DET KONGELIGE
OLJE- OG ENERGIDEPARTEMENT

Justis- og beredskapsdepartementet
Postboks 8005 Dep
0030 OSLO

Deres ref	Vår ref	Dato
15/8216	16/945-	15.03.2016

Høring - "Digital sårbarhet - sikkert samfunn" (NOU 2015:13) - høringssvar fra Olje- og energidepartementet

Viser til brev av 9. desember 2015 fra Justis- og beredskapsdepartementet om høring av NOU 2015:13 – *"Digital sårbarhet - sikkert samfunn"*, der Olje- og energidepartementet er høringsinstans i tillegg til blant andre Oljedirektoratet (OD) og Norges vassdrags- og energidirektorat (NVE). Nedenfor følger innspill fra Olje- og energidepartementet (OED).

OED har sammen med øvrige aktører fra sektorene fått god mulighet til å presentere problemstillinger og sektorperspektiver på digital sårbarhet for Lysneutvalget, og vi vil innledningsvis benytte anledningen til å si at Lysneutvalget etter vår vurdering har presentert en bred og omfattende beskrivelse som belyser en av vår tids viktigste samfunnsutfordringer på en god og hensiktsmessig måte. NOUen vil være et sentralt referansedokument i dialogen med bransjene på våre sektorer i tiden fremover.

Generelle innspill til utvalgets rapport
Departementet har merket seg Lysneutvalgets tydelige fokus på behovet for IKT-sikkerhetskompetanse og støtter dette. Olje- og energisektoren har vært en pådriver for oppbygging av sterke fagmiljøer for cybersikkerhet gjennom å finansiere stillinger og prosjekter knyttet til nettopp dette temaet. Departementet vil også viderebringe budskapet i arbeidet med både kraft og olje/gass og arbeide aktivt for å styrke kompetansen i sektortilsynet gjennom godt samarbeid med NSM og andre IKT-sikkerhetsmiljøer.

Postadresse	Kontoradresse	Telefon*	Saksbehandler
		22 24 90 90	Tone Limbodal
		Org no.	
postmottak@oed.dep.no	http://www.oed.dep.no/	977 161 630	

Vi merker oss Lysneutvalgets påpekninger om viktigheten av å redusere kritikaliteten i viktig infrastruktur og er tilfreds med at Lysneutvalget har merket seg at kraftnettet har en etablert grunnfilosofi om redundans. Olje- og energidepartementet skulle imidlertid også sett at det hadde blitt viet noe større oppmerksomhet omkring egenberedskap ifm omtale av avhengigheten av strøm for å drifte IKT-infrastrukturen. Strøm er med dagens tekniske muligheter noe av det som faktisk er lett å erstatte hvis det faller ut, gitt at man har forberedt seg på dette ved å etablere systemer for reservekraft eller batteriback-up. Det blir mer og mer vanlig å ha systemer for å sikre reservestrøm-forsyning i kortere eller lengre perioder. Dette er tiltak som vil stykke opp verdikjedene som Lysneutvalget har vært opptatt av å redusere sårbarheten.

OED støtter i all hovedsak utvalgets anbefalinger i kapittel 13 Energiforsyningen. OED er overordnet ansvarlig samordnende departement for kraftforsyningen. Mye av beredskapsarbeidet i kraftsektoren er imidlertid delegert til NVE. Blant annet er NVE delegert forskriftskompetanse etter energiloven kapittel 9 som omhandler beredskap. NVE har fastsatt forskrift om forebyggende sikkerhet og beredskap i kraftforsyningen (beredskapsforskriften). OED viser derfor til NVEs høringsuttalelse for en mer detaljert tilbakemelding til utvalgets anbefalinger i kapittel 13.

I det følgende gis det konkret tilbakemelding på noe av det utvalget tar opp i rapportens sektordeler.

Vedrørende IKT-sikkerhet og personvern i AMS i kraftforsyningen
Utvalget hadde ingen konkrete anbefalinger på dette området. Vi ønsker likevel å knytte noen kommentarer til dette feltet.

