SINTEF

2018:00572 - Åpen

Rapport

Kunnskapsprosjekt IKT-sikkerhet; Industrielle kontroll- og sikkerhets-systemer i petroleumsvirksomheten

Forfattere
Lars Bodsberg, Britta Hale, Øyvind Dahl, Tor Olav Grøtan, Martin Gilje Jaatun, Marie Moe, Tor Onshus


Harald Pettersen, Statoil

SINTEF

2018-05-29

SINTEF

SINTEF Teknologi og samfunn

Postadresse:
Postboks 4760 Sluppen
7465 Trondheim

Sentralbord: 73593000
Telefaks: 73592896

ts@sintef.no
www.sintef.no
Foretaksregister:
NO 948 007 029 MVA

Rapport

Kunnskapsprosjekt IKT-sikkerhet; Industrielle kontroll- og sikkerhets-systemer i petroleumsvirksomheten

EMNEORD:
IKT-sikkerhet
Petroleum
CERT
CSIRT

VERSJON

DATO
2018-05-29

FORFATTER(E)
Lars Bodsberg, Øyvind Dahl, Britta Hale, Tor Olav Grøtan, Martin Gilje Jaatun, Marie Moe, Tor Onshus

OPPDRAGSGIVER(E)
Petroleumstilsynet

OPPDRAGSGIVERS REF.
Espen Seljemo

PROSJEKTNR
102017188

ANTALL SIDER OG VEDLEGG:
51+ vedlegg

SAMMENDRAG
Rapporten tar utgangspunkt i de endringene/driverne som påvirker risikobilde innen industrialisert kontroll teknologi (IKT) på innretninger som har petroleumsvirksomhet på norsk sokkel. Formålet med rapporten er å gi økt forståelse for aktørenes egne og sektorvise oppfølginger av IKT-sikkerhet. I rapporten oppsummeres hovedinntrykk fra intervju med fageksperter i olje- og gasselskaper, hos boreriggoperatører og i Petroleumstilsynet. I tillegg har prosjektet intervjuet fageksperter i nasjonale og internasjonale responsmiljø for IKT-sikkerhet (CSIRT/CERT), nasjonale og internasjonale tilsynsmyndigheter, samt leverandører av IKT-sikkerhetstjenester. Rapporten gir også en oversikt over relevante standarder og tilstøtende regelverk, samt aktuelle tilsynsmetoder for Petroleumstilsynet og selskapene selv. Rapporten er spisset innen IKT, operasjonell teknologi (OT) som er tilsynsområdet til Petroleumstilsynet.

Et viktig formål med rapporten er å motivere og bidra til økt kunnskap og innsats rundt IKT-sikkerhet blant personell i petroleumsnæringen som arbeider med prosesstyring, sikkerhet og kontrollsystemer.

UTARBEIDET AV
Lars Bodsberg

SIGNATUR

KONTROLLERT AV
Maria Bartnes

SIGNATUR

GODKJENT AV
Anita Øren

SIGNATUR

RAPPORTNR
2018:00572

ISBN
978-82-14-06882-5

GRADERING
Åpen

GRADERING DENNE SIDE
Åpen

SINTEF

Innholdsfortegnelse

Sammendrag **4**

Executive Summary **6**

1 Innledning **8**

1.1 Bakgrunn 8

1.2 Målsetting 8

1.3 Arbeidsmetode og analytisk rammeverk 9

1.4 Begrensninger og forutsetninger 9

1.5 Viktige begreper 10

1.6 Forkortelser 12

2 Nasjonale rammeverk for IKT-sikkerhet **13**

2.1 Rammeverk for håndtering av IKT-sikkerhetshendelser 13

2.2 Sektorvise responsmiljø (SRM) 13

2.3 NSM - grunnprinsipper for IKT-sikkerhet 14

2.4 Sikkerhetsloven 14

2.5 EUs NIS Direktiv 15

2.6 Enhet for IKT-sikkerhet (CERT) 15

2.6.1 NSM NorCERT 16

2.6.2 SRM - KraftCERT 16

2.6.3 IKT-sikkerhetstjenesteleverandør 16

2.7 Samarbeidsforum IKT-sikkerhetshendelser 17

3 CERT-kapasitet i næringen **18**

3.1 Hovedinntrykk fra intervju med selskaper i petroleumsnæringen 18

4 Operasjonalisering av CERT-varslinger **20**

4.1 Trafikklysprotokoll 20

4.2 Hovedinntrykk fra intervju med selskaper i petroleumsnæringen 21

5 Selskapenes internrevisjonsmetoder **23**

6 CERT løsninger i andre segmenter nasjonalt og internasjonalt **24**

6.1 Informasjonsdeling 24

6.1.1 Tillit 24

6.1.2 Forpliktelse til å dele 24

6.1.3 Samarbeid på tvers av landegrenser 25

6.2 Overvåking og rapportering av IKT hendelser 25
6.2.1 Sensorer for inntrengningsdeteksjonssystem (IDS) 25
6.2.2 Rapportering av IKT-sikkerhetshendelser 25
6.2.3 Kommunikasjon mellom IT- og OT-miljø 26
6.2.4 Definisjon av IKT-sikkerhetshendelse 26
6.3 Sikkerhetsøvelser 26
6.4 Deteksjon og håndtering av sikkerhetsbrudd 27
6.5 Spesielle utfordringer 28

7 Ptils tilsynsmetodikk innenfor IKT-området 29
7.1 Omfang og utbredelse 29
7.2 Hjemmelsgrunnlag 29
7.3 Tilsynsmetode 30
7.4 Resultater av tilsynsaktiviteten 31

8 Øvrige tilsynsetaters tilsynsmetodikk innenfor IKT-området 32
8.1 Hjemmelsgrunnlag 32
8.2 Fokusområde i tilsyn 33
8.3 Risikobasering 33
8.4 Differensiering 34

9 Standarder og regelverk 35
9.1 Standarder og veiledninger for IKT-sikkerhet (OT) i industrielle kontrollsystemer 35
9.2 Standarder for IKT hendelseshåndtering 38

10 Oppsummering og konklusjoner 39
10.1 CERT-kapasitet i næringen 39
10.2 Operasjonalisering av CERT varslinger 40
10.3 CERT løsninger i andre segmenter nasjonalt og internasjonalt 41
10.4 Relevante standarder innen IKT-sikkerhet (OT) og tilstøtende regelverk 42
10.5 Aktuelle internrevisjonsmetoder for selskapene selv 42
10.6 Aktuelle tilsynsmetoder for Ptil 42
10.7 SINTEFs vurdering 43

11 Videre arbeid 44

Referanser 45

BILAG/VEDLEGG

A Standarder, retningslinjer og veiledninger for IKT-sikkerhet i industrielle kontrollsystemer

Sammendrag

Regjeringen har som målsetting at det skal finnes responsmiljøer for IKT-sikkerhet i alle samfunnssektorer. En viktig oppgave for sektorvise responsmiljø er å sikre at alle relevante aktører mottar korrekt varslingsinformasjon hurtigst mulig for å være i stand til å gjøre nødvendige tiltak. De sektorvise responsmiljøene skal være NSM NorCERTs kontaktpunkt ved IKT-sikkerhetshendelser. I dag er det ikke et formelt sektorresponsmiljø innenfor petroleumssektoren. Innenfor denne sektoren pågår det nå et arbeid som ivaretas i en egen prosess, for å avklare og tydeliggjøre innsatsen mellom relevante aktører for å håndtere alvorlige IKT-sikkerhetshendelser.

Denne rapporten er ment å gi økt forståelse for aktørenes og næringens egen oppfølging av IKT-sikkerhet for industrielle kontroll- og sikkerhetssystemer på innretninger som har petroleumsvirksomhet på norsk sokkel.

Rapporten er basert på intervju og gjennomgang av relevant litteratur og dokumenter, samt SINTEFs generelle kompetanse og erfaring innenfor IKT-sikkerhet. Det er gjennomført 18 intervju med fageksperter i olje- og gasselskaper, boreriggselskaper, Petroleumstilsynet, nasjonale og internasjonale responsmiljø for IKT-sikkerhet, nasjonale og internasjonale tilsynsmyndigheter, samt leverandører av IKT-sikkerhetstjenester. Rapporten gir også en oversikt over relevante standarder og tilstøtende regelverk, samt aktuelle tilsynsmetoder for Petroleumstilsynet og selskapene selv.

IKT-sikkerhet omfatter både informasjonsteknologi (IT) og operasjonsteknologi (OT). IT-systemer er administrative systemer/kontorsystemer som bruker IT-teknologi til å behandle informasjon. OT-systemer er kontroll- og sikkerhetssystemer som bruker IT-teknologi til å kontrollere og overvåke industrielle prosesser. Trusler mot IT-systemer (f.eks. hacking av kontorsystemer) kan inngå som en del av et større cyberangrep som medfører driftsforstyrrelser i OT-systemer.

Temaet i denne rapporten er imidlertid primært avgrenset til IKT-sikkerhet for OT-systemer, det vil si beskyttelse av industrielle kontrollsystemer (OT-sikkerhet).

Det er en rekke responsmiljø for IKT-sikkerhet (CERT) i Norge. Noen er på nasjonalt nivå (NSM NorCERT), noen er på sektornivå (f.eks. KraftCERT og HelseCERT), noen er internt i et selskap (f.eks. Telenor CERT) og noen tilbyr IT-sikkerhetstjenester (f.eks. BDO CERT og mnemonic Incident Response Team). Både Equinor (tidligere Statoil) og Gassco har interne CERT.

CERT kapasitet i næringen

Informantene gir inntrykk av å være relativt tilfreds med egen CERT-kapasitet per i dag, men det erkjennes at man alltid kan bli bedre, f.eks innen sanntidsovervåking av sikkerheten i OT-systemer. Det nasjonale IKT-sikkerhetsmiljøet virker til å være et lite, men tett miljø der aktørene har god kjennskap til hverandre. Deling av informasjon og erfaring blant olje- og gasselskaper og boreriggselskaper skjer gjerne i ulike (virtuelle) møteplasser og fora organisert av eksterne aktører (ISAC). Det synes å være større interesse for medlemsskap i ulike ISAC enn i CERT. Det er lite fokus, spesielt blant de mindre aktørene, på systematisk deling av informasjon og erfaringer om IKT-sikkerhetshendelser med hverandre.

Ikke alle olje- og gasselskaper eller boreriggoperatører skiller mellom IKT-sikkerhetshendelser i IT-systemer og OT-systemer. Det er også stor variasjon i fordeling av ansvar for sikkerheten i og mellom IT- og OT-systemer. I den grad skillelinjer beskrives, handler dette om f.eks. sanntidskrav og anledningen til å slå av systemer for å gjøre oppdateringer, og om den krevende balansen mellom driftstilgjengelighet og IKT-sikkerhet.

For noen er det et prinsipielt spørsmål om Ptil bør fokusere kun på OT, eller på både IT og OT. Enkelte vil ikke ha for mange tilsynsmyndigheter innenfor IKT-området, og mener at Ptil ikke bør føre tilsyn med IKT-

sikkerhet i administrative systemer. For andre er det et spørsmål om Ptil's egen kapasitet og kompetanse til å dekke begge. Alle informantene har interne retningslinjer for arbeid med IKT-sikkerhet. Disse er i varierende grad basert på internasjonale standarder. Standarden IEC 62443 og DNV-GLs retningslinje 108 som er basert på denne, blir spesielt nevnt av informatene.

CERT løsninger i andre segmenter nasjonalt og internasjonalt.

Det nasjonale og internasjonale bildet av CERT-løsninger er variert og gir ikke noen klare føringer for organiseringen av sektorresponsmiljø i Norge. Internasjonalt observeres at beslektede sektor-CERT-er samles for bedre ressursutnyttelse. Det er en tendens til at ISAC framstår som like viktig som CERT for den enkelte sektor.

CERT-informantene viser til at antallet CERT-enheter må stå i forhold til den faktiske tilgangen på kompetanse og ressurser, og at en viss form for samordning alltid vil tvinge seg fram. Selv om CERT-funksjoner i stor grad er formaliserte, er personlige nettverk fortsatt veldig viktige for tillitsfull informasjonsdeling, spesielt når det gjelder utveksling av sensitiv informasjon.

Selv om CERT-er opprinnelig har hatt overveiende fokus på IT, er det en internasjonal trend at man i økende grad interessere seg også for OT. Nasjonalt er det spesielt KraftCERT som eksplisitt anerkjenner forskjellen mellom, og aktivt søker å forene håndteringen av IKT-sikkerhet i både IT- og OT-systemer. KraftCERT er et sektorresponsmiljø for energisektoren med ambisjoner om å være en støtte for hele kraftbransjen både i forebyggende arbeid og i håndtering av hendelser.

Aktuelle tilsynsmetoder for Ptil

Gjennomgangen av Ptils tilsynsmetoder innenfor IKT-området viser at metodikken her ikke avviker nevneverdig fra øvrige områder etaten fører tilsyn med. Hjemmelsgrunnlaget som tilsynene bygger på er i mindre grad preskriptivt og detaljorientert enn hva vi finner hos for eksempel NVE. Med få varslede IKT-hendelser og på bakgrunn av at IKT-sikkerhet ikke er en del av RNNP, kan det antas at kunnskapsgrunnlaget for en risikobasert tilsynsmetodikk er noe svakere her enn ved øvrige typer av risikoforhold som Ptil fører tilsyn med.

SINTEFs vurdering

SINTEF anbefaler opprettelse av "Olje-ISAC", samt styrking av KraftCERT som en del av et nasjonalt cybersikkerhetssenter, for håndtering av IKT-sikkerhetshendelser i petroleumsnæringen. IKT-sikkerhetskompetansen i Norge er så begrenset at det ikke er rom for å lage en egen olje-CERT. Et styrket KraftCERT kan bli en viktig ressurs for petroleumsnæringen. Det vil også være lettere å styrke et eksisterende fagmiljø enn å starte et nytt sektorvist responsmiljø innenfor IKT-sikkerhet for petroleum. En Olje-ISAC vil redusere avhengigheten av personlige nettverk for informasjonsdeling, noe som vil være en fordel for de mindre aktørene, og for virksomheter som ikke har bygget opp interne fagmiljø på IKT-sikkerhet.

Vi ser et sterkt behov for at alle aktørene, både oljeselskaper og CERT-aktører, samordner tilnærmingen til IKT-sikkerhet i IT- og OT-systemer siden det i dag er betydelige forskjeller i begrepsbruk, modenhet i tekniske løsninger, og kultur.

Ptils dialog- og tillitsbaserte tilsynsmetodikk innen IKT-sikkerhet synes egnet til å skape oppmerksomhet og spre læring på tvers i næringen. Etaten bør vurdere å konkretisere ytterligere hvilke IKT-relaterte hendelser som omfattes av plikten til å varsle driftsforstyrrelser, samt etablere et mer formelt kunnskapsgrunnlag om IKT-sikkerhet i næringen som grunnlag for risikobasert tilsyn.

Executive Summary

The Norwegian government's goal is to build response readiness for ICT security in all sectors of society. In the petroleum sector there is no current formal sector response community (CERT), but work is currently underway in a separate process, to clarify the stake and contribution of relevant actors in handling critical ICT security incidents.

The purpose of this report is to improve understanding of individual and sector monitoring of ICT security in industrial control and safety systems for facilities with petroleum activity on the Norwegian continental shelf. The report is primarily limited to ICT security for operational technnology, ie the protection of industrial control systems (OT security).

The report is based on interviews, a review of relevant literature and documents, and SINTEF's overall competence and experience in ICT security. Interviews have been conducted with subject area experts from oil and gas companies, drilling rig operators, the Norwegian Petroleum Safety Authority (PSA), national and international incident response teams for ICT security, national and international supervisory authorities, and providers of ICT security services – in total amounting to 18 in-depth interviews Additionally, this report provides an overview of relevant standards and regulations, as well as relevant supervisory practices in the Norwegian PSA and companies themselves.

CERT capacity in the industry
The informants are relatively satisfied with their own CERT capacity today, but it is acknowledged that one can always improve, for example, in real-time monitoring of ICT security of OT systems. The national ICT security environment seems to be a small but tight environment where the actors have a good knowledge of each other. Oil and gas companies and drilling companies share information and experience in various (virtual) meeting places and forums organized by external actors (ISACs). There seems to be greater interest in membership of ISAC than CERT. There is little focus, especially among the smaller companies, on systematic sharing of information and experiences about ICT security events with each other.

Not all oil and gas companies or drilling rig operators distinguish between ICT security incidents in IT and OT systems, and views vary widely concerning who is responsible for security in and between IT and OT. To the extent that a distinction is made, it is often about e.g. reasons for turning off systems to make updates and the demanding balance between operational availability and ICT security in industrial control systems.

There is considerable disagreement amon informants about whether the PSA should focus only on OT, or on both IT and OT. For some, this is a fundamental question, while for others it is only a matter of the PSA's own capacity and competence. All of the interviewees have internal guidelines for working with ICT security which are, to varying degrees, based on the international standard IEC 62443-series and the corresponding DVN-GL Guideline 108.

CERT solutions in other segments nationally and internationally
The national and international image is varied and does not provide clear recommendations for the organization of sector CERTs in Norway. However, comparable international sector CERTs are often grouped for better resource utilization

CERT actors pointed out that the number of CERTs must be in proportion to actual access to expertise and resources. ISACs are often considered to be equally important as CERTs for the individual sector. A need for better communication, however, is a common denominator, and not least of all real contact between CERTs

and key persons within the companies. Even though CERT functions are largely formalized, personal networks are still very important for information sharing, especially when it comes to exchanging sensitive information.

There is a tendency for international CERTs to recognize the difference between ICT security of IT and OT, to address the gap, as well as reconcile the approaches. In Norway, KraftCERT is the most prominent exponent for this way of thinking.

Current supervisory methods from the Norwegian PSA

The review of Norwegian PSA's supervisory practices indicates that methodology in the ICT area does not deviate significantly from other supervisory areas of the agency. However, the regulatory framework within the ICT area is less concrete and prescriptively formulated compared to that of e.g. the Norwegian Water Resources and Energy Directorate. With few notified ICT events and given that ICT security is not a part of the PSA project: "Trends in risk level in the petroleum activity (RNNP)", it can be assumed that the knowledge base for a risk-based supervisory approach is somewhat weaker within the ICT area than with other types of risk areas that the PSA supervises.

SINTEF's assessment

SINTEF recommends the creation of an "Oil ISAC" as well as strengthening of KraftCERT as part of a national cyber security centre for incident handling in ICT security within the petroleum industry. ICT security competence in Norway is so limited that it is not appropriate to create a separate "Oil CERT". Furthermore, it is easier to strengthen an existing incident response community than to start a new CERT within ICT security for the petroleum sector. An Oil ISAC will reduce the overall dependence on personal networks for information sharing, especially for smaller companies, and companies without an established incident response team.

We see a strong need for coordinating and harmonizing ICT security in IT and OT systems, as there are significant differences in terminology, maturity of technical solutions and culture today.

The Norwegian PSA's dialogue and trust-based supervisory methodology in ICT security appears suitable for spreading knowledge and signalling to the industry that the topic is taken seriously by the PSA. PSA should consider detailing further which ICT-related events are covered by the notification obligation, as well as establishing a more formal knowledge base on ICT security in the industry as a basis for the risk-based approach.

1 Innledning

1.1 Bakgrunn

Petroleumsindustrien blir stadig mer avhengig av digitale systemer, og selskapene har ambisiøse planer om økt bruk av digital teknologi.

