



Norsk olje & gass

HØVEDKONTOR /

Postboks 8065, 4068 Stavanger

besøk / Vassholmen 1, 4313 Sandnes

OSLO /

Postboks 5481 Majorstuen, 0305 Oslo

besøk / Middelthunsgate 27, 0368 Oslo

TROMSØ /

Postboks 448, 9008 Tromsø

besøk / Bankgata 9/11, 9008 Tromsø

TEL / +47 51 84 65 00

www.norskoljeoggass.no

Org. nr.: 956 685 818

Justis- og beredskapsdepartementet

Deres referanse

Deres dato

Vår saksbehandler

Aud Nistov

Vår referanse

19-866

Vår dato

06.03.2019

Norsk olje og gass' høringssvar til: NOU 2018:14 – IKT-sikkerhet i alle ledd og utkast til lov som gjennomfører EUs direktiv om sikkerhet i nettverk og informasjonssystemer (NIS-direktivet) i norsk rett

Det vises til Justis- og beredskapsdepartementets høring av 21. desember 2018 med høringsfrist 22. mars 2019.

Norsk olje og gass representerer rettighetshavere, operatørselskaper og leverandører som deltar i petroleumsvirksomheten. Vi har delt vårt høringssvar i henhold til følgende:

- Innledning som beskriver petroleumsvirksomheten
- Kommentarer til NOU 2018:14 – IKT-sikkerhet i alle ledd (Holte-utvalget) og utvalgets fem hovedanbefalingene.
- Kommentarer til Justis- og beredskapsdepartementets fem spørsmål relatert til utkast til lov som gjennomfører EUs direktiv om sikkerhet i nettverk og informasjonssystemer (NIS-direktivet) i norsk rett.
- Norsk olje og gass' oppsummering.

1. Innledning

Petroleumsvirksomheten i Norge er spredd over store geografiske områder. På norsk sokkel er det per 01.01.2019 i alt 60 innretninger og rigger i operasjon (herav betonginnretninger, flytende innretninger og bunnfaste stålinnretninger). I tillegg er det ca. 400 havbunnsinstallasjoner. Disse innretningene opererer 83 felt. Det finnes åtte landanlegg som er tilknyttet felt og rørledninger på norsk sokkel, fra Kårstø i sør til Melkøya i nord. Disse landanleggene (raffinerier, gassprosesseringsanlegg, LNG-anlegg m.fl.) dekker aktuelle behov for transport, lagring og behandling av olje og gass fra tilknyttede felt. Rørledningssystemet som knytter sammen felt og mottaksanlegg på land, herunder terminaler for mottak i UK, Belgia, Frankrike og Tyskland, utgjør hele 15 400 km undervannsrørledninger.

I tillegg kommer selskapenes kontorer på land som står i forbindelse med feltene offshore. Herunder kan også nevnes at en rekke selskaper har overført en del styringsfunksjoner fra hav til land slik at enkelte felt, helt eller delvis, kan opereres i sann tid fra land (stikkord: integrerte operasjoner). Integrerte operasjoner innebærer utnytting av avansert informasjonsteknologi for effektiv sammenkobling av mennesker, teknologi, arbeidsprosesser og organisasjoner, med sikte på å oppnå bedre beslutninger, bedre koordinering og økt yteevne. Teknologier for samhandling gjør det mulig å samarbeide på grunnlag

av sanntidsinformasjon på tvers av faglige disipliner, organisasjoner og geografiske lokasjoner. Petroleumsvirksomheten representerer en høyteknologisk industri, og vi ligger på flere områder langt framme med hensyn til digitalisering sammenliknet med annen industri.

I dag håndteres ivaretagelsen av IKT-sikkerhet og virksomhetsstyring helhetlig for virksomhetenes samlede aktivitet. Norsk olje og gass vil understreke at næringen har en sterk egeninteresse i at sikkerheten (inkludert IKT-sikkerhet) ivaretas på alle anlegg og innretninger.

2. Kommentarer til NOU 2018:14 – IKT-sikkerhet i alle ledd (Holte-utvalgets utredning)

Norsk olje og gass har følgende kommentarer til Holte-utvalgets fem hovedanbefalinger:

2.1 Ad. pkt. 1) Ny lov om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning

2.1.1 Gjeldende regulering i petroleumsvirksomheten

Petroleumsvirksomheten er underlagt petroleumsløven. Beredskap mot bevisste anslag mot denne virksomheten er regulert i petroleumsløvens § 9-3. Sikkerhet er regulert under § 9-2 med tilhørende forskrifter (Rammeforskriften, Styringsforskriften, Aktivitetsforskriften og Innretningsforskriften).

Det er Petroleumstilsynet som fører tilsyn med petroleumsvirksomheten (herunder IKT-sikkerhet) til havs og på åtte landanlegg.

Næringen har selv utarbeidet spesifikke retningslinjer for IKT-sikkerhet i prosess-, kontroll-, sikkerhets- og støttesystemer (Norsk olje og gass – 104 – Anbefalte retningslinjer for IKT-sikkerhet i prosess-, kontroll-, sikkerhets- og støttesystemer:

[104 recommended guidelines on security baseline requirements.pdf](#)

Innretningsforskriften § 34a om Kontroll- og overvåkingssystemer viser i sin veiledning til Norsk olje og gass' retningslinje 104. Denne retningslinjen er således gjort til et normert dokument.

<http://www.ptil.no/innretningsforskriften/category385.html>

For øvrig så vises det til mer informasjon under pkt. 3.1 og 3.4 i dette høringssvaret.

2.1.2 Ny lov om IKT-sikkerhet for samfunnskritiske virksomheter

Holte-utvalget viser til Direktoratet for samfunnssikkerhet og beredskap (DSB) sin rapport om Samfunnets kritiske funksjoner (2016). Petroleumsvirksomheten er eksportrettet og representerer derfor i henhold til DSBs vurderinger ingen samfunnskritisk funksjon.

2.1.3 Forslag om å utarbeide en lov som stiller krav til forsvarlig IKT-sikkerhet i alle norske virksomheter

Petroleumsvirksomheten er en internasjonal næring der samarbeid med og bruk av nasjonale og internasjonale leverandører og underleverandører (som ikke faller inn under petroleumsvirksomhet) er utstrakt. Vi ønsker at petroleumsindustrien blir regulert i samsvar med annen industri, og ønsker i mindre grad særkrav for norsk petroleumsvirksomhet. Når petroleumsvirksomhetens egenart tilsier det, kan særskilte forhold reguleres i henhold til petroleumsløven, men dette må etter Norsk olje og gass sitt skjønn ikke bli hovedregelen for reguleringen. Norsk olje og gass ser det som mest hensiktsmessig med

en sektorovergripende regulering på området IKT-sikkerhet som også kan omfatte petroleumsvirksomheten.

Norsk olje og gass støtter derfor Holte-utvalgets anbefaling om at det bør settes ned et lovutvalg som skal utrede behovet for og eventuelt utarbeide et forslag til en lov som stiller krav om forsvarlig IKT-sikkerhet til alle norske virksomheter. Denne lovens virkeområde (herunder i hvor stor grad petroleumsvirksomheten vil bli omfattet) må drøftes videre i lovarbeidet.

2.2 Ad. pkt. 2) Det må stilles krav om IKT-sikkerhet ved alle offentlige anskaffelser

Petroleumsvirksomheten faller ikke inn under offentlig virksomhet, og Norsk olje og gass er således nøytrale i forhold til denne anbefalingen.

2.3 Ad. pkt. 3) Nasjonalt IKT-sikkerhetssenter

Norsk olje og gass støtter denne anbefalingen da det er hensiktsmessig med en sentral enhet som kan fungere som et kontaktpunkt ved hendelser.

2.4 Ad. pkt. 4) Tydeligere regulering av og ansvar for tilkoblede produkter og tjenester

Norsk olje og gass støtter denne anbefalingen da "Internet of Things", d.v.s. tilkoblede produkter og tjenester, også vil "treffe" petroleumsvirksomheten i stor utstrekning.

2.5 Ad. pkt. 5) Justis- og beredskapsdepartementet må utøve et tydeligere lederskap for nasjonal IKT-sikkerhet

Norsk olje og gass støtter denne anbefalingen med det forbeholdet at ansvarsområdet departementene imellom er blitt endret etter at høringen ble sendt ut fra Justis- og beredskapsdepartementet 21.12.2018. Vi anbefaler at man legger opp til en helhetlig forvaltning, og at man i størst mulig grad avstår fra å fragmentere ansvaret for dette fagområdet.

