|  |  |
| --- | --- |
| **Scenario** | **9 - Teknologisk innovasjon** |
| Øvingsform | Diskusjonsøvelse |
| Modenhetskrav | Lav |
| Forventet tidsbruk | Forberedelse: 8 timerGjennomføring: 2 timerEvaluering: 1 timer |
| Beskrivelse av scenario | * Et kraftselskap ønsker å effektivisere vedlikeholdsarbeidet på turbiner, og tar i bruk et nytt KI-verktøy for dette. KI-verktøyet samler data fra eksisterende prosessmålinger og egne IoT-sensorer som strømmes til leverandørens skyløsning.
* Tanken er at man ved hjelp av maskinlæring skal kunne oppdage der det er risiko for feiltilstander tidlig, og derfor kunne gå over til tilstandsbasert vedlikehold i stedet for periodebasert.
* Analysesleder blir gjort oppmerksom på nyhetssak hvor samme KI-leverandør har blitt hacket, og dette har ført til feilbehandling på flere sykehus i utlandet som har brukt systemet til å planlegge operasjoner. Leder for Helsedirektoratet sier på TV-nyhetene at de ikke er bekymret for liknende problemer I Norge på grunn av det strenge lovverket om risikovurdering ved innføring av KI-systemer.
 |
| Egnede øvingsmål | * Vurdere risikoer ved bruk av et KI-verktøy levert av en leverandør som har vært utsatt for et cyberangrep.
* Diskutere hvordan slike risikoer kan overføres til kraftsektoren.
* Utforske tiltak for å sikre KI-verktøyets pålitelighet og minimere risiko for kritiske feil.
* Øke forståelsen for krav om sikkerhet og overholdelse av regelverk ved innføring av KI-løsninger.
 |
| Egnede roller for øvende | * Beredskapsleder / Innsatsleder
* Loggfører
* Kommunikasjonsansvarlig
* Teknisk personell (IT og OT)
 |
| Roller under øvelse | * Øvingsleder (diskusjonsøvelse)
* Referent
 |
| Øvingsmomenter | 1. Risikoforståelse
2. Tillitt til leverandør
3. Mulige konsekvenser
4. Regulatoriske krav og lovverk
5. Beredskap
6. Data- og systemintegrasjon
 |