|  |  |
| --- | --- |
| **Scenario** | **19 – Kompromittering av skytjenester** |
| Øvingsform | Diskusjonsøvelse |
| Modenhetskrav | Lav |
| Forventet tidsbruk | Forberedelse: 8 timerGjennomføring: 2 timerEvaluering: 1 timer |
| Beskrivelse av scenario | * Minikraft har hyret inn en student som utvikler på deltid. Utvikleren deployer en webapp for testing i AWS.
* Dessverre har utvikleren lekket den hemmelige nøkkelen som gir tilgang til AWS-kontoen på internet ved et uhell. Dette gir tilgang til å spinne opp virtuelle maskiner for den som har nøkkelen.
* En angriper finner nøkkelen og spinner opp 10 kraftige VM-er med mye GPU-ressurser, for å kjøre kryptominere. Dette oppdages når AWS-kontoeier får et varsel om at AWS-regningen for måneden er estimert å bli over 900.000 kroner.
 |
| Egnede øvingsmål | * Øve på bruk av planverk for ekstern skytjeneste
* Øve på involvering av supporttjenester fra plattformleverandør
 |
| Egnede roller for øvende | * Innsatsleder
* Loggfører
* Kommunikasjonsansvarlig
* Teknisk personell (IT)
 |
| Roller under øvelse | * Øvingsleder (diskusjonsøvelse)
* Referent
 |
| Øvingsmomenter | 1. **Identifisering av hendelsen**: Hvordan kan organisasjonen raskt identifisere at en skykonto er kompromittert? Hvilke indikatorer bør de se etter?
2. **Kommunikasjon med skyleverandør**: Hvordan skal organisasjonen kontakte AWS supporttjeneste? Hvilken informasjon bør de ha klar for å få raskest mulig hjelp?
3. **Tilgangshåndtering**: Hvordan kan organisasjonen sikre at hemmelige nøkler og andre sensitive opplysninger ikke lekker ut? Hvilke beste praksiser bør følges?
4. **Skadebegrensning**: Hva kan gjøres umiddelbart for å begrense skaden når en kompromittert konto oppdages? Hvordan kan man raskt stoppe de virtuelle maskinene som kjører kryptominere?
5. **Kostnadshåndtering**: Hvordan kan organisasjonen håndtere den økonomiske belastningen av en slik hendelse? Er det mulig å få refusjon fra AWS?
6. **Intern kommunikasjon**: Hvordan kan situasjonen forklares til ikke-tekniske avdelinger i organisasjonen? Hvilke nøkkelpunkter bør inkluderes for å sikre forståelse?
7. **Etterforskning av hendelsen**: Hvilke trinn bør tas for å etterforske hvordan nøkkelen ble lekket og hvem som kan stå bak angrepet?
8. **Opplæring og bevisstgjøring**: Hvordan kan organisasjonen trene sine ansatte, inkludert utviklere, på sikker håndtering av skykontoer og hemmelige nøkler?
 |