Riksrevisjonen

Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen

Dokument 3:7 (2020–2021)

Forsidefoto: Maksim Kabakou (t.v) og PÃ©ter Gudella/Scandinavian Stockphoto

ISBN-978-82-8229-504-8

Til Stortinget

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

Dokumentet har følgende inndeling:

- Konklusjoner, Utdyping av konklusjoner, Anbefalinger, Statsrådens svar og Riksrevisjonens uttalelse til statsrådens svar
- Vedlegg 1: Riksrevisjonens brev til statsråden i Olje- og energidepartementet
- Vedlegg 2: Statsrådens svar
- Vedlegg 3: Forvaltningsrevisjonsrapport med vurderinger

Riksrevisjonen benytter følgende begreper for kritikk, med denne rangeringen etter høyest alvorlighetsgrad:

1. **Svært alvorlig** brukes ved forhold der konsekvensene for samfunnet eller berørte borgere er svært alvorlige, for eksempel risiko for liv eller helse.
2. **Alvorlig** benyttes ved forhold som kan ha betydelige konsekvenser for samfunnet eller berørte borgere, eller der summen av feil og mangler er så stor at dette må anses som alvorlig i seg selv.
3. **Sterkt kritikkverdig** angir forhold som har mindre alvorlige konsekvenser, men gjelder saker med prinsipiell eller stor betydning.
4. **Kritikkverdig** brukes for å karakterisere mangelfull forvaltning der konsekvensene ikke nødvendigvis er alvorlige. Dette kan gjelde feil og mangler som har økonomiske konsekvenser, overtredelse av regelverk eller saker som er tatt opp tidligere og som fortsatt ikke er rettet opp.

Riksrevisjonen, 23. mars 2021

For riksrevisorkollegiet

Per-Kristian Foss
riksrevisor

Innhold

Olje- og energidepartementet

Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen

Kraftforsyningen er en sentral del av Norges kritiske infrastruktur, og tilgang på elektrisk kraft blir stadig viktigere for å kunne opprettholde normal aktivitet i samfunnet, sikre kritiske samfunnsfunksjoner i krise-situasjoner og opprettholde landets forsvarsevne under beredskap og i krig.

Bruk av ny teknologi, skyløsninger og utenlandske leverandører og integrering av ulike systemer som er koblet til internett øker risikoen for IKT-hendelser i kraftforsyningen. Ifølge nasjonale trusselvurderinger utgjør systemer i kraftsektoren kritisk infrastruktur som er spesielt utsatt for etterretning og avanserte nettverksoperasjoner.

Olje- og energidepartementet skal legge til rette for sikker kraftforsyning gjennom god beredskap og har delegert viktige beredskapsoppgaver til Norges vassdrags- og energidirektorat (NVE). Et av NVEs viktigste mål er å fremme en sikker kraftforsyning. Sikkerhet i kraftforsyningens IKT-systemer er et av flere sentrale områder som skal bidra til å opprettholde en stabil og sikker kraftforsyning. NVE skal påse at beredskapen i kraftforsyningen er god og i tråd med gjeldende krav.

De viktigste selskapene i kraftforsyningen er med i Kraftforsyningens beredskapsorganisasjon (KBO). KBO består av NVE og virksomheter som står for kraftforsyning, som større kraftprodusenter, nettselskaper og fjernvarmeselskaper. KBO-enhetene er underlagt energiloven og kraftberedskapsforskriften, som stiller krav til selskapenes arbeid med IKT-sikkerhet. Kraftberedskapsforskriften ble revidert med virkning fra 1. januar 2019, men også den tidligere forskriften stilte strenge krav til IKT-sikkerheten i kraftforsyningen. Den 1. januar 2019 ble NVE utpekt som sektorvist responsmiljø for å koordinere og håndtere IKT-sikkerhetshendelser i kraftforsyningen. KraftCERT AS har fra 2019 utført enkelte oppgaver innenfor varsling, informasjonsdeling og analyse av IKT-sikkerhetshendelser for å støtte NVE som sektorvist responsmiljø. KraftCERT ble opprettet av store aktører i kraftforsyningen i 2014 for å hjelpe medlemsselskapene med å forebygge og håndtere IKT-sikkerhetshendelser.

Målet med Riksrevisjonens undersøkelse har vært å vurdere i hvilken grad NVEs virkemiddelbruk bidrar til å styrke IKT-sikkerheten i kraftforsyningen. Undersøkelsen omfatter perioden 2016–2020 og tar blant annet utgangspunkt i følgende vedtak og forutsetninger fra Stortinget:

- Energiloven av 29. juni 1990 og kraftberedskapsforskriften av 1. januar 2013, sist endret 1. januar 2019
- Prop. 1 S fra Olje- og energidepartementet i perioden 2016–2020 med tilhørende innstillinger
- Meld. St. 25 (2015–2016) *Kraft til endring – Energipolitikken mot 2030*, jf. Innst. 401 S (2015–2016)
- Meld. St. 38 (2016–2017) *IKT-sikkerhet – Et felles ansvar,* jf. Innst. 187 S (2017–2018)
- reglement for økonomistyring i staten og bestemmelser om økonomistyring i staten fastsatt 12. desember 2003 med endringer, senest 5. november 2015

Rapporten ble forelagt Olje- og energidepartementet ved brev 16. desember 2020. Departementet har i brev 26. januar 2021 gitt kommentarer til rapporten. Kommentarene er i hovedsak innarbeidet i rapporten og i dette dokumentet.

1 Konklusjoner

- NVE har ikke i tilstrekkelig grad påsett at det er god beredskap for å håndtere IKT-angrep i kraftforsyningen:
  - NVEs styring og oppfølging av arbeidet med IKT-sikkerhet i kraftforsyningen er svak.
  - Det er svakheter ved NVEs tilsyn med IKT-sikkerhet i kraftforsyningen.
  - NVE har skjerpet kravene til IKT-sikkerhet i kraftforsyningen, men ikke fulgt opp med tilstrekkelig veiledning.
  - Det er svakheter ved NVEs arbeid med overvåking, varsling og beredskap ved IKT-hendelser.

- Oppfølgingen av leverandørene er mangelfull til tross for at de har stor betydning for IKT-sikkerheten i kraftforsyningen.
- Olje- og energidepartementet sikrer seg ikke god nok styringsinformasjon om IKT-sikkerhetstilstanden i kraftforsyningen og resultatene av NVEs arbeid med IKT-sikkerhet i kraftforsyningen.

2 Utdyping av konklusjoner

2.1 NVE har ikke i tilstrekkelig grad påsett at det er god beredskap for å håndtere IKT-angrep i kraftforsyningen

Samfunnet er avhengig av sikker forsyning av kraft for å opprettholde sine funksjoner og virksomheter. Et IKT-angrep som fører til svikt i strømforsyningen, kan få alvorlige konsekvenser for alle samfunnssektorer og digitale systemer som samfunnet er avhengig av. Selskapene i kraftforsyningen har ansvar for at IKT-sikkerheten er i tråd med regelverket. Undersøkelsen viser at det har vært avdekket svakheter i flere av selskapenes arbeid med IKT-sikkerhet, og at det er en økende risiko for at IKT-angrep kan ramme kraftforsyningen. Dette viser at NVEs arbeid med å styrke og kontrollere IKT-sikkerheten i kraftforsyningen er viktig. NVE skal påse at beredskapen i kraftforsyningen er god og i tråd med gjeldende krav i lover og forskrifter. NVEs virkemidler er i hovedsak regelverksutvikling, veiledning, tilsyn, kompetansehevende tiltak og arbeid med overvåking, varsling og beredskap ved IKT-hendelser. Undersøkelsen viser at NVE har skjerpet kravene til IKT-sikkerhet i kraftforsyningen og styrket systemet for å dele informasjon om trusler, sårbarheter og IKT-sikkerhetshendelser mellom aktørene i kraftforsyningen. Samtidig viser undersøkelsen at det er flere svakheter ved NVEs arbeid med IKT-sikkerheten i kraftforsyningen, både når det gjelder tilsyn og veiledning og arbeidet med overvåking, varsling og beredskap ved IKT-hendelser. Funnene beskrives nærmere nedenfor. Etter Riksrevisjonens samlede vurdering er det alvorlig at NVE ikke i tilstrekkelig grad har påsett at det er god beredskap for å håndtere IKT-angrep i kraftforsyningen.

2.1.1 NVEs styring og oppfølging av arbeidet med IKT-sikkerhet i kraftforsyningen er svak

Riksrevisjonen mener det er kritikkverdig at NVE samlet sett har svak styring og oppfølging av arbeidet med IKT-sikkerhet i kraftforsyningen, noe som har ført til svakheter i gjennomføringen av sentrale oppgaver som tilsyn, veiledning og arbeidet med overvåking, varsling og beredskap ved IKT-hendelser. Etter Riksrevisjonens vurdering har ikke NVE sørget for at det er nok ressurser til å ivareta dette arbeidet, og de har heller ikke sørget for at de har de verktøyene som trengs for å styre og følge opp arbeidet. Videre er NVEs grunnlag for å vurdere statusen og utviklingen i IKT-sikkerhetstilstanden i kraftforsyningen etter vår oppfatning mangelfullt. Det vil si at NVE i liten grad har informasjon om resultatene av eget arbeid. Denne informasjonen kunne ha vært brukt til styring og til å iverksette nødvendige tiltak for å nå målet om å fremme en sikker forsyning av kraft uten avbrudd, også i krisesituasjoner.

NVE har ikke sørget for at det er nok ressurser til arbeidet med IKT-sikkerhet i kraftforsyningen

I Meld. St. 25 (2015–2016) *Kraft til endring - Energipolitikken mot 2030* (energimeldingen) framheves det at kompleksiteten i kraftforsyningen har økt, og at økt bruk av IKT gir økt risiko for et høyere antall uønskede IKT-hendelser. For å styrke IKT-sikkerheten i kraftforsyningen må NVE ifølge energimeldingen og Meld. St. 38 (2016–2017) *IKT-sikkerhet – Et felles ansvar* styrke innsatsen, blant annet ved å utvikle regelverket, styrke arbeidet på tilsyns- og veiledningsområdet og stimulere til større og mer ressurssterke fagmiljøer innenfor IKT-sikkerhet. I energimeldingen går det fram at regjeringen setter arbeidet med IKT-sikkerhet høyt og støtter opp om NVEs prioritering av IKT-sikkerhet i kraftsektoren.

I strategier, risikovurderinger og virksomhetsplaner framhever NVE at arbeidet med IKT-sikkerhet i kraftforsyningen er et prioritert område. Omfanget av NVEs oppgaver på området har økt i takt med digitaliseringen. NVEs samlede budsjettmidler har derimot ikke økt i undersøkelsesperioden, så prioriteringen av arbeidet med IKT-sikkerhet i kraftforsyningen må derfor skje gjennom en intern omdisponering av midler. NVE har ikke overfor departementet gitt uttrykk for at de har behov for mer ressurser til dette arbeidet, utover midlene til å dekke oppgaver som er satt ut til KraftCERT.

Arbeidet med IKT-sikkerhet i kraftforsyningen utføres av beredskapsseksjonen under tilsyn- og beredskapsavdelingen i NVE. NVE har økt antall stillinger med IKT-sikkerhetskompetanse i beredskapsseksjonen fra én til tre fra 2016 til 2018. Den reelle kapasiteten i seksjonen har i gjennomsnitt

vært på om lag to årsverk i perioden 2017–2019. Få ansatte med IKT-sikkerhetskompetanse innebærer sårbarhet ved fravær og uforutsette hendelser. NVE har de siste årene brukt mye av kapasiteten på området til å revidere kraftberedskapsforskriften og veilede enkeltselskaper i de nye kravene. Flere av NVEs oppgaver innenfor arbeidet med IKT-sikkerhet i kraftforsyningen har dermed blitt utsatt. Dette gjelder blant annet gjennomføringen av flere IKT-sikkerhetstilsyn, utarbeidelsen av en endelig skriftlig veileder til kraftberedskapsforskriften og avklaringer om et nytt regime for varsling og deling av sårbarheter og IKT-sikkerhetshendelser.

NVE har ikke sørget for at de har de verktøyene som trengs for å styre og følge opp arbeidet med IKT-sikkerhet i kraftforsyningen

Ifølge økonomireglementet skal NVE fastsette mål og resultatkrav og sikre tilstrekkelig styringsinformasjon og beslutningsgrunnlag for å følge opp aktiviteter og resultater av eget arbeid. Et av NVEs hovedmål, som er fastsatt av Olje- og energidepartementet, er å fremme en sikker kraftforsyning. For å nå dette målet skal NVE blant annet påse at beredskapen er god og i tråd med gjeldende krav. NVE skal rapportere om gjennomførte tiltak og hvordan de bidrar til at hovedmålet nås.

Målene som er satt av departementet, gjenspeiles i NVEs strategier og virksomhetsplaner. NVE har ikke operasjonalisert målene og styringsparameterne i vurderingskriterier som kan brukes i styringen og oppfølgingen av arbeidet med IKT-sikkerhet i kraftforsyningen. NVE har heller ikke identifisert hvilken informasjon som er nødvendig for å kunne vurdere IKT-sikkerheten i kraftforsyningen, eller hvordan arbeidet med IKT-sikkerheten bidrar til dette. I årsrapporten rapporterer NVE om gjennomførte aktiviteter og tiltak, men i liten grad om resultater av tiltakene og hvordan de har bidratt til å fremme en sikker kraftforsyning. Det er lite intern rapportering på oppgavegjennomføring og måloppnåelse i NVE gjennom året. NVE gjennomfører heller ikke systematiske evalueringer av eget arbeid som kan brukes i styringen og oppfølgingen av arbeidet med IKT-sikkerhet i kraftforsyningen. NVE evaluerer for eksempel ikke tilsynene systematisk internt for å vurdere om metodikken, gjennomføringen eller tilsynsrutinene kan forbedres.

Virksomhetsplanen til beredskapsseksjonen angir planlagt ressursbruk for en del hovedoppgaver som faller inn under arbeidet med IKT-sikkerhet i kraftforsyningen, som tilsyn og regelverksutvikling. Mange av oppgavene som faller inn under IKT-sikkerhetsarbeidet inngår imidlertid ikke i seksjonens virksomhetsplan, slik at denne ikke viser det reelle ressursbehovet for dette arbeidet. Det oppstår derfor mange oppgaver gjennom året som NVE ikke har planlagt og satt av ressurser til. På grunn av få ansatte med IKT-sikkerhetskompetanse blir mange av de planlagte oppgavene utsatt. NVE har ikke et ressursstyringsverktøy som kan brukes til å sammenligne faktisk ressursbruk med planlagt ressursbruk, og som kan gi erfaringstall i planleggingsarbeidet. Etter Riksrevisjonens vurdering gjør manglende informasjon om ressursbruk til ulike aktiviteter det vanskelig for de ulike ledernivåene å styre og prioritere mellom NVEs mange ulike oppgaver.

NVE har i undersøkelsesperioden ikke hatt IKT-systemer til å dokumentere valg av tilsynstema og tilsynsobjekter. Det har også vært svakheter i NVEs systemer for å sikre at rutiner for gjennomføring av tilsyn blir fulgt, og at avvik som avdekkes, blir fulgt opp. NVE har heller ikke hatt systemer for å sikre at informasjon fra gjennomførte tilsyn systematiseres, slik at den kan brukes ved valg av framtidige tilsyn, regelverksarbeid og veiledning. NVE har nylig tatt i bruk et nytt tilsynssystem som gjør det mulig å forbedre gjennomføringen av tilsyn og oppfølgingen av frister og avvik. Det nye systemet er imidlertid ikke utviklet for å bli brukt i den overordnede planleggingen av tilsynsvirksomheten eller for å dokumentere risikobaserte utvalg av tilsynstema og -objekter. Systemet brukes foreløpig ikke for å systematisere informasjon fra tilsyn til interne analyseformål, men NVE mener det vil bli mulig når systemet har vært i bruk en stund. Når det gjelder IKT-hendelser, rapporterer selskapene til NVE når hendelsene er avsluttet. Denne rapporteringen skal gi NVE informasjon om selskapenes egne evalueringer og erfaringer. NVE registrerer slike hendelser i flere systemer og regneark som er lite tilrettelagt for oppfølging og læring av hendelser, for interne analyseformål eller som grunnlag for valg av tilsynstema og -objekter. Etter Riksrevisjonens vurdering er det svakheter ved NVEs systemer for å planlegge og følge opp tilsyn og for å følge opp rapporterte hendelser. Deler av dette kan bli bedre med det nye systemet.

NVEs grunnlag for å vurdere statusen og utviklingen i IKT-sikkerhetstilstanden i kraftforsyningen er mangelfullt

I henhold til tildelingsbrevet skal NVE årlig gi Olje- og energidepartementet en vurdering av statusen og utviklingen i IKT-sikkerhetstilstanden i kraftforsyningen. NVE har få kilder for å følge med på denne utviklingen. NVE utarbeider årlige overordnede risikovurderinger og har siden 2016 utarbeidet risiko- og sårbarhetsanalyser (ROS-analyser) og tilstandsvurderinger på oppdrag fra departementet. I de overordnede

risikovurderingene trekker NVE fram risikoen for at NVE ikke har tilstrekkelig grunnlag for å vurdere statusen og risikoen i beredskapen og forsyningssikkerheten.

I 2017 og 2019 utarbeidet NVE to tilstandsvurderinger som gir en oversikt over NVEs informasjon om sikkerhetstilstanden. Tilstandsvurderingene er i hovedsak basert på statistikk om gjennomførte tilsyn, innrapporterte hendelser og avbrudd. Undersøkelsen viser at kildene som brukes i tilstandsvurderingene, er mangelfulle og ikke gir et fullstendig bilde av statusen og utviklingen i IKT-sikkerhetstilstanden:

- NVE har gjennomført få IKT-sikkerhetstilsyn, og tilsynsmetodikken avdekker i liten grad den faktiske IKT-sikkerhetstilstanden i selskapene.
- NVEs informasjon om IKT-sikkerhetshendelser er mangelfull.
- Avbruddstatistikken gir i liten grad informasjon om hvorvidt IKT-sikkerheten er tilstrekkelig for å hindre avbrudd i kraftforsyningen i krisesituasjoner.

Etter Riksrevisjonens vurdering er det kritikkverdig at NVEs grunnlag for å vurdere statusen og utviklingen i IKT-sikkerhetstilstanden i kraftforsyningen samlet sett er mangelfullt.

2.1.2 Det er svakheter ved NVEs tilsyn med IKT-sikkerhet i kraftforsyningen

I henhold til energiloven og kraftberedskapsforskriften er NVE ansvarlig for å føre kontroll med at bestemmelsene i loven og forskriften overholdes. Undersøkelsen viser at det er flere svakheter ved NVEs tilsyn med IKT-sikkerhet i kraftforsyningen. NVE har gjennomført få IKT-sikkerhetstilsyn og har en tilsynsmetodikk som i liten grad avdekker den faktiske IKT-sikkerhetstilstanden. Dette svekker NVEs informasjon om selskapenes etterlevelse av regelverket. I tillegg er det svakheter ved NVEs risikovurderinger når de velger tilsynstema og tilsynsobjekter i forbindelse med IKT-sikkerhetstilsyn, noe som kan ha ført til en mindre effektiv og mindre målrettet tilsynsvirksomhet. Riksrevisjonen mener at svakhetene ved NVEs tilsyn med IKT-sikkerheten samlet sett er sterkt kritikkverdige.

NVE har gjennomført få IKT-sikkerhetstilsyn

Det er om lag 170 KBO-enheter i kraftforsyningen. NVE har de siste seks årene gjennomført om lag fem IKT-sikkerhetstilsyn hvert år. I perioden 2017–2019 førte NVE IKT-sikkerhetstilsyn med om lag halvparten av selskapene som har de viktigste driftskontrollsystemene, det vil si systemene som brukes til å styre og overvåke strømforsyningen. NVE har i liten grad gjennomført tilsyn med de øvrige selskapene i kraftforsyningen. Undersøkelsen viser at flere planlagte IKT-sikkerhetstilsyn ble utsatt på grunn av kapasitetsutfordringer. NVE oppgir at de ikke har oversikt over IKT-sikkerheten i selskapene de ikke har ført tilsyn med. Dette innebærer at NVE i undersøkelsesperioden kun har informasjon om IKT-sikkerhetstilstanden fra tilsyn med en liten andel av selskapene i kraftforsyningen.

NVEs tilsynsmetodikk avdekker i liten grad den faktiske IKT-sikkerhetstilstanden i selskapene

NVE har benyttet den samme metodikken for IKT-sikkerhetstilsyn i over ti år. Metodikken NVE bruker, er tillitsbasert og avdekker om selskapene har systemer for internkontroll. Metodikken gir lite informasjon om hvorvidt internkontrollsystemene fungerer i praksis, og om selskapenes IKT-systemer er godt nok sikret. Vi gjennomførte en undersøkelse i tre selskaper av ulik størrelse i bransjen for å finne ut hvordan disse selskapene arbeider med IKT-sikkerhet og implementering av grunnleggende sikkerhetstiltak. Alle de tre selskapene hadde svakheter som selskapenes internkontrollsystemer ikke hadde fanget opp, og som NVE heller ikke avdekket gjennom sine tilsynsmetoder. Etter Riksrevisjonens vurdering avdekker NVE i liten grad den faktiske IKT-sikkerhetstilstanden i selskapene med sin tilsynsmetodikk.

Det er svakheter ved NVEs risikovurderinger ved valg av tema og selskaper til IKT-sikkerhetstilsyn

I St.meld. nr. 19 (2008–2009) *Ei forvaltning for demokrati og fellesskap* går det fram at tilsynsvirksomhet skal ta utgangspunkt i områder der risikoen er størst, og der sjansene for å redusere risikoen er størst. NVE har i sine planer lagt til grunn at tilsynstema og tilsynsobjekter skal velges på bakgrunn av risiko og vesentlighet. Gode risiko- og vesentlighetsvurderinger krever at tilsynsorganet har god kjennskap til området det føres tilsyn med. Det tilsier at det bør ligge systematisk informasjonsinnhenting til grunn for risiko- og vesentlighetsvurderingen.

NVE gjennomfører tilsyn innenfor mange ulike fagområder. Risikobasert planlegging av tilsyn tilsier at NVE skal vurdere hvilke tema det er viktigst å føre tilsyn med. Undersøkelsen viser at NVE ikke dokumenterer begrunnelsen for temaene de velger til tilsynene, eller hvor mange tilsyn de skal gjennomføre innenfor ulike tema. Undersøkelsen viser at valg av tema og antall tilsyn innenfor ulike tilsynstema i stor grad henger

sammen med hvilke ressurser og kompetanse NVE har til rådighet i de ulike seksjonene, og at utvalget ikke baseres på dokumenterte risikovurderinger av alle tilsynstema i NVE. Ettersom NVEs kapasitet på IKT-sikkerhetskompetanse har økt lite i undersøkelsesperioden, har antall IKT-sikkerhetstilsyn heller ikke økt. Dette innebærer at NVE ikke har fulgt opp den overordnede vektleggingen av risikoen for IKT-angrep og prioriteringen av området i etatens strategier og planer med å øke innsatsen innenfor IKT-sikkerhetstilsyn. Etter Riksrevisjonens vurdering har NVE i liten grad basert valg av tilsynstema på risikovurderinger og dermed ikke rettet tilsynene inn mot de områdene der de kunne hatt størst risikoreduserende effekt.

NVE dokumenterer heller ikke begrunnelsen for valg av selskaper til IKT-sikkerhetstilsyn. Undersøkelsen viser at NVE i hovedsak velger ut selskaper basert på frekvens og vesentlighet. Undersøkelsen viser også at NVE har lite kunnskap om svakheter og dermed om indikasjoner på risiko i selskapene. Slik kunnskap kunne ha vært benyttet til å foreta risikobaserte valg av selskaper. Selv om NVE har lite informasjon om IKT-sikkerheten i selskaper de ikke har ført IKT-sikkerhetstilsyn med, får de noen indikasjoner på svakheter i selskapene, for eksempel gjennom tilsyn med andre tema, gjennom direkte kontakt med selskapene i veiledningsarbeidet eller gjennom selskapenes innrapportering av hendelser. Undersøkelsen viser at NVE i liten grad bruker slik informasjon til å velge selskaper til tilsyn. NVE retter tilsynene inn mot selskapene som er viktigst for kraftforsyningen, og der konsekvensene av et IKT-angrep vil være størst. NVE vurderer imidlertid ikke hvilke av selskapene det er størst risiko for å avdekke avvik hos. Etter Riksrevisjonens vurdering har NVE i liten grad samlet inn og systematisert informasjon som indikerer svak etterlevelse i selskapene, og som kunne vært brukt til å velge ut selskaper til tilsyn. Dette kan ha ført til en mindre effektiv og mindre målrettet tilsynsvirksomhet.

2.1.3 NVE har skjerpet kravene til IKT-sikkerhet i kraftforsyningen, men ikke fulgt opp med tilstrekkelig veiledning

NVE har skjerpet kravene til IKT-sikkerhet i kraftforsyningen, men etter Riksrevisjonens vurdering har ikke NVE fulgt opp regelverksendringene ved å tilby selskapene tilstrekkelig veiledning. Riksrevisjonen mener det er positivt at NVE har arbeidet med kompetanseutvikling både internt og for bransjen, men oppfatter at mangelen på IKT-sikkerhetskompetanse fortsatt er en stor utfordring for IKT-sikkerheten i kraftforsyningen.

I Meld. St. 25 (2015–2016) *Kraft til endring – Energipolitikken mot 2030* står det at styrket IKT-sikkerhet i energiforsyningen krever at NVE kontinuerlig utvikler regelverket når det gjelder IKT-sikkerhet, og at NVE veileder bransjen.

NVE har fra 1. januar 2019 skjerpet kravene til IKT-sikkerhet i kraftforsyningen med den nye kraftberedskapsforskriften, noe som kan bidra til forbedret sikkerhet. Kravene til IKT-sikkerhet i kraftforsyningen i norsk regelverk er strenge sammenlignet med tilsvarende krav i andre europeiske land og andre sektorer i Norge.

Flere av de nye kravene til IKT-sikkerhet er funksjonsbaserte. Det vil si at det er selskapene selv som skal vurdere hvilke sikkerhetsløsninger som gir tilstrekkelig IKT-sikkerhet ut fra egne risikovurderinger. Funksjonsbaserte krav gir selskapene større fleksibilitet til å følge den teknologiske utviklingen og kan tilpasses de enkelte virksomhetenes verdier og risiko, men stiller samtidig høyere krav til kompetanse og kapasitet i selskapene. Undersøkelsen viser at mangel på IKT-sikkerhetskompetanse er en stor utfordring for IKT-sikkerheten i kraftforsyningen. I risiko- og vesentlighetsvurderingene for årene 2017–2020 trekker NVE fram at digitaliseringen har ført til kompetanseutfordringer, og at både NVE og bransjen er avhengige av å styrke kompetansen på IKT-sikkerhetsområdet. For å bidra til kompetanseheving både internt og eksternt har NVE gjennomført mange forskningsprosjekter som belyser ulike sider ved IKT-sikkerheten. NVE har også bidratt til utdanningstilbud, kurs og seminarer om IKT-sikkerhet for ansatte i kraftforsyningen.

Undersøkelsen viser at selskapene i hovedsak er fornøyde med veiledningen de får fra NVE, men at mange av selskapene har behov for mer veiledning. NVE ble forsinket i arbeidet med å få ferdig en endelig veileder for kraftberedskapsforskriften, og veilederen ble først publisert i desember 2020.

2.1.4 Det er svakheter ved NVEs arbeid med overvåking, varsling og beredskap ved IKT-hendelser

Riksrevisjonen mener det er kritikkverdig at beredskapsorganisasjonen i NVE ikke har fått trent nok på å håndtere IKT-angrep mot kraftforsyningen. Undersøkelsen viser at NVE har lite erfaring med å håndtere slike angrep, og at etaten ikke har et oppdatert beredskapsplanverk eller en oppdatert plan for øvelser. Undersøkelsen viser også at NVE ikke har øvd på IKT-angrep mot kraftforsyningen sammen med selskaper og leverandører, med unntak av Statnett.

Riksrevisjonen mener det er positivt at NVE har lagt til rette for å styrke delingen av informasjon om trusler, sårbarheter og IKT-sikkerhetshendelser mellom aktørene i kraftforsyningen. Riksrevisjonen oppfatter imidlertid at svakheter ved selskapenes evne til å oppdage IKT-hendelser og underrapportering fra selskapene fører til at NVE og KraftCERT ikke får nok informasjon til å vurdere beredskapen ved pågående hendelser, få en oversikt over trusselbildet i sektoren og utarbeide tiltak for å forebygge nye hendelser.

NVE har styrket systemet for deling av informasjon om IKT-sikkerhetshendelser i kraftforsyningen

NVE er beredskapsmyndighet og sektorvist responsmiljø og skal ha en sentral rolle ved IKT-sikkerhetshendelser i kraftsektoren. I juni 2019 satte NVE ut oppgavene med å avdekke og dele kunnskap om sårbarheter og trusler med selskapene til KraftCERT, som skal støtte NVE i rollen som sektorvist responsmiljø. Fra 2019, da den nye kraftberedskapsforskriften trådte i kraft, stilte NVE nye krav til selskapenes varsling og rapportering av IKT-hendelser. Alle IKT-sikkerhetshendelser skal nå varsles til KraftCERT. Formålet med endringen var å gi KraftCERT et bredere grunnlag for å dele informasjon om trusler og sårbarheter med selskapene og å gi både KraftCERT og NVE en bedre oversikt over trusselbildet.

Svakheter i selskapenes evne til å oppdage IKT-hendelser, uklare varslingsrutiner og svak kultur for å varsle fører til underrapportering til NVE og KraftCERT

NVE skal ha oversikt over statusen og utviklingen i sikkerhetstilstanden i kraftforsyningen og avklare rutiner og krav til deling av hendelses- og risikoinformasjon. Kraftberedskapsforskriften stiller krav til selskapenes varsling av IKT-sikkerhetshendelser til NVE og KraftCERT. Undersøkelsen viser at det skjer mange IKT-sikkerhetshendelser i kraftselskapene som ikke rapporteres. Dette gjelder i hovedsak hendelser i administrative systemer. Det kan være flere årsaker til underrapporteringen:

- *Uklare varslingsrutiner:* Mange selskaper mangler kriterier for varsling av hendelser, og det har vært uklart hvilke type IKT-hendelser de skal varsle om til NVE og KraftCERT.
- *Svakheter i kraftforsyningens systemer for å oppdage hendelser:* Det er avdekket svakheter i systemene selskapene har for å overvåke og logge IKT-sikkerhetshendelser. KraftCERT anbefaler å innføre et felles sensornettverk i bransjen. Dette kan fange opp mer av uønsket trafikk.
- *Svak kultur for å varsle hendelser:* Undersøkelsen viser at selskapene gjerne avventer å varsle om hendelser fordi de ønsker å løse problemet internt før de deler informasjonen med andre. Dersom selskapene klarer å få situasjonen under kontroll, er det heller ikke sikkert at de rapporterer om hendelsen i ettertid.

Undersøkelsen viser at det er viktig at også mindre alvorlige angrep mot administrative IKT-systemer oppdages for å få stoppet angripere som kan prøve å benytte disse systemene til å få tilgang til driftskontrollsystemene og ramme kraftforsyningen. Tidligere hendelser har vist at angrep har startet i administrative systemer, og at angripere har vært inne i nettverket i flere måneder før de har begynt å innhente informasjon eller gjennomført forstyrrende handlinger. Det er også viktig at slike hendelser rapporteres, slik at andre selskaper kan iverksette tiltak for unngå lignende hendelser. Undersøkelsen viser at NVE så langt i liten grad har hatt oversikt over mindre alvorlige IKT-hendelser. Kravet fra 2019 om at alle hendelser skal varsles til KraftCERT, legger til rette for at KraftCERT og NVE skal få mer informasjon om slike hendelser.

NVE har lite erfaring med å håndtere IKT-angrep som rammer kraftforsyningen, og har ikke et oppdatert beredskapsplanverk

Som beredskapsmyndighet har NVE ansvaret for å samordne arbeidet med forebyggende sikkerhet og beredskap i kraftforsyningen og lede landets kraftforsyning dersom situasjonen blir svært alvorlig. NVE skal ha beredskapsplaner for håndtering av større hendelser, sikkerhetspolitiske kriser og krig og jevnlig gjennomføre øvelser for å vedlikeholde og utvikle kompetansen slik at de er i stand til å håndtere alle ekstraordinære situasjoner.

NVE har et beredskapsplanverk som inkluderer alvorlige IKT-hendelser, og dette skal sikre at kriser og ekstraordinære situasjoner håndteres effektivt. Beredskapsplanverket skal bygge på NVEs egne risiko- og sårbarhetsanalyser (ROS-analyser), det nasjonale risikobildet og evaluering av hendelser og øvelser. NVEs planverk har imidlertid ikke vært oppdatert siden 2017 og er dermed ikke tilpasset nyere trusselvurderinger, ROS-analyser, hendelser og øvelser. I NVEs ROS-analyser er også leverandørers IKT-sikkerhet og beredskapskapasitet tillagt stor betydning, uten at det går fram av beredskapsplanverket hvilken rolle de vil ha under et IKT-angrep.

Det har ikke forekommet IKT-hendelser av en slik alvorlighetsgrad at NVEs beredskapsplanverk har vært tatt i bruk, og NVE har dermed heller ikke fått evaluert håndteringen av alvorlige IKT-hendelser eller oppdatert beredskapsplanverket med bakgrunn i slike hendelser. NVE har imidlertid erfaring med å håndtere alvorlige hendelser som ikke gjelder IKT-sikkerhet, og har også evaluert slike hendelser. Disse hendelsene har imidlertid ikke gitt NVE erfaring med å bruke tiltakskortene for IKT-hendelser.

Undersøkelsen viser at NVE har deltatt på to nordiske IKT-øvelser i perioden 2017–2019, men at etaten i liten grad har øvd på hendelser som er beskrevet i egne tiltakskort. NVE har heller ikke en oppdatert plan for øvelser. I en av øvelsene ble det trent på samhandling med KraftCERT, Nasjonal sikkerhetsmyndighet og Statnett. NVE har ikke deltatt på øvelser som har involvert andre selskaper eller leverandører i kraftforsyningen.

2.1.5 Oppfølgingen av leverandørene er mangelfull til tross for at de har stor betydning for IKT-sikkerheten i kraftforsyningen

Etter Riksrevisjonens vurdering utgjør selskapenes avhengighet og mangelfulle oppfølging av leverandører og det at NVE har lite informasjon om leverandørenes IKT-sikkerhet og beredskap en risiko for IKT-sikkerheten i kraftforsyningen.

Ifølge Meld. St. 25 (2015–2016) *Kraft til endring - Energipolitikken mot 2030* er det en risiko for at selskapene i kraftforsyningen kan bli for avhengige av leverandører. Det påpekes at det er viktig at selskapene gir leverandørene klare signaler om at IKT-sikkerhet står i fokus, og at selskapene hele kontinuerlig bygger opp kompetansen på IKT-drift og IKT-sikkerhet. Ifølge meldingen er det viktig at også myndighetene bygger opp denne kompetansen, slik at de har grunnlag for å forstå risikobildet, noe som er viktig med tanke på at de har ansvar for regelverksutviklingen.

Mange av selskapene i kraftforsyningen har helt eller delvis tjenesteutsatt driften av IKT-systemer, og for noen av selskapene gjelder dette også driftskontrollfunksjoner. Kraftforsyningens IKT-sikkerhet og beredskap er derfor i stor grad avhengig av leverandørenes IKT-sikkerhet. Undersøkelsen viser at det er utfordrende for selskapene å sørge for at de har nok IKT-kompetanse internt, og at leverandørene deres har god nok IKT-sikkerhet. Mange av selskapene i kraftbransjen er små, mens mange leverandører er store multinasjonale selskaper. Dette kan gjøre det utfordrende for selskapene å få gjennomslag for sikkerhetskrav ved kontraktsinngåelse og å gjennomføre sikkerhetsrevisjoner av leverandørene.

Mange selskaper i kraftforsyningen benytter seg av de samme leverandørene av IKT-systemer. Dersom ett enkelt nettselskap mister evnen til å levere strøm i distribusjons- eller regionalnettet, vil det bare ramme et avgrenset område, mens et vellykket angrep mot en leverandør eller et system som er utbredt i kraftforsyningen, vil ramme flere selskaper og større områder. Mange selskaper er svært avhengige av leverandørene sine for å håndtere hendelser og gjenopprette driftskontrollsystemet, og det er risiko for at leverandørene ikke har dimensjonert beredskapen for hendelser som rammer flere selskaper samtidig.

Ingen av leverandørene i kraftforsyningen er utpekt som KBO-enhet, og dermed er de ikke underlagt kraftberedskapsforskriften. NVE kan per i dag ikke føre tilsyn med leverandørenes IKT-sikkerhet eller beredskapskapasitet. Leverandørene plikter heller ikke å varsle NVE om hendelser og kan ikke pålegges oppgaver av NVE ved ekstraordinære situasjoner. NVE får i hovedsak informasjon om leverandørenes IKT-sikkerhet gjennom veiledning og tilsyn med selskapene. Undersøkelsen viser at mange selskaper har mangelfull informasjon om og oppfølging av leverandørenes arbeid med IKT-sikkerhet, noe som også svekker NVEs informasjonsgrunnlag om IKT-sikkerheten i kraftforsyningen.

2.2 Olje- og energidepartementet sikrer seg ikke god nok styringsinformasjon om IKT-sikkerhetstilstanden i kraftforsyningen og resultatene av NVEs arbeid med IKT-sikkerhet i kraftforsyningen

Etter Riksrevisjonens vurdering er det kritikkverdig at Olje- og energidepartementet ikke har etterspurt og sikret seg god nok styringsinformasjon om resultatene av NVEs arbeid med IKT-sikkerhet i kraftforsyningen og om IKT-sikkerhetstilstanden. Riksrevisjonen mener at dette har ført til at departementet ikke har hatt et tilstrekkelig beslutningsgrunnlag for å vurdere nødvendige tiltak innenfor NVEs arbeid med IKT-sikkerhet i kraftforsyningen.

Olje- og energidepartementet skal legge til rette for en sikker kraftforsyning gjennom god beredskap. Departementet har delegert viktige beredskapsoppgaver til NVE. Olje- og energidepartementet skal fastsette mål- og resultatkrav for NVE og følge opp at målene nås. NVEs arbeid med IKT-sikkerhet i kraftforsyningen ligger under hovedmålet om å fremme en sikker kraftforsyning og delmålet om å påse at beredskapen i energiforsyningen er god og i tråd med gjeldende krav.

Olje- og energidepartementet angir ikke hvilken innsats og hvilke resultater som kreves av NVE for at etaten skal nå målet om å fremme en sikker kraftforsyning. NVEs rapportering til departementet om arbeidet med IKT-sikkerhet inneholder i hovedsak beskrivelser av tiltak og aktiviteter som er gjennomført. Departementet får imidlertid lite informasjon om resultatene av NVEs arbeid med IKT-sikkerhet og har derfor lite grunnlag for å vurdere måloppnåelsen og følge opp at målene nås.

NVE rapporterer gjennom avbruddsstatistikk at forsyningssikkerheten i Norge er svært høy. Så langt har det ikke vært avbrudd i strømforsyningen på grunn av IKT-angrep. Dette gir NVE begrenset incentiv til å prioritere arbeidet med å redusere risikoen for at IKT-angrep skal ramme kraftforsyningen, sammenlignet med arbeid som mer løpende virker inn på forsyningssikkerheten, og som påvirker avbruddstatistikken, som generell beredskap og fysisk vedlikehold. Fravær av brudd i strømforsyningen betyr imidlertid ikke nødvendigvis at IKT-sikkerheten i kraftforsyningen er god, slik NVE skal påse. Selv om kraftforsyningen er lite utsatt i fredstid, øker faren for aksjoner mot kraftforsyningen i kriser, og i krig er kraftforsyningen et klart utsatt mål. Statistikken for leveringspålitelighet i fredstid reflekterer dermed ikke risikoen for et alvorlig IKT-angrep i krisesituasjoner og krig. Undersøkelsen viser at det er svakheter i kildene NVE har for å rapportere om IKT-sikkerhetstilstanden i kraftforsyningen, og at Olje- og energidepartementet i liten grad har etterspurt og sikret seg mer informasjon.

3 Riksrevisjonens anbefalinger

Riksrevisjonen anbefaler Olje- og energidepartementet å

- sørge for at NVE styrker arbeidet med IKT-sikkerhet i kraftforsyningen, herunder:
  - videreutvikler verktøy for å styre og følge opp arbeidet
  - sikrer et bedre kunnskapsgrunnlag for IKT-sikkerhetstilstanden
  - vurderer tilsynsmetodikken og gjennomfører risikobaserte IKT-sikkerhetstilsyn
  - sikrer god veiledning til bransjen
  - fortsetter med kompetansehevende tiltak internt og for bransjen
  - videreutvikler systemet for avdekking og deling av IKT-sikkerhetshendelser
  - oppdaterer beredskapsplanverket og gjennomfører flere IKT-øvelser
  - vurderer tiltak for å håndtere utfordringen med å følge opp leverandørenes IKT-sikkerhet
- sørge for at NVEs rapportering gir tilstrekkelig styringsinformasjon om resultatene av NVEs arbeid med IKT-sikkerhet i kraftforsyningen

4 Statsrådens svar

Olje- og energiministeren bemerker at revisjonen er nyttig og at statsråden ønsker å bruke Riksrevisjonens funn og anbefalinger for å videreutvikle og styrke NVEs arbeid med IKT-sikkerhet i kraftforsyningen. Statsråden påpeker at flere av Riksrevisjonens merknader og anbefalinger vil følges opp gjennom arbeid som allerede er påbegynt, herunder:

- *Styring og oppfølging:* NVE er i ferd med å utarbeide en strategi for perioden 2022–2026 som vil gi grunnlag for bedre mål og resultatstyring og NVE vil styrke virksomhetsstyringen sin både med ressurser, prosesser og verktøy.
- *Tilsyn:* NVE har startet arbeidet med å se på hvordan andre metoder kan benyttes i tilsyn og vurderer å utvikle en tilsynsmetodikk som går dypere enn tilsynene gjør i dag. Et slikt arbeid må balanseres opp mot selskapenes eget ansvar for å sikre en god IKT-sikkerhetstilstand i kraftforsyningen.
- *Rapportering av IKT-sikkerhetshendelser:* NVE og KraftCERT har et pågående FOU-prosjekt om analyserammeverk for innrapporterte hendelser.

- *NVEs eget beredskapsarbeid*: Beredskapsplanverket i NVE skal revideres i 2021. I denne oppdateringen skal også samarbeidet med KraftCERT og NVEs rolle som sektorvist responsmiljø (SRM) gjennomgås. I tillegg skal NVE oppdatere den flerårige øvingsplanen.
- *NVEs rapportering til departementet:* I tildelingsbrevet for 2021 er NVE blant annet bedt om å styrke arbeidet med IKT-sikkerhet i kraftforsyningen. Dette inkluderer også oppfølging av tiltak som identifiseres i risiko- og sårbarhetsanalysen for kraftsektoren. Departementet har overfor NVE understreket at det er behov for bedre indikatorer for å beskrive tilstanden i kraftforsyningen. NVE har i tildelingsbrevet for 2021 fått styringsparametere der de skal identifisere og omtale indikatorer for vurdering av tilstanden i kraftforsyningen samt beskrive og vurdere resultater fra tilsyn.

Statsråden framhever at NVE prioriterer veiledning høyt, og mener arbeidet er bredere enn det som framgår av rapporten. Statsråden trekker også fram at det kun er ekstraordinære situasjoner som skal varsles til NVE og mener at Riksrevisjonen ikke har tilstrekkelig grunnlag for å si at det er underrapportering når det gjelder ekstraordinære situasjoner.

Statsråden påpeker at NVE har oppmerksomhet rettet mot leverandørkjeder og ser behov for å øke oppmerksomheten på informasjonssikkerhet hos leverandører og å følge opp virksomhetene i kraftsektoren på dette området.

Statsråden påpeker at revisjonen av arbeidet med IKT-sikkerhet i kraftsektoren kunne hatt større nytte dersom den kom på et noe senere tidspunkt. Den nye kraftberedskapsforskriften trådte i kraft 1. januar 2019 og statsråden mener det er naturlig at regelverksendringer først følges opp gjennom veiledning og deretter tilsyn. Statsråden påpeker at også pandemisituasjonen naturlig nok førte til redusert tilsynsaktivitet i 2020.

5 Riksrevisjonens uttalelse til statsrådens svar

Ettersom kraftberedskapsforskriften ble revidert med virkning fra januar 2019, mener statsråden at revisjonen kunne hatt større nytte dersom den kom på et noe senere tidspunkt. Riksrevisjonen er enig i at det er naturlig at regelverksendringer følges opp gjennom veiledning og deretter tilsyn. Riksrevisjonen påpeker likevel at det også før forskriftsendringen var krav til IKT-sikkerhet i kraftforsyningen og at endringene i hovedsak var en tydeliggjøring av eksisterende krav. Rapporten påpeker svakheter i hvordan NVE over tid har ivaretatt sine virkemidler for å styrke IKT-sikkerheten i kraftforsyningen. De fleste av disse svakhetene oppfatter vi som uavhengige av forskriftsendringen og tidspunktet for revisjonen.

Riksrevisjonen er enig i at underrapportering i hovedsak gjelder mindre alvorlige hendelser, noe som også framgår av undersøkelsen. Riksrevisjonen påpeker samtidig at det er en risiko for at ikke alle alvorlige hendelser oppdages og derfor ikke blir rapportert til NVE. Dersom angripere kommer seg på innsiden av systemene uten å bli oppdaget utgjør dette en trussel som kan benyttes til angrep mot strømforsyningen og føre til svært alvorlige situasjoner.

Riksrevisjonen har ingen ytterligere kommentarer.

Saken oversendes Stortinget.

Vedtatt i Riksrevisjonens møte 16. mars 2021

Per-Kristian Foss **Helga Pedersen**

Anne Tingelstad Wøien **Gunn Karin Gjul** **Arve Lønnum**

Jens A. Gunvaldsen

Vedlegg

Vedlegg 1:

Riksrevisjonens brev til statsråden i Olje- og energidepartementet

Riksrevisjonen

Vår saksbehandler
Anne Margit Grønningsæter Rudsro 22241257
Vår dato 16.02.2021
Vår referanse 2019/01363-265
Deres dato
Deres referanse

Utsatt offentlighet jf. rrevl § 18 (2)

OLJE- OG ENERGIDEPARTEMENTET
Postboks 8148 Dep
0033 OSLO

Att: Statsråd Tina Bru

Oversendelse av Dokument 3:x om Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen til Olje- og energidepartementet

Vedlagt oversendes utkast til Dokument 3:x (2021-2022) *Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen*

Dokumentet er basert på rapport oversendt Olje- og energidepartementet ved vårt brev 16. desember 2020, og på departementets svar 26. januar 2021.

Statsråden bes redegjøre for hvordan departementet vil følge opp Riksrevisjonens merknader og anbefalinger, og eventuelt om departementet er uenig med Riksrevisjonen.

Departementets oppfølging vil bli sammenfattet i det endelige dokumentet til Stortinget. Statsrådens svar vil i sin helhet bli vedlagt dokumentet. Det bes om at svaret oversendes som pdf lagret fra Word, ikke skannet som bilde, slik at innholdet kan gjøres tilgjengelig for alle i samsvar med krav til universell utforming.

Svarfrist: 3. mars 2021.

For riksrevisorkollegiet

Per-Kristian Foss

riksrevisor

Brevet er godkjent og ekspedert digitalt.

Vedlegg: Utkast til Dokument 3:x (2021–2022) *Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen*

Vedlegg 2:

Statsrådens svar

DET KONGELIGE
OLJE- OG ENERGIDEPARTEMENT

Statsråden

Riksrevisjonen
Postboks 8130 Dep
0032 OSLO

Deres ref	Vår ref	Dato
	19/1979-	3.3.21

Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet

Jeg viser til Riksrevisjonens brev av 16. februar d.å. med oversendelse av Dokument 3:x om undersøkelsen av NVEs arbeid med IKT-sikkerhet i kraftforsyningen. Riksrevisjonen ber om en redegjørelse for hvordan departementet vil følge opp Riksrevisjonens merknader og anbefalinger.

Innledningsvis ønsker jeg å bemerke at slike revisjoner er nyttige. Jeg mener at NVE gjør et grundig og godt arbeid med IKT-sikkerhet i kraftsektoren, men det vil alltid finnes muligheter til forbedring. Riksrevisjonen anbefaler at Olje- og energidepartementet sørger for at NVE styrker arbeidet med IKT-sikkerhet i kraftforsyningen gjennom flere ulike tiltak. Jeg ønsker å bruke Riksrevisjonens funn og anbefalinger til å videreutvikle dette viktige arbeidet. Flere av Riksrevisjonens merknader og anbefalinger vil følges opp gjennom arbeid som allerede er påbegynt. Jeg vil i det følgende gjennomgå hovedfunnene i rapporten.

Riksrevisjonen anbefaler at NVE videreutvikler verktøy for å styre og følge opp arbeidet med IKT-sikkerhet i kraftforsyningen. NVE har kartlagt et behov for en ny overordnet strategi som setter søkelys på hvordan NVE skal nå målene sine og prioritere ressurser til viktige innsatsområder. Det utarbeides en strategi for perioden 2022-2026 som vil gi grunnlag for bedre mål og resultatstyring og NVE vil styrke virksomhetsstyringen sin både med ressurser, prosesser og verktøy.

I rapporten anbefales det at NVE styrker tilsynsmetodikken sin og gjennomfører risikobaserte IKT-sikkerhetstilsyn. NVE har startet arbeidet med å se på hvordan andre metoder kan benyttes i tilsyn og vurderer å utvikle en tilsynsmetodikk som går dypere enn tilsynene gjør i

dag. Et slikt arbeid må balanseres opp mot virksomhetenes eget ansvar for å sikre en god IKT-sikkerhetstilstand i kraftforsyningen.

Riksrevisjonen anbefaler at NVE sikrer god veiledning til bransjen og fortsetter med kompetansehevende tiltak internt og for bransjen. Jeg vet at NVE prioriterer veiledning høyt, og at arbeidet er bredere enn det som framgår av rapporten. NVE publiserte ny veiledning for hele kraftberedskapsforskriften 22. desember 2020. Siden den nye forskriften trådte i kraft har NVE sørget for at det har blitt gjennomført en rekke kurs for bransjen om kravene i forskriften. NVE gir også mye veiledning på telefon og e-post mv.

Virksomhetene i kraftforsyningen har ifølge Riksrevisjonen uklare retningslinjer for hvilke IKT-hendelser som skal varsles og svak kultur for å varsle, noe som fører til underrapportering til NVE og KraftCERT. Riksrevisjonen mener derfor at det foreligger et behov for å videreutvikle systemet for avdekking av IKT-sikkerhetshendelser. Her vil jeg vise til at NVE og KraftCERT har et FOU-prosjekt om analyserammeverk for innrapporterte hendelser. Det er kun ekstraordinære situasjoner som skal varsles til NVE. Jeg mener at Riksrevisjonen ikke har tilstrekkelig grunnlag for å si at det er underrapportering når det gjelder ekstraordinære situasjoner.

Riksrevisjonen påpeker at det er behov for å oppdatere beredskapsplanverket og at NVE bør gjennomføre flere IKT-øvelser. Beredskapsplanverket i NVE skal revideres i 2021. I denne oppdateringen skal også samarbeidet med KraftCERT og NVEs rolle som sektorvist responsmiljø (SRM) gjennomgås. I tillegg skal NVE oppdatere den flerårige øvingsplanen.

NVE anbefales å vurdere tiltak for å håndtere utfordringen med å følge opp IKT-leverandørenes IKT-sikkerhet. Jeg mener dette er utenfor NVEs ansvarsområde. Leverandørene skal følges opp av selskapene, og er ikke underlagt kraftberedskapsforskriften (med unntak av det som gjelder kraftsensitiv informasjon) og er dermed utenfor NVEs tilsynsansvar. Jeg er kjent med at NVE likevel har oppmerksomhet rettet mot leverandørkjeder og ser behov for å øke oppmerksomheten på informasjonssikkerhet hos leverandører og å følge opp virksomhetene i kraftsektoren på dette området. Leverandører er blant annet nevnt en rekke ganger i den nye veilederen til kraftberedskapsforskriften.

Den siste anbefalingen fra Riksrevisjonen er at Olje- og energidepartementet bør sørge for at NVEs rapportering til departementet gir tilstrekkelig styringsinformasjon om resultatene av NVEs arbeid med IKT-sikkerhet i kraftforsyningen. Departementets oppmerksomhet på dette arbeidet framgår av styringsdialogen. I tildelingsbrevet til NVE for 2021 er blant annet NVE bedt om å styrke arbeidet med IKT-sikkerhet i kraftforsyningen. Dette inkluderer også oppfølging av tiltak som identifiseres i risiko- og sårbarhetsanalysen for kraftsektoren. I tillegg er NVE bedt særskilt om å følge opp funn og anbefalinger fra Riksrevisjonens forvaltningsrevisjon når resultatene foreligger.

Som ansvarlig departement for kraftforsyningen skal departementet i henhold til samfunnssikkerhetsinstruksen jevnlig avgi tilstandsvurdering av kraftforsyningen til Stortinget. Forrige vurdering ble publisert i Prop. 1 S (2017-2018), og neste vurdering skal utarbeides i forbindelse med Prop. 1 S (2021-2022). Det fremgår av de årlige tildelingsbrevene at NVE skal bistå departementet med å utarbeide en tilstandsvurdering for kraftforsyningen, inkludert indikatorer for en slik vurdering. Departementet har overfor NVE understreket at det er behov for bedre indikatorer for å beskrive tilstanden i kraftforsyningen. Dette fremgår blant annet av tildelingsbrevet for 2021. NVE har i tildelingsbrevet styringsparametere der de skal identifisere og omtale indikatorer for vurdering av tilstanden i kraftforsyningen samt beskrive og vurdere resultater fra tilsyn.

