PETROLEUMSTILSYNET

Arbeids- og sosialdepartementet

Postboks 8019 Dep
0030 OSLO

Vår saksbehandler
Paul Bang

Deres ref.	Vår ref. (bes oppgitt ved svar)	Dato
15/4460	Ptil 2015/1407/PGB/TBH	3.3.2016

Ad høring – Digitalt sårbarhet sikkert samfunn (NOU 2015:13)

Vi viser til departementets forespørsel om eventuelle kommentarer fra Petroleumstilsynet (Ptil) til høringen om «Digitalt sårbarhet sikkert samfunn (NOU 2015:13). Det er særlig kapittel 14 som omtaler olje og gassektoren som er av interesse for Petroleumstilsynet (Ptil). Vi har derfor konsentrert oss om dette kapittelet i våre kommentarer.

Under punkt 14.2 omtaler utvalget roller og ansvar i petroleumsvirksomheten. Hvis hensikten her er å gi en oversikt over alle de ulike myndigheter som er involvert og beskrive rollene disse har, stiller vi spørsmål ved omtalene som er gitt om Direktoratet for samfunnssikkerhet og beredskaps (DSB) og Sjøfartsdirektoratets (SD) roller. Utvalget skriver at «*Direktoratet for samfunnssikkerhet og beredskap (DSB) har et ansvar for oppfølging av prosesstyringsanlegg, på bakgrunn av brann- og eksplosjonsvernloven med forskrifter, samt storulykkeforskriften*». Noe som er riktig hvis hensikten er å omtale ansvarsområdet til DSB på land. Imidlertid har ikke DSB dette ansvaret i petroleumsvirksomheten hvor Ptils er ansvarlig og følger opp virksomheten på sokkelen og navngitte landanlegg både med bakgrunn i petroleumsloven og brann- og eksplosjonsvernloven i egne forskrifter. Omtalen av DSB passer da ikke logisk inn i konteksten under 14.2. Det samme gjelder for omtalen av SD hvor utvalget skriver at «*flytende innretninger er underlagt Sjøfartsdirektoratet*». Dette innebærer ikke riktighet, det er Petroleumstilsynet som følger opp flytende innretninger i petroleumsvirksomheten og gir samsvarsuttalelser i trå med de fastsatte HMS-forskriftene.

Det er på denne bakgrunn viktig å kunne påpeke at Petroleumstilsynet (Ptil) er en sektormyndighet med ansvar for tilsyn med og regulering av sikkerhet, arbeidsmiljø, sikring og beredskap i petroleumsvirksomhet til havs og på enkelte landanlegg. Tilsynet er bemannet og organisert med høyt kvalifiserte medarbeidere med bredde- eller spisskompetanse innenfor sentrale fagområder: arbeidsmiljø, boring og brønn, HMS-styring, konstruksjonssikkerhet, logistikk og beredskap, sikring og prosessintegritet. Etter delegering av ansvaret for oppfølging av petroleumslovens § 9-3 om beredskap mot bevisste anslag fra ASD i 2013, har Ptil lagt ned ressurser i å styrke og bygge opp et fagfelt for å imøtekomme departementets forventninger om en mer prioritert oppfølging og innsats på det sikringsfaglige området.

I utvalgets punkt 14.7 «*Vurderinger og tiltak*» sies det at «*Det er utvalgets oppfatning at dagens sikkerhets- og tilsynsregime gitt med hjemmel i petroleumsloven er for svakt med tanke på den viktigheten anlegg på norsk sokkel har for norsk økonomisk bæreevne og for Norges internasjonale betydning og omdømme som olje og gass-leverandør. IKT-*

sikkerhetsnivået er i dag bestemt av bransjen selv gjennom egenutviklede standarder basert på ISO-standardene for sikkerhetsledelse. I sektoren ser man et behov for å oppdatere disse retningslinjene. I revisjonsarbeidet som pågår, er Petroleumstilsynet ikke invitert med. Utvalget ser at denne modellen gir et sterkt eierskap for bransjen. Den frakoblede myndighetsrollen er uheldig med tanke på de samfunnshensynene som rent bedriftsøkonomisk styring ikke ivaretar. Uønskede hendelser i digitale systemer på norsk sokkel, som i neste omgang kan gi utslag i fysisk skade på anlegg, jf. Tyrkia-hendelsen og Stuxnet, kan få store konsekvenser, ikke bare for Norge, men også for Norges viktige kunder i utlandet. I ytterste konsekvens får alvorlig svikt i leveransene konsekvenser for land som importerer store deler av sin gass og olje fra Norge. Utvalget mener at anlegg på norsk sokkel har betydning for vitale samfunnsinteresser og rikets sikkerhet, og at det ikke kan utelukkes at alvorlige hendelser kan inntreffe i fremtiden. Dette taler for en revisjon av sikkerhets- og tilsynsregimet sektoren har i dag.»

