|  |  |
| --- | --- |
| **Scenario** | **5 - Forsyningskjede-angrep** |
| Øvingsform | Spilløvelse |
| Modenhetskrav | Middels |
| Forventet tidsbruk | Forberedelse: 40 timer  Gjennomføring: 2-6 timer  Evaluering: 2 timer |
| Beskrivelse av scenario | * En systemleverandør er fysisk til stede og skal oppdatere firmware på regulatorer i driftskontrollsystemet. Leverandøren benytter virksomhetens service-laptop, og kobler først til nettverket for å laste ned den nye programvaren. * Ny firmware flashes til regulatorer under en planlagt kort driftsstans. Ved oppstart etterpå tripper systemet ved tilsynelatende jevne mellomrom og det blir brudd i strømproduksjonen. |
| Egnede øvingsmål | * Etablere felles situasjonsforståelse i beredskapsteam * Øve på samhandling med leverandører * Øke virksomhetens evne til å bruke etablert planverk |
| Egnede roller for øvende | * Innsatsleder * Loggfører * Kommunikasjonsansvarlig * Teknisk personell (IT og OT) |
| Roller i spillstab | * Scenarioleder * IT og IT-sikkerhet * Automasjonsavdeling * OT-leverandør * Kundeservice * KraftCert |
| Øvingsmomenter | 1. Oppdatering av fastvare i regulatorer installeres. 2. Regulatorer begynner å feile regelmessig. 3. KraftCERT melder at leverandøren har blitt kompromittert. 4. Leverandøren har ikke nok teknikere. 5. Virksomhetens tekniker har mange gode ideer. |