenkoblet. Den økte og tette sammenkoblingen mellom eksterne anleggssystemer, kontornettverk og internett skaper flere

muligheter for nettverksangrep. Svak IT- og OT-sikkerhet hos leverandører kan dermed utnyttes av trusselaktører for å utnytte sårbarheter i kraftbransjen. Slike angrep har mange potensielle utfall, som eksempelvis forstyrrelse av tjenester og drift.

1.2 Forskrift om sikkerhet og beredskap i kraftforsyningen

Kraftberedskapsforskriften har som formål å redusere samfunnsmessige konsekvenser i ekstraordinære situasjoner, og sikre at kraftforsyningen opprettholdes.[1] Kapittel 6 og 7 i forskriften setter krav til informasjonssikkerhet og beskyttelse av driftskontrollsystem.

Enhetene i Kraftforsyningens beredskapsorganisasjon (KBO) har jf. kraftberedskapsforskriften §6-5 ansvar for at bestemmelsene om informasjonssikkerhet og taushetsplikt for kraftsensitiv informasjon ivaretas i anskaffelser. Videre skal virksomheter jf. kraftberedskapsforskriften §6-9 E sørge for at sikkerhetsnivået opprettholdes eller forbedres ved utsetting av tjenester.

1.3 Riksrevisjonens rapport "Undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen"

IKT-hendelser og cyberangrep rettet mot kraftbransjen kan innebære store konsekvenser for kritiske samfunnsfunksjoner som eksempelvis leveranse av vann, avløp og helsetjenester. Riksrevisjonen publiserte i 2021 rapporten "Undersøkelse av NVEs arbeid med IKT- sikkerhet i kraftforsyningen" hvor de kommer med en rekke anbefalinger for å styrke beredskap og håndtering av dataangrep, inkludert oppfølging og kontroll av leverandørene i kraftforsyningen. NVE har på sin side prioritert arbeidet med IT-sikkerhet over flere år og gjennomført en rekke aktiviteter for å redusere risikoen.

Riksrevisjonens rapport fra 2021 påpeker at *"Oppfølgingen av leverandørene er mangelfull til tross for at de har stor betydning for IKT-sikkerhet i kraftforsyningen"*.[2] Dette viser til at selskapene i kraftforsyningen i stor grad er avhengig av leverandørenes IKT-sikkerhet. Riksrevisjonens undersøkelse viser videre at kraftselskaper har mangelfull informasjon om leverandørenes arbeid med IT-sikkerhet, i tillegg til mangelfull oppfølging.

Et startpunkt for å sikre et bedre informasjonsgrunnlag for IT-sikkerhet i kraftforsyningen er

[1] https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157
[2] https://www.riksrevisjonen.no/rapporter-mappe/no-2020-2021/undersokelse-av-nves-arbeid-med-ikt-sikkerhet-i-kraftforsyningen/

derfor å kartlegge de viktigste leverandørene av IT, OT og IT-sikkerhet.

1.4 Videre beredskapsarbeid i kraftforsyningen

En leverandørkartlegging vil være et viktig underlag for videre beredskaps- og sikkerhetsarbeid i NVE og generelt i kraftbransjen. Som underlag til tilsyn av virksomheter i kraftsektoren oversendes dokumentasjon til NVE. Når NVE etterspør listen over leverandører blir den gjerne laget der og da, som en oversikt i Excel.

For gjennomføringen av en risikovurdering er avdekking av sårbarheter viktig. Å ha en oppdatert oversikt over leverandører er viktig for å kunne avdekke sårbarheter, og mangel på oversikt kan i seg selv være en sårbarhet. I 2018 oppga åtte av ti virksomheter i kraftsektoren at de er avhengige av leverandører for å håndtere hendelser.[3] Denne kartleggingen som er gjort gir et godt grunnlag for videre arbeid, men er kun et øyeblikksbilde og må kontinuerlig oppdateres.

1.4.1 Business Impact Analysis (BIA)

En Business Impact Analysis (BIA) er en aktivitet i kontinuitetsstyring som identifiserer vitale funksjoner og fremhever systemavhengigheter. Prosessen definerer krav for gjenopprettelse av IT-tjenester. Gjennomføringen av en BIA vil gjennom kartlegging av avhengigheter og krav kunne øke bevisstheten rundt sikkerhet. Prosessen består av følgende:

- ➔ Kartlegging av informasjonsverdier
- ➔ Kartlegging av informasjonssystemer som verdien er tilknyttet
- ➔ Vurdering av informasjonsverdier
- ➔ Kartlegging av tilgjengelighetskrav

IT-systemer i kraftbransjen leveres i økende grad av tredjepartsleverandører. Det er viktig å identifisere disse systemene, og i så måte identifisere leverandørene. Vi anser leverandøroversikten som et første steg mot gjennomføring av BIA-er i kraftbransjen. Gjennomføringen av en BIA vil gi økt bevissthet rundt sikkerhet, gi innspill til risikovurdering og beredskapsplaner, fremheve systemavhengigheter, samt forbedre og optimalisere risikostyringen.

[3] Risikostyring av IKT-sikkerhet i leverandørkjeder av Ida-Kristin Johnsen og Vilde Lysgaard

1.5 Avgrensning

Det er gjennomført en innledende kartlegging av leverandører som leverer til mange aktører i kraftbransjen. Denne kartleggingen skal danne utgangspunktet for videre arbeid med leverandøroversikt. Implementering av tekniske verktøy har ikke vært en del av arbeidet. Hovedfokus har vært de største og sektorspesifikke leverandørene, slik at fagsystemer for kraft er tillagt mer oppmerksomhet enn standard kontorstøttesystemer.

Leverandører av nye tjenester eller som ikke enda er tatt i bruk i den norske kraftbransjen er ikke inkludert i denne kartleggingen. Dette gjelder for eksempel fleksibilitetsmarkeder.

Leverandøroversikten er et vedlegg til denne rapporten. Dette grunnet at informasjonen som ligger i oversikten kan anses som sensitiv og kan potensielt utnyttes av trusselaktører.

