Øvelsesplanlegger

Pakke 2 øving 1

«*Aktør har tilgang i nettverket*»

Versjon 0.8

05.12.2024

Innholdsfortegnelse

1 INNLEDNING 3

1.1 BAKGRUNN OG FORMÅL 3
1.2 OPPBYGGING AV VEILEDEREN 3

2 SCENARIO 4

2.1 OVERSIKT SCENARIOER 4
2.2 INNLEDENDE FORHOLD – SKR-OPERATØR MISTER SKRIVETILGANG TIL NOEN SETTPUNKTER 5
2.2.1 Veiledende spørsmål 5
2.3 ESKALERING – AKTIVITET PÅ SOVENDE REGEL I OT-BRANNMUR 6
2.3.1 Veiledende spørsmål 6
2.3.2 Oppfølgingspunkter, avhengig av utfall på diskusjon og beslutninger 6
2.4 ANALYSE 7
2.4.1 Veiledende spørsmål 7
2.5 GJENOPPRETTING 8
2.5.1 Veiledende spørsmål 8
2.5.2 Oppfølgingspunkter, avhengig av utfall på diskusjon og beslutninger 8

3 EKSTRA INFORMASJON TIL FORBEREDELSE OG GJENNOMFØRING 9

3.1 INNLEDNING TIL HENDELSE 9
3.2 HENDELSE 9
3.3 LÆRING 10
3.3.1 Veiledende spørsmål 10
3.4 AKTUELL LITTERATUR 10

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 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 er at kontrollromsoperatørene mister enkelte operasjonelle rettigheter i de industrielle kontrollsystemene.

2.1 Oversikt scenarioer

Denne øvelsen starter ved at en kontrollromsoperatør oppdager at det ikke lenger er mulig å endre settpunkt på enkelte regulatorer. SAS/IACS-ansvarlig tilbakestiller rettighetene for kontrollromsoperatørene, men tre uker senere mister kontrollromsoperatørene igjen muligheten til å endre settpunkter.

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. For å nedskalere omfanget av øvelsen kan det være aktuelt å spille de rollene som ikke er IKT-faglige.

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

Oppgave	Tittel	SAS/IACS-ansvarlig	Lokal driftsledelse	System-ansvarlig drift	IKT-avdeling
2.2	Innledende forhold – Tap av skrivetilgang	x	x	x	x
2.3	Eskalering – bruk av passiv brannmurregel	x	x	x	x
2.4	Analyse	x		x	x
2.5	Gjenoppretting			x	x

2.2 Innledende forhold – SKR-operatør mister skrivetilgang til noen settpunkter

Aktøren endrer tillatelser for SKR-operatøren slik at det ikke lenger er mulig å endre enkelte settpunkter. SAS/IACS-ansvarlig tilbakestiller rettighetene for kontrollromsoperatørene, men noen dager senere mister kontrollromsoperatørene igjen muligheten til å endre settpunkter.

2.2.1 Veiledende spørsmål

SAS/IACS-ansvarlig

- Hvordan går en frem for å finne ut hva som har skjedd?
  - Hvorfor har SKR-operatør mistet skrivetilgang?
  - Hvordan kan systemleverandør bistå?
- Hvem kontaktes/varsles?
- Hvordan får man oversikt over omfanget av situasjonen?
  - Hvilke systemer er påvirket?
  - Hvilke settpunkter er påvirket?
- Hvordan kan situasjonen eskalere?
- Kan man fortsette produksjon med de uregelmessighetene som er oppdaget?
- Hva må gjøres for å sikre installasjonen?

Lokal driftsledelse

- Hvordan blir driftsledelsen varslet om hendelsen?
- Hvordan får man oversikt over omfanget av situasjonen?
  - Hvilke systemer er påvirket?
  - Hvilke settpunkter er påvirket?
- Hvordan kan situasjonen eskalere?
- Kan man fortsette produksjon med de uregelmessighetene som er oppdaget?
- Hvordan varsle om hendelsen?
- Mobiliseres beredskapsledelse?

Systemansvarlig drift/IKT-avdeling

- Hvordan vil systemansvarlig drift og IKT avdelingen kunne bistå i denne situasjonen?
- Hvordan går en frem for å finne ut hva som har skjedd?
  - Hvorfor har SKR-operatør mistet skrivetilgang?
  - Hvordan kan systemleverandør bistå?
- Hvordan får man oversikt over omfanget av situasjonen?
  - Hvilke systemer er påvirket?
  - Hvilke settpunkter er påvirket?
- Hvordan kan situasjonen eskalere?
- Hvem må kontaktes/varsles?

2.3 Eskalering – aktivitet på sovende regel i OT-brannmur

Loggen for brannmuren til de industrielle nettverkene inspiseres. Det oppdages bruk av en regel som ikke har vært brukt på lenge.

