|  |  |
| --- | --- |
| **Scenario** | **15 - DDoS-angrep** |
| Øvingsform | Spilløvelse |
| Modenhetskrav | Middels |
| Forventet tidsbruk | Forberedelse: 40 timer  Gjennomføring: 2-6 timer  Evaluering: 2 timer |
| Beskrivelse av scenario | * En botfarm med kontroll over tusenvis av X- og instagramkontoer poster og forsterker hverandres poster om at Kraftselskapet X kommer til å øke alle prisene med 50% og øke oppsigelsestiden på alle avtaler til 24 måneder. * De utfører så et DDoS-angrep mot kundeserviceavdelingen og nettsiden til Kraftselskapet X. * Selskapet kan ikke motta kundeforespørsler på chat, e-post er nede, og nettsiden er utilgjengelig. Dette er første nyhet på alle nyhetskanaler i Nord-Europa. |
| Egnede øvingsmål | * Øve på beslutninger under usikkerhet * Koordinere krisehåndtering mellom avdelinger * Håndtere et teknisk angrep (DDoS) og gjenopprette systemer * Kommunikasjon med media og eksterne aktører under krise |
| Egnede roller for øvende | * Beredskapsleder / innsatsleder * Loggfører * Kommunikasjonsansvarlig * Teknisk personell (IT og OT) |
| Roller i spillstab | * Scenarioleder * IT og OT-sikkerhet * Media * Kundeservice |
| Øvingsmomenter | 1. En kommunikasjonsovervåker varsler om en plutselig økning i sosial aktivitet på X og Instagram. Bot-kontoer sprer falske rykter om at selskapet skal øke prisene med 50 % og øke oppsigelsestiden til 24 måneder. 2. Kundeservice opplever en kraftig økning i henvendelser om prisøkninger og endringer i avtalevilkår. Kundene uttrykker bekymring og frustrasjon. 3. Et DDoS-angrep slår til mot selskapets nettside, og systemene begynner å gå ned. Kundeserviceportalen er utilgjengelig, og kundene kan ikke komme i kontakt med selskapet. 4. IT-avdelingen begynner å få kontroll over DDoS-angrepet, men tjenestene er fortsatt nede. Offentligheten krever svar, og mediene har begynt å dekke krisen. |