|  |  |
| --- | --- |
| **Scenario** | **2 – Avansert vedvarende trussel (APT)** |
| Øvingsform | Diskusjonsøvelse |
| Modenhetskrav | Middels |
| Forventet tidsbruk | Forberedelse: 8 timer  Gjennomføring: 2 timer  Evaluering: 1 timer |
| Beskrivelse av scenario | * En trusselaktør har kompromittert IKT-systemene til virksomheten, og ønsker å bruke dette til å kartlegge robustheten i det norske kraftsystemet over tid.​ * Trusselaktøren har samtidig kompromittert mange aktører, og har også skaffet seg fotfeste i driftskontrollsystemene for overvåkning av produksjonsdata over tid. ​ * Angrepet oppdages av en annen KBO-enhet, som deler indikatorer som gjør at aktiviteten kan verifiseres basert på brannmurlogger. |
| Egnede øvingsmål | * Øve på beslutninger under usikkerhet * Utvikle samhandling mellom IT og OT * Utvikle evne til å samhandle med andre KBO-enheter og sektorens sentrale responsmiljø |
| Egnede roller for øvende | * Innsatsleder * Loggfører * Kommunikasjonsansvarlig * Teknisk personell (IT og OT) |
| Roller under øvelse | * Øvingsleder (diskusjonsøvelse) * Referent |
| Øvingsmomenter | 1. Beskjed om pågående angrep mot sektoren bekreftet fra IT/SOC 2. Ny informasjon oppdaget om angrep/trusselaktør. Hvordan og hva skal deles? 3. Media viser interesse for angrepet og kontakter informasjonsavdelingen. Hva skal deles eksternt? 4. Nasjonal sikkerhetsmyndighet ber om statusrapport, med vurdering av potensialet for at trusselaktøren kan forstyrre kraftleveranser til sluttbruker 5. Skal virksomheten gå i øydrift inntil videre? 6. Hvordan prioriterer vi ressursbruken? 7. Er digital etterforskning og sikring av bevis viktig? 8. Hvordan sørger vi for at responsen hele tiden har et oppdatert lokalt og eksternt trusselbilde? |