|  |  |
| --- | --- |
| **Scenario** | **10 - Zero-day exploit** |
| Øvingsform | Diskusjonsøvelse |
| Modenhetskrav | Middels |
| Forventet tidsbruk | Forberedelse: 8 timerGjennomføring: 2 timerEvaluering: 1 timer |
| Beskrivelse av scenario | * En nulldagssårbarhet i Chromium blir utnyttet av avanserte aktører i målrettede angrep mot kraftsektoren i flere NATO-land.
* Dette har ført til at flere kraftselskaper har blitt kompromittert. Sårbarheten skal ha vært av typen som ikke krever brukerinteraksjon, slik at om man besøker en spesielt utformet nettside, blir man hacket.
* Det kommer varsel fra KraftCERT om at kraftselskapene som har blitt hacket, har besøkt kunnskapsbasen til en leverandør av digitale vern, og at denne tilgangen til internett normalt sett er en del av det vanlige oppsettet av HMI-ene for dette systemet. Alle kraftselskaper oppfordres til å sjekke om de er rammet eller sårbare, og ta hensiktsmessige grep. Avvik skal rapporteres til beredskapsmyndigheten.
 |
| Egnede øvingsmål | * Øve på bruk av planverk
* Øve på kommunikasjon med myndighets-organer
* Øve på dokumentering av hendelsesforløp, og sikring av spor
 |
| Egnede roller for øvende | * Innsatsleder
* Loggfører
* Kommunikasjonsansvarlig
* Teknisk personell (IT og OT)
 |
| Roller under øvelse | * Øvingsleder (diskusjonsøvelse)
* Referent
 |
| Øvingsmomenter | 1. Identifisering av sårbarheter
2. Aktivering av beredskapsplan
3. Samarbeid med eksterne parter
4. Håndtering av kompromitterte systemer
5. Prioritering av tiltak
6. Gjenoppretting og normalisering
7. Rapportering og dokumentasjon
 |