Øvelsesplanlegger

Pakke 3 øving 1

«Aktør har utført rekognosering»

Versjon 1.0 17.01.2025

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 ved beredskapen, 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 det oppdages mistenkelig samling av informasjon om SAS-nettverk og industrielle kontrollsystemer.

2.1 Oversikt scenarioer

SAS/IACS ansvarlig finner et filområde i på en server i demilitarisert sone (DMZ). På filområdet er det filer som synes å inneholde informasjon om nettverk og innlogging for industrielle nettverk.

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 – filområde oppdages	x	?	x	
2.3	Eskalering - skadevare oppdages			x	x
2.4	Skadevare forsøkes aktivert			x	x

2.2 Innledende forhold – filområde oppdages

Nærmere undersøkelser viser at filene synes å inneholde informasjon, brukernavn og passord, samt annen informasjon som kan gi oversikt over nettverk og funksjoner i de industrielle nettverkene.

2.2.1 Innledende spørsmål

SAS/IACS-ansvarlig

- Hva gjøres umiddelbart?
- Hvordan samhandle med IKT-avdelingen?
- Hvordan samhandle med Systemansvarlig drift?
- Hvordan verifisere informasjonen i filområdet med egen systemdokumentasjon?

IKT-avdeling

- Hva gjøres umiddelbart?
- Hvordan samhandle med Systemansvarlig drift?
- Kan vi definere en indikator i fra det som er funnet?
- Er det noen indikasjoner på at området er opprettet av en legitim bruker?
- Hvem må varsles?

Systemansvarlig drift

- Hvordan samhandle med IKT-avdelingen?
- Hvem har ansvar i situasjonen?

Lokal driftsledelse

- Behov for at driftsledelse involveres?

2.2.2 Veiledende spørsmål

IKT-avdelingen mistenker at en ekstern aktør har fått fotfeste i kontornettverket.

IKT-avdeling

- Hvem har ansvar i situasjonen?
- Hvem må varsles?
- Hvordan kan vi vite om aktøren har gjort mer enn bare informasjonsinnhenting?
- Tilgangskontroll
    - Hvordan er tilgangsstyringen satt opp?
    - Hvem og hvordan administreres tilgangskontroll i virksomheten?
- Er brukernavn og passord gjenbrukt andre steder?
    - Er det rutiner for fornyelse av passord, back-up av systemer?
- Hvor lenge kan aktøren ha hatt tilgang?
- Hvordan fjerner vi tilgang for aktøren?
    - Skal tilgang fjernes eller videre aktivitet overvåkes?
    - Er det behov for ekstern kompetanse?

Systemansvarlig drift

- Hvordan kan vi finne ut om aktøren har påvirket kontrollsystemer eller SAS-nettverket?
    - Hvem og hvordan brukes ressurser for å identifisere dette?
    - Er det behov for støtte fra leverandører / ekstern kompetanse?
- Er brukernavn og passord i de industrielle nettverkene gjenbrukt?
    - Er det rutiner for fornyelse av passord, back-up av systemer?

SAS/IACS-ansvarlig

- Behov for at SAS/IACS-ansvarlig involveres?

Lokal driftsledelse

- Behov for at driftsledelse involveres?

2.2.3 Oppfølgingspunkter, avhengig av utfall på diskusjon og beslutninger

- Brannmur mot kontrollsystemene inneholder ingen logger relatert til hendelsen.
    - Er det behov for støtte fra IKT-leverandør i granskning/evaluering av hendelsen?
- Brannmurlogger har spor av ukjent aktivitet
    - Hvilke fagmiljøer (interne eller eksterne) kan kontaktes for kunnskap og erfaringer?

2.3 Eskalering - skadevare oppdages

Nærmere undersøkelser viser at oversikten over brukernavn og passord samsvarer med hva som benyttes i deler av kontrollnettverket. Det er ingen attributter på filområdet eller filer som kan bistå i å identifisere hvem som har opprettet filene.

IT-administrator oppdager tegn på angrepskode som refererer til samme type brannmurer bedriften benytter i de industrielle nettverkene.