Digitalisering innebærer innføring av digital teknologi for å erstatte, effektivisere eller automatisere manuelle og fysiske oppgaver. Dette vil kunne ha klare positive effekter for HMS og bidra til større konkurransedyktighet.

Samtidig kan utviklingen medføre utfordringer, blant annet knyttet til situasjonsforståelse, informasjonssikring, feilhandlinger og risiko for sabotasje. Næringen må derfor aktivt følge opp endringer i risikobildet som følge av digitalisering.

I desember 2017 ble for eksempel et nytt sofistikert og alvorlig kyberangrep rettet mot kritisk infrastruktur. Det ble oppdaget av leverandøren Schneider Electric og analysert av IKT-sikkerhetsfirmaene Fireeye [1] og Dragos [2]. Skadevaren døpt TRITON/TRISIS utløste nødstopp i Triconex som er et sikkerhetssystem for industriell prosesskontroll på et anlegg i Midt-Østen. Selv om systemet faktisk gjorde det som det skulle gjøre i dette tilfellet, nemlig å gå til en sikker tilstand når skadevaren førte til at en validerings-sjekk mellom redundante systemer feilet, så illustrerer hendelsen at også sikkerhetssystemene som skal beskytte industrielle kontroll- og prosessystemer er sårbare.

En nylig oversikt over trusselbildet mot norsk petroleumssektor i en geopolitisk sammenheng er gitt i NUPI rapporten: *Cyber-weapons in International Politics; Possible sabotage against the Norwegian Petroleum sector* [3].

Petroleumstilsynet (Ptil) har som tilsynsmyndighet behov for å ha god oversikt om IKT-sikkerhet og dette prosjektet og rapporten er en del av en større satsing innenfor området.

Ptil er underlagt Arbeids- og sosialdepartementet (ASD) og har myndighetsansvar for sikkerhet, beredskap og arbeidsmiljø på norsk sokkel.

Ptil skal legge premisser for, og følge opp at aktørene i petroleumsvirksomheten holder et høyt nivå for helse, miljø, sikkerhet og beredskap og gjennom dette også bidra til å skape størst mulig verdier for samfunnet. Ptil skal drive informasjons- og rådgivningsvirksomhet overfor aktørene i petroleumsvirksomheten, samarbeide med andre helse-, miljø-, sikkerhets (HMS)-myndigheter nasjonalt og internasjonalt og bidra til kunnskapsoverføring på HMS-området i samfunnet generelt. Ptil skal gjennom eget tilsyn, og samarbeid med andre myndigheter med selvstendig ansvar på HMS-området, sikre at tilsynet med petroleumsvirksomheten blir ført på en helhetlig måte. Ptils myndighetsområde omfatter også tilsyn med sikkerhet, beredskap og arbeidsmiljø på innretninger og rigger som driver petroleumsaktivitet på norsk sokkel.

1.2 Målsetting

Rapporten har som hovedmål å gi økt forståelse for aktørenes egne og sektorvise oppfølging av IKT-sikkerhet på innretninger som har petroleumsvirksomhet på norsk sokkel.

Et viktig mål for prosjektet har vært å belyse CERT-kapasitet i petroleumsnæringen, vurdere lignende CERT- løsninger i andre segmenter nasjonalt og internasjonalt, samt presentere relevante standarder innen

IKT-sikkerhet for operasjonell teknologi. Et annet viktig mål har vært å belyse aktuelle tilsynsmetoder for Petroleumstilsynet og selskapene selv.

Hovedfokus har vært på IKT-sikkerhet for industrielle kontrollsystemer knyttet til Petroleumtilsynets myndighetsområde. Det vil si at rapporten er spisset mot operasjonell teknologi (OT), ikke mot generell (administrativ) IT.

Et viktig formål med rapporten er å motivere og bidra til økt kunnskap og innsats om IKT-sikkerhet blant personell i petroleumsnæringen som arbeider med OT systemer.

1.3 Arbeidsmetode og analytisk rammeverk

Rapporten er basert på intervju og gjennomgang av relevant litteratur og dokumenter, samt SINTEFs generelle kompetanse og erfaring innenfor IKT-sikkerhet.

Det er gjennomført 18 intervju med fageksperter i olje- og gasselskaper, hos boreriggoperatører og i Petroleumstilsynet. I tillegg har prosjektet intervjuet fageksperter i nasjonale og internasjonale beredskapsenheter for IKT-sikkerhet (CERT), nasjonale og internasjonale tilsynsmyndigheter, samt leverandører av IKT-sikkerhetstjenester. De fleste fagpersonell hadde kompetanse innenfor prosesstyring, sikkerhet og kontrollsystemer.

Alle intervju er basert på en felles semistrukturert intervjuguide. Dette innebærer at intervjuguiden har vært retningsgivende for intervjuene, men at enkelte spørsmål har blitt tilføyd underveis i intervjuet avhengig av hvilke tema informantene har løftet fram.

Intervju med leverandører av industrielle kontrollsystemer har ikke vært en del av prosjektet.

All informasjon fra informanter er anonymisert i rapporten.

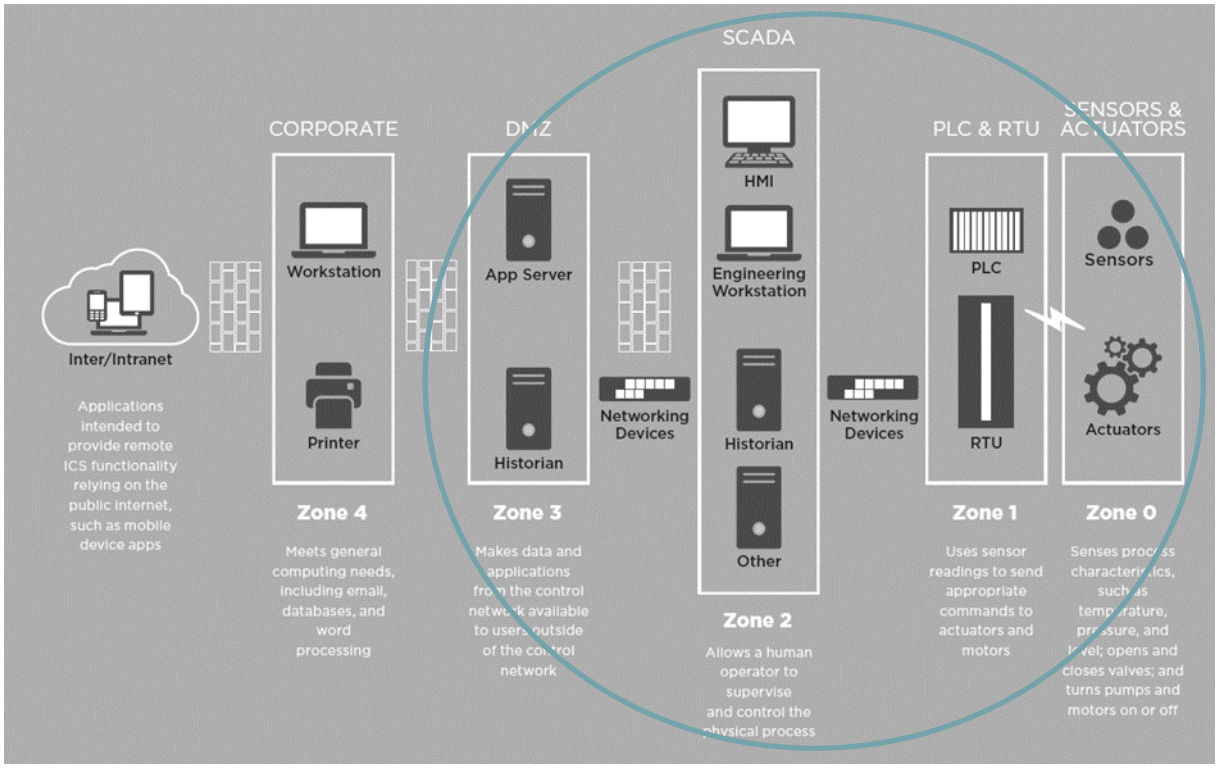
All informasjon som kan knyttes til selskapsnavn i rapporten, er hentet fra åpne kilder.

Prosjektet er meldt til og har fått godkjennelse fra Personvernombudet for forskning (NSD).

1.4 Begrensninger og forutsetninger

Hovedfokus er på IKT-sikkerhet for industrielle kontrollsystemer knyttet til Ptils myndighetsområde (sone 0-3 i Figur 1), og hvordan selskapene sikrer sine systemer mot trusler og begrenser risiko.

Sikring av personopplysninger har ikke vært tema for prosjektet.



Figur 1 Soneinndeling industriellle kontrollsystemer - IT-systemer (sone 4) og OT-systemer (sone 3-0) [4]

1.5 Viktige begreper

"Computer Security Incident Response Team"(CSIRT)/ "Computer Emergency Response Team"(CERT)
Både CSIRT og CERT er betegnelser på en koordinerende responsenhet for informasjonsikkerhetshendelser. CERT var opprinnelig et akronym. Nå er CERT et registrert varemerke eid av Carnegie Mellon University og alle selskap som bruker dette begrepet, må ha lisens. I rapporten brukes CERT som et samlebegrep for CSIRT og CERT.

Informasjonsteknologi vs operasjonell teknologi
Ved vurdering av IKT-sikkerhet i industrielle sikkerhets- og kontrollsystemer kan vi grovt skille mellom:

- Informasjonsteknologi (IT), dvs. teknologi som behandler informasjon, som dokumentbehandling, websider, epost osv. I rapporten brukes begrepet IT-systemer om administrative systemer/kontorsystemer.
- Operasjonell teknologi (OT), dvs. IT-teknologi som støtter, kontrollerer og overvåker industriell produksjon, kontroll- og sikkerhetsfunksjoner. I rapporten brukes begrepet OT-systemer om industrielle kontrollsystemer.

IKT-sikkerhet er beskyttelse av informasjons- og kommunikasjonsteknologi, noe som omfatter både IT- og OT-systemer. Sikring av administrative IT systemer har ikke vært et eget tema i denne rapporten. Det er likevel verdt å nevne at kontorsystemene ofte er et mål for cyberangrep. Når en angriper har fått tilgang til kontorsystemene kan denne tilgangen utnyttes til å samle informasjon som kan brukes i planlegging og forbere-

delser til et cyberangrep på de industrielle kontrollsystemene. En angriper vil for eksempel kunne utnytte tilgang til kontorsystemene til å opprette nye brukere, samle påloggingsinformasjon eller til skanning og kartlegging av infrastruktur.

I denne rapporten er det fokus på sikring av industrielle sikkerhets- og kontrollsystemene på innretninger og flyttbare innretninger, dvs. systemer som støtter, kontrollerer og overvåker produksjon. Det er viktig at disse systemene har høy pålitelighet for å forhindre eller begrense uønskede hendelser som kan føre til skade på mennesker, ytre miljø eller utstyr (sikkerhet). Samtidig må de ha høy pålitelighet for å unngå driftsforstyrrelser og tapt produksjon (driftssikkerhet).

En viktig forskjell mellom IT- og OT-systemer er at OT-systemer er sanntidssystemer som ved driftsavbrudd kan medføre skade på mennesker, miljø og materiell. OT-systemer må også ha høy pålitelighet for å unngå driftsforstyrrelser og tapt produksjon (driftssikkerhet). Ut fra krav til teknisk sikkerhet er OT-systemer utviklet for å være uavhengige av andre IT-systemer. IT-systemer derimot har i stor grad kommunikasjon med andre systemer. Dette betyr for eksempel at det historisk har vært forskjellig filosofi for håndtering av tilgangsrettigheter for IT- og OT-systemer.

"Safety" vs "security"
I internasjonale regelverk og standarder skilles det gjerne mellom "safety" og "security" og mellom beskyttelse av objekter/funksjon og informasjon. En viktig forskjell mellom "safety "og "security" er at "security" omhandler beskyttelse mot villede handlinger i motsetning til "safety", som gjerne er begrenset til ulykker forårsaket av teknisk svikt og/eller utilsiktede menneskelig handlinger.

Det mangler gode omforente begrep på norsk for å beskrive disse begrepene, men noen miljø bruker henholdsvis begrepene *sikkerhet* og *sikring* om begrepene "safety" og "security".

Definisjoner som brukes i rapporten
Tabell 1 viser betydningen av begrep som benyttes i denne rapporten

Tabell 1 Definisjoner

Begrep	Beskrivelse
Sikkerhet	Beskyttelse av verdier så som mennesker, ytre miljø, utstyr og informasjon.
Informasjonssikkerhet	Beskyttelse av informasjon uavhengig av om den er lagret digitalt eller ikke (tilgjengelighet, integritet og konfidensialitet).
IKT-sikkerhet	Beskyttelse av informasjons- og kommunikasjonsteknologi (maskinvare og programvare, samt kommunikasjonssystemer).
IT-sikkerhet	Beskyttelse av informasjonsteknologi (I praksis det samme som IKT-sikkerhet. IKT-sikkerhet brukes som et felles begrep for IKT- og IT-sikkerhet i denne rapporten).
Cybersikkerhet	Beskyttelse av utstyr (komponenter og enheter) og fysiske prosesser som er sårbare gjennom IT. I næringen brukes noen ganger OT-sikkerhet om beskyttelse av industrielle kontrollsystemer.
Driftssikkerhet	Beskyttelse mot tapt produksjon.

1.6 Forkortelser

ASD	Arbeids- og sosialdepartementet.
CERT	*«Computer Emergency Response Team»*. CERT er en koordinerende enhet for informasjonssikkerhet og et registrert varemerke eid av Carnegie Mellon University.
CSIRT	*«Computer Security Incident Response Team»*. Koordinerende enhet for informasjonssikkerhet; synonym for CERT, men dette begrepet er ikke lisensbelagt. I rapporten brukes CERTsom et samlebegrep for CSIRT og CERT.
CIA	*«Confidentiality, Integrity, Availability»* (Konfidensialitet, integritet, tilgjengelighet).
CISO	*«Chief Information Security Officer»* (Leder informasjonssikkerhet).
DSM	*«Distribution Management System».*
FIRST	*«Forum of Incident Response and Security Teams».*
HMI	*«Human Machine Interface»* (Menneske-maskin grensesnitt).
IDS	*«Intrusion Detection System»* (Inntrengingsdeteksjonssystem).
IOC	*«Indicators of Compromise»*.
IT	Informasjonsteknologi. Teknologi som behandler informasjon.
ISAC	*«Information Sharing and Analysis Center.»* ISAC er en (virtuell) møteplass for deling av informasjon og erfaring om trusler mot og bekjempelse av IKT-sikkerhetshendelser. ISAC kan være spesifikk for en sektor.
ICS	*«Industrial Control System»* (Industrielle kontrollsystemer). I petroleumsvirksomheten brukes typisk forkortelsen SAS (se nedenfor).
IRC	*«Internet Relay Chat».*
MSSP	*«Managed Security Service Provider».* Privat tjenesteleverandør/konsulentselskap som leverer nettverksovervåkning og andre sikkerhetskonsulenttjenester.
NCSC	*«National Cyber-Security Center».* Inkluderer oftest også en CERT-funksjon.
NIS	*«The Directive on security of network and information systems - NIS Directive, European Commission».*
NSM	Nasjonal sikkerhetsmyndighet.
OT	Operasjonell teknologi. Teknologi som støtter, kontrollerer og overvåker industriell produksjon, kontroll- og sikkerhetsfunksjoner.
PCS	*«Process Control System»* (Prosesskontrollsystem).
Ptil	Petroleumstilsynet.
TLP	*«Traffic Light Protocol»* (Trafikklysprotokoll).
RNNP	Prosjektet: "Risikonivå i norsk petroleumsvirksomhet".
SAS	*«Safety and Automation System»*. SAS-systemer er en forkortelse som typisk brukes om prosess sikkerhets- og kontrollsystem i petroleumsvirksomheten.
SCADA	*«Supervisory Control and Data Acquisition system».*
SRM	Sektorresponsmiljø.
VDI	Varslingssystem for digital infrastruktur. Driftes fra NorCERT, som ligger innunder NSM, og består av IDS sensorer utplassert hos virksomheter som ansees som en del av kritisk infrastruktur i Norge.

2 Nasjonale rammeverk for IKT-sikkerhet

I Stortingsmelding 38 (2016-2017) "IKT-sikkerhet - Et felles ansvar" [19], som ble behandlet i Stortinget i vårsesjonen 2018, er styrking av nasjonal evne til å avdekke og håndtere digitale angrep et av hovedområdene.

2.1 Rammeverk for håndtering av IKT-sikkerhetshendelser

Justis- og beredskapsdepartementet har utviklet et rammeverk for håndtering av IKT-sikkerhetshendelser som et sentralt tiltak for å bidra til styrking av nasjonal evne til å avdekke og håndtere digitale angrep [24]

Hensikten med rammeverket er å avklare og tydeliggjøre innsatsen mellom relevante aktører for å håndtere alvorlige IKT-sikkerhetshendelser som rammer på tvers av sektorer, samt bidra til å skape god situasjonsoversikt gjennom aggregering og koordinering av informasjon om alle relevante IKT-sikkerhetshendelser. Rammeverket stiller krav til hvilke oppgaver responsmiljøene må ivareta og hvilke egenskaper responsmiljøene må ha. Rammeverket beskriver også hvilke evner virksomhetene selv forutsettes å ha relatert til håndtering av IKT-sikkerhetshendelser.

Målgruppen for rammeverket er offentlige og private virksomheter som har betydning for kritisk infrastruktur og/eller kritiske samfunnsfunksjoner, sektorvise responsmiljøer (SRM), myndigheter som har en rolle knyttet til håndtering av IKT-sikkerhetshendelser og departementene.

Rammeverket er ikke bindende for private rettssubjekter, men alle departementer oppfordres til å innlemme sentrale private aktører gjennom avtaler som sikrer at virksomheter (statlige forvaltningsorganer og private rettssubjekter) rapporterer hendelser til NSM via SRM.

2.2 Sektorvise responsmiljø (SRM)

Nasjonal strategi for informasjonssikkerhet [25] som ble utgitt i 2012, legger til grunn at de sektorvise responsmiljøene (SRM) skal ha en sentral rolle i hendelseshåndtering.). I 2016 utga EU et eget direktiv vedrørende cyber-sikkerhet (se kap 2.5) hvor det står at medlemsstatene bør sørge for at de har velfungerende CSIRTs. Foreløpig er det skjedd lite på området, og det er etablert et begrenset antall norske SRM (se eksempler i kapittel 2.6.2).

Regjeringen har som målsetting at det skal finnes responsmiljøer i alle samfunnssektorer. En viktig oppgave for sektorvise responsmiljø er å sikre at alle relevante aktører mottar korrekt varslingsinformasjon for hurtigst mulig å kunne sette i stand nødvendige tiltak. De sektorvise responsmiljøene skal være NSM NorCERTs kontaktpunkt ved IKT-sikkerhetshendelser.

Sektorvise responsmiljø har myndighet innenfor sektoren og kan pålegge tiltak både ved forebygging og håndtering, mens NSM NorCERT vil ha et overordnet varslings- og koordineringsansvar. Kommunikasjon med individuelle virksomheter skal ivaretas eller foregå koordinert med sektormyndigheter. Virksomhetene selv har et ansvar for å kunne ivareta sikkerhet og håndtere hendelser.

