|  |  |
| --- | --- |
| **Scenario** | **12 – Brannmurkonfigurasjonsfeil** |
| Øvingsform | Diskusjonsøvelse |
| Modenhetskrav | Lav |
| Forventet tidsbruk | Forberedelse: 8 timerGjennomføring: 2 timerEvaluering: 1 timer |
| Beskrivelse av scenario | * Et kraftselskap har leid inn et konsulentfirma for å gjøre en sjekk av oppsett av sikkerhetssystemene for IKT. Konsulentene finner flere feilkonfigurasjoner i brannmuren, blant annet at bade RDP og SSH-trafikk fra internett er tillatt.
* Eskaleringspunkt 1: man oppdager ved undersøkelse av logger at det er flere innlogginger over RDP fra en IP-adresse i Kina.
* Eskaleringspunkt 2: man oppdager mystiske kortvarige ssh-tilkoblinger fra ukjente norske IP-adresser, kun på natten.
 |
| Egnede øvingsmål | * Teste evne til å håndtere tilfeldig oppdaget angrep
* Teste evne til samarbeid med IT drift
* Øve på å vurdere alvorlighetsgrad av et funn i henhold til planverk
 |
| Egnede roller for øvende | * Innsatsleder
* Loggfører
* Kommunikasjonsansvarlig
* Teknisk personell (IT)
 |
| Roller under øvelse | * Øvingsleder (diskusjonsøvelse)
* Referent
 |
| Øvingsmomenter | 1. Mulige handlemåter og prioritering: blokkere først, eller analysere mulighet for utnyttelse først?
2. Kommunikasjon til ledelsen: hvem har ansvaret for gjennomføring av tiltak, og hvorfor var brannmuren feilkonfigurert?
3. Eskaleringspunkt 1: IT-avdelingen har avdekket fra logger at det er flere RDP-innlogginger fra Kina. Dette skjer daglig i en periode på 2 måneder. Det er så lenge man har logger. Hva er hensiktsmessige spørsmål å stille om dette, og hva er mulige handlemåter?
4. På serveren finner IT-teamet ZIP-filer med ukenummer i navnet. Docs\_week<NO>.zip i mappen C:\Temp. De regner med disse har blitt lastet opp av hackeren. Mappene er passordbeskyttet. Hvordan håndterer vi dette?
5. Eksaleringspunkt 2: IT-avdelingen har også søkt etter andre protokoller og funnet at det har vært SSH-sesjoner på natten med varighet opp til 2 minutter. Disse har gått til to forskjellige systemer, til en dedikert server som brukes til styring av adgangskontroll.
6. Ledelsen ønsker en statusrapport. Hva har skjedd, hva er skadevirkningene, og hva er gjort for å få kontroll?
7. Undersøkelse av endringslogg på brannmuren viser at det er systemadminsitratoren Steinar Lurv som har åpnet brannmuren for innlogginger via SSH og RDP fra 0.0.0.0/0, mens oppgaven i Jira viser at den egentlig skulle åpnes fra en spesifikk IP-adresse.
 |