2 Faktorer for vurdering av leverandør

Virksomheter skal identifisere og dokumentere både verdier, leveranser, tjenester, systemer og brukere i sine digitale informasjonssystemer, samt holde denne dokumentasjonen oppdatert, jf kraftberedskapsforskriften. Sikkerhetsnivået skal videre opprettholdes eller forbedres ved utsetting av tjenester. Dette sammenfaller i stor grad med NSMs grunnprinsipper for IKT-sikkerhet punkt 1.1.5, som går ut på at man må kartlegge virksomhetens leveranser, informasjonssystemer og understøttende IKT-funksjoner.[4] En slik kartlegging vil bidra til at verdikjeder, informasjon og avhengigheter blir identifisert og vurdert, og kan videre benyttes som utgangspunkt ved beskyttelse og vedlikehold.

Ettersom det er gjennomført en kartlegging av *viktige* leverandører i kraftbransjen forutsatte dette at det ble etablert noen faktorer for hva som kjennetegner en viktig leverandør. Dette ble gjort i samarbeid med NVE hvor det i en av workshoppene/arbeidsmøtene først ble gjennomført en brainstorming-øvelse med tanker om hva som kan være kriterier for vurdering av leverandør. Etter brainstormingen ble det gjennomført en avstemning hvor deltakerne stemte på hvilke faktorer de anså som viktigst. Disse var som følger:

1. *Operasjonell teknologi (OT), SCADA*:

Operasjonell teknologi og SCADA-systemer har direkte påvirkning på kraftforsyning og strømleveranse. Til forskjell fra andre IT-tjenester kan dette ha direkte påvirkning på selskapets drift og fysiske systemer. Skadepotensialet er dermed stort, slik at det blir naturlig å bruke dette som en faktor.

2. *System-, integrasjons- eller totalleverandør*:

Faktoren indikerer om leverandøren tilbyr løsninger for hele eller deler av kjerneprosessene i kraftforsyningen for en produsent eller distributør. Slike leverandører vil typisk kunne levere komponenter og tjenester i integrerte løsninger, og således stå ansvarlig for sentrale prosesser i produksjonen. F.eks. Validér på smarte målere, som er ansvarlig for å drifte og overvåke AMS-målere og nødvendig infrastruktur for en rekke selskaper.

3. *Dekningsgrad i Norge*:

[4] https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/identifisere-og-kartlegge/kartlegg-styringsstrukturer-leveranser-og-understottende-systemer/

Faktoren viser til om leverandøren er en eneleverandør og hvilke typer selskap som er kunde. Dette kan f.eks. måles ved størrelse, markedsandel, forholdet antall kunder vs. størrelse og leverandørens økonomiske eller operasjonelle status.

I spørreundersøkelsen rangerte virksomhetene hvilke av faktorene de vurderte som viktigst basert på listen som ble generert i workshop. Virksomhetene fremhever følgende spørsmål som mest relevante for å identifisere viktige leverandører:

- Leverer leverandøren operasjonell teknologi som har direkte påvirkning på kraftforsyning og strømleveranse?
- Er dere avhengig av leverandørens kompetanse?
- Forvalter leverandøren kraftsensitiv informasjon?
- Er leverandøren en totalleverandør for systemer som anses viktig i deres virksomhet?
- Er leverandøren lokalisert i eller eid fra land som kan medføre forhøyet risiko?

Prioritetene er i stor grad sammenfallende med de vurderingene som ble gjort i workshop. Faktoren knyttet til dekningsgrad i Norge er mindre relevant for den enkelte virksomhet, men er en vesentlig faktor fra NVE og Riksrevisjonens perspektiv.

Faktorer eller kriterier for hva som utgjør en viktig leverandør kan endre seg over tid og bør dermed revisiteres jevnlig for oppdatering. I så måte må leverandøroversikten være et levende dokument, ikke bare med tanke på hvilke leverandører som inkluderes, men også hva disse leverer og hvilke faktorer ved leverandører som er viktige. Videre kan det være aktuelt å legge til andre indikasjoner på graden av viktighet, f.eks. omsetningstall, antall ansatte eller datastrømmer. Dette er informasjon som kan berike oversikten og gi ny innsikt, men som ikke er tatt med i løsningen i denne omgang da det løses best ved automatisering og dermed krever en teknisk implementering.

3 Leverandøroversikt

Leverandøroversikten er utviklet i et regneark. Selve filen er vedlagt og unntatt offentlighet da denne inneholder informasjon som potensielt kan utnyttes av trusselaktører. Leverandøroversikten inneholder om lag 275 leverandører som er vurdert som leverandører til kraftbransjen. Disse er igjen kategorisert i IT, OT og IT-sikkerhet med noe overlapp mellom kategorier. Videre kan disse filtreres på viktighet.

Faktorene som ble vurdert som sentrale er inkludert i leverandøroversikten, slik at det kan filtreres på *type leverandør*, *type leveranse* og *leveranseinformasjon.* I tillegg har vi inkludert felt for beskrivelse, kommentarer, kunder, kundens viktighet, kilde, geografisk lokalisering og sertifisering IT-drift.

Leverandører av IT-tjenester i norsk kraftforsyning varierer fra globale, anerkjente selskaper, som f.eks. SAP, til mindre, lokale tilbydere og egenutviklede systemer. Disse leverandørene tilbyr blant annet programvareutvikling, systemintegrasjon, arkitektur, datalagringsløsninger, skytjenester, Enterprise Resource Planning (ERP), rådgivning og konsulenttjenester. De aller fleste IT-leverandørene tilbyr også løsninger innen IT-sikkerhet, ofte som en integrert del av sine IT-løsninger. Eksempler på leverandører som opererer i grensesnittet mellom IT og IT-sikkerhet er Microsoft, Dell, IBM og Hewlett Packard Enterprise.