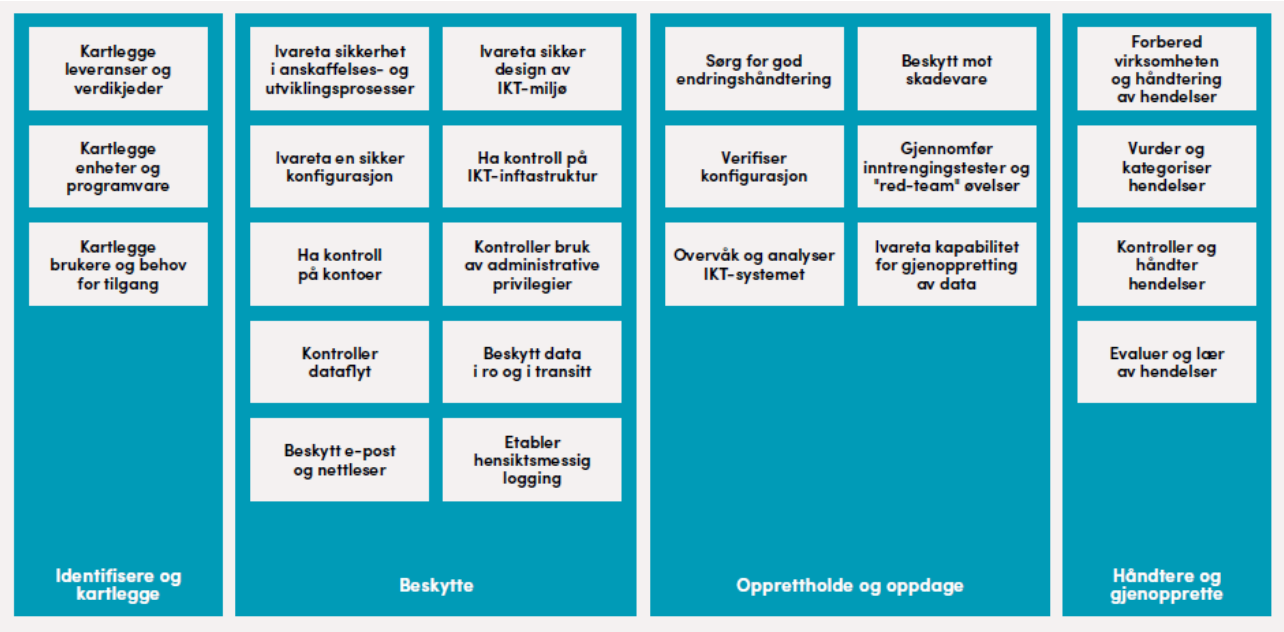
I dag er det ikke et formelt sektorresponsmiljø innenfor petroleumssektoren. Innenfor denne sektoren pågår det nå et arbeid som ivaretas i en egen prosess, for å avklare og tydeliggjøre innsatsen mellom relevante aktører for å håndtere alvorlige IKT-sikkerhetshendelser.

Et eksempel på sektorresponsmiljø er KraftCERT som er en responsfunksjon for energisektoren (se kapittel 2.6.2). Medlemskap i KraftCERT er frivillig, og virksomheten må betale en medlemsavgift.

2.3 NSM - grunnprinsipper for IKT-sikkerhet

Nasjonal sikkerhetsmyndighet (NSM) er Norges ekspertorgan for informasjons- og objektsikkerhet, og det nasjonale fagmiljøet for IKT-sikkerhet. Direktoratet er nasjonal varslings- og koordineringsinstans for alvorlige dataangrep og andre IKT-sikkerhetshendelser. Fagområdene kan grovt fordeles mellom kategoriene "IKT-sikkerhet", "personellsikkerhet" og "fysisk sikkerhet". NSM har fag- og kontrollansvaret for personellsikkerhetstjenesten innenfor sikkerhetslovens virkeområde [31].

Ut fra definisjonen kan det se ut som at håndtering av hendelser er hovedfokuset for en CERT. Imidlertid innbefatter ofte oppgavene til en CERT langt mer enn håndtering og gjenoppretting av IT-hendelser. Også forebygging av hendelser så som kartlegging, beskyttelse, deteksjon og varsling inngår ofte som oppgaver i en CERT. Dette er illustrert i Figur 2 som viser NSM grunnprinsipper for IKT-sikkerhet.



Figur 2 NSM grunnprinsipper for IKT-sikkerhet [31]

2.4 Sikkerhetsloven

Stortinget vedtok 27.02.2018 ny lov om nasjonal sikkerhet (sikkerhetsloven) som er rettet mot å beskytte informasjon som behandles elektronisk og sikre at uvedkommende ikke får tilgang til systemer som er avgjørende for våre grunnleggende nasjonale funksjoner. [20]

> *"Den nye loven tydeliggjør hvem som har ansvaret for forebyggende sikkerhetsarbeid. Det enkelte departement vil ha ansvaret for det forebyggende sikkerhetsarbeidet i sin sektor. Samtidig skal sikkerhetsmyndighetens helhetlige ansvar styrkes. Det blir økt samhandling mellom virksomheter og myndigheter på tvers av samfunnssektorene, og mer utveksling av informasjon, for eksempel trusselvurderinger, mellom sikkerhetsmyndighetene og de virksomhetene som underlegges loven."*

Anvendelse av sikkerhetsloven for petroleumssektoren er under utredning.

2.5 EUs NIS Direktiv

EU utga i 2016 "The Directive (EU) 2016/1148 on the security of network and information systems across the Union (NIS Directive)" [28]. Direktivet har tre hovedmål 1) Forbedre nasjonal cybersikkerhet; 2) Bygge samarbeid på EU-nivå; og 3) Fremme en kultur for risikostyring og hendelsesrapportering blant sentrale aktører. NIS-direktivet har fokus på kritisk infrastruktur, men det er opp til hvert enkelt land å definere hva som omfattes av begrepet kritisk infrastruktur. Betydningen av NIS-direktivet for norsk petroleumsvirksomhet er under utredning.

2.6 Enhet for IKT-sikkerhet (CERT)

Det er en rekke forskjellige responsmiljø for IKT-sikkerhet i Norge. Noen er på nasjonalt nivå, noen er på sektornivå, noen er internt i et selskap og noen leverandører tilbyr IKT-sikkerhetstjenester innenfor beredskap. Eksempel på norske CERT-funksjoner er gitt i Tabell 2. Dette er enheter som alle er medlemmer i det internasjonale forumet FIRST ("Forum of Incident Response and Security Teams" [29]. Nedenfor gjengis kort eksempel på oppgaver for de forskjellige typer enheter.

Tabell 2 Norske CERT som er medlem i FIRST [29]

Kort navn	Fullt navn	Vertsorganisasjon	Type selskap
BDO CERT	BDO CERT	BDO AS	IKT sikkerhets-tjenesteleverandør
BF-SIRT	Basefarm SIRT	Basefarm AS	IKT sikkerhets-tjenesteleverandør
DnB IRT	DNB Security Incident Response Team	DNB ASA	Finansselskap
EkomCERT	EkomCERT	Norwegian Communications Authority (NKOM)	Offentlig
KraftCERT	KraftCERT	KraftCERT AS	Energisektor
HelseCERT	HelseCERT, Norsk Helsenett SF	Norsk Helsenett SF	Offentlig
mIRT	mnemonic Incident Response Team	Mnemo	IKT sikkerhets-tjenesteleverandør
NorCERT	Norwegian Computer Emergency Response Team	Norwegian National Security Authority	Offentlig
Nordic Financial CERT	Nordic Financial CERT	Nordic Financial CERT association	Finanssektor
Statoil CSIRT	Statoil Computer Security Incident Response Team	Statoil ASA	Petroleumssektor
TCERT	Telenor CERT	Telenor Norge AS	IKT selskap
UNINETT CERT	UNINETT CERT	UNINETT AS	Forskning og undervisning
UiO-CERT	University of Oslo Computer Emergency Response Team	University of Oslo	Forskning og undervisning

2.6.1 NSM NorCERT

NSM NorCERT er Norges nasjonale CERT og den operative delen av Nasjonal sikkerhetsmyndighet (NSM) for håndtering av alvorlige dataangrep mot samfunnskritisk infrastruktur og informasjon. NSM NorCERT skal [22]

- *Forebygge alvorlige dataangrep mot samfunnsviktige virksomheter og informasjon*
- *Dele informasjon ved hjelp av spesialrapporter, foredrag og annen utadrettet virksomhet*
- *Koordinere respons til alvorlige IT-sikkerhetsangrep mot kritisk infrastruktur og informasjon*
- *Innhente informasjon om alvorlige sikkerhetstruende hendelser på Internett*
- *Koordinere tidlig sikkerhetsoppdatering av samfunnskritiske datasystemer*
- *Fokusere på deling av informasjon*
- *Til enhver tid ha et oppdatert nasjonalt IKT-risikobilde*
- *Hjelpe frem responsmiljøer i Norge*
- *Gi innspill til nasjonale beredskapssystemer og bistår beredskapsarbeidet*

2.6.2 SRM - KraftCERT

KraftCERT som er et eksempel på et sektorresponsmiljø, ble stiftet i 2014 av Statnett, Statkraft og Hafslund etter initiativ fra NorCERT og Norges Vassdrags- og energidirektorat (NVE). Formålet er å være en støtte for hele kraftbransjen både i forebyggende arbeide og i håndtering av hendelser. [23] Gruppen er spesialisert på overvåking, rådgivning og hendelseshåndtering for medlemmenes behov, og at de innehar spesialisert kunnskap om digitale hendelser i bransjen som skal kunne hjelpe medlemmene.

KraftCERT tilbyr følgende tjenester.

- Sårbarhetsovervåkning
- Trusseletterretning
- Deteksjon
- Incident response/hendelseshåndtering
- Rådgivning
- Øvelser
- Kursing

I tillegg til sektorvise responsmiljø, er det flere selskaper som tilbyr produkter og tjenester innenfor IKT-sikkerhet.

2.6.3 IKT-sikkerhetstjenesteleverandør

Nasjonal sikkerhetsmyndighet (NSM) har opprettet en godkjenningsordning for leverandører som tilbyr tjenester for håndtering av dataangrep. Pr i dag er det to virksomheter som tilfredsstiller NSM sine krav: BDO CERT og mnemonic AS.

Typiske tjenesteleveranser er:

- Deteksjon og håndtering av sikkerhetshendelser gjennom egne sensornettverk som oppdager trusler og avvik
- Varsling av trusler basert på analyse og trusselforståelse
- Strategisk rådgiving
- Testing av sikkerhetsrisiko

2.7 Samarbeidsforum IKT-sikkerhetshendelser

Det eksisterer en rekke samarbeidsfora for deling av informasjon og erfaring vedrørende IKT-sikkerhetshendelser. Noen relevante eksempler er gitt i Tabell 3.

Internasjonalt brukes begrepet ISAC ("Information Sharing & Analysis Centre") om fora for samarbeid mellom offentlig og private for deling av informasjon og erfaring om IKT-sikkerhetshendelser. ONG-ISAC er et eksempel på et samarbeidsforum for olje- og gass selskaper i Nord-Amerika. EE-ISAC er et eksempel på et europeisk samarbeidsforum som blant annet inkluderer flere europeiske energiselskaper. FIRST er et globalt medlemsforum for samarbeid mellom betrodde CERT-aktører. Forumet har pr i dag 421 medlemmer. Norske medlemmer i FIRST er vist i Tabell 2.

Tabell 3 Noen samarbeidsfora for IKT-sikkerhet

Navn	Fullt navn	Formål	Referanse
FIRST	Forum of Incident Response and Security Teams	FIRST brings together a variety of computer security incident response teams from government, commercial, and educational organizations. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large.	https://www.first.org/
TF-CSIRT	Task Force on Computer Security Incident Response Teams	TF-CSIRT provides a forum where members of the CSIRT community can exchange experiences and knowledge in a trusted environment in order to improve cooperation and coordination. It maintains a system for registering and accrediting CSIRTs, as well as certifying service standards. The task force also develops and provides services for CSIRTs, promotes the use of common standards and procedures for handling security incidents, and coordinates joint initiatives where appropriate.	https://tf-csirt.org/
ENISA	The European Union Agency for Network and Information Security	The Agency works closely together with Members States and private sector to deliver advice and solutions. This includes, the pan-European Cyber Security Exercises, the development of National Cyber Security Strategies, CSIRTs cooperation and capacity building, but also studies on secure Cloud adoption, addressing data protection issues, privacy enhancing technologies and privacy on emerging technologies, eIDs and trust services, and identifying the cyber threat landscape, and others.	https://www.enisa.europa.eu/
EE-ISAC	European Energy - Information Sharing & Analysis Centre (EE-ISAC)	EE-ISAC is an industry-driven, information sharing network of trust. Both private utilities and solution providers and (semi)public institutions such as academia, governmental and non-profit organizations share valuable information on cyber security & cyber resilience.	https://www.enisa.europa.eu/
ONG-ISAC	Oil and Natural Gas Information Sharing and Analysis Center	ONG-ISAC serves as a central point of coordination and communication to aid in the protection of exploration and production, transportation, refining, and delivery systems of the ONG industry, through the analysis and sharing of trusted and timely cyber threat information, including vulnerability and threat activity specific to ICS and SCADA systems	http://ongisac.org/

3 CERT-kapasitet i næringen

Vi finner lite informasjon om CERT-kapasitet i næringen gjennom åpne kilder/søk på internett.

Equinor opplyser på sine åpne nettsider at de har et beredskapsteam for datasikring som samarbeider med sikringspersonell i hele selskapet for å beskytte selskapets data [26]. Equinor CSIRT er medlem i FIRST [30]. Gassco opplyser på sine åpne nettsider at Gassco Computer Security Incident Response Team (CSIRT) er ansvarlig for å koordinere IKT-sikkerhetsrelaterte hendelser [27]. Både Equinor og Gassco oppgir lenker for å melde om IKT-sikkerhetshendelser.

3.1 Hovedinntrykk fra intervju med selskaper i petroleumsnæringen

Vi har intervjuet representanter fra to operatørselskap og to boreriggselskap på norsk sokkel. Størrelsen på selskapene har ikke overraskende stor innvirkning på svarene. Det synes som om informantene er rimelig tilfreds med nåtilstanden.

Det er stor variasjon i oppfatningen av forskjellen mellom IT- og OT-systemer, og hvem som skal ha ansvar for hvilke systemer. Det varierer også i hvilken grad informantene oppfatter at det er egne utfordringer med å håndtere IKT-sikkerhetshendelser i OT. Flere påpeker at økt bruk av sanntids deteksjon og overvåking av sikkerhetsbrudd i OT systemer vil kunne være nyttig. Like fullt oppfatter mange at det ikke nødvendigvis lar seg gjøre å slå av systemer for å installere sikkerhetsoppdateringer når sikkerhetsbrudd oppdages.

Sikkerhetsbevissthet ("Awareness") i egen virksomhet oppleves ikke som spesielt dårlig. Flere påpeker at sikkerhetskompetansen hos leverandører kunne vært bedre; dette nevnes ofte i sammenheng med en generell underkapasitet på IKT-sikkerhetskompetanse i bransjen (eller i samfunnet).

De som er medlem av NSMs Varslingssystem for Digital Infrastruktur (VDI) mener det er nyttig, men det påpekes at kostnaden for et slikt medlemskap kan være en utfordring for mindre aktører. Det kan være en utfordring for åpenhet og informasjonsdeling at NSM har både rådgivingsfunksjon og tilsynsfunksjon. Så langt har ikke petroleumsbransjen vært omfattet av sikkerhetsloven, og er dermed ikke underlagt NSMs tilsyn. Respondentene opplever uansett ikke dette som et problem, da NSM skiller tydelig mellom tilsynsfunksjonen og CERT-funksjonen. Mange oppfatter at VDI kobler dem utelukkende til NorCERT, og ikke resten av NSM.

En observasjon fra intervjuene er at selskapene ikke savner en "Olje-CERT" for reaktiv håndtering, men flere er positive til tanken om å ha en sektor-basert proaktiv "CERT-lik" organisasjon. Det finnes møteplasser i dag basert på personlige relasjoner; de større aktørene har kontakt med internasjonale miljøer, mens de mindre later til å lene seg mye på leverandører av sikkerhetstjenester. De mindre selskapene som har utenlandske morselskap med eget CERT (eller lignende), synes å ha varierende grad av interaksjon med denne.

Det brukes i liten grad egne verktøy for informasjonsdeling; det meste gjøres via epost og telefon. Noen nevner NorCERT kryptert Internet Relay Chat (IRC), men dette er fortsatt tekstbasert, på friform. Flere nevner Malware Information Sharing Project (MISP) [8] som en plattform for å utveksle kompromitteringsindikatorer (IOC) som IP-adresser og IDS signaturer, men inntrykket er at dette oppleves mest relevant for IT, ikke OT systemer.

Flere informanter nevner "information overload" som et problem når det gjelder informasjon om sårbarheter og angrep, både fra CERT-aktører og andre kilder – dette gjelder også de som får informasjon fra et internt CERT i morselskap i utlandet. Flere har identifisert et behov for å ha en form for automatisert filtrering av informasjonen slik at alt som ikke er relevant for det enkelte selskapet, fjernes før det blir presentert. Dette ville forutsette at hvert selskap har et system for konfigurasjonskontroll som kan gi komplett oversikt over alt

utstyr med tilhørende programvare og behov for oppdateringer. Det virker ikke som noen av aktørene har en slik komplett oversikt i dag.

Alle informantene sier de har egne retningslinjer/prosedyrer for IKT-sikkerhet; disse er i varierende grad basert på internasjonale standarder og det er de interne retningslinjene som har fokus.

Flere av informantene er bekymret for at Ptil ikke har tilstrekkelig kapasitet med den riktige kompetansen. Kompetanse-bekymringen omfatter også NorCERT, ettersom det konstateres at mange yngre, dyktige medarbeidere rekrutteres av andre firmaer, slik at NorCERT har vanskelig for å opprettholde kompetansen over tid. Ptil nyter stor tillit, og informantene indikerer at det er ting de kan snakke om til Ptil, som de ville kvie seg for å dele med andre aktører, også når sistnevnte agerer på vegne av Ptil.

Informantene er delt når det kommer til Ptils ansvarsområde – noen er svært opptatte av at Ptil kun skal befatte seg med OT, og ikke befatte seg med IT og styringssystem for informasjonssikkerhet. Andre ønsker at Ptil fokuserer på både OT og IT, kun avgrenset til Ptils egen kapasitet.

Alle informantene hevder at de har godt samarbeid med andre aktører på norsk sokkel, og at "vi vet hvem alle er". Imidlertid kan det virke som om de mindre aktørene egentlig ikke deler mye informasjon om håndtering av IKT-hendelser med hverandre, og i hvert fall ikke under håndtering av hendelser. Informantene henviser til forskjellige møteplasser (delvis organisert av eksterne aktører som NorCERT eller leverandører), men deling av informasjon her er ikke relatert til aktive hendelser eller kriser. Deling av informasjon om erfaringer i etterkant av hendelser forekommer oftere, og her ser informantene nytten av å lære av andre internasjonale aktørers erfaringer. Inntil nå har man ikke opplevd større hendelser relatert til IKT sikkerhet på norsk sokkel, så det er lite erfaringsgrunnlag på hvordan hendelseshåndtering av større IKT kriser vil fungere i praksis.