Avslutningsvis ønsker jeg å påpeke at revisjonen av arbeidet med IKT-sikkerhet i kraftsektoren kunne hatt større nytte dersom den kom på et noe senere tidspunkt. Den nye kraftberedskapsforskriften trådte i kraft 1. januar 2019. Jeg finner det naturlig at regelverksendringer først følges opp gjennom veiledning og deretter tilsyn. NVE ga virksomhetene anledning til å tilpasse seg endringene før direktoratet startet å føre tilsyn andre halvår 2019. Pandemisituasjonen førte naturlig nok til redusert tilsynsaktivitet i 2020.

Med hilsen

Tina Bru

Vedlegg 3:

Rapport: NVEs arbeid med IKT-sikkerhet i kraftforsyningen

Revisjonen er gjennomført som forvaltningsrevisjon i henhold til lov om Riksrevisjonen § 9, tredje ledd og instruks om Riksrevisjonens virksomhet § 9. Revisjonen er gjennomført i samsvar med Riksrevisjonens faglige retningslinjer for forvaltningsrevisjon og INTOSAIs standard for forvaltningsrevisjon (ISSAI 3000).

Innhold

Figuroversikt

Faktaboksoversikt

Ordliste og forkortelser

Administrative IKT-systemer	Administrative IKT-systemer omfatter blant annet kundebehandlingssystemer, regnskapssystemer, e-postsystemer og tilhørende servere og klienter (laptoper, smarttelefoner og mer) og er i denne sammenhengen systemer som ikke er driftskontrollsystemer.
AMS	Avanserte måle- og styringssystemer. AMS er toveis informasjons- og kommunikasjonssystemer fra og med elektrisitetsmålere som brukes til avregning for de enkelte målepunktene, til og med sentralsystemet hos nettselskapet eller nettselskapets leverandør.
Beredskapsmyndighet	Som beredskapsmyndighet har NVE ansvaret for å samordne arbeidet med forebyggende sikkerhet og beredskap i kraftforsyningen.
Brytefunksjonalitet i AMS	Brytefunksjonalitet i AMS gjør det mulig å fjernstyre inn- og utkoblingen av strømuttaket i målepunktet til AMS-målere. Det gjør det også mulig å begrense energien og effektuttaket i det enkelte målepunktet.
CERT	Computer Emergency Response Team. CERT er en ekspertgruppe som håndterer IKT-sikkerhetshendelser.
CIM	Crisis Information Management. CIM er et krisestøtteverktøy som NVE bruker til å håndtere hendelser.
Cyberangrep	Se IKT-angrep. NVE bruker ordet *cyberangrep* om det vi i rapporten omtaler som IKT-angrep.
Distribusjonsnettet	Et distribusjonsnett er et nett av ledninger som forsyner sluttbrukerne (husholdninger, tjenesteyting og industri) med strøm.
Driftskontrollfunksjoner	Driftskontrollfunksjoner er alle organisatoriske, administrative og tekniske tiltak for å overvåke, styre og beskytte anlegg i kraftforsyningen.
Driftskontrollsystem	Driftskontrollsystemer er driftssentraler, utstyr, nettverk, datarom, sambandsanlegg og øvrige anlegg og rom, systemer og komponenter som ivaretar driftskontrollfunksjoner.
Driftssentral	Driftssentraler omfatter operatørrom, datamaskinrom, sambandsrom og andre rom som inneholder komponenter som er nødvendige for sentralens drift, inkludert tilhørende utstyr.
Ekom	Ekom er elektronisk kommunikasjon og infrastruktur som må være til stede for at kapasitetskrevende tjenester skal fungere.
Ekstraordinære situasjoner	Ekstraordinære situasjoner er situasjoner der konsekvensene er mulige eller faktiske brudd på krav til beskyttelse av kraftsensitiv informasjon, kompromittering av driftskontrollsystem og brytefunksjonalitet.

Elhub	Elhub er et sentralt IKT-system som støtter og effektiviserer markedsprosesser som strømsalg, flytting og opphør i det norske kraftmarkedet. Det støtter også distribusjon og aggregering av måleverdier for alt forbruk og all produksjon i Norge. Det er Statnetts heleide datterselskap Elhub AS som forvalter Elhub.
FoU	Forsknings- og utviklingsarbeid. FoU vil si kreativ virksomhet som utføres systematisk for å oppnå økt kunnskap om kultur, individ og samfunn, og omfatter også bruken av denne kunnskapen til å finne nye anvendelser.
Hendelseshåndtering	Hendelseshåndtering er aktiviteter som utføres for å stanse eller begrense skade på IKT-systemer og nettverksressurser som er rammet av sikkerhetstruende hendelser eller handlinger, og for deretter å gjenopprette en sikker tilstand.
IKT	Informasjons- og kommunikasjonsteknologi. IKT er alle systemer som utfører sin funksjon gjennom å sende, motta, lagre, prosessere og konvertere informasjon fra andre systemer.
IKT-angrep	IKT-angrep er handlinger som utføres for å skade eller påvirke et IKT-system. Angrepet kan ha som mål å få tilgang til kraftsensitiv informasjon, gjøre et system utilgjengelig eller overta styringen av systemet.
IKT-hendelse	En IKT-hendelse er en hendelse som kan ramme IKT-systemers konfidensialitet, integritet og tilgjengelighet. IKT-hendelser omfatter både tilsiktede handlinger og utilsiktede hendelser. Se IKT-angrep for tilsiktede handlinger.
IKT-sikkerhet	IKT-sikkerhet er beskyttelse av IKT-systemene, samvirket mellom systemene, tjenestene som leveres av systemene, eller informasjon som behandles i systemene. IKT-sikkerhet omfatter sikring av alt IKT-utstyr eller digitalt utstyr, inkludert driftskontrollsystemer. Termen *IKT-sikkerhet* brukes ofte synonymt med *informasjonssikkerhet*, men gjelder bare de delene av informasjonssikkerheten som involverer IKT. Målene med IKT-sikkerhet er gjerne de samme som for informasjonssikkerhet.
IKT-sikkerhetskoordinator	En IKT-sikkerhetskoordinator er en medarbeider i et kraftselskap (KBO-enhet) som skal ha oversikt over IKT-sikkerhetsarbeidet i virksomheten og være faglig kontaktpunkt til beredskapsmyndigheten når det gjelder IKT-sikkerhet. Ifølge kraftberedskapsforskriften skal alle KBO-enheter utnevne en IKT-sikkerhetskoordinator.
Informasjonssikkerhet	Informasjonssikkerhet handler om å sikre at informasjon ikke blir kjent for uvedkommende (konfidensialitet), ikke blir endret utilsiktet eller av uvedkommende (integritet) og er tilgjengelig ved behov (tilgjengelighet). Termen *informasjonssikkerhet* brukes ofte synonymt med *IKT-sikkerhet*. Informasjonssikkerhet omfatter også informasjon som ikke utveksles og lagres i IKT-systemer eller elektronisk på annen måte.
KBO	Kraftforsyningens beredskapsorganisasjon. KBO består av NVE og virksomheter som står for kraftforsyningen, som større kraftprodusenter, nettselskaper og fjernvarmeselskaper (KBO-enheter). NVE organiserer KBO, som ved beredskapshendelser løser oppgaver knyttet til gjenoppretting av kraftforsyningen.

KBO-enheter	KBO-enheter er enheter som eier eller driver kraftproduksjon med tilhørende vassdragsregulering, overføring og distribusjon av elektrisk kraft og fjernvarme og som har klassifiserte anlegg eller systemer etter bestemmelser i kraftberedskapsforskriften. KBO-enhetene har ansvar for å følge bestemmelser i energiloven og kraftberedskapsforskriften.
Klassifisering av anlegg og systemer	Kraftberedskapsforskriften inneholder kriterier for klassifisering av anlegg og systemer eller annet som har vesentlig betydning for driften av, gjenopprettingen av eller sikkerheten i produksjon, omforming, overføring eller fordeling av elektrisk energi eller fjernvarme. Klassifiseringen er fra 1 til 3. Klasse 3 benyttes der betydningen for kraftforsyningen er størst.
Kompromittering	Kompromittering er et vellykket forsøk på å oppnå uautorisert tilgang til systemer, tjenester, ressurser eller informasjon, eller et vellykket forsøk på å kompromittere (forringe) konfidensialiteten, integriteten eller tilgjengeligheten av systemer, tjenester eller informasjon.
KraftCERT	KraftCERT er et privat selskap som i 2014 ble opprettet av aktører i kraftforsyningen for å støtte kraftbransjen med å forebygge og håndtere hendelser. KBO-enhetene skal varsle alle uønskede IKT-hendelser til KraftCERT, og KraftCERT skal innhente og formidle IKT-sikkerhetsinformasjon til KBO-enhetene.
Kraftforsyningen	Kraftforsyningen består av de systemene og leveransene som er nødvendige for å ivareta samfunnets behov for elektrisk energi til oppvarming, husholdninger, produksjon og transport med mer. NVE har det operative ansvaret for kraftforsyningsberedskapen.
Kraftforsyningens distriktssjefer	Kraftforsyningens distriktssjefer er representanter for kraftforsyningen som skal sørge for godt samarbeid og samordning om sikkerhet og beredskap mellom kraftselskapene (KBO-enhetene) i sitt distrikt. Kraftforsyningens distriktssjefer skal ha oversikt over vesentlige beredskapsmessige utfordringer i sitt distrikt, og følge det opp på en hensiktsmessig måte. Kraftforsyningens distriktssjefer samarbeider med NVE med tanke på å ha et oppdatert bilde av beredskapsstatusen rundt omkring i landet.
Kraftforsyningens sentrale ledelse	Kraftforsyningens sentrale ledelse består av beredskapsmyndigheten (NVE) og systemansvarlig (Statnett) og trer i kraft i alvorlige beredskapssituasjoner, som krig.
Kraftprodusent	En kraftprodusent driver med produksjon av elektrisk energi.
Kraftsensitiv informasjon	Kraftsensitiv informasjon er spesifikke opplysninger om kraftforsyningen som kan brukes til å skade anlegg, systemer eller annet eller påvirke funksjoner som har betydning for kraftforsyningen.
NC-Spectrum AS	NC-Spectrum AS er et norsk konsulentselskap med kompetanse innenfor digital infrastruktur og informasjonssikkerhet. Selskapet har kraftbransjen som hovedkundegruppe.
Nettalliansen AS	Nettalliansen AS er en allianse hvor om lag 40 små og mellomstore nettselskaper er medlemmer. Viktige samarbeidsområder er digitalisering, felles innkjøp og kompetanse- og ressursdeling.

Nettfiske	Nettfiske, også kalt phishing, er forsøk på svindel eller manipulasjon der bakmennene, ofte ved å sende en e-post, forsøker å lure brukeren til å oppgi sensitive opplysninger (for eksempel passord) eller klikke på lenker som laster ned skadevare.
Nettselskap	Et nettselskap er en omsetningskonsesjonær som eier overføringsnett eller har ansvar for nettjenester.
Nettverksoperasjon	En nettverksoperasjon er en prosess der trusselaktører søker å skaffe seg urettmessig tilgang til datanettverk hos en spesifikk virksomhet, og der formålet for eksempel er å samle inn etterretning, forberede sabotasje eller manipulere data.
NSM	Nasjonal sikkerhetsmyndighet. NSM er fagorgan for forebyggende sikkerhet og sikkerhetsmyndighet etter lov om nasjonal sikkerhet (sikkerhetsloven). Direktoratet er ekspertorgan for informasjons-, objekt- og IKT-sikkerhet og nasjonal varslings- og koordineringsinstans for alvorlige dataangrep og andre IKT-sikkerhetshendelser. Nasjonalt cybersikkerhetssenter (NCSC) er en del av NSM og skal bidra til å beskytte grunnleggende nasjonale funksjoner, offentlig forvaltning og næringsliv mot cyberangrep.
Områdeovervåking	Områdeovervåking kan beskrives som innhenting, systematisering og tolking av innsamlet kunnskap som blant annet kan gi grunnlag for risiko- og vesentlighetsvurderinger ved utvalg av tema og selskaper til tilsyn.
Redundans	Redundans er reservekapasitet/dublering av kritiske komponenter og funksjoner for å øke påliteligheten til systemet.
Reguleringsmyndigheten for energi	Reguleringsmyndigheten for energi (RME) har vært en egen avdeling i NVE inntil de fra 1. november 2019 ble skilt ut som en uavhengig reguleringsmyndighet i medhold av energiloven § 2-3 og naturgassloven § 4. RMEs oppgave er å sørge for at aktørene i kraftforsyningen overholder regelverket som sikrer like konkurransevilkår i kraftmarkedet og et effektivt drevet strømnett.
Sektorvist responsmiljø	Sektorvist responsmiljø er en funksjon innenfor en samfunnssektor eller et overordnet styringsområde med grunnleggende kapasitet til å koordinere og håndtere uønskede IKT-sikkerhetshendelser. NVE er sektorvist responsmiljø for kraftforsyningen.
Sikkerhetsrevisjon	Sikkerhetsrevisjon er en virksomhets interne kontroll og kvalitetssikring av eget sikkerhetsarbeid.
Statnett SF	Statnett er et statsforetak som bygger, eier og driver det sentrale strømnettet og sørger for at det er balanse mellom forbruk og produksjon.
Sårbarhetsvarsler	Sårbarhetsvarsler er varsler som kan inneholde informasjon om aktuelle sårbarheter, trusler og hendelser og tiltak som selskapet bør iverksette for å unngå å bli rammet.
Tilsyn	Tilsyn brukes i denne rapporten for det NVE kaller «revisjon», som er en av flere metoder NVE bruker for kontroll med virksomhetene. Tilsyn er en uavhengig, systematisk og dokumentert gjennomgang av kvalitetssystemer, rutiner eller enkeltdokumenter som dekker hele eller deler av en virksomhet.

Tjenestenekt	Et tjenestenekt-angrep er et internettangrep som overbelaster en server ved at stor trafikk rettes mot serveren. Hensikten er å hindre at ordinære brukere får normal tilgang til serveren.
Tjenesteutsetting	Tjenesteutsetting går ut på å sette ut basisdrift, applikasjonsdrift eller applikasjonsforvaltning til eksterne tjenesteleverandører. Tjenestene som settes ut, reguleres gjennom en kontrakt med leverandøren.
Underrapportering	Underrapportering viser til IKT-hendelser som ikke har blitt varslet eller rapportert uavhengig av varslingsplikt. Vi omtaler også hendelser som ikke oppdages, og dermed ikke rapporteres av selskapene, som underrapportering.
Uønskede hendelser	Uønskede hendelser omfatter handlinger, forhold eller andre situasjoner som innebærer eller medfører brudd på konfidensialitet, integritet og tilgjengelighet, inkludert kompromittering av sensitiv informasjon, systemfunksjonalitet eller teknologiske sikkerhetstiltak. En uønsket hendelse som forårsakes av en aktør som handler med hensikt, er en tilsiktet uønsket handling. Uønskede hendelser kan gi opphav til ekstraordinære situasjoner.

1 Innledning

1.1 Bakgrunn

1.1.1 Økt risiko for IKT-angrep mot kraftforsyningen

Kraftforsyningen er en sentral del av Norges kritiske infrastruktur, og tilgang på elektrisk kraft blir stadig viktigere for å kunne opprettholde normal aktivitet i samfunnet, sikre kritiske samfunnsfunksjoner i krisesituasjoner og opprettholde landets forsvarsevne under beredskap og i krig. Svikt i forsyningen av elektrisk kraft får konsekvenser for alle samfunnssektorer og digitale systemer som samfunnet er avhengig av.[1]

Kraftforsyningen har gjennomgått en betydelig digitalisering de siste tiårene, og også i årene framover vil det stadig bli tatt i bruk ny teknologi. Økt bruk av informasjons- og kommunikasjonsteknologi (IKT) gir økt risiko for flere uønskede IKT-hendelser, og introduksjon av ny teknologi og bruk av skyløsninger og leverandører i utlandet kan være utfordrende, både med hensyn til sikkerhet og regulering.[2] Ny teknologi gjør det mulig å styre og drifte kraftinfrastrukturen mer effektivt og rette feil raskere, men samtidig bidrar det til økt risiko, særlig når ulike systemer integreres og alt kobles til internett.[3] Ifølge nasjonale trusselvurderinger utgjør systemer innenfor kraftsektoren kritisk infrastruktur som er spesielt utsatt for etterretning og avanserte nettverksoperasjoner.[4] I en kartlegging av IKT-sikkerheten i kraftbransjen som NVE gjennomførte i 2017, meldte 70 prosent av respondentene at de hadde hatt uønskede IKT-sikkerhetshendelser det siste året. Det er med andre ord avgjørende at nett- og kraftselskapene er i stand til å beskytte seg mot digitale angrep og svikt i systemene. Den digitale utviklingen både i energisektoren og samfunnet for øvrig fører til endringer i kraftforsyningens risiko- og sårbarhetsbilde. Lysneutvalget viste til en økende trend mot tjenesteutsetting og bruk av leverandører i kraftbransjen, noe som har innvirkning på IKT-sikkerheten. Utvalget påpekte at virksomhetene må sørge for at relevante IKT-sikkerhetskrav inngår i avtaler med leverandører, og at kravene følges opp. Utvalget trakk også fram at den enkelte virksomhet ikke alltid evner å se hvilke samfunnsmessige konsekvenser det kan få dersom de inngår avtaler med utilstrekkelige IKT-sikkerhetskrav.[5]

1.1.2 NVEs mål og oppgaver

Et av hovedmålene på energi- og vannressursområdet er å legge til rette for en effektiv, sikker og miljøvennlig energiforsyning.[6] Olje- og energidepartementet skal legge til rette for en sikker kraftforsyning gjennom god beredskap i kraftforsyningen og har delegert viktige beredskapsoppgaver til Norges vassdrags- og energidirektorat (NVE).

Et av NVEs viktigste mål er å fremme en sikker kraftforsyning. Sikkerhet i kraftforsyningens IKT-systemer er ett av flere sentrale områder som skal bidra til å opprettholde en stabil og sikker kraftforsyning. NVE skal påse at beredskapen i kraftforsyningen er god og i tråd med gjeldende krav.

NVE er beredskapsmyndighet og leder Kraftforsyningens beredskapsorganisasjon (KBO). KBO består av NVE og virksomheter som står for kraftforsyningen, som større kraftprodusenter, nettselskaper og fjernvarmeselskaper. KBO-enhetene har en selvstendig plikt til å sørge for effektiv sikring og beredskap og iverksette tiltak for å forebygge, begrense og håndtere virkningene av ekstraordinære situasjoner. Per januar 2020 var det om lag 170 enheter i KBO. NVE utnevner også kraftforsyningens distriktssjefer, som skal legge til rette for at KBO-enhetene i et område kan samarbeide om å ivareta sikkerheten og forebygge og håndtere ekstraordinære situasjoner. Den 1. januar 2019 ble NVE dessuten utpekt som sektorvist responsmiljø for håndtering av IKT-hendelser i kraftforsyningen. KraftCERT har fra 2019 etter avtale utført konkrete oppgaver som sektorvist responsmiljø på vegne av NVE. *Forskrift om sikkerhet og beredskap i kraftforsyningen* (kraftberedskapsforskriften) regulerer arbeidet med forebyggende sikkerhet og beredskap i kraftforsyningen. Kraftberedskapsforskriften ble revidert i 2018, med virkning fra 1. januar 2019.

I Meld. St. 25 (2015–2016) *Kraft til endring – Energipolitikken mot 2030* (energimeldingen) går det fram at NVE kontinuerlig skal utvikle regelverket på IKT-sikkerhetsområdet, veilede og samarbeide med bransjen samt gjennomføre tilsyn og øvelser for å styrke IKT-sikkerheten i energiforsyningen.

[1] NOU (2015: 13) *Digital sårbarhet – sikkert samfunn*.
[2] Meld. St. 25 (2015–2016) *Kraft til endring – Energipolitikken mot 2030*.
[3] NVE (2015) *Teknologiskifte i energiforsyningen. Studie om muligheter og sårbarheter*. NVE-rapport nr. 118/2015.
[4] PSTs trusselvurdering 2019.
[5] NOU (2015: 13) *Digital sårbarhet – sikkert samfunn*.
[6] Prop. 1 S (2018–2019) Olje- og energidepartementet.

1.1.3 Indikasjoner på svakheter ved NVEs arbeid med IKT-sikkerhet i kraftforsyningen

NVE har hatt ansvar for regelverket og tilsynet med den fysiske sikkerheten i kraftforsyningen over flere tiår. IKT-sikkerhet i kraftforsyningen er i denne sammenhengen et relativt nytt tema. I NOU (2015: 13) *Digital sårbarhet - sikkert samfunn* (Lysneutvalget) ble det vist til at NVE har begrenset kapasitet til å gjennomføre tilsyn med IKT-sikkerhet, og utvalget foreslo å styrke NVE betraktelig på området tilsyn og veiledning. På grunn av den økte avhengigheten av IKT var det også ifølge utvalget behov for krav om å beskytte informasjon og sørge for at nettverk og systemer er sikre og stabile. Utvalget anbefalte en gjennomgang av sektorregelverk, blant annet for kraftforsyningen. I NVEs overordnede risikovurdering for 2019 og 2020 trekker etaten fram risikoen for at IKT-systemene i kraftforsyningen rammes av cyberangrep som en av tre risikoer under risikoområdet «Forsyningssikkerhet».

1.1.4 Mangel på IKT-sikkerhetskompetanse i kraftforsyningen er en utfordring for IKT-sikkerheten

I NOU (2018: 14) *IKT-sikkerhet i alle ledd* trekkes tilgang til IKT-sikkerhetskompetanse fram som en av de største utfordringene på IKT-sikkerhetsområdet. I 2030 vil det ifølge estimatene være et underskudd på 4100 personer med slik kompetanse i det norske samfunnet. Nasjonal sikkerhetsmyndighet (NSM) vurderer det økende gapet mellom tilgjengelighet av og behov for sikkerhetskompetanse som en nasjonal sårbarhet. Lysneutvalget viste til at flere av selskapene i kraftforsyningen er små med få ansatte, og at det er en kompetanseutfordring å etablere og opprettholde nødvendige fagmiljøer innenfor IKT-sikkerhet. Utvalget anbefalte at NVE i samarbeid med interesseorganisasjonene bør stimulere til større og mer ressurssterke fagmiljøer på IKT-sikkerhet i selskapene.[7]

1.2 Mål og problemstillinger

Målet med undersøkelsen er å vurdere i hvilken grad NVEs virkemiddelbruk bidrar til å styrke IKT-sikkerheten i kraftforsyningen. Målet belyses gjennom følgende problemstillinger:

1. Hva er risikoen for IKT-angrep som rammer kraftforsyningen?
   a. Hvordan er trusselbildet for IKT-angrep i kraftforsyningen?
   b. Hva er sårbarhetene i IKT-sikkerhetsarbeidet i kraftforsyningen?
2. I hvilken grad bidrar NVEs styring til å styrke IKT-sikkerheten i kraftforsyningen?
3. Hvordan ivaretar NVE sitt ansvar for regelverksutforming, veiledning, kompetanseheving og tilsyn i arbeidet med IKT-sikkerhet?
4. Hvordan ivaretar NVE sitt ansvar for overvåking, varsling og beredskap ved IKT-hendelser?
5. Hvordan er Olje- og energidepartementets styring og oppfølging av NVEs arbeid for å styrke IKT-sikkerheten i kraftforsyningen?

Problemstilling 1, om risikoen for IKT-angrep som rammer kraftforsyningen, er en kartlegging som et ledd i å undersøke i hvilken grad NVE bidrar til å styrke IKT-sikkerheten i kraftforsyningen. NVE er revisjonsobjektet i undersøkelsen. Selskapene som omtales i undersøkelsen, er virksomheter som ifølge kraftberedskaps-forskriften er KBO-enheter, som er de viktigste selskapene i kraftforsyningen. KBO-enhetene er ikke revisjonsobjekter i undersøkelsen.

[7] NOU (2015: 13) *Digital sårbarhet – sikkert samfunn*.

2 Metodisk tilnærming og gjennomføring

For å belyse problemstillingene har vi gjennomført dokumentanalyse, intervjuer, saksgjennomgang av IKT-sikkerhetstilsyn, varsler og rapportering om hendelser, spørreundersøkelse til IKT-sikkerhetskoordinatorer i KBO-enhetene og caseundersøkelse om IKT-sikkerheten i utvalgte selskaper. I tillegg har vi sammenstilt og analysert tilgjengelig statistikk og deltatt som observatør på tre av NVEs IKT-tilsyn. Datainnsamlingen er gjennomført i perioden november 2019–november 2020. Undersøkelsesperioden er i hovedsak tidsrommet 2017–2020.

Kraftberedskapsforskriften ble revidert i 2018 med virkning fra 1. januar 2019, og NVE fikk rollen som sektorvist responsmiljø fra 1. januar 2019. NVE trekker fram at det er forskjell på kravene som gjaldt – både for virksomhetene og for NVE som myndighet – for årene 2017–2018 sammenlignet med 2019–2020. NVE mener at kravene til IKT-sikkerhet som gjaldt fram til det nye regelverket trådte i kraft 1. januar 2019, ikke var like spesifikke som kravene i det reviderte regelverket. NVE trekker også fram at kravet om å etterleve NSMs grunnprinsipper først trådte i kraft 1. januar 2019. Ettersom det også før forskriftsendringen i 2019 var krav til IKT-sikkerhet, som er utdypet i veilederen fra 2013, og endringene i stor grad reflekterer det som allerede var god praksis på området, har vi imidlertid kommet fram til at det ikke er nødvendig å skille mellom selskapenes etterlevelse av kravene og NVEs arbeid med IKT-sikkerhet i kraftforsyningen før og etter januar 2019, i undersøkelsen. Det samme gjelder NVEs håndtering av IKT-hendelser, ettersom NVE i rollen som beredskapsmyndighet i stor grad har hatt de samme oppgavene i hele undersøkelsesperioden. Se kapittel 3, *Revisjonskriterier*, for en nærmere beskrivelse av kravene før og etter 2019.

Olje- og energidepartementet påpeker i sine kommentarer til rapportutkastet at Reguleringsmyndigheten for energi (RME) har ansvar for oppfølging av avregningsforskriften, som inneholder IKT-sikkerhetskrav for avanserte måle- og styringssystemer (AMS) og Elhub. RME sitt arbeid har ikke vært en del av undersøkelsen. Kravene til brytefunksjonalitet i AMS, som kan påvirke forsyningssikkerheten, følges opp av beredskapsseksjonen i NVE og inngår i undersøkelsen. Vi har heller ikke undersøkt NVEs oppfølging av de fysiske sikringskravene og kravet om personkontroll i kraftberedskapsforskriften selv om etterlevelsen av disse kravene også vil påvirke IKT-sikkerheten i kraftforsyningen.

2.1 Dokumentanalyse

De oversendte dokumentene er analysert blant annet i tekstanalyseprogrammet NVivo. Følgende dokumenter har vært sentrale for å vurdere hvordan NVEs arbeid bidrar til å styrke IKT-sikkerheten i kraftforsyningen:

- energiloven, kraftberedskapsforskriften og tilhørende skriftlige veiledere
- NSMs rammeverk for håndtering av IKT-sikkerhetshendelser og NSMs grunnprinsipper for IKT-sikkerhet
- *Instruks for økonomi- og virksomhetsstyring i Norges vassdrags- og energidirektorat*
- Olje- og energidepartementets budsjettproposisjoner med tilhørende innstillinger
- referater fra etatsstyringsmøter
- Olje- og energidepartementets tildelingsbrev til NVE
- NVEs årsrapportering
- NVEs høringsnotat, aktørenes høringsinnspill og NVEs oppsummeringsdokument av høringen i forbindelse med endringen av kraftberedskapsforskriften
- NVEs overordnede risiko- og vesentlighetsvurderinger
- risiko- og sårbarhetsanalyser for kraftsektoren
- tilstandsvurderinger for kraftforsyningen og NVEs faktaark om hendelser
- NVEs planer, strategier, rapporter og evalueringer på virksomhets-, avdelings- og seksjonsnivå
- NVEs prosedyre for kontroll og reaksjonsbruk
- databaser, oversikter og rapporter fra tilsynsvirksomheten og reaksjonsregisteret til NVE
- NVEs oversikter over varsler og innrapporterte hendelser
- NVEs beredskapsplanverk
- dokumentasjon på NVEs kompetanse- og utdanningstiltak overfor kraftbransjen
- NVEs årlige forventningsbrev til KBO
- korrespondanse mellom NVE og KraftCERT
- rapporter fra NVEs FoU-prosjekter, inkludert resultater fra NVEs spørreundersøkelser til virksomhetene
- trussel- og risikovurderinger fra NSM, PST, Direktoratet for samfunnssikkerhet og beredskap og Etterretningstjenesten

2.2 Intervjuer/møter

Vi har gjennomført intervjuer for å belyse NVEs arbeid med IKT-sikkerhet i kraftforsyningen. Referatene fra intervjuene er verifisert av intervjuobjektene. Intervjuene er også brukt som grunnlag for utarbeidelsen av spørreundersøkelsen til IKT-sikkerhetskoordinatorene. Vi har gjennomført seks intervjuer med NVE, nærmere bestemt med lederen av tilsyns- og beredskapsavdelingen, lederen av beredskapsseksjonen og medarbeidere som jobber med IKT-sikkerhet i kraftforsyningen. Vi har videre gjennomført intervjuer med representanter fra følgende virksomheter (virksomhetene har selv pekt ut personer som har god kjennskap til temaene):

- Olje- og energidepartementet
- fire selskaper i kraftforsyningen av liten, middels og stor størrelse som har hatt tilsyn av NVE i perioden 2017–2019
- tilsynsmyndighetene i Sverige og Danmark
- Finanstilsynet
- Nasjonal Sikkerhetsmyndighet (NSM)
- Etterretningstjenesten
- Nettalliansen AS, en allianse av 40 små- og mellomstore nettselskap
- konsulentselskapet NC-Spectrum AS
- KraftCERT AS
- Direktoratet for samfunnssikkerhet- og beredskap

Vi intervjuet tilsynsmyndighetene i Danmark og Sverige, Finanstilsynet, NSM og DSB for å få et inntrykk av hvordan andre tilsynsmyndigheter arbeider med tilsyn av IKT-sikkerhet. Vi har brukt intervjuene til å trekke fram eksempler på praksis hos de andre aktørene.

Vi har også hatt tre møter med en referansegruppe for å sikre en god faglig forståelse av IKT-sikkerhetsmessige spørsmål og NVEs myndighetsansvar. Gruppen har gitt tilbakemeldinger på utkast til hovedanalyseplanen, rapporten og spørreundersøkelsen. Referansegruppen har bestått av Martin Gilje Jaatun (forsker SINTEF Digital), Eva Brekka (NC-Spectrum AS), Margrete Raaum (KraftCERT AS), Olav Lysne (forsker Simula Metropolitan) og Øystein Korum (IKT-sikkerhetskoordinator Statnett).

2.3 Saksgjennomgang

Vi har gjennomført en saksgjennomgang av alle NVEs tilsyn som omhandler IKT-sikkerhet eller informasjonssikkerhet i KBO-enheter i perioden 2017–2019, og av NVEs behandling av varsler og hendelsesrapportering fra selskapene i perioden 2016–2019. Formålet var å vurdere hvordan NVE behandler og dokumenterer sakene, som vi har funnet i NVEs arkiv. Utvalget av tilsynssaker besto av 15 IKT-sikkerhetstilsyn som var gjennomført i perioden 2017–2019, herunder 13 tilsyn med IKT-driftskontroll og 2 tilsyn med informasjonssikkerhet. I gjennomgangen av tilsynssakene vurderte vi om NVE følger sine egne interne rutiner for tilsynsgjennomføring slik de går fram i NVEs prosedyrer for kontroll og reaksjonsbruk og i beredskapsseksjonens interne dokumenter. Gjennomgangen av varsler og hendelsesrapportering omfattet alle oppføringer i NVEs oversikt over varsler og innrapporterte hendelser i perioden 2016–2019, som vi fikk oversendt. Vi har vurdert hvordan varsler og rapporteringer ble behandlet og fulgt opp, og om oppfølgingen er dokumentert.

2.4 Analyse av kvantitative data

Vi har gjennomført analyser av statistikk over avbrudd i kraftforsyningen, midler som er tildelt FoU-prosjekter og prioriterte tiltak i NVE og over NVEs tilsyn innenfor områdene generell beredskap og IKT-sikkerhet. Vi har også analysert kvantitative data som belyser trusselbildet mot IKT-systemene til selskapene i kraftforsyningen, herunder hendelser og angrep mot selskapene som er observert av NVE, KraftCERT, NSM og Etterretningstjenesten.

2.5 Observasjon av NVEs arbeid gjennom deltakelse på seminarer, kurs og tilsyn

Vi har deltatt som observatør på tre av NVEs tilsyn som omhandler IKT-sikkerhet i KBO-enhetene, og på den måten fått erfare hvordan tilsynene har blitt gjennomført i praksis. Dette har gitt oss en bedre forståelse av NVEs tilsynsmetodikk, NVEs veiledning til tilsynsobjektene i hvordan kravene kan etterleves og avvik kan lukkes, og vurderingene NVE gjør ved bruk av sanksjoner.

Vi har også deltatt på kurs og seminarer i regi av NVE og andre. Dette inkluderer følgende:

- Internt seminar i NVE om IKT-sikkerhet (3. september 2019)
- Kurs i grunnsikring og kraftberedskapsforskriften i regi av Energi Norge[8] og NVE (25. november 2020)
- NVEs presentasjon av rapporter om NVEs utvikling av revisjonsmetodikk for kartlegging av kraftsensitiv informasjon på internett og sjekkliste for IKT-sikkerhet i anskaffelser og tjenesteutsetting (8. januar 2020)
- «Samfunnssikkerhetskonferansen» arrangert av Direktoratet for samfunnssikkerhet og beredskap (4. februar 2020)
- Konferansen «Vinterkraft» arrangert av Forum for informasjonssikkerhet i kraftforsyningen (11.–12. februar 2020)
- Tilsynskurs for NVEs ansatte (10.–11. mars 2020)
- NVEs webinar om konsekvensene av covid-19 for kraftforsyningen og annet (8. juni 2020)

Ved å delta på disse arrangementene har vi fått forståelse for bransjens utfordringer med IKT-sikkerhet, NVEs tilsynsrutiner og NVEs arbeid med veiledning og kompetansetilbud til selskapene i bransjen.

2.6 Caseundersøkelse

Vi har gjennomført en caseundersøkelse i tre utvalgte selskaper av ulik størrelse i bransjen. Resultatene fra caseundersøkelsen er sammenstilt med andre kilder (dokumentanalyse, NVEs tilsynsrapporter, spørreundersøkelsen og intervjuer) for å belyse IKT-sikkerheten i kraftforsyningen og hvilke krav selskapene har størst utfordringer med å etterleve. Vi valgte de tre selskapene ut fra hvilke selskaper NVE hadde ført IKT-sikkerhetstilsyn med i 2019 og 2020, slik at vi kunne vurdere NVEs tilsynsmetodikk ved å sammenligne det NVE avdekket i tilsynet, med resultatene fra caseundersøkelsen.

Gjennom dokumentanalyse, intervjuer, observasjoner, analyser og tester av kontroller har vi undersøkt hvordan disse selskapene arbeider med IKT-sikkerhet og implementering av grunnleggende sikkerhetstiltak. Undersøkelsen omfattet både administrative systemer og driftskontrollsystemer. I caseundersøkelsen har vi sett nærmere på selskapenes rammeverk for arbeidet med IKT-sikkerhet, klassifisering av verdier, risikoanalyser, etterkontroller og sikkerhetsrevisjoner. I tillegg har vi gjennomført tester av den tekniske sikringen av IKT-systemene i samarbeid med selskapene og deres IKT-leverandører. Testene omfatter analyser av teknisk informasjon, passordoppsett og tilgangsrettigheter samt bruk av analyseverktøy som blant annet tester åpne porter i infrastrukturen og om sonedelingen mellom de administrative systemene og driftskontrollsystemene fungerer.

Utgangspunktet for caseundersøkelsen er kravene i kraftberedskapsforskriften kapittel 6 (Informasjonssikkerhet) og 7 (Beskyttelse av driftskontrollsystem) og anbefalinger fra NSM.[9] Vi har vurdert selskapene ut fra tre nivåer – om kravene etterleves, eller om det er svakheter eller vesentlige svakheter i selskapets etterlevelse av kravene i kraftberedskapsforskriften, god praksis på området eller i gjennomføringen av aktiviteten/tiltaket. Undersøkelsene, som er gjennomført med selskapenes tillatelse, er utført i løpet av perioden fra høsten 2019 til høsten 2020. Selskapene har verifisert resultatene fra caseundersøkelsen.

2.7 Spørreundersøkelse

Vi har gjennomført en spørreundersøkelse som ble sendt til IKT-sikkerhetskoordinatorer i KBO-enhetene for å få informasjon om deres oppfatning om NVEs arbeid med IKT-sikkerhet i kraftforsyningen. Spørreundersøkelsen inneholdt blant annet spørsmål om utfordringer knyttet til forståelsen og etterlevelsen av regelverket, NVEs tilsyn og veiledning og KraftCERTs sårbarhetsvarsler. Før spørreskjemaene ble sendt

[8] En landsomfattende interesse- og arbeidsgiverorganisasjon tilsluttet Næringslivets Hovedorganisasjon med om lag 300 medlemsbedrifter som produserer, transporterer og leverer fornybar energi i Norge.
[9] NSM (2020) *Grunnprinsipper for IKT-sikkerhet,* versjon 2.0.

ut, ble de testet av NVE, referansegruppen og to selskaper i kraftforsyningen. Svarene i spørreundersøkelsen er anonymisert, og ingen identifiserbar informasjon er lagret med svarene.

Spørreundersøkelsen ble sendt til IKT-sikkerhetskoordinatorene i 134 av om lag 170 KBO-enheter. I samråd med NVE ble spørreundersøkelsen ikke sendt til vassdragsregulanter, brukseierforeninger og enkelte andre selskaper, som ble ansett som mindre relevante for undersøkelsen. Spørreundersøkelsen ble gjennomført i september 2020 og hadde en svarprosent på 50 prosent. Vi har ikke informasjon som kan fortelle om det er skjevheter i svarprosenten ut fra karakteristika ved selskapene i utvalget, som selskapsstørrelse. Vi har imidlertid informasjon om hvor mange kunder nettselskapene som inngikk i utvalget har. 80 av de 134 selskapene i utvalget var nettselskaper. Før utsendelse ble nettselskapene kategorisert i tre størrelseskategorier etter antall nettkunder for å ivareta anonymiteten til respondentene. Blant nettselskapene var svarprosenten høyest blant IKT-sikkerhetskoordinatorer i store selskaper.

IKT-sikkerhetskoordinatorene ble i spørreundersøkelsen bedt om å oppgi antall ansatte i selskapet de jobber for. Av de 68 respondentene som besvarte undersøkelsen, tilhørte 16 av dem selskaper med mellom 1 og 20 ansatte, 32 selskaper med mellom 21 og 100 ansatte og 20 selskaper med mer enn 100 ansatte. Svarene på de fleste spørsmålene varierer i liten grad mellom respondentene i selskaper med få og mange ansatte. Vi mener dermed at svarene er tilstrekkelig representative til å kunne gi informasjon om IKT-sikkerhetskoordinatorenes oppfatninger.

3 Revisjonskriterier

3.1 Overordnede mål og krav til IKT-sikkerhet i kraftforsyningen

Ifølge Prop. 1 S (2018–2019) fra Olje- og energidepartementet, jf. Innst. 9 S (2018–2019), er det et overordnet mål for Olje- og energidepartementet å legge til rette for en sikker kraftforsyning gjennom god beredskap i kraftforsyningen. Målet om en sikker kraftforsyning handler både om å opprettholde og forbedre forsyningssikkerheten, minimere konsekvensene av avbrudd og gjenopprette forsyningen på en effektiv måte ved eventuelle avbrudd. Det framheves at kraftforsyningen er en sentral del av Norges kritiske infrastruktur, og at tilgang på elektrisk kraft blir stadig viktigere for å kunne opprettholde normal aktivitet i samfunnet, sikre kritiske samfunnsfunksjoner i krisesituasjoner og opprettholde landets forsvarsevne under beredskap og i krig.

I Meld. St. 25 (2015–2016) *Kraft til endring – Energipolitikken mot 2030*, jf. Innst. 401 S (2015–2016), går det fram at styrket forsyningssikkerhet er et av målene i årene framover, og at samfunnets krav til forsyningssikkerhet er økende. Det framheves at kompleksiteten i energiforsyningen har økt, og at pålitelige driftskontrollsystemer er av avgjørende betydning for effektiv ledelse og drift, håndtering av ekstraordinære situasjoner og rask gjenoppretting ved utfall. Dette gjør at avhengigheten av IKT i energiforsyningen er stor. Det påpekes videre at den teknologiske utviklingen gir behov for økt oppmerksomhet om IKT-sikkerhet, inkludert sikker databehandling og personvern.

Ifølge Meld. St. 38 (2016–2017) *IKT-sikkerhet – Et felles ansvar,* jf. Innst. 187 S (2017–2018), er sentrale tiltak for bedre IKT-sikkerhet i energiforsyningen blant annet å

- styrke tilsyn og veiledning med IKT-sikkerhet
- stimulere til større og mer ressurssterke fagmiljøer innenfor IKT-sikkerhet
- bygge et sterkt operativt fagmiljø for IKT-hendelseshåndtering (KraftCERT)
- vurdere de sikkerhetsmessige forholdene ved å behandle og lagre kraftsensitiv informasjon i utlandet
- gjennomføre risiko- og sårbarhetsanalyse for utvidet bruk av AMS
- utarbeide en oppdatert analyse av kraftforsyningens avhengighet av ekom

I innstillingen til meldingen støtter justiskomiteen regjeringens arbeid med å legge til rette for et styrket samarbeid på tvers av private og offentlige virksomheter for å avdekke og redusere digital sårbarhet i samfunnet.

3.2 Olje- og energidepartementets styring og oppfølging av NVEs arbeid med IKT-sikkerhet i kraftforsyningen – mål og krav

Instruks for departementenes arbeid med samfunnssikkerhet (samfunnssikkerhetsinstruksen) setter krav til departementenes arbeid med samfunnssikkerhet. Det følger av instruksen at Olje- og energidepartementets arbeid med samfunnssikkerhet skal være basert på systematisk risikostyring. Departementet skal kunne dokumentere at det avklarer og beskriver sentrale roller og ansvarsområder innenfor samfunnssikkerhet i sektoren, gjør systematiske risiko- og sårbarhetsanalyser av hendelser som kan true sektorens funksjonsevne, iverksetter nødvendige kompenserende tiltak og utarbeider mål for samfunnssikkerhetsarbeidet i sektoren. Departementet skal ivareta ansvaret for krisehåndtering i sektoren, som blant annet innebærer å ha et planverk for håndtering av uønskede hendelser og sørge for at det øves målrettet i egen sektor og tverrdepartementalt. Som ansvarlig for kritisk infrastruktur skal Olje- og energidepartementet også sørge for at det utarbeides risiko- og sårbarhetsanalyser for kraftforsyningen, og ha oversikt over tilstanden knyttet til sårbarheter for kraftforsyningen.[10]

Olje- og energidepartementet har ifølge *reglement for økonomistyring i staten* (økonomireglementet) og *bestemmelser om økonomistyring i staten* (økonomibestemmelsene) det overordnede ansvaret for at NVE gjennomfører aktiviteter i samsvar med målene i Stortingets vedtak og forutsetninger. Grunnleggende styringsprinsipper er at det skal fastsettes mål- og resultatkrav, og at disse skal oppnås på en effektiv måte. Departementets styring må tilpasses virksomhetens egenart samt risiko og vesentlighet.

[10] Samfunnssikkerhetsinstruksen, del 4 og 5; Direktoratet for samfunnssikkerhet og beredskap (2019) *Veileder til samfunnssikkerhetsinstruksen*.

I økonomireglementet og økonomibestemmelsene går det videre fram at departementet har et overordnet ansvar for at NVE har et fungerende og forsvarlig system for internkontroll, og at etaten bruker tildelte ressurser effektivt og forvalter oppgaver på en forsvarlig måte. Departementet skal sørge for at det blir gjennomført evalueringer for å skaffe kunnskap om måloppnåelse og resultater på området. Frekvensen og omfanget av evalueringer skal bestemmes ut fra virksomhetens egenart, risiko og vesentlighet. Behovet må vurderes opp mot kvaliteten på og omfanget av øvrig rapportering.

3.3 NVEs arbeid med IKT-sikkerhet i kraftforsyningen – mål og krav

NVE er beredskapsmyndighet etter *lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m.* (energiloven) kapittel 9 og *forskrift om delegering av myndighet etter energiloven til Norges vassdrags- og energidirektorat*.

Beredskapsmyndigheten (NVE) skal samordne beredskapsarbeidet og utpeke KBO (Kraftforsyningens beredskapsorganisasjon).[11] KBO består av KBO-enhetene (større kraftprodusenter, nettselskaper og fjernvarmeselskaper), kraftforsyningens distriktssjefer og beredskapsmyndigheten samt kraftforsyningens sentrale ledelse når denne trer i kraft. Kraftforsyningens distriktssjefer skal bidra til å tilrettelegge for hensiktsmessig samarbeid om forebygging og håndtering av ekstraordinære situasjoner i sitt distrikt. Kraftforsyningens sentrale ledelse består av beredskapsmyndigheten med deltakelse fra Statnett SF. I ekstraordinære situasjoner som kan skade eller hindre produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme, kan KBO pålegges oppgaver og plikter. Under beredskap og krig kan OED vedta at kraftforsyningen underlegges KBO, og i slike tilfeller overtar kraftforsyningens sentrale ledelse ansvaret for kraftforsyningen.

Ett av NVEs fire hovedmål er å fremme en sikker kraftforsyning. For å nå dette målet skal NVE overvåke og analysere utviklingen i kraft- og effektbalansene på kort og lang sikt, ha god oversikt over kraftsituasjonen i ulike regioner, være forberedt på mulige knapphetssituasjoner og påse at beredskapen i energiforsyningen er god og i tråd med gjeldende krav. NVE skal ha god kunnskap om forsyningssikkerheten i kraftsystemet.[12]

NVE er ansvarlig for å føre kontroll med at pålegg som er nødvendige for å gjennomføre bestemmelser i eller i medhold av energiloven, jf. § 10-1, og *forskrift om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m.* (energilovforskriften), jf. § 9-2, overholdes. Etter kraftberedskapsforskriften § 8-1 skal beredskapsmyndigheten (NVE) føre kontroll med at bestemmelsene i forskriften overholdes.

I Meld. St. 25 (2015–2016) *Kraft til endring – Energipolitikken mot 2030*, jf. Innst. 401 S (2015–2016), går det fram at NVE kontinuerlig skal utvikle regelverket på IKT-sikkerhetsområdet, veilede og samarbeide med bransjen og gjennomføre tilsyn og øvelser for å styrke IKT-sikkerheten i energiforsyningen. Det framheves at regjeringen setter arbeidet med IKT-sikkerhet høyt, og støtter opp om NVEs prioritering av IKT-sikkerhet i kraftsektoren. Ifølge meldingen må myndighetene bygge opp sin egen kompetanse, slik at de får god forståelse for risikobildet i forbindelse med ansvaret de har for regelverksutviklingen.

Ifølge økonomireglementet har NVEs ledelse ansvar for å gjennomføre aktiviteter som er i tråd med Stortingets vedtak og forutsetninger og med mål og prioriteringer fastsatt av Olje- og energidepartementet. Grunnleggende styringsprinsipper er at det skal fastsettes mål og resultatkrav, og at disse skal oppnås på en effektiv måte. Virksomhetens ledelse skal planlegge og utarbeide strategier med ettårig og flerårig perspektiv tilpasset virksomhetens egenart. Planene skal dokumenteres gjennom interne styringsdokumenter. Virksomheten skal sikre tilstrekkelig styringsinformasjon og beslutningsgrunnlag for å følge opp aktivitetene og resultatene. I virksomhetens rapportering skal det legges vekt på måloppnåelse og resultater. Dette kan omfatte innsatsfaktorer, aktiviteter, produkter og tjenester samt effekter for brukere og samfunn. Ledelsen skal foreta prioriteringer med ettårig og flerårig perspektiv innenfor eget ansvarsområde.

I økonomireglementet står det at alle virksomheter skal etablere systemer og rutiner som har innebygget internkontroll, for å sikre at måloppnåelse og resultater står i et tilfredsstillende forhold til fastsatte mål og resultatkrav, og at eventuelle vesentlige avvik forebygges, avdekkes og korrigeres i nødvendig utstrekning. Ifølge veilederen i internkontroll som er utarbeidet av Direktoratet for forvaltning og økonomistyring, handler internkontroll i praksis om å etablere og bruke strukturer og systemer som gir nødvendig trygghet for at oppgaver blir utført med ønsket kvalitet og effektivitet. Målrettet og effektiv drift innebærer at virksomhetens

[11] Energiloven § 9-1.
[12] Prop. 1 S (2018–2019) Olje- og energidepartementet, jf. Innst. 9 S (2018–2019).

kjerne-, støtte- og styringsprosesser er utformet, gjennomført og fulgt opp på en måte som bidrar til at fastsatte mål og krav blir oppfylt.

I St.meld. nr. 19 (2008–2009) *Ei forvaltning for demokrati og fellesskap* går det fram at tilsynsvirksomhet skal ta utgangspunkt i der det er størst risiko, og der sjansene for reduksjon av risiko er størst. For å sikre at tilsynsvirksomheten innrettes mest mulig effektivt, bør det dermed ligge risiko- og vesentlighetsvurderinger til grunn for tilsynsvirksomheten. Gode risiko- og vesentlighetsvurderinger krever at tilsynsorganet har god kjennskap til området det føres tilsyn med. Det tilsier at områdeovervåking bør ligge til grunn for risiko- og vesentlighetsvurderingen. Områdeovervåking beskrives i NOU (2004: 17) *Statlig tilsyn med kommune-sektoren* som innhenting, systematisering og tolking av kunnskap som er samlet inn på tilsynsfeltet.

Ifølge økonomireglementet skal NVE sørge for at det gjennomføres evalueringer for å få informasjon om måloppnåelse og resultater innenfor hele eller deler av virksomhetens ansvarsområde og aktiviteter. Frekvensen og omfanget av evalueringene skal bestemmes ut fra virksomhetens egenart, risiko og vesentlighet. For tilsynsvirksomheten kan dette innebære å evaluere om planleggingen, gjennomføringen og oppfølgingen av tilsyn er enhetlig, og om tilsynsmetodikken er tilpasset området det føres tilsyn med, og om sanksjonsmulighetene er effektive. Tiltak som iverksettes, skal revurderes i den grad resultatene ikke samsvarer med målene, jf. St.meld. nr. 19 (2008–2009) *Ei forvaltning for demokrati og fellesskap*.

Etter *lov om behandlingsmåten i forvaltningssaker* (forvaltningsloven) har forvaltningsorganer et selvstendig ansvar for å sørge for at en sak er så godt opplyst som mulig, ved utarbeiding av regelverk eller forskrifter. I god forvaltningsskikk er det sentralt å utrede konsekvensene av et nytt regelverk grundig, jf. *instruks om utredning av statlige tiltak* (utredningsinstruksen). Offentlige og private institusjoner og organisasjoner som er berørt av forskriften (tiltaket), skal involveres tidlig, så langt det er hensiktsmessig. Ifølge utrednings-instruksen skal forslag til lover og forskrifter og forslag til tiltak med vesentlige virkninger normalt legges ut på høring, og høringene skal være åpne for innspill fra alle. Høringsfristen skal normalt være tre måneder og ikke mindre enn seks uker. Et forvaltningsorgan har en alminnelig veiledningsplikt innenfor sitt saksområde. Formålet med veiledningsplikten er å gi parter og andre interesserte adgang til å ivareta interessene sine på best mulig måte.

NVE er som beredskapsmyndighet utpekt som sektorvist responsmiljø for IKT-sikkerhetshendelser, jf. kraftberedskapsforskriften § 3-6. Beredskapsmyndigheten er videre gitt fullmakt til å delegere oppgaver innenfor varsling, informasjonsdeling og analyse av IKT-sikkerhetshendelser i kraftforsyningen til én eller flere KBO-enheter. KraftCERT ble i 2014 utpekt som KBO-enhet med responsfunksjon for IKT-sikkerhets-hendelser, for å være en ressurs for beredskapsmyndigheten. I juni 2019 tildelte NVE KraftCERT midler for å styrke sikkerhetsarbeidet i kraftsektoren. Målet var at alle selskaper med betydning for den nasjonale kraftforsyningen skal være omfattet av et felles regime for utveksling og deling av IKT-sikkerhetsinformasjon. KraftCERT skal ivareta varsling, informasjonsdeling og analyse av sikkerhetsinformasjon knyttet til hendelser, sårbarheter og trusler for samtlige KBO-enheter på vegne av beredskapsmyndigheten.[13]

3.4 IKT-sikkerhet i selskapene – mål og krav

Energiforsyningen er samfunnskritisk infrastruktur, og selskapene er underlagt krav om sikkerhet og beredskap gjennom energiloven med forskrifter, blant annet kraftberedskapsforskriften. KBO-enhetene skal sørge for at virksomheten er innrettet på en slik måte og med nok ressurser til at de kan ivareta det ansvaret og de oppgavene de har etter energiloven.