Flere representative OT-leverandører i norsk kraftforsyning tilbyr også IT-løsninger, som f.eks. Hitachi og Emerson. I tillegg er det totalleverandører som leverer både IT-, OT- og IT-sikkerhetstjenester som Siemens og ABB. Et annet slikt eksempel er ABB hvor integrerte kontrollsystemer samler prosess-, kraft-og sikkerhetskontroll i én plattform, inkludert produksjon og automasjon. Det er ikke nødvendigvis slik at kunden må eller velger å benytte seg av alt én leverandør kan tilby. Kunden er da mindre avhengig av leverandøren, samtidig som leverandøren ikke vet om det de leverer blir brukt etter "beste praksis" og dermed kan garantere for sikkerheten i sine produkter. Dette vil spesielt gjelde OT-leverandører som ikke tilbyr IT, drift og andre tjenester. I leverandøroversikten er leverandørene aggregert på tvers av alle kunder.

Kraftselskaper benytter seg av mange ulike leverandører som spesialiserer seg innen IT-sikkerhetsløsninger. Eksempler er Palo Alto og McAfee som leverer brannmurløsninger og antivirusprogramvare.

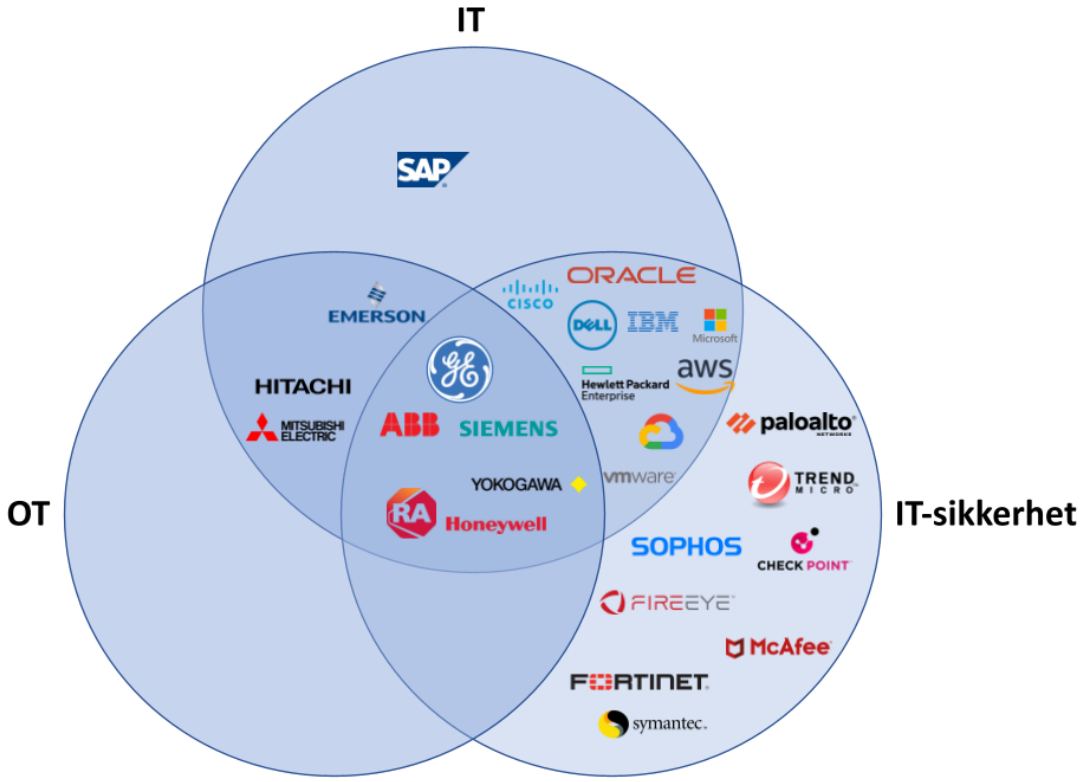

Fig. 2: Oversikt over utvalgte leverandører i norsk kraftforsyning.

Flere leverandører i norsk kraftforsyning opererer på tvers av skillene mellom IT, OT og IT-sikkerhet, noe som vitner om en stadig økende grad av teknologisk integrasjon (se Fig. 3). Dette gjør at det blir vanskeligere å skille leverandørene basert på at en viktig faktor for vurdering av leverandør er at de leverer operasjonell teknologi og SCADA-systemer.

Arbeidsprosess for vedlikehold av leverandøroversikt

En oversikt over sentrale leverandører er et naturlig startpunkt i arbeid med tredjepartsrisiko. Når en oversikt over leverandører er etablert, gir dette mulighet for å både evaluere leverandørene og jobbe videre med det samlede risikobildet.

3.1 Suksesskriterier for et effektivt arbeid med leverandøroversikt

Uavhengig av valgt løsning for videre vedlikehold av leverandøroversikten er det noen forhold som har betydning for at den videre prosessen blir god. Den første er at prosessen må tilfredsstille regulatoriske krav, herunder krav fra EU, som for eksempel NIS-direktivene. Dette er i stadig endring og må monitoreres fortløpende.

Fra spørreundersøkelsen ble det stilt spørsmål om svarene inneholdt kraftsensitiv informasjon. Om lag halvparten av respondentene svarte positivt på dette. Flere respondenter ønsket ikke å svare på spørreundersøkelsen på grunn av dens format. Dette vitner om sikkerhetsbevissthet i kraftbransjen, men også at man må ta høyde for hvordan man skal løse informasjonsinnhenting for vedlikehold av oversikten. Innhenting av informasjon om leverandører må gjøres slik at dette ikke utgjør en sårbarhet i seg selv, og at kraftbransjen har tillit til eieren av oversikten.

Ut over at leverandøroversikten må samsvare med NVEs behov, bør det videre arbeidet med implementering og vedlikehold ta utgangspunkt i virksomhetenes perspektiv. Virksomheter i KBO er pålagt å opprettholde en oversikt over leverandører. Likevel bør NVE tydeliggjøre hensikten med, og behovet for, en samlet leverandøroversikt i sin kommunikasjon til virksomhetene. Ved å synliggjøre synergieffektene ved deling av informasjon, øker verdien av løsningen for brukerne som igjen bidrar til oppslutningen. Det er vurdert som viktig å senke terskelen for bidrag ved å gjøre det enkelt og lite ressurskrevende for brukerne å bidra til oversikten. Dette kan gjøres ved å bruke kjente systemer og standardiserte rammeverk.