4 Operasjonalisering av CERT-varslinger

Informasjonsdeling er en viktig komponent i hendelseshåndtering av cyberangrep. CERT-er utarbeider jevnlig varsler om nye sårbarheter og hendelser. Når en ny skadevare oppdages, videreformidler CERT informasjon fra leverandører, varsler om mottiltak og hvordan skadevaren kan detekteres og fjernes.

Under håndtering og analyse av en hendelse samles det informasjon kalt «Indicators Of Compromise» (IOC), samt «artifakter» fra skadevare-analyse. Dette kan være

- IP-adresser som skadevaren kontakter (skadevaren «ringer hjem» til en kommando og kontrollserver for å motta instruksjoner eller laste ned ytterligere skadevare)
- IP adresser som det sendes «phishing» eposter fra
- filnavn og hash-verdier av filer som skadevaren eller angriperen installerer på systemet
- andre typiske kjennetegn på skadevaren
- info om angriperens «modus operandi».

Disse IOCene deles med andre CERT-er, samt formidles til selskaper som står på CERTs distribusjonslister, ofte i «anonymisert» form ved at identiteten til offeret for cyberangrepet ikke avsløres. For hvert CERT-varsel vurderes også hvilke andre nasjonale og internasjonale CERT-er som bør få informasjon.

Noen eksempler på varslingsveier inkluderer:

- fra NorCERT til det interne respons-teamet hos en virksomhet,
- fra NorCERT til et Sektor CERT og videre til det interne respons-teamet hos en virksomhet, og
- fra et utenlandsk nasjonalt CERT til NorCERT, videre til et sektor CERT og deretter til det interne respons-teamet hos en virksomhet.

4.1 Trafikklysprotokoll

Hensikten med CERT-varsler er at mottaker skal kunne nyttiggjøre seg informasjonen til å sikre sine systemer eller avdekke og håndtere angrep. Dette forutsetter at de har et mottaksapparat og interne systemer og prosesser hvor informasjonen bearbeides videre. IOCer eller informasjon om nye sårbarheter kan for eksempel brukes til å oppdatere brannmurkonfigurasjoner, legge inn signaturer i et inntrengings-deteksjonssystem (IDS), eller søke etter mistenkelige innslag i systemlogger. En virksomhet som operasjonaliserer dette i sine interne prosesser, vil kunne øke sin sikkerhet og evne til å avdekke og håndtere angrep. Om en slik operasjonalisering ikke er på plass, vil CERT-varsler bli overflødig informasjon og kun bidra til å fylle opp innboksen til de som mottar varslene.

Uten tillitsfullt samarbeid bryter partnerskap ned, noe som fører til manglende informasjonsdeling fra etterretningstjenestene, og dermed manglende informasjonsfordeling til CERT-medlemmer. En forutsetning for vellykket deling av informasjon om sikkerhetshendelser, er at den som rapporterer kan stole på at CERT-et bare vil dele videre informasjon som er absolutt nødvendig. Dette betyr at all informasjonsdeling må være strengt behovsbasert.

Spesielt viktig er det at trusselaktørene ikke blir kjent med informasjonen og dermed kan videreutvikle skadevaren eller raffinere angrepsmetodikken sin for å omgå mottiltak. TLP[1] (trafikklysprotokollen) er en standard for informasjonsdeling som sikrer at informasjonseier har kontroll på hvem som mottar informasjon og hvordan denne blir delt videre. Tabell 4 viser nivåer i TLP-protokollen.

[1] https://www.first.org/tlp/

Tabell 4 Trafikklysprotokoll (Oversatt/tilpasset fra FIRST [29])

TLP nivå	TLP:RØD	**Ingen informasjonsdeling utover mottaker** Informasjon kan skade personvern, omdømme eller drift hvis den blir misbrukt.
	TLP:GUL	**Informasjon kan deles internt i mottakers organisasjon eller samarbeidspartere** Informasjonen kan skade personvern, omdømme eller drift hvis den blir misbrukt.
	TLP:GRØNN	**Informasjon kan deles med andre aktører innen sektoren** Informasjonen er nyttig for bevisstheten til alle deltakende organisasjoner og det generelle informasjonssikkerhetsmiljøet.
	TLP:HVIT	**Ingen begrensning på informasjonsdeling** Informasjonen medfører minimal eller ingen forventet risiko for misbruk i henhold til gjeldende regler for publisering.

CERT-varsler om nye sårbarheter som er ment for et større publikum, deles som oftest TLP GRØNN eller HVIT. CERT-varsler som inneholder IOCer som er innhentet i hendelseshåndtering av målrettede angrep, deles ofte TLP GUL. Ved svært sensitiv informasjon blir informasjonen delt muntlig i lukkede møter under TLP RØD.

Det er fortsatt noe forvirring rundt definisjonen av TLP GUL. I den opprinnelige definisjonen var deling begrenset til egen organisasjon.

4.2 Hovedinntrykk fra intervju med selskaper i petroleumsnæringen

Det er stor variasjon blant aktørene i næringen i hvilken grad aktørene har operasjonalisert CERT-varsler i sine interne prosesser og verktøy. Noen informanter oppfatter at CERT-varsler er lite relevante for seg og sin bransje og etterlyser en bedre filtrering av informasjonen. Informanter som ikke kommuniserer direkte med et CERT, uttrykker at de ikke har mottatt CERT-varsler eller har hørt om TLP. Flere ser behov for mer informasjonsdeling, og kan tenke seg en olje-ISAC som kun fokuserer på informasjonsdeling, fremfor et olje-CERT som også bidrar til hendelseshåndtering.

Informasjonsdeling skjer oftest via epost, men noen bruker også informasjonsdelingsplattformer. MISP[2] (Malware Information Sharing Project) blir nevnt av flere aktører. Noen har også utviklet egne plattformer for informasjonsdeling tilpasset interne verktøy og prosesser. Synergi, som er et generelt avvikssystem for rapportering av HMS-hendelser, brukes også til rapportering av IKT-sikkerhetshendelser.

Chatting på NorCERT sin IRC kanal blir nevnt som en nyttig kilde til informasjon for de som deltar i VDI. Det synes som få har fokus på å samle inn og dele IOCer fra egne hendelser med andre aktører i bransjen, dette virker det som det kun er CERT-ene som fokuserer på.

Gradering av informasjon i henhold til sikkerhetsloven kan være en utfordring når aktørene kommuniserer med NorCERT. Noen har opplevd at informasjon som de selv har samlet inn på ugraderte systemer og som de mener burde vært ugradert, har kommet tilbake til dem fra NorCERT som gradert versjon. «Overgradering» av informasjon kan være et problem når man samarbeider med offentlige CERT-aktørerer. En mulig løsning er at man avgraderer informasjonen slik at den kan deles i henhold til TLP. IOCer kan for eksempel deles TLP GUL om man bare fjerner informasjon om hvilken trusselaktør som står bak angrepet.

Noen internasjonale CERT-er har lagt til rette for at liaisoner fra industrien kan være fysisk tilstede i deres lokaler. Dette dreier seg om sikkerhetsklarert personell som fungerer som kontaktpunkter mot de ulike sektorene, og som bidrar til nettverksbygging og informasjonsdeling ut mot de private aktørene.

[2] https://www.misp-project.org

Vårt inntrykk er at de små aktørene har meget begrenset forhold til trafikklys-protokollen (TLP), og at de som mottar TLP-markert informasjon, ofte ikke sender den videre til noen selv om markeringen tillater dette.

5 Selskapenes internrevisjonsmetoder

I tilsynsserien som Ptil gjennomførte mot IKT-sikkerhet i næringen i mai/juni 2017, ble det etterspurt om selskapene har tilfredsstillende internrevisjonsmetoder på plass, og om funn fra revisjonene følges opp på en tilfredsstillende måte. Ptil konkluderte i sin samlede rapport fra tilsynsserien med at selskapene synes å ha tilfredsstillende metodikk på plass som omfatter utsjekk mot interne retningslinjer, bruk av anerkjente normer og standarder, samt eksterne selskaper som også benytter etisk hacking.

På bakgrunn av de intervjuene som er gjennomført med selskapene i denne studien, er det fremkommet begrenset med informasjon om selskapenes internrevisjonsmetoder. Det som har fremkommet av informasjon, tyder allikevel på at det er stor variasjon i hvilken metodikk som benyttes og det er hos enkelte informanter uklart hvilke revisjonsstandarder som ligger til grunn for metodikken i selskapet.

Videre er det varisjoner knyttet til hvilket personell det er som gjennomfører revisjonene. Hos enkelte selskaper er det OT-personell selv som gjennomfører revisjonene, hos andre er ansvaret lagt til selskapets egen revisjonsavdeling, evt. med supplement av innleid ekspertise. Grunnleggende prinsipper for god revisjonspraksis (jf. ISO 19011) omfatter uavhengighet, ojektivitet, upartiskhet og fravær av interessekonflikt [45]. I tilfeller hvor personell som er ansvarlig for drift og vedlikehold av et gitt system også er ansvarlig for gjennomføring av revisjon av det samme systemet, er det sannsynlig at disse prinsippene blir vanskelig å overholde.

6 CERT løsninger i andre segmenter nasjonalt og internasjonalt

I dette kapitlet oppsummeres hovedinntrykk fra intervju med til sammen ti informanter i åtte forskjellige virksomheter. Informantene kommer fra to internasjonale cybersikkerhetssentre (NCSC), fire CERT-er, en ISAC, og en sikkerhetsleverandør (MSSP), hvorav halvparten er nasjonale og halvparten er internasjonale. Av hensyn til anonymisering av informanter, vil vi i dette kapitlet bruke samlebegrepet CERT-aktører for både NCSCer og CERT-miljø og private selskaper som tilbyr produkter og tjenester innenfor IKT-sikkerhet. Størrelsen til aktørene varierer: CERT-informantene har mellom fem og førti ansatte, ISACen har flere tusen medlemmer, og sikkerhetsleverandøren har under to hundre ansatte. Informantene inkluderer fire CERT-ledere, CERT-medlemmer som jobber med hendelseshåndtering, NCSC rådgiver og ledelse, en sikkerhetsrådgiver, en sikkerhetskonsulent og hendelseshåndteringsleder.

6.1 Informasjonsdeling

6.1.1 Tillit

Intervjuene viser at CERT-miljø er avhengige av personlige nettverk ved informasjonsdeling. Dvs. tilgang til informasjon er avhengig av hvem man kjenner. Flere informanter nevner viktigheten av tillit og at tillit skapes gjennom personlige nettverk for informasjonsdeling. Det er lettere å dele sensitiv informasjon med andre som man kjenner personlig. Enkelte epost-lister og uformelle nettverk for informasjonsdeling er også basert på personlige invitasjoner.

Innenfor OT oppleves det vanskelig å vite hvem man kan kontakte siden fagmiljøet er ganske lite. Selv etter en alvorlig hendelse, blir ikke nødvendigvis antivirus selskaper, leverandører eller andre tredjeparter involvert.

Tillit oppleves som en forutsetning for at etterretningstjenester kan dele informasjon med CERT-aktører, for eksempel ved bruk av TLP Rød (ref. Tabell 4). En annen grunn til at tillit oppleves som sentralt ved informasjonsdeling, er at samarbeid mellom virksomheter og organisasjoner som NCSC-er, CERT-er og ISAC-er ofte er frivillig.

6.1.2 Forpliktelse til å dele

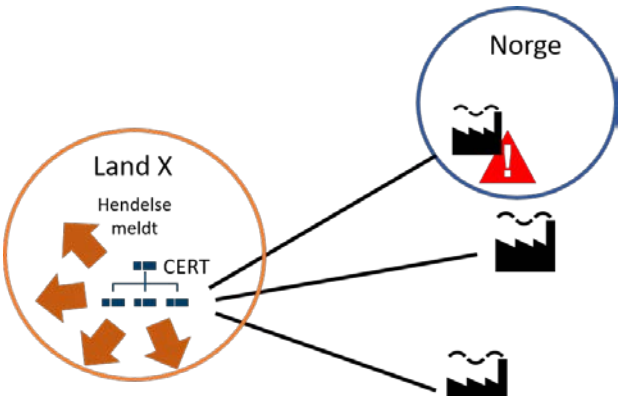
Frivillig informasjonsdeling kan være utfordrende siden bedrifter ikke er forpliktet til å dele selv om informasjon kan være viktig for andre. Denne utfordringen gjelder nasjonalt såvel som internasjonalt.

Regulering er et virkemiddel for å sikre at viktig informasjon og hendelser blir rapportert. I Norge vil for eksempel selskaper som er tilknyttet KraftCERT, være forpliktet til å rapportere alle sikkerhetshendelser. Eventuell videre rapportering til for eksempel NorCERT, kan først skje etter avtale med selskapet.

I dagens regelverk innenfor petroleumsvirksomheten er det krav til umiddelbar varsling til Petroleumstilsynet ved fare- og ulykkessituasjoner som har ført til, eller under ubetydelig endrede omstendigheter kunne ha ført til alvorlig svekking eller bortfall av sikkerhetsrelaterte funksjoner eller barrierer, slik at innretningens eller landanleggets integritet er i fare (Styringsforskriften § 29). I følge veiledningen bør situasjoner der normal drift av kontroll- eller sikkerhetssystemer blir forstyrret av arbeid som ikke er planlagt (IKT-hendelse), varsles.

6.1.3 Samarbeid på tvers av landegrenser

CERT-samarbeid og informasjonsdeling er knyttet til geografi. I ett intervju ble det gitt eksempel på en sikkerhetshendelse som ikke ble rapportert til CERT i landet der den skjedde, men kun ble rapportert til CERT i det landet hvor selskapet har sitt hovedkontor (se Figur 3). Manglende informasjonsdeling på tvers av landegrenser kan dermed føre til at nasjonale CERT ikke har oversikt over alle hendelser i eget land.



Figur 3 Illustrasjon av informasjonsdeling

Ved internasjonalt CERT-samarbeid er det spesielt krevende å forholde seg til en rekke nasjonale forskrifter. Typisk følger CERT-et regelverket i sitt eget land, og overfører ansvar til CERT-et i det andre landet til å følge forskrifter om rapportering av hendelser til sine lokale myndigheter.

NIS-direktivet ble nevnt av flere informanter som et viktig bidrag til forbedret håndtering av IKT-sikkerhetshendelser, inklusive hendelser knyttet til OT-systemer.

6.2 Overvåking og rapportering av IKT hendelser

6.2.1 Sensorer for inntrengningsdeteksjonssystem (IDS)

Sensorer for inntrengningsdeteksjonssystem (IDS) brukes i stor grad for overvåking av IT-systemer, men er lite utbredt for overvåking av OT-systemer innen olje- og gassektoren. En CERT-informant oppgir at de har satt i gang et prosjekt i 2016 hvor man har utplassert sensorer som samler inn informasjon om hvilke systemer som brukes innen OT-nettverkene, slik at de kan sende ut skreddersydde varsler om sårbarheter i disse systemene til sine medlemmer.

CERT-er opplever at de har mer oversikt over IT-sikkerhetshendelser enn OT-hendelser siden OT-systemer ofte mangler løsninger for nettverksovervåkning og inntrengingsdeteksjon. Informantene mener at manglende oversikt gjelder også for CERTets kunder og SAS leverandører.

6.2.2 Rapportering av IKT-sikkerhetshendelser

Flere informanter påpeker forskjell i rapportering og overvåking av sikkerhetshendelser vedrørende IT og OT.

Ved IKT-sikkerhetshendelser er man avhengig av god kommunikasjon med selskapet hvor sikkerhetshendelsen skjer. CERTet tar også ofte kontakt med SAS leverandøren. Dette oppleves som nyttig siden dette gir bedre samarbeid og kontakt med både kundene og SAS leverandøren, samt økt mulighet til å formidle og påvirke IKT-sikkerhetstankegang. Her spiller de personlige kontaktene med leverandøren en viktig rolle. Generelt er ikke håndtering av IKT-sikkerhetshendelser en del av SAS leveransen.

CERTer opplever at manglende teknisk informasjon om OT-systemer er en utfordring ved håndtering av IKT sikkerhetshendelser, samt at det vanskeliggjør overvåking av OT-systemer. Uten innsyn i implementasjonen av protokoller som brukes er det vanskelig å skreddersy IDS løsninger. CERTer og sikkerhetsleverandører ønsker derfor mer samarbeid med leverandører, og gjerne flere åpne løsninger og standarder.

Sikkerhetsoppdateringer kan være en utfordring på OT-systemer, det er gjerne leverandøren som kommer inn og utfører oppdateringer i forhåndsbestemte tidsluker for vedlikehold, og det er stadig en konflikt mellom behovet for oppetid på systemene i forhold til risiko for nedetid om sikkerhetsoppdateringen ikke fungerer som den skal.

6.2.3 Kommunikasjon mellom IT- og OT-miljø

Kommunikasjon mellom IT- og OT-miljø oppleves som vanskelig på grunn av ulik faglig bakgrunn og ulik kultur. Vokabular som brukes i IT, er annerledes enn det som brukes i OT, noe som kan føre til misforståelser og frustrasjon.

En utfordring kan være at IT-personell blir unødig involvert i operasjonelle problemer. En informant refererer til et tilfelle der man trodde at man hadde et sikkerhetsbrudd og satte i gang en stor granskning, før man innså at dette kun var et driftsproblem. Det de trodde var mistenkelig aktivitet på nettverket var resultater av egen aktivitet i forbindelse med hendelseshåndteringen. IT og OT personell kan også være uenige om hva som kvalifiserer som en «hendelse», men samtidig poengteres det at mer samarbeid mellom IT- og OT-miljø er nøkkelen til bedre håndtering av IKT-sikkerhetshendelse, så det er viktig å ikke hindre samarbeid med en for begrensende og detaljert definisjon av OT-sikkerhetsbrudd.

Noen aktører har funnet det de mener er en god balanse med å opprettholde et formelt IT/OT skille mot myndighetene, og faglig samarbeid om teknisk-faglig problemløsning. Det fremholdes at selv om det er ulikheter og det kan være utfordrende å jobbe på tvers av IT og OT, er det viktig å se OT og IT i sammenheng.

6.2.4 Definisjon av IKT-sikkerhetshendelse

Det er forskjellig oppfatning blant CERT-er om hva som defineres som IKT-sikkerhetsbrudd i OT-systemer. Noen informanter har ingen klare definisjoner av IKT-sikkerhetsbrudd, og de vurderer hver hendelse individuelt. Noen CERT-er oppga at deres definisjon av sikkerhetsbrudd innebar at det er kun villede målrettede handlinger som gir sikkerhetsbrudd. Det vil si at de ikke tar med hendelser som skyldes systemfeil. Andre CERT-er ser på IT- og OT-systemer integrert uten å vektlegge skillet mellom IKT- og OT-sikkerhetsbrudd.

Det pågår arbeid hos enkelte CERT-er med å lage en matrise som definerer hva som er et IKT-sikkerhetsbrudd i OT-systemer.

6.3 Sikkerhetsøvelser

Sikkerhetsøvelser er en viktig del av beredskap (se ISO/IEC 27035, NIST SP 800-61 og IEC 62443-2-1 4.3.4.5.1-4 og 4.3.4.5.11).

CERTer mener at sikkerhetsøvelser er viktige. Spesielt kommunikasjon har stort fokus i sikkerhetsøvelsene. Enkelte øver mest på hvordan informasjon blir kommunisert og andre på hvem som skal få informasjon. Noen CERTer organiserer sikkerhetsøvelser flere ganger i året. De fleste fokuserer på store, alvorlige hendelser i sine øvelser.

