|  |  |
| --- | --- |
| **Scenario** | **16 - Man-in-the-Middle (MitM) angrep** |
| Øvingsform | Diskusjonsøvelse |
| Modenhetskrav | Lav |
| Forventet tidsbruk | Forberedelse: 8 timerGjennomføring: 2 timerEvaluering: 1 timer |
| Beskrivelse av scenario | * Energitraderne i Superkraft bruker chatte-app’en “Superchat” til å snakke seg imellom om mulige kontrakter og diskutere investeringer. En angriper har laget en falsk versjon av Superchat, og lurer investeringssjefen over på denne.
* Det dukker opp en “ugyldig sertifikat”-advarsel i nettleseren som investeringssjefen ignorerer. Hackerne snapper opp meldingene på den falske serveren før de blir sendt videre til den ekte Superchat-serveren. På denne måten kan de avlytte kommunikasjonen og manipulere den.
* Dette oppdages først etter at det ble inngått en futures-kontrakt som investeringssjefen var sikker på var en god investering, men hvor det viste seg at han/hun burde visst mye bedre. Ved nærmere undersøkelser oppdaget investeringssjefen at det var avvik I beskjedene som var sendt og mottatt med traderne.
 |
| Egnede øvingsmål | * Øve på beslutninger under usikkerhet
* Øve på samhandling mellom IT og andre
* 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. Sikkerhetskultur i virksomheten
2. Håndtering av feilmeldinger/advarsler
3. Kommunikasjonsprotokoller
4. Etiske dilemmaer med overvåking av kommunikasjon
5. Håndtering av kritiske hendelser
 |