3.2 Prosess for vedlikehold

Basert på arbeidet og kjennskap til markedet beskrives noen forslag til løsninger for hvordan oversikten over leverandører kan vedlikeholdes og videreutvikles. Dette vil i noen grad henge sammen med eierskap og ansvar, noe som behandles i neste kapittel. Løsningsforslagene som beskrives her er tenkt å kunne løses av flere aktuelle eiere og ansvarlige. Aktuelle løsninger

består av en kombinasjon av; aktuelle kilder, verktøy, plattform og en gjennomføringsansvarlig. I tabellen nedenfor synliggjøres konseptuelt ulike alternativer innenfor hver kategori.

Kilde	**Verktøy/virkemiddel**	**Plattform**	**Gjennomføring**
Åpne kilder	Meldeplikt	Standard kontorstøtte applikasjoner som regneark	(Eksternt) konsulenthus
Regnskaps- system, eller ERP, SCM eller tilsvarende	Intervjuer	Hyllevare applikasjoner fra tredjepart	Eksisterende aktør innen kraftbransjen
Manuell innrapportering fra selskap	Spørreskjema	Egenutviklet plattform på egen teknologi stack	NVE
Virksomhetens eller tredjeparts risiko- og sårbarhetsanalyser	E-post	Eksisterende leverandørportal	KraftCERT
Leverandørers og kunders hjemmesider eller sosiale medier.	Ettersyn hos kraftprodusent	Eksisterende offentlige register eller rapporterings- løsninger	Etablering av ny aktør for formålet
Nettverks- monitorering eller kartlegging	Henvisninger		
Offentlige registre	Konsesjonssøknader		
Eksisterende leverandørportaler			

Tabellen over er ikke uttømmende, men gir en rekke mulige løsningsforslag ved å kombinere en eller flere alternativer fra hver kolonne. I det påfølgende synliggjøres fire utvalgte alternativer som fremstår som de mest relevante.

3.3 Løsningsalternativ 1 - nullalternativet med forbedringer

Alternativ 1 er nullalternativet og en videreføring av arbeidet som er gjort i prosjektet. Oversikten er utviklet basert på en kombinasjon av informasjon fra informanter, spørreundersøkelse og åpne kilder. Den er sammenstilt i standard kontorstøtteverktøy ved bruk av regneark. Arbeidet er i dette tilfellet gjennomført av en tredjepart på vegne av NVE, og må vedlikeholdes og eventuelt videreutvikles manuelt.

Styrken med en slik løsning er at den er teknisk enkel å vedlikeholde og det er mulig å heve kvaliteten for hver gjennomføring. Arbeidet kan videreføres uten andre avhengigheter og ressursbruken er begrenset til timebruk. Den legger videre til rette for skjønnsmessige vurderinger fra alle involverte parter.

Svakheten er at den ikke direkte forenkler jobben for virksomhetene. Datanormalisering må gjøres manuelt, noe som er tidkrevende. Løsningen vil trolig ikke gi en fullstendig oversikt over alle leverandører. Videre er berikelse med data fra andre kilder tidkrevende dersom det ikke automatiseres.

3.4 Løsningsalternativ 2 - kjøp av løsning fra tredjepart

Prosessen med å etablere oversikt over leverandører har mye til felles med prosesser som er vel etablerte som pålagt rapportering innen bærekraft eller sektorspesifikke eksempler som finanssektoren med sine strenge krav til undersøkelser og rapportering på Anti-Money Laundering (AML). I disse prosessene er berørte virksomheter pålagt å avklare både eierskap og interesser, samt om sanksjonerte entiteter er involvert eller godtgjøres.

Flere leverandører leverer i dag en teknologisk løsning for å ivareta kravene i åpenhetsloven. Løsningen baserer seg typisk på rapportering via e-post og systematisering av den innrapporterte informasjonen. Denne typen teknologisk løsning er kun et hjelpemiddel for å innhente og systematisere informasjonen. Jobben gjøres av selskapet selv ved at leverandørlister lastes opp i systemet, så sendes e-post ut til opplastede leverandører, med oppfordring om å videresende til eventuelle underleverandører. Deretter skal leverandørene besvare en rekke spørsmål som mappes opp mot ulike risikoparametere. Deretter kan kunden se informasjonen systematisert i et dashboard som synliggjør hvilke leverandører som har forhøyet risiko og burde følges opp manuelt i ettertid.

Styrken med en slik løsning er at store mengder informasjon innhentes relativt enkelt, og kunden trenger ikke gjøre en stor manuell jobb for å nå ut til en stor gruppe respondenter. Det er også en styrke at systemet synliggjør hvilke leverandører som ikke har besvart undersøkelsen, og kunden kan da enkelt følge opp disse leverandørene manuelt.

Svakheten med løsningen er at løsningen baserer seg på tillit og at leverandørene står fritt til å svare som de vil. Selv om man vil anta at informasjonen man får inn er korrekt, kan man ikke være helt sikker på om leverandøren har vært ærlig. Spesielt om det er kritiske spørsmål rundt sikkerhet og/eller compliance.

3.5 Løsningsalternativ 3 - utvikling av egen skreddersydd løsning

Alternativ 3 er utvikling av egen skreddersydd løsning. Et slikt arbeid kan gjøres både av interne ressurser hos den som blir satt til å forvalte løsningen, gjennom bruk av eksterne ressurser som eksempelvis konsulenter, eller en kombinasjon av de to. Løsningen kan være en komplett egenutviklet løsning for datainnsamling, normalisering, berikelse ved bruk av andre kilder, analyse og presentasjon. Alternativt kan man benytte hyllevare og kombinere to eller flere applikasjoner for å lage en integrert løsning for prosessen.

Styrken ved en slik løsning er at den kan være spesialtilpasset NVE og virksomhetenes behov. Videre vil den kunne integreres tett med andre løsninger som anvendes av NVE og virksomhetene.

Avhengig av ambisjonsnivå er denne jobben potensielt omfattende og kan kreve utvikling av egne integrasjoner for å etablere ønsket funksjonalitet. Ulempen er at en slik løsning vil kreve oppdateringer og vedlikehold over tid, som igjen stiller krav til ressurser og prioritering.

3.6 Løsningsalternativ 4 - utvide offentlig rapportering og register

Alternativ 4 er implementering av en innrapporteringsløsning, men til forskjell fra alternativ 2 bygger denne løsningen på et eksisterende system eller offentlig register som for eksempel Altinn, Statistisk sentralbyrå eller Brønnøysundregisteret. Slik kan eksempelvis ERP eller

økonomisystemer også integreres mot rapporteringsprosessen, og benytte data direkte fra hovedbok, som inneholder viktige deler av rapporteringen.

Styrken med denne løsningen er at den integreres tett med eksisterende pålagt rapportering, på tvers av sektor og rapporteringsområder. Videre vil løsningen kunne gi svært detaljert informasjon om leverandører og omfang basert på informasjon fra regnskapssystem og hovedbok. Løsningen har potensial til å være enkel å benytte.

Svakheten er at den krever aksept og tett samarbeid med eksterne aktører. Videre kan det være betenkeligheter knyttet til overrapportering og behandlingsgrunnlag for denne mengden detaljert data fra virksomhetene. Det kan videre være en utfordring med håndtering av kraftsensitiv informasjon på slike plattformer.

3.7 Oppsummering av løsningsforslag

NVE som tilsynsmyndighet og veiledende organ har behov for en oversikt over viktige leverandører for å kunne gi gode sikkerhetsråd til kraftbransjen. Per nå er ikke leverandører omfattet av kraftberedskapsforskriften, men det er ikke utenkelig at dette kan skje i fremtiden. Leverandører besitter ikke bare kraftsensitiv informasjon, men de er også kritiske for selve forsyningssikkerheten av strøm.

Dette prosjektet etablerer en oversikt over viktige leverandører og skal ikke implementere teknologiske løsninger. Forslag til måter å vedlikeholde oversikten på er ikke uttømmende, men gir et representativt utvalg av konseptuelt forskjellige måter å løse oppgaven på.

NVE bør legge ambisjonen på et høyere nivå enn det som er beskrevet som alternativ 1. En løsning utover standard kontorprogramvare, og med mulighet for integrasjoner, en høyere grad av automatisering og visualisering, vil trolig være et godt bidrag til å bedre oversikten og med det sikkerhetsnivået i kraftsystemet. Alternativ 4 vil trolig kreve mye ressursbruk og vil dermed ikke gi ønsket kost/nytte forhold før etter noe tid og modning i resten av sikkerhetsarbeidet i kraftsektoren.

Alternativ 2 eller 3 fremstår dermed som de mest relevante og bør derfor utgjøre et målbilde for hvorledes prosessen kan innrettes over tid. Frem til endelig beslutning er tatt og annen løsning er implementert, anbefales det at NVE bruker og videreutvikler leverandøroversikten.

4 Ansvar og eierskap

I workshop ble det gjennomført en "brainstorming"-øvelse hvor potensielle eiere av en leverandøroversikt ble fremmet, samt fordeler og ulemper ved de ulike potensielle eierne foreslått. Etter brainstormingen stemte deltakerne på hvem de selv mente var best egnet til å eie leverandøroversikten. Det er viktig å presisere at dette var en øvelse og at det som fremkom her ikke nødvendigvis er "fasit". Under vil vi komme inn på hvilket ansvar det innebærer å være eier av leverandøroversikten. Videre vil vi gå gjennom potensielle eiere i rekkefølgen etter hvem som fikk flest stemmer under øvelsen.

4.1 Ansvar

Ansvaret for kraftforsyningen i Norge er tillagt Olje- og energidepartementet, og det operative ansvaret er delegert til NVE som beredskapsmyndighet iht. energiloven kapittel 9.

Kraftforsyningsberedskapen er organisert gjennom Kraftforsyningens beredskapsorganisasjon og inkluderer kraftprodusenter, nettselskaper og andre med klassifiserte anlegg. Ansvaret er tydelig plassert hos NVE, samtidig som det er mulig for NVE å pålegge andre roller i oppdraget.

4.2 Aktuelle eiere av leverandøroversikten

4.2.1 NVE

Riksrevisjonen påpekte i sin rapport at NVE på rapporteringstidspunktet ikke hadde tilstrekkelig oversikt til å oppfylle sitt pålagte ansvar. NVE har myndighet til å pålegge andre KBO-enheter å vedlikeholde og drifte en slik oversikt. Det vil likevel være NVE som eier oversikten og sitter med det endelige ansvaret.

Fordelene ved at NVE eier leverandøroversikten er at de har mye tillit i kraftbransjen og er markedsnøytrale. I tillegg har de tilgang på informasjon fra revisjoner og tilsyn, og kan lagre sensitiv informasjon. NVE jobber også med utvikling av databaser og oversikt over alt annet i kraftforsyningen. Om NVE skal eie leverandøroversikten vil den også få en direkte kobling til NVE beredskap og dens funksjonalitet og bruksområdet vil kunne utvides.

Ulempene med NVE som eier av leverandøroversikten er at arbeidet er prisgitt politiske endringer og tildelinger. Dette er forhold som kan påvirke om NVE har tilstrekkelig med ressurser

til å arbeide med kontinuerlig utvikling av oversikten. Det kan være en mulig interessekonflikt mellom oppgavene som tilsynsmyndighet og veileder, ved at objektiviteten kan utfordres. Dette gjelder i så fall alle områder av kraftforsyningsberedskapen, og ikke bare leverandøroversikten.

4.2.2 KraftCERT

KraftCERT har per nå ikke en fullstendig oversikt over alle leverandører i kraftbransjen. KraftCERT sin oversikt over leverandører er basert på leverandørenes egen rapportering av sårbarheter i ulike systemer. Basert på disse varslene vurderer KraftCERT hvorvidt deres medlemmer har de ulike systemene. Denne praksisen gir ingen fullstendig leverandøroversikt, og usikkerheten som oppstår som følge av dette utgjør en sårbarhet i kraftbransjen.

Fordeler med KraftCERT som eier av leverandøroversikten er at de har leverandører som medlemmer, er non-profit, og er sikkerhetsfokuserte. Dette er en privat organisasjon forankret i kraftforsyningen og som har tillit. En leverandøroversikt vil utvide en eksisterende tjeneste og har en naturlig sammenheng med sikkerhetsvarsler.

Ulempen ved KraftCERT som eier av leverandøroversikten er at det potensielt utfordrer deres nøytralitet. Eierskap, drift og vedlikehold av leverandøroversikten kan forstås som en myndighetsoppgave, ved at den benyttes i NVEs ettersyn med kraftberedskapsorganisasjonen. Denne problemstillingen er nok mer prinsipiell enn praktisk, og er for øvrig lik for NVE. Dermed er det uproblematisk at en aktør sitter på informasjon om hvilke selskaper i kraftbransjen som benytter hvilke leverandører, og som potensielt har sårbarheter og rapporterer informasjonen til tilsynsmyndigheten.

4.2.3 Andre organisasjoner som ble vurdert som eiere

En rekke andre virksomheter ble vurdert i prosessen og vurdert mer eller mindre hensiktsmessig. Enkelte av disse nevnes ved navn under, mens andre kun refereres til i samme kategorier.

ElBits ble vurdert som eier av oversikten fordi de er heleid av kraftbransjen. Potensielle ulemper med ElBits som eier er at det er et relativt nytt selskap og en kommersiell aktør. REN ble også foreslått da de allerede er etablert som beredskapsselskap, men det stilles spørsmål ved om de er nøytrale nok, om de har erfaringen med denne typen oversikter, samt at de er en kommersiell aktør. Statnett har allerede nøytrale myndighetsoppgaver og kunne vært en potensiell eier. I et ressursperspektiv ville det i stor grad være en omfordeling av penger fra NVE, slik at det gir mest mening om NVE da eier oversikten selv.

Et rullerende anbud ble også diskutert, men få fordeler kom til syne ved denne løsningen. Argumentet mot rullerende anbud er faren for at ansvaret for kvalitet og relevans i oversikten kan forvitre.

Videre ble flere andre kategorier eiere vurdert. Dette strekker seg fra departementer, til eksisterende bransjeorganisasjoner og diverse offentlige instanser ble bragt opp, men ble relativt raskt vurdert som mindre aktuelle.

4.3 Oppsummering ansvar og eierskap

Det fremstår naturlig at NVE må eie leverandøroversikten ettersom de både er gjort ansvarlige gjennom lov, samtidig som leverandøroversikten er et viktig verktøy for både ettersyn og veiledning. Samtidig er det mulig å effektivisere arbeidet gjennom økt utveksling av informasjon mellom NVE, KraftCERT og virksomhetene.

5 Drøfting og anbefaling

NVE har gjennom dette arbeidet fått etablert en oversikt over de mest sentrale leverandørene i kraftforsyningen. Oversikten er fremkommet gjennom bruk av kvalitative metoder som workshop og intervjuer, samt kvantitative metoder som spørreundersøkelser og gjennomgang av åpne kilder. Leverandøroversikten danner et godt utgangspunkt for videre arbeid i det som må etableres som en kontinuerlig prosess.

Videre er mulige måter å implementere og videreutvikle leverandøroversikten på i fremtiden vurdert, samt hvem som bør være eier av oversikten og hvem som kan bidra til å forvalte denne. Det er gjort en gjennomgang av kriterier som kan bidra til at en implementering blir vellykket, på en slik måte at det til enhver tid eksisterer en oppdatert oversikt over leverandører i sektoren.

Forståelse for behovet for oversikt over leverandører ser ut til å være godt etablert, både på det utøvende nivået og det kontrollerende nivået. Ambisjonsnivået er imidlertid åpent for diskusjon, da det kan strekke seg fra en enkel liste over leverandører på et overordnet nivå, til en fullstendig oversikt over individuelle komponenter, leverandører og brukere, sammen med kontekstuell informasjon fra andre offentlige kilder. For virksomhetene vil sistnevnte være en naturlig del av god informasjonssikkerhet som krever detaljert oversikt over egne informasjonsverdier og systemer (som beskrevet i NSMs grunnprinsipper). For NVE som kontrollerende nivå kan en aggregert leverandøroversikt være tilstrekkelig. Vurderingen av betydning krever mer detaljert informasjon nødvendig.

For å svare ut Riksrevisjonens funn er det nødvendig å gå ned i detaljene på de ulike IT-, OT- og sikkerhetsleverandørenes arbeid med informasjonssikkerhet og kvalitetssikre dette. Vår anbefaling er at NVE legger til rette for økt samhandling på dette området, men ikke nødvendigvis påtar seg noen rolle i det utøvende arbeidet. Virksomhetene er gjennom kraftberedskapsforskriften pålagt å følge opp egne leverandører, de virksomheter som ikke er underlagt forskriften bør videre motiveres til å føre tilsvarende oversikt over egne leverandører, samt årlig rapportere inn sine leverandører til NVE. NVEs rolle i dette er primært å følge opp arbeidet og ansvarliggjøre virksomhetene. NVEs oversikt bør således være aggregert informasjon fra de ulike aktørene i kraftbransjen.