Ifølge energiloven § 3-1 må alle anlegg for produksjon, omforming, overføring og fordeling av elektrisk energi ha konsesjon. I lovens § 3-5 går det fram at departementet kan sette vilkår for konsesjoner, blant annet om konsesjonærens organisasjon og kompetanse. Den som har fått konsesjon, skal påse at anlegget, driften av anlegget eller virksomheten oppfyller kravene i eller i medhold av energiloven. Virksomhetene skal sørge for effektiv sikring og beredskap, iverksette tiltak for å forebygge, håndtere og begrense virkningene av ekstraordinære situasjoner og gjenopprette den normale situasjonen, jf. energiloven § 9-2.

Beredskapsforskriften fra 2013 stilte krav til KBO-enhetenes arbeid med IKT-sikkerhet, både gjennom generelle krav til varsling, risikovurderinger, beredskapsplaner og internkontrollsystem (kapittel 2), krav til ressurser og reparasjonsberedskap (kapittel 4), generelle sikringskrav (kapittel 5), krav til informasjonssikkerhet (kapittel 6) og mer spesifikke krav til driftskontrollsystemer (kapittel 7).

[13] NVE (2019) *Tildeling av midler til KraftCERT i 2019*. Brev til KraftCERT, 07.06.2019.

Kraftberedskapsforskriften ble revidert med virkning fra 1. januar 2019. Endringene tydeliggjorde blant annet kravene til sikring av IKT-systemer ved at det ble stilt krav til grunnsikring for alle digitale informasjonssystemer, jf. § 6-9.

Formålet med kraftberedskapsforskriften er å sikre at kraftforsyningen opprettholdes, og at normal forsyning gjenopprettes på en sikker og effektiv måte i og etter ekstraordinære situasjoner for å redusere de samfunnsmessige konsekvensene. KBO-enhetene skal uten ugrunnet opphold varsle beredskaps-myndigheten om ekstraordinære situasjoner. De skal uten ugrunnet opphold og senest innen tre uker *skriftlig* innrapportere uønskede hendelser til beredskapsmyndigheten.

I energiloven § 9-3 og kraftberedskapsforskriften kapittel 6 om informasjonssikkerhet er det satt krav om at alle enheter i KBO skal vurdere sikkerheten ved all behandling av informasjon om kraftforsyningen. Enhetene skal kartlegge hvilken informasjon som er sensitiv, hvor den befinner seg, og hvem som har tilgang til den. De skal etablere effektiv avskjerming og beskyttelse av sensitiv informasjon og hindre at andre enn rettmessige brukere får adgang eller kjennskap til den.

KBO-enhetene skal utpeke en beredskapsleder som skal sørge for nødvendig planlegging og utøvelse av beredskapsarbeidet, en beredskapskoordinator som skal ha oversikt over beredskapsarbeidet i virksomheten og være administrativt kontaktpunkt til beredskapsmyndigheten, og en IKT-sikkerhets-koordinator som skal ha oversikt over IKT-sikkerhetsarbeidet i virksomheten og være faglig kontaktpunkt til beredskapsmyndigheten om IKT-sikkerhet. KBO-enhetene skal gjennomføre risikovurderinger om ekstra-ordinære forhold og ha et oppdatert beredskapsplanverk. Videre skal de gjennomføre øvelser slik at de er forberedt på å håndtere alle ekstraordinære situasjoner, og både ekstraordinære situasjoner og øvelser skal evalueres. De skal også ha et internkontrollsystem som dokumenterer og sikrer at krav etterleves. KBO-enhetene skal ha en sikkerhetsinstruks som sikrer at kravene til informasjonssikkerhet ivaretas. Ifølge kraftberedskapsforskriftens bestemmelser om anskaffelser skal KBO-enhetene påse at leverandører er forpliktet til å etterleve bestemmelsene om informasjonssikkerhet og taushetsplikt for kraftsensitiv informasjon. Avtalene skal sikre at KBO-enhetene har rett til å kontrollere, herunder revidere, at leverandøren etterlever bestemmelsene.

I kraftberedskapsforskriften kapittel 7 er det satt krav om at virksomheter med driftskontrollsystemer skal sørge for at disse til enhver tid virker etter sin hensikt og er beskyttet mot alle typer uønskede hendelser. Virksomheter skal blant annet fastsette interne sikkerhetsregler for driftskontrollsystemet og kontrollere brukertilgangen til systemet. Virksomheter skal til enhver tid skal ha tilstrekkelig autorisert personell med nødvendig kompetanse, slik at driftskontrollfunksjonen kan utøves uten ugrunnet opphold, og ha kontroll med ekstern tilkobling til driftskontrollsystemet. I tillegg er det gitt særskilte krav til driftskontrollsystemer i klasse 2 og 3, blant annet at virksomheten skal kunne betjene og manuelt styre anlegg som inngår i virksomhetens driftskontrollsystem dersom driftssentralen blir utilgjengelig. For klasse 2- og 3-selskaper er det også satt krav om at samband i driftskontrollsystemet skal fungere uavhengig av funksjonssvikt i offentlige elektroniske kommunikasjonsnett.

I kraftberedskapsforskriften § 6-9 stilles det krav om at virksomheter skal sikre digitale informasjonssystemer slik at konfidensialitet, integritet og tilgjengelighet ivaretas. Virksomheter skal ha en grunnsikring for digitale informasjonssystemer i henhold til anerkjente standarder og normer. I NVEs foreløpige tilleggsveileder til kraftberedskapsforskriften står det at kravene bygger på NSMs grunnprinsipper for IKT-sikkerhet. NSMs grunnprinsipper definerer et sett med prinsipper og underliggende tiltak for å beskytte informasjonssystemer, data og tjenestene de tilbyr, mot uautorisert tilgang, skade eller misbruk. Grunnprinsippene beskriver hva en virksomhet bør gjøre for å sikre et IKT-system og hvorfor, men ikke hvordan (funksjonsbaserte krav). NSMs grunnprinsipper er et supplement til eksisterende nasjonale og internasjonale regelverk, standarder og rammeverk innenfor IKT-sikkerhet. NSM påpeker at der det finnes bransje-, teknologi- eller sektorspesifikt materiale, bør dette benyttes i tillegg til de generelle standardene som ISO/IEC 27000-serien og NSMs grunnprinsipper.

I Meld. St. 25 (2015–2016) *Kraft til endring – Energipolitikken mot 2030*, jf. Innst. 401 S (2015–2016), framheves det at det å sikre stabil drift, sørge for god IKT-sikkerhet samt å ha evnen til å håndtere feil og sikkerhetshendelser vil kreve kompetent personell. Det framheves at det er risiko for at selskapene i kraftforsyningen i for stor grad kan bli avhengig av leverandører. Det framheves at det er viktig at selskapene signaliserer et tydelig fokus på IKT-sikkerhet til sine leverandører og kontinuerlig bygger kompetanse i selskapene omkring IKT-drift og IKT-sikkerhet. Meldingen framhever også at myndighetene på samme måte

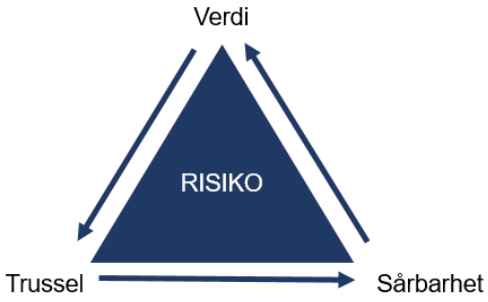
må bygge egen kompetanse for å kunne forstå risikobildet i forbindelse med ansvaret de har for regelverksutviklingen.

Forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv. (forskrift om kraftomsetning og nettjenester, også kalt avregningsforskriften) stiller tekniske krav til elektronisk informasjonsutveksling, jf. § 1-4, samt til kvalitetssikring og migrering av data til Elhub, § jf. 1-6. Forskriften omhandler også nettselskapenes ansvar for sikkerheten i AMS, som blant annet skal hindre misbruk av data og uønsket tilgang til styrefunksjoner, jf. § 4-2.

Statnett SF, som er et statsforetak eid av Olje- og energidepartementet, er systemansvarlig for det norske kraftsystemet, jf. *forskrift om systemansvaret i kraftsystemet*. Statnett har ansvar for driften av kraftsystemet og for at det til enhver tid er balanse mellom produksjon og forbruk av kraft. Statnett eier og drifter det sentrale overføringssystemet.

4 Risiko for IKT-angrep som rammer kraftforsyningen

I dette kapitlet ser vi nærmere på informasjon som belyser risikoen for IKT-angrep som rammer kraftforsyningen. Hensikten er å gi et bakteppe for vurderingen av NVEs arbeid med IKT-sikkerhet i kraftforsyningen i de øvrige kapitlene i rapporten. Vi beskriver risikoen som en funksjon av *verdien* IKT-systemene har for kraftforsyningen, *trusselbildet* for IKT-angrep og *sårbarhet* i form av svakheter i selskapenes arbeid med IKT-sikkerhet. Denne modellen omtales ofte som risikotrekanten.[14]



4.1 Relevante føringer

- KBO-enhetene er underlagt krav til IKT-sikkerhet i energiloven og kraftberedskapsforskriften, som blant annet inneholder
  - generelle krav til risikostyring og dokumentasjon av selskapenes internkontrollsystem
  - mer detaljerte regler for sikkerhetstiltak, dokumentasjon og kontroll av sikkerhetsnivået
- For å konkretisere lovkravene har vi anvendt NSMs grunnprinsipper for IKT-sikkerhet.

4.2 Oppsummering

- Det er risiko for at et IKT-angrep kan ramme kraftforsyningen, noe som vil kunne få store konsekvenser for samfunnet.
- Kraftforsyningen er som kritisk infrastruktur spesielt utsatt for etterretning og er et mål i kriser og i krig.
- Undersøkelsen viser at det er svakheter ved selskapenes arbeid med IKT-sikkerhet i undersøkelsesperioden, blant annet ved selskapenes
  - internkontrollsystem, som skal sikre etterlevelse og fange opp svakheter og mangler i IKT-sikkerhetsarbeidet
  - risikovurderinger og beredskapsplaner
  - kravstilling til og oppfølging av leverandører
  - tekniske tiltak for å sikre og overvåke IKT-systemene
  - gjennomføring av evalueringer og sikkerhetsrevisjoner
- For lite IKT-sikkerhetskompetanse er en utfordring i kraftforsyningen.
- Selskapenes sikring av IKT-systemene og beredskap ved IKT-hendelser er i stor grad avhengig av leverandørene.

4.3 Trusselbildet og konsekvenser av IKT-angrep mot kraftforsyningen

I Prop. 1 S (2018–2019) fra Olje- og energidepartementet framheves det at kraftforsyningen er en sentral del av Norges kritiske infrastruktur, og at tilgang på elektrisk kraft blir stadig viktigere for å kunne opprettholde normal aktivitet i samfunnet, sikre kritiske samfunnsfunksjoner i krisesituasjoner og opprettholde landets forsvarsevne under beredskap og i krig.

NVEs statistikk viser at leveringspåliteligheten for strømforsyningen i Norge har ligget på over 99,96 prosent de siste 20 årene.[15] NVE opplyser i intervju at det fram til nå ikke har forekommet IKT-angrep som har ført til avbrudd i kraftforsyningen. NVE og sikkerhetsmyndighetene trekker likevel fram risikoen for at IKT-angrep kan ramme kraftforsyningen, og framhever betydningen av at selskapene i kraftforsyningen sikrer seg mot alvorlige IKT-angrep. Selv om kraftforsyningen er lite utsatt i fredstid, øker faren for aksjoner mot kraftforsyningen i kriser, og i krig er kraftforsyningen et klart utsatt mål.[16] Statistikken for leverings-påliteligheten i fredstid reflekterer dermed ikke risikoen for et alvorlig IKT-angrep i krisesituasjoner og krig.

[14] NSM (2017) *Risiko og sårbarheter i en ny tid.*
[15] NVE (2020) *Driften av kraftsystemet 2019.* RME-rapport nr. 3/2020.
[16] Fridheim, H., J. Hagen og S. Henriksen (2007) *En sårbar kraftforsyning - Sluttrapport etter BAS3.*

4.3.1 IKT-systemene

Selskapene i kraftforsyningen bruker driftskontrollsystemer til å overvåke og styre anleggene i kraftforsyningen. Driftskontrollsystemene er klassifisert etter forskriftsfestede kriterier som handler om hvor vesentlige anleggene systemene styrer, er, eller hvor stor del av befolkningen som er avhengig av systemene for å få levert strøm. Jo mer vesentlig et driftskontrollsystem regnes for å være, desto strengere krav stilles det til sikkerhetstiltak. Etter at AMS-målere ble installert, kan nettselskapene ved hjelp av IKT-systemer lese av strømforbruk, jordfeil og effekt og koble inn og ut (bryte) strømforsyningen til forbrukerne.[17] Store enkeltbrukere som industribedrifter har ikke målere som kan koble fra strømmen. De øvrige IKT-systemene som brukes i selskapene (for eksempel kundebehandlingssystemer, regnskapssystemer, e-postsystemer og tilhørende servere og klienter), kalles administrative systemer og er i utgangspunktet mindre kritiske for kraftforsyningen.[18] Mens driftskontrollsystemene tidligere var separert fra de administrative systemene, er de i dag koblet sammen og atskilt med logiske skiller.[19] De logiske skillene filtrerer og begrenser hvilken datatrafikk som når driftskontrollsystemene. NVE skrev i 2018 at de fleste uønskede IKT-hendelser har sitt opphav i administrative systemer, og at avanserte trusselaktører ofte bruker administrative systemer som inngangsport til de mer kritiske driftskontrollsystemene.[20] NVE viser til cyberangrepet som rammet strømforsyningen i Ukraina i 2015, som et eksempel på dette, se faktaboks 2.

Bortfall av IKT-systemer for driftskontroll vil ikke i seg selv vil føre til strømavbrudd siden dette bare påvirker selskapets fjernovervåking og -styring, men det vil kunne gi en utfordrende situasjon siden selskapene da må styre anleggene manuelt. Dersom en trusselaktør får tilgang til og manipulerer et selskaps driftskontroll-systemer og brytefunksjonaliteten til AMS-målerne, vil det i verste fall også kunne ramme strømforsyningen til forbrukerne.[21]

4.3.2 Trusselvurderinger

Politiets sikkerhetstjeneste (PST) og NSM peker i sine trussel- og risikovurderinger for 2020 på at kraftsektoren er spesielt utsatt for etterretning. Ifølge PST må aktører i petroleums- og energisektoren regne med at de vil være utsatt for avanserte nettverksoperasjoner. I de aller fleste nettverksoperasjonene PST har sett, er inntrengerne interessert i å hente ut informasjon fra virksomheten. Internasjonalt har de imidlertid også sett eksempler på at trusselaktører har evne og vilje til både å manipulere informasjon og sabotere digitale systemer. Ifølge NSM kan trusselaktører kartlegge sårbarheter i kritisk infrastruktur for å forberede framtidige sabotasjehandlinger. Etterretningstjenesten påpeker at terskelen for å gjennomføre dyptgripende, digital sabotasje er høy fordi en slik operasjon kan oppfattes som en krigshandling, men framhever at veien

[17] NVE (2020) *Smarte strømmålere (AMS)*. Hentedato 25.10.20.
[18] NVE (2017) *Regulering av IKT-sikkerhet.* NVE-rapport nr. 26/2017; NVE (2018) *Oppsummeringsdokument: Endringer i beredskapsforskriften - Krav til IKT-sikkerhet m.m.* NVE-rapport nr. 92/2018.
[19] NOU (2015: 13) *Digital sårbarhet – sikkert samfunn.*
[20] NVE (2018) *Oppsummeringsdokument: Endringer i beredskapsforskriften - Krav til IKT-sikkerhet m.m.* NVE-rapport nr. 92/2018.
[21] Prop. 1 S (2017–2018) Olje- og energidepartementet.

fra evne til faktiske handlinger har blitt kortere.[22] NSM framhever at trusselaktører utvikler metodene sine raskere enn det utvikles mottiltak. Dette bidrar til at risikobildet forverres, og til at IKT-hendelsenes konsekvenser for samfunnet blir større.[23] DSB peker på at dataangrep mot kritiske samfunnsfunksjoner kan få konsekvenser i store deler av samfunnet, og at dette gjelder særlig dersom kraftforsyningen rammes.[24]

NVE utfører ikke egne trusselvurderinger for kraftforsyningen, men benytter seg av sikkerhetsmyndighetenes offentlige trusselvurderinger. I NVEs overordnede risikovurderinger i 2019 og 2020 trekker etaten fram risikoen for at kraftforsyningen rammes av cyberangrep, som en av tre risikoer under risikoområdet «Forsyningssikkerhet».

NVE har siden 2016 på oppdrag fra Olje- og energidepartementet gjennomført risiko- og sårbarhetsanalyser (ROS-analyser) av sjeldne scenarioer som kan true kraftforsyningen. Bakgrunnen for dette er departementets ansvar etter samfunnssikkerhetsinstruksen, som pålegger hovedansvarlige departementer å ha risiko- og sårbarhetsanalyser for de kritiske samfunnsfunksjonene. I ROS-analysene fra NVE er blant annet risikoen for IKT-angrep inkludert. Det går fram av Prop. 1 S (2017–2018) fra Olje- og energidepartementet at det er vanskeligere å vurdere sannsynligheten for tilsiktede hendelser enn for naturhendelser. De statistiske dataene for sistnevnte hendelser er langt mer omfattende og kan også gå langt tilbake i tid.

4.3.3 IKT-angrep

NVE skal varsles om IKT-hendelser, som nærmere beskrevet i punkt 8.5.1. Det har ikke forekommet IKT-angrep som har ført til avbrudd i kraftforsyningen i Norge. NVE har registrert om lag 30 uønskede hendelser knyttet til IKT-systemer og informasjonssikkerhet i selskapene i perioden 2016–2019. Dette inkluderer tilfeller av krypteringsvirus og inntrengingsforsøk i IKT-systemer, mislykkede oppdateringer av programvare, brudd på besøksrestriksjoner for driftssentraler og lekkasjer av kraftsensitiv informasjon. Enkelte hendelser har rammet selskapers driftskontrollsystemer. Disse skyldes svikt i fysisk utstyr tilknyttet driftskontrollsystemet og mislykkede oppdateringer, og ikke IKT-angrep.

KraftCERT har fått informasjon om hendelser fra medlemmene siden opprettelsen i 2014 og skal etter endringen i kraftberedskapsforskriften i 2019 motta varsler om IKT-hendelser fra alle KBO-enheter. KraftCERT behandlet om lag 150 og 200 uønskede IKT-hendelser hos medlemsselskapene i henholdsvis 2018 og 2019. Av disse har 20–50 i året vært større hendelser der KraftCERT har opprettet en egen oppfølgingsprosess. Hendelser KraftCERT ble gjort kjent med i 2019, inkluderer store mengder nettfiske og lenker til skadevare, rekognosering og kompromitteringer[25], både hos leverandører og av selskapenes administrative systemer og driftskontrollsystemer.

Faktaboks 1 KraftCERT

I 2014 gikk Statnett, Statkraft og Hafslund sammen for å opprette KraftCERT, etter et initiativ fra NVE og NSM. KraftCERT ble samme år utpekt til KBO-enhet av NVE og inngikk en avtale med NSM om å ha CERT-funksjonen (Computer Emergency Response Team) i kraftsektoren. KraftCERT har som oppgave å hjelpe kraftbransjen med å forebygge og håndtere hendelser. Fra juni 2019 skal KBO-enhetene varsle alle uønskede IKT-hendelser til KraftCERT, og KraftCERT skal innhente og formidle IKT-sikkerhetsinformasjon til KBO-enhetene. Per november 2020 var 35 av om lag 170 KBO-enheter medlemmer av KraftCERT, inkludert de aller fleste av selskapene med de mest vesentlige driftskontrollsystemene.

KraftCERT oppgir at de fleste hendelsene som varsles til KraftCERT, gjelder administrative systemer, men påpeker at aktører kan bruke tilgangen til slike systemer som inngangsport til driftskontrollsystemene og dermed påvirke kraftforsyningen.[26] Ifølge KraftCERT kan derfor de fleste hendelser bli alvorlige dersom de ikke blir håndtert i tide. Angrepene mot strømforsyningen i Ukraina i 2015, som beskrives i faktaboks 2, er et

[22] Etterretningstjenesten (2019) *Fokus.*
[23] NSM (2017) *Helhetlig IKT-risikobilde 2017.*
[24] Direktoratet for samfunnssikkerhet og beredskap (2019) *Analyse av krisescenarioer 2019.*
[25] KraftCERT definerer kompromittering som «[e]t vellykket forsøk på å oppnå uautorisert tilgang til system, tjenester, ressurser eller informasjon, eller et vellykket forsøk på å kompromittere (forringe) konfidensialitet, integritet eller tilgjengelighet av system, tjeneste eller informasjon». NVE (2020) *Digital kontroll: en studie om innføring og bruk av metrikker i kraftforsyningen for bedre IKT-sikkerhet.* NVE-rapport nr. 22/2020.
[26] KraftCERT (2020) *Digital kontroll: en studie om innføring og bruk av metrikker i kraftforsyningen for bedre IKT-sikkerhet.* NVE-rapport nr. 22/2020.

eksempel på dette. Punkt 8.5 inneholder en nærmere beskrivelse av hendelser NVE og KraftCERT er blitt gjort kjent med.

Faktaboks 2 Cyberangrep mot strømforsyningen i Ukraina i 2015

I cyberangrepet mot ukrainske nettselskaper i 2015 brukte angriperne tilsynelatende legitime e-poster med infiserte vedlegg med skadevare for å få tilgang til selskapenes administrative IKT-systemer. Etter minst seks måneders tilstedeværelse i de administrative systemene tilegnet angriperne seg rettigheter som ga tilgang til driftskontrollsystemene gjennom eksterne tilkoblinger. Dette brukte de til å fjernstyre transformatorstasjoner for å forårsake strømbrudd hos kundene. Angriperne hindret nettselskapene i å reversere endringene som var gjort, og sørget for at selskapenes kundesenter ble oversvømt med forespørsler, slik at selskapene ikke kunne kommunisere med kundene som var rammet. Etter at selskapene hadde klart å gjenopprette strømforsyningen, måtte de drifte strømnettet manuelt, og to måneder etter angrepet måtte enkelte operasjoner fortsatt gjøres manuelt av nettselskapene. Ifølge Etterretningstjenesten tilsier hendelsene i Ukraina at målet ikke var å gjøre mest mulig skade, men å tilegne seg erfaring og kunnskap om sabotasjeoperasjoner mot blant annet strømforsyningen.

Kilde: NVE og Etterretningstjenesten[27]

4.4 Selskapenes arbeid med IKT-sikkerhet

I den foreløpige tilleggsveilederen til kraftberedskapsforskriften anbefaler NVE virksomhetene å integrere sikkerhet i virksomhetens aktiviteter og å etablere et styringssystem for informasjonssikkerhet som ivaretar systematikken for aktivitetene i IKT-sikkerhetsarbeidet, som illustrert i figur 1.

Figur 1 Styringshjul for arbeidet med IKT-sikkerhet

Kilde: Kraftberedskapsforskriften og NSMs veileder i sikkerhetsstyring.

I dette punktet (4.4) ser vi nærmere på svakheter som vi gjennom ulike kilder har identifisert hos KBO-enhetene når det gjelder aktivitetene i styringshjulet i figur 1.

[27] NVE (2017) *Regulering av IKT-sikkerhet.* NVE-rapport 26/2017; Sans Industrial Control Systems (2016) *Analysis of the Cyber Attack on the Ukrainian Power Grid;* Zetter, K. (2016) *Inside the cunning, unprecedented hack of Ukraine's power grid*; Etterretningstjenesten (2018) *Fokus.*

4.4.1 Overordnet informasjon om svakheter ved arbeidet med IKT-sikkerhet i selskapene

NVE fører tilsyn med at selskapene i kraftforsyningen oppfyller kravene til sikkerhet og beredskap i kraftberedskapsforskriften, som er hjemlet i energiloven. NVEs tilsyn med IKT-sikkerhet går i hovedsak ut på å føre tilsyn med driftskontrollsystemer og med informasjonssikkerhet. Tilsyn med informasjonssikkerhet ble innført i 2019 og omhandler i hovedsak kapittel 6 i kraftberedskapsforskriften, mens tilsyn med driftskontroll-systemer omhandler kapittel 7 i tillegg til generelle krav. I tillegg omfatter NVEs generelle beredskapstilsyn enkelte krav som kan være relevante for IKT-sikkerheten, som risikovurderinger, beredskapsplanlegging, internkontrollsystemer og beskyttelse av kraftsensitiv informasjon. Tabell 1 viser antall avvik avdekket i de rene IKT-sikkerhetstilsynene i perioden 2017–2019, fordelt på de ulike aktivitetene i figur 1.

I perioden 2017–2019 gjennomførte NVE 15 IKT-sikkerhetstilsyn, herunder 13 tilsyn med driftskontroll-systemer og 2 tilsyn med informasjonssikkerhet. De to tilsynene med informasjonssikkerhet ble gjennomført høsten 2019 etter innføringen av nye forskriftskrav.

Tabell 1 Antall avvik avdekket i NVEs tilsyn med IKT-sikkerhet i perioden 2017–2019

Krav i kraftberedskapsforskriften	Antall avvik
Planlegge og etablere rammer	
2-10 Internkontrollsystem	4
7-2 Interne sikkerhetsregler	2
Identifisere verdier og gjennomføre risikovurdering	
2-3 Risikovurdering	4
6-9 b Risikovurdering	1
7-3 Dokumentasjon av driftskontrollsystemet	2
Sikre, oppdage og håndtere	
2-4 Beredskapsplanlegging	4
5-6 Sikringstiltak for klasse 3	1
6-3 Beskyttelse, avskjerming og tilgangskontroll	1
6-8 Sikkerhetskopier	2
6-9 c Sikre og oppdage	2
6-10 Brytefunksjonalitet i AMS	1
7-4 Kontroll med brukertilgang	3
7-5 Kontroll ved endringer i driftskontrollsystemet	1
7-6 Kontroll med utstyr i driftskontrollsystemet	3
7-7 Håndtering av feil, sårbarheter og sikkerhetsbrudd	2
7-10 Ekstern tilkobling til driftskontrollsystem	1
7-14 a Sikkerhetskopier	1
7-14 c Overvåking og logging	2
7-14 f Ekstern tilkobling til driftskontrollsystemet	2
7-14 g Systemredundans	3
7-14 j Sikker tidsreferanse	2
Kontrollere	
6-9 f Sikkerhetsrevisjon	1
7-14 b Sikkerhetsrevisjon	3
Totalt	**48**

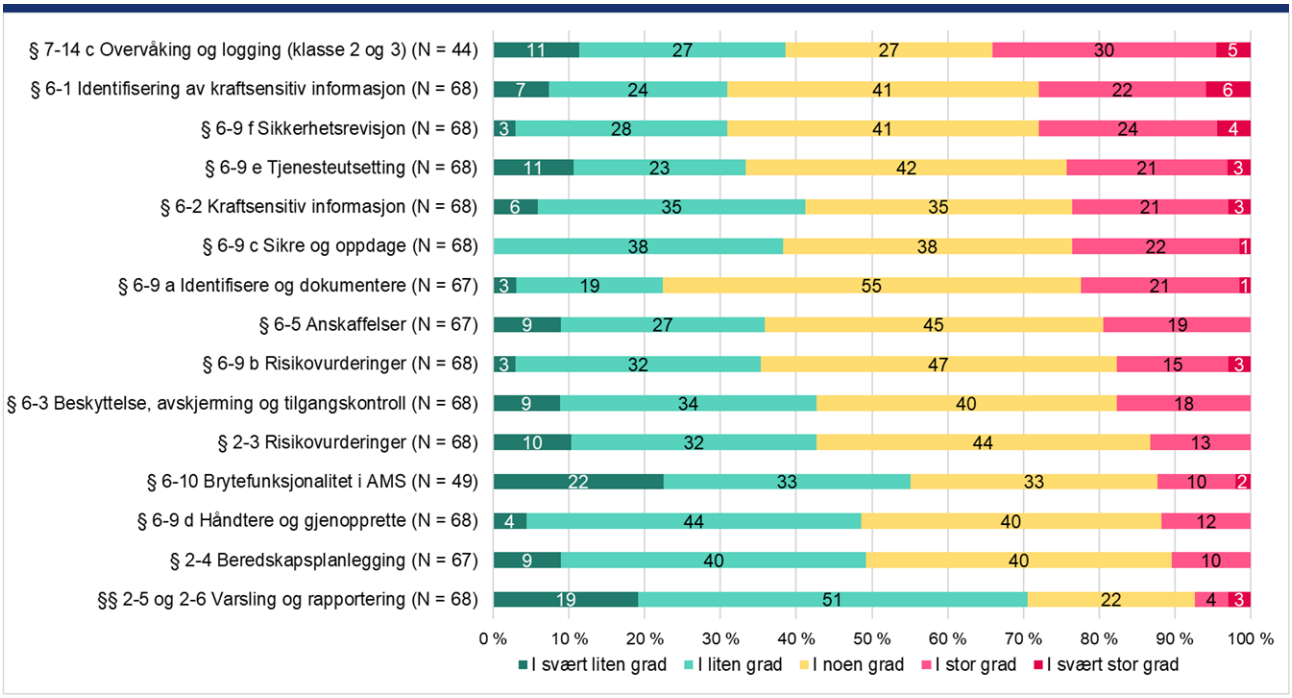
Kilde: NVEs tilsynsrapporter

NVE avdekket totalt 48 avvik i IKT-sikkerhetstilsynene. De fleste avvikene gjelder selskapenes etterlevelse av krav til internkontrollsystem, risikovurderinger og beredskapsplanlegging. En analyse av de generelle beredskapstilsynene i perioden 2017–2019 viser at NVE også ofte avdekket avvik ved disse kravene da. I NVEs årsrapport for 2017 ble mangelfulle risikovurderinger og beredskapsplaner trukket fram blant de mest alvorlige avvikene. 27 av avvikene i IKT-sikkerhetstilsynene gjelder krav om å beskytte driftskontroll-systemene. NVE oppgir at etaten ofte vurderer svakheter i beskyttelsen av driftskontrollsystemer som mer alvorlige enn svakheter i beskyttelsen av andre IKT-systemer. I NVEs prosedyrer for tilsyn står det at det ved tilsyn med sikkerhet i energiforsyningen kan være særlig aktuelt å bruke overtredelsesgebyr for manglende beredskapsplan, mangelfulle risikovurderinger og manglende sikkerhet rundt IKT-systemer. NVE varslet tre

selskaper om pålegg av overtredelsesgebyr fordi de brøt kravene til besøksrestriksjoner for driftssentraler i perioden 2017–2019. NVE skrev i 2019 at de ser alvorlig på slike brudd.[28]

NVE skriver i et faktaark i 2019 at norske kraftprodusenter og nettselskaper viser vilje til å prioritere IKT-sikkerheten, men at komplekse tjenester, mangelfull tilgang til kompetanse og endringer i leverandørmarkedet er utfordrende både for selskapene og myndighetene.[29] At det ikke har vært IKT-angrep som har ført til strømavbrudd i Norge, tyder ifølge NVE på at sektoren har systemer som bidrar til å motstå eller håndtere angrep som har alvorlige konsekvenser. NVE påpeker imidlertid at det også kan skyldes at selskapene ikke oppdager inntrengere som avventer angrep til senere. Ifølge KraftCERT har angripere lyktes med å komme seg på innsiden av selskapers IKT-systemer, både driftskontrollsystemer og administrative systemer. Til tross for at dette ikke har ført til strømavbrudd, viser det svakheter i selskapenes arbeid med å sikre systemene mot IKT-angrep.

Figur 2 IKT-sikkerhetskoordinatorenes svar på om utvalgte krav er utfordrende å etterleve

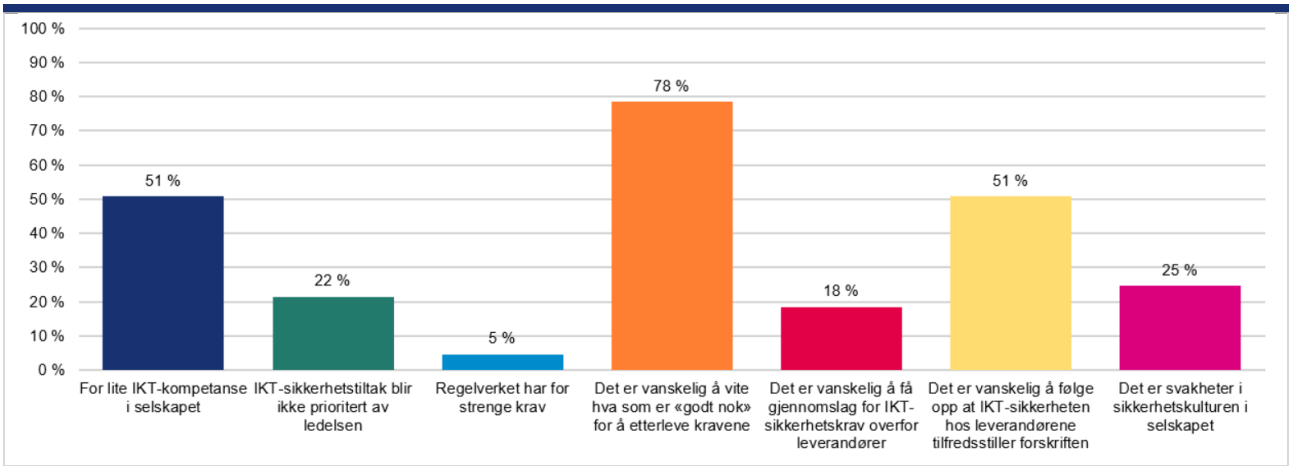


I vår spørreundersøkelse svarte i gjennomsnitt om lag 40 prosent av IKT-sikkerhetskoordinatorene[30] i selskapene at de utvalgte kravene i liten eller svært liten grad er utfordrende å etterleve. Kravene som høyest andel koordinatorer oppga som utfordrende å etterleve, er kravene til overvåking og logging i driftskontrollsystemer, identifisering av kraftsensitiv informasjon samt sikkerhetsrevisjon og tjenesteutsetting. Kravene til overvåking og logging i driftskontrollsystemer og sikring av brytefunksjonalitet i AMS er ikke relevante for alle selskapene. IKT-sikkerhetskoordinatorene som har svart på spørsmål med «Vet ikke / ikke aktuelt», er utelatt i figur 2.

Caseundersøkelsen viser svakheter ved de tre selskapenes rammeverk for IKT-sikkerhetsarbeidet, hvor de skal definere aktiviteter for systematisk internkontroll. Svake rammer for internkontroll vil påvirke alle deler av IKT-sikkerhetsarbeidet. Caseundersøkelsen viser også at de tre selskapene har svakheter i de fleste av aktivitetene som inngår i arbeidet med IKT-sikkerhet. Det er vesentlige mangler i selskapenes arbeid med å risikovurdere IKT-systemer som behandler kraftsensitiv informasjon, og i gjennomføringen av evalueringer og sikkerhetsrevisjoner. I tillegg er det svakheter i selskapenes kravstilling til og oppfølging av leverandører og svakheter i utvalgte tekniske sikkerhetstiltak. De ulike aktivitetene og tiltakene som ble undersøkt i caseundersøkelsen av de tre selskapenes IKT-sikkerhetsarbeid, beskrives nærmere i punktene nedenfor.

[28] NVE (2019) *Oppsummering av uønskede hendelser 2018 i energiforsyningen.* Faktaark nr. 4/2019.
[29] NVE (2019) *Tilstandsvurdering av forsyningssikkerhet og beredskap i kraftforsyningen.* Faktaark nr. 10/2019.
[30] IKT-sikkerhetskoordinatorene i KBO-enhetene skal ha oversikt over IKT-sikkerhetsarbeidet i virksomheten og være faglig kontaktpunkt til beredskapsmyndigheten om IKT-sikkerhet, jf. kraftberedskapsforskriften § 2-2.

Figur 3 IKT-sikkerhetskoordinatorenes svar på hvorfor det er utfordrende å etterleve enkelte av kravene i regelverket (N = 65)



I spørreundersøkelsen ble IKT-sikkerhetskoordinatorene som svarte at det var utfordrende å etterleve ett eller flere av de utvalgte kravene i kraftberedskapsforskriften (se figur 2), spurt om årsakene til dette. Figur 3 viser at nærmere 80 prosent av IKT-sikkerhetskoordinatorene oppga «Det er vanskelig å vite hva som er 'godt nok' for å etterleve kravene» som en årsak. NVE påpeker at dette kan ha en sammenheng med at flere av kravene det ble spurt om i spørreundersøkelsen, først kom inn i forskriften i 2019, og at den endelige veilederen til den nye forskriften ikke forelå på tidspunktet spørreundersøkelsen ble besvart. NVEs regelverk og veiledning beskrives nærmere i kapittel 6. Videre oppga om lag halvparten av IKT-sikkerhetskoordinatorene «Det er vanskelig å følge opp at IKT-sikkerheten hos leverandørene tilfredsstiller forskriften» som årsak. Utfordringer rundt tjenesteutsetting og leverandøroppfølging beskrives nærmere i punkt 4.4.5 og 4.5.

Om lag halvparten av IKT-sikkerhetskoordinatorene oppga «For lite IKT-kompetanse i selskapet» som en årsak til at det kan være vanskelig å etterleve kravene. Andelen som oppga dette, er høyere i de små og mellomstore selskapene (henholdsvis under 20 og under 100 ansatte) enn i de store selskapene. I NVEs rapport *Regulering av IKT-sikkerhet* fra 2017 ble det framhevet at det er et stort sprik mellom selskapene i kraftforsyningen med hensyn til IKT-sikkerhetskompetanse. I rapporten går det fram at flere selskaper, spesielt de største, har svært god kompetanse innenfor IKT og informasjonssikkerhet, men at det samtidig er flere selskaper som ikke har nok kompetanse på sikkerhet i informasjonssystemer. NC-Spectrum AS, et IKT-konsulentselskap som leverer tjenester til selskaper i kraftbransjen, mener at selskaper i kraftbransjen gjennomgående har manglende forståelse for hvor store sårbarheter digitalisering av systemene innebærer, og at sårbarhetsflaten, også mot driftskontrollsystemer, vil øke ytterligere framover. Selskapet mener at mange selskaper i kraftbransjen fortsatt har en stor jobb å gjøre for å redusere sårbarheten i systemene sine. Små selskaper kan ifølge NC-Spectrum AS ha utfordringer med å ansette personell med tilstrekkelig IKT-sikkerhetskompetanse, og sikkerheten til disse selskapene avhenger ofte av enkeltpersoner. Både NC-Spectrum og flere intervjuobjekter trekker imidlertid fram at mindre selskaper kan ha bedre oversikt over systemene sine og infrastrukturen sin enn større selskaper som har flere ansatte med IKT-kompetanse. Dette skyldes at større selskaper er mer komplekse fordi de har mange ansatte, spredt ansvar og en større systemportefølje.

4.4.2 Planlegge og etablere rammer

Kraftberedskapsforskriften stiller krav til selskapenes rammer for IKT-sikkerhetsarbeidet, blant annet gjennom krav til internkontrollsystem (§ 2-10), sikkerhetsinstruks (§ 6-4), ivaretakelse av informasjons-sikkerhet i anskaffelser (§ 6-5) og interne sikkerhetsregler (§ 7-2). Dersom en leverandør av varer eller tjenester kan bli kjent med kraftsensitiv informasjon, skal kontrakten med leverandøren inneholde opplysninger om informasjonssikkerhet, taushetsplikt og hvordan kravene skal overholdes.[31]

[31] NVE (2013) *Veiledning til forskrift om forebyggende sikkerhet og beredskap i energiforsyningen.*

NVE kontrollerer selskapenes internkontrollsystem ved tilsyn med driftskontrollsystemer og generelle beredskapstilsyn. I perioden 2017–2019 gjennomførte NVE totalt 13 tilsyn med driftskontrollsystemer og 61 tilsyn med generell beredskap og avdekket henholdsvis 4 og 27 avvik som gjaldt selskapenes internkontrollsystem. I tilsynsrapportene har NVE begrunnet avvikene med at selskapenes internkontrollsystem ikke inneholder dokumentasjon på at alle kravene i forskriften er på plass, at systemet ikke gjenspeiler den faktiske tilstanden, eller at det ikke fungerer etter hensikten.

I 2017 sendte NVE ut en spørreundersøkelse til 350 virksomheter i kraftbransjen.[32] Spørreundersøkelsen inneholdt spørsmål om hvilke IKT-sikkerhetshendelser og IKT-angrep virksomhetene hadde opplevd de siste tolv månedene, i tillegg til spørsmål om virksomhetenes avhengighet av leverandører og grad av tjenesteutsetting. 88 virksomheter svarte på undersøkelsen. Over halvparten av virksomhetene oppga at de helt eller delvis har tjenesteutsatt driften av administrativ IKT. En betydelig lavere andel oppga at de har satt ut driftskontrollfunksjonen, og av disse virksomhetene oppga henholdsvis 10 og 22 prosent at de har tjenesteutsatt den helt eller delvis. Ingen av de større virksomhetene (mer enn 100 ansatte) oppga at de har satt ut denne funksjonen.

I vår spørreundersøkelse svarte om lag 20 prosent av IKT-sikkerhetskoordinatorene i selskapene at det i stor eller svært stor grad er utfordrende å etterleve kravene til anskaffelser og tjenesteutsetting, se figur 2. NVE fikk i 2018 utarbeidet en rapport om utfordringene med å håndtere IKT-sikkerheten ved anskaffelser og leverandørforhold i energibransjen. Rapporten var basert på intervjuer med energiselskaper og leverandører av driftskontrollsystemer og AMS.[33] Flere av selskapene oppga at de ikke hadde rett til å føre tilsyn med leverandørene sine, mens leverandørene oppga at selskapene varierte med hensyn til om de kontraktsfestet krav om å gjennomføre tilsyn. Både leverandører og energiselskaper oppga at de ikke hadde oversikt over flere enn de nærmeste programvareleverandørene, og at de syntes det var utfordrende å ha kontroll over alle underleverandørene av maskinvare. Flere leverandører mente at energiselskapene ikke hadde tilfredsstillende bestillerkompetanse, og både leverandørene og energiselskapene mente at større selskaper hadde bedre sikkerhetskompetanse enn mindre selskaper. Energiselskapene opplevde at de fikk leverandører til å akseptere sikkerhetskravene, enten ved å redusere omfanget av tjenesteutsettingen eller ved å velge en annen leverandør. Flere av selskapene påpekte imidlertid at det ikke er enkelt å bytte leverandør dersom det viser seg at den eksisterende leverandøren ikke tilbyr tilstrekkelig sikkerhet.

Nettalliansen AS, hvor om lag 40 nettselskaper er medlemmer, opplever at det er lettere for Nettalliansen AS enn for enkeltselskaper å stille krav til leverandører. Når Nettalliansen AS kjøper inn IKT-systemer til selskapene i alliansen, krever de at leverandørene oppfyller kravene i kraftberedskapsforskriften. Også NC-Spectrum AS påpeker at selskapene hver for seg har liten makt til å få gjennom IKT-sikkerhetskrav i avtalene med leverandørene, og særlig i forhandlinger med store internasjonale leverandører har selskapene begrenset med markedsmakt. NC-Spectrum AS mener at mer konkrete IKT-sikkerhetskrav i kraftberedskapsforskriften ville gitt selskapene et bedre utgangspunkt for å forhandle med leverandørene om IKT-sikkerheten i produktene de kjøper.

Caseundersøkelsen viser at alle de tre selskapene har begynt å utarbeide rammeverk for arbeidet med IKT-sikkerhet. Selskapene har utarbeidet brukerinstruks og rutiner for taushetserklæringer, men de har ikke beskrevet interne krav til aktivitetene som inngår i et styringssystem for informasjonssikkerhet. Alle de tre selskapene har inngått avtaler med leverandører hvor de stiller et overordnet krav om at leverandørene skal oppfylle kravene i kraftberedskapsforskriften. Avtalene definerer imidlertid ikke hvilke av kravene leverandøren har ansvar for, hvordan det er forventet at leverandøren skal sikre systemene, eller hvordan implementerte sikkerhetstiltak skal evalueres og følges opp.

4.4.3 Identifisere verdier og gjennomføre risikovurdering

Selskapene skal identifisere kraftsensitiv informasjon (kraftberedskapsforskriften § 6-1) og identifisere og dokumentere verdier, leveranser, tjenester, systemer og brukere i de digitale informasjonssystemene sine (§ 6-9 a). Selskapene skal også gjennomføre risikovurdering av ekstraordinære forhold (§ 2-3) og av de digitale informasjonssystemene ved systemendringer (§ 6-9 b).

Caseundersøkelsen viser at alle de tre selskapene har utarbeidet oversikter over systemer hvor kraftsensitiv informasjon behandles eller lagres. De tre selskapene varierer med hensyn til hvor langt de har kommet med å identifisere og dokumentere verdikjeder og avhengigheter mellom de ulike IKT-systemene og tilhørende

[32] NVE (2017) *Informasjonssikkerhetstilstanden i energiforsyningen.* NVE-rapport nr. 74/2017.
[33] NVE (2018) *IKT-sikkerhet ved anskaffelser og tjenesteutsetting i bransjen.* NVE-rapport nr. 90/2018.

programvare, maskinvare og nettverk. Et av selskapene har utarbeidet scenariobaserte risikoanalyser for IKT-området, men dokumenterer ikke hvordan tiltak følges opp. De to andre selskapene har ikke dokumentert risikovurderinger på IKT-området, og dermed har de heller ikke dokumentert hvilke tiltak de har implementert for å håndtere risiko.

Identifisering av verdier

I vår spørreundersøkelse svarte om lag 30 prosent av IKT-sikkerhetskoordinatorene at det i stor eller svært stor grad er utfordrende å etterleve kravet om å identifisere kraftsensitiv informasjon (kraftberedskaps-forskriften § 6-1). Om lag 20 prosent svarte at det i stor eller svært stor grad er utfordrende å identifisere og dokumentere verdier, leveranser, tjenester, systemer og brukere i de digitale informasjonssystemene (kraft-beredskapsforskriften § 6-9 a), se figur 2. NVE startet i 2019 et prosjekt som skulle kartlegge forståelsen og praktiseringen av bestemmelsene som omhandler kraftsensitiv informasjon, både internt i NVE og blant KBO-enhetene. I forprosjektet gjennomførte NVE en spørreundersøkelse som ble besvart av 127 selskaper i tillegg til ansatte i NVE. Mellom 55 og 75 prosent av respondentene i KBO-enhetene oppga at de i stor eller svært stor grad hadde rutiner for å identifisere hva som er kraftsensitiv informasjon, hvor den befinner seg, og hvem som har tilgang til den. NVEs spørreundersøkelse viste også at mindre virksomheter mangler skriftlige rutiner i større grad enn større selskaper. Enkelte av selskapene oppga manglende rutiner, manglende kompetanse og at regelverket framstår som uklart, som årsaker til dette. I NVEs spørre-undersøkelse oppga også enkelte av respondentene at det er stor usikkerhet rundt hvor mye informasjon som kan deles med andre aktører, og at det er utfordrende å sørge for at NVEs krav får nok oppmerksomhet i selskapet.

Gjennomføring av risikovurdering

NVE oppgir i intervju at flere selskaper mangler kompetanse til å utforme gode risikovurderinger, og at flere selskaper ikke klarer å skille mellom årsaken til en hendelse, og hva som er den faktiske hendelsen, i risikovurderingene. Et av formålene med risikovurderinger er å sortere mellom det som kan forebygges, for eksempel gjennom sikringstiltak, og det som må håndteres ved hjelp av beredskapsplanverk.[34] Dersom selskapene ikke klarer å skille mellom årsaken til en hendelse (for eksempel IKT-angrep) og selve hendelsen (for eksempel bortfall av et IKT-system), kan det føre til at iverksatte tiltak ikke bidrar til å forebygge hendelsen, eller til at beredskapsplanverket ikke er tilrettelagt for å håndtere en hendelse.

I vår spørreundersøkelse oppga 13 og 18 prosent av IKT-sikkerhetskoordinatorene at det i stor eller svært stor grad er utfordrende å etterleve kravet til henholdsvis risikovurderinger (§ 2-3) og risikovurderinger ved systemendringer (§ 6-9b), se figur 2. I perioden 2017–2019 avdekket NVE 32 avvik ved selskapers risikovurderinger i IKT-sikkerhetstilsyn og i tilsyn med generell beredskap. Sammen med kravet til internkontrollsystem er kravet til risikovurderinger det kravet NVE avdekket flest avvik ved i perioden.

I Prop. 1 S (2017–2018) Olje- og energidepartementet står det at det ikke finnes like mye statistikk for tilsiktede hendelser som for naturhendelser, og at det dermed er vanskelig å anslå sannsynligheten for tilsiktede hendelser. NC-Spectrum AS sier i intervju at manglende kunnskap om trusselbildet og risikoen for cyberangrep fører til at det er krevende for selskapene å gjennomføre gode risikovurderinger. Det er enklere for dem å vurdere risikoen for fysiske trusler som skyldes for eksempel dårlig vær, fordi de har bedre statistikk/data og prognoser om denne typen risiko. NC-Spectrum AS' erfaring er at det er stor variasjon i hvordan selskapene vurderer risiko og hvilke tiltak som er nødvendige for å oppnå et tilstrekkelig sikkerhets-nivå. NC-Spectrum AS mener at selskapene som utfører gode risikoanalyser, i større grad tar inn over seg risikoen for at IKT-hendelser kan skje.

4.4.4 Sikre IKT-systemer og oppdage og håndtere IKT-hendelser

I kraftberedskapsforskriften § 6-3 stilles det krav til at selskaper skal beskytte, skjerme og kontrollere tilgangen til kraftsensitiv informasjon. I § 6-9 c står det at selskapene skal sikre IKT-systemene sine slik at de motstår eller begrenser skade fra uønskede hendelser, og overvåke systemene slik at uønskede hendelser oppdages og registreres. I kraftberedskapsforskriften kapittel 7 og § 6-10 stilles det ytterligere krav til sikring av henholdsvis driftskontrollsystemer og brytefunksjonaliteten i AMS. I § 7-6 står det for eksempel at selskapene skal hindre urettmessig tilgang mellom driftskontrollsystemet og andre informasjonssystemer. Dette kan gjøres gjennom logiske skiller, hvor driftskontrollfunksjoner er på et nettverk atskilt fra annen aktivitet.

[34] NVE (2013) *Veiledning til forskrift om forebyggende sikkerhet og beredskap i energiforsyningen.*

I vår spørreundersøkelse oppga om lag 20 prosent av IKT-sikkerhetskoordinatorene at det i stor eller svært stor grad er utfordrende å etterleve kravet om beskyttelse, avskjerming og tilgangskontroll (§ 6-3), jf. figur 2. Om lag 25 prosent av IKT-sikkerhetskoordinatorene oppga at det i stor eller svært stor grad er utfordrende å etterleve kravet om å sikre selskapets digitale informasjonssystemer og oppdage uønskede hendelser (§ 6-9 c). NVE har ved hjelp av kartleggingsverktøy avdekket at det på internett lå informasjon om blant annet hvilket driftskontrollsystem selskaper bruker, og hvor driftssentraler ligger, og flere dokumenter som indikerer brudd på kravene i kraftberedskapsforskriften. NVE har også avdekket brudd på besøksrestriksjoner og publisering av bilder fra driftssentraler. NVE har i tilsyn avdekket flere avvik ved selskapers beskyttelse av driftskontrollsystemet, som vist i tabell 1. Etter forskriftsendringen i 2019 har NVE også avdekket avvik ved selskapers sikring av andre digitale informasjonssystemer.

I caseundersøkelsen kontrollerte vi enkelte grunnleggende sikkerhetstiltak, som logiske skiller, tilgangskontroller og logging, i tre utvalgte selskaper for å få innblikk i hvordan disse selskapene sikrer IKT-systemene gjennom internkontrollen. Tiltakene vil kunne bidra til å begrense omfanget av, avverge eller avdekke et IKT-angrep og gjøre det mulig å analysere angrepet i etterkant. Flere lag av sikkerhetstiltak kan hindre at IKT-systemene blir kompromittert som følge av svikt i ett enkelt tiltak. Vi vurderte ikke de tre selskapenes totale sikkerhetsnivå og heller ikke motstandsdyktigheten i caseundersøkelsen.

Caseundersøkelsen viser at det er variasjon i hvor godt de ulike sikkerhetstiltakene er iverksatt hos selskapene. Enkelte tiltak er etablert i tråd med regelverket og beste praksis, mens det er svakheter og vesentlige svakheter i ivaretakelsen av flere sikkerhetstiltak i alle tre selskapene. Selskapene har ikke avdekket svakhetene i disse tiltakene gjennom egne kontrollaktiviteter.

Loggføring og evne til å oppdage hendelser

NVE har påpekt at selskapene må logge datatrafikk og analysere loggene for å etterleve kravene til varsling og rapportering.[35] Enkelte systemer som brukes i kommunikasjonen mellom selskapenes driftskontroll-systemer og anlegg og utstyr i felt, kan imidlertid være vanskelige å overvåke.[36] NVE oppgir at eldre systemer som ikke tilbyr bruk av personlige brukerkontoer og dermed ikke er tilstrekkelig tilrettelagt for logging, må suppleres med andre tiltak, som manuell logging.