Det varierer hvor ofte man deltar i OT-sikkerhetsøvelser, og noen CERT sier at de ikke deltar i OT-sikkerhetsøvelser. Det bør utvikles gode scenarier som får frem effektene av IT-hendelser i OT-systemer, men dette oppleves som et krevende arbeid. I CERT-miljø utenfor Norge pågår det arbeid med å forberede slike øvelser.

Noen CERT-er deltar årlig på nasjonale øvelser som fokuserer på OT. Siden private aktører ikke nødvendigvis har ressurser til større øvelser, og heller fokuserer på mindre øvelser som f.eks. phishing-øvelser, ønsker flere informanter i større grad å få delta i nasjonale øvelser i regi av myndighetene. Det er stor nytte av å delta i nasjonale så vel som internasjonale sikkerhetsøvelser fordi de gir bedre samarbeid mellom CERT-er og forbedret forståelse av angrepsteknikker og domenekunnskap.

Det virker som det kan være forskjeller mellom hvordan CERTer i forskjellige land arbeider, og at sør-europeiske land arbeider helt annerledes enn nord-europeiske land.

6.4 Deteksjon og håndtering av sikkerhetsbrudd

Deteksjon og håndtering av sikkerhetsbrudd er beskrevet i flere standarder (se ISO/IEC 27035, NIST SP 800-61 og IEC 62443-2-1 4.3.4.5.5-7).

Deteksjon av OT-sikkerhetshendelse kan skje tilfeldig eller gjennom overvåking. Flere informanter ser betydelig verdi av overvåking med tanke på å opprettholde driftsevne. Det kan være en glidende overgang fra IT til OT overvåkning.

Proprietære protokoller og utstyr som leverandører ønsker å hemmeligholde, kan være en utfordring og begrense informasjonsdeling. Mangelfull informasjon om protokoller vanskeliggjør hendelseshåndtering for et CERT og krever avansert «reverse engineering» for å lage deteksjonssystemer. Et CERT nevner at hver gang de legger inn en IDS-sensor, oppdager de merkelige trafikkmønstre som er ikke ondsinnet, men som skyldes konfigurasjonsfeil og etterlatte systemer som man ikke visste sto tilkoblet nettverket. Det er ofte operativt personell som oppdager og varsler hendelser til CERT-et, noe CERT-et er avhengige av. Automatisk overvåking vil i utgangspunktet være kostnadseffektivt, men personell som kjenner systemene godt, er fortsatt en viktig kilde til å detektere avvik.

En mangel på logging blir nevnt av flere CERT-er som grunn for mindre oppmerksomhet av hendelser i OT enn IT. Det tar tid i store virksomheter å bygge opp infrastruktur for overvåking av alle systemer. Flere IKT-sikkerhetsleverandører tilbyr overvåking av OT-nettverk som en tjeneste, men en informant er skeptisk til dette og mener at dette er mer risikabelt enn sårbarhetsskanning for IT. Enkelte ganger opplever CERT-et at de tilbyr hjelp, men at kunden heller vil håndtere situasjonen selv.

Mange av CERTene ønsker ikke å gi detaljerte eksempler på IKT-sikkerhetsbrudd og håndtering av disse, men flere nevner bruk av USB minnepinne, ofte i forbindelse med at leverandør kobler til sitt eget utstyr når de gjør vedlikehold, som en måte skadevare hadde kommet inn på OT-systemene. Cyber-angrep fra statlige aktører ofte blir fremhevet som en stor trussel, men manglende fysisk sikring og adgangskontroll kan være like viktig. Tilgjengelighet og integritet kan like godt trues av en USB-penn som bringes inn av en leverandør som skal utføre vedlikehold og oppdateringer av systemene.

Generelt blir det hevdet at OT-systemer er godt skilt fra hverandre og at det er vanskelig å traversere et nettverk fra IT til OT, ikke minst på grunn av nettverk «airgapping» som er standard praksis i mange OT-systemer. Airgapping betyr at nettverk og systemer er segregert og fysisk isolert fra hverandre. Dette innebærer at virus ikke lett kan nå et nettverk fra et annet. Men hvis brannmurer er feilkonfigurert, eller hvis personell eller en leverandør bruker flyttbare medier som f.eks. USB minnepinne er det fortsatt mulig å spre en virusinfeksjon. Umiddelbar håndtering kan være å skru av maskinen, isolere den, ta ut pluggen, osv. og så kontakte leverandøren. Derimot kan noen sikkerhetsbrudd spre seg for raskt til at man rekker å slå av maskiner når nettverket er stort, eller hvis skadevaren er av type dataorm og sprer seg uten brukerinteraksjon.

Erfaring med tidligere hendelser, i tillegg til gode planer er viktige for effektiv håndtering av sikkerhetsbrudd. Erfaring fører til at personellet vet hva som bør gjøres og har gode instinkter om hvordan man skal reagere i en slik situasjon.

En CERT-informant forteller om en hendelse hvor det ble spredt skadevare i et OT-system i kraftbransjen. Et HMI system kjørte på utdatert Windows XP operativsystem med administratorbruker. Selskapet var klar over at dette medførte høy risiko og hadde derfor stilt krav til SAS leverandøren i forhold til nettverks-segregering knyttet til en spesifikk maskin, noe som forhindret at viruset spredte seg videre fra HMI til prosesskontrollsystemet. Skadevaren førte til økt nettverksaktivitet og dette ble raskt oppdaget av CERT-et som hadde overvåking av nettverket. CERT-et varslet hendelsen til kundens IT-avdeling og ga råd om tiltak overfor kunden, men ingen andre aktører ble varslet.

6.5 Spesielle utfordringer

CERTer anser lav bevissthet om IKT-sikkerhet i selskapers virksomheters styre og ledelse som en utfordring, og noe som kan føre til mangel på nødvendig ressurser til forbedring og utvikling av sikkerhet. Siden sikkerhetsarbeid ikke merkes når man gjør ting rett, kun når noe går galt, er sikkerhetsarbeidet mindre synlig på styrets nivå. Store sikkerhetshendelser skjer så sjelden at organisatorisk ledelse ikke alltid er oppmerksom på viktigheten av å beskytte OT-systemer mot IKT-trusler. Et eksempel på en mulig løsning er at CERT-et organiserer OT-fokuserte møter hvor man inviterer ledere for informasjonssikkerhet (CISOer), med mål om å legge til rette for bedre samspill mellom ledelse og teknikere.

Behovet for data til granskning og etterforskning er ofte oversett. Det er en generell mangel på logging og særlig mangel på å vite hva som skal logges. Organisasjonen er ofte uvitende om hvilken informasjon politiet trenger i en eventuell etterforskning og hva som er nødvendig for å undersøke årsaken til sikkerhetshendelser. For å skaffe bedre forståelse har et CERT bedt politiet om å bli med i ISACer, noe som øker forståelsen av hvordan sikre nødvendige etterforskningsdata. Utfordringer rundt logging og personvernhensyn, sett i lys av ny lovgivning (GDPR) er også en aktuell og kompliserende faktor.

Det er viktig at selskaper vet hvilke kritiske verdier i egen organisasjon som krever beskyttelse. Hver organisasjon er unik, og må tilpasse sin risikohåndtering etter egne behov og kost-nytte vurderinger. Flere CERT-er tilbyr veiledning og publiserer faktaark med anbefalinger og forslag om bruk av IEC 62443 standarder og NIST retningslinjer, men samtidig oppfordrer de til selskapsspesifikke tilpasninger.

Flere informanter sa at informasjonsdeling og samarbeid om IKT-sikkerhetshendelser mellom sektorer er nyttig, men opplever at det tar tid å bygge opp et slikt samarbeid.

Internasjonalt finnes det eksempel på nært samarbeid mellom sektorvise responsmiljø ved at et NCSC har samlet flere sektor CERT-er under én avdeling. Hensikten er å bidra til økt erfaringsdeling vedrørende håndtering av IKT-sikkerhetshendelser og hvordan en hendelse i en sektor kan påvirke andre sektorer. Vi har også sett ett eksempel på en internasjonalt CERT hvor IT og OT behandles innen samme avdeling.

7 Ptils tilsynsmetodikk innenfor IKT-området

I evalueringen av Ptil som ble gjennomført i 2007, ble det vist til Ptils såkalte Basisnotat – der etaten selv, basert på et bredt kunnskapstilfang, løfter frem de utfordringer den står overfor. Som én av syv hovedutfordringer ble det i Basisnotatet understreket at konsekvenser med hensyn til bruk av IKT i petroleumsvirksomheten er uklare. Det ble videre i Basisnotatet understreket at "tilsynet må avklare konsekvensene av denne utviklingen med hensyn til risiko i petroleumsvirksomheten, regelverkets egnethet og tilsynsmetodenes egnethet" (Ptils Basisnotat iht. Agenda Utredning & Utvikling, 2007, s. 55) [32].

I etterkant av evalueringen har det ikke blitt gjort noen videre ekstern utredning av Ptils tilsynsmetodikk innenfor IKT-området. En slik utredning er det heller ikke lagt opp til i denne rapporten, men vi skal se i grove trekk på hvordan etatens tilsynsaktivitet innen IKT-området gjennomføres. Det vil i neste kapittel også vises til øvrige tilsynsetaters tilsyn med IKT-sikkerhet, og det vil bli vurdert hvorvidt elementer fra disse etatenes tilsynsmetodikk er overførbare til Ptils tilsynsregime.

Begrepet "tilsynsmetodikk" har ikke noen avklart definisjon i offentlig forvaltning. Det skal imidlertid understrekes at Ptil legger en bred forståelse av tilsynsbegrepet til grunn for sin tilsynsmetodikk. Selv om kjernen i tilsynsrollen er den konkrete kontrollen av etterlevelse av regelverkskrav, forstår Ptil tilsyn som "heilskapen i kontakten mellom oss og tilsynsobjekta, og omfattar alle aktivitetar som gir oss det nødvendige grunnlaget for å vurdera om selskapa tek ansvar for å driva forsvarleg" [33].

7.1 Omfang og utbredelse

Ptil foretok i 2007 en gjennomgang av IKT-sikkerhet blant operatørselskapene på norsk sokkel. På bakgrunn av endring i trusselbildet (blant annet etter introduksjonen av viruset Stuxnet), påla etaten i 2012 hele næringen å gjennomføre en egenvurdering av IKT-sikkerhet. Egenvurderingen var basert på spørreskjema utarbeidet til bruk sammen med retningslinje 104 fra Norsk olje og gass. I den påfølgende perioden fra 2013 til 2016 ble det gjennomført flere tilsynsmøter om sikringsrisiko og implementering av sikringstiltak hvor IKT-sikkerhet var en del av tematikken, samt enkelte separate IKT-tilsyn. I ettertid er dette fulgt opp med ytterligere tilsyn av selskapenes håndtering av IKT-sikkerhet i 2017. Tilsynsserien i 2017 var rettet mot operatører av felt og anlegg i drift, samt mot redere med innretninger som har samsvarsuttalelse (SUT).

Ptil har i senere tid styrket kompetansen innenfor IKT-området. Styrkingen av kompetanse innenfor området må ses i sammenheng med at antallet alvorlige angrep på IKT-systemer på tvers av næringer øker [34], og med utviklingen innen digitaliseringen av petroleumsvirksomheten. Digitaliseringen innebærer blant annet videreutvikling av integrerte operasjoner, økt utnyttelse av fjernstyringsteknologi, økt automatisering og en mer omfattende bruk av robotteknologi [35][36].

Styrkingen innenfor IKT-området må også ses i sammenheng med føringer gitt fra politisk hold. Disse føringene kommer blant annet til uttrykk gjennom tildelingsbrevene [37][38][39]. I tildelingsbrevet for 2016 ble IKT-sikkerhet for første gang løftet frem som et separat delmål for etatens virksomhet, hvor det ble understreket at "selskapene skal på grunnlag av risikoanalyser iverksette og opprettholde nødvendige sikringstiltak for å hindre bevisste anslag mot petroleumsvirksomheten, samt sørge for at det til enhver tid er beredskap for å håndtere slike anslag. Dette omfatter også trusler mot informasjons- og datasystem" [37].

7.2 Hjemmelsgrunnlag

HMS-regelverket for petroleumssektoren er primært funksjonsbasert. I motsetning til et preskriptivt regelverk innebærer den funksjonsbaserte tilnærmingen at regelverket først og fremst angir hvilke resultater som

skal oppnås, uten å spesifisere hvordan resultatene skal oppnås eller hvilken fremgangsmåte som skal benyttes for å oppnå et gitt resultat. Den funksjonsbaserte tilnærmingen unngår spesifiserte krav på detaljnivå, og vektlegger aktørenes ansvar for selv å implementere løsninger som sørger for at regelverkskravene oppfylles. Til tross for at HMS-regelverket primært er funksjonsbasert, er enkelte krav mer preskriptivt formulert. Dette gjelder først og fremst for områder der bestemte løsninger er hensiktsmessige.

I henhold til varslingsbrev som sendes tilsynsobjektene i forkant av tilsyn med IKT-sikkerhet, blir tilsynsobjektene opplyst om at tilsynet baseres blant annet på styringsforskriften §§ 4 og 5 og petroleumsloven § 9-3. Disse kravene er utpreget funksjonsbaserte:

- Styringsforskriften § 4 om risikoreduksjon, hvor det fremgår at den ansvarlige skal velge tekniske, operasjonelle og organisatoriske løsninger som reduserer sannsynligheten for at det oppstår skade, feil og fare- og ulykkessituasjoner.
- Styringsforskriften § 5 om barrierer, hvor det fremgår at de skal etableres barrierer som reduserer sannsynligheten for at feil og fare- og ulykkessituasjoner utvikler seg og begrenser mulige skader og ulemper.
- Petroleumsloven § 9-3 om beredskap mot bevisste anslag, hvor det fremgår at rettighetshaver skal iverksette og opprettholde sikringstiltak for å bidra til å hindre bevisste anslag mot innretninger og anlegg samt til enhver tid ha beredskapsplaner for slike anslag.

En rekke andre bestemmelser i HMS-regelverket kan også komme til anvendelse ved tilsyn med IKT-sikkerhet. Dette gjelder særlig innretningsforskriften §§ 32 til 34a (henholdsvis om brann- og gassdeteksjonssystem, nødavstengningssystem, prosessikringssystem og kontroll- og overvåkingssystem). Andre generelle bestemmelser innenfor de ulike forskriftene vil også kunne komme til anvendelse. Det er med andre ord ingen klar avgrensning av hvilke bestemmelser i HMS-regelverket som kan komme til anvendelse ved tilsyn med IKT-sikkerhet.

I veiledningene til forskriftene vises det til ulike industristandarder eller andre normgivende dokumenter som en anbefalt måte å oppfylle regelverkets bestemmelser på. Regelverkskrav anses av Ptil dermed å være oppfylt når man legger anbefalte løsninger til grunn som det vises eksplisitt til i veiledningene. Det er mulig å velge alternative løsninger. Selskapet må da dokumentere at kravet er oppfylt minst like godt som ved å følge anbefalt standard. I veiledningen til innretningsforskriften § 34a om kontroll- og overvåkningssystem, og i veiledningen til teknisk og operasjonell forskrift § 33a om kontroll- og overvåkningssystem, vises det til Norsk olje og gass retningslinje 104 (Anbefalte retningslinjer krav til informasjonssikkerhetsnivå i IT-baserte prosesskontroll-, sikkerhets- og støttesystemer) [11].

Blant de selskapene vi har intervjuet, trekkes ikke nevnte retningslinje frem i særlig grad. Gjennom et toårig felles industriprosjekt er det utviklet en ny retningslinje basert blant annet på IEC 62443-serien. Den nye retningslinjen, DNVGL-RP-G108 Cyber security in the oil and gas industry based on IEC 62443, benyttes i de fleste selskapene vi har intervjuet [9]. I intervju med Ptil fremkommer det at denne retningslinjen ikke kan tas inn i veiledningen per i dag, da deler av IEC 62443 fremdeles er i draftversjon.

7.3 Tilsynsmetode

Ptils tilsynsmetode innenfor området IKT-sikkerhet skiller seg ikke prinsipielt fra øvrige områder etaten fører tilsyn med. Som nevnt ovenfor er hjemmelsgrunnlaget på dette området, som for øvrige områder, funksjonsbasert. Videre er prinsippene om internkontroll også gjeldende her. Bruken av virkemidler er også her, som for øvrige områder etaten fører tilsyn med, basert på dialog og på tillit til at aktørene ivaretar det ansvaret som følger av regelverket. Innen IKT-sikkerhet avgrenser Ptil sitt eget tilsynsområde til å gjelde systemer og rutiner knyttet til operasjonell teknologi (OT). Dette betyr at tradisjonelle IT-systemer faller utenfor tilsynsområdet, og at tilsynsområdet dermed er begrenset til industrielle sikkerhets- og kontrollsystemer

(SAS/SCADA). Den klare avgrensningen av tilsynsområdet følges av et mindre klart skille i trusselbildet. Integrasjonen mellom SAS/SCADA-systemer og tradisjonelle IT-systemer (eksempelvis kontorsystemer) gir økt risiko for både bevisste angrep og ikke-intenderte feil [40].

Tilsynsmetodikken for IKT-sikkerhet er systembasert. Det vil si at etaten ikke fokuserer på tekniske detaljer i hvordan sikkerhetssystemene er bygd opp, men på om selskapenes styringssystemer ivaretar regelverkskravene. Blant de selskapene vi har intervjuet er det bred enighet om at en slik innretning av tilsynsaktiviteten er hensiktsmessig. Det å skulle drive teknisk systemevaluering på dette området vil være krevende og legge krav på betydelige tilsynsressurser, da hvert selskap (og til dels hver innretning) har ulike tekniske løsninger for sikkerhet knyttet til operasjonell teknologi.

Generelt sett er Ptils tilsyn risikobasert. For å kunne arbeide risikobasert er etaten avhengig av et visst kunnskapsgrunnlag. Innenfor de øvrige områdene etaten fører tilsyn med utgjør RNNP en viktig del av dette kunnskapsgrunnlaget, kombinert med blant annet varsling av fare- og ulykkessituasjoner og den kontinuerlige kontakten etaten har med næringen. Det fremkommer i intervjuer med Ptil at den kontinuerlig kontakten med næringen (samt øvrige myndighetsorganer) også på området for IKT-sikkerhet gir etaten en god oversikt over utfordringer, trusler og løsninger. I intervjuene med selskapene synes det imidlertid som at det oppfattes som uklart hvilke IKT-hendelser det er som skal varsles til Ptil. Det er utdypet i veiledningen til styringsforskriften § 29 hvilke hendelser dette gjelder, og dette ble sist oppdatert i desember 2017. Det er derfor mulig informantene ikke har vært klar over den siste oppdateringen. Allikevel, med få varslede IKT-hendelser og på bakgrunn av at IKT-sikkerhet ikke er en del av RNNP, kan det antas at kunnskapsgrunnlaget for en risikobasert tilsynsmetodikk er noe svakere her enn ved øvrige typer av risikoforhold som Ptil fører tilsyn med. Etaten bør derfor vurdere om det er hensiktsmessig å dokumentere risiko i form av et formelt utarbeidet risikobilde, utvikling av nye indikatorer eller lignende, slik det har blitt foreslått tidligere [jf. 36].