2.3.1 Veiledende spørsmål

Systemansvarlig drift/IKT-avdeling

- Når ble regelsettet sist gjennomgått og hvordan ble det kvalitetssikret?
- Hvordan går en frem for å finne ut hva regelen innebærer?
    - Kan det være sammenheng mellom regelendring og tapet av skrivetilgang?
    - Hva framgår av logger?
- Hvordan får man oversikt over omfanget av situasjonen?
    - Hvilke systemer er påvirket?
- Hvordan varsle om hendelsen?
    - Ledelse?
    - Organisasjonen?
    - CERT/SRM?

SAS/IACS-ansvarlig / Lokal driftsledelse

- Hvordan blir driftsledelsen informert om eskaleringen?
- Hvilke vurderinger gjøres i forhold til om produksjon kan?
    - Hvordan kontrollere om sikkerhetssystemene er påvirket?
- Hvilke beredskapsmessige tiltak er aktuelle?

2.3.2 Oppfølgingspunkter, avhengig av utfall på diskusjon og beslutninger

- Hvordan kan ekstern kompetanse involveres i undersøkelsen av situasjonen?
- Skal regelen fjernes eller skal den overvåkes?
    - Hvilke vurderinger gjøres?

2.4 Analyse

Undersøkelsesarbeidet med brannmurregelen avdekkes at en aktør har hatt adgang til OT og loggene viser at det har vært trafikk til flere servere i nettverket. Regelen blir fjernet og denne tilgangen til OT blir blokkert.

2.4.1 Veiledende spørsmål

Systemansvarlig drift /IKT-avdeling

- Hvem har ansvar i en slik situasjon?
- Hva bør gjøres med servere på nettverket?
    - Er det installert skadevare?
    - Hvordan kontrollere og sjekke ut serverene?
- Kan enheter i kontrollnettverket være påvirket?
- Hvordan informere?
    - Ledelse?
    - Organisasjonen?

SAS/IACS-ansvarlig

- Hvordan kan SAS/IACS-ansvarlig bistå i undersøkelsene?
- Hvordan informere lokal driftsledelse?
    - Hvordan kan påliteligheten til systemene kontrolleres?

2.5 Gjenoppretting

Analysen har avdekket en av serverne kan ha blitt modifisert.

2.5.1 Veiledende spørsmål

Systemansvarlig drift land/ IKT avdeling

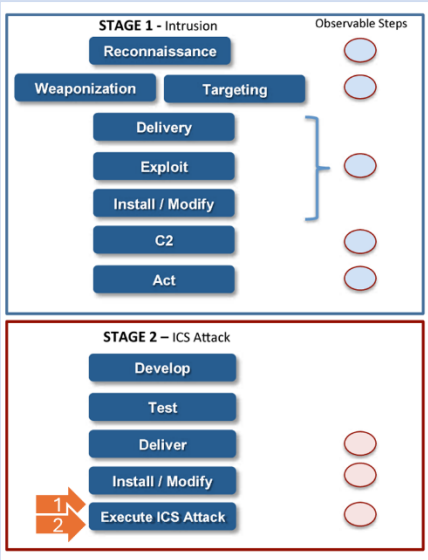
- Når var siste back-up gjennomført?
    - Hvordan gjenopprette rett konfigurasjon?
    - Har vi mulighet til å gjenopprette systemet til slik det var før aktør kom inn?
- Hva vil det bety dersom det er tapt informasjon mellom siste back-up og tidspunkt for gjenoppretning (logghistorikk etc.)?
    - Dersom tapt informasjon, hvilke typer informasjon er tapt?
    - Hvilke konsekvenser kan dette informasjonstapet ha?

2.5.2 Oppfølgingspunkter, avhengig av utfall på diskusjon og beslutninger

- Det viser seg at det er en feil i rutine som blir brukt for å ta backup. Hvordan gå frem for å håndtere dette?

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.



