Øvelsesplanlegger

Pakke 2 øving 2

«Innsider har gjort endringer»

Utgave 0.8 05.12.2024

Innholdsfortegnelse

1 Innledning

1.1 Bakgrunn og formål

Anlegg og installasjoner i petroleumssektoren skal ha beredskapsplaner for håndtering av uønskede hendelser. Næringen har scenarioer som kan knyttes til IKT-hendelser men Havindustritilsynet (Havtil) har i tilsyn sett at det knapt trenes innen IKT-sikkerhet for de industrielle kontroll- og sikkerhetssystemene. Derfor har Havtil fått utarbeidet et sett med trenings- og øvelsesscenarioer. Dette øvelses-opplegget ble utarbeidet av Proactima med Netsecurity som partner. Opplegget er videre bearbeidet av Havtil.

Aktivitetsforskriften § 23 beskriver at «det utføres nødvendig trening og nødvendige øvelser, slik at personellet til enhver tid er i stand til å håndtere operasjonelle forstyrrelser og fare- og ulykkessituasjoner på en effektiv måte». Samme formulering finnes også i teknisk og operasjonell forskrift § 52. Det er altså samme krav til trening og øvelser for anleggene på land som det er til innretningene på sokkelen.

Når vi trener, øker vi personlige ferdigheter og kunnskaper. Øvelser tester samhandling og beredskapsevne, avdekker styrker og svakheter, samt forbereder ledelsen på å håndtere ulike kriser.

1.2 Oppbygging av veilederen

Øvelsesplanleggeren inneholder ulike scenarioer, og det er foreslått hvilke funksjoner som er aktuelle å inkludere i øvelsen. Scenarioene kan benyttes som trening, table top eller spilløvelse.

Veilederen har i del 3 ekstra informasjon til forberedelse og gjennomføring så som:

- et mulig hendelsesforløp i forkant av startpunkt
- sekvensskjema for hendelsen
- relevant fagstoff

2 Scenario

Scenariet for denne veilederen starter ved at det er gjort endringer i kontrollsystemene som har ført til at produksjonen blir delvis nedstengt uten at nedstengningen kan forklares ut fra prosessbetingelsene eller feilsituasjoner på utstyret.

2.1 Oversikt

Øvelsen kan gjerne deles opp i forhold til tilgjengelig tid. Tabellen indikerer hvilke funksjoner/avdelinger som er aktuelle å trene ved bruk av disse scenarioene.

Tabell 1 - Oversikt over hvem som kan trenes/øves i de ulike modulene

Oppgave	Tittel	SAS/IACS-ansvarlig	Lokal driftsledelse	System-ansvarlig drift
2.2	Innledende forhold – Utstyr stoppes	x	x	x
2.3	Eskalering – Ubevisst endring	x	x	
2.4	Villet endring		x	

2.2 Innledende forhold – Utstyr stoppes

Som følge av planmessig veksling mellom utstyrsenheter (eks. duty standby system), startes standby systemet. Etter noe tid stenger systemet ned av ukjent årsak og produksjonen blir påvirket.

2.2.1 Veiledende spørsmål

SAS/IACS-ansvarlig

- Hvordan kartlegge hva som har skjedd?
- Hvorfor skjedde det?
    - Hva kan leses i event-loggen for kontrollsystemet?
    - Hvordan finner man ut hva som forårsaket det?
- Hvilken informasjon finnes i hand-over fra forrige skift?
- Hvordan går man fram for å gjenopprette systemene?

Lokal driftsledelse

- Hvordan kartlegger man hva som har skjedd?
- Hvorfor skjedde det?
    - Hvilke systemer er påvirket av utstyrsstansen?
- Ble sikkerheten til utstyr og de ansatte påvirket?
- Hvor lang nedetid eller forsinkelser kan en forvente?

Systemansvarlig drift

- Hvordan bistå SAS/IACS-ansvarlig og lokal driftsledelse?

2.3 Eskalering – Ubevisst endring

Det avdekkes at det ble gjort en endring i logikken på forrige skift. Endringen blir tilbakestilt og normal produksjon gjenopprettes.

Kari Normann, som jobber på forrige skift, bekrefter å ha utført en kontroll på deler av kontrollsystemet, basert på detaljerte prosedyrer. Hun forteller at hun fulgte instruksene etter beste evne.