3. Utkast til ny lov som gjennomfører EUs direktiv om sikkerhet i nettverk og informasjonssystemer (NIS-direktivet) i norsk rett

Utkast til ny lov som gjennomfører NIS-direktivet, skal forplikte virksomheter som tilbyr samfunnsviktige tjenester og enkelte digitale tjenester, til å gjennomføre IKT-sikkerhetstiltak og varsle om alvorlige IKT-sikkerhetshendelser. Et kriterium for å falle innunder lovens virkeområde er at virksomheten må tilby en tjeneste som er viktig for opprettholdelsen av kritiske samfunnsmessige eller økonomiske aktiviteter. Energi (elektrisitet, olje og gass) er listet opp under dette kriteriet i lovforslaget. Høringsnotatet – pkt. 12.3.2 konkluderer imidlertid med følgende: *"Det er vanskelig å se for seg at virksomheter som driver produksjon av olje og gass på norsk sokkel vil kunne defineres som tilbydere av samfunnsviktige tjenester. Dette sammenholdt med lovens geografiske virkeområde medfører at departementet antar at lovutkastet vil få begrenset betydning for norsk oppstrøms olje- og gassproduksjon."* Norsk olje og gass støtter denne konklusjonen.

Departementet har bedt høringsinstansene om særlig å gi innspill på en rekke spørsmål. Nedenfor følger Norsk olje og gass sine vurderinger av de gitte spørsmålene som må ses på bakgrunn av at petroleumsvirksomheten ikke faller innunder NIS-direktivets virkeområde.

3.1 I hvilken grad arbeides det per i dag systematisk med IKT-sikkerhet i din virksomhet? Følges for eksempel visse standarder for sikkerhetsstyring eller internkontroll?

Petroleumsvirksomheten jobber systematisk med IKT-sikkerhet, både når det gjelder mot anleggene offshore samt landanlegg og kontorer på land. Som eksempel kan det nevnes at IKT-sikkerhet for driftsrelatert utstyr (PCSS – Process Control and Safety Systems) er definert som en barriere på lik linje med andre sikkerhetssystemer på innretningene. For alle barrierer er det i de fleste selskapene en dedikert person TA (Teknisk Autoritet) som står som eier av barrieren som igjen er knyttet opp mot en operasjonell ytelsesstandard. Den operasjonelle ytelsesstandard har en rekke krav og verifikasjonsaktiviteter knyttet til seg, og disse har TA ansvar for å følge opp. Eventuell manglende oppfølging vil bli registrert som en hendelse/avvik i virksomhetenes avvikshåndteringssystem. Ytelsesstandard er basert på Norsk olje og gass' anbefalte retningslinje 104. Flere internasjonale standarder, herunder IEC 62443, brukes også for å følge opp disse aktivitetene. Det blir gjort risikovurderinger av individuelle systemer relevante for drift, og det gjennomføres overordnede sikringsanalyser.

Følgende eksempler på ulike sikringsaktiviteter kan nevnes (listen omfatter kun noen eksempler):

- Sårbarhetstester mot "phishing e-poster" blir gjennomført i de fleste selskaper.
- Sårbarhetssjekker mot internett blir jevnlig gjennomført både internt og av ekstern leverandør.
- Selskapsinterne sårbarhetssjekker og revisjoner gjennomføres jevnlig. Disse inkluderer manuelle sjekker og intervjuer. I tillegg brukes kontraktørselskap for å gjennomføre revisjoner ved behov.
- Infrastrukturen på land er bygd etter «beste praksis» med fysiske lokasjoner som inneholder kopier av alle data og de fleste tjenester. Deler av dataene blir også lagret på offline media.
- IT-recovery planer og back-up systemer er godt utviklet.
- "Cyber security awareness program" og policies/guidelines som setter krav til de ansatte, er blitt utarbeidet og implementert hos de fleste aktørene i petroleumssektoren, og flere selskaper har utviklet/benyttet seg av ulike opplæringsprogram på dette området.
- Det orienteres jevnlig om trusselvurderinger/-landskap i selskapene.
- Det er utarbeidet opplæringsprogrammer for å oppnå økt bevissthet rundt IKT-sikkerhet i de fleste virksomhetene.