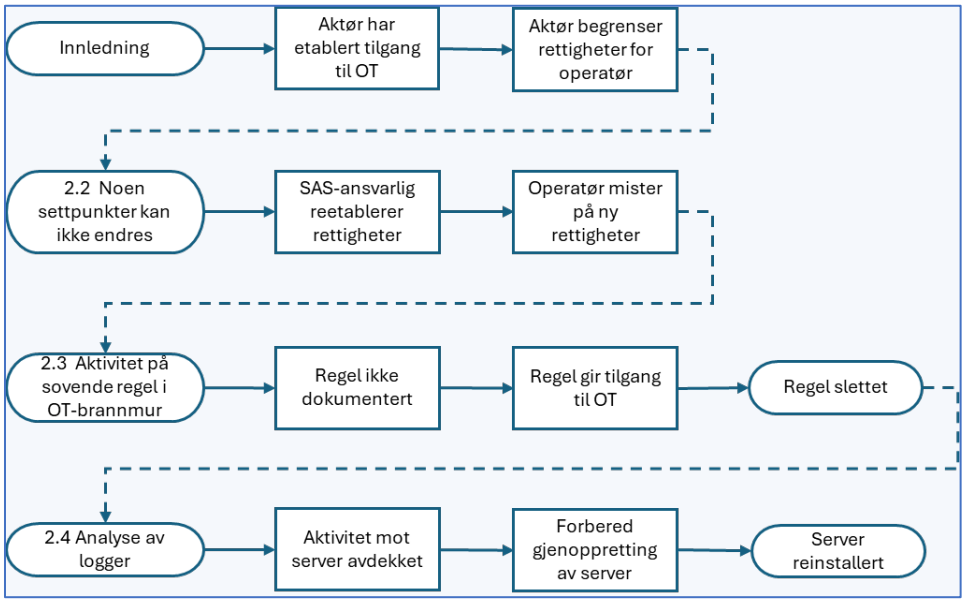
- Aktør har kommet gjennom barrierene for stage 1 og 2
- Angrep:
  - 1) Endring i brukertilganger i operatør-grensesnitt
  - 2) Gjentar endring
- Øvingspunkter:
  - Rotårsak til feilsituasjoner
  - Kontroll av brannmursregler
  - Undersøkelser/forensic
  - Gjenoppretting

3.1 Innledning til hendelse

En aktør har oppnådd tilgang til kontrollnettverket ved å benytte en prosjekt-etablert VPN-forbindelse med tilhørende brannmursregel.

3.2 Hendelse

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



3.3 Læring

Gjennomgang av rutiner, forbedring av systemer for å sikre mot nye angrep etc.

3.3.1 Veiledende spørsmål

Øvingsledelse

- Hvordan involveres deltakerne i sluttrapporten fra øvelsen?

SAS/IACS-ansvarlig

- Er ansvar og roller tydelig beskrevet?
- Dekket definerte rutiner denne typen hendelse?
- Ble rutinene fulgt?
- Hvordan sikrer en læring til øvrige skift?

Lokal driftsledelse

- Er ansvar og roller tydelig beskrevet?
- Dekket definerte rutiner denne typen hendelse?
- Ble rutinene fulgt?
- Er det behov for bedre kompetanse for å håndtere tilsvarende hendelser i fremtiden?
- Hvordan sikrer en læring til øvrige skift?

Systemansvarlig drift / IKT avdeling

- Er ansvar og roller tydelig beskrevet?
    - Er fordelingen av ansvar og oppgaver mellom systemansvarlig drift og IKT-avdelingen avklart?
- Dekket definerte rutiner denne typen hendelse?
- Ble rutinene fulgt?
- Hvordan sikre at læring fra denne hendelsen blir videreført i organisasjonen?

3.4 Aktuell litteratur

Hendelsesforløpet i denne øvelsen er inspirert av cyberangrepene mot strømforsyningen i Ukraina i 2015 og 2016. I hendelsen i desember 2015 opplevde operatørene at de ble sperret ute fra skjermsystemet og at noen betjente funksjoner og slik stengte ned deler av distribusjonsnettet for strøm.

I hendelsen i desember 2016 opplevde de at brytere i distribusjonsnettet ble åpnet og strømforsyningen ble slått av. Når operatørene tilbakestilte bryterne, ble disse nesten umiddelbart åpnet igjen.

Det er vist til rapporten «*Analysis of the Cyber Attack on the Ukrainian Power Grid*»[1] i flere tidligere øvelser. Her beskrives hvordan en aktør fikk tilgang til nettverkene for

[1] nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf

kontrollsystemene. Hendelsen i desember 2016 avdekket bruk av skadevare som aktivt går inn og overstyrer utstyr i de industrielle nettverkene. Skadevaren benytter de samme protokollene som kontrollsystemet benytter og vil derfor vanskelig kunne stoppes ved hjelp av brannmursregler. Denne skadevaren omtales både som Industroyer og Crashoverride. Skadevaren er modulært oppbygd og benytter flere protokoller for kommunikasjon med feltutstyr. Blogposten «*VAnalysis: Industroyer/CrashOverride Malware Attack*»[2] fra virsec gir en kort gjennomgang av hendelsen og rapporten «*CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations*»[3] fra Dragos inneholder også en grundigere teknisk beskrivelse.

[2] https://www.virsec.com/resources/blog/virsec-hack-analysis-deep-dive-into-industroyer-aka-crash-override
[3] https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf