PETROLEUMSTILSYNET

Tilsynsrapport

Rapport	
Rapporttittel **Rapport etter tilsyn med styring av risiko knyttet til informasjonssikkerhet for de industrielle IKT systemene Eldfisk S**	Aktivitetsnummer 009018541

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

Involverte	
Hovedgruppe T-2	Oppgaveleder Asbjørn Ueland
Deltakere i revisjonslaget Espen Seljemo og Asbjørn Ueland	Dato 2.4.2019

1 Innledning

Vi førte tilsyn med styring av risiko knyttet til informasjonssikkerhet for de industrielle IKT-systemene i perioden 4. til 7. februar 2019 hos ConocoPhillips Skandinavia AS og på innretningen Eldfisk S.

Dette var en videreføring av tidligere tilsynsserier innen IKT-sikkerhet som var rettet mot de industrielle IKT-systemene. Disse tilsynsseriene omfattet alle aktørene med petroleumsaktivitet på norsk sokkel.

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

2 Bakgrunn

De industrielle IKT-systemene hos operatørene på norsk sokkel beskyttes gjennom tiltak som også beskytter kontornettverkene. I tillegg er det barrierer og funksjoner som gir aktiv og passiv beskyttelse av de industrielle systemene. Disse funksjonene, når de er intakt, robustgjør sikkerheten og minimerer risiko for at sårbarheter i de industrielle IKT-systemene kan utnyttes fra utsiden, både utilsiktede og tilsiktede handlinger. Noen av disse funksjonene driftes sentralt av selskapene. Øvrige funksjoner for drift og vedlikehold av de industrielle IKT-systemene og tilhørende nettverksutstyr gjøres i hovedsak lokalt på innretningen i tett samarbeid med driftsorganisasjonene.

Tilsynet ble gjennomført med presentasjoner, samtaler med relevant personell, gjennomgang av dokumenter og verifikasjon av de industrielle IKT-systemer.

3 Mål

Målet med tilsynet var å verifisere hvordan selskapet følger opp styring av risiko knyttet til informasjonssikkerhet for de industrielle IKT-systemene som har grensesnitt mot

kontorsystemene. Videre å verifisere prosesser og systemer hos operatøren som benyttes for å sikre oppfølgingen av disse systemene og hvordan dette gjennomføres på hver enkelt enhet. Videre verifiserte vi om det er samsvar mellom overordnede prosedyrer og oppfølgingen av systemene på innretningen.

4 Resultat

Vi har sett på oppbygning av de industrielle IKT-systemene og hvordan disse er segregert og strukturert nettverksmessig. Det ble gjort verifikasjoner av knytninger mellom de ulike systemene og til kontorsystemene, 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. Det ble gjort verifikasjoner på ulike verktøy i systemene for å verifisere at prosedyrer ble fulgt av relevant personell hos selskapet.

Videre ble det etterspurt hvordan de industrielle IKT-systemene ble fulgt opp, enten internt av selskapet eller i form av serviceavtaler med leverandører. Det ble spesifikt etterspurt hvordan sikkerhet- og kontrollsystem, samt elektro- og målesystemer ble fulgt opp av den ansvarlige.

Vi etterspurte oversikt over hvilket utstyr og tilhørende enheter som inngikk i de industrielle IKT-systemer og hvilke rutiner selskapet hadde for oppfølging av sårbarhetsvarsler samt rutiner for sårbarhetsoppdatering. Dette er viktige funksjoner å vedlikeholde for å ivareta integritet i disse systemene til å kunne motstå tilsiktede og utilsiktede handlinger.

Det ble etterspurt prosedyrer, samt verifisering av funksjonene som ivaretar backup- og disaster recovery av de industrielle IKT-systemene. Det ble utført verifikasjoner i felt i ulike utstyrsrom, kontrollrom samt områder hvor arbeidsstasjoner som var benyttet til de industrielle IKT-systemene var plassert. Vi undersøkte hvordan de industrielle IKT-systemene var beskyttet med passive tiltak, bl. a. i form av rutiner for låsing av rom og blokkering av kommunikasjonsporter. Vi har verifisert prosedyre og funksjon for å ivareta fjerntilkobling og pålogging mot de industrielle IKT-systemer.

Vi har undersøkt rutiner for monitorering av trafikk og oppfølging av logger for systemer og enheter i nettverkene for de industrielle IKT-systemene. Dette omfatter både sikkerhet- og kontrollsystemer, nettverkskomponenter, elektroutstyr og fiskale målesystemer.

Trening og øvelser er sentrale elementer i håndtering av hendelser. Vi verifiserte hvordan hendelser i de industrielle IKT-systemene skulle håndteres og hvordan driftsorganisasjonen lokalt og i selskapet sentralt skulle involveres i håndteringen av hendelser. Vi verifiserte bruk og innhold av kompetanseverktøyet som benyttes til å ha oversikt over kompetanse hos utøvende fagpersonell.

Vi gjennomgikk selskapets rapport og funn etter selskapsrevisjon som var utført i 2018.

U.off jf offl. § 24, 3. ledd – start

[redacted]

[redacted]

[redacted]

U.off slutt

6 Deltakere fra oss

Asbjørn Ueland fagområde prosessintegritet (oppgaveleder)
Espen Seljemo fagområde prosessintegritet

7 Dokumenter

Følgende dokumenter ble benyttet under planleggingen og utføringen av tilsynet:

U.off jf offl. § 24, 3. ledd – start

[redacted]

U.off slutt

Vedlegg A Oversikt over intervjuet personell