AMS gir store muligheter og er et ledd i en nødvendig modernisering av kraftnettet. Teknologien kan bli viktig for å opprettholde strømforsyningen i kritiske situasjoner. Bruk av AMS vil blant annet gi nettselskapene langt mer nøyaktig informasjon om den faktiske tilstanden i nettet. Informasjonen kan brukes til å drifte og dimensjonere nettet mer effektivt, og feil og avbrudd blir oppdaget og kan rettes raskere. Med AMS følger en enorme mengder data. For å håndtere dette på en mest mulig effektiv og sikker måte utvikles en sentral løsning for datalagring, Elhub. Hyppige avlesninger av strømforbruket, samt økt datautveksling og -lagring, gjør at det er behov for å ha fokus på personvern og IKT-sikkerhet. Nettselskapene har ansvaret for å ivareta sikkerheten i AMS-løsningen. For å hindre misbruk av data og uønsket tilgang til personopplysninger og styrefunksjoner, stilles det strenge krav til nettselskapene og til Elhub. Eksempler på krav er obligatorisk kryptering av meldingsutvekslingen med Elhub, sikker tilgangskontroll og styringssystem for sikkerhet i Elhub. Nettselskapene må for eksempel sørge for sikker tilgang til kritiske styrefunksjoner som bryterfunksjonen i AMS. Dersom det er kobling mellom AMS-løsningen og driftskontrollsystemet, skal

AMS-løsningen oppfylle krav i beredskapsforskriften, og må sikres i henhold til driftskontrollsystemets klassifisering.
Departementet mener at personvernhensyn er godt ivaretatt når AMS skal tas i bruk. Informasjonsutveksling mellom måleren og nettselskapet vil foregå i et lukket system der bare nettselskapet har tilgang. Informasjonen vil være kryptert. Bortsett fra kunden selv, vil ingen andre enn nettselskapet og kraftleverandøren få tilgang til kundens timesverdier. Kunden vil få oversikt over, og mulighet til å styre, hvem som får tilgang til egne måledata i Elhub. Dette sikres gjennom en personvernløsning på internett-sidene til kraftleverandørene.

Bruken av IKT i energiforsyningen er i utvikling. Hensynet til å optimalisere drift, investeringer og tjenesteutvikling, kan gi en tettere interaksjon mellom systemer som i dag i stor grad er separate. Dette vil kreve en kontinuerlig vurdering av rammene for innføring av ny teknologi og krav til IKT-sikkerhet og personvern.

Når det gjelder en utvidet ROS-analyse for bruk av AMS opp mot driftskontrollsystemet viser departementet til NVEs høringsuttalelse.

Vedrørende KraftCERT
Departementet støtter utvalget i at det er viktig at bransjen har et kompetent felles miljø for hendelseshåndtering som både kan koordinere hendelser internt i sektoren og være kontaktpunkt ut mot andre sektorer. Det blir stadig viktigere å kunne oppdage og håndtere IKT-hendelser raskt. I tillegg til egne forskriftsbestemmelser om dette i beredskapsforskriften, tok NVE i 2013 initiativet til at bransjen opprettet et eget IKT-varslingsmiljø med kapasitet til å koordinere og håndtere uønskede IKT-hendelser i selskapene. KraftCERT har vært operativ siden mai 2015. I dag abonnerer en rekke energiselskap på de IKT-sikkerhetstjenester Kraft-CERT tilbyr, og departementet er opptatt av at flere selskaper vurderer medlemskap der eller på andre måter sikrer at de har tilgang til slik kompetanse.

Utvalget mener videre at det er behov for å evaluere ordningen med sektorvise responsmiljøer sett opp mot det tverrsektorielle behovet for hendelseshåndtering. Utvalget peker på at evalueringen bør se på inndelingen i sektorvise responsmiljøer, og om responsmiljøer med tilsvarende utfordringer bør slås sammen. OED vil her bemerke at selv om sektorene står ovenfor mange av de samme utfordringer, vil ulike sektorer og infrastrukturer kunne ha svært ulik IKT-infrastruktur og -systemer. Departementet vektlegger derfor å støtte opp om de sektorvise responsmiljøene og den kompetansen de innehar angående de sektorspesifikke systemene som benyttes. I handlingsplanen knyttet til nasjonal strategi for informasjonssikkerhet er etablering av sektorvise responsmiljøer et tiltak for å sikre samfunnets evne til å oppdage, varsle og håndtere alvorlige IKT-hendelser. Sektor-CERTer trekkes fram som en viktig forutsetning for effektiv håndtering av IKT-hendelser.

Departementets synspunkt er at det tverrsektorielle behovet for hendelseshåndtering kan ivaretas gjennom bedre koordinering mellom NorCERT og sektor-CERTer, heller enn å revurdere de sektorvise responsmiljøene. KraftCERT vil samarbeide med alle relevante sikkerhetsmiljø i Norge og i utlandet for å innhente informasjon om sårbarheter og IKT-trusler mot energiforsyningen. Spesielt vil samarbeidet med NorCERT være viktig.

