DNV·GL

DIGITALE SÅRBARHETER LYSNEUTVALGET

Digitale Sårbarheter Olje & Gass

Lysneutvalget

Rapport nr.: 2015-0462, Rev. 1
Dokument nr.: 1O8VSAZ-2
Dato: 2015-04-24

Prosjekt navn:	Digitale Sårbarheter Lysneutvalget	DNV GL AS DNV GL Oil & Gas
Rapport tittel:	Digitale Sårbarheter Olje & Gass	Security & Information Risk
Kunde:	Lysneutvalget, C/O Fakturamottak Postboks 4900, Vika 8608 Mo i Rana Norway	Management P.O.Box 408 4002 Stavanger Norway
Kontaktperson:		Tel: +47 51 50 60 00
Dato:	2015-04-24	
Prosjekt nr.:	PP129301	
Organisation unit:	Security & Information Risk Management	
Rapport nr.:	2015-0462, Rev. 1	
Dokument nr.:	1O8VSAZ-2	
Kontrakt for leveranse av denne rapport:		

Hensikt:

Utarbeidet av:	Verifisert av:	Godkjent av:
Pål Børre Kristoffersen Principal Consultant	Mansur Abbasi Senior Consultant	Petter Myrvang Head of Section, Security & Information Risk Management
Tore Hartvigsen Principal Consultant		

DNV GL Distribution:

☒ Unrestricted distribution (internal and external)
☐ Unrestricted distribution within DNV GL
☐ Limited distribution within DNV GL after 3 years
☐ No distribution (confidential)
☐ Secret

Keywords:
Cybersecurity, Security, Digital Vulnerabilities, Oil & Gas, Information Risk Management, Lysneutvalget

Rev. Nr.	Dato	Formål	Utarbeidet av	Verifisert av	Godkjent av
0	2015-04-15	Høringsutkast	Pål Kristoffersen		
1	2015-04-24	Revidert etter høring	Pål Kristoffersen	Mansur Abbasi	Petter Myrvang

INNHOLD

1 SAMMENDRAG

Enhver aktivitet i olje- og gassektoren er forbundet med risiko forårsaket av trusler og sårbarheter. Dette gjelder i økende grad også risiko grunnet digitale sårbarheter. Uønskede hendelser, tilsiktede så vel som utilsiktede, kan ramme enkeltmennesker, bedrifter og samfunnet.

Norske etterretningsmyndigheter advarer om en økning i digitale trusler rettet mot norsk industri. Hendelser de siste årene viser at energi- og petroleumssektoren er blant de mest utsatte. Metodene blir stadig mer innovative og angriperne mer sofistikerte.

1.1 Digitale sårbarheter i olje- og gassektoren

Industrielle automatiserings-, kontroll- og sikkerhetssystemer som benyttes i olje- og gassektoren er i stor grad digitalisert og avhengig av digital teknologi. Tidligere var slike systemer proprietære, mens systemene i dag i stor grad er basert på kommersielt tilgjengelige komponenter som f.eks. PC med Microsoft Windows operativsystem. Det betyr at kjente sårbarheter for slike kommersielle standardprodukter også vil være eksponert i sektoren.

Tidligere ble det benyttet isolerte og proprietære nett mellom prosessutstyr og kontrollsystemer, mens det i dag benyttes nettverk basert på internett-teknologi. Industrielle automatiserings- og kontrollsystemer var tidligere fysisk adskilt fra tradisjonelle informasjonssystemer og åpne nett. Behov for overføring av produksjonsdata til informasjonssystemer, samt fjernvedlikehold, gjør at slik separasjon ikke lenger er praktisk mulig. Det er økende bruk av fjernoperasjon fra land eller nabo-plattformer, og dette kan medføre bruk av delte datanett. Dette betyr at produksjonsutstyr er eksponert for nettverks-relaterte sårbarheter.

Spredning av ondsinnet kode oppstår oftest grunnet menneskelige feil. Det åpnes vedlegg i e-post, det settes inn minnepinner, det lades mobiltelefoner, bærbare datamaskiner kobles til kritiske nett etc. Mobiltelefoner kan også lett etablere internettforbindelser. Brukere lures til å oppgi passord mm. Ved å legge operasjonsrom på land kan oppmerksomheten være mindre og dermed økes sannsynligheten for både utilsiktede og tilsiktede uønskede hendelser. Menneskelige feil ansees som den største digitale sårbarheten i sektoren.

Konsekvensen av uønskede hendelser basert på digitale sårbarheter vil i første rekke være av økonomisk art. Produksjonen må stenges noe som betyr tapte inntekter for næringslivet. Samfunnet vil få reduserte skatter og avgifter. Uønskede hendelser vil få betydning for selskapenes omdømme, og kan påvirke Norges omdømme som stabil produsent og transportør av energi. Dersom sabotasje- og terrororganisasjoner lykkes i å kontrollere vitalt produksjonsutstyr, kan konsekvensen bli miljøødeleggelse og tap av menneskeliv.

1.2 Avhengigheter

For å redusere utslipp av CO_2 fra kraftproduksjon på oljeinstallasjonene, baserer nye feltutbygginger seg ofte på kraftforsyning fra land (elektrifisering). De fleste av disse installasjonene må stenge produksjonen i tilfelle brudd på kraftforsyningen fra land. Det har over lenger tid vært et økende fokus på digitale sårbarheter i distribusjonssystemer for elektrisk kraft. Slike distribusjonssystemer er komplekse nettstrukturer med stor avhengighet til styring og kontrollsystemer.

Store avstander og store havdyp gjør at det er kostbart å etablere datanett til oljeinstallasjoner på norsk sokkel. Ofte benyttes fiberoptiske kabler på havbunnen, og slike kabler er utsatt for skade fra byggevirksomhet, fiskeriaktivitet og erosjon. Det er utfordrende å etablere redundante og helt uavhengige nettverksløsninger. Manglende kommunikasjon kan bety umiddelbar nedstenging av

produksjon på plattformer som opereres fra land eller nabo-plattformer. Dette er også kritisk for rørledninger der bl.a. trykk og mengde må kunne reguleres og overvåkes i hele systemet.

1.3 Samarbeid

Ansvar for forebyggende IKT-sikkerhet innen olje & gassektoren er fragmentert. 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.

Regjeringen bestemte i 2002 at Oljedirektoratet skulle deles, slik at tilsynet med sikkerhet ble lagt til en egen etat. Petroleumstilsynet, i dag underlagt Arbeids- og administrasjonsdepartementet, har faglig myndighetsansvar for sikkerhet, beredskap og arbeidsmiljø i petroleumsvirksomheten på norsk kontinentalsokkel, samt på enkelte anlegg på land. I 2013 fikk Petroleumstilsynet også ansvar for sikring slik det framgår av Petroleumsloven §9 – 3. Petroleumstilsynet har ikke et operativt fokus på digitale sårbarheter som utnyttes til terrorisme, sabotasje og hackervirksomhet. Dette ligger hos NSM, PST og Forsvaret. Disse organisasjonene har ikke et direkte inngrep med olje- og gassektoren med mindre det enkelte selskap har opprettet egen avtale om dette.

Objektsikkerhetsforskriften forvaltes av NSM og regulerer «eiendom som må beskyttes mot sikkerhetstruende virksomhet av hensyn til rikets eller alliertes sikkerhet eller andre vitale nasjonale sikkerhetsinteresser». Ingen av olje- og gass installasjonene er per i dag definert som skjermingsverdig objekt.

Elektrisitetsanleggene som forsyner olje- og gass installasjonene er ikke omfattet av Forskrift om forbyggende sikkerhet og beredskap som forvaltes av Norges vassdrags- og energidirektorat (NVE).

1.4 Beredskap

En uoffisiell, internasjonal undersøkelse blant selskaper i sektoren konkluderte med at kun 40 % av selskapene har etablert en beredskapsplan som dekker digitale sårbarheter. Fokus på krise og beredskap ligger på brann, eksplosjon, utblåsing, mm.

Justis- og beredskapsdepartementet (JD) har et spesielt ansvar for å samordne beredskapsarbeid, og Direktoratet for samfunnssikkerhet og beredskap (DSB) støtter JD i denne rollen. DSB har liten fokus på digitale sårbarheter.

1.5 Fremtidige problemstillinger og trender

Når denne rapporten skrives, er oljeprisen under 60 dollar pr fat, og det er stor usikkerhet om prisutviklingen videre. Dette betyr at sektoren må redusere kostnader for å opprettholde lønnsomhet. Det er en stor utfordring at disse sparetiltakene kan ramme den kontinuerlige forbedringen av sikkerhet. Økt fokus på kost/nytte-vurderinger og nye måter å arbeide på er viktige elementer framover.

Mange av innretningene på norsk kontinentalsokkel er designet for en levetid på mellom 15 og 25 år, og en rekke av disse har fått samtykke til forlenget levetid. Det betyr at mye av utstyr og programvare er utdatert og lite tilpasset dagens digitale sårbarheter.

Digitaliseringen av sektoren pågår kontinuerlig. «The Internet of Things» vil medføre flere enheter med digitale sårbarheter. Mengden av data som skal transporteres øker og standard IT-utstyr vil i økt grad være integrert sammen med de spesialiserte styresystemene.

Risikoen for at sentrale kritiske funksjoner, samfunnsviktig infrastruktur, skjermingsverdig informasjon og mennesker blir rammet av spionasje, sabotasje, terror og andre alvorlige handlinger er økende,

skriver Nasjonal sikkerhetsmyndighet (NSM) i sin årlige rapport, Risiko 2015 /1/. Samtidig håndterte NSM flere alvorlige dataangrep enn noen gang i 2014.

1.6 Overordnede risikoreduserende tiltak

For å redusere risiko implementeres det barrierer, til dels for å hindre at en uønsket hendelse skjer, og til dels for å redusere konsekvensen av at en uønsket hendelse har inntruffet. Det har vært et økende fokus på barrierer som hindrer en uønsket hendelse, men kvaliteten på disse barrierene er i liten grad testet og verifisert. Det er ikke tilstrekkelig kun å basere seg på en brannmur. Andre barrierer inklusive åpning/lukking av tilganger, prosedyrer og arbeidsprosesser må også etableres.

Barrierer som reduserer konsekvensen dersom en uønsket hendelse har inntruffet er mer mangelfulle. Det mangler utstyr og rutiner for å detektere at en trusselaktør har pågående aktiviteter mot en installasjon. Videre mangler innøvde rutiner på å forebygge negative konsekvenser når det er mistanke om at en uønsket hendelse kan inntreffe.

Det bør foreligge funksjonelle krav fra tilsynsmyndigheter om at barrierer mot digitale sårbarheter skal være etablert. Digitale sårbarheter må inkluderes i relevante risikoanalyser.

Selskapene må innarbeide en kultur for å redusere digitale sårbarheter på samme måte som det er en kultur for å hindre brann og eksplosjon. Holdningsskapende arbeid må prioriteres både innen sektoren, men også innen befolkningen generelt. Skoleverket må fokusere på oppførsel ved bruk at digitale medier.

2 INNLEDNING

2.1 Bakgrunn

NOU 2000:24 «Et sårbart samfunn» /2/ utreder olje- og gassvirksomheten, og omtaler at «Større integrering mellom tekniske systemer kan bli en utfordring i forhold til «security»-hensyn». Digitale sårbarheter utredes ikke. Siden rapporten ble skrevet, har dette definitivt blitt en utfordring, og skal utredes i Lysneutvalgets arbeid.

Mens digitale sårbarheter har hatt stor oppmerksomhet innen tradisjonell informasjons- og kommunikasjonsteknologi, har fokus på slike sårbarheter innen prosess- og industrisektoren kommet i de senere år. I 2010 ble man oppmerksom på Stuxnet ormen, som viste at målrettede digitale angrep kunne utnytte digitale sårbarheter og påføre signifikante skader på industrielt utstyr og infrastruktur.

