|  |  |
| --- | --- |
| **Scenario** | **1 – Dataangrep på automasjonssystemer** |
| Øvingsform | Spilløvelse |
| Modenhetskrav | Lav |
| Forventet tidsbruk | Forberedelse: 40 timerGjennomføring: 2-6 timerEvaluering: 2 timer |
| Beskrivelse av scenario | * En målrettet angriper med vilje og evne til å utføre avanserte angrep mot OT-systemer har skaffet seg tilgang ved å utnytte svakheter i internetteksponerte systemer.
* Angriperen har utført intern rekognosering og har klart å få kontroll over en datamaskin som brukes til å konfigurere regulatorer (en engineering workstation).
* Angrepet oppdages gjennom et varsel fra nettverksbasert overvåkning som rapporterer om mistenkelig nettverkstrafikk.
 |
| Egnede øvingsmål | * Etablere felles situasjonsforståelse i beredskapsteam
* Øve på samhandling med leverandører
* Øke virksomhetens evne til å bruke etablert planverk
* Bevisstgjøring rundt eksisterende tiltak
 |
| Egnede roller for øvende | * Innsatsleder
* Loggfører
* Kommunikasjonsansvarlig
* Teknisk personell (IT og OT)
 |
| Roller i spillstab | * Scenarioleder
* IT- og OT-sikkerhet
* KraftCert
* Automasjonsavdeling
* OT-leverandør
* Beredskapsmyndighet
 |
| Øvingsmomenter | 1. Leder for IT-avdelingen får varsel fra en nettverkssensor i driftskontrollsystemet om «mulig uautorisert opplasting av prosjektfil til PLS» og varsler videre beredskapsleder på e-post.
2. Beredskapsteamet kalles inn og erklærer at vi har en pågående sikkerhetshendelse. Ber automasjon rapportere inn.
3. IT-avdelingen har mottatt et varsel fra IT-sikkerhetspartner om utnyttelse av kjent sårbarhet i brannmur FIREX, som er merket som benyttes i virksomheten. IT-avdelingen har iverksatt undersøkelser og har flere tekniske funn, blant annet fra brannmur i OT-nettet.
4. Det er grunn til å tro at angriperen har reprogrammert flere regulatorer basert på nettverksdata. Det må tas en beslutning om veien videre.
5. Leverandøren stiler med personell på stedet for å bistå med gjenoppretting. Kan man stole på at personen som er sendt kommer fra leverandøren?
 |