|  |  |
| --- | --- |
| **Scenario** | **14 – Brudd på personvern** |
| Øvingsform | Diskusjonsøvelse |
| Modenhetskrav | Lav |
| Forventet tidsbruk | Forberedelse: 8 timerGjennomføring: 2 timerEvaluering: 1 timer |
| Beskrivelse av scenario | * En dataanalytiker har tilgang til kundedatabasen via et API, og bruker dette til å lage analysedashbord i PowerBI. API-nøkkelen ble ved et uhell lekket i et offentlig Github-repo.
* En angriper bruker nøkkelen og henter ut alle kundedata. Dataene inneholder adresser, telefonnummer, fakturaer, transaksjonsinformasjon og statistikk fra AMS-målere. Dette legges ut for salg på det mørke nettet.
* Kraftselskapet blir varslet av en anonym person om at disse dataene ligger ut for salg på «DarkPower» et forum for kriminelle som handler i stjålne data fra kraftselskaper.
 |
| Egnede øvingsmål | * Øve på beslutninger under usikkerhet
* Utvikle samhandling mellom IT og OT
* Øve på bruk av planverk
 |
| Egnede roller for øvende | * Innsatsleder
* Loggfører
* Kommunikasjonsansvarlig
* Teknisk personell (IT og OT)
 |
| Roller under øvelse | * Øvingsleder (diskusjonsøvelse)
* Referent
 |
| Øvingsmomenter | 1. Anonymt tips kommer på e-post om at kundedata er lagt ut for salg på det mørke nettet.
2. Tips med lenke til kundedata dukker opp på e-post.
3. Henvendelse fra VG kommer på SMS. De har fått et anonymt tips.
4. Det har kommet en henvendelse til IT-sjefen noen dager tidligere om en lekket API-nøkkel, denne har ikke kommet frem.
5. Det viser seg at data sannsynligvis er lekket via denne API-nøkkelen.
6. Det konstateres at alle kundedata sannsynligvis er lekket.
7. Krisestab er satt, kunder begynner å etterspørre informasjon.
 |