7.4 Resultater av tilsynsaktiviteten

Blant de tilsynene som Ptil har gjennomført med IKT-sikkerhet siden 2013 har det ikke blitt avdekt avvik fra regelverket. Det er dermed heller ikke gitt formelle pålegg om utbedringer. Hos enkelte tilsynsobjekter har det imidlertid blitt påvist forbedringspunkter.

Siden Ptils tilsynsrolle dreier seg om helheten i kontakten mellom etaten og tilsynsobjektene, blir det imidlertid ikke relevant kun å se på resultater av tilsynsaktiviteten i form av antall avdekte avvik og observasjoner, og eventuell effekt av slik avdekking. Dialog, samhandling og likelydende brev er de mest brukte virkemidlene til Ptil [35]. Dette gjelder også innenfor området IKT-sikkerhet. Likelydende brev benyttes blant annet til å informere om de observasjoner etaten har gjort gjennom tilsyn. Dette ble gjort i etterkant av tilsynsserien i 2013 og 2017, hvor alt personell fra selskapene som hadde vært involvert i tilsynene ble invitert til en fagdag. Samtlige aktører vi har intervjuet som ble invitert til fagdagen, opplevde at denne ga faglig merverdi og at slike samlinger kan påvirke næringen i positiv retning. Det er derfor flere av de intervjuede selskapene som uttrykker behov for flere lignende samlinger.

For å oppnå læring på tvers i næringen, publiserer også Ptil resultater fra alle tilsyn på sine nettsider. Dette oppleves positivt av de intervjuede, men de understreker samtidig behovet for at deler av tilsynsrapportene innenfor dette temaområdet unntas offentlighet. Dette hensyntas også av Ptil.

8 Øvrige tilsynsetaters tilsynsmetodikk innenfor IKT-området

Som nevnt er det i denne studien gjennomført intervjuer også med enkelte øvrige tilsynsetater. Disse er Nasjonal sikkerhetsmyndighet (NSM), Direktoratet for samfunnssikkerhet og beredskap (DSB), Norges vassdrags- og energidirektorat (NVE) og britiske Health and Safety Executive (HSE). Intervjuene har primært vært gjennomført for å muliggjøre en kontrast til Ptils tilsynsmetodikk, og for å vurdere hvorvidt elementer fra disse tilsynsetatenes tilsynsmetodikk er overførbare til Ptils tilsynsregime.

Basert på det som er beskrevet i forrige kapittel, kan Ptils tilsynsmetodikk innen IKT-området i korte trekk beskrives som (1) funksjons-, (2) system-, (3) internkontroll- og (4) dialogbasert. Det vil si (1) at regelverket er basert på funksjonskrav og ikke preskriptive krav, (2) at etaten fokuserer på om selskapenes styringssystemer ivaretar regelverkskravene og ikke på tekniske detaljer i hvordan sikkerhetssystemene er bygd opp, (3) at selskapene har et selvstendig ansvar for å ta hånd om regelverkskravene, samt undersøke om fremtidige og gjeldende løsninger ivaretar kravene, og (4) at det viktigste virkemiddelet til økt HMS-standard foregår gjennom en tillitsbasert dialog mellom tilsynsetaten og tilsynsobjektene.

Ptils tilsynsmetodikk innen IKT-området skiller seg fra øvrige tilsynsmyndigheters metodikk på enkelte felt, men har også flere likheter. Forskjeller og likheter presenteres i avsnittene nedenfor, supplert med korte drøftinger angående overførbarhet til Ptils tilsynsregime.

8.1 Hjemmelsgrunnlag

Som nevnt ovenfor er HMS-regelverket for petroleumssektoren primært funksjonsbasert. Dette gjelder også for IKT-området. Dersom vi ser på NVEs regelverk for IKT-sikkerhet i energisektoren er dette vesentlig forskjellig fra Ptils regelverk. Det er spesielt beredskapsforskriften kapittel 7 som omfatter krav til sikring av driftskontrollsystemer. De kravene som inngår i kapittel 7 er dels funksjonsbaserte, men i overveiende grad både detaljerte og preskriptive. Eksempelvis er det i § 7-6 stilt krav til at utstyr som benyttes i driftskontrollsystemet ikke skal benyttes i andre nettverk eller løsninger utenom dette systemet, hverken permanent eller midlertidig. Videre stiller samme paragraf krav til at det ikke er tillatt å benytte personlig eid utstyr i driftskontrollsystemet, og at heller ikke trådløse nettverk er tillatt brukt. Detaljeringsgraden er dermed atskillig rikere enn det vi finner i gjeldende regelverk hos Ptil. Videre har NVE utarbeidet en veileder som beskriver hvordan bestemmelser gitt i beredskapsforskriften kan oppfylles [41]. Veilederen er svært omfattende, og lister blant annet opp alle detaljkrav som må tilfredsstilles for å oppfylle de ulike bestemmelsene.

Tilsvarende som for NVE, har også HSE utarbeidet en veileder for IKT-sikkerhet, kalt Cyber Security for Industrial Automation and Control Systems [42]. Veilederen refererer til relevant regulering, god praksis, øvrige veiledere og standarder (herunder IEC 62443, som Ptil bevisst ikke viser til per i dag). Tilsvarende som for Ptil er det imidlertid få bestemmelser i dagens regelverk for olje- og gassvirksomheten som angår IKT-sikkerhet direkte. HSE benytter derfor generelle bestemmelser knyttet til styring av storulykkesrisiko, samt at det i tilsyn henvises direkte til veilederen og de standarder som benyttes der for å avgjøre om bestemmelsene er oppfylt. I intervju med HSE fremkommer det at de generelle bestemmelsene knyttet til styring av storulykkesrisiko ikke er tilstrekkelige for å drive effektive tilsyn på IKT-sikkerhet. Fra og med mai 2018 vil imidlertid NIS direktivet tre i kraft i Storbritannia. Dette vil, iht. intervju med HSE, gjøre hjemling av pålegg lettere som følge av mer konkrete krav.

Både for NVE og for HSE er det altså enten allerede eksisterende konkrete bestemmelser som regulerer IKT-sikkerhet, eller en bevegelse mot mer konkrete bestemmelser. Innenfor Ptils regelverksregime er det imidlertid ingen tradisjon for detaljerte og preskriptive bestemmelser. Blant de selskaper som er intervjuet er det heller ingen som etterlyser mer konkrete krav. Sett i lys av at Ptils tilsyn innenfor området per i dag ikke har resultert i avdekte avvik, kan det imidlertid argumenteres med at etaten har vært tjent med et mer konkret

hjemmelsgrunnlag. På den andre siden kan det argumenteres med at dagens funksjonsbaserte regelverk er fleksibelt og åpner opp for å ta i bruk nye løsninger, og at dette er spesielt viktig innen et område hvor utviklingen går raskt.

8.2 Fokusområde i tilsyn

Som nevnt ovenfor er Ptils tilsynsmetodikk for IKT-sikkerhet systembasert. De tekniske egenskapene til IKT-systemene og tekniske evalueringer av disse er dermed ikke i fokus. Fokusområdet er heller på hvordan og i hvilken grad selskapene har styringssystemer som ivaretar regelverkskravene. Dette er tilsvarende som for de øvrige tilsynsetatene som er intervjuet. HSE poengterer imidlertid at det i etterkant av en hendelse vil være aktuelt å gjennomføre tekniske evalueringer.

I tillegg til systemfokus fremfor teknisk detaljfokus, preges Ptils IKT-tilsyn av å være rettet mot OT-systemer, og ikke de omkringliggende IT-systemer. Som fremgår av intervjuene med etaten er argumentasjonen for dette at etatens tilsynsområde gjelder regulering av helse, miljø og sikkerhet (HMS) og at det dermed kun vil være relevant å kontrollere forhold som angår HMS (og som i dette tilfellet har et storulykkespotensial knyttet til seg). Den klare avgrensningen av tilsynsområdet har, som nevnt ovenfor, et mindre klart skille i trusselbildet. Integrasjonen mellom industrielle sikkerhets- og kontrollsystemer og tradisjonelle IT-systemer gir økt risiko for både bevisste angrep og ikke-intensjonelle feil.

Med unntak av HSE, opererer de øvrige tilsynsmyndighetene ikke med et prinsipielt skille mellom IT- og OT-systemer, da disse ofte har enten intenderte eller ikke-intenderte koblinger seg imellom. Der HSEs fokusområde i tilsyn utelukkende er rettet mot OT-systemer (tilsvarende den avgrensning vi finner hos Ptil), er til eksempel NVEs tilsyn rettet mot OT så vel som mot IT. Hos NVE er unngåelsen av et skille mellom OT og IT begrunnet med basis i energiloven § 9-2 om beredskapstiltak. § 9-2 pålegger eier eller driver av anlegg som er kritiske for kraftforsyningen en plikt til å sørge for effektiv sikring og beredskap og iverksette tiltak for å forebygge, håndtere og begrense virkningene av ekstraordinære situasjoner. For NVE er det derfor de faktorer som kan innvirke på forsyningssikkerheten som er avgjørende for tilsynsområdet, og ikke om disse faktorene er lokalisert innenfor et OT- eller et IT-miljø, eller i grenseflaten mellom disse.

8.3 Risikobasering

For effektiv risikobasering av tilsynsvirksomheten er Ptil, som andre tilsynsetater som arbeider risikobasert, avhengig av et visst kunnskapsgrunnlag. RNNP er en viktig del av dette kunnskapsgrunnlaget. IKT-sikkerhet er imidlertid ikke en del av RNNP.

I denne studien er det ikke gjort en grundig undersøkelse av hvilke verktøy de øvrige tilsynsetatene besitter for å fremskaffe et tilstrekkelig kunnskapsgrunnlag. HSE planlegger imidlertid en spørreundersøkelse knyttet til temaet IKT-sikkerhet, rettet mot sine tilsynsobjekter i olje- og gassektoren. Hensikten med undersøkelsen vil være å få mer kunnskap om risiko- og sårbarhetsfaktorer. Tilsvarende har NVE i 2017 utarbeidet rapporten *Informasjonssikkerhetstilstanden i energiforsyningen* [43]. Rapporten gir et bilde av sikkerhetshendelser som virksomhetene i kraftbransjen har erfart siste år. Rapporten er, likt HSEs planlagte undersøkelse, basert på en spørreundersøkelse, og er en del av et større prosjekt hos NVE der formålet er å kunne monitorere utviklingen i sikkerhetstilstanden i energisektoren. NSM utarbeider et årlig kunnskapsgrunnlag, kalt *Helhetlig IKT-risikobilde* [44]. Risikobildet retter seg mot ledere og personell med sikkerhetsoppgaver, og skal bidra til bedre IKT-sikkerhet i offentlige og private virksomheter. Risikobildet fremstår derfor mer utadrettet enn som en samling av kunnskap som ligger til grunn for etatens prioriteringer.

Ptil gjennomførte i 2012 tilsyn med IKT-sikkerhet i bore-, prosesskontroll-, sikkerhets- og støttesystemer. Tilsynsaktiviteten ble gjennomført i form av en egenevaluering (spørreskjema) av egen virksomhet basert på

et spørreskjema utarbeidet til bruk sammen med retningslinje 104 fra Norsk olje og gass. Formålet med aktiviteten var å få oversikt over nivået innen IKT-sikkerhet i petroleumsnæringen generelt og hos den enkelte aktør. For å få et strukturert kunnskapsgrunnlag for risikobasering kan lignende egenevalueringer, eventuelt utvikling av nye indikatorer e.l. utvikles og benyttes i den fremtidige kunnskapsinnhentingen. Dette har også blitt foreslått i en tidligere gjennomgang av Ptils tilsynsvirksomhet. Risikobasert tilsyn handler i stor grad om utvelgelse av de mest risikoutsatte tilsynsbojekter, og om prioritering av tilsynstema med størst risikopotensial. Slike prioriteringer muliggjøres gjennom et strukturert og fyldig informasjonstilfang.

8.4 Differensiering

Som nevnt ovenfor, differensierer ikke Ptils tilsyn innen IKT-området mellom store og små aktører. På dette feltet skiller etaten seg fra for eksempel NVEs aktivitet overfor tilsynsobjektene, som i større grad benytter veiledning overfor små aktører og tradisjonelle kontrollaktiviteter overfor store aktører. NVEs begrunnelse for en slik differensiering er (1) at små aktører har et lavere kunnskapsgrunnlag, og (2) at små aktører ikke er samfunnsmessig kritisk for energiforsyningen. Det følger imidlertid av Ptils instruks at etaten er tillagt myndighet for regulering og oppfølging av helse, miljø og sikkerhet. I lys av dette kan det argumenteres med at det vil være lite hensiktsmessig å anvende differensierte tilsynsmetoder basert på størrelse, da kravene til helse, miljø og sikkerhet gjelder uavhengig av det enkelte selskaps størrelse – og at en hendelse hos en liten aktør kan være vel så alvorlig som en hendelse hos en stor aktør.

9 Standarder og regelverk

Det er spesielt følgende lover og forskrifter som kommer til anvendelse i Petroleumtilsynets tilsyn av industrielle kontrollsystem:

- Innretningsforskriften § 34a om kontroll- og overvåkingssystem; Norsk olje og gass retningslinje nr. 104 bør legges til grunn for beskyttelse mot IKT-relaterte farer.
- Styringsforskriften § 4 om risikoreduksjon; den ansvarlige skal velge tekniske, operasjonelle og organisatoriske løsninger som reduserer sannsynligheten for at det oppstår skade, feil og fare- og ulykkessituasjoner.
- Styringsforskriften § 5 om barrierer; etablere barrierer som reduserer sannsynligheten for at feil og fare- og ulykkessituasjoner utvikler seg og begrenser mulige skader og ulemper.
- Petroleumsloven § 9-3 om beredskap mot bevisste anslag; rettighetshaver skal iverksette og opprettholde sikringstiltak for å bidra til å hindre bevisste anslag mot innretninger og anlegg, samt til enhver tid ha beredskapsplaner for slike anslag.

9.1 Standarder og veiledninger for IKT-sikkerhet (OT) i industrielle kontrollsystemer

Nedenfor følger en oversikt over relevante standarder innen IKT-sikkerhet (OT) (se Tabell 5).

Tabell 5 Standarder og veiledninger for IKT-sikkerhet i industrielle kontrollsystemer

Referanse	Tittel	Lenke
Standarder		
IEC 62443 series	Industrial Automation and Control Systems Security	Bestilles: http://www.standard.no/nettbutikk/sokeresultater/?search=62443
Retningslinjer		
DNV-GL-RP-G108	Cyber security in the oil and gas industry based on IEC 62443 (2017)	https://www.dnvgl.com/oilgas/download/dnvgl-rp-g108-cyber-security-in-the-oil-and-gas-industry-based-on-IEC-62443.html
DNV GL-RP-G0496	Cyber security resilience management for ships and mobile offshore units in operation (2016)	https://www.dnvgl.com/maritime/dnvgl-rp-0496-recommended-practice-cyber-security-download.html
NorOG RP 104	104 – Norwegian Oil and Gas recommended guidelines on information security baseline requirements for process control, safety and support ICT systems. (2016)	https://www.norog.no/contentassets/15263fd7f781409286f319bbeb427d93/104-recommended-guidelines-on-security-baseline-requirements.pdf
NIST 800-61 R2	Computer Security Incident Handling Guide	http://dx.doi.org/10.6028/NIST.SP.800-61r2
NIST 800-82 R2	Guide to Industrial Control Systems (ICS) Security (2015)	http://dx.doi.org/10.6028/NIST.SP.800-82r2
NIST	Framework for Improving Critical Infrastructure Cybersecurity, 1.1 Draft 2 (2017)	https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
ISA-TR84.00.09	Cybersecurity Related to the Functional Safety Lifecycle (2017)	Bestilles: https://www.isa.org/store/isa-tr840009-2017,-cybersecurity-related-to-the-functional-safety-lifecycle/56889051
Veiledninger myndigheter		
HSE	Cyber Security for Industrial Automation and Control Systems (IACS)	http://www.hse.gov.uk/foi/internal-ops/og/og-0086.pdf
NSM	Rammeverk for håndtering av IKT-hendelser (2017)	https://nsm.stat.no/publikasjoner/rad-og-anbefalinger/rammeverk-hendelseshandtering/

En overordnet beskrivelse av formål og innhold i standardene er gitt i Vedlegg A.

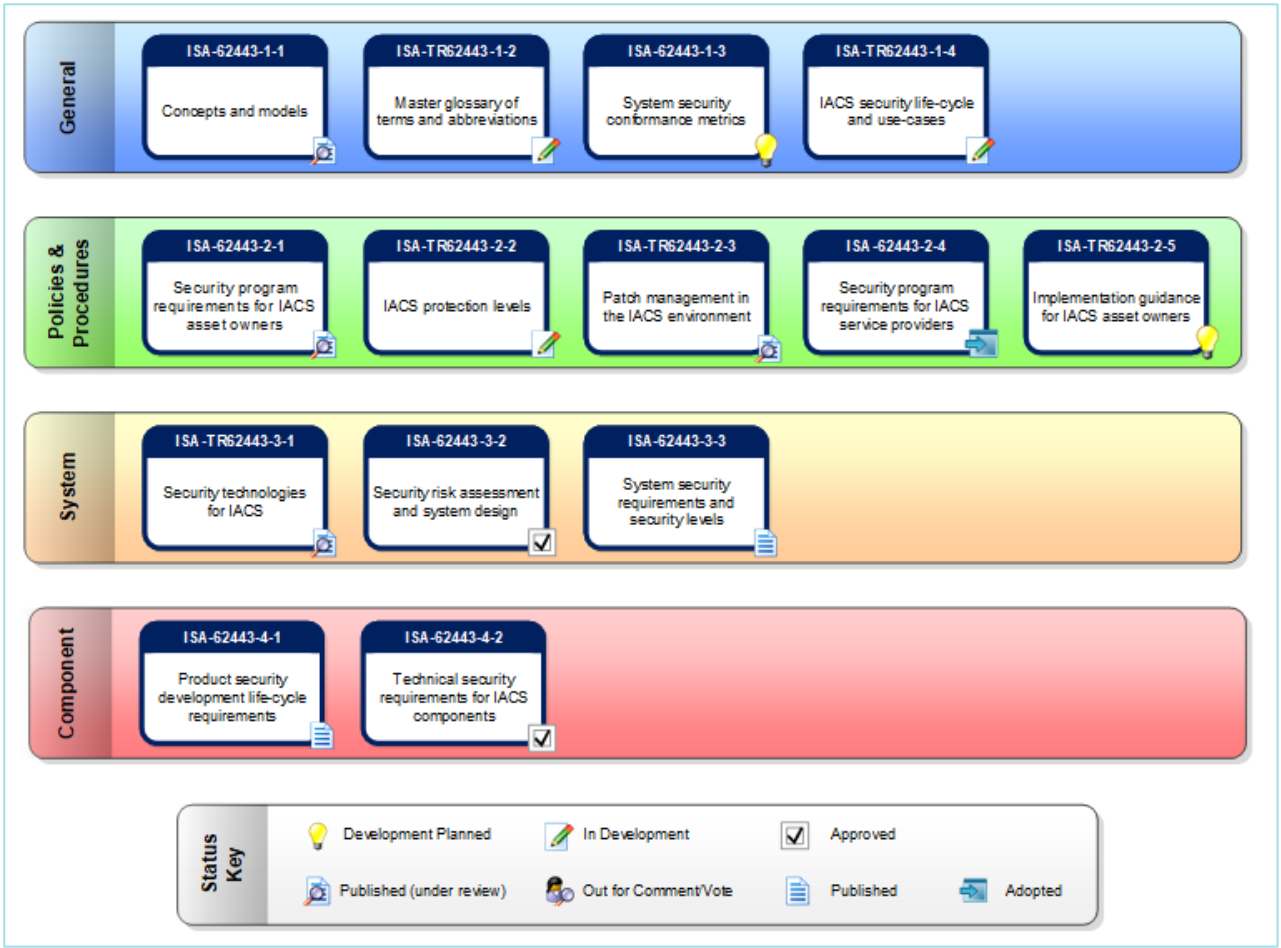
Den sentrale standarden innenfor IKT-sikkerhet (OT), er IEC 62443: "Industrial Automation and Control Systems Security" (se Figur 4). Merk at flere av dokumentene i denne serien fortsatt er under utvikling.

IEC 62443 standarden er grunnlaget for utvikling av DNV GL retningslinje 108 for petroleumssektoren: "Cyber security in the oil and gas industry based on IEC 62443". I tillegg har DNV GL utviklet retningslinje 0496: "Cyber security resilience management for ships and mobile offshore units in operation"

I USA har National Institute for Standards and Technology (NIST) utviklet flere retningslinjer for vurdering av IKT-sikkerhet som også er relevante for petroleumsvirksomheten. I siste revisjon av Norsk olje og gass sin anbefalte retningslinje 104 vedrørende krav til industrielle kontrollsystemer, er implementeringsguiden strukturert i henhold til NIST rammeverket: "Cyber Security Framework" (se Tabell 6).

NVE-rapporten: "Regulering av sikkerhet" [46] lister en rekke standarder og veiledere innenfor bl.a. informasjonssikkehetsledelse, kommunikasjon og sikkerhet i SCADA og kritisk infrastruktur som også er relevant for petroleumsvirksomheten.

En relevant standard med fokus på generell IT er ISO/IEC 27001: "Information technology — Security techniques — Information security management systems " [6]. I arbeidet med Norsk olje og gass sin retningslinje 104 [11] ble det tatt utgangspunkt i IEC 27001 og de tiltakene som er i den standarden.



Figur 4 Dokumenter i IEC 62443 serien

Tabell 6 NIST "Common Security Framework" [14]

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

I henhold til veiledningen til Styringsforskriften § 5 om barrierer, bør standarder som IEC 61508, IEC 61511, IEC 62061 og ISO 13849 legges til grunn for petroleumsvirksomheten til havs. Disse standardene omfatter primært "Functional safety" og er ikke direkte rettet mot IKT-sikkerhet. I veiledningen vises det til Norsk olje og gass retningslinje nr. 070 (NOROG 070) som gir eksempler på bruk av IEC 61508 og IEC 61511. NOROG 070 ble først utgitt høsten 2000 som en veiledning for implementering av 61508/511 og det var ikke noen IKT-sikkerhetsklausul i standardene da. I revisjonen av 070 har det vært fokus på å gå gjennom appendix og oppdatere disse, både i forhold til tallgrunnlaget og utvide med flere typiske løsninger. I og med at det da har kommet andre retningslinjer (og etter hvert standarder for IKT-sikkerhet) har det ikke vært uttrykt behov for å inkludere dette i 070.

9.2 Standarder for IKT hendelseshåndtering

Hendelseshåndtering for IT-systemer er beskrevet i standarden ISO/IEC 27035 [5]. Alle elementene vedrørende hendelsesorientering som nevnes i IEC 62443-2-1, kan passe inn i ISO/IEC 27035, som vist i Tabell 7. I NIST SP 800-61 [6] er hendelseshåndtering inndelt i kun 4 hovedfaser, men koblingen til ISO/IEC 27035 er også her ganske rett fram.

Tabell 7: Faser i hendelseshåndtering i ulike standarder

ISO/IEC 27035	NIST SP 800-61	IEC 62443-2-1
Plan and prepare	Preparation	4.3.4.5.1 Implementer en hendelseshåndteringsplan
		4.3.4.5.2 Kommuniser hendelseshåndteringsplanen
		4.3.4.5.3 Etabler en rapporteringsprosedyre for uvanlige aktiviteter og hendelser
		4.3.4.5.4 Lær ansatte opp til å rapportere sikkerhetshendelser
		4.3.4.5.11 Hold øvelser
Detection and reporting	Detection and analysis	4.3.4.5.5 Rapporter sikkerhetshendelser i god tid
		4.3.4.5.6 Identifiser og responder på hendelser
Assessment and decision		4.3.4.5.7 Identifiser mislykkede og vellykkede IKT-sikkerhetsbrudd
Responses	Containment, Eradication & Recovery	4.3.4.5.6 Identifiser og responder på hendelser
		4.3.4.5.10 Adresser og korriger forhold som oppdages
Lessons Learned	Post-incident activity	4.3.4.5.8 Dokumenter detaljene ved en hendelse
		4.3.4.5.9 Kommuniser detaljene ved en hendelse

10 Oppsummering og konklusjoner

Oppsummering og konklusjoner nedenfor er i stor grad basert på hovedinntrykk fra intervju med fageksperter i olje- og gasselskaper, boreriggoperatører, Petroleumstilsynet, nasjonale og internasjonale enheter for IKT-sikkerhet (CERT), nasjonale og internasjonale tilsynsmyndigheter, samt leverandører av IKT-sikkerhetstjenester.

10.1 CERT-kapasitet i næringen

Inntrykket fra åpne kilder er at kun de største aktørene på norsk sokkel, som Equinor og Gassco, formidler til omverdenen at de tar rapportering av sikkerhetskritiske IKT-hendelser på alvor.

Det er større interesse for informasjonsdeling (ISAC) enn for støtte til hendelseshåndtering (CERT), samtidig som at det er bemerkelsesverdig lite fokus på å dele informasjon og "lessons learned" om sikkerhetshendelser med hverandre.

Informantene gir inntrykk av å være relativt tilfreds med sin egen kapasitet til å håndtere slike hendelser per i dag, men det erkjennes at man alltid kan bli bedre, f.eks innen sanntids overvåking av sikkerheten i OT. På den ene siden gis det inntrykk av et lite men tett miljø der "alle kjenner alle", men informantene peker også spesielt på behov for bedre informasjonsdeling og nettverksaktiviteter som virkemidler for kompetanseheving hos små oljeselskaper. Overraskende nok er det ingen informanter som peker på Norsk Olje og Gass som en viktig aktør i denne sammenhengen.

Fram til nå er andelen av rapporterte hendelser som angår OT-systemer liten, noe som kan bidra til at behovet ikke oppleves som prekært. I omtalen av enkelte IT-hendelser er det imidlertid blitt uttalt at de "heldigvis ikke spredte seg til OT". Dette kan tolkes som at sannsynligheten for hendelser som berører OT er til stede, og ikke minst at konsekvensene ville vært store og til dels vanskelig å håndtere.

Ikke alle olje- og gasselskaper eller boreriggoperatører skiller mellom IKT-sikkerhetshendelser i IT-systemer og OT-systemer. Det er også stor variasjon i synspunkter på hvem som har ansvar for sikkerheten i IT og OT, og i grensesnittet mellom dem. I den grad skillelinjer er beskrevet, handler dette for eksempel om sanntidskrav og anledningen til å slå av systemer for å gjøre oppdateringer, og om den krevende balansen mellom driftstilgjengelighet og IKT-sikkerhet i SAS.

Alle informantene har interne retningslinjer for arbeid med IKT-sikkerhet. Disse er i varierende grad basert på internasjonale standarder. Standarden IEC 62443 og DNV-GL-rapporten som er basert på denne, blir i større grad nevnt av informantene enn retningslinjen fra Norsk Olje og Gass.

Håndtering av IKT-sikkerhetshendelser i prosesskontroll- og sikkerhetssystemer krever ofte bidrag fra SAS-leverandør i tillegg til støtte fra CERT. Noen påpekte at IKT-sikkerhetskompetanse og oppmerksomhet hos SAS-leverandører er mangelfull. Dette ble til dels forklart med mangel på IKT-sikkerhetskompetanse i samfunnet for øvrig, noe som også gir seg utslag i noe tvil om kompetanse/kapasitet hos Ptil, og bekymring for stor gjennomtrekk av ansatte hos NSM NorCERT.

Tilliten til Ptil når det gjelder å dele informasjon på dette området er tilstede, men det er uenighet om hvorvidt Ptil bør fokusere kun på OT, eller på både IT og OT. For noen er dette et prinsipielt spørsmål knyttet til at man ikke vil ha for mange tilsynsmyndigheter inn på IKT-området, eller at Ptil ikke bør fokusere på styringssystem for IT-sikkerhet. For andre er det kun et spørsmål om Ptils egen kapasitet og kompetanse til å dekke begge. I noen grad stilles det imidlertid også spørsmål om Ptil har tilstrekkelig kompetanse på OT-

sikkerhet. I henhold til regelverket har Ptil delegert myndighet for OT-systemene og selskapene har selv totalansvar for både sine IT- og OT-systemer og oppfølging/monitorering av trusler og risiko mot disse.

Medlemsskap i NSM's VDI nettverk oppleves som nyttig, men er et kostnadsspørsmål for mindre aktører. NSMs ulike roller, og disses kopling til VDI, er ikke like tydelig for alle aktørene.

Graden av utnyttelse av CERT-tjenester varierer. Det uttrykkes ikke noe spesifikt behov for en SRM i form av en dedikert "olje-CERT" for å håndtere hendelser. Det opplevde behovet for slik støtte synes å være dekket gjennom en blanding av personlige relasjoner til responsmiljøer, støtte fra morselskap (selv om graden av interaksjon med disse varierer), bruk av leverandører av sikkerhetstjenester, eller et godt samarbeidsklima i næringen der man "vet hvem alle er".

Imidlertid gis et inntrykk av at de mindre aktørene egentlig samarbeider lite, og aller minst i aktive hendelser eller kriser. Det vises til ulike møteplasser (delvis organisert av eksterne aktører), og det fremmes samtidig ønsker om en mer proaktiv CERT-funksjon. Dette kan tolkes som et ønske mer i retning av behov for ISAC enn CERT.

Informasjonsdeling skjer hovedsakelig gjennom generelle verktøy som epost og telefon, eller NSMs krypterte IRC-tjeneste. Utveksling av kompromitteringsindikatorer handler stort sett om IT, ikke OT-systemer.

Aktørene opplever ofte "information overload" forårsaket av både CERT-er og andre kilder. Det uttrykkes ønsker om filtreringsverktøy, men slike vil forutsette en grad av konfigurasjonskontroll som ikke er utbredt i dag (og som vil kreve et betydelig løft).

10.2 Operasjonalisering av CERT varslinger

Det er stor variasjon i om aktørene har operasjonalisert CERT-varsler i sine interne prosesser og verktøy. Noen oppfatter CERT-varsler som lite relevante for seg og sin bransje, og etterlyser en filtrering av informasjonen.

I den grad informasjon deles mellom aktørene, skjer dette via epost, men også via plattformer som MISP og IRC (NorCERT). TLP som sådan er lite kjent blant de som ikke mottar CERT-informasjon. Mindre aktører som er uvante med TLP, videresender ofte ikke informasjon, selv om markeringen tillater dette.

Når aktørene rapporterer til NorCERT oppleves tilfeller av «overgradering», gjennom at «ugradert» informasjon som blir sendt inn, kommer tilbake med «gradering». Dette gjelder både «gradering» i form av TLP kode, men også gradering iht lovverket. Aktører oppfatter at dette kan unngås gjennom kun å kommunisere handlings-/løsnings-orientert informasjon, og utelate informasjon om konkrete trusler/aktører, og derved for eksempel kunne bruke TLP GUL. Det vises også til at internasjonale CERT-er opererer med industri-liaisoner, som fungerer som kontaktpunkter mot ulike sektorer, noe som kan bidra positivt til operasjonalisering av informasjonsdeling.

Ved deling av informasjon om sikkerhetshendelser, er det en forutsetning for aktørene at den som rapporterer, kan stole på at CERT-et bare deler videre informasjon som er absolutt nødvendig. Dette betyr at all informasjonsdeling må være strengt behovsbasert og gjerne filtrert. Kjennskap til og etterlevelse av TLP er en viktig komponent i dette.

Synergi brukes i noen grad til registrering av IKT-hendelser internt hos oljeselskapene.

10.3 CERT løsninger i andre segmenter nasjonalt og internasjonalt

Det er en rekke beredskapsenheter for IKT-sikkerhet i Norge som har CERT-lisens. Noen er på nasjonalt nivå (NSM NorCERT), noen er på sektornivå (f.eks. HelseCERT og KraftCERT som er et frivillig, medlemskapsbasert sektorresponsmiljø for energisektoren), noen er internt i et selskap (f.eks. Telenor CERT) og noen tilbyr IT-sikkerhetstjenester innenfor beredskap (BDO CERT og mnemonic Incident Response Team). Alle de nevnte selskapene er medlemmer i forumet FIRST ("Forum of Incident Response and Security Teams") som er et globalt medlemsforum for samarbeid mellom betrodde CERT-enheter.

Det internasjonale bildet er variert og gir ikke noen klare føringer for organiseringen av SRM-er i Norge. Internasjonalt observeres at beslektede sektor-CERT-er samles for bedre ressursutnyttelse. Selv om CERT-er opprinnelig har hatt overveiende fokus på IT, er det en internasjonal trend at man i økende grad begynner å interessere seg også for OT. Nasjonalt er det spesielt KraftCERT som representerer en tilsvarende trend, der man eksplisitt anerkjenner forskjellen mellom, og aktivt søker å forene håndteringen av IT og OT.

CERT-aktørene viser til at antallet CERT-enheter må stå i forhold til den faktiske tilgangen på kompetanse og ressurser, men at en viss form for samordning alltid vil tvinge seg fram. Det er en klar tendens til at ISAC framstår som like viktig som CERT for den enkelte sektor. Bedre kommunikasjon er imidlertid en fellesnevner, og ikke minst reell kontakt mellom CERT-er og sentrale personer i selskapene.

Selv om CERT-funksjoner i stor grad er formaliserte, er personlige nettverk fortsatt veldig viktige for tillitsfull informasjonsdeling, spesielt når det gjelder utveksling av sensitiv informasjon. Selskaper er i liten grad forpliktet av regelverk til å dele informasjon med andre. I noen grad skapes imidlertid slike forpliktelser gjennom medlemskap i nettverk (f.eks KraftCERT), men videreformidling (f.eks. til NorCERT) krever fremdeles samtykke.

Petroleum-regelverkets krav om rapportering av driftsforstyrrelser dekker også IKT-hendelser. Imidlertid vil hendelser som utløser CERT-aktiviteter ikke nødvendigvis bli oppfattet som en fullbrakt driftsforstyrrelse. Internasjonale selskaper kan også erfare problemer knyttet til at rapportering av hendelser til moderselskapets nasjonale CERT ikke medfører videreformidling til den nasjonale CERT-en som er "nærmest" hendelsen. Når et stort selskap opererer internasjonalt og rapporterer sikkerhetshendelser bare til CERT-et i det samme landet hvor det har sitt hovedkontor, er det også en regelverksutfordring fordi et slikt problem er knyttet til lovforskjeller mellom land og kompleksiteten som følger av å prøve å følge for mange reguleringer.

Det er samtidig utfordrende for CERT-er å få god oversikt og overvåke IKT-sikkerhet i OT-systemer. Hovedfokus er og har vært på IT. Det er reelle tekniske forskjeller mellom IT og OT. Proprietære løsninger og omfattende "airgapping" i OT-domenet har en positiv primæreffekt, men skaper også uheldige ringvirkninger. IDS kan f.eks. ikke uten videre fungere like godt i en OT-kontekst, det er ulike tradisjoner for administrasjon av brukerrettigheter, og systemenes autonomi er varierende .

Ulik terminologi og generelle språkforskjeller mellom IT og OT kan dessuten også hindre kunnskaps- og erfaringsoverføring som kunne sikret OT-systemer bedre. I verste fall kan slike ulikheter også skape misforståelser som fører til sikkerhetshendelser, f.eks gjennom at aktivitet på IT-området forstyrrer OT-funksjonen, eller at driftsproblemer på OT forveksles med sikkerhetsbrudd. Den kommunikative utfordringen har blitt synliggjort gjennom faktiske (OT-) hendelser som ikke er blitt kommunisert verken til antivirus-selskaper, leverandører eller andre tredjeparter. Den faktiske definisjonen av et sikkerhetsbrudd er heller ikke tilstrekkelig avstemt mellom IT og OT, og det er eksempler på at lokal problemløsning i forbindelse med særegne IT/OT-kombinasjoner ikke blir kommunisert til andre interessenter.

Bedre samarbeid er ønskelig, men dette vanskeliggjøres også av at selve OT-miljøet i næringen og blant leverandørene er relativt lite, og at det er krevende for et CERT å finne de rette kontaktene. Et CERT er avhengig av god kommunikasjon med både selskapet og leverandøren for å løse faktiske problemer, men det er lite tradisjon for dette, sammenlignet med IT. Her spiller både (mangel på) personlige kontakter og innsikt i f.eks. proprietære protokoller inn, noe som kan kreve betydelig og tidkrevende "reverse engineering", ikke minst når dette kombineres med nettrafikkmønster i OT-domenet som er vesensforskjellig fra det som erfares i IT-domenet. Det er også en begrunnet skepsis mot bruk av løsninger for sårbarhetsskanning, tredjeparts overvåkning o.l. i OT-domenet.

Mangelfull logging i OT-domenet trekkes fram som en viktig faktor som hindrer god nok evne til deteksjon, håndtering og gransking etter hendelser.

Sikkerhetsøvelser trekkes inn som et viktig tiltak, men flere CERT-er sier at OT ikke er en del av deres øvingsaktivitet. Det er også betydelige nasjonale forskjeller på dette området.

Fra CERT-hold observeres manglende kommunikasjon mellom teknisk og ledelsesnivå i selskapene. Man ser en tendens til at den kritiske problemløsningen på teknisk nivå foregår i "det stille" og ikke blir verken observert eller verdsatt, med det resultat at vellykket arbeid kan medføre mindre tilgang på ressurser, og dermed større risiko.

I forhold til krisesituasjoner vektlegger noen informanter kommandokjeden, mens andre legger mer vekt på klare roller og kommunikasjon.

10.4 Relevante standarder innen IKT-sikkerhet (OT) og tilstøtende regelverk

Den sentrale standarden innenfor IKT-sikkerhet (OT), er IEC 62443: "Industrial Automation and Control Systems Security". Flere av dokumentene i denne serien fortsatt er under utvikling. IEC 62443 standarden er grunnlaget for utvikling av DNV GL retningslinje 108 for petroleumssektoren: "Cyber security in the oil and gas industry based on IEC 62443". De fleste informantene i studien nevner IEC 62443 og/eller DNV-GL-rapporten som er basert på denne.

10.5 Aktuelle internrevisjonsmetoder for selskapene selv

Det synes å være er stor variasjon i hvilken metodikk for internrevisjon som benyttes hos selskapene, samt variasjon i inngående kjennskap til metodikken blant de intervjuede. Det er også variasjon knyttet til hvilket personell det er som gjennomfører revisjonene i selskapene. Hos enkelte selskaper er det OT-personell selv som gjennomfører revisjonene, hos andre er ansvaret lagt til selskapets egen revisjonsavdeling, evt. med supplement av innleid ekspertise. I tilfeller hvor personell som er ansvarlig for drift og vedlikehold av et gitt system også er ansvarlig for gjennomføring av revisjon av det samme systemet, er det sannsynlig at prinsipper for god revisjonspraksis (uavhengighet, ojektivitet, upartiskhet og fravær av interessekonflikt) blir vanskelig å overholde.