2.3.1 Innledende spørsmål

IKT-avdeling

- Hvilke tiltak kan gjøres for å beskytte brannmuren?
  - Er det noen utestående SW-oppdateringer?
  - Hvordan identifisere og hvordan dele indikatorer (IoC)?
- Hvordan samhandle med Systemansvarlig drift?
- Hvem må varsles?

Systemansvarlig drift

- Hvordan samhandle med IKT-avdelingen?
- Hvem har ansvar i situasjonen?

SAS/IACS-ansvarlig

- Hvilke konsekvenser vil en eventuell isolering av brannmuren ha?
  - … for driften av kontrollsystemene?
  - … for driften av innretningen?
- Hvordan samhandle med driftsledelse?

2.3.2 Oppfølgingspunkter, avhengig av utfall på diskusjon og beslutninger

- Brannmur mot kontrollsystemene inneholder ingen logger relatert til hendelsen.
  - Er det behov for støtte fra IKT-leverandør i granskning/evaluering av hendelsen?
- Brannmurlogger har spor av ukjent aktivitet
  - Hvilke fagmiljøer kan kontaktes for kunnskap og erfaringer?

2.4 Skadevare forsøkes aktivert

For å beskytte brannmur og avdekke informasjon om aktør, er brannmuren oppdatert og blir nøye overvåket.
Det blir detektert at skadevaren aktiveres uten at det lykkes å gjøre skade.

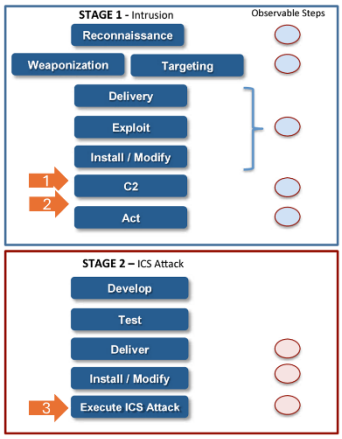
2.4.1 Innledende spørsmål

IKT-avdeling

- Hva gjøres umiddelbart?
- Hvordan kan taktikker, teknikker og prosedyrer (TTP) avdekkes?
    - Hvordan identifisere og hvordan dele indikatorer (IoC)?
- Hvordan samhandle med sektor CERT?

3 Ekstra informasjon til forberedelse og gjennomføring

Dette kapittelet inneholder bakgrunnsinformasjon 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.



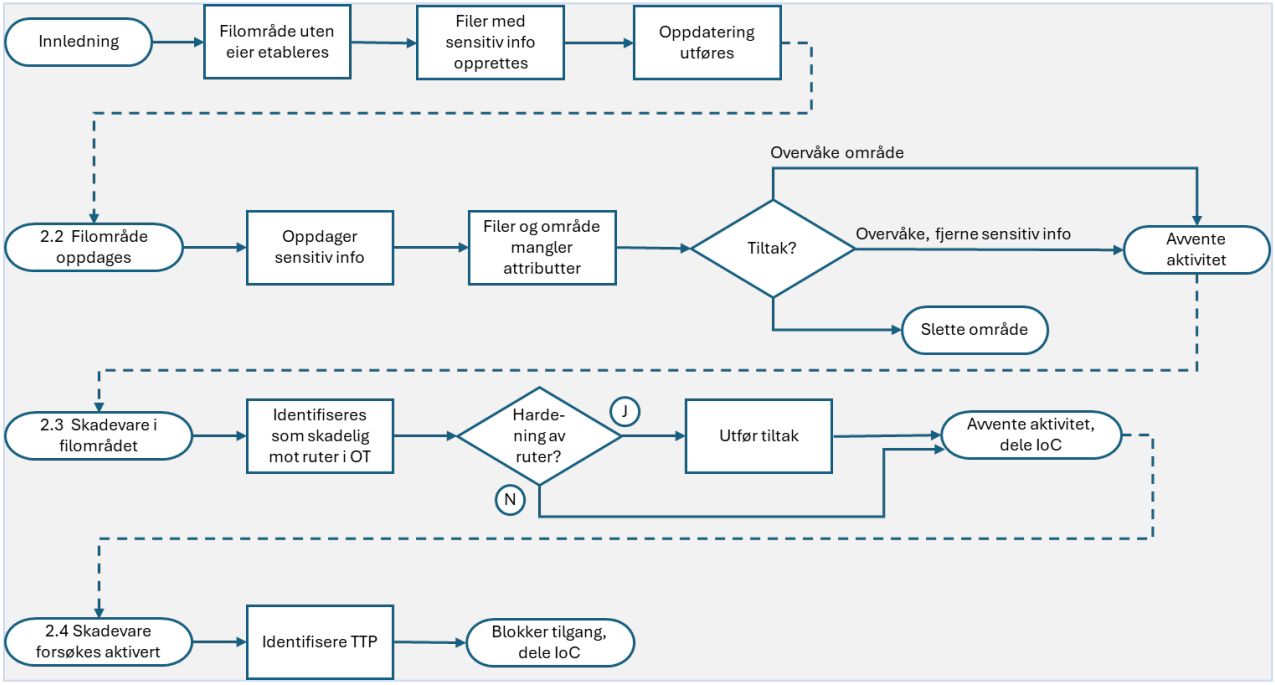
- Aktør har kommet gjennom barriere for stage 1 og samler informasjon lokalt
- Angrep:
  - 1) Informasjonsinnhenting
  - 2) Rekognosering mot OT-grensesnittet
  - 3) Skadevare aktiveres
- Øvingspunkter:
  - Avklare ansvar
  - Informasjonsdeling
  - Undersøkelser/forensic