Noen relevante standarder og rammeverk som benyttes av petroleumsnæringen innen IKT-sikkerhet er (merk at listen ikke er uttømmende):

Standarder utgitt av International Electrotechnical Committee (IEC):

- IEC 62443- Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program

Standarder utgitt av DNV GL:

- DNVGL-RP-G108 - Cyber security in the oil and gas industry based on IEC 62443

Standarder utgitt av International Organization for Standardization (ISO):

- ISO 27001 - Ledelsessystemer for informasjonssikkerhet - Krav
- ISO 27002 - Informasjonsteknologi - Sikringsteknikker - Tiltak for informasjonssikring
- ISO 27031 - Informasjonsteknologi - Sikringsteknikker - Retningslinjer for informasjons- og kommunikasjonsteknologiberedskap for forretningskontinuitet

Standarder utgitt av Standard Norge – Norsk Standard (NS):

- NS 5830 - Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger
- NS5831 - Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger - Krav til sikringsrisikostyring
- NS 5832 - Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger - Krav til sikringsrisikoanalyse

Standarder utgitt av American Petroleum Institute (API):

- API780 Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries

Retningslinjer utgitt av Norsk olje og gass (normative):

- Norsk olje og gass – 104 – Anbefalte retningslinjer for IKT-sikkerhet i prosess-, kontroll-, sikkerhets- og støttesystemer

I tillegg nevnes ulike rammeverk:

- Cyber security framework (CSF) from the National Institute of Standards and Technology (Nist) <http://www.nist.gov/cyberframework/>
- Cobit 5 (Control Objectives for Information and Related Technologies) is a good-practice framework for information technology (IT) management and IT governance. COBIT provides an implementable "set of controls over information technology and organizes them around a logical framework of IT-related processes and enablers.

3.2 Beskriv hvilke positive konsekvenser forslaget til gjennomføring av NIS-direktivet vil få for din virksomhet.

Norsk olje og gass viser til vår redegjørelse i dette høringssvaret under innledningen til kap. 3 der det framgår at petroleumsvirksomheten faller utenfor NIS-direktivets virkeområde. Innholdet i NIS-direktivet er imidlertid slik Norsk olje og gass ser det, langt på vei i samsvar med den måten petroleumsvirksomheten jobber med IKT-sikkerhet per i dag.

3.3 Beskriv hvilke negative konsekvenser forslaget til gjennomføring av NIS-direktivet vil få for din virksomhet.

Norsk olje og gass viser til pkt. 3.2. i dette høringssvaret.

3.4 Er din virksomhet per i dag underlagt krav til IKT-sikkerhet og varsling? Hvilket regelverk – lover, forskrifter eller annet – er det som stiller slike krav?

Petroleumsloven stiller krav om sikkerhet og forsvarlig petroleumsvirksomhet. Regelverket legger til grunn at selskapene selv vurderer risiko, setter akseptkriterier og beslutter relevante tiltak (både forebyggende og avbøtende tiltak). Etter styringsforskriftens § 29 skal operatøren sikre varsling til Petroleumstilsynet ved fare- og ulykkessituasjoner som har ført til, eller under ubetydelig endrede omstendigheter kunne ført til død, alvorlig og akutt skade, akutt livstruende sykdom, alvorlig svekking eller bortfall av sikkerhetsrelaterte funksjoner eller barrierer, slik at innretningens eller landanleggets integritet er i fare. Dette gjelder for både tilsiktede IKT-hendelser som påvirker anleggenes integritet, og for alvorlige utilsiktede IKT-hendelser.

EUs General Data Protection Regulation (GDPR), finanslovgivningen og regulering av handel med olje og gass, stiller tilsvarende krav til varsling ved ulike typer hendelser.

Flere av selskapene i petroleumsvirksomheten er medlemmer av NorCERT eller tilsvarende internasjonale CERT-miljøer (der hovedkontoret er lokalisert). Dette er imidlertid frivillige medlemskap.

3.5 Bør en slik lov som foreslås i denne høringen vedtas selv om vi ikke er forpliktet til det i henhold til EØS-avtalen?

Det vises her til dette høringssvaret under innledningen til kap. 3.

4. Oppsummering

Norsk olje og gass mener at det bør være en sektorovergripende regulering på området IKT-sikkerhet. Vi støtter således Holte-utvalgets forslag om at det bør settes ned et lovutvalg som skal utrede behovet for og eventuelt utarbeide et forslag til en lov som stiller krav om forsvarlig IKT-sikkerhet til alle norske virksomheter.

Petroleumsvirksomheten reguleres etter et funksjonsbasert regelverk. Norsk olje og gass anbefaler at reguleringen av IKT-sikkerhet på et nasjonalt sektorovergripende nivå også bør være funksjonsbasert.

Dersom det er behov for ytterligere redegjørelse av enkelte punkter, stiller Norsk olje og gass gjerne i et møte med departementet.

Med vennlig hilsen
Norsk olje og gass



Knud Thorvaldsen
Viseadministrerende direktør
Norsk olje og gass