

Forsvarsdepartementet

Levert elektronisk på:
<https://www.regjeringen.no/id2606681>

Saksbeh./tlf.nr.: Kjetil Sørli/91304648
Deres ref./Deres dato: 2015/3139-254/FD V
3/ENWA/ 02.07.2018
Vår ref.: 18/00366-3
Vår dato: 28.09.2018

Statnetts høringssvar - Forskrifter til ny sikkerhetslov

Viser til Forsvarsdepartements høring på forslag til forskrifter til ny sikkerhetslov. I det følgende gis Statnetts høringssvar.

Innledning

Statnetts anlegg og systemer er kritisk infrastruktur. Selskapet eier og driver hoveddelen av transmisjonsnettet i Norge (tidligere omtalt som sentralnettet) og utenlandsforbindelsene. I tillegg er Statnett systemansvarlig i det norske kraftsystemet. Selskapet er ikke underlagt dagens sikkerhetslov (med unntak av § 29a), men energilovens sikkerhet - og beredskapsbestemmelser på blant annet områder som informasjons - og objektsikkerhet. Statnett er et statsforetak opprettet i henhold til statsforetaksloven og eid av staten ved Olje - og energidepartementet.

Generelle tilbakemeldinger

I Statnetts høringssvar i januar 2017 til NOU 2016:19 med forslag til ny sikkerhetslov ble det vist til at selskapet allerede er underlagt energilovens beredskapsforskrift, og det ble reist tvil om forsyningssikkerheten bedres med en dobbeltregulering og et delt myndighetsansvar for sikkerhet i sektoren. Videre at forslaget til ny lov vil ha en kostnadsdrivende effekt for Statnett, og dermed for våre kunder. Statnetts primære syn var og er at svakheter ved reguleringen av sikkerhet i energiforsyningen best lar seg løse ved endringer og justeringer i energilovens beredskapsforskrift. Sekundært var og er det vårt syn at sikkerhetsloven kun skal anvendes der det er klare mangler i energilovens beredskapsforskrift.

Med høringsutkastet til nye forskrifter er Statnett positiv til forslaget om utvidet adgangsklarering. Dette vil bidra til å minske gapet mellom de risikoene som PST og E-tjenesten beskriver er rettet mot kritisk infrastruktur, og virksomhetenes evne til å håndtere disse.

Videre er Statnett positiv til at det legges opp til større grad av fleksibilitet, for eksempel ved vurdering av sikkerhetsmessig skikkethet av utenlandsk personell, ved sikring av informasjon

gradert til BEGRENSET og at det på flere områder legges opp til funksjonelle krav. Samtidig betinger dette at det foreligger gode veiledninger, tilgjengelige kurs og tilgjengelig rådgivning. Ikke minst gjelder dette for virksomheter som ikke tidligere har vært underlagt sikkerhetsloven.

Statnett har store investeringer hvor leverandører opererer globalt med tilhørende potensial for sikkerhetsbrudd. Selv om antallet leverandørnivåer for enkelte typer anskaffelser aktivt kan besluttes begrenset fra Statnetts side, vil det uansett være krevende å håndtere risiko i alle ledd. Slik sett vil forskriftene kunne bidra til å gi et sterkere lovmessig grunnlag for å håndtere sikkerheten i anskaffelser til kritisk infrastruktur. Samtidig vil det etter Statnetts syn også begrense markedet, og føre til et økt kostnadsnivå på varer og tjenester. Forskriftene legger også opp til ulike godkjennings- og klareringsprosesser som kan være utfordrende i tidskritiske anskaffelser, og det bør legges vekt på at regelverket i størst mulig grad legger til rette for effektive og forutberegnelige anskaffelser. Også her vil gode veiledninger, og ikke minst en forståelse hos regulerende myndigheter om dagens leverandørmarked være avgjørende for at virksomhetene skal evne å oppnå formålet i lov og forskrift.

Statnett er underlagt energilovens beredskapsforskrift. Denne inneholder funksjonelle krav, men også detaljerte og spesifikke krav til forebyggende sikkerhet for å sikre funksjonsdyktighet for anlegg og systemer. Etter Statnetts syn må det legges vekt på at råd og veiledning til sikkerhetslovens forskrifter ikke går på tvers av råd og veiledning til energilovens beredskapsforskrift.

Spesifikke tilbakemeldinger

Til 4.1.1, side 13

Departementet ber om høringsinstansenes syn på om det bør gis mer detaljerte krav til sikring av infrastruktur, og i så fall hvilke krav som bør stilles. Kraftsektoren er allerede underlagt detaljerte krav til sikring av infrastruktur. Statnett foreslår at sektorer som i dag i stor grad har detaljert krav til sikring av infrastruktur i sektorlovverk, skal fortsette å benytte sektorlovverkets detaljerte krav uavhengig av om bestemmelsene i sikkerhetslovens forskrifter er detaljerte eller ikke. Det er etter Statnetts syn sektormyndighetene som innehar tilstrekkelig nærhet og kompetanse til å stille relevante og konkrete krav til egen sektor. Samtidig vil det etter Statnetts syn være riktig at sikkerhetslovens forskrifter skal kunne fylle eventuelle hull i sektorlovgivningen, men at dette kan skje ved at sektorlovgivningen harmoniserer egne krav med sikkerhetslovens forskrifter.