10.6 Aktuelle tilsynsmetoder for Ptil

Gjennomgangen av Ptils tilsynsmetoder innenfor IKT-området viser at metodikken her ikke avviker nevneverdig fra øvrige områder etaten fører tilsyn med. Hjemmelsgrunnlaget som tilsynene bygger på er i mindre grad preskriptivt og detaljorientert enn hva vi finner hos for eksempel NVE. Sett i lys av at Ptils tilsyn innenfor området per i dag ikke har resultert i avdekte avvik, kan det argumenteres med at etaten hadde vært tjent

med et mer konkret hjemmelsgrunnlag. På den andre siden kan det argumenteres med at dagens funksjonsbaserte regelverk er fleksibelt og åpner opp for å ta i bruk nye løsninger, og at dette er spesielt viktig innen et område hvor utviklingen går raskt.

Med få varslede IKT-hendelser og på bakgrunn av at IKT-sikkerhet ikke er en del av RNNP, kan det antas at kunnskapsgrunnlaget for en risikobasert tilsynsmetodikk er noe svakere her enn ved øvrige typer av risikoforhold som Ptil fører tilsyn med. Etaten bør derfor vurdere om det er hensiktsmessig å dokumentere risiko i form av et formelt utarbeidet risikobilde, egenevaluering fra selskapene, utvikling av nye indikatorer eller lignende.

10.7 SINTEFs vurdering

SINTEF anbefaler opprettelse av "Olje-ISAC" for bedre informasjonsdeling, samt styrking av KraftCERT som en del av et nasjonalt cybersikkerhetssenter for håndtering av IKT-sikkerhetshendelser innenfor petroleumsnæringen.

IKT-sikkerhetskompetansen i Norge er så begrenset at det ikke er rom for å lage en egen olje-CERT. Ved styrking av KraftCERT kan dette CERT-et være en ressurs for petroleumsnæringen. Det vil også være lettere å styrke et eksisterende fagmiljø enn å starte en ny SRM innenfor IKT-sikkerhet. En Olje-ISAC vil redusere avhengigheten av personlige nettverk for informasjonsdeling, noe som vil være en fordel for de mindre aktørene, og for virksomheter som ikke har bygget opp interne fagmiljø på IKT-sikkerhet.

Det er veldig varierende IKT-kompetanse i næringen i dag og spesielt de små selskapene bør styrke sin kompetanse. Dette kan innebære at bransjen generelt ikke er godt nok forberedt for til dels marginale endringer i fremtidige trusselbilder der næringen kan fremstå som et mål (som illustrert i [1], [2] og [3]). Aktualiteten av dette er ikke opp til oss å vurdere, men vi vil påpeke at slike forhold kan endres raskt. Det samme kan påpekes om forventede sårbarheter knyttet til fremtidig teknologisk konvergens mellom IT og OT. Ptil må vurdere om slike sårbarheter er relevante i dagens situasjon, og om, eventuelt når, bransjen må forberede seg sikkerhetsmessig på slike utviklingstrekk i både trusselbilde og sårbarhetsbilde. SINTEFs anbefaling er å være i forkant av dette.

Vi ser uansett et sterkt behov for at alle aktørene, både oljeselskaper og CERT-aktører, samordner tilnærmingen til IKT-sikkerhet i IT- og OT-systemer siden det i dag er betydelige forskjeller i tekniske løsninger, terminologi og kultur.

Regelverket bør bli tydeligere på hvilke krav som gjelder for IKT-sikkerhet. Dette kan oppnås ved å henvise til konkrete industristandarder, slik tilfellet er hos HSE.

Når det gjelder etatens kunnskapsgrunnlag om IKT-sikkerhet i næringen, bør dette styrkes for å kunne drive tilstrekkelig risikobasert. Dette kan eksempelvis oppnås ved å gjennomføre tilsynsaktivitet som innebærer myndighetsinitierte egenevalueringer. Videre bør det tydeliggjøres, enten i styringsforskriften eller i veiledningen til denne, hvilke IKT-relaterte hendelser som omfattes av plikten til å varsle driftsforstyrrelser.

11 Videre arbeid

Basert på denne studien anbefaler SINTEF at Ptil bidrar til videre arbeid på følgende områder:

- Supplerende studier som utdyper denne rapporten basert på intervjuer med leverandører av industrielle kontrollsystemer, underleverandører og andre aktører i den digitale verdikjeden.
- Studier som vurderer sårbarheten knyttet til fremtidige teknologiske trender, sammen med plausible endringer i trusselbildet
- IT/OT kombinasjonen er kritisk for mange sektorer, ikke bare for petroleumsnæringen. Ptil bør bidra til å bringe dette feltet videre gjennom å utrede hensiktsmessige CERT/ISAC-ordninger basert på anbefalingene i denne rapporten, og tilretteleggelse for systematisk erfaringsdeling om IKT sikkerhet innen IT/OT-kombinasjonen
- CERT o.l. aktiviteter har en betydelig uformell dimensjon, bl.a. avhengighet av tillit som bygges og vedlikeholdes "på siden" av de styringsmessige selskapstrukturene som Ptil ansvarliggjør gjennom sin tilsynsvirksomhet. Det er her en anledning og et behov for å kapitalisere på årelang praksisnær forskning fra HMS/safety. Ptil bør aktivt støtte forskning som belyser sammenhengen mellom praksisfeltet ("work as done") for integrasjon av IT og OT, og standarder, styringsprinsipper og andre uttrykk for "work as imagined".
- Nye ordninger bør støttes av følgeforskning. Nærstudier av ISAC/CERT-aktiviteter basert på aksjonsforskning vil kunne forsterke positive utviklingstrekk. Felles læringshistorier kan danne basis for systematisk trening på tilpasningsevne (resiliens) i kritiske situasjoner.
- Utvikling av et rammeverk for etablering av et mer formelt kunnskapsgrunnlag for gjennomføring av risikobasert IKT-tilsyn.

SINTEF

Referanser

[1] Fireeye. (2017) Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure, https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

[2] Dragos. (2017) Trisis, https://dragos.com/blog/trisis/

[3] Muller, Lilly Pijnenburg, Lars Gjesvik and Karsten Friis. (2018) Cyber-weapons in International Politics; Possible sabotage against the Norwegian Petroleum sector, NUPI report 3/2018, Oslo

[4] Fireeye. https://www.fireeye.com/

[5] ISO/IEC 27035-1 (2016) Information technology -- Security techniques -- Information security incident management -- Part 1: Principles of incident management

[6] IEC 62443 (2010) Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program https://webstore.iec.ch/publication/7030http://www.standard.no/nettbutikk/sokeresultater/?search=62443

[7] ISO/IEC 27001: "Information technology — Security techniques — Information security management systems — Requirements" https://www.iso.org/isoiec-27001-information-security.html

[8] Malware Information Sharing Project (MISP) https://www.misp-project.org

[9] DNV-GL-RP-G108. (2017) Cyber security in the oil and gas industry based on IEC 62443, https://www.dnvgl.com/oilgas/download/dnvgl-rp-g108-cyber-security-in-the-oil-and-gas-industry-based-on-IEC-62443.html

[10] DNV GL-RP-G0496. (2016) Cyber security resilience management for ships and mobile offshore units in operation, https://www.dnvgl.com/maritime/dnvgl-rp-0496-recommended-practice-cyber-security-download.html

[11] Norwegian Oil and Gas RP 104. (2016) 104 – Norwegian Oil and Gas recommended guidelines on information security baseline requirements for process control, safety and support ICT systems. (2016), https://www.norog.no/contentassets/15263fd7f781409286f319bbeb427d93/104-recommended-guidelines-on-security-baseline-requirements.pdf

[12] NIST 800-61 R2. Computer Security Incident Handling Guide, http://dx.doi.org/10.6028/NIST.SP.800-61r2

[13] NIST 800-82 R2. (2015) Guide to Industrial Control Systems (ICS) Security, http://dx.doi.org/10.6028/NIST.SP.800-82r2

[14] NIST. (2018) Framework for Improving Critical Infrastructure Cybersecurity https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[15] ISA-TR84.00.09. (2017) Cybersecurity Related to the Functional Safety Lifecycle, https://www.isa.org/store/isa-tr840009-2017,-cybersecurity-related-to-the-functional-safety-lifecycle/56889051

[16] HSE. Cyber Security for Industrial Automation and Control Systems (IACS), http://www.hse.gov.uk/foi/internalops/og/og-0086.pdf

[17] NSM. (2017) Rammeverk for håndtering av IKT-hendelser, https://nsm.stat.no/publikasjoner/rad-og-anbefalinger/rammeverk-hendelseshandtering/

[18] Norges vassdrags- og energidirektorat. (2017) Regulering av IKT- sikkerhet; rapport nr 26-2017, ISBN 978-82-410-1578-6

[19] Meld. St. 38 (2016–2017) "IKT-sikkerhet — Et felles ansvar", Tilråding fra Justis- og beredskapsdepartementet 9. juni 2017, godkjent i statsråd samme dag. (Regjeringen Solberg) https://www.regjeringen.no/no/dokumenter/meld.-st.-38-20162017/id2555996/

[20] ISA 99 committee, http://isa99.isa.org/ISA99%20Wiki/Home.aspx

[21] Regjeringen (2018) https://www.regjeringen.no/no/aktuelt/bedre-digital-sikring/id2592072/

[22] NSM NorCERT. https://nsm.stat.no/norcert

[23] KraftCERT. https://www.kraftcert.no/

[24] NSM. (2018) Rammeverk for håndtering av IKT-hendelser, https://www.nsm.stat.no/globalassets/dokumenter/vedlegg-til-rammeverk-for-handtering-av-ikt-hendelser/rammeverk-for-handtering-av-ikt-sikkerhetshendelser.pdf
[25] Regjeringen. (2012) Nasjonal strategi for informasjonssikkerhet, https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/nasjonal_strategi_infosikkerhet.pdf
[26] Statoil. https://www.statoil.com/no/how-and-why/health--safety-and-security.html
[27] Gassco. https://www.gassco.no/samfunn-og-sikkerhet/CSIRT/
[28] EU (2016) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN
[29] FIRST. Forum of Incident and Response Team. https://www.first.org/
[30] FIRST Teams. https://www.first.org/members/teams/statoil_csirt
[31] NSM. https://www.nsm.stat.no/
[32] Agenda Utredning & Utvikling (2007). Et helhetlig risikobasert tilsyn. En evaluering av Petroleumstilsynet. Agenda Utredning & Utvikling, Oslo. https://evalueringsportalen.no/evaluering/et-helhetlig-risikobasert-tilsyn-en-evaluering-av-petroleumstilsynet/Evaluering%20av%20Ptil%20-%20Et%20helhetlig%20risikobasert%20tilsyn.pdf/@@inline
[33] Ptil (2018). Kva er tilsyn? http://www.ptil.no/kva-er-tilsyn/category712.html
[34] Nasjonal sikkerhetsmyndighet (2018). Årsrapport 2017. NSM, Oslo. https://www.nsm.stat.no/globalassets/rapporter/arsrapporter/nsm-arsrapport-2017_web_enkeltsider.pdf
[35] Engen, O.A. m.fl. (2017). Helse, arbeidsmiljø og sikkerhet i petroleumsvirksomheten. Rapport fra partssammensatt arbeidsgruppe. Arbeids- og sosialdepartementet, Oslo.
[36] Gressgård, L.J. (2018). Digitalisering i petroleumsnæringen - Utviklingstrender, kunnskap og forslag til tiltak. IRIS, Stavanger.
[37] Arbeids- og sosialdepartementet (2016) Tildelingsbrev 2016 – Petroleumstilsynet. ASD, Oslo.
[38] Arbeids- og sosialdepartementet (2017) Tildelingsbrev 2017 – Petroleumstilsynet. ASD, Oslo.
[39] Arbeids- og sosialdepartementet (2018) Tildelingsbrev 2018 – Petroleumstilsynet. ASD, Oslo.
[40] NOU 2015:13 (2015). Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden. Departementenes sikkerhets- og serviceorganisasjon, Oslo.
[41] NVE (2013). Veiledning til forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften). Norges vassdrags- og energidirektorat, Oslo.
[42] HSE. Cyber Security for Industrial Automation and Control Systems. http://www.hse.gov.uk/foi/internalops/og/og-0086.pdf
[43] Azam, Namrah (2017). Informasjonssikkerhetstilstanden i energiforsyningen. Norges vassdrags- og energidirektorat, Oslo.
[44] NSM (2017). Helhetlig IKT-risikobilde. Nasjonal sikkerhetsmyndighet, Oslo.
[45] ISO 19011: 2011. Retningslinjer for revisjon av styringssystemer. International Organization for Standardization, Geneve.
[46] NVE (2017) Regulering av IKT- sikkerhet; Et helhetlig og fremtidsrettet sikkerhetsregime for forsyningssikkerhet i en digitalisert energisektor, http://publikasjoner.nve.no/rapport/2017/rapport2017_26.pdf

Vedlegg

Standarder, retningslinjer og veiledninger for IKT-sikkerhet (OT) i industrielle kontrollsystemer

Referanse	Tittel	
Standarder		
IEC 62443 series	Industrial Automation and Control Systems Security	The goal in applying the 62443 series is to improve the safety, availability, integrity and confidentiality of components or systems used for industrial automation and control, and to provide criteria for procuring and implementing secure industrial automation and control systems. Conformance with the requirements of the 62443 series is intended to improve electronic security and help identify and address vulnerabilities, reducing the risk of compromising confidential information or causing degradation or failure of the equipment (hardware and software) of processes under control. The content of the series is directed towards those responsible for specifying, designing, developing, implementing, or managing industrial automation and control systems. This information also applies to users, system integrators, security practitioners, and control systems manufacturers and vendors.

Referanse	Tittel	
Retningslinjer		
DNV-GL-RP-G108	Cyber security in the oil and gas industry based on IEC 62443 (2017)	This recommended practice for implementing IEC 62443 (3-2, 3-3 and 2-4) in the oil and gas sector was produced based on a joint industry project (JIP) with participation from industry and Petroleum Safety Authority (PSA) Norway, A common and practical approach on how to secure industrial automation and control systems (IACS) in the oil and gas sector is provided. The recommended practice intends to follow the regulatory requirements defined by PSA for the Norwegian continental shelf and by Health and Safety Executive (HSE) for the UK oil Sector.
DNV GL-RP-G0496	Cyber security resilience management for ships and mobile offshore units in operation (2016)	This recommended practice guides owners, managers and operators of ships and mobile offshore units towards enhanced cyber security of their assets in operation. In addition, this RP is intended to help IT and industrial automation control system professionals to join their efforts towards building and maintaining cyber security resilience of the total set of the assets and processes employed to conduct the company's business. Following a risk based approach, the decisoins of what is critical and high priority is then left at the discretion of the organisation.
Norwegian Oil and Gas RP 104	104 – Norwegian Oil and Gas recommended guidelines on information security baseline requirements for process control, safety and support ICT systems. (2016)	This document contains guidance on how to implement the Norwegian Oil and Gas information security baseline requirements (ISBRs) in process control, safety and support (PCSS) ICT systems. The implementation guidance in this document is considered "good practice" for information security, but the organisation should adapt these proposed solutions in accordance with their own information security policy and regulations, and aligned with their national legislation. Implementing the information security controls and measures exactly as described in this guidance is not mandatory. Other methods and techniques may be used as long as the objectives of the ISBRs are achieved.
NIST 800-61 R2	Computer Security Incident Handling Guide	The publication assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively. This publication provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident. The guidelines can be followed independently of particular hardware platforms, operating systems, protocols, or applications.

Referanse	Tittel	
Retningslinjer		
NIST 800-82 R2	Guide to Industrial Control Systems (ICS) Security (2015)	This document provides guidance on how to secure Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), while addressing their unique performance, reliability, and safety requirements. The document provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks
NIST	Framework for Improving Critical Infrastructure Cybersecurity, 1.1 Draft 2 (2017)	The Framework, created through collaboration between government and the private sector, uses a common language to address and managecybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses.The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The Framework consists of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational Profiles. Through use of the Profiles, the Framework will help the organization align its cybersecurity activities with its business requirements, risk tolerances, and resources.
ISA-TR84.00.09	Cybersecurity Related to the Functional Safety Lifecycle (2017)	This document is intended to address and provide guidance on integrating the cybersecurity lifecycle with the safety lifecycle as they relate to Safety Controls, Alarms, and Interlocks (SCAI), inclusive of Safety Instrumented Systems (SIS). This scope includes the work processes and countermeasures used to reduce the risk involved due to cybersecurity threats to the Industrial Automation and Control System (IACS) network. This scope provides recommendations to ensure SCAI are adequately secured due to the potential for cyber attacks that can act like common mode failures that initiate a hazardous demand and also prevent instrumented protection functions, including the SIS, from performing their intended purpose. The scope is intended to address cybersecurity from both external and internal threats. Although not directly within the scope, enterprise networks, business networks and process information networks (demilitarized zones) that represent a threat vector to the SCAI systems, or contain countermeasures that reduce the risk to the SCAI systems from external cyber threats, are included.

Referanse	Tittel	
Veiledninger myndigheter		
HSE	Cyber Security for Industrial Automation and Control Systems (IACS)	This Operational Guidance represents the Health and Safety Executive (HSE) interpretation of current standards on industrial communication network and system security, and functional safety in so far as they relate to major hazards workplaces. This guidance does not cover protection of critical infrastructure (e.g. utility networks) or protection of information on corporate networks. For the purpose of the enforcement management model, this guidance is an interpretive standard. This Operational Guidance could contribute towards a suitable demonstration of compliance with relevant H&S legislation, in order to demonstrate cyber security risks have been managed to as low as reasonably practicable (ALARP). Alternative equivalent means may also be used to demonstrate compliance.
NSM	Rammeverk for håndtering av IKT-hendelser (2017)	Rammeverket beskriver en systematisk tilnærming til håndtering av IKT-sikkerhetshendelser på tvers av virksomheter og sektorer for å sikre en effektiv nasjonal sektorovergripende håndteringsevne, hvor det enkelte departements konstitusjonelle ansvar også ivaretas. De etablerte beredskapsprinsippene legges til grunn. Rammeverket beskriver også de forutsetningene som må være på plass for at håndtering av IKT-sikkerhetshendelser skal kunne foregå i henhold til rammeverket. Forholdet til andre elementer i en mer omfattende hendelseshåndtering, eksempelvis etterforskning, beskrives i den grad det er nødvendig for helhetsforståelsen. Målet er at den enkelte virksomhet som forvalter kritisk infrastruktur og/eller kritiske samfunnsfunksjoner5 skal utøve sin rolle og sitt ansvar raskt og formålseffektivt som del av en større, koordinert respons for å gjenopprette sikker tilstand for berørte systemer, utføre skadevurdering og begrense følgeskader for andre IKT-systemer. Dette inkluderer informasjonssystemer som håndterer sikkerhetsgradert informasjon. Rammeverket forutsetter at den enkelte virksomhet utarbeider egne detaljerte planer for håndtering av alvorlige IKT-sikkerhetshendelser som henger sammen med øvrig beredskapsplanverk.

Teknologi for et bedre samfunn

www.sintef.no