I 2015 gjennomførte NVE et skriftlig tilsyn med 31 selskaper som avdekket 40 avvik ved selskapenes etterlevelse av kravet til overvåking og logging i driftskontrollsystemer. I en rapport utarbeidet for NVE i 2017 står det at norske virksomheter innen energiforsyningen logger mest av driftshensyn, og at det er nødvendig med økt fokus på logging av sikkerhetshensyn.[37] I vår spørreundersøkelse oppga 35 prosent[38] av IKT-sikkerhetskoordinatorene at det i stor eller svært stor grad er utfordrende å etterleve kravet til overvåking og logging, se figur 2.

I 2020 skrev KraftCERT på oppdrag fra NVE en rapport om hvordan innføring og bruk av indikatorer og sensornettverk i kraftforsyningen kunne styrke IKT-sikkerheten. I den forbindelse gjennomførte KraftCERT intervjuer og en spørreundersøkelse som viste at selskapene ønsket seg mer statistikk og bedre oversikt over angrepsforsøk og IKT-sikkerhetshendelser.[39] Slik statistikk kunne hjelpe dem med å fordele ressurser og sette ledelsen i stand til å ta beslutninger basert på empiri. Flere av selskapene oppga også at sikkerhetskompetansen i ledelsen kunne vært bedre, og at dette kunne bidratt til at det også ble stilt flere krav til statistiske data. I rapporten anbefaler KraftCERT at det utvikles en database med indikatorer som selskapene skal bruke, og et rammeverk for innsamling og bearbeiding av slik informasjon.

NSM driver det nasjonale sensornettverket «Varslingssystem for digital infrastruktur» (VDI), som består av sensorer som er utplassert hos virksomheter som anses som en del av den kritiske infrastrukturen i Norge. Dette inkluderer enkelte selskaper i kraftforsyningen. Sensornettverket utløser alarmer ved observasjoner av kjente trusler i deltakervirksomhetenes nettverk. Truslene behandles og rapporteres til virksomhetene av NSMs sikkerhetsanalytikere. KraftCERT trekker fram i en rapport at også HelseCERT kan oppdage uønskede hendelser og skadevare tidlig ved hjelp av sensorer i stamnettet og hos enkelte nøkkelselskap. I KraftCERTs rapport fra 2020 anbefaler KraftCERT at det innføres et sensornettverk i kraftforsyningen, som

[35] NVE (2017) *Regulering av IKT-sikkerhet.* NVE-rapport nr. 26/2017.
[36] NVE (2017) *Metodikk for informasjonsinnhenting etter IKT-sikkerhetshendelser i driftskontrollsystem.* NVE-rapport nr. 14/2017.
[37] NVE (2017) *Logging og logganalyse i energiforsyningen*. NVE-rapport nr. 1/2017.
[38] Kravet gjelder kun selskaper med driftskontrollsystemer i klasse 2 og 3, så IKT-sikkerhetskoordinatorer som har svart «Vet ikke / ikke aktuelt» er ikke medregnet.
[39] KraftCERT (2020) *Digital kontroll: en studie om innføring og bruk av metrikker i kraftforsyningen for bedre IKT-sikkerhet.* NVE-rapport nr. 22/2020.

sammen med innrapportert statistikk fra selskapene kan bidra til å gi en løpende oversikt over sikkerhetstilstanden i sektoren.

Sikring av brytefunksjonalitet i AMS

Ifølge NVE kan uønsket tilgang til brytefunksjonaliteten i AMS-målere få like alvorlige konsekvenser som uønsket tilgang til driftskontrollsystemene. En masseutkobling via AMS-måleres brytefunksjon vil føre til at svært mange mennesker mister strømmen.[40] Før beredskapsforskriften ble endret i 2019, stilte NVE i hovedsak krav til sikkerheten i AMS-systemene gjennom 1) funksjonskrav til «sikkerhet mot misbruk av data og uønsket tilgang til styrefunksjoner» (forskrift om kraftomsetning og nettjenester) og 2) krav til sikring ved eventuell integrasjon med driftskontrollsystemer (beredskapsforskriften).[41] Etter at det ble innført mer spesifikke krav til sikringen av brytefunksjonaliteten i AMS, gjennomførte NVE i 2019 to tilsyn hvor disse kravene var tema. Ett av tilsynene avdekket avvik.

Som en del av FoU-prosjektet *Informasjonssikkerhetstilstanden i energiforsyningen* fikk NVE i 2017 gjennomført penetrasjonstester av tre selskaper.[42] I rapporten til prosjektet står det at testene viste at driftskontrollsystemene generelt var bedre beskyttet mot innsidetrusler enn AMS-løsningene, og at det er større risiko for at en trusselaktør som har fått fotfeste i det administrative nettverket, kan få tilgang til brytefunksjonaliteten i AMS-løsningen. NVE påpekte også at flere AMS-løsninger, også brytefunksjonaliteten, driftes av leverandører slik at datainnbrudd hos en AMS-leverandør potensielt kan utnyttes til å skru av strømmen til individuelle forbrukere hos mange selskaper samtidig. Det er få leverandører av AMS-målere og enkelte større samarbeidsallianser for drift av AMS-løsninger.[43] NC-Spectrum AS sier i intervju at nettselskapers samarbeid om innkjøp av AMS-systemer har bidratt til å presse ned prisen og effektivisere implementeringen av AMS, men at dette ikke har forbedret leverandørenes holdning til IKT-sikkerhet. Ifølge NC-Spectrum AS har det vært et skille mellom det selskapene fikk presentert i forkant, og det de har opplevd når de har implementert og testet systemene. 12 prosent av IKT-sikkerhetskoordinatorene i vår spørreundersøkelse oppga at det i stor eller svært stor grad er utfordrende å etterleve kravet til sikring av brytefunksjonalitet i AMS, se figur 2.

Håndtering av hendelser

Kraftberedskapsforskriften stiller krav til selskapenes beredskapsplanlegging, øvelser og varsling om hendelser, jf. kapittel 2. Videre stiller den krav til at selskapene skal drive de anleggene de har ansvaret for, og gjenopprette nødvendige funksjoner i og etter ekstraordinære situasjoner, jf. § 4-3.

I perioden 2017–2019 avdekket NVE i IKT-sikkerhetstilsyn fire avvik ved selskapers beredskapsplanlegging samt flere avvik ved etterlevelsen av krav til sikkerhetskopier, redundans og håndtering av feil, sårbarheter og sikkerhetsavbrudd. I generelle beredskapstilsyn har NVE avdekket 22 avvik ved selskapers beredskaps-planlegging, 9 avvik som gjelder kravet til øvelser, og 9 avvik ved selskapers etterlevelse av kravet til varsling og rapportering. 10 prosent av IKT-sikkerhetskoordinatorene i vår spørreundersøkelse oppga at det i stor eller svært stor grad er utfordrende å etterleve kravet til beredskapsplanlegging i forskriften. Dette er blant de tre kravene NVE oftest avdekket avvik ved i perioden 2017–2019. NVE har begrunnet mange av avvikene ved beredskapsplanleggingen med at selskapene ikke kunne vise til at beredskapsplanverket bygget på gjennomførte risikovurderinger. Avvikene som gjelder kravet til øvelser, skyldes ofte at selskapene ikke har en oppdatert, flerårig øvelsesplan som dekker relevante ekstraordinære forhold.

Før driftskontrollsystemer ble tatt i bruk for å fjernstyre anleggene i kraftforsyningen, måtte selskapene ha ansatte til stede på anleggene for å overvåke og betjene installasjonene manuelt.[44] Ved et omfattende IKT-angrep som slår ut driftskontrollsystemene, må selskapene i kraftforsyningen kunne drifte anleggene sine manuelt. I Prop. 1 S (2017–2018) skriver Olje- og energidepartementet at selv om det i kraftberedskapsforskriften stilles krav om at selskapene i kraftforsyningen skal kunne overvåke og styre sine anlegg manuelt, vil bortfall av IKT-systemer likevel gi en utfordrende situasjon i sektoren.

I en spørreundersøkelse utført av NVE i 2017 oppga over 70 prosent av virksomhetene at de enten var sterkt eller middels avhengige av selskapets IKT-leverandør for å håndtere hendelser.[45] Når det gjaldt

[40] NVE (2018) *Oppsummeringsdokument: Endringer i beredskapsforskriften - Krav til IKT-sikkerhet m.m.* NVE-rapport nr. 92/2018; NVE (2017) *Regulering av IKT-sikkerhet*. NVE-rapport nr. 26/2017.
[41] NVE og SINTEF Energi AS (2017) *Evaluering av NVEs veileder til sikkerhet i AMS.* NVE-rapport nr. 44/2017.
[42] NVE (2017) *Informasjonssikkerhetstilstanden i energiforsyningen.* NVE-rapport nr. 90/2017.
[43] NVE (2016) *Smarte målere (AMS) Status og planer for installasjon per 1. halvår 2016*. NVE-rapport nr. 79/2016.
[44] Fridheim, H., J. Hagen og S. Henriksen (2001) *En sårbar kraftforsyning - Sluttrapport etter BAS3.*
[45] NVE (2017) *Informasjonssikkerhetstilstanden i energiforsyningen.* NVE-rapport 74/2017.

håndtering av hendelser i driftskontrollsystemet, oppga 70 prosent av virksomhetene det samme, og over 75 prosent oppga at de var avhengige av leverandøren for å gjenopprette driftskontrollsystemet.

Samme spørreundersøkelse inneholdt også spørsmål om hvilke IKT-sikkerhetshendelser og IKT-angrep virksomhetene hadde opplevd de siste tolv månedene. 62 virksomheter (om lag 75 prosent av virksomhetene) oppga at de hadde opplevd uønskede IKT-hendelser de siste tolv månedene. Av disse oppga 42 prosent at de ikke rapporterte den mest alvorlige hendelsen til noen. 6 prosent av respondentene oppga at de hadde rapportert hendelsene til NVE, 24 prosent hadde rapportert dem til administratoren av det aktuelle tekniske systemet, 18 prosent hadde rapportert dem til KraftCERT eller tilsvarende, og 10 prosent hadde rapportert dem til andre aktører som politiet eller leverandører av antivirusprogram.[46] 6 prosent svarte «Vet ikke» på spørsmålet om hvem de hadde rapportert den mest alvorlig hendelsen til. I NVE-rapporten som omtaler undersøkelsen, står det at den manglende rapporteringen av hendelser kan skyldes at rapporteringsplikten bare gjelder KBO-enheter (undersøkelsen ble sendt til 350 virksomheter i kraftforsyningen, men bare om lag halvparten av disse er KBO-enheter), og at det bare er ekstraordinære hendelser som skal rapporteres til NVE. Da NVEs spørreundersøkelse ble gjennomført, var KBO-enhetene ikke pliktig til å varsle KraftCERT om uønskede IKT-hendelser (dette kravet ble innført i kraftberedskapsforskriften i 2019).

KraftCERT skriver i en rapport fra 2020 at mer informasjon om IKT-sikkerhetshendelser vil gjøre både selskaper og samfunnet bedre rustet til å gjennomføre tiltak for å redusere risikoen for alvorlige hendelser.[47] Spørreundersøkelsen viser at de fleste IKT-sikkerhetskoordinatorene mener det i liten eller svært liten grad er utfordrende å etterleve kravene til varsling og rapportering, se figur 2. Likevel er det underrapportering av IKT-hendelser i kraftforsyningen, noe som kan ha ulike årsaker, og som beskrives nærmere i punkt 8.5.

4.4.5 Kontrollere IKT-sikkerheten

Selskapene har ansvaret for at bestemmelsene om informasjonssikkerhet og taushetsplikten for kraftsensitiv informasjon ivaretas i anskaffelser, jf. kraftberedskapsforskriften § 6-5. Dette har vært et krav siden 2013. Fra 2019 stilles det krav til at selskapene jevnlig gjennomfører sikkerhetsrevisjon av sine digitale informasjonssystemer (§ 6-9 f), inkludert av systemer som er driftet av leverandører, og at øvelser og ekstraordinære situasjoner evalueres, jf. § 2-9.

I perioden 2017–2019 avdekket NVE i IKT-sikkerhetstilsyn og tilsyn med generell beredskap 25 avvik hos selskaper som følge av brudd på kravene til sikkerhetsrevisjon og evaluering av øvelser og ekstraordinære situasjoner. Avvikene har i de fleste tilfeller blitt begrunnet med at selskapene enten oppgir at de ikke har gjennomført eller ikke kan dokumentere at de har gjennomført jevnlige sikkerhetsrevisjoner.

Caseundersøkelsen viser at det er vesentlige mangler i to av selskapenes gjennomføring av evalueringer og sikkerhetsrevisjoner. Ingen av de tre selskapene evaluerer sikkerhetstiltak jevnlig og systematisk. Det er også svakheter ved selskapenes oppfølging av at leverandørene etterlever avtalte sikkerhetskrav. Caseundersøkelsen har avdekket svakheter på en rekke områder som kunne vært avdekket gjennom evaluering av sikkerhetstiltak, sikkerhetsrevisjoner eller oppfølging av leverandørene.

Oppfølging av leverandører

Om lag halvparten av IKT-sikkerhetskoordinatorene i vår spørreundersøkelse oppga at en årsak til at det kunne være vanskelig å etterleve kravene i kraftberedskapsforskriften, skyldtes at det var vanskelig å følge opp IKT-sikkerheten hos leverandørene og påse av den tilfredsstiller kravene i forskriften, se figur 3. I intervju med flere selskaper kommer det fram at det kan være utfordrende å føre tilsyn med leverandører, og at det krever mye ressurser og kompetanse for å verifisere at leverandørenes sikkerhetstiltak er implementert. I vår spørreundersøkelse svarte om lag 30 prosent av IKT-sikkerhetskoordinatorene at det i stor eller svært stor grad er utfordrende å etterleve kravet til sikkerhetsrevisjon (kraftberedskapsforskriften § 6-9 f), se figur 2.

I en undersøkelse utarbeidet for NVE om energiselskapers anskaffelser i 2018 oppga kun ett av de seks intervjuede selskapene at de hadde gjennomført tilsyn hos leverandøren etter kontraktsinngåelsen.[48] Også i en undersøkelse fra 2020 utført for NVE viser intervjuer med enkelte selskaper i energiforsyningen at de i liten grad gjennomfører tilsyn med leverandørenes informasjonssikkerhet.[49] Nettalliansen AS oppgir i intervju

[46] Respondentene kunne i spørreundersøkelsen oppgi flere svaralternativer på hvem hendelsen ble rapportert til. Andelen svar summeres derfor til over 100 prosent.
[47] KraftCERT (2020) *Digital kontroll: en studie om innføring og bruk av metrikker i kraftforsyningen for bedre IKT-sikkerhet.* NVE-rapport nr. 22/2020.
[48] NVE (2018) *IKT-sikkerhet ved anskaffelser og tjenesteutsetting i bransjen.* NVE-rapport nr. 90/2018.
[49] NVE og Proactima (2020) *Kartlegging av bruk av tingenes internett (IOT/IIoT) i norsk kraftforsyning.* NVE-rapport nr. 2/2020.

at det er vanskelig for små selskaper å gjennomføre sikkerhetsrevisjoner av leverandører. Nettalliansen AS leverer IKT-løsninger til sine medlemsselskaper og oppgir at det gjennomføres sikkerhetsrevisjoner av disse. Medlemsselskapene har imidlertid en rekke IKT-løsninger utover fellesløsningene, og det er ifølge Nettalliansen AS vanskelig og dyrt for selskapene å gjennomføre sikkerhetsrevisjoner av disse systemene, slik forskriften stiller krav til. Både Nettalliansen AS og NC-Spectrum AS opplever at leverandørene er mer opptatt av funksjonaliteten enn av IKT-sikkerheten i systemene de tilbyr. NC-Spectrum AS opplever at det gjennomgående er uoverensstemmelser mellom hvordan sikkerheten i systemene blir presentert av leverandører før en kontraktsinngåelse, og det selskapene senere ser ved sikkerhetsrevisjoner. I en rapport utarbeidet for NVE forteller en leverandør at energiselskapene ofte sender kraftsensitiv og annen sensitiv informasjon på ukryptert e-post, mens to energiselskaper hadde opplevd at leverandører hadde gitt seg selv tilgang til systemer i strid med selskapenes sikkerhetsrutiner.[50] I det ene tilfellet hadde leverandøren gitt sine ansatte dobbelt så mange administratorbrukere som avtalt, og i det andre hadde leverandøren lagt inn en bakdør til systemet uten å be om tillatelse. Begge episodene ble av leverandørene begrunnet i et ønske om å yte god service til energiselskapet.

NVE oppfatter at oppfølgingen av multinasjonale selskaper som blir en del av den kritiske infrastrukturen, er en utfordring som gjelder i hele samfunnet. Før 2013 inngikk NVE sikkerhetsavtaler med selskaper som leverte driftskontrollsystemer, konsulenttjenester, entreprenørtjenester og annet til kraftforsyningen, og etaten gjennomførte enkelte tilsyn med etterlevelsen av disse avtalene. Det ble ikke ført tilsyn med leverandørene av driftskontrollsystemer, men NVE arrangerte møter med de største leverandørene hvor de blant annet diskuterte hvordan leverandørene håndterte sikkerheten til selskapene, og hvordan de kunne gjennomføre service av driftskontrollsystemene på en sikker måte. NVE opplevde disse leverandørene som profesjonelle i denne sammenhengen. I løpet av 2013 ble ordningen med sikkerhetsavtaler mellom NVE og leverandørene avviklet, men NVE beholdt ansvaret for å føre tilsyn med leverandørenes beskyttelse av sensitiv informasjon. NVE oppgir i intervju at de ikke har ført tilsyn med leverandører i årene etter 2013, og at etaten har prioritert å føre tilsyn med KBO-enhetene. Mellom 2013 og 2019 var KBO-enhetene pålagt å opplyse leverandørene (og underleverandører) om at NVE kunne føre tilsyn med om de etterlevde kravene til informasjonssikkerhet. I utredningen som lå til grunn for endringene i kraftberedskapsforskriften, ble det trukket fram at dette kravet var problematisk ved bruk av utenlandske leverandører siden norsk jus ikke gjelder utenfor Norges grenser. I den nye kraftberedskapsforskriften er denne opplysningsplikten fjernet, og NVE, som ikke lenger har denne tilsynsmyndigheten overfor leverandørene, oppgir at selskapene nå har fått et større ansvar og rett til å føre tilsyn med leverandørene sine. NVE påpeker at de fortsatt har hjemmel til å gjennomføre kontroll med leverandører som holder til i Norge, ut fra energiloven § 9-3 (Informasjons-sikkerhet) andre ledd. NVE opplyser at direktoratet ikke har ført tilsyn med selskapenes leverandører etter § 9-3, og at de heller ikke har konkrete planer om dette framover.

4.4.6 Forbedre styringen og sikringen av IKT-systemer

Ifølge kraftberedskapsforskriften § 2-10 skal selskapene ha et internkontrollsystem som dokumenterer at de har etablert en systematikk for å sikre etterlevelse av kravene i kraftberedskapsforskriften. I veilederen til kraftberedskapsforskriften skriver NVE at avvik og feil må håndteres i henhold til selskapets internkontroll-system. NVE anbefaler også at revisjonsrapporter er tema på selskapets ledermøte eller i andre relevante fora.

I NVEs tilsyn med IKT-sikkerhet og tilsyn med generell beredskap i perioden 2017–2019 avdekket de flest avvik ved kravet til internkontrollsystem. En saksgjennomgang av IKT-sikkerhetstilsyn i perioden 2017–2019 viser at NVE har lukket 14 av 15 tilsynssaker på bakgrunn av tilsynsobjektenes tilbakemeldinger. Den gjenværende saken gjelder et avvik NVE avdekket i et tilsyn med et selskap i 2017. Avviket gjaldt selskapets internkontrollsystem. Siste dokumenterte oppfølging av saken er fra september 2018. NVE oppgir i desember 2020 at de jobber med å avslutte saken.

NC-Spectrum AS oppfatter at mange leverandører mangler vilje til å rette opp sårbarheter og øke sikkerhetsnivået når selskapene påpeker dette. Ifølge NC-Spectrum AS opplever selskapene at leverandører i liten grad lar seg påvirke til å øke sikkerheten. Leverandørene har også ofte manglende forståelse for at kraftforsyningen er kritisk infrastruktur som har strenge sikringsbehov.

Caseundersøkelsen viser at det er svakheter i alle de tre selskapenes gjennomføring av evalueringer og sikkerhetsrevisjoner, noe som gjør at selskapene har få avvik å følge opp. Caseundersøkelsen viser at det

[50] NVE (2018) *IKT-sikkerhet ved anskaffelser og tjenesteutsetting i bransjen.* NVE-rapport 90/2018.

for to av selskapene er svakheter i dokumentasjonen og oppfølgingen av avvik som er avdekket. Videre er det svakheter i selskapenes dokumentasjon av statusen for sikkerhetsarbeidet ettersom de i liten grad har gjennomført evalueringer og sikkerhetsrevisjoner og dermed mangler grunnlag for å vurdere statusen.

4.5 Konsentrasjonsrisiko i leverandørmarkedet for IKT-systemer

Kraftforsyningen består av mange kraftprodusenter og nettselskaper som forsyner brukere med strøm. Et enkelt nettselskaps bortfall av evnen til å levere strøm i distribusjons- eller regionalnettet vil derfor ikke føre til strømavbrudd i hele landet. Imidlertid kan et vellykket angrep mot en tjenesteleverandør eller mot et system som er utbredt i kraftforsyningen, ramme flere selskaper og større områder. I NVE-rapporten *Regulering av IKT-sikkerhet* fra 2017 står det at dersom det er svært få leverandører for viktige produkter eller tjenester, vil det skapes et avhengighetsforhold som kan være en risiko, og at dette blant annet kan være knapphet på ressurser, personavhengighet eller leverandørspesifikke feil som får konsekvenser for store deler av bransjen. En feil eller et angrep som rammer flere aktører, kan også føre til at det ikke finnes nok personell eller reservedeler til å rette opp etter hendelsen. NVE har ikke hjemmel til å overprøve hvilke leverandører selskapene bruker, og påpeker at dette også ville vært vanskelig å praktisere. I NVE-rapporten *Regulering av IKT-sikkerhet* fra 2017 ble det videre påpekt at andre aktører enn dagens KBO-enheter kunne ha betydning for forsyningssikkerheten, for eksempel leverandører som styrer deler av infrastrukturen i distribusjonsnettet, eller viktige aktører i det økonomiske segmentet. Arbeidsgruppen anbefalte å gjøre energiloven gjeldende for flere enn KBO-enheter, for eksempel viktige digitale tjenestetilbydere.

NVE kan ved enkeltvedtak bestemme at også andre virksomheter som eier eller driver anlegg, systemer eller annet som har vesentlig betydning for driften eller gjenopprettingen av eller sikkerheten i produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme, skal være KBO-enheter.[51] I 2014 begrunnet NVE innlemmelsen av KraftCERT i KBO blant annet med at KraftCERT – gjennom sammenstilling av informasjon og egne analyser – ville produsere sensitiv informasjon om energi-forsyningen som er mer omfattende enn det KraftCERT vil motta fra det enkelte selskap.[52] I 2020 vedtok NVE at Nordpool AS og European Market Coupling Operator AS skulle inngå som enheter i KBO på grunn av sine roller i markedet for krafthandel.[53] Per november 2020 var ingen av selskapenes leverandører av viktige IKT-tjenester, for eksempel leverandører av driftskontrollsystemer eller AMS-løsninger, blitt innlemmet i KBO. NVE oppgir at det ikke har vært aktuelt å utnevne noen leverandører til KBO-enheter.

Det er få leverandører av både driftskontrollsystemer og AMS-systemer, men NVE mener at disse leverandørene er solide, og at store leverandører av administrative systemer sikrer løsningene sine godt. Verken KraftCERT eller NVE har skriftlige oversikter over hvilke leverandører og IKT-systemer KBO-enhetene bruker. NVE mener at de ikke har noen hjemler som tillegger dem en slik oppgave. I et brev til NVE i 2018 anbefalte KraftCERT at KraftCERT laget en database over leverandører av sikkerhetsløsninger, med en oversikt over type leverandør, geografisk plassering og leverandørens kapasitet/størrelse. KraftCERT skrev at de på den måten også kunne sørge for at alle sikkerhetsleverandører blir sitt ansvar bevisst og forstår at det forventes noe av dem kvalitetsmessig. KraftCERT skrev videre at dette vil ikke være en ordentlig sertifisering, men kunne brukes til å kontrollere om alle leverandører vet hvordan de skal respondere på et varsel eller en hendelse. KraftCERT oppgir imidlertid i intervju i 2020 at de har kommet fram til at de ikke ønsker å samle denne informasjonen på ett sted, siden det hadde vært sårbart dersom andre fikk tilgang til informasjonen. KraftCERT oppgir at de skaffer seg informasjon om hvilke systemer som brukes i bransjen, gjennom dialog med medlemsselskapene.

Finanstilsynet og NSM har i motsetning til NVE henholdsvis meldeplikt og et verifikasjonsregime ved tjenesteutsetting. Finansforetakene har meldeplikt til Finanstilsynet ved utkontraktering av tjenester, men Finanstilsynet sier det vil være svært vanskelig å overprøve beslutninger om utkontraktering dersom det ligger en god risikovurdering til grunn for beslutningen. Etter *lov om nasjonal sikkerhet* (sikkerhetsloven) må leverandører som skal få tilgang til skjermingsverdig informasjon, godkjennes på forhånd av NSM. NSM undersøker blant annet leverandørenes eierforhold og styring, fører tilsyn med hvordan leverandørene etterlever kravene i sikkerhetsloven, og utarbeider en leverandøroversikt over årlige oppdrag. Ifølge NSM har de et ganske godt bilde av leverandørene som er underlagt sikkerhetsloven, og hvilke virksomheter leverandørene leverer varer og tjenester til, takket være verifikasjonsregimet.

[51] Kraftberedskapsforskriften § 3-1 andre ledd.
[52] NVE (2014) *Vedtak om medlemskap i Kraftforsyningens Beredskapsorganisasjon (KBO) for KraftCERT AS*, 22. desember 2014..
[53] NVE (2020) *Vedtak om at Nord Pool AS og European Market Coupling Operator AS skal inngå i Kraftforsyningens beredskapsorganisasjon (KBO)*, 19. mars.2020.

NVE gir uttrykk for at leverandørsituasjonen utgjør en konsentrasjonsrisiko som NVE per i dag ikke har virkemidler for å gjøre noe med. I kraftforsyningen er det ikke rapporteringskrav knyttet til selskapenes leverandørbruk eller en lignende meldeplikt ved utkontraktering, slik det er i finansbransjen. NVE oppgir at det ved revidering av beredskapsforskriften ble vurdert ulike løsninger for de nye kravene, og at Finanstilsynets krav til meldeplikt ble vurdert i denne sammenhengen. Ved revisjonen av kraftberedskapsforskriften tok NVE inn deler av ordlyden i Finanstilsynets regulering av selskapers utkontraktering av tjenester.

5 NVEs styring av arbeidet med IKT-sikkerhet i kraftforsyningen

I dette kapitlet beskriver vi hvordan NVE styrer og følger opp arbeidet med IKT-sikkerhet i kraftforsyningen ved å fastsette mål og strategier og følge opp om målene nås.

5.1 Relevante føringer

NVE skal

- fremme en sikker kraftforsyning og påse at beredskapen i energiforsyningen er god og i tråd med gjeldende krav
- prioritere arbeidet med IKT-sikkerhet i kraftsektoren
- sikre tilstrekkelig styringsinformasjon og beslutningsgrunnlag for å følge opp aktivitetene og resultatene
- etablere systemer og rutiner for internkontroll

5.2 Oppsummering

- NVE har utarbeidet strategier, risikovurderinger og virksomhetsplaner som framhever at arbeidet med IKT-sikkerhet i kraftforsyningen er et prioritert område for NVE.
- NVE har ikke operasjonalisert målene og styringsparameterne fra departementet i vurderingskriterier som kan brukes til å styre og følge opp arbeidet med IKT-sikkerhet i kraftforsyningen.
- Beredskapsseksjonens planer viser ikke det totale ressursbehovet for arbeidet med IKT-sikkerhet i kraftforsyningen.
- NVE har ikke et ressursstyringsverktøy for å planlegge og følge opp arbeidet med IKT-sikkerhet i kraftforsyningen.
- Flere av NVEs oppgaver innenfor arbeidet med IKT-sikkerhet i kraftforsyningen har blitt utsatt på grunn av kapasitetsutfordringer.
- Det er lite intern og ekstern rapportering om mål og resultater av NVEs arbeid med IKT-sikkerhet i kraftforsyningen.

5.3 Strategisk planlegging

NVEs arbeid med IKT-sikkerhet i kraftforsyningen er organisert i beredskapsseksjonen (TBB) under tilsyns- og beredskapsavdelingen (TB). Beredskapsseksjonen har ansvar for å følge opp kraftforsynings-beredskapen og driften, vedlikeholdet og moderniseringen i energiforsyningen og fører tilsyn med selskapenes etterlevelse av kapittel 9 om beredskap i energiloven, kraftberedskapsforskriften og enkelte paragrafer i energilovforskriften. I 2019 hadde NVE 603 ansatte.[54] Av disse var 67 ansatt i tilsyns- og beredskapsavdelingen og 18 i beredskapsseksjonen. Tre av de ansatte i beredskapsseksjonen har IKT-sikkerhetskompetanse som spesialfelt.

5.3.1 Tildelingsbrev

NVEs strategi- og planleggingsarbeid tar utgangspunkt i tildelingsbrevene fra Olje- og energidepartementet. I tildelingsbrevene for 2017–2020 er et av de fire hovedmålene som departementet har satt for NVE, å fremme en sikker kraftforsyning. For å nå dette hovedmålet skal NVE som et delmål påse at beredskapen i kraftforsyningen er god og i tråd med gjeldende krav. Styringsparameterne som er satt for dette delmålet, er:

- Beskriv de viktigste tiltakene og hvordan disse bidrar til å fremme hovedmålet.
- Gi en vurdering av statusen og utviklingen i sikkerhets- og beredskapstilstanden i kraftforsyningen.
- Beskriv samarbeidet med energibransjen, myndighetsorganer og andre nordiske land innenfor kraftforsyningsberedskap, og gi en vurdering av hvilken betydning samarbeidet har for å fremme en sikker kraftforsyning.

Olje- og energidepartementet har ikke satt noen spesifikke mål eller styringsparametere for NVEs arbeid med IKT-sikkerhet i kraftforsyningen. Både NVE og departementet oppfatter at dette arbeidet ligger under

[54] NVEs årsrapport for 2019.

hovedmålet om å fremme en sikker kraftforsyning. I tildelingsbrevene har imidlertid Olje- og energidepartementet gitt noen spesifikke føringer som gjelder IKT-sikkerhet i kraftforsyningen. NVE skal blant annet styrke regelverket for IKT-sikkerhet og være sektorvist responsmiljø for IKT-sikkerhetshendelser i kraftsektoren.

5.3.2 Strategier

NVEs virksomhetsstrategi for 2017–2021 tar utgangspunkt i målene fra Olje- og energidepartementet. Det framheves i strategien at NVE skal ha stort fokus på IKT-sikkerhet i kraftforsyningen.

Tilsyns- og beredskapsavdelingen (TB) har utarbeidet egne strategier for avdelingen for perioden 2018–2020 og 2020–2022. Strategiene skal gi mål og retning for hvordan oppgavene i avdelingen skal løses, og for hvordan ressurser i avdelingen skal prioriteres i et treårsperspektiv. Avdelingens strategi for perioden 2018–2020 inneholder sju prioriterte strategipunkter (ansvarsområder), hvor ett av punktene er «Vi skal prioritere IKT-sikkerhet og ha særlig fokus på styrings- og driftskontrollsystemer». Arbeidet med IKT-sikkerhet i kraftforsyningen inngår også som en del av flere av de andre punktene. Strategien for 2020–2022 inneholder de samme punktene i tillegg til et punkt om å synliggjøre tilsynsarbeidet internt og eksternt. Begge strategiene framhever at IKT blir stadig viktigere i driften av vassdrags- og energianlegg på grunn av den raske teknologiutviklingen, digitalisering og effektivisering. Strategiene inneholder en rekke tiltak for å nå strategipunktene, og de fleste tiltakene er tilnærmet like for de to strategiperiodene. Tiltakene omfatter de fleste oppgavene som inngår i NVEs arbeid med IKT-sikkerhet i kraftforsyningen, som arbeid med regelverk, veiledning, tilsyn og kompetanseoppbygging.

5.3.3 Overordnede risiko- og vesentlighetsvurderinger

NVE utarbeider årlige overordnede risiko- og vesentlighetsvurderinger som inngår i styringsdialogen med Olje- og energidepartementet. Ifølge NVE har risikovurderingene fungert som et styringsredskap ved at de påpekte risikoene prioriteres i tilsyns- og beredskapsavdelingen og beredskapsseksjonen. I alle risikovurderingene for årene 2017–2020 trekker NVE fram utfordringer som følge av digitaliseringen og at både NVE og bransjen er avhengige av å styrke kompetansen på området. Behovet for å styrke kompetansen på IKT-sikkerhet i kraftforsyningen er blant annet begrunnet med utfordringer knyttet til utvikling av nye driftssentralkonsepter, utvidet bruk av IKT, smarte strømmålere (AMS) og trusselbildet på området.

I risikovurderingene for 2017 og 2018 – under risikoområdet «Forsyningssikkerhet» under hovedmålet «Fremme en sikker kraftforsyning» – trakk NVE fram risikoen for at regelverket ikke var utviklet i takt med nye utfordringer, og for at beredskapen ved hendelser i energiforsyningen ikke var tilstrekkelig operativ. Et av tiltakene som skulle redusere risikoen, gikk ut på å revidere beredskapsforskriften, med økte krav til IKT-sikkerhet. I risikovurderingen for 2017 sto det at NVE ville prioritere IKT-sikkerhet i energiforsyningen høyere. De ville rette større oppmerksomhet på IKT-sikkerhet i energiforsyningen gjennom tilsyn og andre regulatoriske tiltak og øke kompetansen på feltet gjennom FoU. Ifølge risikovurderingene for 2017 og 2018 var det også en risiko for at NVE ikke hadde tilstrekkelig grunnlag for å vurdere status og risiko i beredskapen og forsyningssikkerheten. Et av de nye tiltakene gikk ut på å øke kvaliteten i grunnlagsdataene på områdene forebyggende sikkerhet og beredskap.

I 2019 og 2020 er risikoen for at kraftforsyningen rammes av cyberangrep, trukket fram som en av tre risikoer under risikoområdet «Forsyningssikkerhet». NVE framhever at bransjen må ha god risikoforståelse og sikre seg mot og være forberedt på å takle cyberangrep mot vital infrastruktur. Dette krever et aktivt tilsyn, veiledning, godt sikkerhetsarbeid og god håndteringsevne blant virksomhetene og i NVE og KraftCERT. Begge årene foreslås følgende nye tiltak for å redusere risikoen for cyberangrep mot kraftforsyningen: NVE skal avklare sin egen og KraftCERTs rolle og ansvar når det gjelder forebygging og håndtering av IKT-hendelser og styrke bransjens forståelse av utfordringer gjennom samarbeidsprosjekter m.m. I tillegg skal NVE bidra til å styrke kompetansen internt og eksternt gjennom kompetansefremmende tiltak og FoU som styrker forvaltningen, herunder doktorgradsstudier om sikkerhet i driftskontrollsystemer.

5.4 Planer og ressursstyring

I en evaluering av NVE som ble gjennomført i 2016 på oppdrag fra Olje- og energidepartementet, gikk det fram at det var behov for å styrke den overordnede og helhetlige styringen i NVE ved etablering og forbedring av virksomhetsplaner. [55] Evalueringen anbefalte NVE å ta i bruk en enhetlig mal for

[55] Menon Economics (2016) *Evaluering av NVE*. Menon-publikasjon nr. 23/2016

virksomhetsplanene. Virksomhetsplanene burde være koblet til mål i tildelingsbrevet og operasjonalisert i mål og delmål. Videre burde delmålene operasjonaliseres i konkrete tiltak, med frister og fordeling av ansvar for å følge opp tiltakene. I tillegg ble det anbefalt å allokere planlagt ressursbruk per person til alle aktiviteter og innføre et system for timeregistrering for prosjekter og aktiviteter. Dette skulle bidra til å forbedre styringen og vurderingen av ressursbehov i framtidige virksomhetsplaner.

5.4.1 Planer og ressursstyringsverktøy

NVE utarbeider årlige virksomhetsplaner for hele virksomheten som angir prioriterte oppgaver for de ulike avdelingene for planåret. De prioriterte oppgavene gjenspeiler NVEs risikovurderinger og strategier. I 2017 og 2018 var revisjon av beredskapsforskriften en av de prioriterte oppgavene i virksomheten, mens avklaring av sektorvist responsmiljø var en av de prioriterte oppgavene i 2018 og 2019. I NVEs virksomhetsplan for 2017 er det en kolonne kalt «forventet effekt (bidrag til samfunnet)» for hver oppgave. Den forventede effekten av oppgavene innenfor arbeidet med IKT-sikkerhet i kraftforsyningen var i hovedsak «sikker energiforsyning». I 2018 og 2019 var denne kolonnen tatt ut av virksomhetsplanen.

Tilsyns- og beredskapsavdelingen utarbeider også årlige virksomhetsplaner for avdelingen. De er ført inn i regneark og beskriver avdelingens oppgaver og leveranser, fordelt på de ulike seksjonene. I regnearkene står det om oppgavene er en del av NVEs virksomhetsplan, og hvilken prioritet oppgavene har (1., 2. og 3. prioritet). Når det gjelder beredskapsseksjonen, inneholder avdelingens planer de prioriterte oppgavene fra NVEs virksomhetsplan i tillegg til seksjonens mer faste oppgaver, som tilsyn og veiledning innenfor kraftforsyningsberedskap og seminarer og foredrag. Planene inneholder også flere prosjekter som har relevans for arbeidet med IKT-sikkerhet, som «Prosjekt om kraftsensitiv informasjon», «Utvikling av tilsyn i TB», «Informasjonssikkerhetstilstanden» og «Digitalt styringssystem for tilsyn». I regnearkene er det en kolonne kalt «Mål, bakgrunn og forventet effekt og resultat av oppgave (bidrag til samfunnet)». De forventede målene for eller effektene av oppgavene innenfor IKT-sikkerhet i kraftforsyningen er på et overordnet nivå, som «sikker energiforsyning» og «økt IKT-kompetanse i sektoren», og er ikke operasjonalisert i målbare indikatorer.

Beredskapsseksjonen utarbeider også årlige virksomhetsplaner. NVE oppgir at det ikke er lagt føringer for hvordan seksjonenes virksomhetsplaner skal utformes, og at beredskapsseksjonen har jobbet og fortsatt jobber med å finne en hensiktsmessig form på disse planene. NVE oppgir at seksjonens virksomhetsplaner ikke godkjennes på ledernivå. Beredskapsseksjonens virksomhetsplan for 2017 og 2018 er et dokument som kobler overordnede oppgaver, som tilsyn, FoU-prosjekter og regelverksutvikling, til poster på NVEs budsjett. For 2019 og 2020 har seksjonen også utarbeidet et regneark hvor hovedoppgavene er fordelt på de ansatte i seksjonen med et anslag for antall planlagte ukeverk til postene på budsjettet og enkelte andre oppgaver. NVE oppgir at regnearket brukes for å få oversikt over om noen av de ansatte har blitt satt opp på for mange oppgaver. Det brukes ikke for å styre de ansattes tidsbruk innenfor hovedoppgavene de er satt opp på. Regnearket for 2019 og 2020 viser ikke ressursbehovet for flere av de prioriterte oppgavene fra NVEs overordnede virksomhetsplan innenfor arbeidet med IKT-sikkerhet i kraftforsyningen, som arbeidet med å avklare rollen som sektorvist responsmiljø og utarbeide ROS-analyser til departementet. De ansatte som arbeider med IKT-sikkerhet i kraftforsyningen, er heller ikke satt opp med ressurser til uforutsette oppgaver som dukker opp i løpet av året. Beredskapsseksjonen oppgir at det i løpet av året kommer mange forespørsler og nye oppgaver som gjør arbeidet i seksjonen uforutsigbart og vanskelig å planlegge. Dette gjelder særlig forespørsler om veiledning fra selskapene og henvendelser fra departementet. Andre slike oppgaver er høringer om andre sektorers reguleringer, EU-regulering, innsynskrav, bidrag til og samarbeid med andre sektormyndigheter og NSM eller Nasjonalt cybersikkerhetssenter. NVE oppgir at det er vanskelig å forutse omfanget av slike aktiviteter. Hvilke aktiviteter innenfor arbeidet med IKT-sikkerhet som kan planlegges, påvirkes ifølge NVE også av hvilke midler de i løpet av året blir tildelt gjennom interne budsjettprosesser i NVE (ordinære driftsmidler), FoU-midler og midler til prioriterte tiltak. Når seksjonens virksomhetsplan utformes, er det ikke klart hvilke interne midler de vil få i løpet av året. Dermed er det heller ikke klart om enkelte oppgaver kan gjennomføres eller ikke, noe som gjør at seksjonens planer i liten grad omtaler forventninger og mål for slike oppgaver. Det er ikke angitt mål eller resultatindikatorer for arbeidet med IKT-sikkerhet i beredskapsseksjonens virksomhetsplaner.

Ifølge NVE gir oppgavefordelingen i beredskapsseksjonen seg selv ut fra de ansattes arbeidsområde og fagbakgrunn. NVE benytter ikke et ressursstyringsverktøy eller et timeregistreringsverktøy i planleggingen og oppfølgingen av arbeidet. Selv om det i seksjonens virksomhetsplan estimeres hvor mange ukesverk hver ansatt vil bruke på ulike oppgaver, fører ikke de ansatte timer på de ulike oppgavene de arbeider med. NVE påpeker at mye av arbeidet i beredskapsseksjonen består i å veilede og besvare henvendelser fra

selskapene, departementet og andre, og at denne typen arbeid kan være vanskelig å kvantifisere i et ressursstyrings- eller rapporteringsverktøy. NVE har dermed ikke erfaringstall fra slike oppgaver som kunne vært brukt i planleggingen. NVE oppgir at bestillinger fra departementet og håndtering av eventuelle hendelser har førsteprioritet, noe som også kan gjøre det utfordrende å utføre arbeidet som er planlagt for året, siden seksjonens virksomhetsplan ikke i tilstrekkelig grad tar hensyn til slike uforutsette henvendelser.

NVE har årlige planer for tilsynsvirksomheten på virksomhetsnivå og på seksjonsnivå med konkret oppgavefordeling og tidsfrister, se punkt 7.3.2. Beredskapsseksjonen oppgir at også FOU-prosjekter, interne prosjekter, foredrag for bransjen og bestillinger fra departementet har faglige mål og konkrete tidsfrister.

5.4.2 Kunnskapsgrunnlag for å vurdere arbeidet med IKT-sikkerhet i kraftforsyningen

NVE har ikke operasjonalisert målene og styringsparameterne fra departementet i vurderingskriterier som kan brukes til å styre og følge opp arbeidet med IKT-sikkerhet i kraftforsyningen, i virksomhetsplanene. Arbeidet med IKT-sikkerhet er i NVEs strategier og virksomhetsplaner beskrevet som tiltak for å nå målet om å fremme en sikker kraftforsyning. NVE har ikke beskrevet hvilke vurderingskriterier som skal brukes for å rapportere om hvordan tiltakene innenfor arbeidet med IKT-sikkerhet i kraftforsyningen bidrar til å fremme en sikker kraftforsyning, og de har heller ikke identifisert hvilken informasjon som er nødvendig for å vurdere dette. NVE påpeker i intervju at det er krevende å følge med på utviklingen av IKT-sikkerheten i kraftforsyningen uten gode sikkerhetsindikatorer og statistikk, og dermed er det også utfordrende å måle sammenhengen mellom NVEs arbeid med å styrke IKT-sikkerheten i kraftforsyningen og resultater i form av den faktiske IKT-sikkerhetstilstanden. NVE framhever at sikkerhetstilstanden også påvirkes av mange forhold som NVE i liten grad kan påvirke. Ifølge NVE er det gjennomgående vanskelig å dokumentere at selskapenes forebyggende sikkerhetsarbeid har hatt effekt. Det NVE kan dokumentere, er avbruddsstatistikken, statistikk over gjennomførte tilsyn og rapporterte hendelser. Ifølge NVE betyr god sikkerhet fravær av hendelser, mens fravær av observerte hendelser ikke nødvendigvis betyr god sikkerhet, siden det også kan skyldes at hendelser ikke blir oppdaget. NVE påpeker at det også er utfordrende å sammenligne NVEs arbeid med arbeidet til virksomheter med tilsvarende oppdrag i andre land på grunn av ulik organisering og regelverk.

NVE opplyser i intervju at det i tilskuddet til KraftCERT ligger en forventning om at KraftCERT skal bistå med å gi en oversikt over sikkerhetstilstanden på IKT-området. NVE forventer at endringen i kraftberedskapsforskriften som sier at alle uønskede IKT-hendelser skal varsles til KraftCERT, på sikt vil bidra til at KraftCERT mottar mer informasjon om hendelser også i administrative IKT-systemer, som de vil dele med NVE på et overordnet nivå.

KraftCERT har fått i oppdrag av NVE å lage indikatorer for IKT-sikkerheten i bransjen og et rammeverk for overvåkingen av trussel- og sårbarhetsbildet i bransjen. Dette arbeidet skal bidra til å gi både NVE og departementet en bedre oversikt over IKT-sikkerhetstilstanden. KraftCERT skriver i rapporten fra dette arbeidet at KraftCERT og NVE erfarer at det ikke er nok relevant informasjon tilgjengelig fra kraftbransjen for å utarbeide tilfredsstillende statistikk og trusselbilder.[56] Ifølge KraftCERT er innrapporteringen av tilstandsinformasjon mangelfull, noe som gjør de enkelte selskapene og kraftsektoren som helhet mer sårbare, og innsamlingen og registreringen av denne typen informasjon er heller ikke standardisert. I tillegg skriver KraftCERT at det ikke er noen helhetlig overvåking av og oversikt over det reelle angrepstrykket mot kraftforsyningen. KraftCERT anbefaler derfor at KBO-enhetene tar i bruk indikatorer, og at det utarbeides et rammeverk for innsamling og bearbeiding av resultatene fra indikatorene. I rapporten foreslår KraftCERT indikatorer selskapene kan bruke, som «antall detekterte angrepsforsøk» og «antall sårbarheter som førte til sikkerhetsoppdateringer», og indikatorer som kan brukes i et nasjonalt perspektiv, som «volum angrepsforsøk fordelt på kjente aktører». KraftCERT anbefaler også at det legges til rette for et sensornettverk i kraftforsyningen, og viser til at bruken av sensornettverk i helse- og utdanningssektorene har gitt gode resultater. NVE opplyser i intervju at arbeidet med å utvikle et rammeverk for å analysere IKT-hendelser ikke er fullført, men at KraftCERTs rapport gir et bedre kunnskapsgrunnlag for det videre arbeidet.

5.4.3 Budsjettering

Både NVE, tilsyns- og beredskapsavdelingen og beredskapsseksjonen har hatt stabile budsjetter i perioden 2017–2020, og antall ansatte har ligget på omtrent samme nivå i denne perioden. NVE viser til at det er bevilget midler til å finansiere avtalen med KraftCERT over statsbudsjettet (to millioner kroner i 2019 og

[56] KraftCERT (2020) *Digital kontroll: en studie om innføring og bruk av metrikker i kraftforsyningen for bedre IKT-sikkerhet.* NVE-rapport nr. 22/2020.

2020). Dette skjedde i dialog mellom Olje- og energidepartementet og NVE, og midlene ble øremerket i tildelingen i 2019 og 2020. NVE har ikke meldt inn behov for økte midler over statsbudsjettet til arbeidet med IKT-sikkerhet i kraftforsyningen. NVE viser til at tilsyn med IKT-sikkerhet i kraftforsyningen er sektoravgifts-finansiert, og at ressursene til tilsyns- og beredskapsavdelingen styres gjennom interne budsjettprosesser. I følge NVE gjøres den ressursmessige prioriteringen av IKT-sikkerheten i kraftforsyningen gjennom intern disponering av ressurser. Slik NVE vurderer det, har både seksjonen og avdelingen prioritert temaet IKT-sikkerhet innenfor sine rammer.

Internt i NVE kan seksjonene søke om midler til såkalte prioriterte tiltak og FOU-prosjekter, og en økende andel av disse midlene er tildelt prosjekter som omhandler IKT-sikkerhet i kraftforsyningen, se punkt 6.4. I perioden fra 2017 til 2020 økte andelen midler som gikk til FoU-prosjekter om IKT-sikkerhet av den totale andelen FoU-midler, fra 4,4 prosent til 9,1 prosent. Andelen som gikk til IKT-sikkerhetsrelaterte tiltak av den totale andelen midler til prioriterte tiltak, økte fra 3,5 prosent i 2017 til 13,9 prosent i 2019 og 8,9 prosent i 2020. Disse midlene gikk ned fra 1,2 millioner kroner i 2019 til 650 000 kroner i 2020.

5.4.4 Kapasitet

I perioden 2015–2016 så NVE at det var behov for å styrke arbeidet med IKT-sikkerhet i kraftforsyningen. I 2016 ba ledelsen i NVE tilsyns- og beredskapsavdelingen om å øke kapasiteten med ett årsverk innenfor IKT-sikkerhet, og dette ble gjort ved å omgjøre en av stillingene i seksjonen til arbeidet med IKT-sikkerhet. I 2018 ansatte seksjonen en person til med IKT-sikkerhetskompetanse. Fagekspertisen til beredskaps-seksjonen innenfor feltet IKT-sikkerhet består per november 2020 av tre ansatte: to fulltidsansatte og én ansatt som utfører enkelte oppgaver i seksjonen og samtidig tar doktorgrad i sikkerhet i driftskontroll-systemer. I perioden 2017–2019 hadde beredskapsseksjonen i gjennomsnitt om lag to årsverk med IKT-kompetanse til arbeidet med IKT-sikkerhet i kraftforsyningen. NVE påpeker at seksjonen er tverrfaglig sammensatt, med en hovedvekt av ansatte som har spesialkompetanse innenfor andre områder enn IKT-sikkerhet. NVE har også lært opp tre elkraftingeniører til å være med og gjennomføre IKT-sikkerhetstilsyn og til å bidra ved enkelte andre oppgaver på dette området. Gruppen som fører tilsyn med IKT-sikkerhet, består dermed av flere enn de ansatte som har spesialkompetanse på IKT-sikkerhetsområdet, og utgjør totalt seks personer. NVE mener ordningen med å benytte ansatte med annen fagkompetanse til IKT-sikkerhetstilsyn vil øke NVEs kvalitet og kapasitet på området.

Omfanget av oppgaver innenfor arbeidet med IKT-sikkerhet har økt i takt med digitaliseringen i kraftforsyningen. I undersøkelsesperioden brukte NVE mye tid på å endre regelverket og utforme tilhørende skriftlig veileder, gi direkte veiledning til enkeltselskaper, avklare rollen som sektorvist responsmiljø og iverksette kompetansetiltak til bransjen (kurs, foredrag). Flere av oppgavene innenfor arbeidet med IKT-sikkerhet i kraftforsyningen ble forsinket eller utsatt på grunn av kapasitetsutfordringer, blant annet utarbeidelsen av en endelig veileder til kraftberedskapsforskriften, enkelte IKT-tilsyn og avklaringen av KraftCERTs rolle. Sykefravær, permisjoner og doktorgradsarbeid førte til forsinkelser i 2019, mens arbeid i 2020 også ble utsatt på grunn av NVEs oppfølging av selskapenes beredskap under covid-19.

Selv om det er få ansatte som arbeider med IKT-sikkerhet i NVE, mener NVE at beredskapsseksjonens budsjett og midlene som har vært tildelt FoU og prioriterte tiltak, har sørget for at det samlede ressursnivået for NVEs arbeid med å styrke IKT-sikkerheten i kraftforsyningen de siste årene har vært akseptabelt. NVE har brukt eksterne konsulenter og studenter for å gjennomføre noen av FoU-prosjektene. NVE påpeker imidlertid at det er behov for å øke antall ansatte som arbeider med dette feltet framover, og at det lave antallet ansatte med IKT-sikkerhetskompetanse er sårbart for sykdom og annet fravær. At NVE i 2019 ble utpekt som sektorvist responsmiljø og som tilsynsmyndighet etter sikkerhetsloven, der IKT-sikkerhet er et viktig fagfelt, øker ressursbehovet ytterligere.

Både i NVEs strategier, virksomhetsplaner og risikovurderinger trekkes styrket intern kompetanse på dette feltet fram som et viktig tiltak. Både i 2018 og 2019 skrev NVE i en stillingsanalyse for en fast IKT-stilling i beredskapsseksjonen at «[s]eksjonen trenger å styrke kapasitet og kompetanse innen IKT-sikkerhet». NVE oppgir at det er utfordrende for dem å rekruttere personer med IKT-sikkerhetskompetanse, og i 2019 utlyste seksjonen en stilling som ikke fikk kvalifiserte søkere. NVE framhever også at det er viktig å balansere seksjonens behov for elkraftkompetanse mot IKT-sikkerhetskompetanse, og at NVE har behov for folk med begge typer kompetanse ettersom elkraft og digitale systemer smelter mer og mer sammen.

