Beredskapsøvelser for cyberangrep mot industrielle kontrollsystemer i petroleumssektoren

Guro Hotvedt & Andrea N. Skytterholm

Motivasjon

- Kobling mellom IT og Operasjonell Teknologi (OT)
- Økt angrepsflate
- Rapport fra DNV GL, “Trening og Øvelse”
    - Viser mangel på veiledere

Tiltak 24: Utgi egne eller vise til andres eksisterende veiledere for trening og øvelse

Det anbefales at Ptil enten gir ut en egen veileder som beskriver forventinger til trening og øvelser, eller viser til eksisterende veiledere der dette er beskrevet. I kapittel 4.3 er det presentert eksempler på veiledere for trening og øvelse utgitt av DSB, Difi og NVE.

Forskningsområde

- Fokusere på tabletop-øvelser
- Ønsket å undersøke hva som kjennetegner realistiske og hensiktsmessige scenarier

- Liste med kriterier
- Scenarier

Lister med kriterier

Individuelle scenarier:

- Basert på dagens trusselbilde
- Presentert i flere deler hvis passende
- Plausibelt
- Tilpasset organisasjonens systemer og har korrekte tekniske detaljer
- Ikke ha potensial til å stenge ned en plattform
- Utfordrende
- Gir mestring

Scenariosamling:

- Skalerbart
- Tilpasningsegnet
- Scenarier for både tekniske øvelser og prosedyre-øvelser
- Variasjon i innhold

Scenariosamling

Ransomware

De industrielle kontrollsystemene blir kryptert og låst. Videre truer angriperne med å stenge kjernegeneratoren hvis ransom ikke blir betalt.

Attack with USB stick enabling 4G

Et innsideangrep der en tekniker kobler inn en 4G dongle som muliggjør 4G tilkobling. Dette gjør at angriperen kan koble seg på interne nett via denne 4G koblingen.

Supply Chain Attack with Information Gathering

SOC varsles om data forsøkt sendt til en IP-adresse som ikke er definert i brannmuren. Det viser seg at spyware har kommet inn via en bakdør i en ny komponent fra en leverandør.

Disconnection of Detectors

Tre kontrollromsoperatører observerer at gassdetektorene slutter å respondere. De undersøker videre og antar det er en teknisk feil. Får så beskjed av SOC om at de er under et cyberangrep.

IACS Insider Attack

SOC oppdager at data sendes via en port som vanligvis ikke er i bruk. Porten er åpnet av en ansatt som kommer fra et høyrisikoland, og har blitt truet av aktører i hjemlandet til å åpne porten.

Industrial Internet of Things

Angripere har endret på dataen landorganisasjonen mottar fra IIoT enhetene. De tar dermed beslutninger basert på feil datagrunnlag.

Access to IACS via Remote Support

En kompromittert leverandør logger på kontrollsystemene med fjernaksess gjennom 2FA. Angriperne har installert malware hos leverandøren slik at de også får en tilkobling når han/hun logger på operatørens systemer.

Disruption of Safety Systems

En ansatt kjenner gasslukt og ingen gassdetektorer i det aktuelle området har gitt utslag. En kompromittert oppdatering av brann- og gass-systemet har ført til økning av grensen for akseptable gassnivåer.

Hvordan kan dette hjelpe industrien?

- Red-team brukes ofte
  - Dyrt og tidkrevende
- Tabletop-øvelser
  - Kan gjennomføres i løpet av noen timer
  - Krever lite ressurser

- Vår scenariosamling er et utgangspunkt
  - Må tilpasses
- Bruke kriteriene når egne scenarier utarbeides

→ Effektivisere planlegging og gjennomføring av beredskapsøvelser

→ Øke antall gjennomførte øvelser

Spørsmål?

gurohotvedt@gmail.com

andreaskytterholm@gmail.com