5.1 Oppsummering og anbefalinger

Det er gjennom arbeidet blitt tydelig at det er NVE som har ansvaret og bør eie leverandør-oversikten for kraftbransjen. Ansvar og eierskap er ikke ensbetydende med at arbeidet med videreutvikling og forvaltning må gjøres av NVE alene, men kan støttes av tredjeparter som tidligere beskrevet. Arbeidet viser at NVE på kort sikt bør videreføre arbeidet med leverandøroversikten i sin nåværende form, mens NVE på lang sikt bør videreutvikle leverandøroversikten enten gjennom implementering av ny, eller ved kjøp av tilpasset løsning fra tredjepart. Dette er beskrevet som løsningsalternativ 2 og 3. Mer utfyllende fremmes følgende anbefalinger basert på arbeidet:

- NVE bør eie leverandøroversikten, men samtidig være tydelig på virksomhetenes selvstendige ansvar for egne leverandører. NVE bør jobbe tett med virksomhetene generelt og KraftCERT spesielt for å videreutvikle oversikten.
- NVE bør på kort sikt videreføre arbeidet med leverandøroversikten i sin nåværende form
    - NVE bør anbefale Business Impact Analysis som som rammeverk for denne delen av sikkerhetsarbeidet.
    - NVE bør tilby enkle rammeverk og formater for å øke informasjonsutveksling og forenkle jobben med sammenstilling.
    - NVE bør integrere informasjon som fremkommer i tilsynsarbeidet for å kvalitetssikre og oppdatere leverandøroversikten.
    - Data fra tidligere gjennomførte tilsyn og konsesjonssøknader integreres i leverandøroversikten i størst mulig grad.
    - Informasjon om informasjonssikkerhetsarbeidet leverandørene bør legges til.
    - Kriteriene for hvilke leverandører som vurderes som viktig, og hvilke leverandører som tilfredsstiller disse, må revisiteres jevnlig.
    - Ytterligere analyse og visualisering av data i oversikten kan bidra til ny innsikt i leverandørmarkedet som ikke allerede er allment kjent.
- NVE bør på sikt jobbe for å videreutvikle leverandøroversikten enten gjennom implementering av ny, eller ved kjøp av tilpasset løsning fra tredjepart.
    - Gjennom å bygge erfaring med leverandøroversikten vil kravstilling og prioritering av ressurser til arbeidet bli enklere.
    - Løsningen bør legge til rette for økt informasjonsdeling mellom virksomhetene i kraftbransjen.

6 Vedlegg - tilleggsmateriale

6.1 Gjennomføring av prosjektet

Prosjektet er gjennomført av PwC på vegne av NVE. PwC har hatt runder internt med ressurser som har god kjennskap til kraftsektoren, samt aktører i kraftbransjen. Dette har vært nøkkelpersoner fra både NVE, KraftCERT og andre selskaper som enten jobber med IT-sikkerhet i kraftbransjen eller som jobber tett med leverandører.

For å etablere en oversikt over de viktigste IT-, OT- og IT-sikkerhetsleverandørene til kraftforsyningen er det viktig å skape konsensus rundt noen faktorer for vurdering av leverandører. PwC gjennomførte en workshop sammen med NVE for å komme frem til noen faktorer som indikerer at en leverandør er viktig. Disse faktorene ble tatt med i videre intervjurunder, samt presentert for KBO-enhetene i en spørreundersøkelse som ble utsendt. Denne spørreundersøkelsen ble sendt til KBO-enhetene mot slutten av prosjektet for å kvalitetssikre og supplementere allerede innsamlet data. Basert på kontaktinformasjon fra NVE sendte PwC spørreundersøkelsen til totalt 126 selskaper. Antall respondenter endte på 35.

Etter at intervjuene og workshops var gjennomført, og spørreundersøkelsen besvart, ble innhentet data fremstilt i en oversikt over leverandører i kraftforsyningen.

Videre ble det gjennomført en til workshop sammen med NVE for å utarbeide en arbeidsprosess for vedlikehold av leverandøroversikten, samt diskutere hvem som skulle ha ansvar for dette.

6.2 Oversikt over møter og møtedeltakere

Møte	Deltakere	Dato
Oppstartsmøte	PwC og NVE	17. april 2023
Intern kartlegging (PwC)	PwC	10. mai 2023
Intern kartlegging (PwC)	PwC	23. mai 2023

Workshop leverandørkartlegging	PwC og NVE	24. mai 2023
Samtale med KraftCERT	PwC og KraftCERT	2. juni 2023
Samtale Validér	PwC og Validér	12. juni 2023
Samtale Nettalliansen	PwC og Nettaliansen	13. Juni 2023
Workshop arbeidsprosess	PwC, NVE og utvalgte aktører i sektor	15. juni 2023
Samtale om Achilles registrering	PwC	29. Juni 2023
Samtale NC-Spectrum	PwC og NC-Spektrum	21. August 2023
Forankringsmøte med gjennomgang av foreløpige funn	PwC og NVE	28. September 2023
Avslutningsmøte med overlevering av rapport til NVE	PwC og NVE	20. Oktober 2023

6.3 Datakilder og formater

For å kunne kartlegge de viktigste leverandørene av IT, OT og IT-sikkerhet var det i første omgang nyttig å få et innblikk i hvilke kilder og formater kraftbransjen selv bruker for å tilegne seg informasjon om ulike leverandører. Det ble derfor i en workshop sammen med NVE gjennomført en øvelse for å kartlegge hvor informasjon om leverandører i kraftindustrien finnes. I tillegg fikk vi supplerende svar fra spørreundersøkelsen som ble sendt ut til alle KBO-enhetene.

Selskaper i kraftbransjen sitter på mye informasjon om leverandørene da mange har faste leverandører de har samarbeidet med i mange år. I tillegg er det vanlig å samarbeide med andre

selskaper, danne allianser eller være en del av bransjeorganisasjoner. Dette kan for eksempel være Nettalliansen, Fornybar Norge eller Distriktsenergi. På denne måten kan selskapene dele erfaringer og informasjon om leverandører med hverandre. Det er også vanlig å kontakte leverandørers referanser, altså andre kunder i kraftbransjen.

Når NVE etterspør lister over leverandører som underlag til tilsyn, er det deres erfaring at dette er noe som blir laget der og da, og at disse listene ikke er fullstendige. En slik oversikt er svært viktig for selskapene selv da f.eks. en beredskapshendelse kan skape spørsmål om hvem som skal involveres.