5.5 Rapportering, oppfølging og kontroll

5.5.1 Årsrapportering

NVE rapporterer på målene som er satt av departementet, i årsrapporten. Arbeidet med IKT-sikkerhet i kraftforsyningen rapporteres under hovedmålet om å fremme en sikker kraftforsyning og delmålet om å påse at beredskapen i kraftforsyningen er god og i tråd med gjeldende krav. Rapporteringen består i hovedsak av en beskrivelse av aktivitetene som er gjennomført for å bidra til å fremme hovedmålet, som utvikling av regelverk, veiledning og tilsyn. NVE rapporterer i liten grad om hvordan aktivitetene har bidratt til å fremme hovedmålet, eller om statusen og utviklingen i sikkerhets- og beredskapstilstanden i kraftforsyningen. I årsrapportene for perioden 2017–2019 rapporterte NVE om tilsynsvirksomheten. Årsrapportene for 2017 og 2018 beskriver hvilke tema NVE konsentrerte seg om, og inneholder en omtale av alvorlighetsgraden på de avvikene som ble funnet. En lignende omtale av avvik og alvorlighetsgrad inngår ikke i årsrapporten for 2019. I årsrapportene for alle de tre årene vises det til at antallet og typen avvik var på samme nivå som tidligere år. Dette forklares med at tilsynene var gjennomført hos virksomheter som ikke hadde hatt tilsyn tidligere. NVE peker på at en virksomhet sjelden har avvik ved en påfølgende kontroll, og at dette tyder på at kontrollene har den tiltenkte effekten. I planen for tilsynsaktivitet for 2020 skriver beredskapsseksjonen imidlertid at det – til tross for at det i flere år har blitt ført tilsyn med blant annet virksomhetenes risikovurderinger (kraftberedskapsforskriften § 2-3) og beredskapsplaner (kraftberedskapsforskriften § 2-4) – er vanskelig å si om tilstanden er vesentlig forbedret.

5.5.2 Tilstandsvurderinger og ROS-analyser

NVE mener flere dokumenter kan brukes for å si noe om utviklingen i sikkerhetstilstanden og resultatene av NVEs arbeid med å styrke IKT-sikkerheten i kraftforsyningen. Prop. 1 S (2017–2018) fra Olje- og energidepartementet inneholder en tilstandsvurdering av kraftforsyningen som NVE ga innspill til. I tilstandsvurderingen trekkes det fram at avbruddsstatistikken viser at leveringspåliteligheten av strøm er høy, og at avbrudd i kraftforsyningen ofte skyldes naturgitte hendelser. I tilstandsvurderingen står det videre at det i trusselvurderinger vises til at systemer i kraftsektoren er utsatt for etterretning, men at det er vanskeligere å vurdere sannsynligheten for tilsiktede hendelser enn for naturhendelser. Årsaken er at det finnes mye mer statistikk om sistnevnte enn førstnevnte hendelser.

I 2017 gjennomførte NVE også FoU-prosjektet *Informasjonssikkerhetstilstanden i energiforsyningen.* Målet var å etablere et første situasjonsbilde av IKT-sikkerheten i kraftforsyningen ved å utvikle et spørreskjema og en analytisk metode for å analysere sikkerhetstilstanden i kraftforsyningen over tid. NVE ba alle selskaper i kraftforsyningen om å svare på en spørreundersøkelse om selskapenes avhengighet av leverandører og deres erfaring med uønskede IKT-hendelser. I tillegg ble det gjennomført inntrengingstest av tre selskaper for gi ytterligere forståelse av den digitale sårbarheten. Ifølge NVE bidrar slike kartlegginger av selskapenes erfaringer med IKT-hendelser til å gi et aggregert bilde av sikkerhetstilstanden i bransjen, men de må suppleres med andre datakilder siden svarene avhenger av selskapenes interne systemer for å oppdage og registrere hendelser. NVE oppgir at de planlegger å gjenta undersøkelsen i 2021.

På bestilling fra Olje- og energidepartementet publiserte NVE et faktaark i 2019, som en forenklet oppdatering av tilstandsvurderingen fra 2017, med blant annet statistikk for leveringspålitelighet og en oversikt over hvilke avvik som oftest var avdekket i tilsyn med kraftberedskap og vedlikehold i perioden 2015–2018.[57] Under temaet IKT-sikkerhet viser NVE til at digitaliseringen har ført til endringer i risiko- og sårbarhetsbildet, og at komplekse tjenester, mangelfull tilgang til kompetanse og endringer i leverandørmarkedet er utfordrende både for selskapene og myndighetene. I forbindelse med den oppdaterte tilstandsvurderingen utarbeidet NVE også en oversikt over uønskede hendelser NVE hadde blitt kjent med, med en nærmere beskrivelse av enkelte hendelser som gjaldt IKT-angrep og informasjonssikkerhet.[58] Slike hendelser er nærmere beskrevet i punkt 8.5.1. Tilstandsvurderinger er et kapittel i budsjettproposisjonen for Olje- og energidepartementet hvert fjerde år, og NVE vil utarbeide en ny tilstandsvurdering i 2021.

I tillegg til tilstandsvurderingene har NVE utarbeidet ROS-analyser og overordnede risikovurderinger. Her trekker NVE fram at det er risiko for at IKT-angrep kan ramme kraftforsyningen, og at NVE mangler kunnskap om selskapenes IKT-sikkerhet på flere områder.

[57] NVE (2019) *Tilstandsvurdering av forsyningssikkerhet og beredskap i kraftforsyningen.* Faktaark nr. 10/2019.
[58] NVE (2019) *Oppsummering av uønskede hendelser 2018 i energiforsyningen.* Faktaark nr. 4/2019.

NVE oppgir i intervju at de ikke har et mål om å dokumentere den konkrete risikoen eller sårbarheten i hvert selskap. NVE mener den oversikten de har over IKT-sikkerhetstilstanden i selskapene, i hovedsak er oppnådd gjennom tilsyn og dialog med selskapene. I tillegg mottar NVE varsler om ekstraordinære situasjoner og informasjon om uønskede IKT-hendelser som bidrar til etatens kunnskapsnivå. Tilsynene er stikkprøvekontroller og går ikke i dybden. NVE sier at det ikke er et mål for NVE å ha oversikt over IKT-systemene i alle KBO-enheter. NVE har ikke kunnskap om sikkerhetstilstanden til selskaper der de ikke har ført tilsyn eller mottatt informasjon gjennom veiledning eller hendelsesrapportering. NVE oppgir at de foreløpig ikke har god oversikt over hvordan selskapene etterlever de nye kravene i kraftberedskaps-forskriften. Kraftberedskapsforskriften inneholder systemkrav, som innebærer at selskapene skal ha internkontrollsystemer som viser at de følger kravene. Med bakgrunn i blant annet NVEs kunnskap, kapasitet og tilnærming til tilsyn har etaten vurdert at det ikke er hensiktsmessig å kontrollere effekten av den tekniske sikringen av de digitale systemene hos selskapene. NVE anser at selv om denne tilnærmingen kan medføre at hvert enkelt tilsyn har mindre effekt, får NVE besøkt flere virksomheter, og etaten anser at metodikken har en god effekt på den generelle forsyningssikkerheten og sikkerhetsbevisstheten i det enkelte selskapet.

Selv om NVE ser at det er behov for mer informasjon om sikkerhetstilstanden i selskapene, oppgir de at det er en grense for hvor mye informasjon de velger å hente inn. Dette skyldes blant annet at sensitiviteten øker når store mengder informasjon blir samlet, og selv om sensitiv informasjon skjermes i etatens saksbehandlingssystemer, kan digitale systemer ha sårbarheter som en eller annen gang kan utnyttes. NVE framhever at de dessuten har begrenset kapasitet til å analysere så store mengder data. Dermed blir spørsmålene som gjennomgås i tilsynet, et viktig verktøy i tillegg til dokumentgjennomgangen før tilsynet. NVE trekker også fram at det ikke nødvendigvis er deres rolle å ha så inngående kunnskap om selskapenes systemer siden regelverket er basert på at selskapene selv er ansvarlige for sin egen sikkerhet, og funksjonskravene gir dem frihet til å velge hvilke løsninger de vil bruke.

5.5.3 Intern rapportering og oppfølging

Tilsyns- og beredskapsavdelingen rapporterer tre ganger i året til økonomiseksjonen om avdelingens foreløpige forbruk opp mot budsjettet. Økonomiseksjonen sammenstiller rapporteringen fra alle avdelingene og presenterer dette for direktørmøtet i NVE. Ved rapporteringen for første tertial gjøres det ofte omprioriteringer, mens det ved rapporteringen for andre tertial i mindre grad gjøres endringer. NVE følger ikke systematisk opp at oppgavene i den overordnede virksomhetsplanen til NVE blir gjennomført. På avdelingsnivå i tilsyns- og beredskapsavdelingen foretas det en statusgjennomgang av tiltakene i virksomhetsplanen ca. halvveis i året, med mulighet for omprioritering av ressurser og fokus. Beredskaps-seksjonen går gjennom status hvert halve år og i forbindelse med planleggingen av neste års oppgaver og av enkeltoppgaver ved behov. NVE oppgir at rapportering på arbeidet med IKT-sikkerhet i kraftforsyningen skjer i linjen fra medarbeiderne til seksjonsleder og som orienteringssaker på seksjonsmøter. NVE framhever at etaten har en organisasjonsstruktur med kort avstand til ledere, og at uformell kommunikasjon er en viktig del av rapporteringen. Rapportering på FoU skjer på NVEs FoU-dager og gjennom sluttrapporter på FoU. Rapportering av tilsynsvirksomheten beskrives i punkt 7.5.

5.5.4 Evaluering

NVE har ikke selv evaluert eller fått andre til å evaluere etatens arbeid med å styrke IKT-sikkerheten i energiforsyningen. NVE oppgir i intervju at de har vært opptatt med å endre regelverket de seneste årene, og at de for tiden er i ferd med å utarbeide veiledere. Etaten har ikke brukt ressurser på å evaluere resultatene av eget arbeid i denne perioden. NVE forventer at effekten av tiltak som ble iverksatt i 2019, først kommer på lengre sikt (om flere år), og derfor har de heller ikke prioritert å evaluere tiltakene ennå. NVE viser ellers til Sikkerhetsutvalgets arbeid fra 2016, som inneholder en vurdering av regelverket på området.[59]

NVE opplyser i intervju at beredskapsseksjonen ikke har gjennomført noen evalueringsprosjekter som har gått gjennom hele eller deler av seksjonens organisering og arbeidsprosesser siden 2015. Mange av oppgavene innenfor IKT-sikkerhetsarbeidet i beredskapsseksjonen er ikke prosjektorganiserte, men løper kontinuerlig, og det er derfor ikke noe naturlig stoppunkt for evaluering. Seksjonen diskuterer imidlertid erfaringer fra forrige års oppgavegjennomføring i planleggingen av kommende års aktiviteter, for eksempel

[59] Forsvarets forskningsinstitutt (2016) *Vurdering av forebyggende sikkerhet innen kraft, petroleum og luftfart*. FFI-rapport nr. 16/00702.

av tilsyn. I NVE er det også flere møter per år mellom ansatte i ulike deler av seksjonen som arbeider med tilsyn, hvor erfaringer deles.

5.5.5 Internkontroll

NVE oppgir at de ikke har et samordnet kvalitetssystem eller felles rutiner for jevnlig gjennomgang og oppdatering av rutiner. NVE har etablert et felles rammeverk for hvor og hvordan styringsdokumenter skal opprettes, skrives, godkjennes, lagres og publiseres. NVEs avdelinger har ansvaret for alltid å ha oppdaterte og godkjente styringsdokumenter for sine områder. Styringsdokumentene inneholder rammer/føringer, prosesser og prosedyrer for hvordan oppgaver skal utføres. NVE oppgir at det er et mål å ha kvalitets-håndbøker i alle seksjoner, men at dette arbeidet ikke er fullført. Sammenlignet med andre seksjoner i NVE har beredskapsseksjonen få dokumenter som beskriver hvordan seksjonens arbeid skal utføres, utover tilsynsvirksomheten. Beredskapsseksjonen er i ferd med å utarbeide enkelte nye prosedyrer for hvordan ansatte skal løse arbeidsoppgaver, for eksempel en rutinebeskrivelse for utnevning av nye distriktssjefer for kraftforsyningen. NVE oppgir i intervju at kvalitetssikring i linjen sikrer god internkontroll av oppgavene som utføres med IKT-sikkerhet i kraftforsyningen.

6 NVEs arbeid med regelverk, veiledning og kompetanseheving innenfor IKT-sikkerhet

I dette kapitlet beskriver vi hvordan NVE har revidert regelverket for IKT-sikkerhet, og hvordan de veileder selskapene i kraftforsyningen om regelverket. Kapitlet inneholder også en beskrivelse av hvordan NVE har arbeidet med kompetanseheving internt og eksternt.

6.1 Relevante føringer

- Styrket IKT-sikkerhet i energiforsyningen krever at NVE kontinuerlig utvikler regelverket for IKT-sikkerhet i bransjen.
- NVE må bygge opp sin egen kompetanse, slik at de får god forståelse for risikobildet i forbindelse med ansvaret de har for regelverksutviklingen.
- NVE skal stimulere til mer ressurssterke fagmiljøer innenfor IKT-sikkerhet.
- NVE har en veiledningsplikt på IKT-sikkerhetsområdet. Formålet med veiledningsplikten er å sette selskapene i stand til å ivareta interessene sine på best mulig måte.

6.2 Oppsummering

- Regelverket er blitt endret med tydeligere krav til sikring av alle digitale systemer.
- Mange selskaper opplever at det er vanskelig å forstå hva som er godt nok for å etterleve regelverket.
- NVEs arbeid med å utarbeide endelig skriftlig veileder til kraftberedskapsforskriften har blitt forsinket.
- Selskapene er i stor grad fornøyd med veiledningen de får fra NVE, men mange selskaper har behov for mer veiledning om IKT-sikkerhet.
- NVE har gjennomført flere FoU-prosjekter og bidratt til utdanningstilbud, kurs og seminarer for å heve kompetansenivået innenfor IKT-sikkerhet i bransjen.

6.3 Regelverk og veiledning om IKT-sikkerhet i kraftforsyningen

6.3.1 Utviklingen av regelverket for IKT-sikkerhet

Kravene til IKT-sikkerhet i kraftforsyningen er gitt i energiloven med forskrifter, hovedsakelig i kraftberedskapsforskriften. Denne forskriften, som tidligere het *forskrift om forebyggende sikkerhet og beredskap i energiforsyningen* (beredskapsforskriften), ble vedtatt første gang i 2002. Den økende avhengigheten av IKT førte til økt oppmerksomhet rundt sikring av driftskontrollsystemene. I 2013 ble forskriften revidert, og NVE utga samtidig en veileder til forskriften. Beredskapsforskriften fra 2013 inneholdt krav om at alle enheter i KBO skulle arbeide systematisk med tiltak for å forebygge og håndtere ekstraordinære hendelser som kunne ramme kraftforsyningen. Den inneholdt generell plikt for sikring av anlegg og systemer, i tillegg til mer spesifikke krav til beskyttelse av driftskontrollsystemer.

I 2016–2017 gjennomførte NVE et prosjekt der de vurderte behovet for å revidere regelverket for IKT-sikkerhet i energisektoren.[60] Prosjektet var en oppfølging av Lysneutvalgets[61] anbefaling til NVE om å gå gjennom sektorregelverket og se på et funksjonsbasert regelverk og bruk av standarder. Lysneutvalget viste at den økende avhengigheten av IKT i ulike sektorer, blant annet energiforsyningen, skapte behov for krav om å beskytte informasjon og sørge for at nettverk og systemer er sikre og stabile. Prosjektet fikk innspill fra bransjen, leverandører, interesseorganisasjoner og andre myndigheter. Arbeidet resulterte i NVE-rapporten *Regulering av IKT-sikkerhet* (2017), som pekte på behovet for endringer i regelverket med bakgrunn i de utfordringene digitaliseringen og teknologiskiftet i energiforsyningen hadde medført.

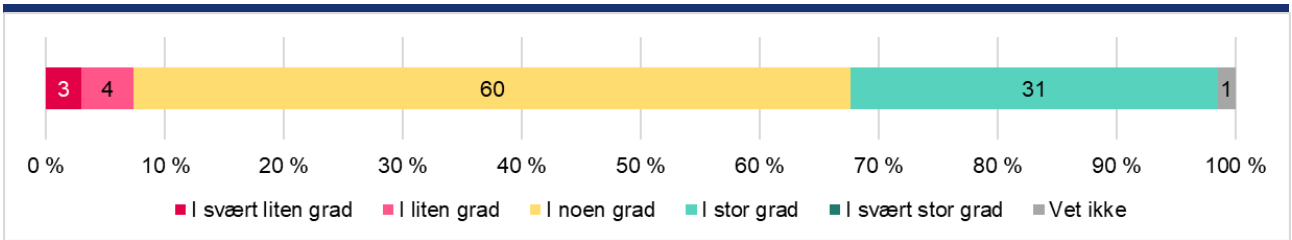
Den nye kraftberedskapsforskriften trådte i kraft 1. januar 2019. Samtidig publiserte NVE en foreløpig tilleggsveileder for endringene i forskriften. Det ble gjort flest endringer i kapittel 6, om informasjonssikkerhet, og noen mindre endringer i kapittel 7, om driftskontrollsystemer. Endringene tydeliggjorde blant annet kravene til sikring av IKT-systemer og stilte krav til grunnsikring for alle digitale informasjonssystemer (§ 6-9), jf. NSMs grunnprinsipper for IKT-sikkerhet fra august 2017. Forskriften fikk også inn nye krav til IKT-sikkerhet

[60] NVE (2017) *Regulering av IKT-sikkerhet*. NVE-rapport nr. 26/2017.
[61] NOU (2015: 13) *Digital sårbarhet – sikkert samfunn*.

i AMS. NVE viser til at kraftberedskapsforskriften inneholder strenge krav til IKT-sikkerhet sammenlignet med andre norske sektorer og andre europeiske land. Da EU-direktivet (NIS-direktivet) om IKT-sikkerhet ble innført i Norge, var det ikke nødvendig å gjøre endringer i kraftberedskapsforskriften fordi de nye kravene allerede var dekket.

NVE oppfatter at de nye kravene i kraftberedskapsforskriften har blitt positivt mottatt av bransjen, og at de har gjort det lettere for IKT-ansvarlige i bransjen å få gjennomslag for å forbedre sikkerheten i virksomheten de arbeider i. Etter at kraftberedskapsforskriften trådte i kraft, har NVE fått tilbakemelding fra bransjen på kurs og konferanser der NVE har holdt foredrag, og i skriftlige og muntlige henvendelser. Dette har gitt NVE informasjon om hvilke krav som er uklare. NC-Spectrum AS gir i intervju uttrykk for at endringene med strengere krav til grunnsikring av administrative systemer var hensiktsmessige, men at de burde ha blitt innført tidligere. Mange av IKT-systemene i kraftbransjen er etablert med tanke på funksjonalitet framfor sikkerhet, og det gjelder både driftskontrollsystemer og administrative systemer. NC-Spectrum AS gir uttrykk for at det er krevende å etablere god sikkerhet etter at systemene er tatt i bruk. Da blir det ofte en avveining mellom å sikre systemer ved å fjerne funksjonalitet og effektive arbeidsprosesser.

Figur 4 IKT-sikkerhetskoordinatorenes svar på om arbeidet med den nye kraftberedskapsforskriften har ført til forbedring (N = 68)



Om lag 30 prosent av IKT-sikkerhetskoordinatorene som svarte på vår spørreundersøkelse, oppga at endringene i kraftberedskapsforskriften i stor grad har ført til forbedring i selskapet. Hvor god IKT-sikkerhetstilstanden var i selskapet før den nye forskriften ble innført, kan virke inn på svarene.

6.3.2 Økt behov for IKT-sikkerhetskompetanse når regelverket er funksjonsbasert

I spørreundersøkelsen oppga nærmere 80 prosent av IKT-sikkerhetskoordinatorene at en av årsakene til at det er vanskelig å etterleve kravene i kraftberedskapsforskriften, jf. figur 3, er at «det er vanskelig å vite hva som er 'godt nok' for å etterleve kravene». Flere av kravene vi spurte om i spørreundersøkelsen, kom først inn i forskriften i 2019, blant annet § 6-9. Kravet i § 6-9 om sikring av alle IKT-systemer er et funksjonskrav, det vil si at selskapene selv skal velge løsninger for å ivareta IKT-sikkerheten ut fra egne risikovurderinger. Bruk av funksjonsbaserte krav er i tråd med utviklingen av annet regelverk, for eksempel sikkerhetsloven og Finanstilsynets IKT-forskrift. I forbindelse med høringen om kraftberedskapsforskriften viste NVE til at den praktiske implementeringen av kravene – fordi de er funksjonskrav – kan tilpasses den enkelte virksomhets økonomiske verdier og behov for forebyggende sikkerhet og beredskap.[62] NVE gir i intervju uttrykk for at funksjonsbaserte krav er best egnet for IKT-sikkerhetskrav fordi de er bedre tilpasset de kontinuerlige endringene i teknologien. Funksjonsbaserte krav stiller imidlertid større krav til kompetanse og kapasitet i selskapene, samtidig som kraftforsyningen består av mange små selskaper med begrensede ressurser til sikkerhetsarbeidet.[63] Kompetanseutfordringen for små selskaper ble også påpekt av Lysneutvalget, som anbefalte større fagmiljøer. Når regelverk er funksjonsbaserte, er det ifølge NVEs rapport *Regulering av IKT-sikkerhet* (2017) viktig at myndighetene tilbyr tilstrekkelig veiledning i regelverksforståelse og kontinuerlig vurderer om selskapene etterlever kravene til tilstrekkelige og forsvarlige løsninger. Rapporten anbefaler at NVE i en skriftlig veileder presiserer hva som er god sikkerhet, og henviser til internasjonale standarder og gode veiledere der det er hensiktsmessig.

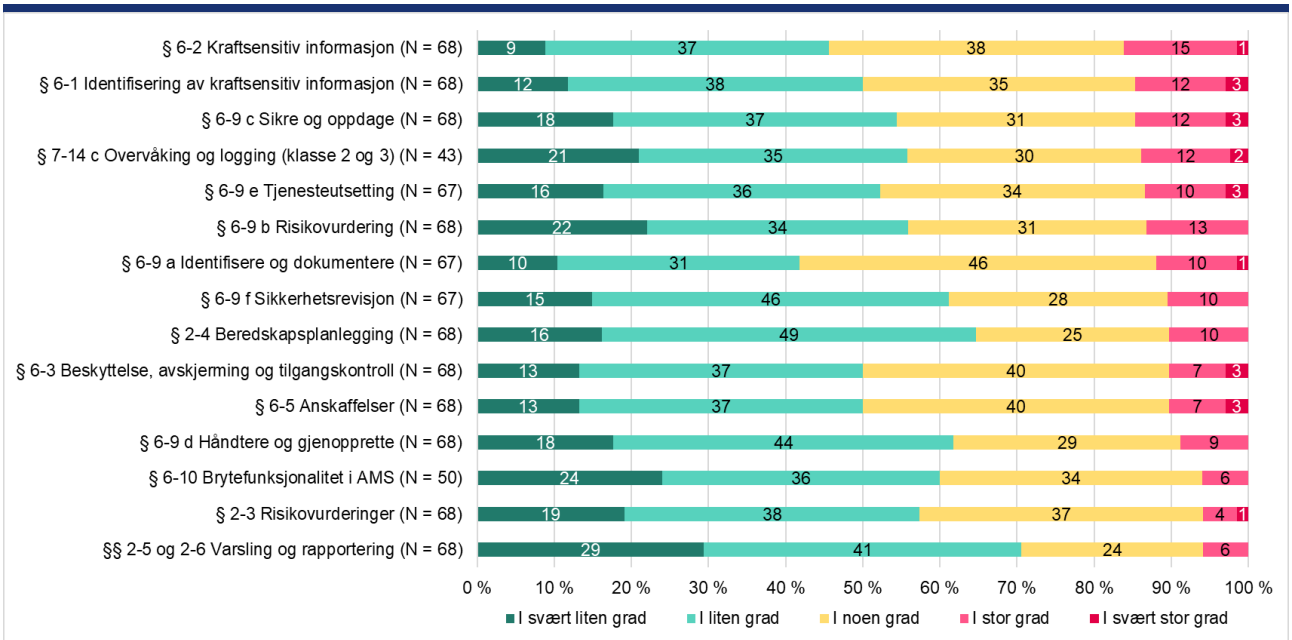
Rapporten påpeker også at valget av funksjonskrav gjør det mer krevende for NVE å angi hva som konkret ligger i et krav, og når de skal gi avvik ved tilsyn. Når NVE skal føre tilsyn, må funksjonskravene kunne brytes ned slik at NVE kan vurdere om kravene i regelverket er tilfredsstilt eller ikke. NVE påpeker at det å føre tilsyn med hvordan selskapene etterlever funksjonskravene, krever tilsynspersonell med høy

[62] NVE (2018) *Oppsummeringsdokument: Endringer i beredskapsforskriften - Krav til IKT-sikkerhet m.m.* NVE-rapport nr. 92/2018.
[63] NVE (2017) *Regulering av IKT-sikkerhet*. NVE-rapport nr. 26/2017.

kompetanse og veiledere som tilsynspersonellet kan bruke til å fastslå hva som er godt nok for å oppfylle kravene. NVE understreker overfor selskapene at de ikke godkjenner selskapets sikkerhetstiltak ved tilsyn, men vurderer om selskapets løsning etterlever kravene i kraftberedskapsforskriften. Under tilsynet må virksomheten dokumentere tiltakene de har valgt, og vise eller beskrive risikovurderingen som ligger til grunn. NVE gjør en skjønnsmessig vurdering av om selskapets risikovurderinger er i samsvar med kravene i regelverket. NVE mener at de gjennom tilsyn kan avdekke om selskapene har hatt en god prosess med utformingen av sine risikovurderinger og i hvilken grad selskapene avdekker risikoer eller ikke. NVE viser også til at mange av de mindre selskapene samarbeider om IKT-sikkerhet gjennom Nettalliansen AS.

Når det gjelder selskapenes oppfatning av det funksjonsbaserte regelverket, påpeker NVE at det er et gjennomgående skille mellom selskapene i sektoren: Mindre selskaper foretrekker ofte konkrete krav, slik at de kan bruke forskriften som spesifikasjonskrav i bestillinger av IKT-tjenester, mens større selskaper ofte ønsker funksjonsbaserte krav, slik at de kan velge løsninger og tilpasse dem slik det passer dem best. Flere aktører vi har intervjuet, støtter i stor grad at NVE har valgt et funksjonsbasert regelverk, men sier at det er utfordrende for selskapene å forstå hva som er godt nok for å etterleve kravene, og at mange selskaper ikke har tilstrekkelig kompetanse eller kapasitet til å gjøre gode risikovurderinger. NC-Spectrum AS oppgir i intervju at selskapene ville hatt et bedre utgangspunkt for å forhandle med leverandørene om sikkerhetsnivået dersom NVE hadde fastsatt konkrete IKT-sikkerhetskrav i forskriften.

Figur 5 IKT-sikkerhetskoordinatorenes svar på om utvalgte krav er utfordrende å forstå



I vår spørreundersøkelse svarte i gjennomsnitt om lag 55 prosent av IKT-sikkerhetskoordinatorene i selskapene at de utvalgte kravene i liten eller svært liten grad er utfordrende å forstå. Rundt en tredel oppfatter at det i noen grad er utfordrende å forstå kravene. De kravene som IKT-sikkerhetskoordinatorene mener er mest utfordrende å forstå, er kravet til å identifisere kraftsensitiv informasjon, kravet til å sikre informasjonssystemer og oppdage uønskede hendelser og kravet til overvåking og logging.

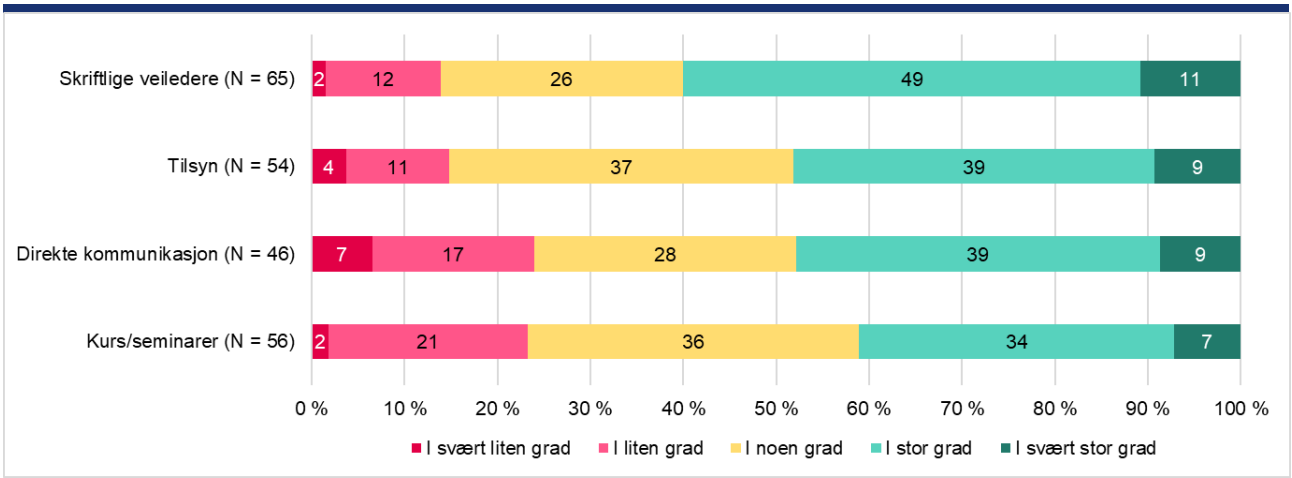
NVE oppfatter at selskapene synes noen av kravene er uklare, og trekker særlig fram kravet om å identifisere kraftsensitiv informasjon og problemstillinger rundt leverandører. Når det gjelder hva som skal defineres som kraftsensitiv informasjon, bidrar informasjon som allerede er tilgjengelig fra ulike karttjenester, og åpenhetskravene i norsk forvaltning til usikkerheten rundt dette kravet. NVE startet i 2019 et forprosjekt som blant annet skulle kartlegge forståelsen av bestemmelsene om kraftsensitiv informasjon, både internt og eksternt. NVE sendte i den forbindelse en spørreundersøkelse til KBO-enhetene og ansatte i NVE. På spørsmål om forskriften er tydelig når det gjelder å identifisere hva kraftsensitiv informasjon er, svarte 16 prosent av selskapene at forskriften i liten eller svært liten grad er tydelig, mens 25 prosent av de ansatte i NVE svarte det samme. 34 prosent av selskapene og 51 prosent av de ansatte i NVE svarte verken/eller på om forskriften er tydelig på dette punktet. NVE har også opplevd at det overfor selskapene kan være

utfordrende å argumentere for at enkelte informasjonslekkasjer medfører brudd på kravet om å beskytte kraftsensitiv informasjon.

6.3.3 NVEs veiledning

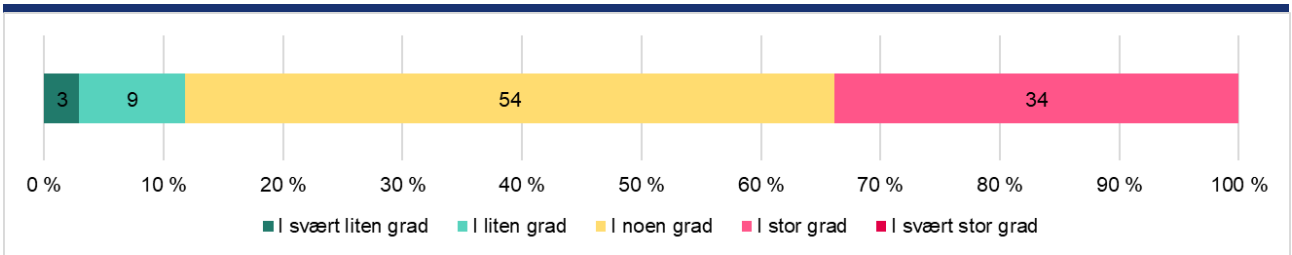
NVE veileder selskapene i kraftsektoren om hvordan de skal forstå kravene i regelverket, gjennom skriftlige veiledere, kurs, seminarer, tilsyn og direkte kontakt med selskapene. NVE viser i intervju til at selskapene har behov for god veiledning fra etaten for å kunne vite om sikkerhetstiltakene de har valgt, oppfyller funksjonskravene i forskriften. I NVEs overordnede risikovurdering for 2019 går det fram at manglende veiledning og kontroll øker risikoen for at regelverket ikke overholdes. Dette begrunnes med at mye nytt regelverk gir behov for å sikre at aktørene forstår og kan følge regelverket, og at tilsyn og kontroll er nødvendig når nytt regelverk er innført.

Figur 6 IKT-sikkerhetskoordinatorenes svar på om NVEs veiledning har vært tilfredsstillende



I spørreundersøkelsen svarte i gjennomsnitt om lag halvparten av IKT-sikkerhetskoordinatorene at de i stor eller svært stor grad er fornøyd med de ulike formene for veiledning de får fra NVE. Av NVEs former for veiledning er IKT-sikkerhetskoordinatorene mest fornøyde med NVEs skriftlige veiledere. Flere aktører i bransjen (KBO-enheter og konsulentselskaper) gir også i intervju uttrykk for at selskapene er fornøyde med den veiledningen de får fra NVE om IKT-sikkerhet. Samtidig viser spørreundersøkelsen at 34 prosent av IKT-sikkerhetskoordinatorene opplever at de i stor grad har behov for mer veiledning om IKT-sikkerhet fra NVE, se figur 7.

Figur 7 IKT-sikkerhetskoordinatorenes svar på om de har behov for mer veiledning om IKT-sikkerhet fra NVE (N = 68)



Hvor ofte selskapene tar kontakt med NVE for å få veiledning, varierer, men flere selskaper gir uttrykk for at NVE svarer raskt på henvendelser og gir gode svar. Flere aktører gir uttrykk for at de ansatte som arbeider med IKT-sikkerhet i NVE, har god kompetanse, men at NVE har for få ressurser til dette arbeidet.

NVEs skriftlige veiledere

I NVE blir begrepet *veileder* brukt om offentlige myndigheters råd og informasjon. Veiledere forklarer formålet med og innholdet i ulike bestemmelser i forskrifter og gir råd om hvordan man kan oppfylle krav som er satt i lover eller forskrifter. Mange av NVEs forskrifter stiller funksjonskrav uten å si hvilken framgangsmåte eller teknisk løsning som er riktig for å oppfylle kravet. I slike tilfeller er det ifølge NVEs prosedyrer om forskrifts-arbeid ofte hensiktsmessig å utarbeide veiledere om hvilke løsninger NVE aksepterer som forskriftsmessige.

NVEs foreløpige tilleggsveileder til kraftberedskapsforskriften gjaldt bare de av bestemmelsene i forskriften som var endret. Veilederen til beredskapsforskriften fra 2013 gjaldt fram til den endelige veilederen ble publisert, så langt ikke annet fulgte av tilleggsveilederen.[64] I den foreløpige tilleggsveilederen sto det at NVE tok sikte på å revidere hele veilederen i løpet av 2019, men dette arbeidet ble forsinket. Den endelige veilederen ble publisert på NVEs nettside i desember 2020. I den endelige veilederen viser NVE til forskriftstekst, ordforklaringer, veiledning om hvordan kravet kan oppfylles, og lenker til eksterne kilder til veiledning.[65] Veilederen inneholder også fiktive caser med problemstillinger som NVE har erfart i kontakten med selskapene, for å formidle NVEs forvaltningspraksis til selskapene. NVE oppgir at de vil oppdatere veilederen ved behov, og at det utarbeides en rutine for dette.

I vår spørreundersøkelse oppga 60 prosent av IKT-sikkerhetskoordinatorene at de i stor eller svært stor grad er fornøyd med de skriftlige veilederne fra NVE, se figur 6. 14 prosent oppga at de i liten eller svært liten grad er fornøyd med de skriftlige veilederne. Både Nettalliansen AS og NC-Spectrum AS gir i intervju uttrykk for at det var uheldig at veilederen til forskriften ikke var klar da forskriften trådte i kraft, og at mange selskaper etterlyser den oppdaterte veilederen. Både i intervjuer og i kommentarer til spørreundersøkelsen har flere selskaper også etterlyst en oppdatert veileder til kraftberedskapsforskriften. Ifølge KraftCERT gir medlemsbedriftene uttrykk for at de oppfatter den foreløpige veilederen til forskriften som tidvis uklar, og at den ikke dekker en del sentrale tema. KraftCERT oppgir at de får tilbakemelding fra selskaper om at de ønsker mer presise konkretiseringer i NVEs veileder. Dette gjelder for eksempel uttrykk som *sikkert nok* og *tilstrekkelig* og kravene til skylagring.

Ifølge NVE bør både veilederen om risiko- og sårbarhetsanalyser i kraftforsyningen og veilederen om sikkerhet i AMS oppdateres. NVEs veileder om risiko- og sårbarhetsanalyser i kraftforsyningen er fra 2010. I en NVE-rapport fra 2020 som kartlegger bruk av tingenes internett, vises det til at bransjen har gjennomgått en omfattende teknologisk utvikling siden 2010, noe som gjør at det er behov for å oppdatere denne veilederen.[66] NVE oppgir at arbeidet med å oppdatere veilederen om risiko- og sårbarhetsanalyser i kraftforsyningen ikke vil bli prioritert før veilederen til kraftberedskapsforskriften er oppdatert. NVEs gjeldende veileder om sikkerhet i avanserte måle- og styringssystemer (AMS) er fra 2012. I en evaluering av denne veilederen i 2017 ble det vist til at sårbarheter og trusselbildet i cyberdomenet er i stadig endring, noe som krever kontinuerlig tilpasning av sikkerhetsarbeidet.[67] Dermed er det naturlig å oppdatere veilederen om sikkerhet i AMS jevnlig. NVE oppgir i intervju at arbeidet med å oppdatere denne veilederen er påbegynt, men at det har stoppet opp som følge av manglende ressurser.

NVE utga en sjekkliste for IKT-sikkerhet i anskaffelser og tjenesteutsetting i kraftforsyningen i januar 2020. Ifølge NVE er det viktig at det blir tatt hensyn til IKT-sikkerheten allerede i en tidlig fase av en anskaffelse eller tjenesteutsetting. Samtidig må IKT-sikkerhet være et tema gjennom hele levetiden til produktet eller tjenesten som er anskaffet, inkludert ved avhending eller skifte av leverandør. Flere aktører gir uttrykk for at denne sjekklisten er et godt tiltak fra NVEs side.

Veiledning gjennom direkte kommunikasjon

NVE veileder også selskapene gjennom å svare på telefoner og e-post, holde foredrag på aktuelle konferanser og ha møter med bransjen. I tillegg veileder NVE selskapene om endringer i regelverk i årlige forventningsbrev til KBO. NVE opplyser i intervju at det går mye tid til å svare på forespørsler fra selskapene og deres leverandører om IKT-sikkerhet. NVE oppgir at tidsbruken på hver henvendelse varierer, men anslår at NVE bruker om lag ett dagsverk i uka på å besvare slike henvendelser. NVE oppfatter at selskapene har lav terskel for å ta kontakt når det er ting de lurer på, og at både små og større selskaper tar kontakt. NVE opplever at dialogen med selskapene som tar kontakt, er god, og at det gir dem et godt innblikk i hvordan

[64] NVE (2018) *Foreløpig tilleggsveileder til kraftberedskapsloven*.
[65] NVE (2020) *Veiledning til kraftberedskapsforskriften.*
[66] NVE (2020) *Kartlegging av bruk av tingenes internett (IoT/IIoT) i norsk kraftforsyning*. NVE-rapport nr. 2/2020.
[67] NVE og SINTEF Energi AS (2017) *Evaluering av NVEs veileder til sikkerhet i AMS.* NVE-rapport nr. 44/2017.

selskapene jobber med IKT-sikkerhet. NVE oppgir at de prioriterer henvendelser fra selskapene høyt, og at behandlingen av disse går foran de mer langsiktige oppgavene i seksjonen.

NVE oppgir at de mottar både enkle og mer omfattende forespørsler om veiledning. Henvendelsene kan variere fra spørsmål der svaret går direkte fram av kraftberedskapsforskriften, til omfattende og prinsipielle spørsmål. NVE har formulert skriftlige svar på enkelte problemstillinger. NVE oppgir at det hender at de i veiledningen anbefaler eller fraråder konkrete løsninger selskapene vurderer. Dette danner da presedens for NVEs senere vurderinger av tilsvarende saker. Den nye veilederen til kraftberedskapsforskriften inneholder eksempler på problemstillinger som NVE har erfart i kontakt med selskapene.

NVE oppgir at de arkiverer alle skriftlige svar der de veileder om kraftberedskapsforskriften, slik at de kan bruke dem når de utarbeider veilederen til forskriften. Ifølge NVE blir alle komplekse saker arkivert, mens enklere henvendelser ofte behandles over telefon, uten at de arkiveres. På spørsmål om NVE deler informasjonen i de skriftlige svarene med andre selskaper enn det som sendte forespørselen, oppgir NVE at svaret ikke automatisk deles med andre selskaper. Dersom informasjonen i slike svar deles, skjer det hovedsakelig på konferanser og i fora der NVE deltar. I tillegg blir viktig informasjon tatt inn i årlige informasjonsskriv til KBO-enhetene. NVE har også som praksis å be selskaper presentere løsningene sine på bransjesamlinger dersom etaten tenker det kan være til hjelp for andre. NVE presiserer at problem-stillinger de diskuterer med ett selskap, ikke nødvendigvis er relevante for alle i KBO, og at de dermed er selektive med hva de deler med øvrige selskaper.

I spørreundersøkelsen oppgir om lag 70 prosent av IKT-sikkerhetskoordinatorene at de har fått veiledning om IKT-sikkerhet gjennom direkte kommunikasjon med NVE, det vil si i form av samtaler, e-post og i brev. I underkant av halvparten av disse svarer at de i stor eller svært stor grad er fornøyd med denne veiledningen, se figur 6.

NVEs veiledning gjennom tilsyn

NVE påpeker i intervju at det er viktig at tilsynspersonellet som fører tilsyn med hvordan selskapene etterlever funksjonskravene, har veiledere som de kan bruke til å fastslå hva som er godt nok for å oppfylle kravene. NVE understreker at formålet med tilsynet er å få informasjon om selskapet etterlever kravene. NVE oppgir at de i liten grad har kapasitet til å gi omfattende veiledning under tilsynene, men at orienteringer om avvik eller svar på eventuelle spørsmål fra selskapene, kan ha en veiledende funksjon. I NVEs prosedyrer for kontroll og reaksjonsbruk går det fram at NVE ved avvik skal være varsomme med å gi råd eller anbefalinger om konkrete løsninger dersom et avvik kan lukkes på flere måter. I slike tilfeller kan NVE heller gi utfyllende informasjon om innholdet i kravene og hva som generelt er viktig for å oppfylle dem. Når et avvik bare kan lukkes på én måte, bør NVE-ansatte som deltar i tilsynet, ifølge prosedyrene informere om dette. De kan henvise til veiledere eller annet informasjonsmateriell dersom det finnes. I spørre-undersøkelsen oppga 80 prosent av IKT-sikkerhetskoordinatorene at de har fått veiledning gjennom tilsyn, og av disse er i underkant av halvparten i stor eller svært stor grad fornøyd med veiledningen, jf. figur 6. Nettalliansen AS oppfatter at selskapene gjennomgående får god veiledning om hvordan avvik kan lukkes under tilsyn, og at det har vært en positiv utvikling i veiledningen i tilsynsrapportene.

6.4 NVEs arbeid med å heve kompetansen innenfor IKT-sikkerhet internt og i kraftforsyningen

I NVEs overordnede risiko- og vesentlighetsvurderinger for 2019 – under risikoen for at IKT-systemene i kraftforsyningen rammes av cyberangrep – trekkes det fram at den teknologiske utviklingen er rask, og at bransjen må ta i bruk ny teknologi på en sikker måte. Det står at NVE skal være en pådriver for å utvikle kompetanse gjennom FoU og kompetansehevende tiltak for å oppfylle bransjens behov i dag og i framtiden. Videre står det at på grunn av det funksjonsbaserte regelverket er det svært viktig at NVE selv har oppdatert kunnskap og kan gi god veiledning og at NVE skal bidra til å styrke kompetansen internt og eksternt gjennom kompetansefremmende tiltak og FoU som styrker forvaltningen, herunder doktorgradsstudier. Det går også fram at NVE arbeider med å utforme flere tiltak for å styrke kompetansen i bransjen.

Når det gjelder NVEs interne kompetanseoppbygging, viser NVE til at en ansatt tar doktorgrad om sikkerhet i driftskontrollsystemer, og at dette vil bidra med viktig kunnskap. NVE holder seg oppdatert på hvilke krav de bør stille til selskapene, blant annet gjennom samarbeid med utdanningsinstitusjoner og andre forsknings-miljøer. NVE viser også til at NSM har invitert dem til å være med og utarbeide en veileder for industrielle

kontrollsystemer[68], og at det kan være svært verdifullt for etaten å samarbeide med et stort fagmiljø som NSM om å utforme god praksis på dette feltet. NVE har også dialog med leverandører, og leverandører tar iblant kontakt for å høre om NVE mener at løsningene de utvikler, er i tråd med forskriften. NVE påpeker også at tilsyn med IKT-sikkerhet er et ganske ungt tilsynsområde, også for andre etater enn NVE, og at det er nyttig å dele erfaringer med andre myndigheter, for eksempel NSMs samhandlingsarena for sektortilsyn etter sikkerhetsloven. I tillegg deler NVE en plass i det nye nasjonale cybersikkerhetssenteret med KraftCERT, noe som ifølge NVE bidrar til jevnlig informasjonsutveksling.

NVE oppgir i intervju at FoU på IKT-sikkerhetsområdet har økt de siste årene, noe som er i tråd med avdelingens strategi. NVE legger vekt på kontinuerlig utviklingsaktivitet innenfor IKT-sikkerhet for å holde seg oppdatert på den digitale utviklingen i bransjen. Etaten opprettholder IKT-sikkerhetskompetansen ved å ha kontakt med forskningsmiljøer i inn- og utland og ved å gjennomføre egne og delta i andres FoU-prosjekter. NVE har tildelt midler til IKT-sikkerhetsprosjekter i beredskapsseksjonen fra midler som er satt av til FoU-prosjekter og til prioriterte tiltak i NVE i perioden 2017–2020. I 2020 pågår det seks FoU-prosjekter om IKT-sikkerhet. Prosjektene handler om

- forsyningssikkerhet i smartgrids
- tverrfaglig lab for cyberfysisk sikkerhet hos NTNU
- kraftsensitiv informasjon
- sikkerhet i digitale verdikjeder og komponenter i kraftforsyningen
- effektive sikkerhetstiltak for driftskontrollsystemer
- utvikling av cybersikkerhetskompetanse for kraftbransjen

Når det gjelder prioriterte tiltak har beredskapsseksjonen i perioden 2017–2020 blant annet fått midler til et eget prosjekt om kraftsensitiv informasjon sammen med juridisk seksjon, opplæringsprosjektet «CyberSmart» og utvikling av IKT-sikkerhetskurs for bransjen.

I spørreundersøkelsen oppga om lag halvparten av IKT-sikkerhetskoordinatorene som synes det kan være utfordrende å etterleve kravene i regelverket, at en årsak til dette er at det er for lite IKT-kompetanse i selskapet, jf. figur 3. NVE viser i intervju til at de siden 2016 har jobbet systematisk med kompetansetiltak for å øke IKT-sikkerhetskompetansen i bransjen. NVE samarbeider med NTNU CCIS[69] på Gjøvik, som utvikler informasjonssikkerhetskurs for bransjen. NVE har også i samarbeid med Energi Norge, NSM, NTNU, KraftCERT og Elvia arrangert fire kurs for bransjen om grunnsikringskravene i den nye forskriften. I forventningsbrevet til KBO for 2019 går det fram at NVE har styrket samarbeidet med universitetene og bransjeforeningene. Målet er å utvikle FoU-prosjekter og relevant utdanning, inkludert etterutdanning, innenfor IKT-sikkerhet/driftskontrollsikkerhet.

I 2017 tok NVE initiativ til et prosjekt som skulle styrke IKT-sikkerhetskompetansen hos ungdom, Cyber-Smart, og NVE ga ut en rapport om prosjektet i 2019.[70] Prosjektet er omtalt i *Nasjonal strategi for digital sikkerhetskompetanse* (2019). NVE oppgir i intervju at de startet dette prosjektet på eget initiativ fordi de så at det var behov for økt IKT-sikkerhetskompetanse i samfunnet og bransjen, og fikk med seg andre aktører fra akademia og NSM. NVE viser til at denne typen tiltak var omtalt i Lysneutvalgets rapport. Prosjektet skulle blant annet bidra til å heve kunnskapen og interessen for IKT-sikkerhet blant ungdom ved å kurse elever og lærere på ungdomsskoler og videregående skoler. I 2019 avsluttet NVE engasjementet i prosjektet med å overlevere en rapport til justisministeren. I oktober 2020 ansatte NTNU en prosjektleder i deltidsstilling for å videreutvikle prosjektet nasjonalt. NVE er fra høsten 2020 medlem i styringsgruppen for CyberSmart.

NVEs kurs og seminarer om IKT-sikkerhet har ifølge NVE bidratt til å rette oppmerksomheten mot forebyggende sikkerhet og beredskap i energiforsyningen. Etaten har blant annet arrangert energiberedskapskonferanser, arrangert årsmøter for distriktssjefene i kraftforsyningen, deltatt på samlinger med KBO og holdt foredrag. NVE opplyser at konferanser og seminarer i NVE-regi som regel evalueres ved at deltakerne får tilsendt et spørreskjema i etterkant av konferansen og seminaret.

Flere aktører som er intervjuet, gir uttrykk for at de stort sett er fornøyd med NVEs kurs og konferanser om IKT-sikkerhet og beredskap. I spørreundersøkelsen oppga i overkant av 80 prosent av IKT-sikkerhetskoordinatorene at de har deltatt på kurs og seminarer, og av disse svarte om lag 40 prosent at de i stor eller svært stor grad er fornøyd med veiledningen NVE gir på kursene og seminarene, jf. figur 6.

[68] Industrielle kontrollsystem omfatter blant annet driftskontrollsystemer brukt i kraftforsyningen.
[69] Centre for Cyber and Information Security.
[70] NVE (2019) *CyberSmart - educating the future workforce*. NVE-rapport nr. 20/2019.

7 NVEs tilsyn med IKT-sikkerhet i kraftforsyningen

Dette kapitlet beskriver hvordan NVE planlegger, gjennomfører og følger opp tilsyn med IKT-sikkerhet.

7.1 Relevante føringer

- NVE er ansvarlig for å føre kontroll med at bestemmelsene i energiloven og kraftberedskapsforskriften overholdes.
- NVE skal påse at beredskapen i energiforsyningen er god og i tråd med gjeldende krav.
- Risiko- og vesentlighetsvurderinger bør ligge til grunn for NVEs tilsynsvirksomhet.

7.2 Oppsummering

- NVE har gjennomført om lag fem IKT-sikkerhetstilsyn i året i perioden 2014–2019.
- Flere planlagte IKT-sikkerhetstilsyn er blitt utsatt i løpet av undersøkelsesperioden.
- NVE har ikke informasjon om IKT-sikkerheten i selskaper hvor de ikke har ført tilsyn.
- NVE gjennomfører stikkprøvebasert kontroll av internkontrollsystemet til selskapene under IKT-sikkerhetstilsyn.
- NVE har ikke dokumentert at det ligger risikovurderinger til grunn for valg av tema for tilsynene.
- NVE velger i hovedsak ut tilsynsobjekter basert på selskapenes vesentlighet og i mindre grad ut fra informasjon om svakheter i selskapene.

7.3 Planlegging av IKT-sikkerhetstilsyn

7.3.1 Formål og organisering

NVEs tilsyn omfatter både kontroll og reaksjoner. Formålet med tilsynene er å

- kontrollere om regelverk, tillatelser og andre vedtak, inkludert vilkår, etterleves
- korrigere brudd på regelverk, tillatelser og andre vedtak med hensiktsmessige reaksjoner
- sikre at målet med regelverket nås
- vurdere om regelverk, tillatelser og vedtak er hensiktsmessig utformet
- vurdere tilstanden og utviklingen på det aktuelle tilsynsområdet

NVEs tilsyn med IKT-sikkerhet ligger under tilsynsområdet energiforsyningsberedskap og utføres av beredskapsseksjonen. Beredskapsseksjonen har ansvar for å føre tilsyn med reparasjonsberedskap, sikringstiltak av transformatorstasjoner og driftssentraler, generell beredskap, driftskontroll og informasjons-sikkerhet. NVEs tilsyn med IKT-sikkerhet består i hovedsak av tilsyn med driftskontrollsystemer og tilsyn med informasjonssikkerhet. I tillegg omfatter generelle beredskapstilsyn enkelte krav som også er relevante for IKT-sikkerheten, som risikovurderinger, beredskapsplanlegging, internkontrollsystem og beskyttelse av kraftsensitiv informasjon. Tilsyn med informasjonssikkerhet, som ble gjennomført av NVE for første gang i 2019, omhandler i hovedsak kapittel 6 i kraftberedskapsforskriften, mens tilsyn med driftskontrollsystemer omhandler kapittel 7 i tillegg til generelle krav.

