PETROLEUMSTILSYNET

Tilsynsrapport

Rapport	
Rapporttittel **Tilsynsrapport - styring av risiko knyttet til informasjonssikkerhet for de industrielle IKT-systemene Valhall PH**	Aktivitetsnummer 054006028

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

Involverte	
Hovedgruppe T-3	Oppgaveleder Asbjørn Ueland
Deltakere i revisjonslaget Espen Seljemo og Asbjørn Ueland	Dato 18.6.2019

1 Innledning

Vi førte tilsyn med styring av risiko knyttet til informasjonssikkerhet for de industrielle IKT-systemene i perioden 11. til 14. og 27 mars 2019 hos Aker BP og Valhall PH.

Dette var en videreføring av tidligere tilsynsserie innen IKT-sikkerhet som var rettet mot de industrielle IKT-systemene. Tilsynet var godt lagt til rette med presentasjoner, samtaler, dokumenter og gjennomgang på utvalgte systemer.

2 Bakgrunn

De industrielle IKT-systemene beskyttes gjennom tiltak som også beskytter kontor-nettverkene. 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 selskapet. Øvrige funksjoner for drift og vedlikehold av de industrielle IKT-systemene og tilhørende nettverksutstyr gjøres i hovedsak lokalt på innretningen i tett samarbeid med driftsorganisasjonen.

Tilsynet ble gjennomført med presentasjoner, samtaler med relevant personell, gjennomgang av dokumenter og inspeksjon 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. Hensikten med tilsynet er å verifisere prosesser og systemer hos operatøren som benyttes for å sikre oppfølgingen av disse systemene og hvordan dette gjennomføres på hver enkelt enhet. Verifisere 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. Det sett på koblinger mellom ulike kontrollsystem for boring, elektro og strøm fra land, samt målesystemer og telekommunikasjonssystemer.

Vi verifiserte deres filosofi og styrende dokumentasjon for IKT-sikkerhet av de industrielle IKT-systemene og prosedyrer for disse systemene på Valhall innretningene.

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 gjorde vi verifikasjoner i felt, strøm fra land moduler og tilhørende utstyrsrom. Vi hadde verifikasjon og samtale med kontrollrom samt andre områder på Valhall hvor arbeidsstasjoner som var benyttet til de industrielle IKT-systemene var plassert.

Videre ble det etterspurt hvordan de industrielle IKT-systemene ble fulgt opp, både internt av selskapet og i form av serviceavtaler med leverandører. Det ble spesifikt etterspurt hvordan sikkerhet- og kontrollsystem, boresystemer, elektro, strøm fra land, telekommunikasjon 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. Utstyrsoversikt er nødvendig for å ivareta integritet i disse systemene slik at nødvendige sårbarhetsoppdateringer kan implementeres for å motstå tilsiktede og utilsiktede handlinger.
Det ble etterspurt prosedyrer for og verifisering av funksjonene som ivaretar backup- og disaster recovery av de industrielle IKT-systemene, samt om personellet kjente til disse prosedyrene og hadde trening i disse oppgavene.

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 ubrukte 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 datatrafikk og oppfølging av hendelseslogger for systemer og enheter i alle nettverkene for industrielle IKT-systemer.

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. Trening og øvelser er vesentlige tiltak for å forberede organisasjonen til å håndtere hendelser. Vi verifiserte om selskapet hadde kompetansematrise for utførende personell som jobbet med de industrielle IKT-systemer.

Vi verifiserte påloggingskonter med tilhørende adgangsnivå som ble benyttet ved driftsoppgaver og ved endringer. Det ble etterspurt hvilke rutiner som ble benyttet for vedlikehold av brukerkonto og passordregime.

Vi verifiserte prosedyrer og system for bruk av USB-enheter samt annen programvare som ble benyttet til filoverføring til industrielle IKT-systemer.

4.1 Generelt

U.off jf offl. § 24, 3. ledd

[redacted]

[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