I olje- og gassektoren har eksplosjonen i en oljerørledning i den tyrkiske byen Erzincan, 7. august 2008, vært en tankevekker. Flere år etter ulykken ble årsaken presentert, og det var tydelige indikasjoner på at dette var resultatet av et digitalt angrep. Hackere hadde slått av alarmer, slått av kommunikasjonslinjer og økt trykket i rørledningen.

Det er mange indikasjoner på at hele verdikjeden i petroleumssektoren nå er et mål for tilsiktede digitale angrep. E-tjenesten vurderer det digitale sikkerhetsbildet for 2015 /3/som følger:

> *«Nettverksbaserte etterretningsoperasjoner blir stadig mer målrettede, og teknisk avanserte, og fremmed etterretning angriper nå daglig norsk digital infrastruktur».*
>
> *«Sabotasjeaksjoner i det digitale rom vil i økende grad bli benyttet som virkemiddel ved fremtidige konflikter, kriser og kriger. Dersom fremmede makter gjennom nettverksbaserte etterretningsoperasjoner i fredstid erverver seg inngående kjennskap til kritisk infrastruktur, kan kunnskapen senere benyttes til å gjennomføre sabotasjeaksjoner. Flere stater utvikler skadevare som vil kunne brukes til å sabotere infrastruktur eller forstyrre kritiske samfunnsfunksjoner. Sabotasjeoperasjoner mot kraftforsyning, telekommunikasjon, betalingstjenester, politiske beslutningsorganer, samt militær kommando og kontroll, vil kunne forårsake betydelig skade.»*

I august 2014 henvendte NSM seg til 300 norske bedrifter innen olje- og energibransjen for å advare om et pågående komplekst og målrettet dataangrep. *«Dette åtaket er komplekst og målretta. Skadevara er skreddersydd, og vert ikkje fanga opp av andre kontrollrutinar. Det tyder på at det er ein aktør med store ressursar som står bak»* sa Hans Christian Pretorius, avdelingsdirektør i operativ avdeling hos NSM til NRK. /26/

2.2 Hensikt

Digitalt sårbarhetsutvalg (Lysneutvalget) ble nedsatt av regjeringen den 20. juni 2014, og er ledet av professor Olav Lysne. Utvalget skal foreslå konkrete tiltak for å styrke beredskapen og redusere den digitale sårbarheten i samfunnet. Utvalget skal levere sin utredning i form av en NOU til Justis- og beredskapsdepartementet innen utgangen av september 2015.

Mandatet til Lysneutvalget er omfattende og spenner over områder som sårbarhet i kritisk infrastruktur og samfunnsfunksjoner, datakriminalitet, personvern og sikring av informasjon. Lysneutvalget skal blant annet beskrive og analysere de digitale sårbarhetene som Norge står overfor i dag og nærmeste fremtid innen kritiske samfunnsfunksjoner og kritisk infrastruktur. Utvalget skal videre vurdere hvilke

konsekvenser denne sårbarheten kan få for enkeltmennesker, næringsliv og samfunnssikkerhet, samt se på samarbeid mellom offentlige og private aktører.

DNV GL bistår Lysneutvalget med dette arbeidet innen den norske olje- og gassektoren.

2.3 Metodikk

For å kartlegge digitale sårbarheter innen olje- og gassvirksomheten har DNV GL benyttet følgende metodikk:

- Innsamling av relevant erfaring
- Gjennomføring av arbeidsmøter med relevante aktører:
    - Operatører av felt
    - Utbyggingsprosjekter
    - Tilsynsmyndigheter
    - Operatører av infrastruktur for kommunikasjon
    - Operatør av rørledninger
    - Lysneutvalget
- Utarbeidelse av rapport

I arbeidsmøtene ble det benyttet kjent risikoanalysemetodikk. Deltakerne presenterte sårbarheter og årsaker, konsekvens og sannsynlighet ble diskutert. Risikoreduserende tiltak ble deretter diskutert.

2.4 Arbeidsgruppe

Følgende personer har bidratt på arbeidsmøter, samt kvalitetssikring av rapport:

- Mansur Abbasi, DNV GL
- Janne Hagen, Lysneutvalget
- Tore Hartvigsen, DNV GL
- Ragnar Heksem, Lundin
- Lars Idland, Statoil
- Are Jacobsen, Gassco
- Lene B. Kaland, Lysneutvalget
- Reidulf Klovning, Norsk olje og gass
- Pål Kristoffersen, DNV GL
- Sofie Nystrøm, Lysneutvalget
- Sven Haakon Olsen, Gassco
- Arnt Erling Skavdal, Tampnet
- Per Helge Svensson, Tampnet
- Anders Tysdal, Tampnet

- Asbjørn Ueland, Petroleumstilsynet
- Rune Wærstad, Norske Shell

DNV GL har organisert arbeidet, og er ansvarlig for rapporten.

2.5 Forkortelser og definisjoner

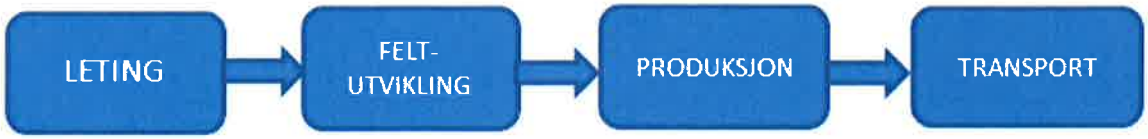
BOP	Blow Out Preventer
CERT	Computer Emergency Response Team
DSB	Direktoratet for samfunnssikkerhet og beredskap
DwH	Deepwater Horizon
GPS	Global Positioning System
IKT	Informasjon- og kommunikasjonsteknologi
IOGP	International Oil And Gas Producers Association
IT	Informasjonsteknologi
JD	Justis- og beredskapsdepartementet
NAC/NAP	Network Access Control/ Network Access Protection
NOROG	Norsk olje og gass
NOU	Norsk Offentlig Utredning
NSM	Nasjonal Sikkerhetsmyndighet
NVE	Norges vassdrags- og energidirektorat
OD	Oljedirektoratet
OT	Operasjonsteknologi
PTIL	Petroleumstilsynet
RISI	Repository of Security Incidents
SCADA	Supervisory Control and Data Acquisition
SIS	Safety Instrumented System
TCP/IP	Transmission Control Protocol/Internet Protocol
USB	Universal Serial Bus
VPN	Virtual Private Network

3 DIGITALE SÅRBARHETER I OLJE- OG GASSEKTOREN

3.1 Verdikjede

Den norske olje- og gassvirksomheten assosieres ofte med de store produksjonsinstallasjonene som henter hydrokarboner opp fra grunnen, de store landbaserte prosessanlegg som produserer olje- og gassprodukter, og de lange rørledningene på havbunnen som transporterer olje og gass til Europa. I olje- og gassvirksomhetens verdikjede inngår også sentrale ledd som salg, markedsføring, foredling, transport, forskning, myndighetsrapportering, med mer. I virksomheten skiller en mellom oppstrømsaktiviteter som de aktiviteter som gjøres for å bringe borestrøm opp fra grunnen og prosessere denne og nedstrømsaktiviteter som aktiviteter for å bringe olje- og gass produkter ut til forbrukere. I alle ledd i både opp- og nedstrømsaktiviteter, er informasjonssystemer vitale for alle operasjoner som utføres. Olje- og gassektoren er dermed digitalt sårbar i alle ledd i verdikjeden.

I de videre diskusjoner i dette dokument fokuseres det på den digitale sårbarhet i de fire leddene i verdikjeden hvor olje- og gassvirksomheten er spesiell i forhold til annen industri. Det fokuseres på den digitale sårbarheten i letevirksomhet, under feltutvikling, i produksjonsfasen og i transport av olje og gass til Europa i de store rørledningssystemene.



3.2 Letevirksomhet

Letefasen er en informasjonsintensiv fase. Formålet med leteaktivitetene er å finne nye forekomster av hydrokarboner som kan utvinnes. Enorme mengder data samles inn. Disse representerer store verdier for olje- og gasselskapene blant annet for å kunne vurdere verdi og lønnsomhet i mulige nye utbyggingsprosjekter. Kunnskap om verdien av nye felt kan påvirke børsverdien for selskapene. Viktige beslutninger om investeringer og samarbeidsforhold tas basert på informasjon om størrelser og hvilken type sammensetning (olje, gass, kondensat) man finner på feltet.

Den digitale sårbarheten til disse data betraktes primært å være relatert til *beskyttelse for tilgang til, sletting eller manipulasjon av dataene*. Datastrukturene er sammensatte og man trenger spesialistkompetanse både for å kunne navigere i datastrukturen men også for å kunne tolke og forstå dataene. Et strengt regime for informasjonsforvaltning er nødvendig for å beskytte disse data. Det er ikke kjent at det har vært noen hendelser i forhold til digital sårbarhet med denne type data. Det virker som bedriftene er bevisste på verdien av sin lete- og utvinningsrelatert informasjon, og beskytter denne godt.

Dokumenter med sammendrag og konklusjoner fra letevirksomhet vil være av meget stor interesse for utenforstående, og kan være et mål for digital spionasje. Digitale sårbarheter som kan medføre at slik informasjon kommer på avveie er primært *manglende oppmerksomhet og opplæring hos de ansatte* samt *manglende rutiner for klassifisering og behandling av sensitiv informasjon*.

Databasen «Diskos» er sentral i norsk- olje og gassvirksomhet. Diskos er en nasjonal lagringsbase for lete- og utvinningsrelatert informasjon. Databasen er opprettet og utformet av Oljedirektoratet og oljeselskapene representert på norsk sokkel. Basen inneholder til dels konfidensiell informasjon, og består hovedsakelig av brønn- og seismikkdata for norsk kontinentalsokkel. Mens oljeselskapene ikke har tilgang til hverandres data, har ansatte i offentlig virksomhet slik tilgang påpekte Riksrevisjonen i sin rapport til Stortinget. Diskos styres av Oljedirektoratet og inneholder nesten alle kartdata som finnes for norsk sokkel. «Dataene kan ha stor betydning for konkurransen mellom oljeselskapene, og være mål for dataangrep fra andre stater» sier riksrevisor Per-Kristian Foss til Bergens Tidende /27/.