Vedrørende EUs regelverk på IKT-sikkerhet
Signaler fra EU-kommisjonen medfører også et økt fokus på IKT-sikkerhet. I denne sammenhengen er det viktig at Justis- og beredskapsdepartementet (JD) som overordnet ansvarlig samordnende departement for IKT-sikkerhet i sivil sektor, i tråd med midlertidige retningslinjer for forvaltningens arbeid med EØS- og Schengen-saker, bidrar aktivt og jobber for å påvirke EUs beslutningsprosesser. OED har selv god erfaring med deltakelse i komitearbeid. Dette gir en god mulighet til å påvirke tidlig i utviklingen av EU-regelverk, selv om Norge som oftest ikke har stemmerett i slike prosesser.

Utvalget anbefaler at JD aktivt følger opp arbeidet med NIS-direktivet, både med tanke på hvilke konsekvenser direktivet kan få for Norge, men også for å gi føringer og stille krav til andre departementer og forberede sektorene på å implementere direktivet. OED støtter at JD aktivt følger opp prosessen med dette direktivet, og forutsetter at JD involverer relevante sektordepartement (som f.eks. OED, FIN og SD) i arbeidet.

Vedrørende krav til bemanning i kraftsektoren
I kapittel 13.3.1 Konsesjoner nevner utvalget at den opphevede kompetanseforskriften tidligere ga NVE mulighet til å stille krav til bemanning i nettselskapene. Lysneutvalget viser til at det var ekspertgruppen ledet av Reiten som konkluderte med at dette kravet kunne være konkurransevridende og at forskriften på den bakgrunn nå er opphevet. Dette forskriftsarbeidet startet imidlertid før ekspertgruppen leverte sine anbefalinger, men ekspertutvalget støttet en slik endring i sin rapport. Bakgrunnen for å oppheve kompetanseforskriften og erstatte denne med en ny, mindre omfattende bestemmelse i energilovforskriften var å gi selskapene mer fleksibilitet til selv å bestemme organisering av egen virksomhet. Med den nye bestemmelsen står selskapene friere til å vurdere om det er mest hensiktsmessig å sette ut oppgaver til eksterne tjenesteytere, eller utføre oppgavene med egne ansatte. Kravene til blant annet leveringskvalitet, beredskap og forsvarlig drift er de samme som før forskriftsendringen. Den nye bestemmelsen sikrer at selskapene fremdeles må ha tilstrekkelig egenbemanning til å lede virksomheten i enhver situasjon og følge opp innhold og utførelse av oppgaver som er satt bort til andre.

Vedrørende vurderinger og tiltak knyttet til olje- og gassektoren
Departementet vil påpeke noen unøyaktigheter i omtalen under kapittel 14. Antallet operatører og rettighetshavere på norsk sokkel endrer seg stadig, blant annet på grunn av oppkjøp og fusjoner. Det er derfor vanskelig i kvantifisere antallet selskaper på norsk

sokkel nøyaktig. På side 146 står det at det i dag er nær 40 selskaper på norsk sokkel. Det er i dag i overkant av 50 rettighetshavere på norsk sokkel.

Under pkt. *14.7 Vurderinger og tiltak* står det følgende:
"*Utvalget mener at anlegg på norsk sokkel har betydning for vitale samfunnsinteresser og rikets sikkerhet, og det kan ikke utelukkes at alvorlige hendelser kan inntreffe i fremtiden*".

Norsk sokkel har utvilsomt en viktig økonomisk betydning for Norge totalt sett. Departementet mener likevel at utvalget i sin beskrivelse tillegger enkeltanlegg på norsk sokkel en overdimensjonert betydning for samfunnets interesser og for den nasjonale sikkerheten.

Utvalget foreslår en rekke tiltak med tanke på IKT-sikkerheten innenfor olje- og gassektoren, som alle i større eller mindre grad trekker i retning av sterkere offentlig involvering i og kontroll av bransjens IKT-systemer. Olje- og energidepartementet mener problemstillingene som beskrives og tiltakene som foreslås må tas alvorlig og forfølges videre for å identifisere eventuelle behov for mer utfyllende regelverk og gjennomføring av eventuelle tiltak mot digital sårbarhet. Departementet vil imidlertid avslutningsvis understreke at man i det videre arbeid må legge til grunn at operatørselskapene har et selvstendig ansvar og en sterk økonomisk egeninteresse i å ivareta IKT-sikkerheten i egen virksomhet, noe utvalget også påpeker på side 148.

Med hilsen

Sigmund Johansen (e.f.)
ekspedisjonssjef

Tone Limbodal
seniorrådgiver

Dokumentet er elektronisk signert og har derfor ikke håndskrevne signaturer.