Til 4.1.2 – 4.1.4, sidene 13 og 14

Departementet skriver at sektordepartementenes vurdering: "[...] skal basere seg på virksomhetens vurdering av skadefølger ved bortfall av objekter eller infrastrukturens funksjon.". Statnett ønsker å understreke viktigheten av tett dialog mellom sektordepartement og virksomhet i prosessen som fører til identifisering, utpeking og klassifisering. Det skyldes at det kun er virksomheten selv som har detaljert oversikt og kompetanse på egne objekter og systemer, og som i detalj kjenner hvilke risikoreduserende tiltak som allerede er på plass.

Til 4.5.4 og 4.6.3, side 22 og 23

Departementet skriver:

Dersom utenlandsk personell fra en leverandør som driver sin virksomhet utenfor norsk jurisdiksjon skal få tilgang til skjermingsverdig informasjon, informasjonssystem, infrastruktur

og objekt hos oppdragsgiveren, må personellet oppfylle kravene til autorisasjon og klarering som gjelder for den aktuelle tilgangen.

Statnett ønsker å gjøre oppmerksom på at en rekke kritiske IKT-systemer er avhengig av driftsstøtte i form av fjernaksess fra spesialister i land utenfor norsk jurisdiksjon. I dette ligger det et potensial for at enkeltpersoner med kritisk kompetanse hos leverandør ikke blir klarert i hjemlandet. Det kan igjen føre til at virksomheten ikke får tilgang til nødvendig ekspertise ved kritiske driftshendelser. Statnett ønsker derfor å understreke behovet for fleksibilitet slik departementet beskriver på side 22:

Departementet ser at § 8-7 i utgangspunktet vil dekke behovet for å kunne gi utenlandsk personell tilgang til sikkerhetsgradert informasjon og skjermingsverdige objekter og infrastruktur av hensyn til behovet for kompetanse, uten at dette i for stor grad går på bekostning av behovet for kontroll med personellet av hensyn til nasjonale sikkerhetsinteresser. Departementet ber derfor om høringsinstansenes syn på behovet for og hensiktsmessigheten av den unntaksbestemmelsen som er foreslått i myndighetsforskriften § 11, og vil vurdere bestemmelsen i lys av høringsinnspillene.

Videre ønsker Statnett å understreke viktigheten av at virksomhetsforskriftens § 19 om unntak for sikkerhetskrav blir vedtatt. For enkelte kritiske systemer er det i praksis ikke et alternativ å avslutte samarbeidet med leverandøren selv om kritisk personell ikke er klarert. Statnett støtter videre departementets vurdering på side 27 hvor det står:

I de sektorene som har stor utenlandsk kontaktflate og som er særlig avhengig av utenlandsk ekspertise og kompetanse, som for eksempel kraft, petroleum, samferdsel og finanssektoren, vil krav til klarering ved anskaffelser kunne gi relativt høye økonomiske og administrative konsekvenser for virksomhetene.

Til 4.6.3. side 23

Departementet skriver at:

Når det gjelder behovet for kompetanse som Norge ikke har tilstrekkelig tilgang på nasjonalt, antar departementet at denne som utgangspunkt kan anskaffes som en sikkerhetsgradert anskaffelse fra land Norge har et sikkerhetssamarbeid med.

Dette kan forstås slik at sikkerhetsgraderte anskaffelser fra land utenfor Norge kun er nødvendig dersom det ikke er tilgang på tilstrekkelig kompetanse nasjonalt. Dersom departementet mener at en virksomhet har adgang til å unnta sikkerhetsgraderte anskaffelser fra anskaffelsesregelverket, slik at anskaffelsen kan begrenses til nasjonale leverandører, bør dette komme tydelig frem.

Til 4.6.4. side 23-24

Statnett er ikke underlagt dagens sikkerhetslov, med unntak av varslingsplikten i § 29a. Bestemmelsen er aktivt benyttet av Statnett for å nekte anskaffelser fra enkeltland for enkelte typer anlegg og systemer. Erfaringen er at varslingsplikten ikke er forutsigbar og mulig å praktisere ut over å nekte anskaffelser fra de land som PST og E-tjenesten viser til i sine enhver tid ugraderte trussel- og risikovurderinger. Selskapet er langt på vei overlatt til egne vurderinger og har utarbeidet en prosess og metodikk for å håndtere bestemmelsen og de risikoreduserende tiltakene uten støtte og veiledning fra relevante myndigheter. Dagens § 29a er krevende å håndtere, og sett utenfra oppleves det som om at lovendringen i sin tid ble vedtatt uten at virksomhetene i praksis ble satt i stand til å etterleve bestemmelsen. Det er heller per i dag ikke publisert noen veiledning

på området. Dette til tross for at det i Forsvarsdepartementets høring datert 19. mai 2015 om forslag til endringer i sikkerhetsloven blir foreslått: "[...] at Nasjonal sikkerhetsmyndighet utarbeider generelt veiledningsmateriale som gjøres tilgjengelig for aktuelle virksomheter. Dette for at varslingsplikten skal kunne bli forutsigbar og mulig å praktisere [...]. Videre så la departementet i samme forslag til grunn at det vil: "[...] være nødvendig å utforme en veileder eller instruks som forklarer hva varslingsplikten vil innebære [...].

I høringsnotatet til forskrifter til ny sikkerhetslov datert 02.07.2018 skriver departementet:

Departementet antar at det vil være mer hensiktsmessig at myndigheter med sektoransvar lager veiledere med momenter som kan vektlegges i vurderingen. Departementet ber om høringsinstansenes innspill på om det er nødvendig med ytterligere forskriftsbestemmelser knyttet til denne bestemmelsen.

Statnett er av den oppfatning at dagens § 29a og videreføringen av denne i den nye sikkerhetslovens § 9-4, og i forslag til virksomhetsforskrift § 18, ikke er forutsigbar og mulig å praktisere før en veiledning er publisert. Adgangen til å redusere risikoen i form av konkurransebegrensende tiltak innenfor anskaffelsesregelverkets rammer er uklar, og bør belyses i en veiledning. Videre at denne må utformes i samråd med virksomheter som har erfaring med store anskaffelser i et globalt leverandørmarked.

Varslingsplikten etter sikkerhetslovens § 9-4 gjør det, etter Statnetts erfaring med dagens § 29a, utfordrende å sette opp en realistisk tidsplan for anskaffelsen, som ofte er tidskritisk. For å få til et effektivt og fungerende varslingsregime, mener Statnett at det i forskrifts form bør gis føringer for departementets saksbehandlingstid av slike varsler.

Til 4.6.6. side 25

Statnett støtter forslaget om at ansvaret for kontroll av om leverandørene oppfyller sikkerhetskravene i sikkerhetsloven med forskrifter, legges til klareringsmyndigheten for leverandørklarering.

Til § 47 andre ledd, virksomhetsforskriften

I denne står følgende:

Nasjonal sikkerhetsmyndighet godkjenner skjermingsverdige informasjonssystemer som er utpekt som, eller er av avgjørende betydning for funksjonaliteten i, et objekt eller en infrastruktur klassifisert KRITISK eller MEGET KRITISK.

Driftskontrollsystemer i kraftforsyningen kan tenkes å bli definert som KRITISK eller MEGET KRITISK. I § 47 fremgår det at Nasjonal sikkerhetsmyndighet i så fall skal godkjenne disse.

Driftskontrollsystemer er komplekse og spesialiserte systemer, og innsikt og forståelse av drift og sikkerhet krever spesialisert kompetanse. Dette er systemer som uavhengig av en godkjenning må fortsette drift, og som det tar lang tid å erstatte. Det reises derfor spørsmål om det er hensiktsmessig at slike systemer skal godkjennes av en myndighet, eller om det i stedet er hensiktsmessig at relevante myndigheter fører tilsyn, og gir avvik fra lov og forskrift hvis dette blir identifisert.

Vedrørende sikkerhetsmyndighetenes godkjenning av utenlandske leverandører

Det følger av ny sikkerhetslov § 9-2 første ledd at

Dersom en utenlandsk leverandør eller dennes personell må klareres eller gis tilgang til sikkerhetsgradert informasjon, skal sikkerhetsmyndigheten godkjenne leverandøren før det inngås en sikkerhetsavtale.

Statnett kan ikke se at det i forskriftene er gitt utfyllende regler om hvordan denne godkjenningen skal foregå. Forholdet mellom sikkerhetsmyndighetens godkjenning og klareringsmyndighetens leverandørklarering fremstår som noe uklart. Statnett ber derfor departementet vurdere om det bør gis utfyllende regler i forskriftene om sikkerhetsmyndighetens godkjenning av utenlandske leverandører. Forskriftene bør også vise til hva sikkerhetsmyndigheten skal legge vekt på ved vurderingen av om leverandøren skal godkjennes, og hvorvidt virksomheten skal ha en rolle ved en slik godkjenningsprosess.

Med vennlig hilsen

Øivind K. Rue (sign.)
Konserndirektør Drift og marked

Kjetil Sørli (sign.)
Seksjonsleder Sikkerhet og beredskap