Sanntids IKT systemer er vitale under borevirksomheten. Storulykken på Deepwater Horizon (DwH) skjedde under boring av en brønn på Macondofeltet i Mexicogolfen. For å illustrere hvordan digitale sårbarheter på en boreplattform kan bidra til utilsiktede ulykker og hva konsekvensene av en slik ulykke kan bli, er hendelsesforløpet som førte til ulykken kort gjengitt:

Den 20. april 2010 skjedde en utblåsing, eksplosjon og brann om bord på den flyttbare innretningen Deepwater Horizon (DwH). DwH opererte på oppdrag for BP i Mexicogolfen og var eid og driftet av Transocean. Hendelsen utviklet seg umiddelbart til en katastrofe. Elleve av de som var om bord da ulykken inntraff, omkom, og flere fikk alvorlige skader. Innretningen sank etter to døgn. Mer enn fire millioner fat olje strømmet ukontrollert ut av brønnen før lekkasjen ble stoppet 87 dager senere etter omfattende forsøk på å tette brønnen og ved hjelp av avlastningsboring.
Brønnen var designet slik at den senere skulle kunne brukes som en produksjonsbrønn. Under boreprosessen traff man på høyere trykk enn man hadde forventet noe som førte til endringer i det planlagte boreprogrammet. En måtte også gjøre endringer pga. operasjonelle problemer som oppstod underveis. DwH var utstyrt med de mest moderne, databaserte sikkerhetssystemer relatert til overvåkning av brønn, avstengning av brønn, frakopling av rigg, kraftforsyning, deteksjon og varsling av mannskap. Under ulykken sviktet alle disse informasjonssystemene helt eller delvis. Det ble i den påfølgende granskning påvist at det var kjent at flere av informasjonssystemene hadde feil og mangler og at dette var blitt ignorert og akseptert. Det var flere kjente programvarefeil på riggen. Et brønnspark (oppstår når formasjonstrykket i en petroleumsbrønn overskrider det hydrostatiske trykket og brønnvæske strømmer ut) var tidligere erfart på grunn av en slik feil. Datamaskinene som kontrollerte boreoperasjonene fungerte dårlig, i perioder hadde man ikke oversikt over tilstanden i brønnen. Et nytt system var bestilt, men feil i nytt operativsystem gjorde at gammel programvare ikke lot seg kjøre på det nye operativsystemet. Noen av riggens alarmsystemer, inkludert riggens generelle alarmsystemer, var slått av. Dette medførte at selv om sensorer på riggen registrerte høye gassnivåer, giftig gass eller brann, og overførte disse signaler til brann- og gassvarslingssystemet, så ble ingen alarm aktivert. Blow Out Preventeren (BOP) stengte ikke av brønnen slik den skulle gjøre. Det er uklart om den ble skadet under ulykken eller om den allerede var i ustand. Det var gjort observasjoner om lekkasjer fra BOPens hydrauliske kontrollsystem uten at man hadde gjort noe med dette. Myndighetene hadde krevd en resertifisering av BOPen, men dette ville nødvendiggjøre en nedstengning i 90 dager, og var ikke utført.

Faktaboks 1: Deepwater Horizon ulykken /13/

3.3 Feltutvikling

Utvikling og utbygging av nye felt er en investeringsintensiv fase. Mange aktører er involvert, som produsenter av hele eller store deler av installasjonene, utstyrsleverandører og tjenesteleverandører. Konkurransen er hard og et tilslag på et tilbud kan være «leve eller dø» for et selskap. Olje- og gasselskapene har velfungerende, velprøvde og sikre anbuds- og evalueringsprosesser. Strenge regler sørger for at informasjon om konkurrenters tilbud beskyttes, kun er tilgjengelig for et fåtall personer og bare blir benyttet til det som er formålet. Denne type informasjon kan være et mål for digital spionasje.

Gjennom forskning, erfaringer og samarbeid i bransjen har norsk industri bygd opp en stor ekspertise på feltutvikling av olje- og gassinstallasjoner til havs. Dette er en kunnskap som gir bransjen konkurransefordeler både for norske og internasjonale feltutbyggingsprosjekter. Slik kunnskap og dokumentasjon er ettertraktet og må beskyttes.

I byggefasen designes og dokumenteres installasjonene. Dokumentasjon om datanett, adresser, m.m. utveksles mellom leverandører og oljeselskap. Slik informasjon vil være av stor verdi for trusselaktører.

Digitale sårbarheter som kan medføre at slik informasjon kommer på avveie er primært *manglende oppmerksomhet og opplæring hos de ansatte, manglende rutiner for klassifisering og behandling av sensitiv informasjon* og *manglende herding og oppdatering av programvare.*

Utstyr for prosesskontroll tilpasses og utvikles i byggefasen. For å redusere kostnader benyttes standardkomponenter som f.eks. PC med Microsoft Windows eller Linux. *Det betyr at kjente sårbarheter for disse kommersielle produktene også vil være eksponert. Programvare som utvikles er i liten grad designet, utviklet og testet med tanke på digitale sårbarheter.*

Underleverandører spiller en viktig rolle ved design og produksjon av nye installasjoner. *Det er stor bekymring for at manglende sikkerhetskultur hos underleverandører* medfører at *digitale sårbarheter etableres i feltutviklingsfasen, og blir med prosjektene over i produksjonsfasen.*

Konsekvensen av uønskede hendelser grunnet digitale sårbarheter i feltutviklingsfasen er primært av økonomisk art for næringslivet.

Fra November 2009 har koordinerte og målrettede cyber angrep blitt utført mot globale olje-, energi- og petrokjemibedrifter. Disse angrep har inkludert «social engineering», «spear-phishing», angrep og utnyttelse av sårbarheter i Microsoft Windows operativsystem og bruk av remote administrasjonsverktøy for målrettet å høste inn sensitiv konkurranseutsatt informasjon om operasjoner og prosjekt finansiering i forhold til olje- og gass anbud og drift.

Faktaboks 2: McAfee White Paper: Global Energy Cyberattacks:"Night Dragon" /14/

3.4 Produksjon

Tidligere ble det benyttet proprietære nettverk mellom prosessutstyr og kontroll- og sikkerhetssystemer, mens det i dag benyttes i hovedsak nettverk basert på internett-teknologi (TCP/IP). Industrielle automatiserings- og kontrollsystemer var tidligere fysisk adskilt fra tradisjonelle informasjonssystemer og åpne nett. *Overføring av produksjonsdata til informasjonssystemer og fjernvedlikehold gjør at slik fullstendig separasjon i dag ikke er praktisk mulig*. Dette betyr at produksjons-utstyr er mer eksponert for nett-relaterte sårbarheter. Bryter en angriper gjennom forsvarsmekanismene til kontroll- eller sikkerhetssystemet kan vedkommende bl.a.:

- Gi kommandoer til kontrollsystemet som han ikke er autorisert til
- Sende falske meldinger til kontrollsystemets operatører om å initiere feilaktige aksjoner
- Forstyrre kontrollsystemets funksjonalitet ved å forsinke eller blokkere flyten av informasjon
- Gjøre uautoriserte forandringer i kontrollsystemet som modifikasjon av alarmgrenser eller andre konfigurasjonssettinger
- Sette resurser utilgjengelig
- Plante skadelig programvare som kan kommunisere med prosesser utenfor kontrollsonene

Personell som opererer installasjonene og bemanner kontrollrom kan påføre installasjonene stor skade. Spredning av ondsinnet kode oppstår oftest grunnet menneskelige feil. *Det åpnes vedlegg i e-post, det settes inn minnepinner, det lades mobiltelefoner, bærbare datamaskiner kobles til kritiske nett etc. Mobiltelefoner kan også lett etablere internettforbindelser. Brukere lures til å oppgi passord mm. Ved å legge operasjonsrom på land kan oppmerksomhet være mindre og gi muligheter flere for slike sårbarheter. Mangelfull avlåsing og merking av rom, skap, kabling bidrar til slike sårbarheter. Utro tjenere med omfattende rettigheter kan påføre virksomheten stor skade.*

Fjern-operasjon fra land eller nabo-plattformer kan medføre bruk av delte datanett. For å få redundante nettløsninger benyttes det ofte felles, delte datanett. *Slike nett kan være sårbare for avlytting og kommunikasjonsenheter har operatørgrensesnitt som er sårbare. Et tjenestenektangrep på et lite beskyttet segment (f.eks. brukt til underholdningsformål) i et delt nettverk kan medføre at kritiske segmenter blir berørt. Ettersom datanettet går via en rekke plattformer, vil strømstans på en plattform kunne berøre nettforbindelsen fra andre plattformer.*

Datanett i Nordsjøen er primært basert på fiberoptisk kabling på havbunnen. Det har vært få skader på denne infrastrukturen, men i områder med grunt vann (15-20 meter) og med mye havstrøm har det oppstått 5-6 skader over de siste 15 årene.

Kontrollsystemene blir anskaffet og drevet i grenselandet mellom to kulturer, informasjonsteknologi (IT) og operasjonsteknologi (OT). *Manglende kommunikasjon og forståelse mellom disse miljøene kan medføre digitale sårbarheter*. Eksempelvis prioriteres normalt konfidensialitet som den viktigste egenskap i et IT miljø, mens tilgjengelighet prioriteres høyest i et OT miljø. Løpende oppdatering av programvare kan aksepteres i et IT miljø, men kan kreve mer omfattende testing i et OT miljø.

De eldste anlegg representerer en større digital trussel enn de nye. Kontrollsystemer anskaffet til de eldste anlegg var isolerte og ikke tiltenkt oppkoplet i nettverk og integrert med andre IT systemer. *Disse kontrollsystemene inneholder ikke det samme nivå av feiltoleranse og innebygget sikkerhet som nyere systemer*.

Olje- og gassinstallasjoner benytter i stor utstrekning underleverandører som kommer med sitt utstyr og sine systemer i komplette pakker i form av moduler/«containere». Dette er ikke minst vanlig i tilknytning til boreoperasjoner. Slike moduler skal tilknyttes strøm og nett. *Det er vanskelig å kontrollere hvilke digitale sårbarheter hver enkelt modul medfører grunnet manglende dokumentasjon*. IT komponenter fra land som Norge ikke har sikkerhets-samarbeid med kan være spesielt sårbare.

> Flere stater har utviklet, eller er i ferd med å skaffe seg, avanserte virus for å kunne utnytte sårbarheter mot denne typen kontrollsystemer. Også terrorist- eller ekstremistgrupper, globale næringslivsbedrifter, hackergrupper og mulig også enkeltpersoner kan ha interesse av å bryte seg inn i denne typen systemer. Sabotasjeangrep mot kritisk infrastruktur og samfunnskritiske tjenester via denne typen systemer kan potensielt utrette stor skade

Faktaboks 3: Fra NSM sin rapport om sikkerhetstilstanden 2014./12/

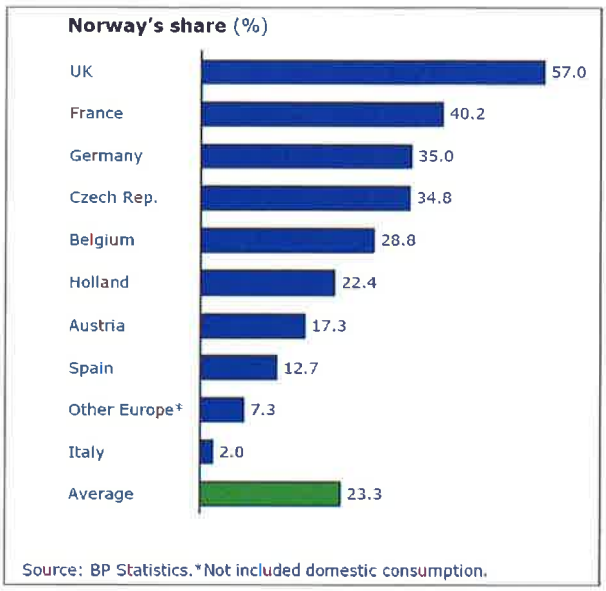
Konsekvensen av uønskede hendelser basert på digitale sårbarheter i produksjonsfasen vil i første rekke være av økonomisk art. Produksjonen må stenges noe som betyr tapte inntekter for næringslivet. Samfunnet vil få reduserte skatter og avgifter. Uønskede hendelser vil få betydning for selskapenes omdømme, og kan påvirke Norges omdømme som stabil produsent og transportør av energi. Dersom sabotasje- og terrororganisasjoner lykkes i å kontrollere vitalt produksjonsutstyr, kan konsekvensen bli miljøødeleggelse og tap av menneskeliv. Olje- og gassektoren er spesielt utsatt fordi det behandles

store mengder brann og eksplosjonsfarlig materiale, fordi ansatte bor på installasjonene og fordi mye av aktiviteten skjer til havs med store avstander fra land.

3.5 Transport

Norge er en viktig leverandør av olje og gass til Europa. Olje og gass blir i hovedsak levert gjennom rørledninger men også med skip.