Ptils oppfølging av sikring og beredskap, herunder beredskap mot bevisste anslag tar på generelt grunnlag utgangspunkt i den delegerte myndighet vi har fått etter PLs kapittel 9, *Særskilte krav til sikkerhet*, som inkluderer oppfølging av sikkerhet, beredskap og beredskap mot bevisste anslag. Da presiseringen om beredskap mot bevisste anslag i § 9-3 kom inn i PL, og Ptil ble delegert myndighet for å følge opp denne, foretok Ptil en vurdering av det eksisterende regelverket og fant dette tilstrekkelig for å kunne forta innledende tilsyn på området for å kunne få oversikt over hvordan selskapene organiserte sitt sikringsarbeid. Til grunn for denne prioriteringen lå en vurdering av at det viktigste var å følge opp at petroleumsnæringen hadde iverksatt forbedringstiltak baser på kunnskap fra Statoils In Amenas rapport og Gjørv-kommisjonens rapport. Det ble også forutsatt at det skulle startes et regelverksarbeid innen 2-3 år som skulle basere seg på erfaringer fra tilsynet. Dette regelverksarbeidet er igangsatt og foreløpige konklusjoner slår fast at det er behov for å utvikle dette til i større grad å omfatte sikringsfaglige forhold, eksempelvis innen innsatsområdene fysisk sikring, IT-/informasjonssikkerhet og personellsikkerhet.

Ptils regelverk er risikobasert og funksjonelt utformet. Det baserer seg på et utstrakt samvirke mellom partene i arbeidslivet gjennom et trepartssamarbeid og forutsetter også et utstrakt partssamarbeid hos de enkelte aktører. I tillegg foregår det et utstrakt frivillighetsarbeid med utforming av normerende dokumenter hvor både industrien selv og myndighetene er sentrale bidragsytere. Ved å etablere en regelverksstruktur som gir funksjonelle og mer overordnede krav på det lovpålagte nivået, krever dette at man henter detaljerte spesifikasjoner fra andre ikke lovpålagte kilder som veiledninger, normer og standarder for å oppfylle regelverkets krav til forsvarlighet. Dette er en felles utfordring for myndighetene og industrien hvor den regulerende myndigheten kan dra nytte av de normeringsarbeider industrien selv gjennomfører ut fra egne behov, og samtidig sikre et forsvarlighetsnivå i regelverket og legge til rette for og stimulere til en god erfaringsoverføring i industrien. På sikringsområdet har Ptil deltatt som observatør/deltaker i arbeidet med å utarbeide bransjestandarden NOROG-104, men ikke i revisjonen av denne. Ptil har også deltatt i standardiseringsarbeider i regi av Norsk Standard/ISO på sikringsområdet. (NS/K 296 Samfunnssikkerhet og ISO TC 292 Security and resilience)

I pkt 14.7.1 *«Overføre sikkerhetstradisjonen innen HMS til det digitale området»* sier utvalget at *«Olje- og gassektoren har en lang sikkerhetstradisjon, en sterk sikkerhetskultur og høy kompetanse når det gjelder HMS. Selskapene har selv bygd ut infrastrukturen som er på norsk sokkel, inklusiv kommunikasjonsinfrastruktur. Arbeidet med IKT-sikkerhet er også så langt drevet av bransjen selv og Norsk olje og gass, samt gjennom initiativer til samarbeid som den enkelte virksomhet tar overfor Nasjonal sikkerhetsmyndighet og andre sikkerhets-virksomheter. Bransjen selv har tatt initiativ for bedre IKT-sikkerhet og utviklet en felles standard for sikkerhetsstyring, samt etablert samarbeid innen forebyggende sikkerhet.*

