PETROLEUMSTILSYNET

Revisjonsrapport

Rapport	
Rapporttittel **Statoil sin håndtering av hendelser knyttet til IKT og informasjonssikkerhet, og tilhørende barrierestyring**	Aktivitetsnummer **001000189**

Gradering		
☑ Offentlig (deler er u.off)	☐ Begrenset	☐ Strengt fortrolig
☐ Unntatt offentlighet	☐ Fortrolig	

Involverte	
Hovedgruppe T – 1	Oppgaveleder Asbjørn Ueland
Deltakere i revisjonslaget Jan Henrik Schou Straumsheim (PwC), Svein Anders Eriksson, Tommy Bugge Hansen, Anthoni Larsen og Asbjørn Ueland	Dato 30.01.17

1 Innledning

Petroleumstilsynet (Ptil) har gjennomført tilsynsaktivitet med Statoil sin håndtering av hendelser knyttet til IKT og informasjonssikkerhet. Aktiviteten ble gjennomført i form av møter med Statoil sin organisasjon på Forus 3. november 2016 og 9. desember 2016 samt en dokumentgjennomgang 8. desember 2016.

Tilsynet ble varslet i brev av 31. oktober 2016.

2 Bakgrunn

Ptil har i mange år hatt fokus på næringen sitt arbeid med beskyttelse av datasystemene på anlegg og innretninger som ivaretar styring av prosessene, overvåker mulige gassutslipp eller branntilløp samt foretar sikker nedstengning (sikkerhets- og kontrollsystemer). I oktober 2016 ble det kjent at vedlikeholdsarbeid på en server i produksjonsmiljøet på Mongstad medførte forstyrrelser for den pågående lasteoperasjonen. Statoil gjorde rede for denne hendelsen i et møte hos Ptil 28. oktober og forklarte hvordan arbeid utført av en underleverandør i India førte til denne hendelsen.
Statoil valgte å utkontraktere en del IKT-tjenester i 2012. Dette var en sentral, forretnings-messig beslutning som innebar at drift av IKT-utstyr i deler av teknisk nett ble overført til HCL i India. Utkontraktering medfører endringer i forutsetningene når en skal vurdere trusler og risikobilde for drift av IKT-systemer. I dette tilsynet har vi ikke vurdert Statoils risiko-vurderinger som lå til grunn for omleggingene i 2012.
Da det kom fram at det var flere hendelser som kunne knyttes til arbeid som ble utført av underleverandør i India, valgte Ptil å undersøke Statoil sin beskyttelse av sikkerhets- og kontrollsystemer og hendelseshåndtering knyttet til IKT og informasjonssikkerhet grundigere.

3 Mål

Målsetning med aktiviteten var å verifisere at Statoil har robuste løsninger for barrierestyring innen informasjonssikkerhet for sikkerhets- og kontrollsystemer ved å ha fokus på Statoil sin håndtering av hendelser knyttet til IKT og informasjonssikkerhet. Videre har vi fulgt opp barrierestyring for informasjonssikkerhet for sikkerhets- og kontrollsystemer.

4 Resultat og gjennomføring

Tilsynet ble gjennomført som planlagt og i henhold til vårt varselbrev av 27. oktober 2016. Både i presentasjoner og under påfølgende diskusjoner viste Statoil stor grad av åpenhet.

Det er vårt inntrykk at Statoil har arbeidet systematisk for å styrke fundamentet for informasjonssikkerhet. Dette har resultert i et CSIRT (Computer Security Incident Response Team)-miljø med kontakter både til nasjonale og internasjonale miljøer. Statoil har også utarbeidet interne krav for beskyttelse av sikkerhets- og kontrollsystemer som er basert på anerkjente internasjonale standarder. Denne kunnskapen benyttes i samarbeidsprosjekter i næringen.

Statoil har, med sin store portefølje av plattformer og anlegg, mange ulike løsninger for sikkerhets- og kontrollsystemer som representerer mange generasjoner og leverandører av slike systemer. Beskyttelsen av systemene består av en kombinasjon av lokal løsning for den enkelte installasjon og en sentral løsning. De lokale løsningene for de installasjonene vi har sett på synes å være tilpasset de spesifikke forholdene på de aktuelle installasjonene.

Ptil har i tilsynet gått gjennom oversikter over IKT-hendelser og fått disse beskrevet. Noen av hendelsene avdekket at arbeidsutførelsen ikke var i samsvar med interne prosedyrer. Vi har gjennomgått dokumentasjon for utvalgte hendelser. Videre er gapanalyser av utvalgte anlegg undersøkt. Disse analysene vurderer anlegget/innretningen opp mot siste versjon av Statoil sine tekniske krav til informasjonssikkerhet for industrielle automasjons- og kontrollsystemer.

Vi har ikke identifisert avvik men det er et forbedringspunkt i forhold til varslingsplikt.

5 Observasjoner

Ptils observasjoner deles generelt i to kategorier:

- Avvik: Knyttes til de observasjonene hvor vi mener å påvise brudd på regelverket.
- Forbedringspunkt: Knyttes til observasjoner hvor vi ser mangler, men ikke har nok opplysninger til å kunne påvise brudd på regelverket.

5.1 Forbedringspunkter

5.1.1 Varslingsplikt

Forbedringspunkt:
Det ble ikke sendt melding om hendelse som ifølge Statoil sin dybdestudie potensielt kunne ha medført "svekking/bortfall av sikkerhetsfunksjoner og barrierer".

Begrunnelse:
I mai 2014 ble det utført vedlikeholdsarbeid på en server i produksjonsmiljøet på Mongstad som medførte forstyrrelser for den pågående lasteoperasjonen. I følge Synergi-rapporten er dette arbeidet utført på en måte som ikke er i samsvar med prosedyre for arbeid på automasjonssystemer. Hendelsen førte til at den gjenværende del av lasteoperasjonen måtte gjennomføres med manuell styring i samsvar med allerede etablert prosedyre for dette. Manuell styring innebærer at kvaliteten på leveransen er «off spec», noe som innebærer et begrenset økonomisk tap for Statoil. Den aktuelle serveren påvirker ikke øvrige deler av anlegget på Mongstad og hendelsen påvirker ikke anleggets integritet.

Statoil sin interne dybdestudie påpeker imidlertid at hendelsen potensielt kunne ha medført "Svekking/bortfall av sikkerhetsfunksjoner og barrierer".
U.off, jf offl. § 24, 3.ledd

Sladdet

U.off. slutt
Vi er ikke blitt forelagt dokumentasjon som imøtegår denne vurderingen.

Krav:
Styringsforskriften § 29 – om varsling og melding til tilsynsmyndighetene av fare- og ulykkessituasjoner

6 Andre kommentarer

Rapportering i Synergi

Statoil benytter Synergi for oppfølging av hendelser. Storparten av hendelsene som blir registrert har ikke en kritikalitet som innebærer at de omfattes av styringsforskriftens § 29 om varsling og melding.

Som del av tilsynet fikk vi en oversikt over vesentlige IKT-hendelser som var registrert. En del av disse ble gjennomgått og vi undersøkte også dokumentasjonen til de sakene vi mente var av alvorlig karakter. Hendelsen på Mongstad er omtalt ovenfor. De andre forholdene som vi har undersøkt er vurdert til å være av mindre alvorlig karakter.

Tekniske krav og risikoanalyse

Statoil sine tekniske krav til de industrielle automasjons- og kontrollsystemer baserer seg på IEC 62443 og National Institute of Standards and Technology's Cyber Security Framework (NIST CSF). For at rammeverket for risikovurdering skal fungere hensiktsmessig er det en forutsetning at alle funksjonene (Identify – Protect – Detect – Respond – Recover) med underliggende kategorier adresseres.

Statoil har gjennomført gap-analyser av de enkelte anlegg og innretninger opp mot gjeldende krav. Vi ba om å få se tre av disse; et anlegg/innretning som har få avvik, en innretning bygget omkring år 2000 samt et anlegg/innretning som har omfattende avvik. Gapanalysene henviser flere steder til selskapets overordnede risikovurderingsprosess for sikkerhetsrisiko. I møte med Statoil fremkom det at dette er en vurdering på selskapsnivå. Det kom ikke fram at det var gjort risikovurderinger i forhold til mulige anleggsspesifikke trusler. En fullgod risikovurdering bør inkludere anleggsspesifikke trusler for å være mest mulig relevant.

U.off, jf offl. § 24, 3.ledd

Sladdet

U.off. slutt

Arbeid på automasjonssystemer, tillatelser og fjerntilgang

Styrende dokumenter regulerer arbeid på automasjonssystemer. Dokumentene omfatter bl.a. beskrivelse av modifikasjon, utarbeidelse av endringsunderlag, arbeidstillatelse og

fjerntilgang. Ved bruk av tilgangskontrolløsningen Access@Plant sikrer Statoil at arbeidsprosessene blir fulgt.

I dokumentet for tidsbegrenset fjerntilgang via Access@Plant er det beskrevet at "*det er et grunnprinsipp at ansvarlig personell på anlegget skal være komfortabel med at arbeids-operasjonen utføres som fjernarbeid, og regulere om og når det skal åpnes for arbeidet*". Det framkommer av Synergirapporter at ansvarlig personell på anlegg / innretning opplever at arbeid blir gjennomført med fjerntilgang uten at de ansvarlige er komfortable.

Videre er det noe arbeid som blir gjennomført med fjerntilgang uten bruk av tilgangs-kontrolløsningen Access@Plant. Dette skyldes tekniske begrensninger i det aktuelle utstyret. Gjennomgangen av hendelser viste at arbeidsutførelsen noen ganger ikke har vært gjort i samsvar med Statoil sine styrende dokumenter. Statoil har erkjent denne problemstillingen og arbeider med å finne løsninger på dette. Statoil opplyste videre at det på tidspunktet for tilsynet var innført vesentlige begrensninger i antallet personer som har tilgang til å utføre arbeid med fjerntilgang som ikke er tilgangskontrollert gjennom Access@Plant.

7 Deltagere fra Petroleumstilsynet

Jan Henrik Schou Straumsheim	PwC
Svein Anders Eriksson	F-Logistikk & Beredskap (1. møte)
Tommy Bugge Hansen	F-Logistikk & Beredskap
Anthoni Larsen	F-Logistikk & Beredskap (1. møte)
Asbjørn Ueland	F-Prosessintegritet (oppgaveleder)

8 Dokumenter

Følgende dokumenter ble benyttet under planlegging og gjennomføringen av aktiviteten:

U.off, jf offl. § 24, 3.ledd

Sladdet

Sladdet

U.off. slutt

Vedlegg A

Møtedeltakere.