Rapporten «The partnership between the Norwegian Oil & Gas Industry and the EU countries» /6/ utarbeidet av firmaet Econ på oppdrag av Norsk olje og gass, gjengir fakta relatert til leveranser av olje og gass til Europa. Denne rapporten viser tydelig hvor viktig norske gassleveranser til Europa er og også hvor viktig petroleumsaktivitetene på norsk sokkel er for næringslivet i Europa.



Faktaboks 4: Andel gass produsert i Nordsjøen i forhold til forskjellige nasjoners totale gassforbruk i 2013/6/

Rørledninger er eksponerte for sabotasje og ulykker siden de i store områder ligger ubeskyttet. *I tillegg er det også automatiserings- og kontroll- og sikkerhetssystemer som påvirker selve flyten av hydrokarboner i rørene. Disse systemene kan være digitalt sårbare*. Rørledningssystemene inkluderer stigerør, prosessanlegg og mottaksterminaler.

Gassco er operatør av det norske transportsystemet for gass. I følge kravene til beredskap i Petroleumsloven skal Gassco til enhver tid opprettholde en effektiv beredskap med sikte på å møte alle tenkelige farer og ulykkessituasjoner. Gasscos beredskapsorganisasjon bygger på nært samarbeid med Statoil og andre tjenesteleverandører, myndigheter og nødetater.

Rørledningen fra Baku i Azerbaijan går via Tbilisi Georgia til Cheyhan i Tyrkia. Statoil er sammen med 10 andre foretak, deleier i rørledningen. Rørledningen er utstyrt med sensorer for hver mil. Trykk, oljeflyt og andre kritiske indikatorer blir sent til et sentralt kontrollrom gjennom et trådløst overvåkningssystem. Kamera overvåker hele den 1.099 mil lange rørledningen. Eksplosjonen den 7-august-2008 aktiverte ikke et eneste feilsignal. Tyrkiske myndigheter hevder at en feilfunksjon forårsaket eksplosjonen, kurdiske separatister (PKK) hevder at de står bak. Hovedeieren, BP hadde rørledningen operativ igjen etter tre uker.
Det har senere vist seg at 60 timer med overvåkningsvideoer var slettet av hackere. Et infrarødt overvåkningskamera som ikke var koplet til det samme nettverk, viser to menn med bærbare datamaskiner som opphold seg nær rørledningen noen dager før eksplosjonen. Senere undersøkelser har avslørt at hackerne utnyttet et svakt punkt i systemet, selve overvåknings-kameraene. Kameraenes kommunikasjon programvare hadde sårbarheter som hackerne brukte til å få tilgang til og komme seg inn i det interne datanettverket. Inne i nettverket fant hackerne en maskin som benyttet et Windows operativsystem og som var ansvarlig for alarmstyringsnettverket. De kunne plassere egen kode her som gjorde det mulig å snike seg tilbake når de måtte ønske. Det sentrale element i angrepet var å få kontroll over styringssystemet slik at de kunne øke trykket i rørledningen uten at alarmer ble iverksatt. Angriperne kunne infiltrere programvaren på flere ventilstasjoner uten å trenge inn på hovedkontrollsentralen. De kunne øke trykket slik at dette forårsaket en eksplosjon og de kunne manipulere overvåkningssystemene slik at det ikke ble sendt meldinger om feilfunksjonering og lekkasjer til kontrollrommet.

Faktaboks 5: Digital sabotasje på rørledning i Tyrkia /16/

I mars 2012 rapporterte Department of Homeland Security (DHS) i USA at det pågikk et dataangrep på operatører av USAs naturgass-rørledninger. Hendelsen dro oppmerksomheten til en video som Federal Bureau of Investigation (FBI) hadde fått tak i. I 2011 oppfordret Al Qaeda til elektronisk Jihad mot kritisk infrastruktur i USA. Disse cybersecurity hendelsene koplet med alvorlige hendelser fra nylige ulykker med rørledninger, har gitt økt bekymring i den amerikanske kongressen om cybersikkerhet tiltak for USAs rørledninger.

Det har ikke vært noen tilfeller i USA hvor undersøkelser har avslørt at cyber angrep har forårsaket skade, men det er flere dokumenterte eksempler hvor problemer med kontrollsystemer knyttet til rørledningene har bidratt til ulykker som har fått katastrofale konsekvenser:

San Bruno, CA – I 2010 eksploderte en naturgassrørledning som drepte 8 personer, skadet 60 andre og ødela 37 boliger. Feil i og utilgjengelig kontrollsystem, trykkavlesning og andre mangler i kontrollsystemet var delaktig i for høyt trykk som ødela rørledningen.
Marshall, MI - I 2010 rant 809,000 gallons med råolje ut i Kalamazoo elven. Flere forskjellige kontrollsystemfeil, inkludert feilhåndtering av alarm for trykk, forsinket håndteringen og førte til økt omfang av lekkasjen.
Bellingham, WA—I 1999 eksploderte en bensinrørledning som forårsaket at 3 personer døde samt $45 millioner i skade på vannforsyning og annen eiendom. Kontrollsystemet som styrte drift av rørledningen feilet og tillot ikke å analysere tilstanden på rørledningen og respondere på driftsproblemene som førte til feilen.

Selv om alle disse hendelsen er utilsiktede er de eksempler på konsekvenser en vil kunne erfare etter et cyber angrep.

Faktaboks 6: US Congressional Research Service: Pipeline Cybersecurity: Federal Policy /19/

Konsekvenser av uønskede hendelser basert på digitale sårbarheter innen transport vil i første rekke gi økonomiske tap og tap av omdømme. Mottakere av gass i Europa er avhengig av stabile og forutsigbare leveranser. Uønskede hendelser kan få betydning for Norges omdømme som gasseksportør. Det transporteres eksplosivt materiale, og dersom sabotasje- og terrororganisasjoner lykkes i å kontrollere vitalt produksjonsutstyr, kan konsekvensen bli miljøødeleggelse og tap av menneskeliv.

3.6 Topp 10 digitale sårbarheter i olje- og gassektoren

For å oppsummere observasjonene er det laget en overordnet opplisting av de 10 antatt mest relevante digitale sårbarheter i sektoren. Disse sårbarhetene er ikke innbyrdes sortert i henhold til kritikalitet:

1. Manglende oppmerksomhet og opplæring hos de ansatte
2. Fjernarbeid
3. Bruk av standardprodukter med kjente sårbarheter i produksjonsmiljø
4. Mangelfull sikkerhetskultur hos underleverandører
5. Mangel på separasjon av datanett
6. Mobile lagringsenheter (inklusive smarttelefoner)
7. Datanett mellom landinstallasjoner og oljefelt
8. Manglende fysisk sikring av datarom, kablingsskap, m.m.
9. Sårbar programvare
10. Utdaterte styresystemer på installasjoner

4 SÆRSKILTE TEMAER

4.1 Avhengighet av kraftforsyning og datakommunikasjon

Kraftproduksjonen på land som alternativ til kraftproduksjon på olje- og gass installasjonene, er et miljøtiltak som nå innføres på en rekke installasjoner. I henhold til innstilling nr. 114 (1995-1996) fra Stortingets energi- og miljøkomite, besluttet Stortinget (St.prp. nr. 65 (1996-97)) at «Ved alle nye feltutbygginger skal det legges fram en oversikt over energimengden og kostnadene ved å elektrifisere installasjonen fremfor å bruke gassturbiner» /22/.

Martin Linge blir det syvende feltet på norsk sokkel som får strømtilførsel fra land. Til nå er tilsvarende løsning etabler for Gjøa, Valhall, Ormen Lange, Troll A, Snøhvit og Goliat feltene. Stortinget har besluttet at Johan Sverdrup-feltet skal dekke sitt kraftbehov fra land, og at feltene Gina Krog, Ivar Aasen og Edvard Grieg senest innen 2022 også skal forsynes med kraft fra land /23/.

Det store energibehovet til en olje- og gassinstallasjon stiller krav til elektrisitetsproduksjon og infrastruktur på land og vil ha betydning for den innenlandske kraftbalansen.

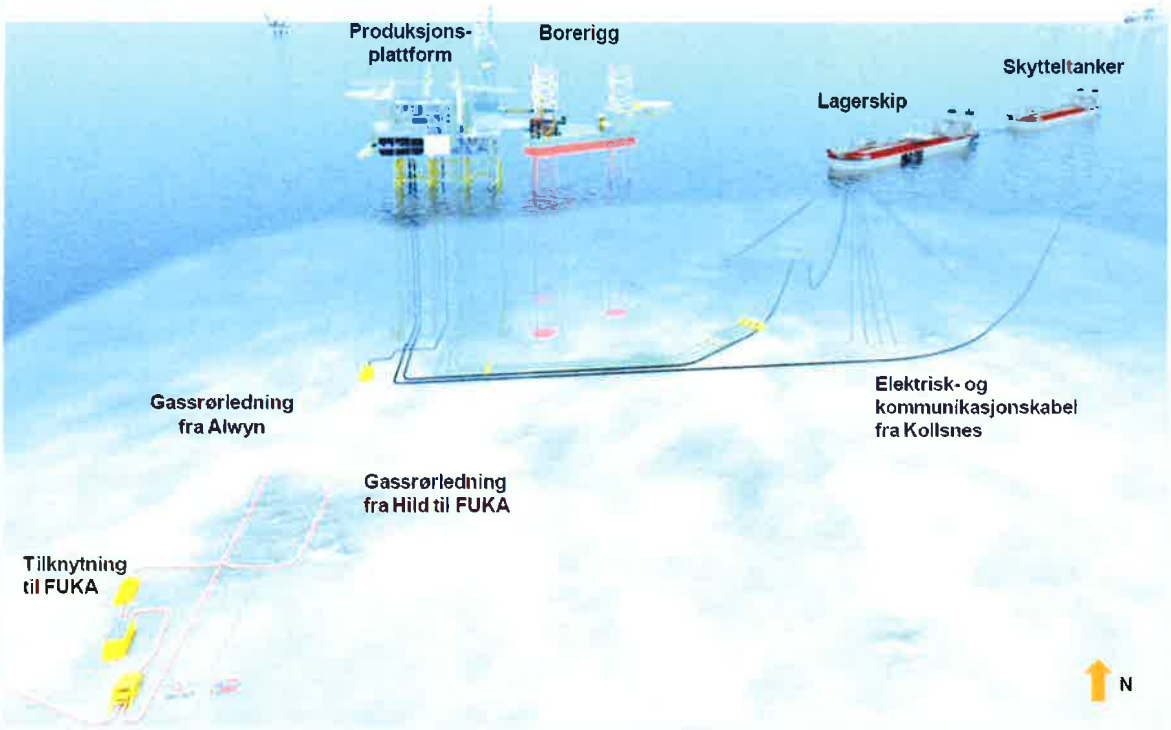
Utfall i leveranse av elektrisk kraft vil medføre at produksjonen på installasjonen stopper dersom ikke system for reservekraftproduksjon er etablert.

> Kraftproduksjonen er av vesentlig betydning for alle funksjoner og sektorer i samfunnet. Forstyrrelser i leveranse av elektrisk kraft kan få lammende effekter på samfunnets evne til å levere varer og tjenester til befolkningen. Effekten på evnen til styring på alle nivåer i samfunnet vil etter NSMs vurdering også trolig være svært omfattende. Omfattende eller langvarig stans i energiforsyning reduserer også mest sannsynlig statssikkerheten og den nasjonale handleevnen. Det at enkelte virksomheter og departementer ikke har fulgt sikkerhetslovens skadevurderingssystematikk for utpeking og klassifisering av skjermingsverdige objekter medfører en risiko for at objekter er klassifisert feil. Etter NSMs vurdering kan dette medføre at det ikke er iverksatt nødvendige sikringstiltak, og det kan medføre at det er iverksatt unødvendig ressurskrevende sikringstiltak.

