|  |  |
| --- | --- |
| **Scenario** | **3 – Brudd på integritet i sanntidsdata** |
| Øvingsform | Diskusjonsøvelse |
| Modenhetskrav | Middels |
| Forventet tidsbruk | Forberedelse: 8 timer  Gjennomføring: 2 timer  Evaluering: 1 timer |
| Beskrivelse av scenario | * En bruker er kompromittert hos en leverandør som fyller ut en arbeidsordre og får denne godkjent. * Den kompromitterte brukere får åpnet for fjerntilgang til driftskontrollsystemet og installerer en skadevare som bruker en DNS-tunnel ut til internett for å nå angriperens infrastruktur. * Angrepet fører til manipulasjon av rapporterte produksjonsdata, som er grunnlag for offentlige statistikker. ​ |
| 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. En falsk arbeidsordre blir utfylt og sendt. 2. Arbeidsordren godkjennes, og skadevare installeres med ved bruk av den påfølgende autoriseringen av BjørneKraft. 3. Manipulasjon av sanntidsdata blir iverksatt av skadevaren Hvordan kan integriteten av produksjonsdata verifiseres? Hva er våre første tiltak? Husk kommunikasjon med relevante aktører. 4. Beskjed fra Bjørnekraft om mulig datainnbrudd, og at det er gjort forsøk på å komme inn i deres tjenester. 5. En operatør oppdager at interne målinger ikke samsvarer med data fra Historian. 6. Aktivering av beredskapsplan, men hendelsen kan ikke bare løses internt. 7. Media får nyss om hendelsen, og det begynner å spre seg rykter om sabotasje i organisasjonen. Hvordan skal dette håndteres, og av hvem? |