|  |  |
| --- | --- |
| **Scenario** | **4 – Fjernaksesskompromittering** |
| Øvingsform | Spilløvelse |
| Modenhetskrav | Middels |
| Forventet tidsbruk | Forberedelse: 40 timerGjennomføring: 2-6 timerEvaluering: 2 timer |
| Beskrivelse av scenario | * Kraftselskapet bruker en brannmurløsning som støtter SSLVPN.
* En sårbarhet i brannmuren gjør at angriperen får tilgang i nettverket og beveger seg lateralt til interne servere i driftskontrollsystemet.
* Aktiviteten oppdages når virksomheten får et varsel fra NVE/NSM om at det er sårbarheter I SSLVPN-løsning X som blir masseutnyttet på internett.
 |
| Egnede øvingsmål | * Etablere felles situasjonsforståelse i beredskapsteam
* Øve på virksomhetens evne til å bruke etablert planverk
* Bevissthet rundt eksisterende tiltak og sårbarheter
 |
| Egnede roller for øvende | * Innsatsleder
* Loggfører
* Kommunikasjonsansvarlig
* IT-sjef / Teknisk personell (IT og OT)
 |
| Roller i spillstab | * Scenarioleder
* KraftCert
* Teknisk personell (IT)
* Brannmurleverandør
* Journalist
 |
| Øvingsmomenter | 1. IT-sjef får et varsel fra NSM om massiv utnyttelse av en sårbarhet i en SSLVPN-løsning som er bygd inn i mange brannmurer.
2. Uvanlig aktivitet blir oppdaget på interne servere.
3. Beredskapsteam kalles inn.
4. IT starter dypere undersøkelser, de finner flere ting på interne servere og brannmur.
5. Det virker som et rekognoserings-angrep, men det er umulig å være sikker på at det ikke kan påvirke driften.
 |