Faktaboks 7: Fra NSM sikkerhetsvurdering 2014 av kraftproduksjonen /12/

Som eksempel på et felt under utbygging som er avhengig av kraftforsyning på land og som har kontrollrom på land, er en beskrivelse av Martin Linge feltet tatt med.

Utbyggingsplanen for Martin Linge feltet består av en integrert brønnhode-, produksjons- og boligplattform hvor brønnstrømmen fra olje- og gassreservoarene blir behandlet. Gass skilles fra olje og vann før gassen transporteres til land. Gass eksporteres via rørledninger til St. Fergus gass terminal i Skottland. Adskillelse av olje og vann skjer på en ombygget tankbåt som ligger 3,4 km fra hovedplattformen. Tankbåten blir ombygget til å være en flytende lagrings- og lossingsenhet og blir også forsynt med strøm fra land via plattformen. Vann sendes tilbake til plattformen og blir reinjisert i feltet gjennom en egen brønn. Oljen blir eksportert via tankere som kopler seg til den ombygde tankbåten. En 161 km lang strøm og fiberkabel vil bli lagt fra Kollsnes i Hordaland ut til produksjonsplattformen på feltet. Fra Kollsnes vil digital kommunikasjon bli etablert gjennom offentlige datanettverk til Totals kontor i Dusavika ved Stavanger. Her etableres det sentrale kontrollrommet for feltet. Et lokalt kontrollrom vil også bli etablert på plattformen som en reserveløsning. Det etableres også fiber og strømkabler fra plattformen til den ombygde tankbåten. En alternativ kommunikasjonsvei etableres også fra Martin Linge via Huldra plattformen til land. Martin Linge vil ha dieselgeneratorer for å generere nødstrøm.



Faktaboks 8: Planlagt strøm og fiberoptisk kommunikasjon i Totals Martin Linge prosjekt /30/.

Økt årvåkenhet mot mulig virusangrep

NVE har bedt kraftforsyningen om økt årvåkenhet og skjerping av datasikkerheten i forbindelse med det nye viruset Duqu.

0

Sikkerheten rundt kontrollsystemene som styrer norsk kraftforsyning er god, og NVE har ingen indikasjoner på at noen virksomheter i kraftforsyningen er infisert med Duqu. Det nye viruset er konstruert for å innhente informasjon som kan brukes til målrettede angrep mot ulike typer kontrollsystem.

NVE har bedt virksomhetene i kraftforsyningen om å øke årvåkenheten og skjerpe datasikkerheten i eget selskap for å forhindre at Duqu infiserer kritiske systemer. NVE oppfordrer også selskapene om å ta kontakt med sine leverandører av datasikkerhetstjenester og prosesskontrollsystem for å få råd og veiledning.

Sikring av systemene som styrer norsk kraftforsyning er regulert i "Forskrift om beredskap i kraftforsyningen". For de viktigste anleggene stilles det svært strenge krav til datasikkerhet, og NVE har i lengre tid hatt høy fokus på at selskapene etterlever kravene gjennom tilsyn, rådgivning og samarbeid med virksomhetene i kraftforsyningen.

Faktaboks 9:Fra NVE sin hjemmeside /15/

Sikring av systemene som styrer norsk kraftforsyning er regulert i "Forskrift om beredskap i kraftforsyningen". For de viktigste anleggene stilles det svært strenge krav til datasikkerhet, og NVE har i lengre tid hatt høy fokus på at selskapene etterlever kravene gjennom tilsyn, rådgivning og samarbeid med virksomhetene i kraftforsyningen. *De elektriske anleggene som forsyner oljeinstallasjonene er ikke omfattet av denne forskriften.*

Datakommunikasjon til oljeinstallasjoner på kontinentalsokkelen er primært basert på fiberoptisk kabel, men i noen grad også radiolinje eller satellittkommunikasjon. Firmaet Tampnet opererer det største offshore kommunikasjonsnettverket i Nordsjøen og betjener de fleste olje- og gassinstallasjoner i Nordsjøen ved fiberkabler og punk-til-punkt radiolinje forbindelser. Tampnet har dermed en unik rolle som infrastrukturleverandør til norsk olje- og gassvirksomhet. De kan tilby redundans ved å kombinere linjeforbindelsene og reduserer dermed sårbarheten for utfall. Tampnets hovedprodukt er å levere stabil og pålitelig fysisk kommunikasjon mellom to punkter. Sikring av trafikken på nettverket og bruk av nettverket er brukeren selv ansvarlig for. Tampnet eies av det svenske investeringsselskapet EQT partners. *Det er behov for flere uavhengige nettløsninger for å redusere risiko for feil.*

Det er stor skipsaktivitet i relasjon til olje- og gassvirksomheten. En rekke fartøy holder posisjon tett inn til oljeinstallasjonene ved hjelp dynamiske posisjoneringssystem som er avhengig av posisjonssignaler fra satellitt (GPS). En kollisjon mellom en plattform og f.eks. et forsyningsfartøy eller en flytende boligplattform kan få alvorlige konsekvenser. Likeledes vil feil i posisjoneringssystem kunne medføre alvorlige hendelser ved dykkeaktivitet. Antall fartøyer på kollisjonskurs har blitt sterkt redusert de siste årene, blant annet p.g.a. en utvidet radarovervåkning av installasjonene.

4.2 Avhengigheten av andre innsatsfaktorer

Forståelsen for den digitale sårbarheten i virksomheten og evnen til å innføre tilstrekkelige tiltak for å beskytte seg for digitale trusler er relatert til kulturen i virksomheten. En god kultur for å ta de digitale

trusler på alvor er avhengig av den generelle sikkerhetskulturen i sektoren og vilje til å bruke ressurser på adekvate og tilstrekkelige tiltak. Petroleumstilsynet sier i sin hovedrapport /7/ etter gjennomgang av DwH ulykken at «Sikkerhetskulturen i Olje- og Gassnæringen har en sammenheng med kostnadskutt, utsatt vedlikehold og manglende investeringer i sikkerhetssystemer. Dette er et ledelsesansvar. I stedet for å ta inn over seg usikkerheten aktørene står overfor i forkant av en uventet hendelse, klandrer vi dem for at de ikke på forhånd skjønte det vi ser så tydelig i ettertid. I stedet for å lære noe om hvor stor usikkerhet vi står ovenfor i beslutningene vi fatter, blir vi etterpåkloke. Igjen blir konsekvensen at vi undervurderer behovet for robuste beslutninger fordi vi lærer oss å undervurdere usikkerhet om fremtiden».

Etter DwH-ulykken er det igjen reist spørsmål om sikkerhetskulturen i oljesektoren, Norge inkludert. Petroleumstilsynet sier i sin rapport /7/: «Olje- og gassnæringen er en internasjonal næring som påvirkes av globale forhold, og granskingsrapportene bekrefter behovet for å se på DwH-ulykken som resultatet av en systemfeil, det vil si feil over tid i et system av sammenhengende, til dels gjensidig avhengige aktører og prosesser. Vi kan med andre ord ikke distansere oss fra denne ulykken. Når presidentkommisjonen etter DwH-ulykken utfordrer sikkerhetskulturen i hele industrien, gjelder dette også industrien i Norge, myndighetene inkludert.»

4.3 Samarbeid mellom næring, interesseorganisasjoner og myndigheter

De sentrale aktører i arbeidet med regelverk og avtaler som er relatert til digital sårbarhet innen olje- og gassvirksomheten er:

Norsk olje og gass (NOROG). En interesse- og arbeidsgiverorganisasjon for oljeselskaper og leverandørbedrifter knyttet til utforskning og produksjon av olje og gass på norsk kontinentalsokkel. NOROG er en landsforening i NHO, Næringslivets Hovedorganisasjon.

Petroleumstilsynet (PTIL) er et selvstendig, statlig tilsynsorgan med myndighetsansvar for sikkerhet, beredskap og arbeidsmiljø i petroleumsvirksomheten. Petroleumstilsynet var tidligere en del av Oljedirektoratet. Regjeringen bestemte i slutten av 2002 at Oljedirektoratet skulle deles, slik at tilsynet med sikkerhet ble lagt til en egen etat (PTIL). Petroleumstilsynet er nå underlagt Arbeids- og sosialdepartementet.

Oljedirektoratet (OD) ligger under Olje- og energidepartementet og er det statlig fagdirektorat og forvaltningsorgan for norsk petroleumsvirksomhet. OD har et nasjonalt ansvar for data fra norsk kontinentalsokkel.

Operatørselskapene. Ifølge ODs faktasider er 37 selskaper registrert som operatører på norsk sokkel.

Leverandørindustrien er tatt med som et samlebegrep på alle de som leverer produkter og tjenester til petroleumsvirksomheten.

Det er ikke etablert en formell prosedyre for melding av digitale trusler fra myndighetene til bedriftene i olje- og gassektoren. Ved en hendelse i 2014 sendte NSM melding til Petroleumstilsynet som brukte sitt kontaktnett til å varsle bedriftene. Petroleumstilsynet har etterpå blitt kritisert for at meldingen ble gitt til feil personer og at personer som burde blitt informert, ikke ble det. Det finnes ingen spesiell kontaktliste for melding om digitale trusler fra sikkerhetsmyndighetene til selskapene. De største selskap, som Statoil, har etablert en egen direkte dialog med sikkerhetsmyndighetene og blir fortløpende oppdatert om trusselbildet gjennom denne dialogen. De store internasjonale selskap blir oppdatert fra sine sentrale fagmiljøer. Det kan se ut som at de mindre selskap ikke har tilsvarende muligheter og har en større utfordring med å bli oppdatert om nye trusler.

Det anbefales at en prosedyre for melding av trusler som sikkerhetsmyndighetene finner det riktig å overbringe næringen etableres. Prosedyren bør inneholde detaljert informasjon med hvem som skal informere, hvem som skal informeres og på hvilken måte en slik melding skal gis.

Det finnes ingen sentral registrering av hendelser eller nesten hendelser relatert til digitale sårbarheter som bedriftene har erfart. Læring og koordinering mellom bedriftene blir derfor ikke optimal. Bransjen bør diskutere hvordan slik erfaringsutveksling skal fungere og hva myndighetenes rolle i denne forbindelse bør være.

Hendelser og nestenhendelser med et alvorlig skadepotensiale skal rapporteres til Petroleumstilsynet. Bedriftene i olje- og gassvirksomheten informerer om kontinuerlige og omfattende angrep på sine IKT systemer. Ingen hendelser som skyldes digitale angrep har så langt blitt rapportert til Petroleumstilsynet. Hvor grensen går for å rapportere og hva som skal rapporteres virker uklart. Det samme gjelder koordinert innsamling av denne type data. Når ikke koordinert registrering skjer får en også begrenset mulighet til læring. Manglende rapportering kan skyldes at bedriftene er redd for sitt omdømme men er kanskje også et uttrykk for at bedriftene ikke anser disse truslene som så alvorlige at de vil kunne få alvorlige konsekvenser for produksjonen. Manglende åpenhet om erfarte digitale trusler og manglende utveksling av erfaring med slike trusler gjør at samarbeidet i sektoren ikke er optimalt. En manglende klar autoritet på området kan være en av årsakene. Både Petroleumstilsynet og Norsk olje og gass har tatt initiativ til aktiviteter for å få satt arbeidet med digitale trusler på dagsorden.

Det har i flere år pågått et eget prosjekt i regi av Norges Forskningsråd for å evaluere eksisterende regelverk og reflektere bredt over hva som betegner en robust regulering i norsk olje- og gassvirksomhet og hvilke forutsetninger som er viktige for å få et mer robust regelverk. Prosjektet har dratt inn ekspertise og erfaringer fra flere miljøer, flere parter og ulike land./10/

Norsk olje og gass startet i 2005 (Den gang OLF – Oljeindustriens Landsforening) et arbeid for å etablere retningslinjer for IKT-sikkerhet for styrings- og sikkerhetssystemer. Bakgrunnen var en dramatisk økning i mengden virusangrep, hendelser på norsk sokkel og for å etablere et reaksjonsmønster tilpasset «normal IT-drift».

