Høringsuttalelse

Sak

Høringsuttalelse forslag til EU-direktiv om sikkerhet og informasjonssystemer

Dokumentet sendes til: Justis og beredskapsdepartementet

Saksbehandler/Adm. enhet:

Rikke C. Arnulf /Seksjon for sikkerhet og beredskap

Dokument ID: 16/01054

Dato: 23.09.2016

Bakgrunn

Justis- og beredskapsdepartementet har oversendt høringsbrev vedr. forslag til EU-direktiv om sikkerhet i nettverk og informasjonssystemer (NIS-direktivet).

I høringsbrevet er svarfristen satt til 15.9.2016. Statnett beklager at dette svaret kommer etter utløpet av fristen.

Dette notatet inneholder en vurdering av mulige konsekvenser for de lover og forskrifter som etter Statnetts vurdering vil kunne omfattes av en gjennomføring av direktivet i norsk rett, samt eventuelle følger en etterlevelse vil ha for Statnett.

Kommentarer

1. Berørte lover og forskrifter i norsk rett.

Direktivet setter krav til

- etablering av nasjonale rammeverk for IKT-sikkerhet,
- etablering av internasjonale samarbeidsfora, og
- IKT-sikkerhet for virksomheter.

NOU 2015: 13 *Digital sårbarhet – sikkert samfunn* peker på at NIS-direktivet vil kunne ha konsekvenser for *Sikkerhetsloven* og dens virkeområde. Per 2015 var denne under revisjon. NOUen anbefaler at i påvente av ny sikkerhetslovgivning og en eventuell implementering av NIS-direktivet fra EU bør krav til IKT-sikkerhet gjøres tydelig i forskrifter. Det foreligger nå en lovendring vedr. anskaffelser til kritisk infrastruktur (se www.lovdata.no LOV-2016-08-12-78), men denne er ikke satt i kraft ennå og inkluderer ikke bestemmelser fra NIS-direktivet.

NOU 2015:13 omtaler ikke NIS-direktivet spesifikt i forhold til kraftsektoren, men anbefaler å videreutvikle KraftCERT som et sterkt fagmiljø innen operativ hendelseshåndtering og at NVE må tydeliggjøre krav om tilknytning til et operativt fagmiljø for hendelseshåndtering, enten mot KraftCERT eller mot andre miljøer. Siden NIS-direktivet setter krav til

- etablering av en eller flere CSERT, som skal dekke samfunnskritiske virksomheter, herunder kraftsektoren, og
- krav til samfunnskritiske virksomheter, herunder kraftsektoren,

vil direktivet også kunne medføre endringer i energiloven med forskrifter, herunder beredskapsforskriften.

2. Energiloven og beredskapsforskriften (bfe)

CHAPTER IV SECURITY OF THE NETWORK AND INFORMATION SYSTEMS OF OPERATORS OF ESSENTIAL SERVICES, Artikkel 14 og 15 i NIS-direktivet, setter krav til sikkerhet i nettverk og informasjonssystemer hos virksomheter i kraftsektoren og implementering av disse.

Krav til sikkerheten i nettverkene og informasjonssystemene tilhørende virksomhetene i henhold til Artikkel 14 paragraf 1 er allerede etablert som krav til IKT-sikkerhet for driftskontrollsystemer (bfe) og AMS (AMS-forskriften). Det er også krav i bfe om at tiltak for IKT-sikkerhet skal være basert på løpende risikovurderinger. Statnett vurderer derfor dagens forskriftskrav i bfe som dekkende for Artikkel 14, paragraf 1. Eventuelle justeringer i disse kravene basert på en nasjonal strategi (ref. Artikkel 7), kan implementeres i bfe.

Bfe setter også krav om en helhetlig risikovurdering i forhold til å opprettholde forsyningssikkerhet, inklusive kritikalitetsvurdering av IKT-systemer som er nødvendige for driftskontrollfunksjoner. Dette vurderer Statnett også som dekkende for Artikkel 14, paragraf 2.

Kravene i Artikkel 14 paragrafene 3 og 4 om varsling av hendelser som har en alvorlig forstyrrende effekt på leveransen er langt på vei implementert i bfe i form av krav til virksomhetene om hendelsesrapportering inklusive varsling til beredskapsmyndighet (NVE). Regulering av varsling til nasjonal kompetent myndighet og nasjonal CSIRT (NorCERT) vil etter Statnetts vurdering kunne implementeres i sektorovergripende lov/forskrift som gjøres gjeldende for sektormyndighet (NVE) og evt. understøttende sektorspesifikk nasjonal CSIRT (KraftCERT).

Kravene i Artikkel 14 paragrafene 5 og 6 er i hovedsak krav til nasjonal CSIRT (NorCERT) og nasjonal myndighet (NSM?) om hendelseshåndtering i form av viderevarsling internasjonalt og behandling av informasjonsflyt underveis. Dette bør etter Statnetts vurdering være krav som implementeres i relevant sektorovergripende lov og forskrift (se Sikkerhetsloven under). Eventuelle krav om informasjon til befolkningen (the public) bør utformes som krav / retningslinjer der nærmeste sektoransvarlige myndighet (NVE for kraftsektoren) og den/de berørte virksomheter (KBO-enheter i kraftsektoren) skal konsulteres og eventuelt være ansvarlig for å informere (nærhetsprinsippet).