Bruk av åpne kilder er også en metode for å tilegne seg informasjon om leverandører. Dette kan for eksempel være gjennom nettsider som proff.no, Brønnøysundregistrene, US sanctions list eller tilbudsdatabaser som Doffin. Man kan også tilegne seg denne informasjonen gjennom tjenester levert av eksempelvis Dun & Bradstreet, Holte Smartkalk og Factlines AS. Leverandørnettverk, som Achilles og Sellihca, er også vanlig. Achilles drifter Utilities Nordics & Central Europe (UNCE), en EU-godkjent kvalifiseringsordning og et leverandørregister for hele den nordiske og sentraleuropeiske energibransjen. Achilles sin løsning slik den fremkommer medio 2023 ser ikke ut til å gi nødvendig informasjon i denne sammenheng. Eksempler på andre former for åpne kilder kan være deltakeroversikter fra bransje- organisasjoner og konferanser, Konkurransetilsynet og Foretaksregisteret.

KraftCERT sitter også på mye informasjon, men dette er varslingsbasert og generer ikke en fullstendig oversikt over leverandører. Sårbarhetsvarsler er omfattende og vil ikke nødvendigvis være dekkende.

I mange tilfeller er det mulig å tilegne seg informasjon gjennom leverandørene selv gjennom deres egenvurderinger eller leverandørpresentasjoner. Mange selskaper i kraftbransjen inngår også egne informasjonssikkerhetsavtaler med leverandører, og det gjennomføres risikovurderinger eller tredjepartsvurderinger av leverandør.

6.4 Svar fra spørreundersøkelsen

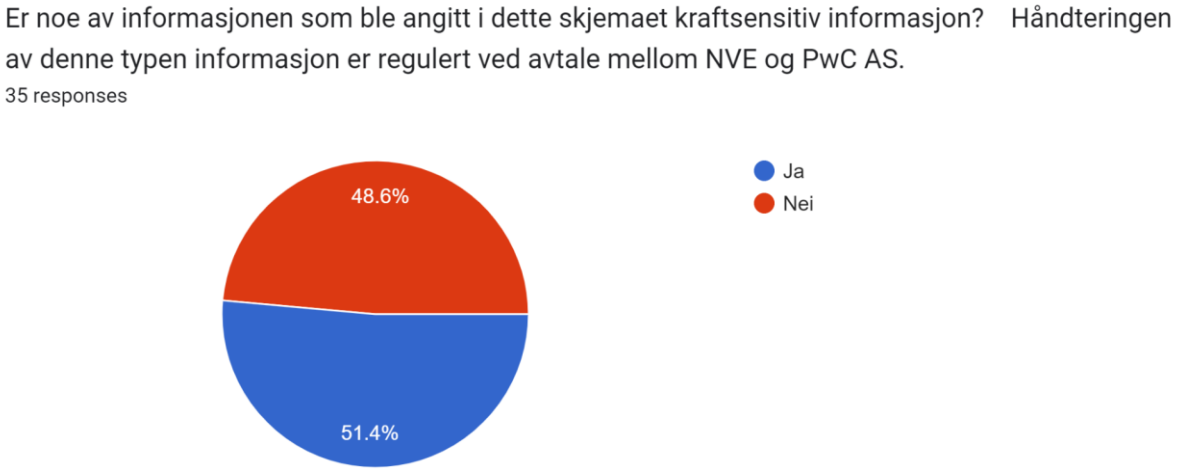

Fig. 3: Resultatet fra spørsmål om respondenter oppga kraftsensitiv informasjon i spørreundersøkelsen.

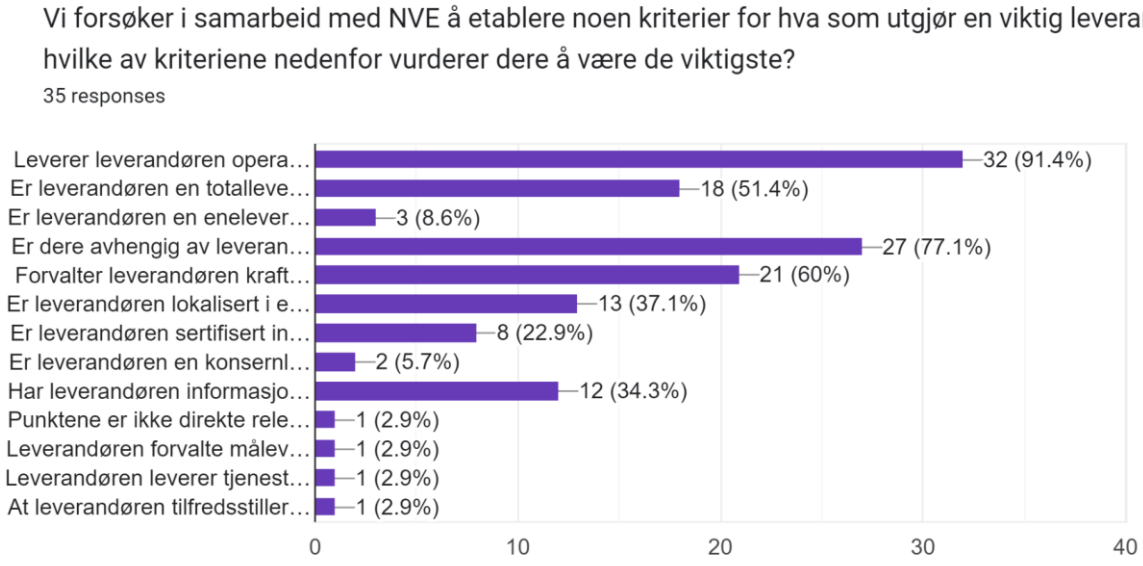

Fig. 4: Resultater fra spørreundersøkelse om viktigste faktorer for vurdering av leverandør.

NVE

Norges vassdrags- og energidirektorat

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