STORTINGET

# Innst. 574 S

**(2020–2021)**

Innstilling til Stortinget
frå kontroll- og konstitusjonskomiteen

Dokument 3:7 (2020–2021)

**Innstilling frå kontroll- og konstitusjonskomiteen om Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen**

Til Stortinget

## 1. Samandrag

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.

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 til Riksrevisjonen gitt kommentarer til rapporten. Kommentarene er i hovedsak innarbeidet i Riksrevisjonens dokument.

## 1.1 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.

## 1.2 Utdyping av konklusjoner

### *1.2.1 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.

#### 1.2.1.1 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 Riksrevisjonens 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.

#### 1.2.1.2 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. Riksrevisjonen 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 til-

synene 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.

#### 1.2.1.3 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.

#### 1.2.1.4 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-sikkerhetshendel-

ser 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.

#### 1.2.1.5 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 leveran-

dører. 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.

#### *1.2.2 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.

### 1.3 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

### 1.4 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.

### 1.5 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 Riksrevisjonen som uavhengige av forskriftsendringen og tidspunktet for revisjonen.

Riksrevisjonen er enig i a 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.

## 2. Merknader frå komiteen

Komiteen, medlemene frå Arbeidarpartiet, leiaren Dag Terje Andersen, Eva Kristin Hansen og Magne Rommetveit, frå Høgre, Svein Harberg og Bente Stein Mathisen, frå Framstegspartiet, Solveig Horne, frå Senterpartiet, Nils T. Bjørke, frå

Sosialistisk Venstreparti, Freddy André Øvstegård, frå Venstre, Terje Breivik, og uavhengig representant Ulf Isak Leirstein, viser til Riksrevisjonen si undersøking av NVE sitt arbeid med IKT-tryggleik i kraftforsyninga, jf. Dokument 3:7 (2020–2021). Komiteen viser til at kraftforsyninga er ein sentral del av den kritiske infrastrukturen i Noreg. Tilgang på elektrisk kraft vert stadig viktigare for å kunne oppretthalde normal aktivitet i samfunnet, sikre kritiske samfunnsfunksjonar i krisesituasjonar og oppretthalde forsvarsevna til landet under beredskap og i krig. Komiteen viser også til at IKT-system i kraftsektoren er kritisk infrastruktur som er særskilt utsett for etterretning og avanserte nettverksoperasjonar, ifølgje nasjonale trusselvurderingar.

Komiteen viser til at målet med Riksrevisjonen si undersøking har vore å vurdere i kva grad NVE sin verkemiddelbruk medverkar til å styrke IKT-tryggleiken i kraftforsyninga. Undersøkinga omfattar perioden 2016–2020.

Komiteen viser til at Riksrevisjonen har konkludert med at NVE ikkje i tilstrekkeleg grad har sikra at det er god beredskap for å handtere IKT-angrep i kraftforsyninga. Komiteen merkar seg at Riksrevisjonen etter ei samla vurdering har kome til at dette er alvorleg.

Komiteen viser til at Riksrevisjonen har funne at NVE si styring og oppfølging av arbeidet med IKT-tryggleik i kraftforsyninga er svak. Komiteen merkar seg at Riksrevisjonen meiner det er kritikkverdig at NVE samla sett har svak styring og oppfølging av arbeidet med IKT-tryggleik i kraftforsyninga. Vidare merkar komiteen seg at Riksrevisjonen meiner det er kritikkverdig at NVE sitt grunnlag for å vurdere statusen og utviklinga i IKT-tryggleikstilstanden i kraftforsyninga samla sett er mangelfullt. Komiteen viser vidare til at det er svakheiter ved NVE sitt tilsyn med IKT-tryggleiken i kraftforsyninga. Komiteen merkar seg at Riksrevisjonen meiner svakheitene ved NVE sine tilsyn med IKT-tryggleiken samla sett er sterkt kritikkverdige. Vidare har NVE skjerpa krava til IKT-tryggleik i kraftforsyninga, men har ikkje følgt det opp med tilstrekkeleg rettleiing. Det er også svakheiter ved NVE sitt arbeid med overvaking, varsling og beredskap ved IKT-hendingar.

Komiteen merkar seg at Riksrevisjonen vurderer det som kritikkverdig at Olje- og energidepartementet ikkje har etterspurt og sikra seg god nok styringsinformasjon om resultata av NVE sitt arbeid med IKT-tryggleiken i kraftforsyninga og om IKT-tryggleikstilstanden.

Komiteen stiller seg bak funna og kritikken frå Riksrevisjonen.

Komiteen merkar seg at olje- og energiministeren meiner slike revisjonar er nyttige, og at statsråden ynskjer å bruke Riksrevisjonen sine funn og tilrådingar for å vidareutvikle og styrke NVE sitt arbeid med IKT-tryggleik i kraftforsyninga. Komiteen meiner Riksrevisjonen sitt arbeid er viktig, og synest det er positivt at arbeidet vert opplevt som nyttig.