3.1 Innledning til hendelse

Det oppdages et filområde som inneholder filer med sensitiv informasjon og det er ikke tydelig hvem som har opprettet området eller filene.

3.2 Hendelse

Det er muligheter for at filområdet er opprettet og at informasjonen er samlet av en aktør som på illegitim måte har etablert tilgang til systemene, via legitim fjerntilgang eller gjennom legitim bruker.



3.3 Læring

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

Øvingsledelse

- Hvordan involveres deltakerne i sluttrapporten fra øvelsen?

IKT avdeling

- Er ansvar og roller tilstrekkelig beskrevet?
- Hvordan støtter definerte rutiner håndteringen av hendelsen?
- Ble rutinene fulgt? Hvilke endringer bør gjøres?
- Hvordan sikres beskyttelse av systemdokumentasjon?

Systemansvarlig drift

- Er ansvar og roller tilstrekkelig beskrevet?
- Hvordan støtter definerte rutiner håndteringen av hendelsen?
- Ble rutinene fulgt? Hvilke endringer bør gjøres?

SAS/IACS-ansvarlig

- Er ansvar og roller tilstrekkelig beskrevet?
- Hvordan støtter definerte rutiner håndteringen av hendelsen?
- Ble rutinene fulgt? Hvilke endringer bør gjøres?
- Hvordan sikrer en læring til alle skift?

Lokal driftsledelse

- Hvordan støtter definerte rutiner håndteringen av hendelsen?
- Hvordan sikrer en læring til alle skift?

3.4 Aktuell litteratur

Eksempelet i denne øvingen der det oppdages at sensitiv informasjon samles og lagres lokalt, er neppe sannsynlig. De fleste aktører forsøker å være usynlige, og hvis mulig benytte funksjoner som allerede er tilgjengelige i nettverket.
Amerikanske myndigheter har i samarbeid med myndigheter i Canada, Storbritannia, Australia og New Zealand utarbeidet veiledningen *Identifying and Mitigating Living Off the Land Techniques*[1]. Sammendraget i rapporten er på tre sider og inneholder punkter med beste praksis for deteksjon og hardening.

I angrepet på el-forsyningen i Ukraina i desember 2015, startet dette våren 2015 og det er sannsynlig at det var en del muligheter for å detektere aktivitetene i forkant av hendelsen (*Analysis of the Cyber Attack on the Ukrainian Power Grid*[2] s. 23). Det er også vist til denne rapporten i øving 1 i pakke 1.

[1] https://media.defense.gov/2024/Feb/07/2003389936/-1/-1/0/JOINT-GUIDANCE-IDENTIFYING-AND-MITIGATING-LOTL.PDF
[2] https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf