PETROLEUMSTILSYNET

Tilsynsrapport

Rapport	
Rapporttittel **Rapport etter tilsyn med styring av risiko knyttet til informasjonssikkerhet for de industrielle IKT-systemene**	Aktivitetsnummer 001904022

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

Involverte	
Hovedgruppe T-L	Oppgaveleder Asbjørn Ueland
Deltakere i revisjonslaget Asbjørn Ueland og Espen Seljemo	Dato 5.2.2019

1 Innledning

Vi førte tilsyn med styring av risiko knyttet til informasjonssikkerhet for de industrielle IKT-systemene den 10 og 11.12.2018 hos Equinor Tjeldbergodden.

Dette var en videreføring av en tilsynsserie rettet mot IKT-sikkerhet fra 2017 som den gang var rettet mot informasjonssikkerhet for de industrielle IKT-systemene på selskapsnivå.

Tilsynet var godt lagt til rette med presentasjoner, samtaler, dokumenter og gjennomgang av utvalgte systemer.

2 Bakgrunn

De industrielle IKT-systemene beskyttes gjennom tiltak som også beskytter kontornettverkene. I tillegg er det barrierer og funksjoner som gir aktiv og passiv beskyttelse av disse systemene. Disse funksjonene, når de er intakt, robustgjør sikkerheten og minimerer risiko for sårbarheter som kan påvirke de industrielle IKT-systemene fra utsiden, både utilsiktede og tilsiktede handlinger. Noen av disse funksjonene driftes sentralt av selskapet. Drift og vedlikehold av de industrielle IKT-systemene og tilhørende nettverksutstyr gjøres i hovedsak lokalt på anlegget i tett samarbeid med driftsorganisasjonen.

Tilsynet ble gjennomført med presentasjoner, samtaler med relevant personell, gjennomgang av dokumenter og inspeksjon av de industrielle IKT-systemene i kontrollrom samt tilhørende utstyrsrom.

3 Mål

Målet med tilsynet var å se på hvordan den lokale driftsorganisasjonen fulgte opp de industrielle IKT-systemene med tilhørende nettverksutstyr og enheter for å sikre ytterligere beskyttelse og robustgjøring. Vi ønsket å få en oversikt over prosesser og systemer som benyttes for å sikre oppfølgingen av de industrielle IKT-systemene og hvordan dette gjennomføres og følges opp av de ansvarlige.

4 Resultat

Vi har sett på oppbygning av de industrielle IKT-systemene og hvordan disse er segregert og strukturert nettverksmessig. Det ble sett på koblinger mellom de ulike systemene, både logiske koblinger i form av brannmursregler og fysiske koblinger mellom systemer og nivåer i topologi.

Vedlikehold og oppfølging i drift av de industrielle IKT-systemene ble verifisert ved samtaler og gjennomgang av dokumentasjon for de ulike systemene. Vi etterspurte oversikt over hvilket utstyr og tilhørende enheter som inngikk i disse systemene og hvilke rutiner selskapet hadde for oppfølging av sårbarhetsvarsler og rutiner for sårbarhetsoppdatering av de industrielle IKT- systemene. Dette er viktige funksjoner å vedlikeholde for å robustgjøre systemer til å motstå tilsiktede og utilsiktede handlinger.

Videre ble det etterspurt hvordan de industrielle IKT- systemene ble fulgt opp av selskapet eller i form av serviceavtaler mot underleverandører. Backup- og disaster recovery prosedyre samt verifisering og testing av disse funksjonene ble også etterspurt i tilsynet.

Det ble sett på selskapets interne avvik og DISPer for de industrielle IKT-systemene. Vi la vekt på hvilke svekkelser og sårbarheter som kunne føre til manglende robusthet og hvilke vurderinger som var lagt til grunn.

Det ble gjort verifiseringer i forhold til styringsforskriftens krav om risikoreduksjon og om interne krav (§§ 4 og 8) samt krav i teknisk og operasjonell forskrift til industrielle IKT-systemer, om trening og øvelser og om vedlikehold (§§ 33a, 52 og 58). Videre så vi på hvordan gapanalysen for de industrielle IKT-systemene mot selskapskravene i TR1658 versjon 5 har blitt fulgt opp.

Vi hadde verifikasjon i felt på en elektrosubstasjon hvor arbeidsstasjon for å monitorere det elektriske anlegg med tilhørende utstyr var installert. Videre hadde vi verifikasjon i det sentrale tekniske rommet for å se på de fysiske installasjonene og segregering av komponenter for de industrielle IKT-systemene, blant annet servere, noder og tilhørende nettverksutstyr.

Under tilsynet hadde vi verifikasjon av rutiner for brukerkonto og passordregime som ble benyttet for de industrielle IKT-systemene. Regelmessig endring av passord skal hindre uvedkommende å få adgang til systemer og enheter på system og enheter. Brukerkonto og passordregime ivaretar sikkerheten ved at det identifiserer brukeren som er pålogget og begrenser tilgang i henhold til planlagt aktivitet. Videre undersøkte vi hvor beskrivelser og dokumentasjon for oppbygning av de industrielle IKT-systemene ble lagret og hvem som hadde tilgang til dokumentområdet.

Vi etterspurte om monitorering av datatrafikk foregikk for å avdekke unormal aktivitet i og mellom systemene ble utført. Videre etterspurt vi hvordan løsningen for tilgangskontroll Access@plant ble benyttet for fjerntilkobling mot de industrielle IKT-systemene og hvilke prosedyrer som ble benyttet ved godkjenning og verifikasjon av tilgangskontroll.

Det ble også etterspurt om selskapet hadde planlagt og utført trening og øvelse på hendelser i de industrielle IKT-systemene.

U.off jf offl. § 24, 3. ledd

[redacted]

U.off slutt

5 Observasjoner

Vi har to hovedkategorier av observasjoner:

- *Avvik*: Observasjoner der vi *påviser* brudd på/manglende oppfylling av regelverket.
- *Forbedringspunkt*: Observasjoner der vi *mener å se* brudd på/manglende oppfylling av regelverket, men ikke har nok opplysninger til å kunne påvise det.

U.off jf offl. § 24, 3. ledd

[redacted]

[redacted]

[redacted]

U.off slutt

7 Deltakere fra oss

Asbjørn Ueland	fagområde prosessintegritet	(oppgaveleder)
Espen Seljemo	fagområde prosessintegritet	

8 Dokumenter

Følgende dokumenter ble benyttet under planleggingen og utføringen av tilsynet:

U.off jf offl. § 24, 3. ledd

[redacted]

U.off slutt

Vedlegg A Oversikt over intervjuet personell