Artikkel 14 paragraf 7 inneholder bestemmelser som bør reguleres som kompetanse til den nasjonale myndighet som representerer Norge i Cooperation Group (ref. Artikkel 11). Bestemmelsene om kompetanse bør inneholde anvisning om at relevante nasjonale sektormyndigheter skal konsulteres ved utarbeidelse av retningslinjer som berører virksomheter i egen sektor.

Artikkel 15 setter krav til lovgivningen som regulerer kontroll med etterlevelse av virksomhetenes plikter etter Artikkel 14. For kraftsektoren er dette fullt ut implementert i energiloven og bfe, der krav til virksomhetene er knyttet til tilsyn fra sektormyndighet (NVE) og fullt innsyn i dokumentasjon relatert til etterlevelse, samt etterlevelse av pålegg om å rette avvik. I en sektorovergripende lov / forskrift kan kompetanse for å utføre tilsyn og gi pålegg med fordel gis til sektormyndighet når krav om IKT-sikkerhet er gitt i sektorspesifikk lov/forskrift, i dette tilfellet NVE. Nasjonal myndighet (competent authority) for IKT—sikkerhet, bør kunne ha kompetanse til å gi retningslinjer for sektorvise tilsynsmyndigheter med formål å

samordne fokus og metoder for tilsyn knyttet til IKT-sikkerhet. I den konteksten bør retningslinjene samsvare med intensjonen i Artikkel 19 om bruk av anbefalte internasjonale standarder for styring, ledelse og kontroll relatert til informasjonssikkerhet.

3. Sikkerhetsloven med forskrifter

Statnett er pt. ikke underlagt andre bestemmelser i sikkerhetsloven enn §29 a om anskaffelser til kritisk infrastruktur (se www.lovdata.no LOV-2016-08-12-78).

Imidlertid er det sannsynlig at generelle (sektorovergripende) krav til IKT-sikkerhet for samfunnskritiske virksomheter også vil kunne medføre endringer i sikkerhetsloven med forskrifter (jf NOU 2015:13). Slike endringer vil også kunne bli gjort gjeldende for virksomheter i kraftsektoren, også Statnett.

Statnett ønsker at nye bestemmelser som også omfatter virksomheter i kraftsektoren i størst mulig grad innarbeides i energiloven med forskrifter. Dette begrunnes med at krav til sikkerheten i nettverkene og informasjonssystemene tilhørende virksomhetene allerede er etablert som krav til IKT-sikkerhet for driftskontrollsystemer (beredskapsforskriften) og AMS (AMS-forskriften). Beredskapsforskriften har også per i dag bestemmelser med kriterier for å identifisere virksomheter av betydning for å opprettholde forsyningssikkerhet av elektrisk kraft og vil dermed være egnet også for å identifisere Operatører av essensielle tjenester (ref. sector Energy, subsector Electricity i direktivets ANNEX II TYPES OF ENTITIES FOR THE PURPOSES OF POINT (4) OF ARTICLE 4).

Kraftsektoren har pt. etablert en sektorspesifikk nasjonal CSIRT, KraftCERT. Den er i hht. beredskapsforskriften definert som KBO-enhet og underlagt bestemmelser som i stor grad samsvarer med NIS-direktivets krav til nasjonale CISIRTer (ref. ANNEX I REQUIREMENTS AND TASKS OF COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRTs)). Statnett ser det derfor som naturlig at eventuelle krav til KraftCERT i medhold av ANNEX I også implementeres i beredskapsforskriften.

Krav som regulerer samordning og varsling ved hendelser mellom nasjonal CSIRT (NorCERT) og sektorspesifikke CSIRTS (som KraftCERT) kan med fordel implementeres i Sikkerhetsloven som sektorovergripende bestemmelser der.

Krav til samordning og varsling innen en sektor bør implementeres i sektorspesifikk lov og forskrift der det allerede finnes. For kraftsektoren inneholder beredskapsforskriften per nå bestemmelser om samordning og varsling mellom virksomheter (KBO-enheter) og myndighet (NVE). Statnett mener at dette med fordel kan videreføres også ved implementering av NIS-direktivets bestemmelser i Article 14 paragraf 3-6. Dette støtter også beredskapsprinsipper om nærhet og likhet.

Konklusjon

Statnett vurderer at krav i NIS-direktivet relatert til virksomheter i kraftsektoren mest effektivt kan implementeres ved mindre justeringer av sektorspesifikk lov og forskrift, energiloven og beredskapsforskriften (bfe).

I den grad det er behov for samordning ~~på~~ med nasjonal myndighet for IKT-sikkerhet og nasjonal CSIRT (NorCERT), kan dette tillempes i sektorovergripende lov og forskrift med fokus på samordning mot sektormyndighet (NVE) og sektorspesifikk CSIRT (KraftCERT).

Statnett vurderer derfor at en tilpasning av norsk lovgivning for å implementere NIS-direktivet for kraftsektoren, i liten grad vil medføre endringer for virksomheter i kraftsektoren som er regulert av energiloven og beredskapsforskriften. Statnett ser det imidlertid som positivt at tilsvarende virksomheter ellers i Europa også

underlegges direktivets krav, og at dette kan bidra til å lette utvekslingen av informasjon i kraftsystemene i et europeisk perspektiv.

Allerede pågående arbeid i Statnett med å innrette styring av informasjonssikkerhet mot internasjonale standarder vil også bidra til at det vil bli enklere å tilpasse Statnetts virksomhet til et tilsynsregime som over tid vil kreve dokumentasjon på etterlevelse etter slike standarder.