Det funksjonelle regelverket plasserer et stort ansvar på virksomhetene, som daglig opplever digitale trusler. For å redusere risiko implementerer selskapene barrierer, dels for å hindre at en uønsket hendelse skjer, dels for å redusere konsekvensene av en uønsket hendelse som har inntruffet. Det har vært økende oppmerksomhet rundt barrierer som hindrer en uønsket hendelse, men kvaliteten på disse barrierene er i liten grad testet og verifisert. ***Utvalget mener at bransjen bør videreutvikle den gode sikkerhetstradisjonen innen HMS, og overføre denne tradisjonen til det digitale området. Utvalget vil her henvise til arbeidet som gjøres i EU med hensyn til personvern og IKT-sikkerhet.»***

Vi oppfatter her at Lysneutvalget ønsker å gi honnør til den samarbeidsform og dialog som er utviklet under HMS-regimet i petroleumsvirksomheten og overføre disse prinsippene til IKT-sikkerhetsområdet. Ptil har i sin oppfølging av beredskap mot bevisste anslag lagt til grunn at den samme *«sikkerhetstradisjonen»* er til stede også på det digitale området. Ptil oppfatter at IKT sikkerhet er noe næringen har tatt til seg og jobber seriøst med. Prinsippene med å utvikle en god sikkerhetskultur og gode styringssystemer for oppfølging og kontinuerlig forbedring blir anvendt også på dette området selv om dette må tilpasses nye forutsetninger. Et viktig bidrag her vil være å videreutvikle og tilpasse regelverket på fagområdet. Bransjen sitt arbeid med å etablere retningslinje NOROG-104 og det pågående revisjonsarbeidet av denne retningslinjen kan også sees som tegn på dette. Her sikter en mot å oppdatere og modernisere retningslinjen, og en viser også til nyere standarder for konkretisering av retningslinjen.

Videre har DNV GL i november -2015 tatt initiativ til en JIP for å utarbeide standardiserte krav til Cybersikkerhet for olje- og gassnæringen med utgangspunkt i ISA/IEC standardene 62443-3-3, 62443-2-4 og 62443-4-2. Dette arbeidet er et initiativ for å konkretisere implementeringsløsninger i forhold til kravene i retningslinje NOROG-104 slik de framstår før moderniseringen av retningslinjen. I dette arbeidet deltar både operatørene, leverandørene og spesialistleverandører.

Henvisningen til arbeidet som gjøres i EU med hensyn til personvern og IKT-sikkerhet *«2012/0011 «EUROPA-PARLAMENTETS OG RÅDETS FORORDNING om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse»* oppfattes ikke primært å gjelde de konkrete forholdene som forordningen omhandler, men mer det fokus som settes på området datasikkerhet og behovet for at dette også er et tema i de enkelte selskapenes ledelse.

I punkt 14.7.2. *Verdivurdere sektorens anlegg og IKT-systemer, og etablere regelverk for digitale sårbarheter,* påpeker utvalget at «*Sikkerhetsloven og dens virkeområde er under revisjon. I påvente av ny sikkerhetslovgivning og en eventuell implementering av NIS-direktivet fra EU bør krav til IKT-sikkerhet gjøres tydelig i forskrifter. Kapittel 9 i petroleumsloven stiller krav til sikkerhet. I 2013 fikk Petroleumstilsynet også ansvar for sikring og beredskap mot bevisste anslag, slik det fremgår av petroleumsloven §9-3. Den omtalte lovparagrafen har ingen forskrifter eller juridiske forarbeider knyttet til seg. De sentrale forskriftene for den digitale sårbarheten i sektoren finnes i HMS-forskriftene for petroleumsaktiviteten og i arbeidsmiljøforskriftene. Forskriftene er ikke konkrete når det gjelder digitale trusler, men omfatter implisitt også digital sikkerhet. Utvalget mener at det bør foreligge krav fra tilsynsmyndigheten (Petroleumstilsynet) om at barrierer mot digitale sårbarheter skal være etablert.*

Ingen av olje- og gassinstallasjonene er per i dag definert som skjermingsverdige objekter i henhold til sikkerhetsloven. Behovet for beskyttelse bør uansett vurderes i lys av virksomhetens betydning for statens inntekter, og som utvalget har påpekt ovenfor den internasjonale betydningen olje- og gasseksporten har for våre viktige samarbeidspartnere. I påvente av ny sikkerhetslov, samt eventuelle pålegg og direktiver fra EU, anbefaler utvalget at det settes i gang et arbeid med verdivurdering og klassifisering av anlegg og IKT-systemer».