2.3.1 Veiledende spørsmål

Lokal driftsledelse / SAS/IACS-ansvarlig / Systemansvarlig drift

- Hva er bedriftens rutiner for arbeid på kontrollsystemet?
- Er det klart for alle hvem som har tillatelse til å utføre endringer i kontrollsystemet?
- Hvem skal involveres når ansatte har brutt rutinene?

2.4 Villet endring

Det viser seg at Kari ikke bare har utført den planlagte aktiviteten, men også med vilje har utført endringene som førte til at utstyrsenheten stoppet.

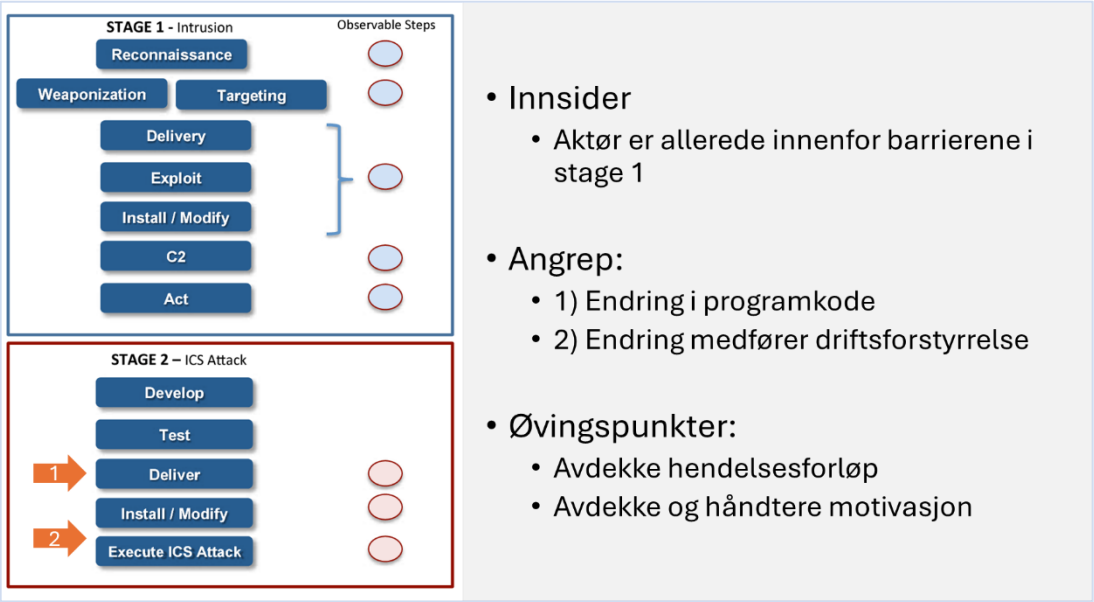
2.4.1 Veiledende spørsmål

Lokal driftsledelse / Systemansvarlig drift

- Hvordan håndteres denne situasjonen?
- Hvem skal involveres?
- Hvordan kan vi forebygge slike hendelser?

3 Ekstra informasjon til forberedelse og gjennomføring

Dette kapittelet inneholder bakgrunns-informasjon om målrettet cyberangrep mot industrielle IKT-systemer. Digitale angrep følger ofte faste mønster, på engelsk kalt kill chain. Figuren viser hvilke steg som er med i denne øvelsen og hvilke øvingspunkter som er innarbeidet i veilederen.