Dette førte til at følgende Norsk olje og gass retningslinjer ble etablert:

- 104 Anbefalte retningslinjer krav til informasjonssikkerhetsnivå i IKT-baserte prosesskontroll-, sikkerhets- og støttesystemer /25/.
- 110 Recommended guidelines for implementation of information security in Process Control, Safety and Support ICT systems during the engineering, procurement and commissioning phases. /33/
- 123 Recommended guidelines for classification of process control, safety and support ICT systems based on criticality. /34/

I sektoren er det en oppfatning om at det er behov for å oppdatere disse retningslinjer.

Resultat av PTILs tilsyn i 2012 (basert på egenevaluering fra selskapene)

Basert på et spørreskjema som inneholder de samme retningslinjer som Norsk olje og gass retningslinje 104 ble bedriftene bedt om å gjøre en egenevaluering av den digitale sårbarheten.

Rapporten indikerer at det står dårligst til for borerigger. Spesielt scoret borerigger svakere på kriterier som at brukerne må ha tilstrekkelig forståelse for sikkerhetsrisiko og akseptabel bruk av systemene samt for planer for gjennomrettelser etter at mulige hendelser har inntruffet.

Tilsynet omfattet landanlegg, produksjonsanlegg og borerigger
De svakeste punktene samlet sett var:

Brukerne av prosess kontroll systemer, sikkerhets og støtte IKT systemer skal være utdannet i Informasjonssikkerhetskrav og akseptable bruk av IKT systemer
- Manglende forståelse for sikkerhetsrisiko og akseptabel bruk av systemene

Planer for å opprette drift etter en ulykke skal dokumenteres og testes for kritisk prosesskontroll, sikkerhets og IKT støttesystemer.
- Manglende planer

Prosesskontroll, sikkerhets og IKT støttesystemer skal kun anvendes for tiltenkt formål
- Systemene brukes også til andre formål

Prosesskontroll, sikkerhets og IKT støttesystemer skal ha adekvat, oppdatert og aktiv beskyttelse mot skadelig programvare.
- Krevende å ha oppdatert beskyttelse mot virus o.l.

Faktaboks 10: Resultat fra Petroleumstilsynets presentasjon av tilsyn med IT sikkerhet i olje- og gassvirksomheten /20/

4.4 Internasjonalt samarbeid.

Det virker ikke som det finnes noen internasjonal bransjearena for digital sårbarhetsvurdering hvor norsk olje- og gassvirksomhet er representert. Gjennom bransjeorganisasjoner, standardiseringsarbeid, fagforum, etc. deltar det representanter fra norsk olje- og gassvirksomheter, men det finnes ikke et koordinert organ som spesifikt håndterer digitale trusler i næringen. De digitale trusler som virksomheten står ovenfor har mange fellesnevnere med det andre virksomheter erfarer. Læring og erfaringsutveksling i disse fora kan også være hensiktsmessig.

Petroleumstilsynet samarbeider med internasjonale organisasjoner som beskrevet i kapittel 4.7.

EU-kommisjonen la i oktober 2012 fram et forslag til en ny lov for helse, miljø og sikkerhet (HMS) for oljeinstallasjoner i Europa. Bakgrunnen var DwH-ulykken i Mexicogolfen i 2010. Den europeiske industrien skal, gjennom de nasjonale myndighetene, regelmessig vurdere og forbedre sikkerhetsstandarder for offshore-operasjoner. Regelverket innebærer blant annet omfattende økonomisk ansvar for alle operatører. Selskaper må også melde inn beredskapsplaner før de kan drive leteboring eller utvinning.

Den norske oljeindustrien mener spesielt at det norske trepartssamarbeidet med arbeidstakermedvirkning er en mangel i forslaget fra EU. Det nye regelverket skulle egentlig være en forordning. Dette er en slags EU-lov, som i motsetning til et direktiv betyr at de gjelder i medlemslandene på lik linje med landets egne lover. EU tonet etter protester ned regelverket, og det er nå foreslått som et direktiv. Olje- og gassvirksomheten mener at det regelverket Norge har utarbeidet over 40 år vil svekkes dersom de nye EU-reglene blir innført.

I sin redegjørelse til Stortinget 8. mai 2012 sa daværende utenriksminister Jonas Gahr Støre at forordningen ikke anses som EØS-relevant. I 2012 behandlet Stortinget arbeidslivsmeldingen. I sin innstilling skrev komiteen at de mener forslaget ikke vil bidra til å styrke sikkerhetsnivået på norsk sokkel, og ønsker derfor at forordningen ikke skal innlemmes i norsk rett.

21. mai 2013 stemte Europaparlamentet for innføringen av direktivet.

Faktaboks 11: Norsk oljevirksomhet ønsket ikke at EUs Offshoredirektiv skulle innføres i Norge /17//18/

4.5 Beredskap og operativ håndtering av relevante tilsiktede og utilsiktede hendelser

Selskapet FOX IT har gjort en undersøkelse blant amerikanske oljeselskaper som konkluderer med at 60 % av selskapene ikke har en beredskapsplan for digitale sårbarheter /31/. Arbeidsgruppen mener at dette er relevant også for selskapene på norsk sokkel. Mens selskapene har stor fokus på beredskap i forhold til brann og eksplosjoner mm, har mange av selskapene hverken planer eller rutiner for å håndtere en hendelse basert på digitale sårbarheter. Det er få av selskapene som har etablerte rutiner for å koble seg fra Internett, eller for å sperre forbindelse mellom selskapets IT nettverk og selskapets produksjonsnettverk. Det øves for lite på slike hendelser.

På samme måte er fokus hos tilsynsmyndigheter (PTIL og DSB) knyttet til beredskap og operativ håndtering knyttet til ulykker.

Kun noen få aktører er tilknyttet NSM's «Computer Emergency Response Team» (CERT). Det må avklares om sektoren skal etablere en egen slik tjeneste eller evt. benytte andre sektorielle tjenester som er under etablering.

4.6 Uklarheter i dagens lovverk og tilsynsregime

Det norske tilsynsregime i olje- og gassektoren er basert på prinsippet om egenregulering eller internkontroll. Dette er annerledes enn i for eksempel det amerikanske regimet hvor en praktiserer en detaljert, foreskrivende og etterlevelsesbasert modell. Den norske modellen er basert på målstyring og ansvarliggjøring av hver enkelt bedrift, kombinert med sanksjonsmidler fra myndighetenes side. Det norske regimet kan derfor virke overordnet og ikke detaljstyrende på forhold som bl.a. har med den

digitale sikkerheten å gjøre. Mer regelverk og mer myndighetstilsyn er ikke uten videre håndterbart for sikkerhetsmyndighetene. Det norske regelverket inneholder en rekke krav som regulerer myndighetenes kontroll av selskapene og som regulerer søknader, rapporter, varslinger m.m. fra selskapene til myndighetene. Selskapene har detaljkunnskap om virksomheten, noe sikkerhetsmyndighetene ikke har. Bedre digital sikkerhet kan ikke forenkles til et krav om mer myndighetskontroll. Myndighetene må påvirke næringen gjennom forskningsprosjekter, bevisthetskampanjer, informasjon om trusselsituasjonen og ved å etablere fora og møteplasser hvor en bygger kunnskap, utveksler erfaring og stimulerer til forebyggende tiltak. På denne måten vil også de små aktørene få mulighet til å dele erfaringer med de store aktørene.

De sentrale forskrifter for den digitale sårbarheten i sektoren finnes i HMS-forskriftene for petroleumsaktiviteten og Arbeidsmiljøforskriftene. Forskriftene er ikke konkrete i forhold til digitale trusler men innbefatter også digital sikkerhet.

I litteraturen om regulering beskrives også «hybride» tilnærminger hvor målstyringsprinsippet og det detaljerte, foreskrivende prinsipp kombineres. Ansvarliggjøring, myndiggjøring (påvirkning og innflytelse) og trepartssamarbeid er sentrale i en slik «hybrid» tilsynsmodell /7/. En slik modell vil ikke være i konflikt med den norske reguleringsmodellen og bør også vurderes i forhold til hvordan et fremtidig tilsynsregime for sektorens arbeid med den digitale sårbarheten skal være.

HMS-forskriftene for petroleumsaktiviteten

HMS-forskriftene /24/ er en integrert særregulering for HMS i petroleumsvirksomheten til havs og på enkelte landanlegg. Forskriftene er utarbeidet og håndhevet av HMS-myndighetene på sine respektive myndighetsområder i fellesskap.

Rammeforskriften: § 10 Forsvarlig virksomhet

Virksomheten skal være forsvarlig både ut fra en enkeltvis og samlet vurdering av alle faktorer som har betydning for planlegging og gjennomføring av virksomheten når det gjelder helse, miljø og sikkerhet. Det skal også tas hensyn til de enkelte virksomhetenes egenart, stedlige forhold og operasjonelle forutsetninger.
Et høyt nivå for helse, miljø og sikkerhet skal etableres, opprettholdes og videreutvikles

Styringsforskriften: § 4 Risikoreduksjon

Ved reduksjon av risiko som nevnt i rammeforskriften § 11, skal den ansvarlige velge tekniske, operasjonelle og organisatoriske løsninger som reduserer sannsynligheten for at det oppstår skade, feil og fare- og ulykkessituasjoner.
Det skal dessuten etableres barrierer som nevnt i § 5. De løsningene og barrierene som har størst risikoreduserende effekt, skal velges ut fra enkeltvis og samlet vurdering. Kollektive vernetiltak skal foretrekkes fremfor vernetiltak som er rettet mot enkeltpersoner.

Faktaboks 12: HMS-forskriftene er generelle og dekker også etablering og bruk av digitale systemer. /24/

Arbeidsmiljøforskriftene

Forskrifter til arbeidsmiljøloven er fastsatt av Arbeids- og sosialdepartementet og håndhevet av Arbeidstilsynet og Petroleumstilsynet på sine respektive myndighetsområder. I tillegg gjelder en rekke andre enkeltforskrifter enten i kraft av seg selv, eller indirekte gjennom innarbeidelse i HMS-forskriftene. De mest sentrale forskriftsbestemmelsene for helse, miljø og sikkerhet i olje- og gassvirksomheten

finnes i HMS-forskriftene og i arbeidsmiljøforskriftene. Hovedregelen er at en forskrift fastsatt i medhold av en lov, gjelder på lovens virkeområde, med mindre annet framgår av den enkelte forskrift.

Petroleumstilsynet har faglig myndighetsansvar for sikkerhet, beredskap og arbeidsmiljø i petroleumsvirksomheten på norsk kontinentalsokkel, samt på enkelte anlegg på land. Det er andre etater som har tilsynsansvar for øvrig nedstrømsaktivitet så som prosessindustri som benytter olje- eller gass-produkter eller distribusjon og salg av olje- og gass-produkter. Her har bl.a. Arbeidstilsynet (Arbeids- og sosialdepartementet), Miljødirektoratet (Klima- og miljødepartementet), DSB (Justis- og beredskapsdepartementet) en rolle. Petroleumstilsynet har ikke et operativt fokus på digitale sårbarheter som utnyttes til terrorisme, sabotasje og hackervirksomhet. Dette ligger hos NSM, PST og Forsvaret.

Objektsikkerhetsforskriften forvaltes av NSM og regulerer «eiendom som må beskyttes mot sikkerhetstruende virksomhet av hensyn til rikets eller alliertes sikkerhet eller andre vitale nasjonale sikkerhetsinteresser». Ingen olje- og gass installasjoner er per i dag definert som skjermingsverdig objekt. Dette bør vurderes sett i lys av virksomhetens betydning for statens inntekter.