Utvalget kommenterer at § 9-3 ikke har «*forskrifter eller juridiske forarbeider knyttet til seg*». Som redegjort for over gjorde Ptil en vurdering av om eksisterende regelverk under kapittel 9 var tilstrekkelig for å kunne følge opp den nye § 9-3 og konkluderte med at man i en første fase hadde tilstrekkelig grunnlag, men at man innen en tidsperiode på 2 til 3 år basert på Ptils og virksomhetenes erfaringer med sikringsarbeidet, skulle igangsette et internt regelverksprosjekt med sikte på å tydeliggjøre krav til sikring som følge av den nye bestemmelsen. Ptils utgangspunkt i dette arbeidet er at sikring av sektoren best reguleres gjennom det samlede sektorregelverket med en helhetlig regulering av sikkerhet og sikring, Dette dekker krav til beskytte personell, miljø og materielle verdier mot utilsiktede og tilsiktede uønskede hendelser. Vårt mål er å tydeliggjøre hvordan regelverkets krav til blant annet risiko- og barrierestyring skal forstås innenfor sikringsområdet. Tilpasninger i regelverket skal etter planen tre i kraft 1. januar 2017.

Når det gjelder verdivurdering og klassifisering av anlegg og IKT-systemer, henvises til det arbeidet som ble gjort i forbindelse med sikkerhetslovens virkeområde og utvelgelse av skjermingsverdige objekter. OED har sektoransvaret for å vurdere om noen objekter er skjermingsverdige og utarbeidet i forbindelse med en henvendelse fra Nasjonal sikkerhets-myndighet (NSM), hvor departementene ble bedt om å innmelde eventuelle skjermingsverdige objekter innen petroleumssektoren, et notatet «*Utvelgelse av skjermingsverdige objekter etter sikkerhetsloven – forholdet til petroleumsvirksomheten.*», hvor de konkluderte med at det ikke var grunnlag for å utpeke skjermingsverdige objekter i norsk petroleumsvirksomhet etter sikkerhetsloven og forskrift om objektsikkerhet, men at infrastruktur og funksjoner er beskyttelsesverdige. Ptil har tatt dette til etterretning, og et eventuelt nytt arbeid på dette området må komme som et overordnet initiativ hvor det også vil være behov for en klargjøring av hvilke prinsipper som skal benyttes for en slik

verdivurdering og tiltak. Ptil prioriterer å videreutvikler eget regelverk i tråd med de behov vi har observert og diskutert med næringen på IKT-feltet.

I pkt 14.7.3 Tydeliggjøre rolle og kapasitet hos Petroleumstilsynet sier utvalget at «*Det norske tilsynsregimet i olje- og gassektoren er basert på prinsippet om internkontroll, tre-partssamarbeidet og risikobasert tilnærming innen HMS. Det norske regimet kan derfor virke overordnet og ikke detaljstyrende på forhold som blant annet har med den digitale sikkerheten å gjøre. Det norske regelverket inneholder en rekke krav som regulerer myndighetenes kontroll av selskapene, i tillegg til å regulere søknader, rapporter, varslinger med mer fra selskapene til myndighetene. Selskapene har kunnskap om verdikjeden. Petroleumstilsynet har faglig myndighetsansvar for sikkerhet, beredskap og arbeidsmiljø i petroleumsvirksomheten på norsk kontinentalsokkel, samt på enkelte anlegg på land. Utvalget observerer at Petroleumstilsynet har verdikjedekompetanse og kompetanse på teknisk sikkerhet i sektoren, men begrenset kapasitet når det gjelder tilsyn med sektorens IKT-sikkerhet og sårbarhet. Utvalget foreslår derfor at Petroleumstilsynet styrkes betraktelig på dette området.*»

Som nevnt innledningsvis, har Ptil etter delegasjon av myndighetsansvaret for å følge opp § 9-3 prioritert å bygge opp et eget fagområde for å imøtekomme departementets forventninger om en mer presisert oppfølging og innsats på det sikringsfaglige området. Fagfeltet er omfattende og utfordrende og inneholder mange spissfaglige komponenter som Ptil i dag har ansvar for å føre tilsyn med. Ptil har blant annet valgt å ha fokus på en systemtilnærming og bruker det eksisterende regelverket som grunnlag for tilsyn med blant annet barrierer. Likevel er det en utfordring at tilsynet i dag har begrenset kompetanse og ressurser til å gå i dybden innen alle sider av IKT-sikring, herunder blant annet kontornettverket som vil kunne være en inngangsvektor til styringssystemene, men også i seg selv påvirke driften ved en uønsket hendelse. Vi tar derfor utvalgets syn om styrking av kompetanse til etterretning og er enig i at Ptil med fordel kunne ha styrket sin kompetanse innen IKT sikkerhet eksempelvis gjennom å få tilført ressurser som et ekstraordinært tiltak.