Tilsyns- og beredskapsavdelingen koordinerer tilsynsarbeidet i NVE med blant annet felles retningslinjer for kontroll og reaksjoner og felles planlegging av tilsyn. NVE har siden 2008 hatt én gruppe som skal sikre fast forvaltningspraksis og likebehandling ved bruk av reaksjoner, og én gruppe som skal koordinere tilsyn i NVE med standardiserte prosedyrer og diskusjon av tilsynsfaglige spørsmål og tilsynsmetodikk. NVE har utarbeidet felles prosedyrer for kontroll og reaksjonsbruk i etaten og gjennomfører årlige interne kurs i innholdet i prosedyrene. Prosedyrene bygger på NVEs strategi og skal

- legge felles rammer for kontrollaktiviteten
- gi grunnlag for hensiktsmessige valg av reaksjoner og reaksjonsnivå
- bidra til enhetlig praksis i NVE
- sikre kvaliteten i tilsynsarbeidet i NVE gjennom høy faglig og metodisk kompetanse
- sikre intern og ekstern samordning

7.3.2 Planer for tilsynsvirksomheten

NVE utarbeider årlig en felles tilsynsplan for hele virksomheten. Formålet med tilsynsplanen er å sikre at NVEs tilsynsvirksomhet styres på en helhetlig måte, og synliggjøre hva som skal være tema for årets tilsyn. Tilsynsplanen skal konkretisere målene og tiltakene som er fastsatt for de ulike tilsynsområdene i NVEs strategi. I tillegg utarbeider NVE en årlig revisjonsplan med informasjon om alle planlagte tilsyn i NVE for kommende år.

Beredskapsseksjonen utarbeider årlige tilsynsplaner for seksjonen. Disse planene inneholder informasjon om hvilke kriterier seksjonen skal bruke for å velge tilsynsobjekt og tema, en oppsummering av områdeovervåkingen fra året før, et flerårig perspektiv for tilsynsvirksomheten og rutinebeskrivelser for gjennomføring av revisjoner. Beredskapsseksjonen utarbeider også en tilsynsoversikt med oversikt over alle seksjonens tilsyn for kommende år, hvor de enkelte tilsynene er angitt med virksomhet, tema, dato, revisjonslag og revisjonsleder. Tilsynsoversikten brukes ifølge beredskapsseksjonen til planlegging og rapportering av tilsyn i seksjonen og skal oppdateres løpende gjennom året. Tilsynsoversiktene for årene før 2019 inkluderer en sjekkliste med saksbehandlingsoppgaver knyttet til dokumentasjon, oppdatering av interne regneark og tidspunkter for varsling av tilsynsobjekt. Informasjon om gjennomførte tilsyn i disse oversiktene er i hovedsak fylt ut, men for enkelte tilsyn framkommer det ikke om NVE har avsluttet tilsynssaken. Tilsynsoversiktene for 2019 og 2020 er oppdaterte, men inneholder ikke en like detaljert sjekkliste som tidligere år.

7.3.3 Områdeovervåking

I beredskapsseksjonens tilsynsplaner for perioden 2017–2020 står det at tilsyn skal gjennomføres med utgangspunkt i en vurdering av risiko og vesentlighet, og at områdeovervåking skal ligge til grunn for denne vurderingen. Områdeovervåkingen inkluderer resultater fra tidligere tilsyn, oversikt over klassifiserte anlegg, kunnskap om alvorlige hendelser, vurdering av trusler og sårbarheter, resultater fra feil- og avbruddsrapportering (FASIT), innrapportering fra publikum, andre myndigheter eller KBO-enheter om mistanke om forskriftsbrudd samt om det er spesielle forhold som gjelder energiforsyningen til samfunnsviktige funksjoner.

Beredskapsseksjonen har en database med oversikt over alle de om lag 170 KBO-enhetene og kontaktinformasjon til viktige personer i selskapene. NVE har etablert en digital løsning hvor selskapene skal holde selskapets kontaktinformasjon oppdatert. Beredskapsseksjonen har også en database med oversikt over klassifiserte anlegg, inkludert driftskontrollsystemer. KBO-enhetene som har størst betydning for kraftforsyningen, har de høyest klassifiserte driftskontrollsystemene (klasse 3), og disse er underlagt de strengeste kravene i kraftberedskapsforskriften. Hvilken klasse – og dermed hvilke sikringskrav et driftskontrollsystem er underlagt – går fram av kraftberedskapsforskriften. NVE har begynt på arbeidet med å skaffe seg oversikt over hvilken klasse alle driftskontrollsystemene til KBO-enhetene tilhører. NVE oppgir at denne oversikten ikke er ferdigstilt, og at dette arbeidet er blitt nedprioritert. NVE mener at mangler i oversikten i hovedsak gjelder de minst vesentlige systemene i klasse 1.

I NVEs overordnede risikovurderinger for 2017 og 2018 skriver etaten at det er en risiko for at den ikke har tilstrekkelig grunnlag for å vurdere status og risiko i beredskapen og forsyningssikkerheten. Et av de nye tiltakene som skulle bøte på dette, gikk ut på å øke kvaliteten i grunnlagsdataene på områdene forebyggende sikkerhet og beredskap. Ifølge NVE var kvaliteten på dataene akseptabel, men datagrunnlaget kunne fortsatt videreutvikles og utnyttes mer effektivt for å gjennomføre tilsyn basert på risiko og vesentlighet, og for å ha oversikt over tilstanden og risikoen og sårbarheten i energiforsyningen. I den overordnede risikovurderingen for 2020 påpekte NVE at tilgang til relevante data av god kvalitet er avgjørende for NVEs tilsyn og for håndteringsevnen ved strømbrudd.

7.3.4 Valg av tema og omfang av IKT-sikkerhetstilsyn

I NVEs overordnede tilsynsplaner for 2018–2020 står det at utvalget av tema for de enkelte fagområdene er basert på blant annet tildelingsbrev for 2019, erfaringer og interne prioriteringer. I beredskapsseksjonens tilsynsplaner for perioden 2017–2020 står det at «tilsynet kombineres til et antall tema som gir en rasjonell gjennomføring av tilsynene. Dette vil gi god dekning i valg av tilsynsobjekter og nødvendig bredde i omfanget av kontroll.»

I beredskapsseksjonens tilsynsplaner er det angitt hvor mange tilsyn som skal gjennomføres innenfor de ulike temaene hvert år. Det er om lag 170 selskaper i KBO. I perioden 2017–2019 gjennomførte beredskapsseksjonen tretten tilsyn med driftskontrollsystemer og to tilsyn med informasjonssikkerhet. Nivået på om lag

fem IKT-sikkerhetstilsyn i året har vært stabilt i NVE siden 2014. Totalt gjennomførte beredskapsseksjonen 145 tilsyn i perioden. Flesteparten av tilsynene i seksjonen er generelle beredskapstilsyn og tilsyn med sikringstiltak og er rettet mot fysisk sikring. Både det årlige antallet tilsyn og fordelingen av tilsynene på IKT-sikkerhet og øvrige tema innad i seksjonen var stabile i perioden. Begrunnelsen for valg av tema og antall tilsyn innenfor hvert tema er ikke dokumentert, verken i NVEs overordnede tilsynsplaner eller beredskaps-seksjonens tilsynsplaner. NVE oppgir at det har vært endringer i hvor mange tilsyn NVE gjennomfører med ulike tema, men at slike endringer ofte tar tid. Ifølge NVE tilpasses aktiviteten for hvert tilsynstema etter den generelle og spesifikke kompetansen som etaten til enhver tid har tilgjengelig. NVE påpeker at de ansattes fagkompetanse påvirker hvor stor fleksibilitet NVE har til å endre omfanget av tilsynsaktiviteten innenfor ulike tema.

I perioden utsatte beredskapsseksjonen tilsyn med IKT-sikkerhet i fem selskaper. Ett av disse tilsynene gjelder KraftCERT, og dette har blitt utsatt flere ganger. Av de øvrige fire utsatte tilsynene ble tre gjennomført året etter at det var planlagt, mens ett foreløpig ikke er blitt gjennomført. Beredskapsseksjonen utsatte IKT-sikkerhetstilsyn oftere enn tilsyn med andre tema i perioden 2017–2019. NVE påpeker at omfanget av IKT-sikkerhetstilsyn må ses i sammenheng med andre aktiviteter, som arbeidet med revisjonen av kraftberedskapsforskriften og veilederen til denne. At tilsyn ikke har blitt gjennomført som planlagt, skyldes ifølge NVE også sykdom blant nøkkelpersonell. IKT-sikkerhetstilsyn krever spesialisert kompetanse, og særlig de senere årenes arbeid med det nye regelverket og tilhørende veiledning har krevd mye ressurser fra ansatte med kompetanse på IKT-sikkerhet. NVE viser også mer generelt til at bransjen bør få opplæring når det innføres nytt regelverk, og at det nye regelverket bør få virke en stund før NVE fører tilsyn med etterlevelsen. Dette er bakgrunnen for at det ble gjennomført få tilsyn med informasjonssikkerhet i 2019.

7.3.5 Valg av tilsynsobjekter (selskaper)

I NVEs overordnede tilsynsplaner for 2018–2020 står det at tilsynsobjektene for hvert enkelt tilsynsområde skal velges ut med henblikk på kriteriene risiko, vesentlighet, erfaringer, geografisk spredning og spredning i foretakets størrelse og type. NVE har ikke dokumentert hvilke kriterier som ligger til grunn for de konkrete valgene av tilsynsobjekter i perioden 2017–2020, verken i de overordnede tilsynsplanene eller i beredskaps-seksjonens tilsynsplaner for samme periode.

NVE oppgir at tilsynsobjektene for IKT-sikkerhetstilsynene i perioden 2017–2019 ble valgt ut med bakgrunn i vesentlighet og samlet tilsynsfrekvens. Når det gjelder tilsynsfrekvens, valgte NVE store selskaper som det var lenge siden det hadde blitt ført tilsyn med. I årene fram til 2019 gjennomførte NVE i hovedsak IKT-sikkerhetstilsyn med store selskaper. NVE gjennomførte tilsyn med om lag halvparten av selskapene med de viktigste driftskontrollsystemene (klasse 3) i perioden 2017–2019. Etter at NVE fikk innspill fra noen av de store selskapene om at de også burde føre tilsyn med mindre selskaper, har NVE fra 2019 også valgt ut noen små selskaper for tilsyn. NVE begrunner dette med at også svikt i de mindre selskapenes IKT-systemer kan få konsekvenser for kraftforsyningen. NVE viser til at IKT-sikkerhetstilsynene ikke gjennom-føres isolert, men er en del av en helhet med flere andre tilsynsområder for å oppnå sikkerhet og beredskap i kraftforsyningen. NVE oppgir i intervju at de ulike seksjonene i tilsyns- og beredskapsavdelingen koordinerer oversiktene over hvilke selskaper og tema det skal føres tilsyn med. Når selskaper velges ut, tar beredskapsseksjonen også hensyn til eventuelle andre tilsyn som gjennomføres i selskapene, slik at tilsynene blir fordelt på en rimelig måte som gjør at det ikke blir for stort trykk på enkeltselskaper i en periode. NVE samarbeider også med Direktoratet for samfunnssikkerhet og beredskap om å koordinere tilsyn med tilgrensende tematikk, noe som også kan påvirke valget av tilsynsobjekter.

Hvilke selskaper som blir valgt med utgangspunkt i disse kriteriene, avgjøres ifølge NVE etter en total-vurdering og baseres normalt ikke på observert risiko om svakheter i selskapene. NVE bruker i liten grad informasjon fra aktiviteter og kilder i områdeovervåkingen til å foreta et risikobasert valg av tilsynsobjekter. Beredskapsseksjonen har som regel ikke konkret informasjon om sikkerhetstilstanden eller IKT-hendelser i selskapene de velger ut som tilsynsobjekter, men legger ofte til grunn digital risiko som forekommer i alle selskaper av en viss type og størrelse. Små selskaper har ofte mangler i IKT-sikkerheten (både styrings-system, internkontrollsystem og konkrete tiltak) fordi de har færre ressurser og mindre kompetanse på IKT-sikkerhet, noe som gjør at de er særlig utsatt for uønskede IKT-hendelser. NVE påpeker imidlertid at konsekvensene ved svikt i disse selskapene er lavere. Store selskaper bruker gjennomgående flere ressurser på IKT-sikkerhet, men har samtidig en større angrepsflate og høyere kompleksitet i systemene, noe som også øker den samlede risikoen for uønskede IKT-hendelser. I noen tilfeller der et selskap har vært utsatt for hendelser, eller der store endringer i selskapet øker risikoen for regelbrudd (som omorganisering),

har imidlertid tilsynsteamet vurdert å føre selskapet opp på neste års tilsynsliste. Ifølge NVE er risikoperspektivet dermed ikke helt utelatt i utvelgelsen.

I NVEs tilsynsplan for 2019 framheves det at områdeovervåkingen i 2020 bør utvides, for eksempel gjennom en spørreundersøkelse om utvalgte tema fra kraftberedskapsforskriften. Også i tilsynsplanen for 2020 står det at spørreundersøkelser og andre undersøkelser bør inngå i en mer omfattende områdeovervåking i perioden 2022–2025. Det står også at områdeovervåkingen bør omfatte skriftlig kontroll og andre undersøkelser. NVE oppgir i intervju at beredskapsseksjonen ikke har kunnet prioritere dette på grunn av situasjonen med covid-19, som seksjonen har ansvar for å håndtere som beredskapsmyndighet i kraftforsyningen. I beredskapsseksjonens tilsynsplan for 2020 står det at spørreundersøkelser kan være effektivt for å få informasjon om mange KBO-enheter. Spørsmålene bør ta utgangspunkt i resultater fra områdeovervåkingen, og resultatene bør inngå i ny områdeovervåking. Det står videre at spørre-undersøkelser krever enkle spørsmål og er en type tilsyn som både er ressurskrevende og krever spesiell oppmerksomhet. Beredskapsseksjonen trekker fram at et viktig formål med skriftlige spørreundersøkelser er å gjøre KBO-enhetene mer bevisst på viktige forhold. I perioden 2017–2019 gjennomførte NVE flere spørreundersøkelser med relevans for IKT-sikkerheten i kraftforsyningen som en del av FoU-prosjekter. I 2018 fikk KBO-enhetene spørsmål om rutinene for varsling og rapportering til NVE og kraftforsyningens distriktssjefer ved ulike typer hendelser, og i 2019 fikk KBO-enhetene og NVEs egne ansatte spørsmål om behandlingen av kraftsensitiv informasjon. Som en del av utrullingen av AMS har NVE også bedt om jevnlig rapportering fra nettselskapene, blant annet om hvordan de har planlagt å bruke brytefunksjonen i AMS.[71]

7.3.6 Valg av kontrollmetode

I NVEs prosedyrer står det at kontroll er aktiviteter som har som mål å undersøke etterlevelsen av gitte krav.

- Kontroll av virksomheten kan gjennomføres i planleggings-, utbyggings-, drifts- og avviklingsfasen.
- Kontrollen kan gjelde hele eller deler av virksomheten, anlegg, bygninger eller produkter.
- Kontrollen kan rette seg mot overordnede systemer, spesifikke krav eller konkrete problemstillinger.
- Kontrollen kan utføres på eget initiativ eller på oppfordring fra andre.
- Flere kontrollmetoder kan kombineres.

Videre står det at valg av kontrollmetode må vurderes i hvert enkelt tilfelle, og at det er hensiktsmessig at denne konkretiseringen går fram av seksjonens årlige tilsynsplan for hvert tilsynsområde. Metodene som kan benyttes i NVE, er som følger:

- *Revisjon* (omtales som *tilsyn* i denne rapporten) er en uavhengig, systematisk og dokumentert gjennomgang av en virksomhets anlegg, bygninger, produkter, systemer eller dokumenter.
- *Inspeksjon* er en uavhengig og dokumentert fysisk kontroll av anlegg, bygninger og produkter for å kontrollere om gitte krav etterleves. Inspeksjon kan blant annet benyttes for å verifisere opplysninger gitt ved revisjon.
- *Dokumentkontroll* er å innhente og gjennomgå dokumenter (bilder og skriftlig materiale uansett lagringsmedium). Innhenting omfatter både innsendt informasjon og informasjon som er hentet inn fra åpne kilder.
- *Spørreundersøkelse* er en skriftlig innhenting av informasjon hos flere virksomheter samtidig gjennom et sett av likelydende spørsmål.
- *Innrapportering* er kontroll av informasjon som kommer fram gjennom innrapporteringsordninger etter regelverk eller vedtak.
- *Laboratoriekontroll* er fysisk testing av produkter utført av andre enn NVE.

NVE oppgir at det er kontrollmetoden *revisjon* (tilsyn) som er blitt brukt ved kontroll av selskapenes IKT-sikkerhet i perioden 2017–2019. Det går ikke fram av NVEs overordnede tilsynsplaner eller av beredskaps-seksjonens tilsynsplaner hvilke vurderinger som ligger til grunn for valg av tilsynsmetodikk på dette området. NVE har vurdert det slik at revisjon er en egnet metode for kontroll siden regelverket stiller krav om at selskapene skal ha internkontroll. Kontrollmetodene inspeksjon og innrapportering brukes i liten grad i beredskapsseksjonen og har ikke blitt benyttet i forbindelse med krav til IKT-sikkerhet. Inspeksjoner gjennomføres som oftest under oppføring og endring av anlegg, som er mindre aktuelt for beredskaps-seksjonen siden seksjonens revisjonsobjekter er virksomheter i drift. Metoden innrapportering brukes blant

[71] NVE (2018) *Smarte målarar. NVE-*rapport nr. 5/2018.

annet i seksjon for damsikkerhet som mottar årlig innrapportering fra dameiere i tråd med damsikkerhetsforskriften § 2-10. Dameierne må blant annet rapportere inn om de har et internkontrollsystem, en beredskapsplan og gjennomført en øvelse, og også andre deler av NVE krever omfattende årlig rapportering av tekniske og økonomiske data.

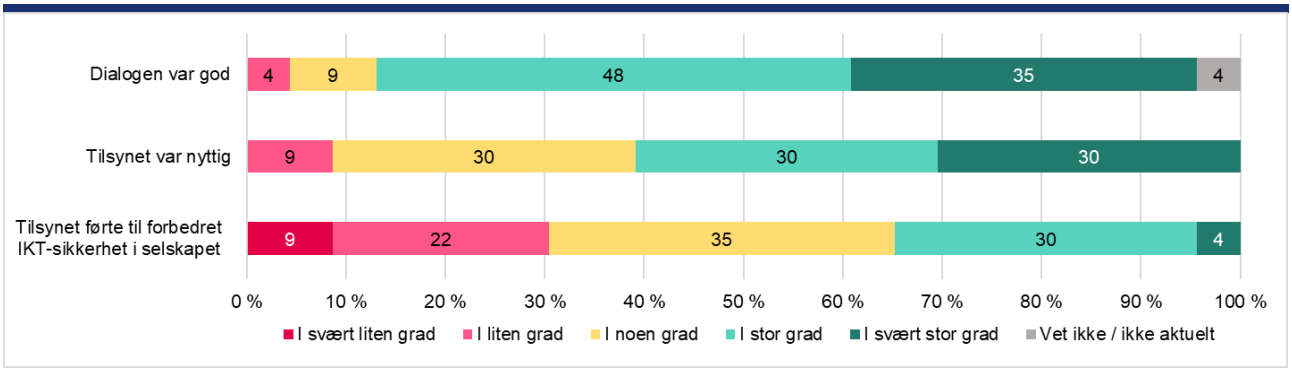
Flere tilsynsmyndigheter stiller krav til at selskaper skal innrapportere informasjon som er relevant for å vurdere IKT-sikkerheten. Finanstilsynet ber finansforetakene årlig innrapportere egenvurderinger av foretakenes sårbarhet for trusler og spør blant annet om foretakenes organisering av sikkerhetsarbeidet, prosesser for risikoanalyser, sikkerhetstester og loggføring i systemer.[72] På bakgrunn av denne egenrapporteringen og andre kilder utformer Finanstilsynet en årlig risiko- og sårbarhetsanalyse, hvor det vurderer risikobildet for IKT-sikkerheten i finanssektoren. NSM oppgir i intervju at de ber virksomhetene som er underlagt sikkerhetsloven, årlig sende inn en egenevaluering av hvordan de innfrir kravene i sikkerhetsloven. Også Energistyrelsen i Danmark oppgir at de i forkant av tilsyn med selskaper i elektrisitetssektoren, ber selskapet sende inn en egenevaluering av hvordan de håndterer ulike krav.

7.4 Gjennomføring av IKT-sikkerhetstilsyn

7.4.1 Selskapenes opplevelse av IKT-sikkerhetstilsyn

Alle selskapene vi har intervjuet som hadde tilsyn med IKT-sikkerheten i perioden 2017–2019, har gitt uttrykk for at tilsynet har vært positivt og nyttig for selskapet. Flere brukte mye tid på å forberede tilsynet. Forberedelsene gikk i hovedsak ut på å oppdatere maler og annen dokumentasjon og skaffe seg bedre oversikt over IKT-sikkerheten i selskapets systemer. Selskapene hadde også dialog med IKT-leverandører for å sjekke at ting var i orden. Selskapene oppgir at det i liten grad var behov for å gjøre endringer i IKT-systemene i forbindelse med tilsynet, men at enkelte sikkerhetstiltak har blitt forbedret på grunn av tilsynet, for eksempel når det gjelder tilgangsstyring til IKT-systemer. Et større kraftselskap oppgir at de har brukt tilsynet som en anledning til å få gjort nødvendige oppdateringer og til å øke ledelsens oppmerksomhet på IKT-sikkerhet. Selskapet mener at tilsynet fra NVE har vært viktig for å øke forståelsen for sikkerhetsområdet internt, særlig i ledelsen. NC-Spectrum AS' og KraftCERTs hovedinntrykk er også at selskapene hovedsakelig opplever IKT-tilsynene som positive og nyttige. Ifølge KraftCERT ser det ut til at resultater fra tilsyn kan brukes som brekkstang for å få gjennom investeringer i økt IKT-sikkerhet.

Figur 8 IKT-sikkerhetskoordinatorenes svar på hvordan de opplevde NVEs tilsyn som omhandlet IKT-sikkerhet (N = 23)



I vår spørreundersøkelse svarte over 80 prosent av IKT-sikkerhetskoordinatorene som har deltatt på IKT-sikkerhetstilsyn i løpet av de siste tre årene, at de i stor eller svært stor grad opplevde at dialogen i tilsynet var god. Flertallet opplevde også tilsynet som nyttig. Om lag en tredel svarte at tilsynet i liten eller svært liten grad førte til forbedret IKT-sikkerhet i selskapet.

Flere selskaper opplever at NVE har endret seg når det gjelder tonen og stemningen under tilsynsbesøket, som nå oppleves som god. Selskapene oppgir i intervju at de har en klar oppfatning av at begge parter har hatt samme fokus og mål for tilsynet, nemlig å bidra til forbedring. Selskapene opplever at dialogen med NVE var god både før og under tilsynet. Selskapene synes at NVE ga konstruktive tilbakemeldinger og så ut

[72] Finanstilsynet (2020) *Risiko- og sårbarhetsanalyse (ROS) 2020.*

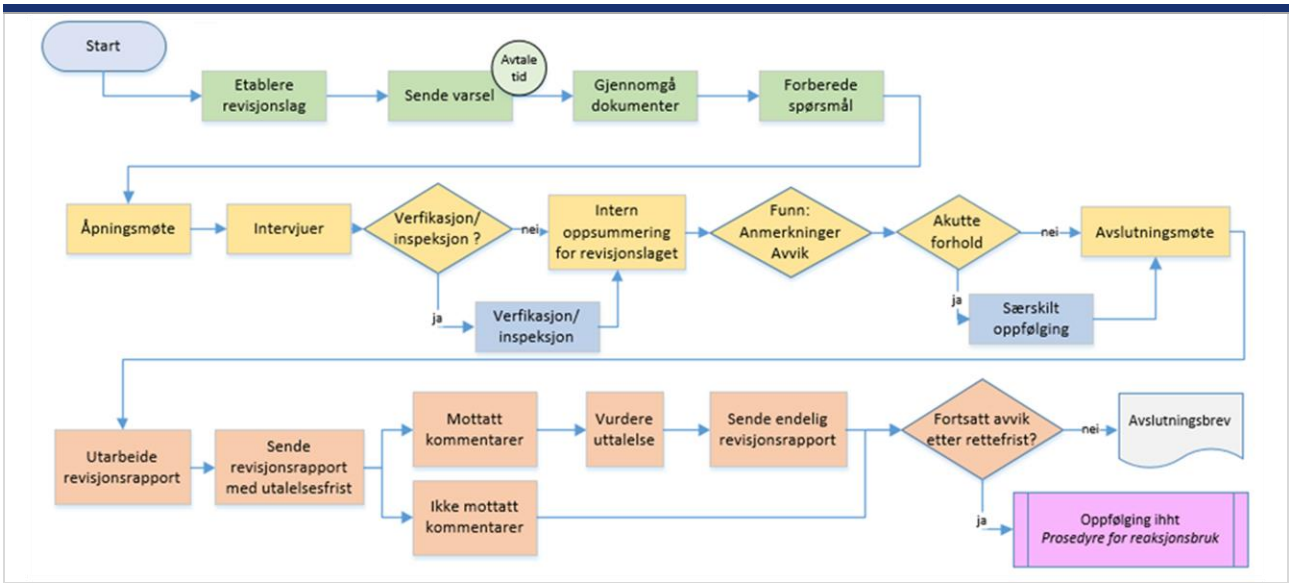
til å forstå bransjens utfordringer. Nettalliansen AS mener også at NVEs tilsyn etter kraftberedskaps-forskriften er i en positiv utvikling, og at det har skjedd en stor forbedring fra tilsyn lenger tilbake i tid, da det var større avviksfokus og mindre læringsfokus. Selskapene mener tilsynsrapporten gjenspeilte tilsynsbesøket på en god måte, og at avvikene som NVE ga, var riktige og forståelige.

7.4.2 Rutiner og praksis ved gjennomføring av IKT-sikkerhetstilsyn

Gjennom tilsyn skal NVE kontrollere om kravene til IKT-sikkerhet i energiloven og kraftberedskapsforskriften etterleves, og gi avvik ved brudd på kravene. NVE kan også gi anmerkning, som er en påpekning av forhold med forbedringsmulighet eller forhold som bør vurderes nærmere av virksomheten, men som ikke er brudd på gitte krav. Når avvik er avdekket, kan NVE benytte ulike reaksjonsformer. NVE kan fatte vedtak om tilbaketrekking av tillatelse, overtredelsesgebyr, tvangsmulkt, retting, stans og omsetningsforbud. Når NVE avdekker avvik i tilsyn med IKT-sikkerhet, benytter de i all hovedsak reaksjonen vedtak om retting. Tilsyns-objektet plikter da å rette opp avvikene. NVE kan også anmelde en overtredelse eller ilegge overtredelses-gebyr for overtredelser av et forbud eller påbud fastsatt i lov, forskrift eller enkeltvedtak. I prosedyrene står det at det ved tilsyn med sikkerhet i energiforsyningen kan være særlig aktuelt å bruke overtredelsesgebyr for blant annet manglende beredskapsplan, mangelfulle risikovurderinger og manglende sikkerhet rundt IKT-systemer. NVE avdekket åtte avvik i selskapers risikovurderinger og beredskapsplanlegging i perioden 2017–2019. NVE benyttet ikke andre reaksjoner enn vedtak om retting for disse avvikene. NVE varslet imidlertid om overtredelsesgebyr i tre tilfeller i perioden 2017–2019, som følge av at uvedkommende ble sluppet inn i selskapenes driftssentral. Da NVE vurderte disse sakene, la de vekt på at regelverksbruddet er irreversibelt og dermed ikke kan rettes i ettertid. To av disse sakene kommer ikke fram i NVEs reaksjons-register, selv om alle varsler og vedtak om reaksjoner skal registreres.[73] NVE benyttet ikke tvangsmulkt som reaksjon på avvik i perioden, men varslet tvangsmulkt etter et tilsyn med generell beredskap, hvor tilsynsobjektet ikke hadde lukket et avvik ved kravet til beredskapsplanlegging i henhold til fristen.

Ifølge NVEs prosedyrer er tilsyn en grundig gjennomgang av dokumentasjon, som gjennomføres hos virksomheten etter et fastsatt mønster (figur 9). NVEs prosedyrer inneholder rutinebeskrivelser av de ulike stegene i prosessen.

Figur 9 Flytdiagram for gjennomføring av tilsyn



En saksgjennomgang av IKT-sikkerhetstilsyn i perioden 2017–2019 viser at NVE i hovedsak følger interne prosedyrer for tilsynene. Tilsynsobjektene varsles innen rimelig tid før tilsynet, tilsynsrapporter godkjennes av seksjonsleder, og tilsynsobjektene får som regel en rimelig uttalelsesfrist. NVE mottar i all hovedsak en bekreftelse på at tilsynsobjektet har lukket avdekkede avvik sammen med en beskrivelse av hvordan det er gjort. NVE har avsluttet to tilsynssaker der tilsynsobjektene har bekreftet at avvikene var lukket uten å beskrive hvordan. Ved flere tilsyn hvor tilsynsobjektet ikke har lukket avvik innen fristen, har NVE imidlertid

[73] NVE (2019) *Oppsummering av uønskede hendelser 2018 i energiforsyningen.* Faktaark nr. 4/2019.

brukt lang tid på å purre på selskapet. Ett av de femten IKT-sikkerhetstilsynene NVE gjennomførte i perioden 2017–2019, har ikke blitt lukket, og den sist lagrede dokumentasjonen på saken, hvor NVE ber selskapet oppgi om avviket er lukket, er fra september 2018. Saksgjennomgangen viser videre at det varierer om NVE dokumenterer avvik i interne oversikter. I NVEs nye applikasjon for gjennomføring av tilsyn (se nærmere omtale i punkt 7.6) er det enklere å hente ut informasjon om avvik siden avvikene som gis i tilsyn, automatisk registreres i applikasjonen når man utformer tilsynsrapport. Ifølge NVE kan det være aktuelt å eksportere informasjon fra applikasjonen for å analysere hyppig forekommende avvik og lignende.

Dokumentasjon ved lukking av avvik

Tilsynsrapportene er standardiserte og inneholder en beskrivelse av hvilket krav som er brutt, NVEs dokumentasjon av avviket, en beskrivelse av hvordan avviket skal lukkes, og fristen tilsynsobjektet har for å lukke avviket. NVEs dokumentasjon av avviket består som oftest av at selskapet i tilsynet selv har oppgitt at de ikke oppfyller et krav eller mangler dokumentasjon som viser at kravet etterleves. NVEs prosedyrer stiller ikke krav til at virksomheten skal dokumentere hvordan avvik er lukket. NVE oppgir i intervju at hvis avviket gjelder dokumentasjon av selskapets systemer, for eksempel mangler i en prosedyre eller risikovurdering, lukker NVE som regel avviket hvis selskapet bekrefter at dette er på plass, men i enkelte tilfeller kan det innhentes nye eller oppdaterte dokumenteter. NVE oppgir at de sjelden innhenter dokumenter i etterkant av tilsynet, men oftest ber om en forklaring på hvordan avviket er lukket.

7.4.3 NVEs tilsynsmetodikk ved IKT-sikkerhetstilsyn

NVE oppgir i intervju at det ligger et internkontrollperspektiv til grunn for tilsynsmetodikken, det vil si at NVE kontrollerer om selskapet har systemer for å sikre at de etterlever kravene i kraftberedskapsforskriften. Beredskapsseksjonen har utarbeidet standardiserte spørreskjemaer for de ulike tilsynene de gjennomfører etter kraftberedskapsforskriften. Vårt inntrykk etter intervjuer med Finanstilsynet, NSM og tilsyns-myndighetene for kraftforsyningen i Danmark og Sverige er at NVE i hovedsak bruker samme tilsynsmetode som de andre tilsynsmyndighetene.

I rapporten *Bruk av digitale verktøy i tilsyn med IKT-sikkerhet* som er utarbeidet for NVE i 2020, står det at dokumentkontroll og intervju gjerne gir et godt bilde av virksomhetens rutiner og hvordan IKT-sikkerheten burde være, men ikke av hvordan tilstanden faktisk er.[74] NVE bruker i stor grad den samme metodikken når de gjennomfører IKT-sikkerhetstilsyn som de gjorde for over ti år siden.[75]

I caseundersøkelsen har vi ved hjelp av utvalgte tester og undersøkelser sett nærmere på hvordan tre selskaper arbeider med IKT-sikkerhet. NVE førte tilsyn med IKT-sikkerhet i alle de tre selskapene i 2019 eller 2020. I tillegg har vi vært observatør ved fire av NVEs IKT-sikkerhetstilsyn i samme periode. I case-undersøkelsen fant vi flere svakheter og mangler som ikke ble avdekket i NVEs tilsyn. Disse gjaldt både gjennomføringen av risikoanalyser, evalueringer og sikkerhetsrevisjoner og grunnleggende sikkerhetstiltak (se punkt 4.4). Det ble avdekket flere svakheter og mangler som selskapene selv ikke var klar over, og som selskapenes internkontrollsystemer ikke hadde fanget opp. Noen av dem ble avdekket gjennom de samme metodene som NVE bruker, som dokumentanalyse, intervjuer og inspeksjon/observasjon. Vi gjennomførte også analyser og tester for å kontrollere selskapenes praksis og sikkerhetstiltak på utvalgte områder.

Hvorvidt beredskapsseksjonen kunne ha endret tilsynsmetodikken fra å sjekke at selskapene har et internkontrollsystem, til å undersøke hvordan IKT-sikkerheten faktisk er hos selskapene, er ifølge NVE et ressursspørsmål. NVE regner i gjennomsnitt to ukeverk på ett tilsyn, og hvert tilsyn gjennomføres av to ansatte. NVE oppgir at de to som gjennomfører tilsynet, bruker om lag tre dagsverk hver på selve dokumentgjennomgangen og intervjuet med selskapet. NVE oppgir at ressursbruken på hvert enkelt tilsyn har vært et bevisst valg for å nå flere virksomheter med tilsynsvirksomheten. NVE trekker imidlertid fram at det med tanke på de nye kravene som ble innført i 2019, kan være hensiktsmessig å snevre inn antall områder som tas opp i ett og samme tilsyn, for eksempel å gjennomføre tilsyn som bare går i dybden på leverandøroppfølgningen i selskapet. Ved å gå mer i dybden på færre områder kan etaten få mer informasjon om disse områdene, men det må veies opp mot at de da får rettet oppmerksomheten mot færre områder. Beredskapsseksjonen har også vurdert om det kan være hensiktsmessig å gjøre tematisk bredere eller mer grundige tilsyn av utvalgte selskaper enn i dag og for eksempel kontrollere flere tema i kraftberedskapsforskriften samtidig. I beredskapsseksjonens tilsynsplan for 2020 står det at det på bakgrunn

[74] NVE (2020) *Bruk av digitale verktøy i tilsyn med IKT-sikkerhet.* NVE-rapport nr. 38/2020.
[75] Forsvarets forskningsinstitutt / Hagen, J. og Fridheim, H. (2007) *Beskyttelse av samfunnet 5: Sårbarhet i kritiske IKT-systemer - sluttrapport.* FFI-rapport nr. 2007/01204.

av vurderinger av risiko og vesentlighet kan vurderes å gå i dybden hos de største KBO-enhetene. Beredskapsseksjonen foreslår at det gjennomføres et større tilsyn med selskapets overordnede planverk, stedlig kontroll av et anlegg, tilsyn med datasikkerhet, inkludert driftskontrollsystemet, og for eksempel et eget tilsyn med reparasjonsberedskap og vedlikehold. På denne måten blir det mulig å se om det er en sammenheng mellom KBO-enhetens rutiner og systemer for å etterleve kravene i forskriften og den faktiske etterlevelsen. I et notat til Olje- og energidepartementet fra 2016 skriver NVE at inntrengingstester som tester om systemer er robuste nok, kan supplere tilsynsvirksomheten til NVE.

NVE gjennomførte i 2019 et FoU-prosjekt som skulle bidra til å gi konsistente metoder for å avdekke ubevisst deling av kraftsensitiv informasjon og forbedre NVEs argumentasjon overfor selskaper som har brutt krav om å beskytte kraftsensitiv informasjon. NVE skrev i prosjektsøknaden at de trenger en større verktøykasse, og at dagens tilsynsmetodikk i liten grad gjør det mulig å kartlegge ubevisst informasjons-lekkasje. NVE har også tatt initiativ til et studentdrevet prosjekt som kartlegger enkelte andre tilsynsmyndigheters og kontrollorganers bruk av digitale verktøy i tilsyn.[76]

NVE oppgir at omfanget av dokumentasjonen beredskapsseksjonen ber tilsynsobjektet oversende i forkant av tilsyn, begrenses både av kapasiteten ansatte i beredskapsseksjonen har til å gå gjennom dokumentasjonen, og av risikoen for utilsiktede lekkasjer ved håndtering av kraftsensitiv informasjon. Ifølge NVE kan all informasjon som er koblet til internett, potensielt lekke, og beredskapsseksjonen gjør derfor en vurdering av hvilke dokumenter det er nødvendig å hente inn. Seksjonen kunne for eksempel hentet inn teknisk informasjon fra selskapene for å kontrollere hvordan de administrerer brukere og brukerrettigheter, men gjør ikke dette på grunn av informasjonens sensitivitet og risiko for å lekke informasjon utilsiktet. Så langt er NVEs vurdering at resultatet av en mer omfattende dokumentgjennomgang før tilsynet ikke ville stått i forhold til den ekstra arbeidsinnsatsen det ville kreve.

7.5 Rapportering og evaluering av IKT-sikkerhetstilsyn

7.5.1 Rapportering

Beredskapsseksjonen rapporterer om tilsynsvirksomheten for foregående år i den årlige tilsynsplanen. I tilsynsplanen for 2020 skriver beredskapsseksjonen at det til tross for at det i flere år har blitt ført tilsyn med blant annet virksomhetenes risikovurderinger (kraftberedskapsforskriften § 2-3) og beredskapsplaner (kraftberedskapsforskriften § 2-4), er vanskelig å si om tilstanden er vesentlig forbedret.

For hvert tilsyn opprettes det en egen sak i NVEs arkivsystem, hvor også tilsynsrapportene lagres. NVE samler ikke informasjonen fra de ulike tilsynene til interne analyseformål og som en del av område-overvåkingen. Ifølge NVE kan data i den nye applikasjonen brukes til å lage rapporter om tilsynene til dette formålet, men dette har foreløpig ikke vært prioritert i utviklingen av det nye systemet.

I prosedyrene står det at det skal legges vekt på å synliggjøre NVEs tilsynsvirksomhet og funn og på den måten øke effekten av tilsynsvirksomheten. Videre står det at revisjonsrapporter er offentlige med mindre de inneholder taushetsbelagte opplysninger, og at revisjonsrapporter uten taushetsbelagte opplysninger skal legges ut på NVEs nettsted. NVE offentliggjør ikke rapporter fra tilsyn med driftskontrollsystemer og informasjonssikkerhet. Dette skyldes ifølge NVE risikoen for å avsløre sårbarheter ved kraftsystemet. NVE mener at etatens seminarer og publikasjoner om avvik, hendelser og sårbarheter og det årlige forventnings-brevet til KBO-enhetene gir selskaper, leverandører, myndigheter og allmennheten nok informasjon om hva som blir avdekket i tilsyn med kraftforsyningen.

7.5.2 Evaluering

NVE oppgir at hvert enkelt gjennomførte IKT-sikkerhetstilsyn ikke evalueres systematisk internt i NVE eller ved hjelp av brukerevalueringer fra tilsynsobjektet. NVE oppgir at antall tilsyn tilsier at det uansett hadde blitt en lite grundig evaluering. Imidlertid diskuterer tilsynsteamet ofte hvordan ting fungerte, i etterkant av tilsynet, og disse diskusjonene kan ha en korrigerende funksjon for framtidige tilsyn. NVE har ved flere anledninger invitert selskaper som har hatt tilsyn, til å dele sine opplevelser av tilsynet på forskjellige konferanser. Hvis det under et tilsyn viser seg at tilsynspersonellet tolker regelverket ulikt, vil tilsynsteamet

[76] NVE (2020). *Bruk av digitale verktøy i tilsyn med IKT-sikkerhet.* NVE-rapport nr. 38/2020.

diskutere og evaluere dette i etterkant, men at dette blir gjort, og hva som er konklusjonen, blir normalt ikke dokumentert.

7.6 IKT-systemer for IKT-sikkerhetstilsyn

Riksrevisjonen har tidligere påpekt at NVE mangler en felles systemløsning for å sikre nødvendig styringsinformasjon for tilsynsvirksomheten, at etaten benytter grunnlagsdatabaser som ikke har tilfredsstillende kvalitet, og at det er svakheter ved dokumentasjon i tilsynsprosessen, spesielt i planleggingen av tilsyn og i områdeovervåkingen.

I årene fram til 2020 har beredskapsseksjonen i hovedsak benyttet tilsynsoversikten til planlegging, oppfølging og intern rapportering av tilsyn. NVE oppgir at oversikten skal holdes oppdatert, og at en av de ansatte i seksjonen har hatt ansvar for å følge opp at beredskapsseksjonens tilsynsoversikt blir fylt ut, og at frister blir overholdt. Planlagte tilsyn har også blitt lagret i NVEs overordnede tilsynsplan i begynnelsen av året med tanke på å koordinere ulike tilsynsområder. Dokumentasjonen og korrespondansen for hvert enkelt tilsyn har blitt lagret i arkiv. I perioden 2017–2019 fylte beredskapsseksjonen ut informasjon om hvilke avvik og eventuelle overtredelsesgebyr som ble gitt til hvilke selskaper, i flere regneark, som NVEs reaksjons-register og fram til og med 2018 i et eget regneark kalt «Oppsummering funn».

Fra 2020 har beredskapsseksjonen tatt i bruk NVEs nyutviklede applikasjon for saksbehandling av tilsyn. Etter NVEs oppfatning vil applikasjonen gi systemløsningen som tidligere er etterspurt av Riksrevisjonen. Tilsynspersonellet bruker applikasjonen i hele tilsynsprosessen – fra varsling om tilsyn til lukking av avvik og bruk av reaksjonsmidler. Dette ble i NVE tidligere gjort ved å fylle ut maler og sende brev fra arkiv. I applikasjonen flettes informasjonen som oppgis av saksbehandleren, inn i NVEs standardiserte maler, og dokumentene kan sendes fra applikasjonen til tilsynsobjektet eller til NVEs arkiv for intern godkjenning. For hver tilsynssak finnes det en oversikt over tilsynets status, avvik og anmerkninger, kontaktpersoner og referanser til dokumentasjon som er arkivert i forbindelse med tilsynet. Verktøyet gir oversikt over alle tilsyn i NVE og kan blant annet sorteres etter parametere som type tilsyn, ansvarlig seksjon, tilsynsobjekt og saksbehandlingsstatus. NVE oppgir at den nye applikasjonen vil forenkle saksbehandlernes planlegging og gjennomføring av tilsyn og oppfølging av avvik ved at den automatisk henter standardtekst/informasjon, gjenbruker relevant informasjon, produserer brev og gir påminnelser ved frister. Dette vil ifølge NVE bidra til å sikre avviksoppfølgingen.

NVEs nye applikasjon for saksbehandling av tilsyn vil inntil videre ikke føre til endringer i bruken av de manuelt utfylte oversiktene/regnearkene i planleggingen av tilsyn. NVE forventer at data fra applikasjonen vil kunne inngå i vurderinger av risiko og vesentlighet, men at applikasjonen foreløpig ikke er laget for å dokumentere begrunnelsen for valget av tilsynsobjekter. Ifølge beredskapsseksjonen kan dette være aktuelt når også andre seksjoner som fører tilsyn med andre områder har tatt i bruk applikasjonen.

8 NVEs overvåking, varsling og beredskap ved IKT-hendelser

I dette kapitlet beskriver vi hvordan NVE ivaretar oppgaven med å samordne arbeidet med forebyggende sikkerhet og beredskap for IKT-hendelser i kraftforsyningen.

8.1 Relevante føringer

- NVE har som beredskapsmyndighet ansvaret for å samordne arbeidet med forebyggende sikkerhet og beredskap i kraftforsyningen.
- Det forutsettes at selskapene etablerer, eller har tilgang til, nok ressurser til å håndtere IKT-sikkerhetshendelser.
- KraftCERT skal fra juni 2019 ivareta oppgaver innenfor varsling, informasjonsdeling og analyse av IKT-sikkerhetshendelser i kraftforsyningen.
- KraftCERT skal gi råd til NVE ved ekstraordinære situasjoner og hendelser relatert til IKT-sikkerhet.

8.2 Oppsummering

- NVE har styrket systemet for deling av informasjon om IKT-hendelser.
- Underrapportering av IKT-hendelser fører til at NVE og KraftCERT ikke får oversikt over trusselbildet i sektoren og ikke får delt nyttig informasjon om hendelsene til de andre KBO-enhetene.
- Mange av KBO-enhetene får ikke alle KraftCERTs varsler om trusler og sårbarheter.
- Mange selskaper oppfatter at det er uklart hvilke typer IKT-hendelser som skal varsles, og til hvilken instans.
- NVE har nedprioritert å avklare rutinene for varsling og rapportering av IKT-hendelser på grunn av kapasitetsmangel.
- NVE har ikke oppdaterte beredskapsplaner for IKT-hendelser.
- NVE har ikke erfaring med å håndtere IKT-hendelser som har rammet kraftforsyningen.
- NVE har i perioden 2017–2019 deltatt på to større IKT-øvelser.

8.3 Varslingskrav og beredskapsplanlegging

8.3.1 Krav til varsling og rapportering fra selskapene

Selskapene i kraftforsyningen har varslingsplikt om sikkerhetstruende, uønskede hendelser. Etter kraftberedskapsforskriften § 2-5 skal selskapene uten ugrunnet opphold varsle NVE om ekstraordinære situasjoner. For IKT-sikkerhetshendelser kan det for eksempel gjelde

- forsøk på inntrenging og/eller manipulasjon av hele eller deler av driftskontrollsystemet og det avanserte måle- og styringssystemet (AMS)
- situasjoner hvor kraftsensitiv informasjon er blitt kjent for andre enn rettmessige brukere, eller hvor det er mistanke om dette
- omfattende feil og sikkerhetstruende hendelser i driftskontrollsystemer

Etter kraftberedskapsforskriften § 2-6 skal selskapene rapportere om visse IKT-hendelser til NVE. Selskapene skal uten ugrunnet opphold og senest innen tre uker skriftlig sende en rapport om uønskede hendelser til NVE og gi utdypende opplysninger om hendelsen. Kraftberedskapsforskriften og den foreløpige tilleggsveilederen gir eksempler på hva slags type hendelser dette gjelder, blant annet de som er nevnt under kravet til varsling etter § 2-5. Selv om forskriften gir eksempler på hendelser som kan forårsake en ekstraordinær situasjon, er ikke listen uttømmende, og selskapene må selv vurdere om det er andre situasjoner som bør varsles til NVE.[77]

Etter endringene i kraftberedskapsforskriften i 2019 skal selskapene også varsle om uønskede hendelser i de digitale informasjonssystemene til den NVE bestemmer, jf. § 6-9 c, og NVE bestemte i 2019 at dette skal være KraftCERT. Den foreløpige tilleggsveilederen inneholder noen eksempler på hva som skal varsles etter § 6-9 c, som datainnbrudd, oppdagelse av skadevare eller sabotasjeforsøk. KraftCERT gir uttrykk for at det

[77] NVE (2018) *Forventninger og informasjon til KBO* 2018. Brev til KBO, 12. februar 2018.

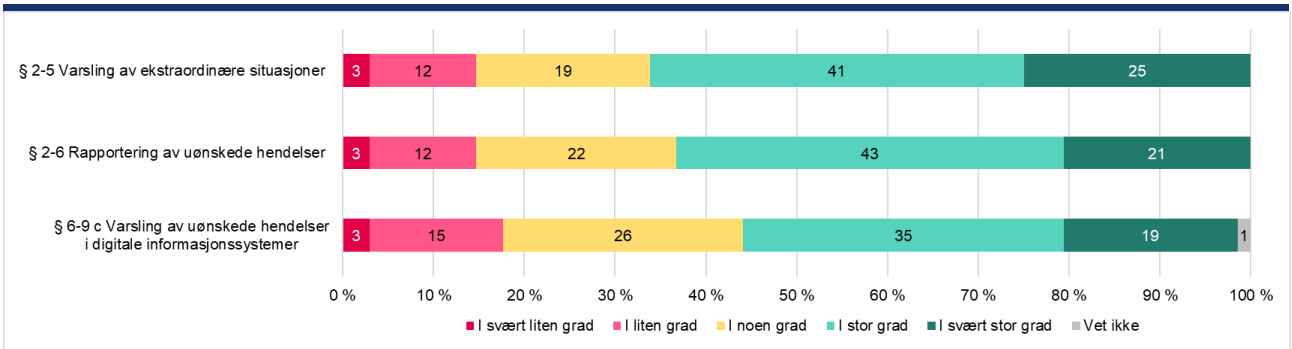
er positivt at selskapene nå skal varsle alle hendelser, også mindre alvorlige hendelser i administrative systemer. KraftCERT mener i tillegg at endringene i kraftberedskapsforskriften har gjort det klart at hendelser i administrative IKT-systemer også kan være kritiske for kraftforsyningen. Ifølge KraftCERT vil denne typen angrep i større grad enn tidligere kunne vurderes som ekstraordinære situasjoner og være varslingspliktige etter § 2-5 (i tillegg til etter § 6-9 c). KraftCERT mener dette er fornuftig siden forsøk på angrep eller rekognosering i administrative systemer også kan ha store konsekvenser for kraftforsyningen.

I juni 2019 informerte NVE KBO-enhetene om etableringen av sektorvist responsmiljø i brev. I brevet skrev NVE at sektorvist responsmiljø for IKT-sikkerhetshendelser i kraftforsyningen er en funksjon som vil bli ivaretatt av NVE med støtte fra KraftCERT.[78] NVE framhevet at for at modellen med sektorvist responsmiljø skal fungere, må det være et samspill mellom responsmiljøet og sektorens virksomheter, som for kraftforsyningen betyr informasjonsutveksling mellom NVE, KraftCERT og den enkelte KBO-enheten. NVE informerte ikke om hvem selskapene skal varsle etter kraftberedskapsforskriften 6-9 c, men i den foreløpige tilleggsveilederen til forskriften gikk det fram at NVE planla å sette ut oppgaven til KraftCERT. I februar 2020 informerte NVE KBO-enhetene i sitt årlige forventningsbrev til KBO om at selskapene skal varsle KraftCERT om alle uønskede IKT-hendelser.

NVE har laget et utkast til retningslinjer for varsling og rapportering i KBO. Retningslinjene er sendt på høring, men ikke vedtatt. Utkastet gir ikke mer veiledning om hvor alvorlig hendelsen skal være for at man skal varsle/rapportere, enn det som allerede er formidlet i kraftberedskapsforskriften, den foreløpige veilederen og brev til KBO. NVE påpeker i forventningsbrevet til KBO for 2020 at den kollektive evnen til læring og beskyttelse vil bli bedre hvis alle har lav terskel for å varsle.

Uklarheter om hva og hvem som skal varsles

Figur 10 IKT-sikkerhetskoordinatorenes svar på om det er klart hvilken instans det skal varsles eller rapporteres til etter kravene i kraftberedskapsforskriften (N = 68)



I vår spørreundersøkelse oppga i gjennomsnitt over halvparten av IKT-sikkerhetskoordinatorene at det i stor eller svært stor grad er klart hvem de skal varsle og rapportere om IKT-hendelser til etter de tre aktuelle kravene i kraftberedskapsforskriften, jf. figur 10. I figur 5 i punkt 6.3.2 går det fram at bare 6 prosent av IKT-sikkerhetskoordinatorene synes at kravene til varsling og rapportering i §§ 2-5 og 2-6 i stor grad er utfordrende å forstå. Intervjuer med flere selskaper viser imidlertid at selskapenes tolkning av kravene ofte ikke stemmer overens med det NVE har ment, selv om selskapene mener det er klart hvor de skal varsle. Enkelte tror at alle IKT-hendelser bare skal varsles til KraftCERT, mens andre tror at alle hendelser skal varsles til NVE og bare de mest alvorlige til KraftCERT.

Både Nettalliansen AS og NC-Spectrum AS oppgir at de også har inntrykk av at det kan være uklart for selskapene hva som skal varsles til NVE, og hva som skal varsles til KraftCERT, men at dette begynner å bli bedre. Begge gir uttrykk for at selskapene mener det er klare rutiner for varsling av ekstraordinære situasjoner til NVE etter § 2-5, men at det er uklare krav til hvilke hendelser som skal varsles til KraftCERT etter § 6-9. KraftCERT oppfatter også at det for mange selskaper, og særlig små selskaper, er uklart at de skal varsle KraftCERT om alle IKT-hendelser. Fordi selskapene parallelt skal varsle flere instanser om samme hendelser, mener KraftCERT at det er viktig å få på plass en løsning som gjør at selskapene kun trenger å varsle ett sted, og i denne løsningen huke av for hvem som skal ha varselet. Ifølge KraftCERT er

[78] NVE (2019) *Etablering av sektorvist responsmiljø - informasjon til KBO*. Brev til KBO, 24.06.2019.

det behov for å gi selskapene i KBO tydeligere informasjon om hvilke typer hendelser de skal varsle til henholdsvis NVE og KraftCERT, og hvordan de skal sende varslene. KraftCERT oppgir i november 2020 at de har planlagt å delta i møter for distriktssjefene i kraftforsyningen med KBO-enhetene framover for å informere om KraftCERTs rolle og de nye varslingsrutinene. I tillegg planlegger KraftCERT å gjennomføre flere webinarer, særlig rettet mot mindre selskaper, blant annet for å øke selskapenes bevissthet rundt nytten av å varsle om flere hendelser til KraftCERT.