I 2013 fikk Petroleumstilsynet også ansvar for sikring slik det framgår av Petroleumsloven §9-3. Denne lovparagrafen har ingen forskrifter eller juridiske forarbeider tilknyttet seg. Ei heller er det etablert noen kobling opp mot norske standarder innen sikring (NS 5832/NS 5831 + terminologi).

De elektriske anleggene som forsyner oljeinstallasjonene er ikke omfattet av Forskrift om forbyggende sikkerhet og beredskap som NVE forvalter, fordi anleggene kun er til for petroleumsvirksomhetenes eget forbruk.

4.7 Beskrivelse av internasjonale problemstillinger

Petroleumstilsynets DwH rapport med vurderinger og anbefalinger for norsk olje- og gassektor, inneholder en beskrivelse av internasjonale problemstillinger og pågående samarbeid på generelt nivå /7/. Teksten under er i det vesentligste hentet fra dette dokumentet:

I dag reises det blant annet krav om en internasjonal sikkerhetsregulering og -koordinering, og etablering av tverrnasjonale regelverkskrav. Fra flere hold er det tatt til orde for mer ensartede internasjonale sikkerhetsregimer i olje- og gassvirksomheten.

Norsk olje og gass har utarbeidet en egen rapport Deepwater-Horizon – lessons learned and follow-up (2012). Arbeidet i Norsk olje og gass blir koordinert med andre internasjonale initiativer, herunder arbeidet som pågår i International Association of Oil & Gas Producers (OGP) og Oil and Gas UK. Dette arbeidet følges opp jevnlig. I etterkant av DwH-ulykken etablerte OGP-gruppen Global Industry Response Group (GIRG) som har hatt som mandat å sikre at lærepunkter etter storulykken i Mexicogulfen blir identifisert og implementert i industrien. OGP anbefalinger inkluderer opprettelse av tre nye industrigrupper som skal fremme kontinuerlig forbedring og investering i utstyr, prosedyrer og adferd som vil redusere sannsynligheten og omfanget av brønnhendelser.

Petroleumstilsynets oppfølging av DwH-ulykken har inkludert samhandling med fagmiljøer og myndigheter nasjonalt og internasjonalt, for eksempel gjennom samarbeidsorganer som North Sea Offshore Authorities Forum (NSOAF) og International Regulators' Forum (IRF). Petroleumstilsynet tok initiativ til å arrangere et ekstraordinært møte i IRF i Washington DC i september 2010 med utgangspunkt i DwH-ulykken og Montara-utblåsingen utenfor Australia. Hensikten var å styrke samarbeidet mellom de nasjonale myndighetene og dele erfaringer med deres oppfølging av petroleumsvirksomheten, samt å få en oppdatert oversikt over hvilke tiltak og prosjekter som nå er på gang i medlemslandene og da spesielt i USA.

Det ekstraordinære medlemsmøtet drøftet også nødvendige endringer i programmet for den planlagte IRF Offshore Safety Conference, som senere ble avholdt i oktober 2010 i Vancouver BC, Canada. I samsvar med konklusjonene og anbefalingene fra denne konferansen besluttet IRF-landene å arbeide videre med fem prioriterte områder for offshore sikkerhet:

- Sikkerhetskultur og ledelse.
- BOP-integritet og brønnkontroll.
- Bruk av standarder og beste praksis i industrien.
- Utvikling av ytelsesindikatorer for måling av medlemslandenes helse-, miljø- og sikkerhetsnivå.
- Etablering av kriterier som medlemmene kan bruke

EUs energikommisær har innledet en tett dialog med både næring og myndigheter i Europa, inkludert Norge, for å vurdere ulike tiltak. Energikommisæren har blant annet utpekt NSOAF som et forum som kommisjonen ønsker å søke råd hos. Det er tatt tilsvarende initiativ i OSPAR-regi og Russlands initiativ gjennom G8/G20 kalt GMEP (Global Marine Environment Protection Initiative) kan også nevnes som et aktuelt internasjonalt initiativ./7/

4.8 Fremtidige problemstillinger og trender

Investeringsviljen til tiltak for å forebygge mot digitale trusler i olje- og gassvirksomheten på norsk sokkel vil bli utfordret i nedgangstider på lik linje med sikkerhetskulturen generelt sett. Viljen til å investere i sikringstiltak i et område hvor man så langt ikke har hatt alvorlig konsekvenser av hendelser, vil bli satt på prøve.

Datavolumene øker med eksponentiell hastighet i olje- og gassvirksomheten som i all annen virksomhet. Volumet av industridata i verden fordobles hvert 1,2 år. Datalagring er billig og datainnsamlings-teknologi utvikles stadig. Stadig smartere og flere sensorer overvåker og kontrollerer de fysiske prosessene. «Internet of Things» er blitt et begrep som indikerer at fysiske enheter kan kommunisere via internett. Moores lov, som sier at prosessor og prosesseringskapasitet fordobles hver 18 måned, har bevist sin gyldighet gjennom 50 år. Data samles inn fra stadig flere kilder, noe som medfører at variasjon og antall datatyper øker. Teknologi til å prosessere og benytte de store datamengdene er blitt en begrensning. Forskning og utvikling pågår for å frembringe løsninger som vil gjøre muligheten til å navigere, analysere og kombinere store datamengder. Dette skaper ikke bare muligheter for olje- og gassvirksomheten, men også nye trusler. Intelligente enheter som kan motta kontrollsignaler utenfra, kan manipuleres hvis ikke tilgangen beskyttes godt nok. Ved å analysere store datamengder kan mønstre avdekkes som avslører rutiner i anvendelse, bruksmønster, svakheter og mangler i teknologi, tilstand på utstyr, osv. Slik kunnskap kan brukes illegalt.

Nye forretningsmodeller hvor leverandører selv får ansvar for å samle inn, overvåke og forbedre eget utstyr diskuteres i sektoren. Dette vil nødvendigjøre at leverandørene får direkte tilgang til sensordata og innsamlet historikk samt mulighet til å oppdatere sin programvare. Flere aktører med tilgang til kritiske produksjonssystemer vil øke eksponeringen for inntrengning av skadelig programvare.

Også i olje- og gassvirksomheten forventer vi at den informasjon vi trenger skal være enkelt tilgjengelig når vi trenger den og uansett hvor vi befinner oss. Vi stoler på at de beskyttelsesmekanismer som er etablert er tilstrekkelige, uten at vi selv forstår hvordan de virker og om de virker. Ledere er selv blitt databrukere og etterspør informasjon digitalt som vedlegg til en mail eller i et rapporteringsverktøy som han selv kan operere. Slik informasjon kan enkelt distribueres ut av organisasjonen og bli tilgjengelig for

andre enn de tiltenkte. Holdningskampanjer og bevissthet på alle nivåer i en organisasjon om den digitale sårbarheten er like viktige som de fysiske barrierer som en bedrift etablerer.

5 RISIKOREDUSERENDE TILTAK

5.1 Generisk modell

Risiko kan aksepteres, reduseres, unngås eller overføres til andre parter. I denne rapporten fokuseres det på å redusere risiko. For å redusere sannsynligheten for hendelser basert på digitale sårbarheter, innføres mottiltak. Ved å innføre tilstrekkelig med mottiltak samt ved å verifisere at disse mottiltakene er riktig utført kan risiko bli akseptabel.

For å vurdere risiko gjennomføres regelmessig risikoanalyse. En risikoanalyse er en strukturert analyse som omfatter systematisk identifisering og kategorisering av risiko for mennesker, miljø og økonomisk verdi.

Mottiltak mot hendelser basert på digitale sårbarheter kan administreres og visualiseres som barrierer. Barrierer implementeres dels for å hindre at en uønsket hendelse skjer, dels for å redusere konsekvensen av at en uønsket hendelse har inntruffet. Petroleumstilsynet har utarbeidet «Prinsipper for barrierestyring i petroleumsvirksomheten" /8/.

I dette kapittelet gis en overordnet beskrivelse av mottiltak i forhold til de topp 10 digitale sårbarheter som er beskrevet i kapittel 3.6. Det vises deretter eksempler på tekniske barrierer som er relevante for sårbarhetene.

5.2 Manglende oppmerksomhet og opplæring

Mottiltak mot denne sårbarheten er først og fremst å innarbeide en sikkerhetskultur i hele virksomheten som er forankret i ledelsen. Det må gjennomføres oppmerksomhetstrening.

5.3 Fjernarbeid

Ved å åpne for fjernarbeid via åpne nett, innfører man en alvorlig sårbarhet som krever omfattende mottiltak. Det er vanlig i olje og gassektoren å anskaffe egne systemer for å kontrollere slik tilgang. Sterk autentisering av bruker, sikre tuneller (VPN) og tilgangsstyring basert på kortvarige arbeidsordre er viktige mottiltak.

5.4 Bruk av standardprodukter med kjente sårbarheter i produksjonsmiljø

Det viktigste mottiltaket er å oppdatere produktene umiddelbart etter at produsentene har produsert rettelser, men slik oppdatering er meget utfordrende i et produksjonsmiljø. Rettelser kan påvirke tilgjengelighet og integritet, og det kreves rutiner å teste rettelsene før de settes i produksjon.

5.5 Sikkerhetskultur hos underleverandører

Ansvar for sikkerhet må innarbeides og tydeliggjøres i kontrakter med underleverandører, konsulenter, m.m. Slikt personell må gjennomføre den samme oppmerksomhetstrening og opplæring som egne ansatte.

5.6 Separasjon av datanett

Produksjonsnett, interne datanett og internett er i stor grad adskilt med brannmur, men det kreves flere barrierer. NSM har laget en relevant veiledning «Hvordan forebygge, oppdage og håndtere dataangrep» /11/.

5.7 Mobile lagringsenheter (inklusive smarttelefoner)

Oppmerksomhetstrening og opplæring er viktig for at brukere skal forstå risiko ved bruk av mobile lagringsenheter. Likeledes må det være etablert rutiner og veiledninger. Fysisk blokkering eller deaktivering av USB porter, blåtann og trådløse nett kan være nødvendig (herding).

5.8 Datanett mellom landinstallasjoner og oljefelt

På land reduseres risiko ved å benytte datanett fra forskjellige nettleverandører med adskilte føringer, forskjellige og uavhengige nettverkskomponenter samt forskjellige drifts og overvåkningssentere. På kontinentalsokkelen er det primært en leverandør, og slik redundans er ikke tilgjengelig. For å sikre at redundante løsninger fungerer, må det etableres rutiner for redundanstester. På lenger sikt vil nye satellittbaserte «høyhastighetsløsninger» gi et reelt redundant alternativ.

5.9 Fysisk sikring av datarom, koplingsskap, m.m.

På olje- og gassinstallasjoner er det utstakt bruk av merking inklusive fargemerking av soner. Fysisk avlåsing og adgangssystem er i liten grad etablert og kan være i konflikt med rømningsveier. Ved å flytte kontrollrom til land, må det settes strengere krav til avlåsing av datarom, kommunikasjonsrom og kabling.

5.10 Sårbar programvare

Tiltak for å redusere risiko for digitale sårbarheter i programvare er å innarbeide krav, verifisere at sikkerhet er innarbeidet i hele utviklingsprosessen («Secure Software Development Lifecycle»), samt testing og verifikasjon. Systemer må penetrasjonstestes før de settes i produksjon, inklusive testing av kjente applikasjonsrelaterte sårbarheter. Testing med maskin-simulatorer («Hardware in the Loop») kan sikre at programvaren håndterer uforutsette signaler.

5.11 Utdaterte installasjoner

Det er meget vanskelig å få gjennomslag for kostbare produksjonsstopp for å oppdatere mottiltak på en installasjon som er i senfase. Strengere krav eller oppfølging av krav fra tilsynsmyndigheter kan være nødvendig, men også disse må også være basert på en kost/nytte-betraktning.

5.12 Barrierer

De påfølgende faktabokser viser eksempler på barrierer som er relevante i forhold til topp 10 digitale sårbarheter som beskrevet i kapittel 3.6.

Barriere for å hindre en hendelse	Oppmerksomhet	Fjernarbeid	Standardprodukter	Kultur underlev.	Separasjon av nett	Mobil lagring	Datanett	Fysisk sikring	Programvare	Utdaterte inst.
Anti-spionprogramvare	X	X	X	X	X	X			X	
Antivirus programvare	X	X	X	X	X	X			X	
Blokkere kjøring av ikke autoriserte programmer	X	X	X	X	X	X			X	
Blokkere/deaktivere USB porter	X	X		X	X	X				
Brannvegg	X	X	X	X	X	X			X	
Gjestenett	X			X	X	X				
Herding av programvare	X	X	**X**	X	X	X	X		X	X
Klassifisering av utstyr, dokumenter mm.	X		X	X	X	X				
Kontroll av enheter som kobles til nett (NAC/NAP)	X	X	X	X	X	X	X			
Krypterte disker på mobilt utstyr	X	X	X	X	X	X				
Krypterte minnepinner	X	X	X	X	X	X				
Ledelsesforankring / Etablering av sikkerhetskultur.	**X**	X	X	X	X	X	X	X	X	X
Merke kritikalitet på rom, utstyr, kabler mm	X			X	X		X			
Minste privilegiers prinsipp / Oppdeling av oppgaver	X	X	X	X	X				X	
Oppdatering av programvare	X	**X**	**X**	X	X		X		X	**X**
Oppdeling av datanett	X	**X**			**X**		X			
Oppmerksomhetstrening	**X**	**X**		X	X	X				
Penetrasjonstest		X	X	X	**X**		X		**X**	
Revisjon fysisk sikring	X							X		
Rutiner for behandling av klassifisert utstyr, dokumenter mm.	X	X		X		X				
Rutiner for å håndtere minnepinner	X	X		X		**X**				
Sikkerhet i utviklingsmiljø									**X**	
Sikre tuneller (VPN) for fjernarbeid	X	**X**		X						
Sikring av operatørgrensesnitt							X			
Tilgangsstyring basert på tidsbegrensede arbeidsordre		**X**		X						
To-faktor autentisering	X	**X**		X						
Tydeliggjøre ansvar i ansettelseskontrakt / kontrakt med underleverandører, konsulenter mm.	X	X	X	**X**	X	X	X	X	X	
Vaske e-post	X			X						
Vaske webtrafikk	X			X						

Faktaboks 13: Barrierer for å hindre at en uønsket hendelse skjer

Barriere for å hindre en hendelse	Oppmerksomhet	Fjernarbeid	Standardprodukter	Kultur underlev.	Separasjon av nett	Mobil lagring	Datanett	Fysisk sikring	Programvare	Utdaterte inst.
Anti-spionprogramvare (Legger ondsinnet programvare i karantene og sender alarm)	X	X		X		X				
Antivirus programvare (Legger ondsinnet programvare i karantene og sender alarm)	X	X		X		X				
Beredskapsplan	X	X	X	X	X	X	X	X	X	X
Digital etterforskning (Samle spor)	X	X		X		X				
Loggovervåkning	X	X	X	X	X	X	X		X	
Nettverksovervåking	X	X	X	X	X	X	X		X	
Rutiner for å koble fra enheter og nett	X	X		X	X	X	X			
System for å oppdage inntrenging (Intrusion detection system)	X	X		X	X	X	X			
Tilbakelegging av sikkerhetskopi (Rent system)	X	X	X	X	X	X	X		X	
Tilkobling til CERT	X	X		X	X	X	X		X	

Faktaboks 14: Barrierer for å redusere konsekvensen av en hendelse

6 REFERANSER

/1/ Risiko 2015, Nasjonal Sikkerhetsmyndighet:
http://nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2015-web.pdf

/2/ NOU 2000:24, Et sårbart samfunn — Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet:
https://www.regjeringen.no/contentassets/1c557161b3884335b4f9b89bbd32b27e/no/pdfa/nou200020000024000dddpdfa.pdf

/3/ Fokus 2015 er Etterretningstjenesten ugraderte vurdering av områder som anses som særlig relevante for norsk sikkerhet og nasjonale interesser:

http://forsvaret.no/fakta/undersokelser-og-rapporter/fokus

/4/ The Repository of Industrial Security Incidents:

http://www.risidata.com/

/5/ Cisco 2014 Annual Security Report:

http://www.cisco.com/web/offers/lp/2014-annual-security-report/index.html

/6/ The partnership between the Norwegian Oil & Gas Industry and the EU countries:
https://www.norskoljeoggass.no/no/Publikasjoner/Konjunkturrapport/Partnership--industry-and-EU/

/7/ PTIL 2011: Deepwater Horizon-ulykken – Vurderinger og anbefalinger for norsk petroleumsvirksomhet:

http://www.ptil.no/getfile.php/PDF/Hovedrapport%2013.6.2011.pdf

/8/ Prinsipper for barrierestyring i petroleumsvirksomheten, Petroleumstilsynet:
http://www.ptil.no/getfile.php/PDF/Prinsipper%20for%20barrierestyring%20i%20petroleumsvirksomheten.pdf

/9/ Regjeringen: St.prp. nr 65 (1996-97):

https://www.regjeringen.no/nb/dokumenter/stprp-nr-65-1996-97-/id201412/?docId=STP199619970065000DDDEPIS&q=&navchap=1&ch=3

/10/ Forskningsrådet: Store forskjeller mellom USA og Norge:
http://www.forskningsradet.no/prognett-petromaks/Nyheter/Store_forskjeller_mellom_USA_og_Norge/1253959752411?lang=no

/11/ NSM: Hvordan forebygge, oppdage og håndtere dataangrep:
http://nsm.stat.no/globalassets/dokumenter/temahefter/apt_2014_web.pdf

/12/ NSM 2014:, Sikkerhetstilstanden 2014:

https://nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/rst_2014.pdf

/13/ Vinnem, J.E., Utne, I.B., Skogdalen, J.E. (2011):Looking Back and Forward: Could Safety Indicators Have Given Early Warnings about the Deepwater Horizon Accident? Deepwater Horizon Sudy Group. Working Paper – Jan-2011: http://ccrm.berkeley.edu/pdfs_papers/DHSGWorkingPapersFeb16-2011/CouldSafetyIndicatorsHaveGivenEarlyWarningsAboutDeepwaterHorizonAccident-JES_IBU_JEV_DHSG-Jan2011.pdf

/14/ From McAfee White Paper: Global Energy Cyberattacks:"Night Dragon": http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf

/15/ Fra NVE sin hjemmeside: http://www.nve.no/no/Nyhetsarkiv-/Nyheter/NVE-ber-om-okt-arvakenhet-mot-mulig-virusangrep/

/16/ Bloomberg Business: Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar: http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar

/17/ Stavanger Aftenblad: Norge avviser EU direktivet: http://www.aftenbladet.no/energi/Norge-avviser-offshore-direktiv_-EU-har-doren-pa-glott-3182211.html

/18/ EU-s Offshore direktiv: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:178:0066:0106:EN:PDF

/19/ US Congressional Research Service, Pipeline Cybersecurity: Federal Policy:2012 http://fas.org/sgp/crs/homesec/R42660.pdf

/20/ PTIL: Tilsyn med IKT-sikkerhet i bore- prosesskontroll, sikkerhets- og støttesystemer innen petroleumsnæringen:2012 http://www.ptil.no/getfile.php/PDF/Seminar%202013/IKS-sikkerhet/Presentasjon%20resultater%20fra%20tilsyn%20med%20IKT-sikkerhet.pdf

/21/ PTIL: Forskriften om helse, miljø og sikkerhet i petroleumsvirksomheten og på enkelte landanlegg: 2013 http://www.ptil.no/rammeforskriften/category381.html

/22/ Regjeringen: St.prp nr. 65 (1996-97) https://www.regjeringen.no/nb/dokumenter/stprp-nr-65-1996-97-/id201412/?docId=STP199619970065000DDDEPIS&q=&navchap=1&ch=3

/23/ NVE: Kraft fra land til Johan Sverdrup-feltet: http://webfileservice.nve.no/API/PublishedFiles/Download/201201635/1363807

/24/ HMS forskriften: http://www.ptil.no/om-regelverket/category699.html

/25/ Norsk Olje & Gass: Anbefalte retningslinjer krav til informasjonssikkerhetsnivå i IKT-baserte prosesskontroll-, sikkerhets- og støttesystemer:
https://www.norskoljeoggass.no/Global/Retningslinjer/Integrerte%20operasjoner/104%20-%20Recommended%20guidelines%20for%20information%20security%20baseline%20requirements%20for%20process%20control%20safety%20and%20support%20ICT%20systems.pdf

/26/ Stavanger Aftenblad: Oljebedriftene trues av dataangrep:2014
http://www.aftenbladet.no/energi/Oljebedrifter-trues-av-dataangrep-3493347.html

/27/ Bergens Tidende: Mangler kontroll med hemmelige oljedata: 2014
http://www.bt.no/nyheter/lokalt/Manglet-kontroll-med-hemmelige-oljedata-3258995.html

/28/ Macondo the gulf oil disaster. Chief Counsel's report: 2011
http://www.eoearth.org/files/164401_164500/164423/full.pdf

/29/ National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling. Deeo water – The Gulf Oil Disaster and the Future of Offshore Drilling. Recommendations: 2011
http://www.eoearth.org/files/164401_164500/164423/full.pdfhttp://www.eoearth.org/files/164401_164500/164420/osc_deep_water_summary_recommendations_final.pdf

/30/ Total E&P Norge: Plan for utbygging, anlegg og drift av Hild
http://www.total.no/Normal/Documents/Norsk/Plan%20for%20utbygging%20og%20drift%20av%20Hild%20Del%202%20Konsekvensutredning.pdf

/31/ FOX IT: Cyber security: 60 percent of oil and gas companies do not have an Incident Response Plan in place
https://www.fox-it.com/en/news/cyber-security-60-percent-oil-gas-companies-incident-response-plan-place/

/32/ Norsk olje og gass: Deepwater-Horizon – lessons learned and follow-up (2012)
http://www.norskoljeoggass.no/no/Publikasjoner/Handboker/Deepwater-Horizon---lessons-learned-and-follow-up/

/33/ Norsk Olje & Gass: Recommended guidelines for implementation of information security in Process Control, Safety and Support ICT systems during the engineering, procurement and commissioning phases:
https://www.norskoljeoggass.no/no/Publikasjoner/Retningslinjer/Integrerte-operasjoner/110-Recommended-guidelines-for-implementation-of-information-security-in-Process-Control-Safety-and-Support-ICT-systems-during-the-engineering-procurement-and-commissioning-phases/

/34/ Norsk Olje & Gass: Recommended guidelines for classification of process control, safety and support ICT systems based on criticality:
https://www.norskoljeoggass.no/no/Publikasjoner/Retningslinjer/Integrerte-operasjoner/123-Recommended-guidelines-for-classification-of-process-control-safety-and-support-ICT-systems-based-on-criticality/

About DNV GL

Driven by our purpose of safeguarding life, property and the environment, DNV GL enables organizations to advance the safety and sustainability of their business. We provide classification and technical assurance along with software and independent expert advisory services to the maritime, oil and gas, and energy industries. We also provide certification services to customers across a wide range of industries. Operating in more than 100 countries, our 16,000 professionals are dedicated to helping our customers make the world safer, smarter and greener.