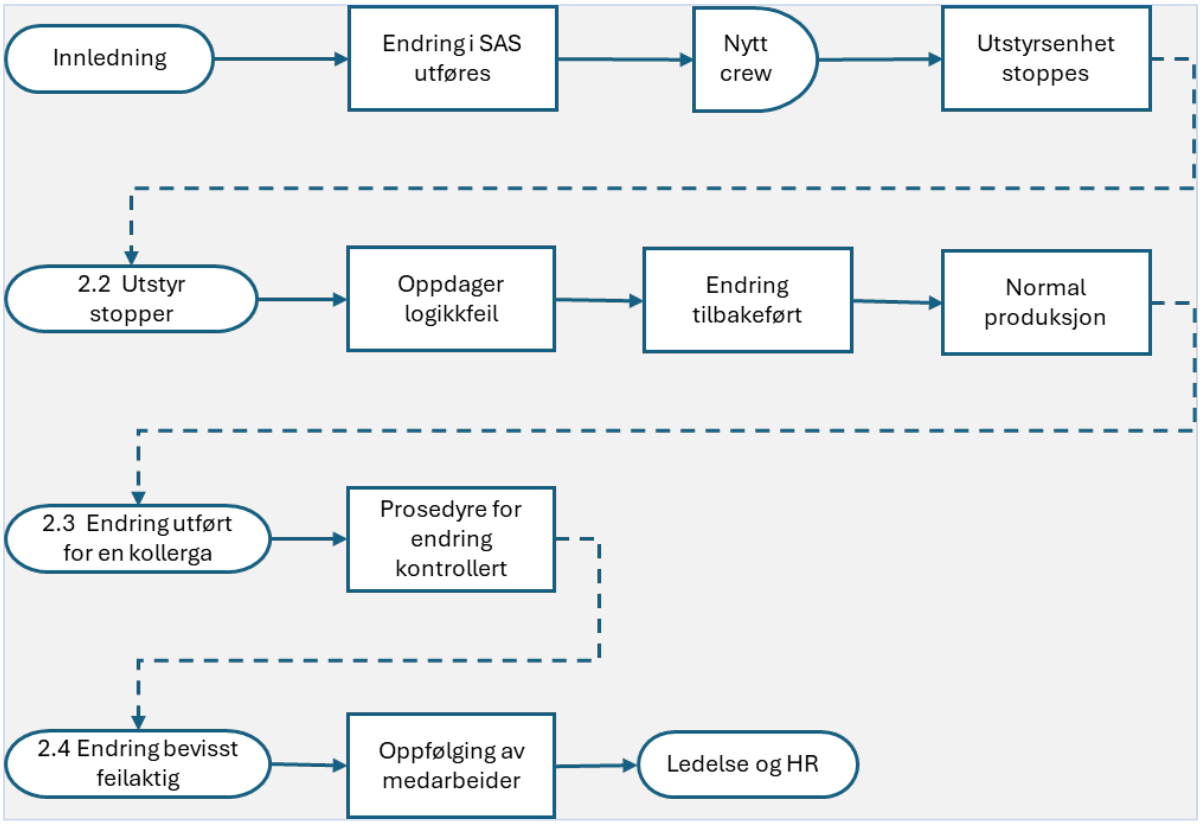
3.1 Innledning til hendelse

Hendelsesforløpet tar utgangspunkt i at en medarbeider med lovlig tilgang til kontrollsystemene gjør en endring som ved et senere tidspunkt fører til at produksjonen forstyrres som følge av at en utstyrsenhet stanses.

Øvingen diskuterer ikke hvorfor denne medarbeideren velger å gjøre en slik handling. Slike forhold diskuteres i rapporten som er vist til i kap. 3.4.

3.2 Hendelse

I utarbeidelsen av øvingen er det tatt utgangspunkt i følgende forløp:



3.3 Læring

Gjennomgang av rutiner, avklaring av ansvarsforhold og forbedring av systemer.

Øvingsledelse

- Hvordan involveres deltakerne i sluttrapporten fra øvelsen?

SAS/IACS-ansvarlig

- Hvordan støtter definerte rutiner rutinesjekk og endringer i kontrollsystemene?
- Hvilke rettigheter har de ansatte til å arbeide på kontrollsystemene?
- Hva kan gjøres for å forhindre at bevisste feilhandlinger skjer igjen?

Lokal driftsledelse

- Hvordan sikres at nøkkelpersonell blir godt nok ivaretatt?
- Hvordan er rutinene for håndtering av handlingene som framkommer i denne øvelsen?

Systemansvarlig drift

- Hvordan sikres at nøkkelpersonell blir godt nok ivaretatt?
- Hvordan er rutinene for håndtering av handlingene som framkommer i denne øvelsen?

3.4 Aktuell litteratur

Bruk av innsider er en angrepsteknikk som benyttes av ulike trusselaktører. Mitre skriver på sine nettsider at «This technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls. Efforts should focus on minimizing the amount and sensitivity of data available to external parties.»

Havindustritilsynet fikk i 2019 gjennomført et prosjekt for å styrke kunnskapen om håndtering av innsiderisiko. Rapporten er tilgjengelig på nettsidene til Havtil.