NVE viser i intervju til at de i brevet til KBO i februar 2020 informerte selskapene om at de skal varsle KraftCERT om alle uønskede IKT-hendelser. NVE oppgir at de har nedprioritert å avklare rutiner for varsling og rapportering av IKT-hendelser på grunn av ressursmangel. NVE har ikke satt noen terskelverdier for når angrep mot administrative systemer skal varsles til KraftCERT. Ifølge NVE vil den digitale veilederen til kraftberedskapsforskriften gi selskapene ytterligere veiledning om hvilke hendelser som skal varsles etter § 2-5 og § 6-9. Ifølge NVE er det ikke mulig å spesifisere klart hvor grensen går for hvilke IKT-hendelser selskapene skal varsle til KraftCERT. En slik presisering av terskelverdier kan lages dersom man har sensornettverk og et automatisert system som reagerer på type datatrafikk og mengde, men ifølge NVE er ikke bransjen der ennå.

8.3.2 Beredskapsplanverk for håndtering av IKT-hendelser

I de overordnede risikovurderingene for perioden 2018–2020 påpeker NVE at digitale trusler og risikoen for cyberangrep krever god håndteringsevne hos virksomhetene og i NVE. Ifølge NVEs risikorapport for 2020 er det viktig at sektoren har på plass gode rutiner for å håndtere eventuelle hendelser. Videre må NVE avklare sin egen og KraftCERTs rolle ved forebygging og håndtering av IKT-hendelser. NVE trekker fram at roller og ansvar skal avklares i etatens beredskapsplanverk. NVEs beredskapsplanverk skal sikre at NVE er i stand til å ivareta rollen som beredskapsaktør, slik at kriser og ekstraordinære situasjoner blir håndtert effektivt. Beredskapsplanverket består av NVEs grunndokument og beredskapsplaner for ulike typer hendelser og er tilgjengelig på NVEs intranett. NVE har tiltakskort for ulike typer akutte energihendelser som skal operasjonalisere beredskapsplanene og gi mer detaljerte prosedyrebeskrivelser for ulike typer hendelser. Grunndokumentet angir overordnede prinsipper for NVEs beredskapsplanverk som ansvarsfordeling, rollebeskrivelser og beredskapsnivå for hele organisasjonen. Grunndokumentet danner grunnlaget for de hendelsesbaserte beredskapsplanene, som inneholder rammer og retningslinjer for håndtering av ulike typer hendelser. En av beredskapsplanene til NVE gjelder akutte energihendelser og inkluderer IKT-hendelser. Beredskapsplanen gir retningslinjer for NVEs rolle og interne ansvarsfordeling, samarbeid med andre aktører i beredskapssituasjoner (som KBO, NSM, KraftCERT og Olje- og energidepartementet), henvisning til sjekklister og tiltakskort som er relevante for denne typer hendelser, og terskler for å sette beredskap, som inkluderer visse varsler fra NSM. Ifølge NVEs grunndokument skal beredskapsplanene oppdateres årlig. Beredskapsplanen for akutte energihendelser ble sist godkjent i oktober 2017.

NVE har en døgnkontinuerlig vaktordning, og beredskapsvakten mottar varsler om hendelser. Varslene registreres i NVEs interne krisestøtteverktøy CIM (Crisis Information Management). CIM er et nettbasert verktøy for å loggføre og håndtere hendelser og gir oversikt og kronologi over informasjon, handlinger og korrespondanse om registrerte hendelser. Siden NVE skal loggføre alt som er relatert til hendelsen i CIM, kan CIM også brukes til læring og forbedring i etterkant av hendelser. CIM inneholder blant annet kontakt-informasjon og tiltakskort. NVE har flere tiltakskort som er relevante for behandling av IKT-hendelser, og NVE oppgir at tiltakskortene er det operative verktøyet ved etatens håndtering av hendelser. Tiltakskortene sier blant annet hvem som skal varsles internt og eksternt ved ulike beredskapsnivåer. Et av tiltakskortene for alvorlige IKT-hendelser inneholder anbefalinger om hvilket beredskapsnivå ulike hendelser utløser i NVE. En av hendelsene er angrep mot driftskontrollsystemer, hvor beredskapsnivået avhenger av vesentligheten til driftskontrollsystemene som blir angrepet. I NVEs grunndokument står det at beredskapsplanverket skal være basert på egne ROS-analyser, det nasjonale risikobildet og evaluering av hendelser og øvelser. Tiltakskortet for alvorlige IKT-hendelser inneholder ikke informasjon om hvilket beredskapsnivå NVE skal sette ved alle scenarioer som er beskrevet i NVEs ROS-analyser. NVE oppgir at beredskapsplanverket for IKT-hendelser bygger på NVEs erfaringer med hendelser de vanligvis håndterer, og ikke på mer alvorlige scenarioer som ROS-analysene beskriver. Ifølge NVEs grunndokument for beredskap skal tiltakskortene til enhver tid være oppdatert. NVEs tiltakskort for alvorlige IKT-hendelser ble sist oppdatert i januar 2017. Dette innebærer at tiltakskortet ikke er oppdatert ut fra senere års vurderinger fra nasjonale sikkerhets- og etterretningstjenester.

I grunndokumentet for beredskap er det satt kriterier for hva ulike beredskapsnivåer innebærer (fra normalsituasjon/grunnberedskap til høy beredskap), og hvilke tiltak som skal iverksettes ved ulike beredskapsnivåer, blant annet hvilke eksterne aktører som skal varsles. I tiltakskortet for alvorlige IKT-hendelser går det fram at fra og med initialfasen (normalsituasjon) skal Olje- og energidepartementet, KraftCERT, NSM og Nasjonal kommunikasjonsmyndighet varsles når NVE har satt beredskap. Olje- og energidepartementet har ifølge et internt notat om oppfyllelse av kravene i samfunnssikkerhetsinstruksen satt kriterier for når NVE skal varsle departementet. Disse kriteriene er knyttet til det aktuelle tidsrommet og antall kunder som er rammet av strømbruddet som følge av hendelsen. NVE skal også skjønnsmessig vurdere om en hendelse skal varsles departementet med bakgrunn i nyhetsbildet og aktuelle hendelser som gjelder kraftsystemet. NVE oppgir at Olje- og energidepartementet har formidlet kriteriene til NVE i et brev av 2014, og at det har vært dialog om dette i ettertid. NVEs beredskapsplanverk og tiltakskort for IKT-hendelser inneholder ikke de konkrete kriteriene for varsling som departementet har kommunisert til NVE. NVE oppgir imidlertid at de i praksis har lavere terskel for å varsle departementet enn kriteriene departementet har satt. NVE har ikke egne systemer som viser hvor mange kunder som kan rammes dersom et selskap varsler om en hendelse, men selskapene har oversikt over dette, og denne informasjonen skal være med i varslene til NVE. NVE er ikke ferdig med å utarbeide beredskapsplanverket for samhandlingen med KraftCERT etter inngåelsen av avtalen mellom NVE og KraftCERT i 2019.

8.4 KraftCERTs varsler om trusler og sårbarheter til selskapene

8.4.1 KraftCERTs kilder til informasjon om sårbarheter

KraftCERT har fra opprettelsen i 2014 hatt rollen som sektor-CERT for kraftforsyningen. Per november 2020 var 35 av om lag 170 KBO-enheter medlemmer av KraftCERT. Flesteparten av medlemmene er store og mellomstore selskaper i kraftforsyningen. I rollen som sektor-CERT har KraftCERT fulgt med på informasjon om sårbarheter i systemene som medlemsselskapene bruker. KraftCERT har tilgang til flere kilder til informasjon om sårbarheter i administrative systemer og driftskontrollsystemer som er utbredt i kraftforsyningen. Kildene er for eksempel selskapenes systemleverandører og informasjonstjenester KraftCERT abonnerer på. KraftCERT viser i intervju til at de har skaffet seg informasjon om hvilke systemer og leverandører medlemsbedriftene har, slik at de vet hvilke systemer de skal overvåke og sende sårbarhetsvarsler om. KraftCERT oppgir at de ikke har tilsvarende informasjon om systemer og leverandører i selskapene i KBO som ikke er medlem av KraftCERT. I tillegg har KraftCERT fått informasjon om sårbarheter gjennom varsler om IKT-hendelser fra medlemmene. Fra 2020 har de også mottatt noen varsler fra selskaper som ikke er medlemmer.

8.4.2 KraftCERTs varsler om trusler og sårbarheter til selskapene

Varsler til alle KBO-enhetene

I perioden 2014–2018 sendte KraftCERT varsler om alvorlige IKT-sikkerhetshendelser til NVE og ba NVE om å videresende disse til alle selskapene i KBO. KraftCERT oppgir at omfanget av slike varsler har vært lavt, om lag fire–fem varsler per år. I tildelingsbrevet til KraftCERT for 2020 står det at KraftCERT skal formidle relevant og aktuell IKT-sikkerhetsinformasjon til alle selskapene rutinemessig og rettidig. KraftCERT oppgir i intervju at de fram til 2020 tolket oppgaven fra NVE dithen at de bare skulle varsle alle selskapene i KBO om hendelser som kan true kritisk infrastruktur, eller angrep som med stor sannsynlighet kan ramme bredt i kraftbransjen. I juni 2019 begynte KraftCERT å sende ut varsler direkte til alle selskapene, og i løpet av siste halvdel av 2019 sendte de ut fem slike varsler. Selskapene mottok altså omtrent like mange varsler i 2019 som de tidligere hadde fått videresendt fra NVE.

KraftCERT mener formuleringen i tildelingsbrevet om at de skal ivareta varsling, informasjonsdeling og analyse av sikkerhetsinformasjon for samtlige selskaper på vegne av NVE, kan gi inntrykk av at KraftCERTs ansvar for å informere selskapene om sårbarheter, det vil si sende ut varsler om trusler og sårbarheter, er større enn det i praksis har vært. Dette henger sammen med finansieringen av KraftCERT. I 2019 og 2020 ble KraftCERT tildelt 2 millioner kroner for å ivareta oppgavene som del av sektorvist responsmiljø. Før dette ble KraftCERT utelukkende finansiert av medlemsavgiften fra medlemsselskapene. Hoveddelen av KraftCERTs finansiering kommer fremdeles fra medlemsavgiften. I et brev til KBO-enhetene i 2019 viste NVE til at delegeringen av oppgaver knyttet til KraftCERTs rolle i sektorvist responsmiljø ikke ville påvirke

KraftCERTs etablerte medlemsordning med levering av eksklusive tjenester til medlemmene.[79] KraftCERT oppgir at de er avhengig av at medlemsbedriftene opplever at de får merverdi av medlemskapet, utover informasjonen som alle selskapene får. KraftCERT oppfatter imidlertid at alle selskapene i kraftforsyningen har behov for informasjonen om sårbarheter og hendelser fra KraftCERT, og spesielt de mindre selskapene som har mindre IKT-kompetanse. KraftCERT oppgir at de har hatt mye dialog med NVE om hvordan de kan løse dette slik at flere av selskapene får varslene fra KraftCERT uten at medlemsselskapene opplever det som urimelig.

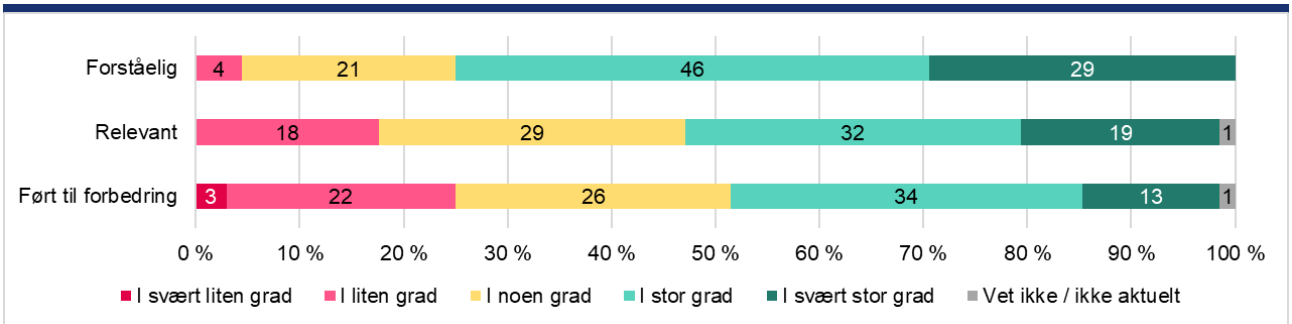
Varsler til KraftCERTs medlemmer

KraftCERT har siden oppstart i 2014 sendt ut varsler om trusler og sårbarheter til medlemsselskapene flere ganger i uka. Varslene inneholder informasjon om aktuelle sårbarheter, trusler og hendelser og en liste med tiltak som selskapet bør iverksette for å unngå å bli rammet. KraftCERT har også en portal der medlemmene kan logge seg på for å få tilgang til informasjon. KraftCERT skiller mellom varsler basert på IKT-sikkerhets-hendelser som selskapene har varslet om, og sårbarhetsvarsler som gjelder svakheter i systemene.

Per oktober 2020 sendte KraftCERT ut regelmessige sårbarhetsvarsler direkte til 50 virksomheter i kraft-forsyningen. Dette er i hovedsak KBO-enheter samt enkelte konsulentselskaper som videresender varslene til enkelte selskaper. KraftCERT har ikke oversikt over nøyaktig hvor stor andel av KBO-enhetene som faktisk mottar alle varslene om trusler og sårbarheter, men anslår at dette gjelder om lag hundre KBO-enheter. KraftCERT påpeker at det er mange små selskaper som fortsatt ikke mottar alle varslene. Kraft-CERT opplyser om at de arbeider med å øke medlemsmassen, og at de har differensiert medlemsprisene ut fra størrelsen på selskapet for å få med flere små selskaper. KraftCERT oppgir at de i 2020 også har senket terskelen for hvilke varsler som deles med alle selskapene, og at de sender ut flere varsler om sårbarheter og hendelser til hele KBO enn tidligere. Begrunnelsen er at KraftCERT ser at det er viktig for alle selskapene å motta varslene, og at de bidrar til en generell bevisstgjøring om IKT-sikkerhet og tiltak som bør iverksettes. Hoveddelen av varslene om sårbarheter og hendelser går imidlertid fortsatt bare til medlemsselskapene.

Selskapenes opplevelse av varslene fra KraftCERT

Figur 11 IKT-sikkerhetskoordinatorenes svar på om varslene fra KraftCERT har vært forståelige, relevante og ført til forbedring (N = 64)



75 prosent av IKT-sikkerhetskoordinatorene oppga at varslene fra KraftCERT i stor eller svært stor grad har vært forståelige, mens i overkant av 50 prosent oppga at de har vært relevante. I underkant av 50 prosent av IKT-sikkerhetskoordinatorene ga uttrykk for at varslene i stor eller svært stor grad har ført til forbedring. Svarene på spørreundersøkelsen kan variere fordi selskapene bruker ulike systemer, og fordi de i ulik grad har satt ut driftsoppgaver til leverandører. Kraftselskapene vi har intervjuet har stort sett vært fornøyd med varslene om trusler og sårbarheter de har mottatt fra KraftCERT. Noen selskaper oppgir i intervju at de har fått iverksatt tiltak som har bedret sikkerheten, basert på varslene fra KraftCERT. Et selskap forteller i intervju at et varsel fra KraftCERT førte til at selskapet oppdaget en inntrenging i et system. På grunn av varslet fikk selskapet iverksatt tiltak slik at svakheten ble utbedret og hendelsen ikke fikk konsekvenser. Et annet selskap gir i intervju uttrykk for at varslene fra KraftCERT har ført til at de har fått gjort nødvendige

[79] NVE (2019) *Etablering av sektorvist responsmiljø - informasjon til KBO*. Brev til KBO, 24.06.2019.

oppgraderinger i systemene sine, og at varslene hjelper selskapet med å opprettholde en høy bevissthet om IKT-sikkerheten over tid.

8.5 Varsling av IKT-sikkerhetshendelser

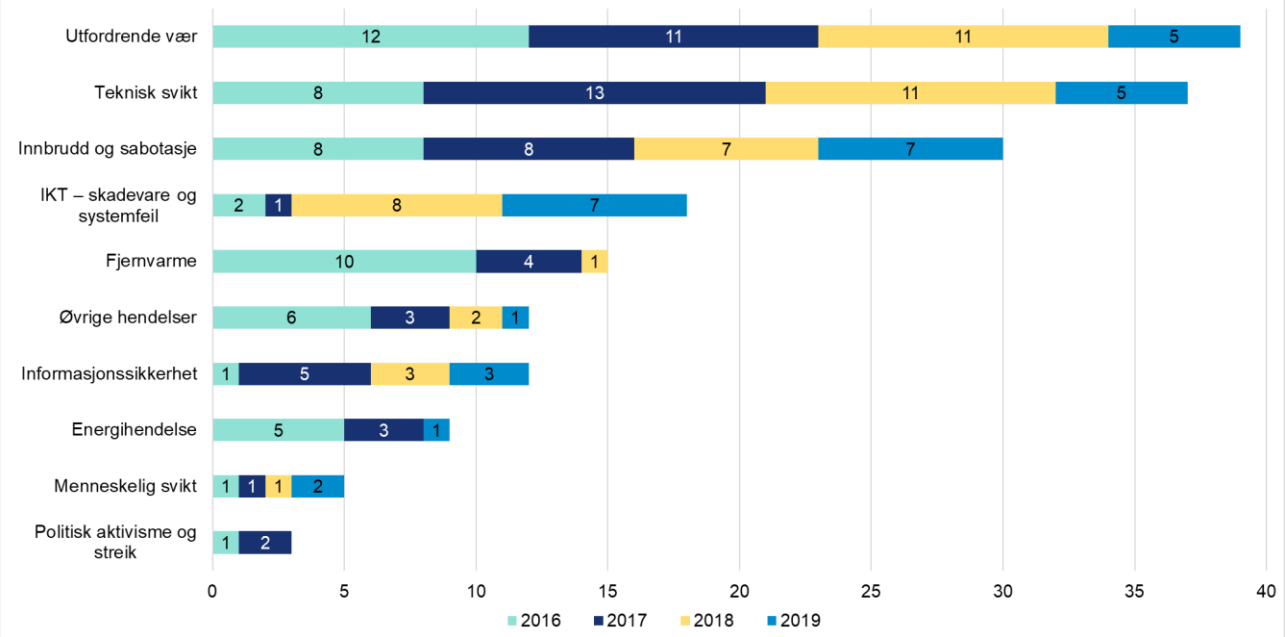
Bakgrunnen for at selskapene skal varsle og rapportere om uønskede IKT-hendelser, er at det skal det gi NVE informasjon om

- pågående situasjoner, slik at de kan vurdere beredskapen og samle informasjon
- sikkerhetstilstanden i sektoren
- sårbarheter i systemer og hos leverandører, som kan brukes til å innrette tiltak som kan forebygge nye hendelser
- selskapets evaluering av og erfaringer fra avsluttede hendelser

8.5.1 Varsler og rapportering om IKT-hendelser til NVE

Kraftberedskapsforskriften stiller krav om at KBO-enhetene skal varsle NVE om ekstraordinære situasjoner når de oppstår, og rapportere uønskede hendelser i ettertid.

Figur 12 Totalt antall hendelser rapportert til NVE i perioden 2016–2019



Kilde: NVE

I perioden 2016–2019 rapporterte KBO-enhetene om 180 uønskede hendelser til NVE. Om lag 30 av disse gjelder kategoriene «IKT – skadevare og systemfeil» og «Informasjonssikkerhet». Enkelte hendelser i de andre kategoriene er også knyttet til IKT-sikkerhet. De fleste hendelsene som er rapportert til NVE, er forårsaket av utfordrende vær som fører til at trær faller over kraftledninger, og teknisk svikt, som feil på utstyr i strømnettet. Utfordrende vær er også årsaken til flest strømbrudd.[80] Hendelsene NVE har registrert, inkluderer krypteringsvirus og inntrengingsforsøk i IKT-systemer, mislykkede oppdateringer av programvare, brudd på besøksrestriksjoner for driftssentraler og lekkasjer av kraftsensitiv informasjon. Enkelte hendelser har rammet selskapers driftskontrollsystemer. Disse skyldes svikt i fysisk utstyr tilknyttet driftskontroll-systemene og mislykkede programvareoppdateringer, og ikke IKT-angrep.

NVE oppgir at de ikke har mottatt varsler om IKT-hendelser der forsyningssikkerheten har vært skadelidende og som det har vært nødvendig å varsle videre til Olje- og energidepartementet. Spørreundersøkelsen fra 2017 viste at tre selskaper hadde opplevd hendelser som omfattet driftskontrollsystemene i løpet av det siste

[80] Prop. 1 S (2017-2018) Olje- og energidepartementet.

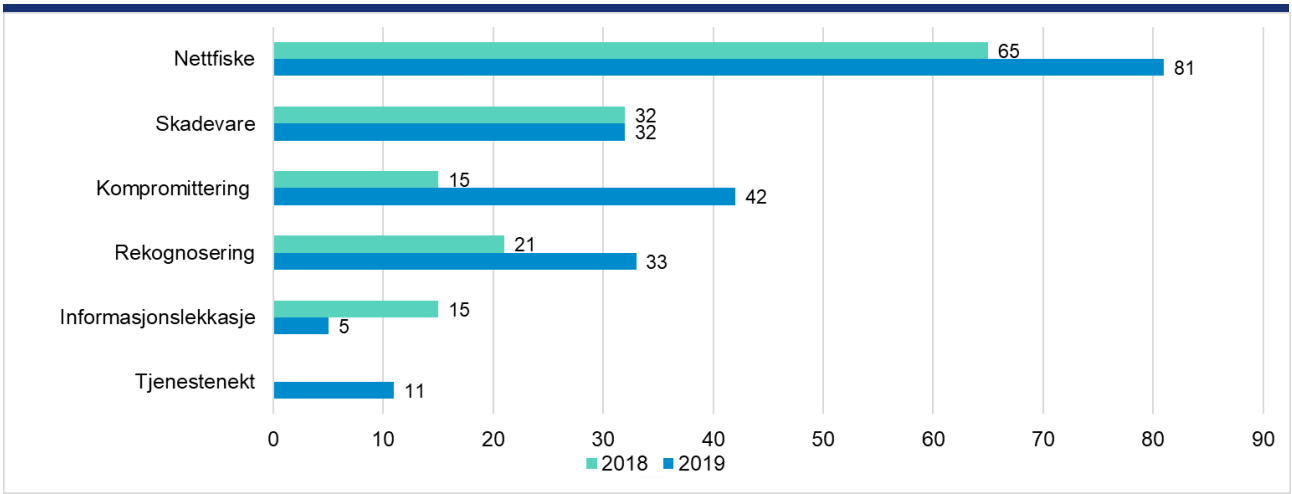
året. KraftCERT oppgir at de får rapporter om ca. to–tre hendelser i driftskontrollsystemer i året, det vil si omtrent like mange som NVE mottar.

I en spørreundersøkelse som NVE gjennomførte i 2017, ba etaten virksomheter i kraftbransjen oppgi hvilke informasjonssikkerhetshendelser de hadde opplevd de siste tolv månedene.[81] Spørreundersøkelsen viste at nærmere 70 prosent av de 88 virksomhetene som svarte, hadde opplevd uønskede IKT-sikkerhetshendelser det siste året. 59 prosent av virksomhetene sa at de hadde hatt hendelser som var alvorlige. Om lag halvparten oppga å ha opplevd bedrageri (fakturasvindel, svindel-e-post eller andre former for manipulering). De fleste oppga at dette hovedsakelig dreide seg om svindelforsøk via e-post og brev, men at forsøkene var blitt oppdaget og stoppet. Om lag 40 prosent hadde opplevd å få virus og skadevare i systemene sine, og rundt 30 prosent hadde opplevd forsøk på datainnbrudd og dataskadeverk. Over 10 prosent oppga at IKT-hendelser hadde hatt negative konsekvenser som tapt produksjon, økonomiske tap, omdømmetap eller svekket markedsposisjon. 40 prosent av virksomhetene som hadde hatt alvorlige hendelser, oppga at det ikke var gjort noen endringer innad i organisasjonen i etterkant av hendelsen. Tre selskaper i spørre-undersøkelsen oppga at IKT-sikkerhetshendelser hadde rammet driftskontrollsystemene deres.

8.5.2 Varsler om IKT-hendelser til KraftCERT

KraftCERT har siden opprettelsen i 2014 mottatt varsler om IKT-hendelser fra sine medlemmer. Hendelser som er blitt varslet til KraftCERT, kan også ha blitt varslet til NVE etter kravene i kraftberedskapsforskriften. Etter endringene i kraftberedskapsforskriften fra 2019 skal alle KBO-enhetene varsle om uønskede IKT-hendelser til KraftCERT. KraftCERT oppgir at de fra 2020 også har begynt å motta noen varsler fra KBO-enheter som ikke er medlemmer.

Figur 13 Totalt antall IKT-hendelser behandlet av KraftCERT i 2018 og 2019



Kilde: KraftCERT

KraftCERT behandlet om lag 150 uønskede IKT-hendelser i 2018 og om lag 200 hendelser i 2019. Av disse har 20–50 hendelser hvert år vært større hendelser der KraftCERT har opprettet en egen oppfølgings-prosess. KraftCERT anslår at to–tre hendelser hvert år har vært knyttet til driftskontrollsystemer. Nettfiske utgjør flesteparten av hendelsene som rapporteres til KraftCERT, og ifølge KraftCERT mottar KBO-enhetene enorme mengder e-poster med lenker til skadevare. Ifølge KraftCERT har det vært et jevnt høyt nivå av rekognoseringer i 2019, og noe av denne rekognoseringen ser ut til å være målrettet. KraftCERT oppgir at de har jobbet med mistanke om kompromitteringer[82] både i administrative systemer og i driftskontroll-systemer. Kompromitteringer har skjedd både i selskapenes egne systemer og hos leverandørene. KraftCERT ser en økning i angrep mot leverandørene til selskapene i kraftforsyningen. Det er også et jevnt høyt nivå av automatiserte innloggingsforsøk mot selskapenes internetteksponerte tjenester, og selskaper

[81] NVE-rapport (2017) *Informasjonssikkerhetstilstanden i energiforsyningen.* NVE-rapport 74/2017. Respondentene besto i hovedsak av IKT-sikkerhetskoordinatorer for nettselskaper, kraftprodusenter eller konsern i kraftbransjen.
[82] KraftCERT definerer kompromittering som «[e]t vellykket forsøk på å oppnå uautorisert tilgang til system, tjenester, ressurser eller informasjon, eller et vellykket forsøk på å kompromittere (forringe) konfidensialitet, integritet eller tilgjengelighet av system, tjeneste eller informasjon.».

uten flerfaktorautentisering har en svært høy sannsynlighet for å bli kompromittert gjennom automatiserte gjentakende påloggingsforsøk.

Ifølge KraftCERT er de fleste hendelsene som rapporteres til dem, ikke alvorlige, men noen kunne ha blitt alvorlige dersom de ikke hadde blitt håndtert i tide.[83] KraftCERT oppgir at de fleste hendelsene gjelder administrative systemer, men påpeker at slike hendelser må håndteres i tide. Aktører kan nemlig bruke tilgangen til administrative systemer som en inngangsport til driftskontrollsystemene og dermed også påvirke kraftforsyningen.

I rapporteringen til NVE i 2019 oppgir KraftCERT at man kan regne med en relativt stor underrapportering om IKT-hendelser i norsk kraftsektor. Både NSM og KraftCERT oppfatter at det er underrapportering av IKT-sikkerhetshendelser i alle sektorer. Olje- og energidepartementet oppgir i sine kommenterer til utkastet til hovedanalyserapport at det ikke er grunnlag for å si at det er underrapportering til NVE når det gjelder ekstraordinære situasjoner og påpeker at det er kun ekstraordinære situasjoner som skal varsles til NVE.

KraftCERT mener underrapportering fører til at verken NVE eller KraftCERT får et godt nok situasjonsbilde over sikkerhetstilstanden i kraftforsyningen. Ettersom KraftCERT ikke kan forutse hvem som forsøker å få tilgang til selskapenes systemer, vil informasjon om rekognoseringsfasen til trusselaktører være svært nyttig for KraftCERT. Underrapporteringen av hendelser kan også føre til at NVE og KraftCERT ikke får delt nyttig informasjon om hendelser i et selskap til de andre KBO-enhetene.

8.5.3 Mulige årsaker til underrapportering

Flere aktører mener underrapportering av IKT-hendelser i kraftforsyningen blant annet kan skyldes *uklare varslingsrutiner* for hva og hvem som skal varsles i selskapene (jf. punkt 8.3.1). NVE gjennomførte i 2018 en spørreundersøkelse for å kartlegge hva som ligger til grunn for selskapenes varsling og rapportering til NVE. Resultatene fra undersøkelsen viser at omtrent halvparten av KBO-enhetene mangler kriterier for når det skal rapporteres til NVE etter ekstraordinære hendelser. I punkt 4.4.3 går det fram at NVE har gitt mange avvik i perioden 2017–2019 til selskapers risikovurderinger. Dersom selskapene ikke har definert hva som utgjør ekstraordinære situasjoner, kan også det føre til at hendelser ikke rapporteres til NVE i tråd med kravene i kraftberedskapsforskriften. I tilleggsveilederen til kraftberedskapsforskriften oppfordres selskapene til å varsle NVE dersom de er i tvil om en situasjon skal varsles.

I tillegg trekker flere aktører fram at det kan være en *manglende kultur for å varsle* i selskapene. Både Nettalliansen AS og KraftCERT erfarer at enkelte selskaper avventer å varsle om hendelser fordi de ønsker å løse problemet internt før de deler informasjonen med andre. Og hvis selskapene klarer å få situasjonen under kontroll, er det ikke sikkert at de i ettertid vil varsle om dette. Ifølge NC-Spectrum AS er det også en utfordring at selskapene gjennomgående er for dårlige til å varsle og dele informasjon om hendelser i systemene sine. NC-Spectrum AS mener dette skyldes at det skjer mange mindre alvorlige IKT-hendelser, og at disse blir en vanlig del av hverdagen som IKT-miljøet i selskapene ikke mener det er nødvendig å varsle om. Det er ifølge NC-Spectrum AS viktig å bidra til en holdningsendring i selskapene, slik at det ikke blir sett på som et tegn på dårlig kontroll at selskapet opplever og varsler om IKT-hendelser.

Svakheter i selskapenes evne til å overvåke systemene og oppdage IKT-angrep trekkes også fram som en årsak til underrapportering. Disse svakhetene beskrives nærmere i punkt 4.4.4.

8.5.4 Informasjonsutveksling mellom NVE og KraftCERT

NVE og KraftCERT oppgir at de utveksler informasjon om uønskede hendelser og trusler i ukentlige møter. Dette gjelder både informasjon om tekniske varsler fra NSM, aktuelle sårbarheter/trusler for eksempel hos leverandører og i systemer, og varsler om uønskede IKT-hendelser som NVE og KraftCERT har mottatt fra selskapene. KraftCERT anonymiserer varslene de får fra selskapene, før de informerer NVE.

8.6 Håndtering av uønskede IKT-hendelser

8.6.1 Håndtering av IKT-hendelser

NVE skal ha grunnleggende kapasitet til å koordinere og håndtere uønskede IKT-sikkerhetshendelser. I tildelingsbrevet til KraftCERT for 2019 og 2020 står det at KraftCERT skal gi råd til NVE ved ekstraordinære

[83] NVE og KraftCERT (2020) *Digital kontroll: en studie om innføring og bruk av metrikker i kraftforsyningen for bedre IKT-sikkerhet.* NVE-rapport nr. 22/2020.

situasjoner og hendelser knyttet til IKT-sikkerhet og på forespørsel bidra til beredskapsmyndighetenes håndtering og oppfølging av varsler og rapporter.

NVE oppgir at det så langt ikke har funnet sted noen store IKT-sikkerhetshendelser i kraftforsyningen der forsyningssikkerheten har vært skadelidende og det har vært nødvendig å ta i bruk NVEs beredskaps-planverk for IKT-hendelser. Det innebærer at sektoren ikke har erfaring med å håndtere denne typen ekstraordinære IKT-hendelser. NVE har som rutine å evaluere større hendelser der NVEs interne beredskapsorganisasjon har vært involvert, men ettersom det ikke har vært noen større IKT-hendelser, har slike hendelser heller ikke blitt evaluert. NVE gjennomfører «Beredskapsleders faglunsj» to ganger i året, hvor hendelser som har funnet sted, blir gjennomgått og forbedringer i beredskapshåndteringen blir diskutert. IKT-hendelser i kraftforsyningen har ikke blitt tatt opp i dette forumet.

Beredskapsvakten i NVE mottar varsler om ekstraordinære situasjoner etter kraftberedskapsforskriften § 2-5 og loggfører varslene i krisestøtteverktøyet CIM. Ifølge NVE er hensikten med kravet til varsling av ekstraordinære situasjoner etter § 2-5 at NVE skal gjøres kjent med pågående situasjoner for å vurdere beredskapen og samle informasjon. Ifølge NVE avhenger beredskapsvaktens behandling av varsler av hva slags type hendelse som er varslet, og oppfølgingsbehovet i etterkant.

En saksgjennomgang av oppføringer i krisestøtteverktøyet CIM og en oversikt over innrapporterte hendelser viser at NVE fikk meldt inn seks pågående hendelser knyttet til IKT-sikkerhet i perioden 2017–2019. Tre av hendelsene gjaldt mulige brudd på krav til besøksrestriksjoner for driftssentraler og beskyttelse av kraftsensitiv informasjon, og de øvrige tre gjaldt IKT-angrep og IKT-hendelser. En gjennomgang av NVEs dokumentasjon av disse hendelsene viser følgende:

- NVE fulgte opp fire av hendelsene med omfattende dialog med berørte parter og varsel om overtredelsesgebyr ved to av hendelsene.
- Ved en av hendelsene skulle NVE ta kontakt med rapporterende part, men det går ikke fram av dokumentasjonen om NVE fulgte opp saken, eller hvilke konsekvenser hendelsen fikk.
- Ved et av varslene går det ikke fram hvilket selskap hendelsen gjelder, eller om NVE har besvart eller håndtert varslet.
- Tre av de seks hendelsene har status «under oppfølging/veiledning» i NVEs oversikter, til tross for at sakene er fra 2017 og 2018 og lukket i arkivet.

NVEs behandling av informasjon om hendelser som er rapportert i etterkant av hendelsen, omtales nærmere i punkt 8.7.

8.6.2 Øvelser

I Meld. St. 25 (2015–2016) *Kraft til endring – Energipolitikken mot 2030* går det fram at styrket IKT-sikkerhet i energiforsyningen krever at NVE blant annet gjennomfører øvelser. Lysneutvalget anbefalte også at NVE gjennom veiledningsrollen skal være pådriver for flere øvelser på IKT-sikkerhetsområdet, både i sektoren og overfor andre sektorer det er naturlig å samarbeide med. NVEs grunndokument for beredskap sier at ledelse og avdelinger, seksjoner og regionskontorer med beredskapsansvar jevnlig skal gjennomføre øvelser med et innhold og omfang som lar dem vedlikeholde og utvikle kompetansen slik at de er i stand til håndtere alle aktuelle ekstraordinære situasjoner. Det skal øves på tvers av nivåer, og det skal øves sammen med andre som NVE samvirker med i kriser, både internt og eksternt. NVE skal ha en flerårig øvelsesplan, og avdelingene skal ta initiativ til øvelser for hele eller deler av NVE og for egen avdeling. Evaluering av øvelser og hendelser skal danne grunnlaget for læring og oppdatering av NVEs beredskapsplanverk. NVE oppgir i intervju at de har som rutine å evaluere øvelser der NVEs interne beredskapsorganisasjon har vært involvert.

NVE oppgir at selv om det ikke har forekommet IKT-hendelser i kraftforsyningen der den interne beredskaps-organisasjonene har vært involvert, øves organisasjonen jevnlig gjennom håndtering av andre hendelser som har ført til strømbrudd, som naturhendelser. NVE hadde en øvelseskalender for perioden 2017–2019, men har ikke utarbeidet en tilsvarende øvelseskalender for 2020 og framover. NVE har utformet en oversikt over IKT-øvelser som etaten har deltatt på eller arrangert i perioden 2008–2020. Den viser at NVE har deltatt i flere IKT-øvelser etter 2015 enn i årene før. I perioden 2017–2019 deltok NVE i IKT-øvelsene «Black Screen 1» og «Black Screen 2» i regi av de nordiske systemoperatørene Statnett og Fingrid. IKT-øvelsene har ikke omfattet samhandling med selskaper og leverandører i kraftforsyningen, med unntak av Statnett. NVE påpeker at øvelser med andre scenarioer enn IKT-angrep også bidrar til å utvikle NVEs håndteringsevne.

NVE har utarbeidet en internevaluering av øvelsen «Black Screen 1». Dette var en nordisk øvelse som simulerte angrep mot systemoperatørenes driftskontrollsystemer, og som for Norges del omfattet NVE, NSM, Statnett og KraftCERT. Evalueringen viser at disse aktørene trente på samhandling under øvelsen, og at informasjonsdelingen fungerte godt. I internevalueringen trekkes det fram at KraftCERT er en viktig ressurs i norsk krisehåndtering. Et av læringspunktene etter øvelsen var at det er nyttig og viktig å ha tett dialog med KraftCERT og NSM for å forstå det som skjer, og at det er viktig å ha med ansatte fra andre deler av NVE ved IKT-hendelser. Et av tiltakene etter øvelsen var å videreutvikle den gode relasjonen med KraftCERT og å øve mer på IKT-hendelser. Det går ikke fram av NVEs internevaluering om NVE brukte beredskaps-planverket for IKT-hendelser i øvelsen, og NVEs beredskapsplan og tiltakskort ble ikke oppdatert i etterkant av øvelsen. NVE påpeker at NVEs deltakelse i eksternt initierte øvelser om IKT-sikkerhet har redusert behovet for egeninitierte øvelser, og at prosessen med regelverksendringer og etablering av samarbeid med KraftCERT ikke har gjort det naturlig å gjennomføre egeninitierte øvelser i undersøkelsesperioden.. NVE påpeker at det har skjedd store endringer i de ulike aktørenes roller de siste årene når det gjelder IKT-hendelser. NVE har ikke gjennomført øvelser med KraftCERT etter at det i 2019 ble bestemt at KraftCERT skal støtte NVE i rollen som sektorvist responsmiljø i kraftforsyningen.

8.7 Behandling og evaluering av rapporterte IKT-hendelser

NVE oppgir i intervju at de har som rutine å evaluere hendelser der NVEs interne beredskapsorganisasjon har vært involvert. Ifølge NVE er hensikten med kravet til rapportering i kraftberedskapsforskriften § 2-6 at NVE skal få informasjon om selskapets egen evaluering og erfaringer etter avsluttede hendelser. NVE vurderer på bakgrunn av informasjonen i rapporteringen om det må gjennomføres tiltak. Ifølge NVE inngår uønskede hendelser også i deres vurdering av tilstanden i kraftforsyningen.[84]

NVE har ikke gjeldende rutinebeskrivelser for intern håndtering og oppfølging av rapporteringer etter § 2-6, men oppgir at de jobber med å få dette på plass. NVE har laget en beskrivelse av NVEs gjeldende praksis for behandling av rapportering fra selskapene. Rapporteringer om uønskede hendelser og etterrapportering av ekstraordinære situasjoner etter § 2-6 lagrer NVE i arkiv og et regneark. NVEs regneark over innrapporterte hendelser kan også inneholde informasjon om hendelser NVE har avdekket selv eller blitt informert om fra andre kilder, for eksempel KraftCERT. NVE oppgir at alle hendelser følges opp, men at oppfølgingen kan variere: NVE kan ta hendelsen til orientering, be om en etterfølgende rapport, be om et møte med selskapet eller følge opp med et tilsyn. NVE arkiverer korrespondansen om den innrapporterte hendelsen. Måten NVE arkiverte innrapporterte hendelser på før 2019, gjør det ikke mulig å vurdere om hendelsene er ferdigbehandlet.[85] Hendelser fra og med 2019 er arkivert som egne saker med tilhørende informasjon, og det går fram av sakens status i arkiv om de er ferdigbehandlet eller ikke.

Gjennomgangen av NVEs dokumentasjon av registrerte IKT-hendelser i perioden 2016–2019 viser følgende:

- For alle hendelser går det fram hvilket selskap hendelsen gjelder, og at oppfølgingen av hendelsen er blitt tilordnet en fagperson i NVE.
- For mange av hendelsene beskriver det rapporterende selskapet hendelsens årsak og konsekvenser og hvilke tiltak som er iverksatt for å unngå at hendelsen gjentas. For andre hendelser framgår ikke dette av selskapenes rapportering.
- Flere hendelser er kategorisert som tilsynsrelevante, uten at det går fram om hendelsene har utløst tilsyn av NVE. Det går fram at oppfølgingen av flere av hendelsene er blitt nedprioritert.
- Flere eldre hendelser oppgis å være under oppfølging eller veiledning uten at det går fram om det er blitt foretatt noe mer i saken.

NVE har flere regneark og systemer hvor de registrerer IKT-hendelser, herunder hendelsesoversikten, CIM-verktøyet og arkiv. I NVEs arkiv er det registrert flere hendelser som pågikk da NVE ble informert, og som NVE har fulgt opp, men som ikke er registrert i NVEs hendelsesoversikter og hendelsesverktøy. Dette gjør at NVEs oversikt over hendelser er lite tilrettelagt for oppfølging av selskaper og interne analyseformål. NVE oppgir at de er i gang med å videreutvikle den nyutviklede applikasjonen som fra 2020 brukes til tilsyn, slik at den også skal inkludere en oversikt over innrapporterte hendelser.

[84] NVE (2019) *Tilstandsvurdering av forsyningssikkerhet og beredskap i kraftforsyningen.* Faktaark nr. 10/2019,
[85] Dette skyldes at hendelsene er lagret som enkeltdokumenter og ikke saker, og at de dermed ikke kan få annen status enn at dokumentasjonen er «journalført» eller «arkivert».

KraftCERT skal årlig rapportere om utførte aktiviteter til NVE og utarbeide en rapport med oversikt over IKT-sikkerhetstilstanden i kraftforsyningen.[86] KraftCERTs årsrapport til NVE for 2019 inneholder en oppsummering av KraftCERTs utførte oppgaver og informasjon om hendelser og sikkerhetstilstanden i kraftbransjen. Ifølge KraftCERT bygger rapporteringen om hendelser og sikkerhetstilstanden hovedsakelig på informasjon om varsler om hendelser i medlemsbedriftene siden KraftCERT ikke fikk noen varsler fra ikke-medlemmer i 2019.

[86] NVE (2019) *Tildeling av midler til KraftCERT i 2019*. Brev til KraftCERT, 07.06.2019.

9 Olje- og energidepartementets styring og oppfølging av NVEs arbeid med IKT-sikkerhet i kraftforsyningen

I dette kapitlet beskriver vi hvordan Olje- og energidepartementet styrer og følger opp NVEs arbeid med IKT-sikkerhet i kraftforsyningen gjennom fastsettelse av mål og oppfølging av resultater.

9.1 Relevante føringer

- Olje- og energidepartementet skal
  - legge til rette for en sikker kraftforsyning gjennom god beredskap i kraftforsyningen
  - sørge for at det utarbeides risiko- og sårbarhetsanalyser for kraftforsyningen og ha oversikt over tilstanden knyttet til sårbarheter for kraftforsyningen
  - fastsette mål- og resultatkrav for NVE og følge opp at målene nås
  - ha et overordnet ansvar for at NVE har et fungerende og forsvarlig system for internkontroll og bruker tildelte ressurser effektivt og forvalter oppgaver på en forsvarlig måte
  - sørge for at det blir gjennomført evalueringer for å skaffe kunnskap om måloppnåelse og resultater på området

9.2 Oppsummering

- NVEs arbeid med IKT-sikkerhet i kraftforsyningen inngår som tiltak for å nå målet om sikker kraftforsyning.
- Rapporteringen om NVEs arbeid med IKT-sikkerhet i kraftforsyningen inneholder i hovedsak beskrivelser av tiltak og aktiviteter som er gjennomført.
- Olje- og energidepartementet innhenter lite informasjon om resultatene av NVEs arbeid med IKT-sikkerhet i kraftforsyningen.

9.3 Olje- og energidepartementets styring og oppfølging av NVEs arbeid med IKT-sikkerhet i kraftforsyningen

9.3.1 Etatsstyringsdialog

Olje- og energidepartementet skal legge til rette for en sikker kraftforsyning gjennom god beredskap i kraftforsyningen og har delegert viktige beredskapsoppgaver til NVE. Olje- og energidepartementets etatsstyring av NVE skjer hovedsakelig gjennom tildelingsbrev og ved oppfølging og rapportering i samsvar med dette.[87] Styringsdialogen er beskrevet i instruksen for økonomi- og virksomhetsstyring i NVE. Dokumenter som inngår i den årlige styringsdialogen, er budsjettproposisjoner og tildelingsbrev, NVEs årsrapporter og NVEs overordnede risiko- og vesentlighetsvurderinger.

Det gjennomføres to årlige etatsstyringsmøter mellom Olje- og energidepartementet og NVE. En gjennomgang av referatene fra etatsstyringsmøtene i perioden fra 2017–2019 viser at temaet forsynings-sikkerhet og IKT-sikkerhet har vært omtalt noen ganger. Blant annet ble departementet i mai 2019 informert om revisjonen av kraftberedskapsforskriften og om arbeidet med å bygge opp kompetanse på cyber-sikkerhet. Olje- og energidepartementet har blitt informert om prosessen med rolleavklaring mot KraftCERT i etatsstyringsmøtene. NVE oppfatter at departementet har hatt større oppmerksomhet på IKT-sikkerhet de senere årene. De siste årene har departementet vektlagt digitale trusler, det sikkerhetspolitiske bildet og klima/værhendelser innenfor målet om en sikker kraftforsyning. Olje- og energidepartementet oppgir i intervju at det meste av departementets styring og oppfølging av NVE skjer i formell styringsdialog, og at kontakten mellom departementet og NVE utover faste møter er styrt av hendelser og øvelser. Ettersom NVE ikke har varslet Olje- og energidepartementet om alvorlige IKT-sikkerhetshendelser, har kontakten i liten grad handlet om IKT-sikkerhet. Departementet møter også NVE i mange ulike fora, for eksempel deltar ansatte i departementet ofte på NVEs seminarer om IKT-sikkerhet i kraftforsyningen. Departementet overlater i stor

[87] Olje- og energidepartementet (2016, oppdatert 2020). *Instruks for økonomi- og virksomhetsstyring i Norges vassdrags- og energidirektorat*.

grad konkrete prioriteringer og faglige vurderinger til NVE, noe NVE synes er naturlig siden de er beredskapsmyndighet for kraftforsyningen.

9.3.2 Prioriteringer, mål og styringsparametere

Olje- og energidepartementet har ikke satt egne mål og resultatkrav for NVEs arbeid med IKT-sikkerhet i kraftforsyningen, men oppgir at det ligger under hovedmålet om å fremme en sikker kraftforsyning. Et av delmålene som skal bidra til at NVE når dette hovedmålet, går ut på å påse at beredskapen i kraftforsyningen er god og i tråd med gjeldende krav. Styringsparameterne som er satt for dette delmålet, er som følger:

- Beskriv de viktigste tiltakene og hvordan disse bidrar til å fremme hovedmålet.
- Gi en vurdering av statusen og utviklingen i sikkerhets- og beredskapstilstanden i kraftforsyningen.
- Beskriv samarbeidet med energibransjen, myndighetsorganer og andre nordiske land innenfor kraftforsyningsberedskap og gi en vurdering av hvilken betydning samarbeidet har for å fremme en sikker kraftforsyning.

Styringsparameterne som er satt for målet om å fremme en sikker kraftforsyning, er både aktivitetskrav og resultatkrav. NVE skal beskrive tiltak og hvordan tiltakene har bidratt til å fremme en sikker kraftforsyning. Olje- og energidepartementet har ikke gitt noen styringsparametere innenfor IKT-sikkerhetsarbeidet som gjør det mulig å følge utviklingen på området sammenlignet med et gitt mål.

Olje- og energidepartementet har også gitt andre føringer på IKT-sikkerhet. I tildelingsbrevene til NVE for 2017 og 2018 ba departementet NVE om å vurdere regelverket og tilhørende veiledning med tanke på å styrke IKT-sikkerheten i energiforsyningen, herunder følge opp anbefalingene fra Lysneutvalget.[88] I tildelingsbrevet til NVE for 2019 og 2020 går det fram at departementet legger til grunn at NVE – i tråd med NVEs rolle som beredskapsmyndighet – er sektorvist responsmiljø for IKT-sikkerhetshendelser i kraftsektoren, eventuelt i samarbeid med andre aktører. I tildelingsbrevet til NVE for 2020 går det fram at NVE skal følge opp *Nasjonal strategi for digital sikkerhet (2019)* og *Nasjonal strategi for digital sikkerhetskompetanse (2019)*, både i egen virksomhet og i kraftsektoren.[89]

9.3.3 Rapportering på mål og styringsparametere

NVE rapporterer om måloppnåelse på krav fra Olje- og energidepartementet i årsrapportene. I NVEs årsrapporter for 2018 og 2019 går det – under rapporteringen om hovedmålet om at NVE skal fremme en sikker kraftforsyning – fram at forsyningssikkerheten er vurdert som god, og at det er lite sannsynlig at det skjer store uønskede hendelser. Det vises til at bransjen blir mer digitalisert og dermed sårbar for digitale angrep. NVE legger derfor stor vekt på å følge opp IKT-sikkerhet i sektoren. Gjennomgangen av rapporteringen for 2017–2019 viser at NVE beskriver arbeidet med ulike tiltak for å styrke forsyningssikkerheten, men at de skriver lite om hvordan de ulike tiltakene har bidratt til å nå hovedmålet om å fremme en sikker kraftforsyning.

Olje- og energidepartementet oppgir i intervju at de har forståelse for at det er krevende å rapportere på resultatkravet om hvordan arbeidet til NVE bidrar til å fremme en sikker kraftforsyning, og at de ikke forventer at NVE skal rapportere årlig på dette. Siden 2016 har Olje- og energidepartementet vært opptatt av å få bedre informasjon om resultater og utviklingen i kraftforsyningen. Olje- og energidepartementet har siden 2016 bedt NVE om å rapportere om utviklingen av tilstanden i kraftforsyningen. I budsjettproposisjonen for 2018 publiserte Olje- og energidepartementet en tilstandsvurdering for kraftforsyningen, som blant annet var basert på innspill fra NVE, jf. omtale i punkt 5.5.2. På bestilling fra departementet lagde NVE et faktaark med en forenklet og oppdatert tilstandsvurdering i 2019 og en oppsummering av uønskede hendelser i kraftforsyningen. Olje- og energidepartementet oppgir i intervju at de mener at de får tilstrekkelig informasjon om statusen og utviklingen i sikkerhetstilstanden i kraftforsyningen, selv om det finnes områder der det er vanskelig å finne god statistikk, og der foreliggende statistikk har svakheter. Et eksempel er underrapporteringen av hendelser. Departementet oppgir at de har diskutert svakheter i statistikken og statistikkgrunnlaget med NVE. Olje- og energidepartementet gir uttrykk for at det er krevende å finne gode indikatorer på utviklingen i sikkerhetstilstanden i kraftforsyningen, og at det også gjelder IKT-sikkerhet. Departementet har i styringsdialogen bedt NVE om å arbeide med å finne bedre indikatorer, men påpeker at også departementet selv har et ansvar for å finne gode indikatorer.

[88] NOU (2015: 13) *Digital sårbarhet – sikkert samfunn*
[89] Departementene 2019. *Nasjonal strategi for digital sikkerhet*; Departementene 2019. *Nasjonal strategi for digital sikkerhetskompetanse*.

Olje- og energidepartementet skriver i budsjettproposisjonen for 2020 at de vurderer at NVE gjennom sitt arbeid har bidratt til å ivareta sikkerheten og beredskapen i kraftforsyningen. Omtalen av NVEs arbeid med IKT-sikkerhet i budsjettproposisjonene for 2018 og 2019 gir også inntrykk av at departementet er fornøyd med NVEs arbeid med IKT-sikkerhet. I alle budsjettproposisjonene for årene 2018–2020 viser departementet til at NVE prioriterer arbeidet med IKT-sikkerhet i kraftforsyningen gjennom ulike tiltak. Departementet gir i intervju uttrykk for at NVE har en risikobasert tilnærming i prioriteringen mellom de ulike oppgavene sine. NVE har vært utsatt for kutt i bevilgningene de senere årene, i likhet med alle statlige etater som følge av ABE-reformen.[90] Olje- og energidepartementet har dermed ikke økt bevilgningene til NVE selv om IKT-sikkerhet er framhevet som et prioritert område i meldinger, men mener at NVE har store muligheter til å omprioritere midler selv. NVE har ikke bedt Olje- og energidepartementet om økte ressurser til arbeidet med IKT-sikkerhet i kraftforsyningen, med unntak av midler til KraftCERTs oppgaver.

NVE skal årlig identifisere risikoen for mangelfull oppnåelse av mål- og resultatkravene i de overordnede risiko- og vesentlighetsvurderingene og rapportere om slik risiko til departementet. Videre skal de angi hvilke tiltak som er eller vurderes iverksatt for å redusere risikoen. I perioden 2017–2020 trakk NVE i de overordnede risiko- og vesentlighetsvurderingene fram flere risikoer innenfor området forsyningssikkerhet som er knyttet til arbeidet med IKT-sikkerhet i kraftforsyningen. Begge årene gikk de nye risikoreduserende tiltakene ut på å avklare NVEs og KraftCERTs roller og ansvar når det gjelder forebygging og håndtering av IKT-hendelser, og å styrke bransjens forståelse av utfordringer gjennom samarbeidsprosjekter m.m. I tillegg skulle NVE bidra til å styrke kompetansen internt og eksternt gjennom kompetansefremmende tiltak og FoU som styrker forvaltningen, herunder doktorgradsstudier. Departementet oppgir at de i liten grad er involvert i oppfølgingen av tiltak som er nevnt i risiko- og vesentlighetsvurderingene til NVE, og viser til at NVE skal prioritere tiltak innenfor IKT-sikkerhet. Gjennomgangen av referater fra etatsstyringsmøter i perioden 2017–2019 viser at NVEs overordnede risiko- og vesentlighetsvurderinger jevnlig har blitt tatt opp i etatsstyringsmøtene, men at risiko og gjennomføring av tiltak som gjelder IKT-sikkerhet i kraftforsyningen, ikke har blitt diskutert.