Komiteens medlemmer fra Høyre, Fremskrittspartiet, Venstre og uavhengig representant viser til at kraftberedskapsforskriften ble revidert med virkning fra 1. januar 2019. Fra januar 2019 har NVE hatt rollen med å koordinere og håndtere IKT-sikkerhetshendelser i kraftforsyningen. KraftCERT har bistått med varsling, informasjonsdeling og analyse av sikkerhetshendelser for å støtte NVE i denne oppgaven. Disse medlemmer merker seg at statsråden påpeker at mye er forbedret etter at Riksrevisjonens undersøkelse ble avsluttet.

Disse medlemmer merker seg videre statsrådens svar om at Riksrevisjonens funn og anbefalinger vil være nyttige bidrag i det påbegynte arbeidet med å videreutvikle og styrke NVEs arbeid med IKT-sikkerhet i kraftforsyningen. Som en del av dette utarbeider NVE en ny strategi for perioden 2022–2026, som vil gi grunnlag for bedre mål og resultatstyring. Metoden for tilsyn skal gjennomgås, og NVE og KraftCERT har i fellesskap et pågående FOU-prosjekt om analyserammeverket for innrapporterte hendelser. Videre revideres beredskapsplanverket i NVE i 2021, og den flerårige øvingsplanen oppdateres. Disse medlemmer viser også til at statsråden i sitt svar til Riksrevisjonen fremhever at NVE er bedt om å styrke arbeidet med IKT-sikkerhet i kraftforsyningen og bedre rapporteringen til departementet på tilstanden i kraftforsyningen. Det fremgår av tildelingsbrevet for 2021 at NVE har fått styringsparametere der de skal identifisere og omtale indikatorer for vurdering av tilstanden i kraftforsyningen og beskrive og vurdere resultatene fra tilsyn.

Komiteen merkar seg at Riksrevisjonen har tilrådd Olje- og energidepartementet å:

- sørge for at NVE styrker arbeidet med IKT-tryggleiken i kraftforsyninga, irekna:
  - vidareutviklar verktøy for å styre og følgje opp arbeidet
  - sikrar eit betre kunnskapsgrunnlag for tilstanden for IKT-tryggleiken
  - vurderer tilsynsmetodikken og gjennomfører risikobaserte tilsyn med IKT-tryggleiken
  - sikrar god rettleiing til bransjen
  - held fram med kompetansehevande tiltak internt og for bransjen
  - vidareutviklar systemet for avdekking og deling av IKT-tryggleikshendingar
  - oppdaterer beredskapsplanverket og gjennomfører fleire IKT-øvingar

- vurderer tiltak for å handtere utfordringa med å følgje opp leverandørane sin IKT-tryggleik
- sørge for at NVE si rapportering gjev tilstrekkeleg styringsinformasjon om resultata av direktoratet sitt arbeid med IKT-tryggleik i kraftforsyninga.

Komiteen støttar tilrådingane og ber Riksrevisjonen følgje utviklinga innanfor IKT-tryggleiken i kraftforsyninga vidare.

Komiteen viser til at kraftforsyninga er ein del av den kritiske infrastrukturen. Komiteen meiner det er viktig å vere budd på krisesituasjonar, og at faren for aksjonar mot kraftforsyninga aukar i slike krisesituasjonar. I krig er kraftforsyninga eit klart utsett mål. Sikker kraftforsyning er ein del av beredskapen, og det er alvorleg at forvaltinga ikkje har sikra god nok beredskap for denne kritiske infrastrukturen. Komiteen viser til at Riksrevisjonen samla sett har funne grunnlag for alvorleg kritikk, og ventar at statsråden vil følgje området tett opp vidare.

Fleirtalet i komiteen, medlemene frå Arbeidarpartiet, Senterpartiet og Sosialistisk Venstreparti, viser til at Riksrevisjonen over lang tid har rapportert svak informasjonstryggleik i sentrale samfunnsfunksjonar og i statlege verksemder, jf. Dokument 3:2 (2020–2021), Dokument 1 (2019–2020), Dokument 1 (2018–2019), Dokument 1 (2017–2018), Dokument 1 (2016–2017), Dokument 1 (2015–2016), Dokument 3:2 (2015–2016), Dokument 3:2 (2014–2015) og Dokument 1 (2014–2015).

Fleirtalet viser til at risikovurderinga frå Nasjonal sikkerhetsmyndigheit for 2021 legg vekt på at det digitale risikobildet er skjerpa, og at pandemien har gitt auka risiko. Det er gjennomført alvorlege angrep mot demokratiske institusjonar som syner at risikoen er reell. Digital beredskap er ein kritisk samfunnsfunksjon. Fleirtalet oppfordrar difor regjeringa til å gå gjennom og vurdera om dei tverrgåande verkemidla, kompetansen og risikoforståinga i staten er tilstrekkeleg for å møta dei truslane som er identifiserte.

## 3. Tilråding frå komiteen

Komiteen har elles ingen merknader, viser til dokumentet og rår Stortinget til å gjere følgjande

vedtak:

Dokument 3:7 (2020–2021) – Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen – vert lagt ved møteboka.

Oslo, i kontroll- og konstitusjonskomiteen, den 25. mai 2021

**Dag Terje Andersen**
leiar

**Magne Rommetveit**
ordførar

Svanemerketrykksak, 2041 0654 Trykk og layout: Stortingets grafiske seksjon