|  |  |
| --- | --- |
| **Scenario** | **18 – Tyveri av legitimasjon** |
| Øvingsform | Spilløvelse |
| Modenhetskrav | Middels |
| Forventet tidsbruk | Forberedelse: 40 timer  Gjennomføring: 2-6 timer  Evaluering: 2 timer |
| Beskrivelse av scenario | * Per Bjarne jobber i IT-avdelingen hos Superkraft. En dag finner han ikke adgangskortet sitt i gangen hjemme når han skal på jobb. Han kjører til jobben og varsler om at kortet er borte, men sikkert bare er på avveie hjemme. Han får et lånekort for dagen. * I løpet av natten har uvedkommende vært inne i kontorbygget til Superkraft. De har plugget inn en RaspberryPi med mobilmodem i en ledig port konfigurert i admin-VLAN i en svitsj som ikke var låst inn. Senere undersøkelser viser at noen hadde brukt Per Bjarnes adgangskort klokken 2:15 på natten. * En uke senere varsler Per Bjarne at han fortsatt ikke kan finne adgangskortet sitt, og ber om å få et nytt et. Det gamle kortet blir sperret og man iverksetter rutinemessig en sjekk om kortet har blitt brukt i mellomtiden. Da merker man at noen brukte det klokken 2:15 på natten en uke tidligere. |
| Egnede øvingsmål | * Øve på samarbeid mellom fysisk sikkerhet, IT-avdeling og ledelse under en sikkerhetshendelse. * Trene på avdekking av uautorisert nettverkstilgang og håndtering av mistenkelige enheter. * Forbedre rutiner for logganalyse og monitorering av sensitive områder. * Evaluere kommunikasjon under krisesituasjoner, internt og eksternt. |
| Egnede roller for øvende | * Beredskapsleder/innsatsleder * IT-sjef eller IT-sikkerhet * Loggfører * Kommunikasjon |
| Roller i spillstab | * Adgangskontroll * IT-avdeling * Per Bjarne * Media |
| Øvingsmomenter | 1. Adgangskontroll mottar en melding fra Per Bjarne om at han har mistet adgangskortet sitt. Han varsler om at han tror det bare er borte midlertidig. 2. En uke etter at adgangskortet ble meldt tapt, finner man ut at kortet har blitt brukt til et mistenkelig innbrudd, og selskapet står i fare for at flere systemer kan være kompromittert. Selskapets ledelse og ansatte må informeres. 3. Det blir funnet en RaspberryPi i et serverrom som det har vært jevnlig trafikk på siden den ble installert. FSHARE-1 er brukt av prosjektet «Nettutbedring ny kraftstasjon Høymarka». Alle filene derfra kopieres over til 10.10.1.2 hver natt klokken 03:00. Dette er IP-en som RaspberryPI-en hadde. |