Siden 2016 har Olje- og Energidepartementet bedt NVE om å utarbeide risiko- og sårbarhetsanalyser (ROS-analyser) for kraftforsyningen. I ROS-analysene som NVE har utført for departementet, er blant annet risiko for IKT-angrep inkludert. Departementet tar stilling til om risiko som avdekkes i ROS-analysene er akseptabel eller om det må iverksettes tiltak for å redusere den. Dersom departementet vurderer at risikoen ikke er akseptabel, skal det iverksettes tiltak i sektoren. Tiltak som departementet vurderer at NVE må følge opp, må eventuelt tas inn i tildelingsbrevet til NVE. Samtidig viser Olje- og energidepartementet til at NVE som beredskapsmyndighet også på eget initiativ kan prioritere å sette i gang tiltak.

Olje- og energidepartementet ga i 2016 Menon Economics i oppdrag å gjennomføre en evaluering av NVE.[91] Evalueringsrapporten konkluderte med at NVE i stor grad hadde nådd de overordnede målene, men at etaten kunne utført oppgavene med større effektivitet, for eksempel ved å styrke den helhetlige styringen på tvers av avdelinger og seksjoner og ved å innføre mer integrerte IKT-systemer. Det ble også avdekket mangler i NVEs interne styringssystemer. NVE har utarbeidet forbedringstiltak basert på evalueringsrapporten og sendt en rapport om oppfølgingen av Menon-rapporten til departementet, med informasjon om hvordan etaten arbeider med ulike tiltak. Departementet ble i et etatsstyringsmøte i 2016 informert om at oppfølgingen av Menon-rapporten inngår i NVEs virksomhetsplaner. Olje- og energidepartementet har jevnlig blitt informert av NVE om det nye IKT-systemet for tilsynsgjennomføring i ulike etatsstyringsmøter. Departementet er blitt gjort kjent med at innføringen av systemet har tatt lang tid, og at det har blitt utsatt ved flere anledninger.

Direktoratet for samfunnssikkerhet og beredskap gjennomførte våren 2020 et tilsyn med Olje- og energidepartementets samfunnssikkerhetsarbeid.[92] I tilsynsrapporten går det fram at tilsynets inntrykk er at det er høy oppmerksomhet på samfunnssikkerhet og beredskap i departementet, men at det er enkelte svakheter. Tilsynet ga avvik når det gjaldt øvelser og evaluering av hendelser og øvelser. Det ble for eksempel vist til at departementet ikke øver målrettet, ikke har en øvingsplan og ikke evaluerer sin egen deltakelse i øvelser eller håndtering av hendelser systematisk.

[90] Avbyråkratiserings- og effektiviseringsreformen (ABE-reformen) har medført at statlige virksomheter har fått årlige kutt i budsjettene på 0,5 prosent.
[91] Menon Economics (2016) *Evaluering av NVE*. Menon-publikasjon nr. 23/2016.
[92] Direktoratet for samfunnssikkerhet og beredskap (2020) *Rapport fra tilsyn med olje- og energidepartementets samfunnssikkerhetsarbeid*.

10 Vurderinger

10.1 NVE har samlet sett ikke i tilstrekkelig grad påsett at det er god beredskap for å håndtere IKT-angrep i kraftforsyningen

Kraftforsyningen er en sentral del av Norges kritiske infrastruktur, og tilgang på elektrisk kraft blir stadig viktigere for å kunne opprettholde normal aktivitet i samfunnet, sikre kritiske samfunnsfunksjoner og opprettholde landets forsvarsevne under kriser og i krig. Kraftforsyningen er som kritisk infrastruktur å anse som særskilt utsatt for etterretning og angrep fra aktører som har som mål å kartlegge sårbarheter for å forberede framtidige sabotasjehandlinger. Undersøkelsen viser at det er økende risiko for at IKT-angrep kan ramme kraftforsyningen og få store konsekvenser for samfunnet.

De viktigste selskapene i kraftforsyningen inngår i KBO (Kraftforsyningens beredskapsorganisasjon). KBO-enhetene er underlagt energiloven og kraftberedskapsforskriften. Undersøkelsen viser at det har vært avdekket svakheter i flere av selskapenes arbeid med å beskytte seg mot trusselen for IKT-angrep. Dette gjelder blant annet internkontrollsystemer, risikovurderinger, beredskapsplaner, leverandøroppfølging, tekniske tiltak for å sikre og overvåke IKT-systemene og gjennomføring av evalueringer og sikkerhets-revisjoner. Undersøkelsen viser at mangel på IKT-sikkerhetskompetanse er en stor utfordring i bransjen.

Olje- og energidepartementet skal legge til rette for en sikker kraftforsyning gjennom god beredskap i kraftforsyningen og har delegert viktige beredskapsoppgaver til NVE. Som en del av målet med å fremme en sikker kraftforsyning skal NVE påse at beredskapen i kraftforsyningen er god og i tråd med gjeldende krav.

Undersøkelsen viser at NVE har skjerpet kravene til IKT-sikkerhet i kraftforsyningen og styrket systemet for å dele informasjon om IKT-sikkerhetshendelser. Undersøkelsen viser samtidig at det er flere svakheter ved NVEs arbeid med IKT-sikkerheten i kraftforsyningen. Hovedfunnene fra undersøkelsen beskrives nærmere nedenfor. Etter vår vurdering har NVE samlet sett lite informasjon om IKT-sikkerhetstilstanden i kraft-forsyningen, og etaten har ikke i tilstrekkelig grad påsett at det er god beredskap for å håndtere IKT-angrep i kraftforsyningen.

10.2 NVE har skjerpet kravene til IKT-sikkerhet i kraftforsyningen, men ikke fulgt opp med tilstrekkelig veiledning

Kontinuerlige endringer gjennom bruk av ny teknologi, skyløsninger, utenlandske leverandører, integrering av systemene og tilkobling av disse systemene til internett øker risikoen for IKT-hendelser i kraftforsyningen. I Meld. St. 25 (2015–2016) *Kraft til endring – Energipolitikken mot 2030* går det fram at styrket IKT-sikkerhet i energiforsyningen krever at NVE kontinuerlig utvikler regelverket når det gjelder IKT-sikkerhet, og at NVE veileder bransjen.

10.2.1 NVE har skjerpet kravene til IKT-sikkerhet i kraftforsyningen

I 2016 begynte NVE å følge opp Lysneutvalgets anbefaling om å gjennomgå regelverket for IKT-sikkerhet i kraftforsyningen. NVE gjennomførte i 2017 og 2018 et omfattende regelverksarbeid som resulterte i den reviderte kraftberedskapsforskriften. Forskriften trådte i kraft fra januar 2019. I den nye forskriften har NVE innført tydeligere krav til sikkerhet i alle digitale systemer, også administrative IKT-systemer, og i AMS. NVE har skjerpet kravene til IKT-sikkerhet i kraftforsyningen, noe som kan bidra til forbedret sikkerhet. Kravene til IKT-sikkerhet i kraftforsyningen i norsk regelverk er strenge sammenlignet med andre europeiske land og andre sektorer i Norge.

10.2.2 NVE har arbeidet med kompetanseutvikling i kraftforsyningen, men det er fortsatt mangel på IKT-sikkerhetskompetanse

Ifølge Meld. St. 38 (2016–2017) *IKT-sikkerhet – Et felles ansvar* er ett tiltak for å bedre IKT-sikkerheten i kraftforsyningen å stimulere til mer ressurssterke fagmiljøer innenfor IKT-sikkerhet.

I risiko- og vesentlighetsvurderingene for årene 2017–2020 trekker NVE fram at digitaliseringen har ført til kompetanseutfordringer, og at både NVE og bransjen er avhengige av å styrke kompetansen på området. Undersøkelsen viser at om lag halvparten av IKT-sikkerhetskoordinatorene mener at for lite IKT-kompetanse

i selskapet er en av årsakene til at det kan være vanskelig å etterleve kravene. For å bidra til kompetanseheving både internt og eksternt har NVE gjennomført en rekke FoU-prosjekter som belyser ulike sider ved IKT-sikkerheten. NVE har også bidratt til utdanningstilbud, kurs og seminarer om IKT-sikkerhet for ansatte i kraftforsyningen. I tillegg deltar NVE i ulike samarbeidsfora for å holde seg oppdatert på området, og én av NVEs ansatte tar doktorgrad i sikkerhet i driftskontrollsystemer. Etter vår vurdering er det positivt at NVE har arbeidet med kompetanseutvikling, men mangel på IKT-sikkerhetskompetanse er fortsatt en stor utfordring for IKT-sikkerheten i kraftforsyningen.

10.2.3 NVE har ikke gitt tilstrekkelig veiledning til selskapene

NVE har etter forvaltningsloven en veiledningsplikt overfor selskapene, slik at de har mulighet til å ivareta interessene sine på best mulig måte. Flere av de nye kravene til IKT-sikkerhet er funksjonsbaserte. Det vil si at det er selskapene selv som skal vurdere hvilke sikkerhetsløsninger som gir tilstrekkelig IKT-sikkerhet ut fra egne risikovurderinger. Funksjonsbaserte krav gir større fleksibilitet til å følge den teknologiske utviklingen og kan tilpasses de enkelte virksomhetenes verdier og risiko, men stiller samtidig høyere krav til kompetanse og kapasitet i selskapene.

Undersøkelsen viser at det er vanskelig for mange av selskapene å forstå kravene og hva NVE anser som «godt nok». Manglende forståelse av funksjonsbaserte krav kan være én årsak til manglende etterlevelse av kravene. Siden flere av kravene i regelverket er funksjonsbaserte, er det derfor nødvendig at NVE tilbyr tilstrekkelig veiledning i regelverksforståelse og gjennom tilsyn vurderer om løsningene selskapene har valgt, tilfredsstiller regelverkets krav. NVE gir selskapene i kraftsektoren veiledning om hvordan de skal forstå krav i regelverket, gjennom skriftlige veiledere, kurs og seminarer, ved tilsyn og i direkte kontakt med selskapene. Undersøkelsen viser at selskapene i hovedsak er fornøyde med veiledningen de får fra NVE, men at mange av dem har behov for mer veiledning. NVE laget en foreløpig veileder til de nye kravene i kraftberedskapsforskriften, men den endelige veilederen ble forsinket, og ble først publisert i desember 2020. Undersøkelsen viser at NVE bruker mye ressurser til å svare på henvendelser fra enkeltselskaper uten at de har hatt et system for å dele denne veiledningen med resten av bransjen. NVE har til nå gjennomført få IKT-sikkerhetstilsyn etter det nye regelverket. Dermed er det lite forvaltningspraksis som viser NVEs vurderinger av hva som er godt nok for å etterleve regelverket. NVE har heller ikke hatt et system for å dele forvaltningspraksisen ved tilsyn av enkeltselskaper med resten av bransjen. Den nye veilederen til kraftberedskapsforskriften inneholder informasjon om NVEs forvaltningspraksis på området. Slik informasjon vil også bli inkludert gjennom løpende oppdateringer av den digitale veilederen.

Etter vår vurdering har ikke NVE fulgt opp regelverksendringene med tilstrekkelig veiledning til selskapene.

10.3 Det er svakheter ved NVEs tilsyn med IKT-sikkerhet i kraftforsyningen

NVE er i henhold til energiloven og kraftberedskapsforskriften ansvarlig for å føre kontroll med at bestemmelsene i loven og forskriften overholdes.

10.3.1 NVE har gjennomført få IKT-sikkerhetstilsyn

Det er om lag 170 KBO-enheter i kraftforsyningen. NVE har de siste seks årene gjennomført om lag fem IKT-sikkerhetstilsyn hvert år. I perioden 2017–2019 førte NVE IKT-sikkerhetstilsyn med om lag halvparten av selskapene som har de viktigste driftskontrollsystemene. NVE har i liten grad gjennomført tilsyn med de øvrige selskapene i kraftforsyningen. Undersøkelsen viser at flere planlagte IKT-sikkerhetstilsyn ble utsatt i perioden 2017–2019 på grunn av kapasitetsutfordringer. NVE oppgir at de ikke har oversikt over IKT-sikkerheten i selskapene de ikke har ført tilsyn med. Dette innebærer at NVE i undersøkelsesperioden kun har informasjon om IKT-sikkerhetstilstanden fra tilsyn med en liten andel av selskapene i kraftforsyningen.

10.3.2 NVEs tilsynsmetodikk avdekker i liten grad den faktiske IKT-sikkerhetstilstanden i selskapene

NVE har benyttet den samme metodikken for IKT-sikkerhetstilsyn i over ti år. Metodikken NVE bruker er tillitsbasert og avdekker om selskapene har systemer for internkontroll. Metodikken gir lite informasjon om hvorvidt internkontrollsystemene fungerer i praksis, og om selskapenes IKT-systemer er godt nok sikret. De tre selskapene som inngikk i vår caseundersøkelse, hadde svakheter som selskapenes egne kontrollsystemer ikke hadde fanget opp, og som NVE heller ikke avdekket gjennom sine tilsynsmetoder.

Etter vår vurdering avdekker NVE i liten grad den faktiske IKT-sikkerhetstilstanden i selskapene med sin tilsynsmetodikk. NVE har gjennomført et prosjekt for å vurdere om de skal videreutvikle tilsynsmetodene de bruker ved IKT-sikkerhetstilsyn. Etaten har også vurdert om det kan være aktuelt å gjøre mer omfattende undersøkelser av enkelte tema framover.

10.3.3 Det er svakheter ved NVEs risikovurderinger ved valg av tema og selskaper for IKT-sikkerhetstilsyn

I St.meld. nr. 19 (2008–2009) *Ei forvaltning for demokrati og fellesskap* går det fram at tilsynsvirksomhet skal ta utgangspunkt i der det er størst risiko, og der sjansene for reduksjon av risiko er størst. NVE har i sine planer lagt til grunn at tema og selskaper ved tilsyn skal velges på bakgrunn av risiko og vesentlighet.

NVE gjennomfører tilsyn innenfor mange ulike fagområder. Risikobasert planlegging av tilsyn tilsier at NVE skal vurdere hvilke tema det er viktigst å føre tilsyn med. Undersøkelsen viser at NVE ikke dokumenterer begrunnelsen for de temaene de velger for tilsynene, eller hvor mange tilsyn de skal gjennomføre innenfor ulike temaer. Undersøkelsen viser at valg av tema og omfang innenfor ulike tilsyn i stor grad henger sammen med hvilke ressurser og kompetanse NVE har til rådighet i de ulike seksjonene, og at utvalget ikke baseres på dokumenterte risikovurderinger hvor alle tilsynstemaer i NVE inngår. Ettersom kapasiteten på IKT-sikkerhetskompetanse har økt lite i undersøkelsesperioden, har antall IKT-sikkerhetstilsyn heller ikke økt. Dette til tross for at risikoen for IKT-angrep er vektlagt i NVEs overordnede risikovurderinger, og at IKT-sikkerhet i kraftforsyningen er trukket fram som et prioritert område i NVEs strategier og planer. Etter vår vurdering har NVE i liten grad basert valg av tema for tilsynene på risikovurderinger og dermed ikke rettet tilsynene inn mot områder der de kunne hatt størst risikoreduserende effekt.

Selskapenes driftskontrollsystemer er klassifisert ut fra hvor viktige de er for kraftforsyningen, og sier derved noe om hvor vesentlige selskapene er for kraftforsyningen. NVEs oversikt over klassifiseringen av selskapenes driftskontrollsystemer er imidlertid ufullstendig, noe som svekker grunnlaget NVE har for å velge ut tilsynsobjekter basert på vesentlighet. NVE oppgir at de foretar flest tilsyn blant de viktigste selskapene. Undersøkelsen viser at NVE velger ut tilsynsobjekter til IKT-sikkerhetstilsyn i hovedsak basert på frekvens og vesentlighet. NVE dokumenterer ikke begrunnelsen for valg av tilsynsobjekter.

Gode risiko- og vesentlighetsvurderinger krever at tilsynsorganet har god kjennskap til området det føres tilsyn med.[93] Det tilsier at områdeovervåking bør ligge til grunn for risiko- og vesentlighetsvurderingen. Undersøkelsen viser at NVE har lite kunnskap om svakheter og dermed om indikasjoner på risiko i selskapene. Slik kunnskap kunne ha vært benyttet til å foreta risikobaserte valg av tilsynsobjekter. Seksjonen som har ansvar for arbeidet med IKT-sikkerhet i kraftforsyningen, har i undersøkelsesperioden bare brukt tilsyn som metode for å kontrollere IKT-sikkerheten i kraftforsyningen, mens andre seksjoner i NVE og andre tilsynsmyndigheter også bruker innrapportering fra selskapene som en metode for å skaffe seg mer systematisk informasjon om tilstanden i selskapene. Selv om NVE har lite informasjon om IKT-sikkerheten i selskaper de ikke har ført IKT-tilsyn med, får de noen indikasjoner på svakheter i selskapene, for eksempel gjennom tilsyn med andre tema, gjennom direkte kontakt med selskapene i veiledningsarbeidet eller gjennom selskapenes innrapportering av hendelser. Undersøkelsen viser at NVE i liten grad bruker slik informasjon til å velge tilsynsobjekter.

NVE retter tilsynene inn mot selskapene som er viktigst for kraftforsyningen, og der konsekvensene av et IKT-angrep vil være størst. NVE vurderer imidlertid ikke hvilke av selskapene det er størst risiko for å avdekke avvik hos. Etter vår vurdering kunne NVE effektivisert og målrettet tilsynsvirksomheten hvis de hadde samlet og systematisert mer informasjon om indikasjoner på svak etterlevelse i selskapene og lagt denne informasjonen til grunn for valg av tilsynsobjekter.

10.4 Svakheter ved NVEs arbeid med overvåking, varsling og beredskap ved IKT-hendelser

10.4.1 NVE har styrket systemet for å dele informasjon om IKT-sikkerhetshendelser i kraftforsyningen

NVE er beredskapsmyndighet og sektorvist responsmiljø for IKT-sikkerhetshendelser i kraftsektoren. NVE har fra juni 2019 satt ut oppgaven med å avdekke og dele kunnskap om sårbarheter og trusler med

[93] St.meld. nr. 19 (2008–2009) *Ei forvaltning for demokrati og fellesskap.*

selskapene til KraftCERT, som skal støtte NVE i rollen som sektorvist responsmiljø. KraftCERT er et privat selskap som er opprettet av store aktører i kraftforsyningen, og som siden 2014 har hjulpet medlems-selskaper med å forebygge og håndtere IKT-sikkerhetshendelser. Fra 2019 stilte NVE nye krav til selskapenes varsling og rapportering av IKT-hendelser. Formålet med kravene var å gi KraftCERT et bredere grunnlag for å dele informasjon om trusler og sårbarheter med selskapene, og å gi både KraftCERT og NVE en bedre oversikt over trusselbildet. Etter vår vurdering har NVE lagt til rette for å styrke delingen av informasjon om trusler, sårbarheter og IKT-sikkerhetshendelser i kraftforsyningen.

10.4.2 Mange selskaper får ikke KraftCERTs jevnlige varsler om trusler og sårbarheter

KraftCERT har fra 2019 blitt tildelt midler fra staten for å ivareta oppgaver med å avdekke og dele kunnskap om sårbarheter og trusler, men er fortsatt i hovedsak finansiert av medlemsselskapene. Om lag 35 av 170 KBO-enheter er medlemmer av KraftCERT. For at medlemmene skal få merverdi av medlemskapet og fortsette å betale medlemsavgiften, har KraftCERT delt mer informasjon med dem enn med øvrige selskaper. Bare de mest alvorlige varslene, om lag fem varsler per år, har vært sendt til samtlige selskaper. I tillegg har en del mindre selskaper fått videresendt samtlige varsler gjennom avtale med Nettalliansen eller konsulentselskaper. KraftCERT anslår at om lag 70 selskaper bare har fått de mest alvorlige varslene. Dette betyr at mange av selskapene i kraftforsyningen ikke får jevnlige varsler om sårbarheter og trusler med anbefalinger om tiltak som kan forbedre IKT-sikkerheten i selskapene.

10.4.3 Svakheter i selskapenes evne til å oppdage IKT-hendelser, uklare varslingsrutiner og svak kultur for å varsle fører til underrapportering til NVE og KraftCERT

NVE skal avklare rutiner og krav for deling av hendelses- og risikoinformasjon og ha oversikt over statusen og utviklingen i sikkerhetstilstanden i kraftforsyningen. Kraftberedskapsforskriften stiller krav til selskapenes varsling av IKT-sikkerhetshendelser til NVE og KraftCERT.

Undersøkelsen viser at det skjer mange IKT-sikkerhetshendelser i kraftselskapene som ikke rapporteres. Underrapporteringen gjelder i hovedsak mindre alvorlige angrep mot administrative IKT-systemer, mens ekstraordinære situasjoner som skal varsles NVE i stor grad varsles. Undersøkelsen viser at det kan være flere årsaker til underrapportering:

- *Uklare varslingsrutiner:* Mange selskaper mangler kriterier for varsling av hendelser, og det har vært uklart hvilke type IKT-hendelser de skal varsle om til NVE og KraftCERT.
- *Svakheter i kraftforsyningens systemer for å oppdage hendelser:* Det er avdekket svakheter i systemene selskapene har for å overvåke og logge IKT-sikkerhetshendelser. KraftCERT anbefaler å innføre et felles sensornettverk i bransjen. Dette kan fange opp mer uønsket trafikk.
- *Svak kultur for å varsle hendelser:* Undersøkelsen viser at selskapene gjerne avventer å varsle om hendelser fordi de ønsker å løse problemet internt før de deler informasjonen med andre. Dersom selskapene klarer å få situasjonen under kontroll, er det heller ikke sikkert at de vil rapportere om hendelsen i ettertid.

Undersøkelsen viser at det er viktig at også mindre alvorlige angrep mot administrative IKT-systemer oppdages for å få stoppet angripere som prøver å benytte disse systemene til å få tilgang til driftskontrollsystemene og ramme kraftforsyningen. Tidligere hendelser har vist at angrep har startet i administrative systemer, og at angripere har vært inne i nettverket i flere måneder før de har begynt å innhente informasjon eller gjennomført forstyrrende handlinger. Det er også viktig at slike hendelser rapporteres slik at andre selskaper kan iverksette tiltak for unngå lignende hendelser. Mer rapportering om IKT-hendelser og sårbarheter i systemer vil gi mer informasjon som kan deles i sektoren og brukes til å innrette tiltak som kan forebygge nye hendelser. Undersøkelsen viser at NVE så langt i liten grad har hatt oversikt over mindre alvorlige IKT-hendelser. Kravet fra 2019 om at alle hendelser skal varsles til KraftCERT, legger til rette for at KraftCERT og NVE skal få mer informasjon om slike hendelser.

Etter vår vurdering fører svakheter ved selskapenes evne til å oppdage IKT-hendelser og underrapportering fra selskapene til at NVE og KraftCERT ikke får tilstrekkelig informasjon som gjør at de kan vurdere beredskapen ved pågående hendelser, oversikt over trusselbildet i sektoren eller informasjon om sårbarheter i systemer og leverandører som kan brukes til å innrette tiltak som kan forebygge nye hendelser.

10.4.4 NVE har lite erfaring med å håndtere IKT-angrep som rammer kraftforsyningen, og har ikke et oppdatert beredskapsplanverk

NVE har som beredskapsmyndighet ansvaret for å samordne arbeidet med forebyggende sikkerhet og beredskap i kraftforsyningen. NVE skal lede landets kraftforsyning dersom situasjonen blir svært alvorlig. NVE skal ha beredskapsplaner for håndtering av større hendelser, sikkerhetspolitiske kriser og krig. NVE skal jevnlig gjennomføre øvelser med et innhold og omfang som lar dem vedlikeholde og utvikle kompetansen slik at de er i stand til å håndtere alle aktuelle ekstraordinære situasjoner.

NVE har et beredskapsplanverk som inkluderer alvorlige IKT-hendelser, og dette skal sikre at kriser og ekstraordinære situasjoner håndteres effektivt. Beredskapsplanverket skal bygge på NVEs egne risiko- og sårbarhetsanalyser (ROS), det nasjonale risikobildet og evaluering av hendelser og øvelser. NVEs planverk har imidlertid ikke vært oppdatert siden 2017 og er dermed ikke tilpasset nyere trusselvurderinger, ROS-analyser, hendelser og øvelser. I NVEs ROS-analyser er også leverandørers IKT-sikkerhet og beredskaps-kapasitet tillagt stor betydning, uten at det går fram av beredskapsplanverket hvordan deres rolle vil være under et IKT-angrep.

Det har ikke forekommet IKT-hendelser av en slik alvorlighetsgrad at NVEs beredskapsplanverk har vært tatt i bruk, og NVE har dermed heller ikke evaluert håndteringen av alvorlige IKT-hendelser eller oppdatert beredskapsplanverket ut fra slike hendelser. NVE har imidlertid erfaring med å håndtere alvorlige hendelser som ikke gjelder IKT-sikkerhet, og har evaluert slike hendelser. Disse hendelsene har imidlertid ikke gitt NVE erfaring med å bruke tiltakskortene for IKT-hendelser.

NVE deltok på to større IKT-øvelser i perioden 2017–2019, «Black Screen 1» og «Black screen 2». Den interne evalueringen etter den første av disse øvelsene viser at det ble trent på samhandling med KraftCERT og NSM. Øvelsen gjaldt angrep mot nordiske systemoperatørers driftskontrollsystemer, og andre selskaper eller leverandører i kraftforsyningen enn Statnett deltok ikke i øvelsen. I NVEs interne evaluering av øvelsen står det at det er viktig å ha tett dialog med KraftCERT og NSM for å forstå det som skjer, og det vises til at KraftCERT er en viktig ressurs ved hendelseshåndtering. Tiltakene NVE ønsket å implementere etter øvelsen, gikk blant annet ut på å videreutvikle den gode relasjonen med KraftCERT og øve mer på IKT-angrep. Undersøkelsen viser at NVE har deltatt i nordiske IKT-øvelser, men at etaten i liten har grad øvd på hendelser som er beskrevet i egne tiltakskort. NVE har heller ikke en oppdatert plan for øvelser.

Undersøkelsen viser at NVE har lite erfaring med å håndtere IKT-angrep som rammer kraftforsyningen, og at etaten ikke har et oppdatert beredskapsplanverk eller en oppdatert plan for øvelser. Undersøkelsen viser også at NVE ikke har øvd på IKT-angrep mot kraftforsyningen sammen med selskaper og leverandører, med unntak av Statnett. Samlet sett mener vi dette gjør at beredskapsorganisasjonen i NVE ikke har fått trent nok på å håndtere IKT-angrep mot kraftforsyningen.

10.5 Oppfølgingen av leverandørene er mangelfull til tross for at de har stor betydning for IKT-sikkerheten i kraftforsyningen

Undersøkelsen viser at IKT-sikkerheten og beredskapen i kraftforsyningen i stor grad avhenger av leverandører. Mange av selskapene i kraftforsyningen har helt eller delvis tjenesteutsatt driften av IKT-systemer, og for noen av selskapene gjelder dette også driftskontrollfunksjoner. Undersøkelsen viser at en av hovedårsakene til at det er vanskelig for selskapene å etterleve kravene til IKT-sikkerhet i kraftberedskapsforskriften, er at mange av selskapene mangler IKT-sikkerhetskompetanse, og at det er utfordrende å sikre at leverandørene deres har god nok IKT-sikkerhet. Undersøkelsen viser at flere selskaper i liten grad stiller tydelige krav til IKT-sikkerhet i avtaler med leverandørene og sjelden gjennomfører sikkerhetsrevisjoner for å sikre at avtalene følges. Mange av selskapene i kraftbransjen er små, mens mange leverandører er store multinasjonale selskaper. Dette kan gjøre det utfordrende for selskapene å få gjennomslag for sikkerhetskrav ved kontraktsinngåelse og å gjennomføre sikkerhets-revisjoner.

NVE får i hovedsak informasjon om leverandørenes IKT-sikkerhet gjennom veiledning og tilsyn med KBO-enhetene. I tilsyn avdekker NVE om selskapene har rutiner og systemer for å følge opp sikkerheten i anskaffelser, og NVE har gitt flere avvik til selskaper for manglende gjennomføring av sikkerhetsrevisjon. Ved tilsyn med selskaper som har tjenesteutsatt store deler av driften av IKT-systemer, består NVEs informasjonsgrunnlag i stor grad av informasjonen selskapene selv har om leverandørenes arbeid med IKT-

sikkerhet. Undersøkelsen viser at mange selskaper har mangelfull informasjon og oppfølging av leverandørenes arbeid med IKT-sikkerhet.

Mange selskaper i kraftforsyningen benytter seg av de samme leverandørene av IKT-systemer. Mens ett enkelt nettselskaps bortfall av evnen til å levere strøm i distribusjons- eller regionalnettet bare rammer et avgrenset område, kan et vellykket angrep mot en leverandør eller et system som er utbredt i kraftforsyningen, ramme flere selskaper og større områder. Mange selskaper er svært avhengige av sine leverandører for å håndtere hendelser og gjenopprette driftskontrollsystemet, og det er risiko for at leverandørene ikke har dimensjonert beredskapen for hendelser som rammer flere selskaper samtidig. NVE har ikke utpekt noen leverandører som KBO-enheter, og leverandører med virkeområde utenfor Norge kan ikke underlegges norsk lovgivning.

NVE kan følge opp leverandører med virkeområde i Norge for eventuelle brudd på taushetsplikten for kraftsensitiv informasjon, men kan ikke selv føre tilsyn med leverandørenes IKT-sikkerhet eller beredskapskapasitet. Leverandører er ikke pliktig til å varsle NVE om hendelser og kan heller ikke pålegges oppgaver av NVE ved ekstraordinære situasjoner. Ved en beredskapssituasjon er det dermed risiko for at NVE ikke har tilstrekkelig informasjon om situasjonen og kraftforsyningens evne til å håndtere hendelsen og gjenopprette rammede funksjoner. Ettersom NVE ikke kan føre tilsyn med leverandørenes IKT-sikkerhet, får de ikke informasjon utover det som avdekkes i NVEs tilsyn med enkeltselskaper, eller gjennom informasjon om enkeltselskapers sikkerhetsrevisjoner av leverandører. Dette gjelder for eksempel leverandørenes evne til å håndtere hendelser som rammer mange selskaper på likt.

Etter vår vurdering utgjør selskapenes avhengighet og mangelfulle oppfølging av leverandører, og det at NVE har lite informasjon om leverandørenes IKT-sikkerhet og beredskap en risiko for IKT-sikkerheten i kraftforsyningen.

10.6 NVEs styring og oppfølging av arbeidet med IKT-sikkerhet i kraftforsyningen er svak

10.6.1 NVE har ikke sørget for nok ressurser til arbeidet med IKT-sikkerhet i kraftforsyningen

I Meld. St. 25 (2015-2016) *Kraft til endring – Energipolitikken mot 2030* framheves det at kompleksiteten i energiforsyningen har økt og at økt bruk av IKT gir risiko for at antall uønskede IKT-hendelser vil kunne øke. Det framgår av energimeldingen og Meld. St. 38 (2016–2017) *IKT-sikkerhet – Et felles ansvar* at styrket IKT-sikkerhet i energiforsyningen krever at NVE styrker sitt arbeid, blant annet utvikler regelverket, styrker tilsyn og veiledning med IKT-sikkerhet og stimulerer til større og mer ressurssterke fagmiljøer innen IKT-sikkerhet. Det framheves i energimeldingen at regjeringen setter arbeidet med IKT-sikkerhet høyt, og støtter opp om NVEs prioritering av IKT-sikkerhet i kraftsektoren.

NVE framhever i sine strategier, risikovurderinger og virksomhetsplaner at arbeidet med IKT-sikkerhet i kraftforsyningen er et prioritert område. Omfanget av NVEs oppgaver i arbeidet med IKT-sikkerhet i kraftforsyningen har økt i takt med digitaliseringen. NVEs samlede budsjettmidler har ikke økt i undersøkelsesperioden så prioritering av arbeidet med IKT-sikkerhet i kraftforsyningen må derfor skje med intern omdisponering av midler. NVE har ikke overfor departementet gitt uttrykk for at de trenger økte ressurser til arbeidet, utover midlene til å dekke oppgavene som er satt ut til KraftCERT.

NVE har økt antall stillinger med IKT-sikkerhetskompetanse i beredskapsseksjonen fra én til tre fra 2016 til 2018. Den reelle kapasiteten i seksjonen med denne kompetansen har i gjennomsnitt vært på om lag to årsverk i perioden 2017–2019. Få ansatte innebærer en større sårbarhet ved fravær og uforutsette hendelser. NVE har de siste årene brukt mye av kapasiteten på området til å revidere kraftberedskapsforskriften og veilede enkeltselskaper i de nye kravene. Flere av NVEs oppgaver innenfor arbeidet med IKT-sikkerhet i kraftforsyningen har dermed blitt utsatt. Dette gjelder blant annet gjennomføringen av flere IKT-tilsyn, utarbeidelsen av en endelig skriftlig veileder til kraftberedskapsforskriften og avklaringer om et nytt regime for varsling og deling av sårbarheter og IKT-sikkerhetshendelser. Etter vår vurdering har NVE ikke sørget for nok ressurser til arbeidet med IKT-sikkerhet i kraftforsyningen.

10.6.2 NVE har ikke sørget for at de har de verktøyene som trengs for å styre og følge opp arbeidet med IKT-sikkerhet i kraftforsyningen

Det framgår av økonomireglementet at NVE skal fastsette mål og resultatkrav og sikre tilstrekkelig styringsinformasjon og beslutningsgrunnlag for å følge opp aktiviteter og resultater av eget arbeid. Et av NVEs hovedmål fra Olje- og energidepartementet er å fremme en sikker kraftforsyning, og for å nå målet skal NVE blant annet påse at beredskapen er god og i tråd med gjeldende krav. NVE skal rapportere om gjennomførte tiltak og hvordan de bidrar til å nå hovedmålet.

Målene som er satt av departementet, gjenspeiles i NVEs strategier og virksomhetsplaner. NVE har ikke operasjonalisert målene og styringsparameterne i vurderingskriterier som kan brukes i styringen og oppfølgingen av arbeidet med IKT-sikkerhet i kraftforsyningen. NVE har heller ikke identifisert hvilken informasjon som er nødvendig for å kunne vurdere sikkerheten i kraftforsyningen, og hvordan arbeidet med IKT-sikkerhet bidrar til dette. I årsrapporten rapporterer NVE om gjennomførte aktiviteter og tiltak, men i liten grad om resultater av tiltakene og hvordan de har bidratt til å fremme en sikker kraftforsyning. Det er lite intern rapportering på oppgavegjennomføring og måloppnåelse i NVE gjennom året. NVE gjennomfører heller ikke systematiske evalueringer av eget arbeid som kan brukes i styringen og oppfølgingen av arbeidet med IKT-sikkerhet i kraftforsyningen. NVE evaluerer for eksempel ikke tilsynene systematisk internt for å vurdere om metodikken, gjennomføringen eller tilsynsrutinene kan forbedres.

Virksomhetsplanen til beredskapsseksjonen angir planlagt ressursbruk for en del hovedoppgaver som faller inn under arbeidet med IKT-sikkerhet i kraftforsyningen, som tilsyn og regelverksutvikling. Mange av oppgavene som faller inn under IKT-sikkerhetsarbeidet inngår imidlertid ikke i seksjonens virksomhetsplan, slik at denne ikke viser det reelle ressursbehovet for dette arbeidet. Det oppstår derfor mange oppgaver gjennom året som NVE ikke har planlagt og satt av ressurser til. På grunn av få ansatte med IKT-sikkerhetskompetanse blir mange av de planlagte oppgavene utsatt. NVE har ikke et ressursstyringsverktøy som kan brukes til å sammenligne faktisk ressursbruk med planlagt ressursbruk, og som kan gi erfaringstall i planleggingsarbeidet. Etter vår vurdering gjør manglende informasjon om ressursbruk på ulike aktiviteter det vanskelig for de ulike ledernivåene å styre og prioritere mellom NVEs mange ulike oppgaver.

NVE har i undersøkelsesperioden hatt mangelfulle IKT-systemer for å dokumentere valg av tema og tilsynsobjekter og for å sikre at rutiner for gjennomføring av tilsyn blir fulgt, og at avvik som avdekkes i tilsynene, blir fulgt opp. NVE har heller ikke hatt systemer for å sikre at informasjon fra gjennomførte tilsyn brukes som en del av områdeovervåkingen som skal brukes til valg av framtidige tilsyn, regelverksarbeid og veiledning. NVE har nylig tatt i bruk en ny applikasjon for tilsyn som gjør det mulig å forbedre gjennomføringen av tilsyn og oppfølgingen av frister og avvik. Det nye systemet vil imidlertid ikke kunne brukes i den overordnede planleggingen av tilsyn eller til å dokumentere risikobasert valg. Systemet har heller ikke blitt tatt i bruk for å hente ut rapporter til interne analyseformål som en del av områdeovervåkingen, men NVE mener dette vil bli mulig når systemet har vært i bruk en stund. NVE mottar rapportering når IKT-hendelser er avsluttet hos selskapene. Denne rapporteringen skal gi NVE informasjon om selskapenes egen evaluering og erfaringer. NVE registrerer hendelser i flere systemer og regneark som er lite tilrettelagt for oppfølging og læring av hendelser, for interne analyseformål eller som grunnlag for valg av tilsyn. Etter vår vurdering er det svakheter ved NVEs systemer for planlegging og oppfølging av tilsyn og for oppfølging av rapporterte hendelser. Deler av dette kan bli bedre med det nye systemet.

Etter vår vurdering har NVE samlet sett ikke sørget for at de har de verktøyene som trengs for å styre og følge opp arbeidet med IKT-sikkerhet i kraftforsyningen.

10.6.3 NVEs grunnlag for å vurdere statusen og utviklingen i IKT-sikkerhetstilstanden i kraftforsyningen er mangelfullt

I henhold til tildelingsbrevet skal NVE årlig gi Olje- og energidepartementet en vurdering av statusen og utviklingen i sikkerhetstilstanden i kraftforsyningen. NVE har få kilder for å følge med på denne utviklingen. NVE har utarbeidet to tilstandsvurderinger som samler NVEs informasjon om sikkerhetstilstanden, i 2017 og 2019, i tillegg til en oversikt over uønskede hendelser i kraftforsyningen. Dokumentene baserer seg i hovedsak på statistikk om gjennomførte tilsyn og innrapporterte hendelser og avbruddsstatistikk. Undersøkelsen viser at hovedkildene for NVEs informasjon om IKT-sikkerhetstilstanden er mangelfulle og ikke gir et fullstendig bilde av statusen og utviklingen i IKT-sikkerhetstilstanden:

- NVE har gjennomført få IKT-sikkerhetstilsyn, og tilsynsmetodikken avdekker i liten grad den faktiske IKT-sikkerhetstilstanden i selskapene.

- NVEs informasjon om IKT-sikkerhetshendelser er mangelfull.
- Avbruddstatistikken gir i liten grad informasjon om hvorvidt IKT-sikkerheten er tilstrekkelig for å hindre avbrudd i kraftforsyningen i krisesituasjoner.

I tillegg til tilstandsvurderingene har NVE utarbeidet ROS-analyser og overordnede risikovurderinger. Her trekker NVE fram at det er risiko for at IKT-angrep kan ramme kraftforsyningen, og at NVE mangler kunnskap om selskapenes IKT-sikkerhet på flere områder. I risikovurderingene for 2017 og 2018 trekker NVE fram risikoen for at etaten ikke har tilstrekkelig grunnlag for å vurdere status og risiko i beredskapen og forsyningssikkerheten.

Det er ifølge NVE kjent at det skjer en rekke IKT-angrep i kraftforsyningen. På grunn av underrapportering og uklarheter i varslingsrutiner er det imidlertid mangler i statistikken. Ifølge NVE betyr ikke nødvendigvis fravær av hendelser god sikkerhet fordi det kan skyldes at hendelser ikke blir oppdaget.

Etter vår vurdering er NVEs grunnlag for å vurdere statusen og utviklingen i IKT-sikkerhetstilstanden i kraftforsyningen samlet sett mangelfullt. Dette innebærer at NVE i liten grad har informasjon om resultatene av eget arbeid som kan brukes til å styre arbeidet og til å iverksette tiltak som er nødvendige for å nå målet om å fremme en sikker forsyning av kraft uten avbrudd, også i krisesituasjoner.

10.7 Olje- og energidepartementet sikrer seg ikke god nok styringsinformasjon om IKT-sikkerhetstilstanden i kraftforsyningen og resultatene av NVEs arbeid med IKT-sikkerhet i kraftforsyningen

Olje- og energidepartementet skal legge til rette for en sikker kraftforsyning gjennom god beredskap. Departementet har delegert viktige beredskapsoppgaver til NVE. Olje- og energidepartementet skal fastsette mål- og resultatkrav for NVE og følge opp at målene nås. NVEs arbeid med IKT-sikkerhet i kraftforsyningen ligger under hovedmålet om å fremme en sikker kraftforsyning og delmålet om å påse at beredskapen i energiforsyningen er god og i tråd med gjeldende krav.

Olje- og energidepartementet er lite tydelig når det gjelder hvilken innsats og hvilke resultater som skal til for at NVE når sitt mål om å fremme en sikker kraftforsyning. NVEs rapportering til Olje- og energidepartement om arbeidet med IKT-sikkerhet inneholder i hovedsak beskrivelser av tiltak og aktiviteter som er gjennomført. Departementet får imidlertid lite informasjon om resultatene av NVEs arbeid med IKT-sikkerhet og har derfor lite grunnlag for vurdere måloppnåelsen og følge opp at målene nås.

NVE rapporterer gjennom avbruddsstatistikk at forsyningssikkerheten i Norge er svært høy. Så langt har det ikke vært avbrudd i strømforsyningen på grunn av IKT-angrep. Dette gir NVE begrenset incentiv til å prioritere arbeidet med å redusere risikoen for at IKT-angrep skal ramme kraftforsyningen, sammenlignet med arbeid som mer løpende virker inn på forsyningssikkerheten, og som påvirker avbruddstatistikken, som generell beredskap og fysisk vedlikehold. Fravær av brudd i strømforsyningen betyr imidlertid ikke nødvendigvis at IKT-sikkerheten i kraftforsyningen er god, slik NVE skal påse. Selv om kraftforsyningen er lite utsatt i fredstid, øker faren for aksjoner mot kraftforsyningen i kriser, og i krig er kraftforsyningen et klart utsatt mål. Statistikken for leveringspålitelighet i fredstid reflekterer dermed ikke risikoen for et alvorlig IKT-angrep i krisesituasjoner og krig. Undersøkelsen viser at det er svakheter i kildene NVE har for å rapportere om IKT-sikkerhetstilstanden i kraftforsyningen, og at Olje- og energidepartementet i liten grad har etterspurt mer informasjon. Etter vår vurdering har Olje- og energidepartementet ikke sikret seg god nok styringsinformasjon om resultatene av NVEs arbeid med IKT-sikkerhet i kraftforsyningen og om beredskapen i kraftforsyningen for å forebygge og håndtere IKT-angrep.

11 Referanseliste

Lover og forskrifter

- *Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m.* (energiloven).
- *Forskrift om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m.* (energilovforskriften).
- *Forskrift om sikkerhet og beredskap i kraftforsyningen* (kraftberedskapsforskriften) av 1. januar 2019, som erstattet *Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen* (beredskapsforskriften) av 1. januar 2013.
- *Forskrift om delegering av myndighet etter energiloven til Norges vassdrags- og energidirektorat.*
- *Forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv.* (forskrift om kraftomsetning og nettjenester, også kalt avregningsforskriften).
- *Forskrift om systemansvaret i kraftsystemet.*
- *Lov om behandlingsmåten i forvaltningssaker* (forvaltningsloven).

Stortingsdokumenter

Proposisjoner til Stortinget

- Prop. 1 S (2017−2018) Olje- og energidepartementet.
- Prop. 1 S (2018−2019) Olje- og energidepartementet.
- Prop. 1 S (2019−2020) Olje- og energidepartementet.
- Prop. 1 S (2020−2021) Olje- og energidepartementet.

Stortingsmeldinger

- St.meld. nr. 19 (2008–2009) *Ei forvaltning for demokrati og fellesskap.*
- Meld. St. 25 (2015–2016) *Kraft til endring – Energipolitikken mot 2030.*
- Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn – Samfunnssikkerhet.*
- Meld. St. 38 (2016–2017) *IKT-sikkerhet − Et felles ansvar.*

Innstillinger til Stortinget

- Innst. S. nr. 321 (2008–2009) *Innstilling fra kommunal- og forvaltningskomiteen om ei forvaltning for demokrati og fellesskap.*
- Innst. 401 S (2015–2016) *Innstilling fra energi- og miljøkomiteen om Kraft til endring – Energipolitikken mot 2030.*
- Innst. 187 S (2017–2018) *Innstilling fra Justiskomiteen om IKT-sikkerhet. Et felles ansvar.*

Regelverk og instrukser

- *Reglement for økonomistyring i staten* (økonomireglementet) og *Bestemmelser om økonomistyring i staten* (økonomibestemmelsene), fastsatt 12. desember 2003.
- *Bevilgningsreglementet*, vedtatt av Stortinget 26. mai 2005.
- *Instruks for departementenes arbeid med samfunnssikkerhet* (samfunnssikkerhetsinstruksen).
- *Instruks om utredning av statlige tiltak* (utredningsinstruksen).
- *Instruks for økonomi- og virksomhetsstyring i Norges vassdrags- og energidirektorat*, fastsatt 1. januar 2016 med endringer, senest 1. januar 2020.

Tildelingsbrev

- Olje- og energidepartementet (2018–2020). *Tildelingsbrev til Norges vassdrags- og energidirektorat*.

Offentlige utredninger (NOU)

- NOU (2004: 17) *Statlig tilsyn med kommunesektoren.*
- NOU (2015: 13) *Digital sårbarhet – sikkert samfunn.*
- NOU (2018: 4) *IKT-sikkerhet i alle ledd.*

Høringer og høringssvar

- NVE (2017) *Forslag til endringer i beredskapsforskriften Krav til IKT-sikkerhet m.m.* Høringsdokument 6/2017.
- NVE (2018) *Oppsummeringsdokument: Endringer i beredskapsforskriften - Krav til IKT-sikkerhet m.m.* NVE-rapport nr. 92/2018.

Veiledere

- NVE (2012) *Veileder til sikkerhet i avanserte måle- og styringssystem.* Veileder nr. 7/2012.
- NVE (2013) *Veiledning til forskrift om forebyggende sikkerhet og beredskap i energiforsyningen*. Veileder nr. 1/2013.
- NVE (2015) *Øvelser: En veileder i hvordan planlegge og gjennomføre øvelser innen energiforsyningen*. Rapport nr. 39/2015.
- NVE (2018) *Foreløpig tilleggsveileder til kraftberedskapsforskriften. Oppdateringer etter revisjon.*
- NVE (2020) *Veiledning til kraftberedskapsforskriften.*
- NSM (2018, 2020) *Grunnprinsipper for IKT-sikkerhet.*
- NSM (udatert) *Veileder i sikkerhetsstyring,* versjon 1.
- NSM (2017) *Rammeverk for håndtering av IKT-sikkerhetshendelser,* versjon per 07.12.2017.
- Direktoratet for samfunnssikkerhet og beredskap (2019) *Veileder til samfunnssikkerhetsinstruksen.*
- Direktoratet for forvaltning og økonomistyring (2013) *Veileder i internkontroll.*

Rapporter, evalueringer og strategier

- Fridheim, H., J. Hagen og S. Henriksen (2001) *En sårbar kraftforsyning - sluttrapport etter BAS3.* FFI-rapport nr 2001/02381.
- Forsvarets forskningsinstitutt / Hagen, J. og Fridheim, H. (2007) *Beskyttelse av samfunnet 5: Sårbarhet i kritiske IKT-systemer - sluttrapport*. FFI-rapport nr. 2007/01204.
- NVE og Proactima (2012) *Utredning om CSIRT-funksjon for norsk kraftforsyning*. NVE-rapport nr. 69/2012.
- NVE og Forsvarets forskningsinstitutt (2015) *Teknologiskifte i energiforsyningen. Studie om muligheter og sårbarheter.* NVE-rapport nr. 118/2015.
- Forsvarets forskningsinstitutt (2016) *Vurdering av forebyggende sikkerhet innen kraft, petroleum og luftfart*. FFI-rapport nr. 16/00702.
- Menon Economics (2016) *Evaluering av NVE*. Menon-publikasjon nr. 23/2016.
- Sans Industrial Control Systems (2016) *Analysis of the Cyber Attack on the Ukrainian Power Grid.*
- NVE (2016) *Smarte målere (AMS).* NVE-rapport nr. 79/2016.
- NVE (2016) *Strategi for NVE 2017 - 2021.*
- NSM (2017) *Helhetlig IKT-risikobilde 2017.*
- NSM (2017) *Risiko og sårbarheter i en ny tid*
- NVE (2017–2020) *Årsrapport.*
- NVE (2017) *Logging og logganalyse i energiforsyningen.* NVE-rapport nr.1/2017.
- NVE og BDO (2017) *Metodikk for informasjonsinnhenting etter IKT-sikkerhetshendelser i driftskontrollsystem.* NVE-rapport nr. 14/2017.
- NVE (2017) *Regulering av IKT-sikkerhet.* NVE-rapport nr. 26/2017.
- NVE og SINTEF Energi AS (2017) *Evaluering av NVEs veileder til sikkerhet i AMS*. NVE-rapport 4/2017.
- NVE (2017) *Informasjonssikkerhetstilstanden i energiforsyningen.* NVE-rapport nr. 74/2017.
- NVE (2017) *Informasjonssikkerhetstilstanden i energiforsyningen.* NVE-rapport nr. 90/2017.
- PST (2017–2019 og 2020) Trusselvurderinger.

- NSM (2017, 2019 og 2020) Risikorapporter.
- Etterretningstjenesten (2017–2019) *Fokus.*
- NVE (2018) *IKT-sikkerhet ved anskaffelser og tjenesteutsetting i bransjen.* NVE-rapport nr. 90/2018.
- NVE (2018) *Smarte målarar.* NVE-rapport nr. 5/2018.
- NVE (2019) *Oppsummering av uønskede hendelser 2018 i energiforsyningen.* Faktaark nr. 4/2019.
- NVE (2019) *Tilstandsvurdering av forsyningssikkerhet og beredskap i kraftforsyningen.* Faktaark nr. 10/2019.
- NVE (2019) *CyberSmart - educating the future workforce.* NVE-rapport nr. 20/2019.
- Departementene (2019) *Nasjonal strategi for digital sikkerhet*.
- Departementene (2019) *Nasjonal strategi for digital sikkerhetskompetanse*.
- Finanstilsynet (2020) *Risiko- og sårbarhetsanalyse (ROS) 2020.*
- NVE og Proactima (2020) *Kartlegging av bruk av tingenes internett (IOT/IIoT) i norsk kraftforsyning.* NVE-rapport nr. 2/2020.
- NVE (2020) *Driften av kraftsystemet 2019.* RME-rapport nr. 3/2020.
- NVE (2020) *Bruk av digitale verktøy i tilsyn med IKT-sikkerhet.* NVE-rapport nr. 38/2020.
- NVE og KraftCERT (2020) *Digital kontroll: en studie om innføring og bruk av metrikker i kraftforsyningen for bedre IKT-sikkerhet.* NVE-rapport nr. 22/2020.
- NVE (2020) *Utvikling av cybersikkerhetskompetanse for kraftbransjen*. NVE-rapport nr. 45/2020.
- Direktoratet for samfunnssikkerhet og beredskap (2020). *Rapport fra tilsyn med olje- og energidepartementets samfunnssikkerhetsarbeid.*

Brev

- NVE (2018) *Forventninger og informasjon til KBO 2018*. Brev til KBO-enhetene, 12. februar 2018.
- NVE (2019) *Tildeling av midler til KraftCERT i 2019*. Brev til KraftCERT, 7. juni 2019.
- NVE (2019) *Etablering av sektorvist responsmiljø - informasjon til KBO*. Brev til KBO 24. juni 2019.
- NVE (2019) *Forventninger og informasjon til KBO for 2019*. Brev til KBO-enhetene, 4. mars 2019.
- NVE (2020) *Tildeling av midler til KraftCERT i 2020*. Brev til KraftCERT, 5. juni 2020.
- NVE (2020) *Forventninger og informasjon til KBO-enheter for 2020*. Brev til KBO-enhetene, 20. februar 2020.

Vedtak

- NVE (2014) *Vedtak om medlemsskap i Kraftforsyningens Beredskapsorganisasjon (KBO) for KraftCERT AS*, 22. desember 2014.
- NVE (2020) *Vedtak om at Nord Pool AS og European Market Coupling Operator AS skal inngå i Kraftforsyningens beredskapsorganisasjon (KBO)*. 19. mars 2020.

Internettkilder

- NVE (2020) *Smarte strømmålere (AMS). <https://www.nve.no/stromkunde/smarte-strommalere-ams/>* [Hentedato 25.10.20]
- Zetter, Kim (2016) *Inside the cunning, unprecedented hack of Ukraine's power grid*. I: Wired. <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/> [Hentedato 27. april 2020]