I vurderinger av styrking av spissfaglig kompetanse vil det også være viktig å få avklart hvilke prinsipper som skal prioriteres og legges til grunn i oppfølgingen, og hvilke kompetanse og rolle Ptil skal ha i gjennomføringen av tilsyn i forhold til egne ressurser og bruk av andre relevante bistandsetater. Kunnskap på systemnivå sammen med muligheten til å være synlig i bransjen i forhold til sentrale problemstillinger er viktig samtidig som oppfølgingen på selskaps- og innretningsnivå må ivaretas.

I punkt 14.7.4 «*Vurdere tilknytning til responsmiljø for IKT-hendelser*» hevder utvalget at «*Sektoren mangler et felles responsmiljø. Bransjen er internasjonal og består av utenlandske og norske selskaper. De utenlandske selskapene kan være del av større internasjonale konsern og ha sikkerhetssamarbeid via sitt moderselskap eller eget responsmiljø innad i virksomheten. Bare noen få aktører i bransjen er tilknyttet NSM NorCERT. De små selskapene, som ikke er en del av et CSIRT-samarbeid, faller utenfor. Det er ikke etablert noe felles kontaktpunkt for sektoren som myndighetene eksempelvis kan benytte til varsling om nettbaserte angrep. Det er også få formelle fora der sektoren kan utveksle erfaringer. Utvalget anbefaler at virksomhetene i sektoren enten inngår et samarbeid med KraftCERT eller finner andre løsninger for operativt samarbeid. Ved valg av KraftCERT kan sektoren oppnå synergier som følge av likhet i teknologi, slik som styringssystemer. Dette er i tråd med*

løsninger som er valgt internasjonalt, slik som blant annet ICS-CERT i USA. Dette vil eventuelt aktualisere en debatt om alternativ tilknytning for KraftCERT.

Barrierer som reduserer konsekvensene av en uønsket hendelse, er mer mangelfulle i bransjen enn forebyggende barrierer. Det har vært økende oppmerksomhet rundt barrierer som hindrer en uønsket hendelse, men kvaliteten på disse barrierene er i liten grad testet og verifisert. Bransjen har en egen beredskapsorganisasjon som skal tre i kraft ved større hendelser, jf. sivilt beredskapssystem. Utvalget er ikke kjent med at denne har øvd på å håndtere store IKT-hendelser. Utvalget anbefaler derfor at sektoren gjennomfører øvelser i håndtering av uønskede IKT-hendelser.»

Ptil tar utvalgets uttalelser her til etterretning, men vil samtidig presisere at KraftCERT er et ideelt aksjeselskap, opprettet av Hafslund, Statkraft og Statnett som skal betjene energiforsyningen i Norge. Per 01.12.2015 er 45 kraftselskaper og ett vann- og avløpsselskap medlemmer. Hvis en skal foreta en utvidelse til også å kunne betjene vår næring, må dette godkjennes gjennom flere instanser blant annet styret i KraftCert samtidig som en må utvide staben av analytikere. En slik utvidelse må også ha forankring i relevant departement. Vår prioritering er å følge opp at den enkelte aktør og næringen som helhet har forsvarlige CERT-løsninger som er robuste og inkluderer videreutvikling og kontinuerlig forbedring.

Når det gjelder krav om øvelser i forhold til IKT, så følges dette opp på normal måte gjennom tilsyn, og egne tilsyn rettet mot selskapenes øvelser. For å understøtte utvalgets anbefaling her, er dette noe som kan tas opp i forbindelse med sikringstilsyn. Så langt er Ptil kjent med at det er gjennomført øvelser hvor IKT-hendelser er belyst. Ptil vil innhente relevante erfaringer herfra.

Ptil slutter seg også til at det er behov for et «single point of contact» mellom næringen og myndighetene. Det vil også være behov for å formidle informasjon fra andre kilder en myndighetene. For IKT-sikringshendelser har Ptil hatt funksjon som informasjonsformidler mellom NSM/NorCert og petroleumsnæringen og fulgt opp selskapenes tiltak i møter og tilsyn med pliktsubjektene.

Med hilsen

Anne Vatten.
Direktør Juss og
Rammevilkår

Finn Carlsen
Fagdirektør

Dette brevet er godkjent elektronisk i Petroleumstilsynet og har derfor ingen signatur