|  |  |
| --- | --- |
| **Scenario** | **20 – Kompromittering av IoT-enhet** |
| Øvingsform | Spilløvelse |
| Modenhetskrav | Middels |
| Forventet tidsbruk | Forberedelse: 40 timerGjennomføring: 2-6 timerEvaluering: 2 timer |
| Beskrivelse av scenario | * Minikraft har kjøpt billige overvåkningskameraer fra Alibaba.com. Disse fungerer utmerket og tillater de ansatte å sjekke tilstanden rundt i anlegget via mobiltelefonen.
* IT-avdelingen får et varsel fra Politiet at IP-adresser fra Minikraft er blitt brukt til å forsøke å bryte seg inn i webserverne til Diamantbanken. IT-avdelingen ser raskt at IP-adressene det gjelder er to av de billige kameraene.
 |
| Egnede øvingsmål | * Håndtere varsel om hendelse fra tredjepart (Politiet)
* Samhandling mellom fysisk og digital sikkerhet
 |
| Egnede roller for øvende | * Innsatsleder
* Loggfører
* Kommunikasjonsansvarlig
* Teknisk personell (IT og OT)
* Vaktsjef (som bruker kameraer)
 |
| Roller i spillstab | * Scenarioleder
* IT-sikkerhet
* Teknisk personell
* Kontoradministrator
* Beredskapsmyndighet (politi)
* Vaktpersonell
* Kommunikasjonssjef i diamantbanken
 |
| Øvingsmomenter | 1. Identifisere at IP-adresser gjelder billige kameraer
2. Tegne på forsøk på lateral bevegelse fra IP-kameraer til interne systemer
3. IT-avdeling oppdager at passord fra IP-kamera også er brukt på admin-panel for låsesystem
4. Trusselrapport viser at trusselaktør som målretter seg mot slike kameraer ofte bygger inn bakdører
5. Teknisk analyse av kamera finner tegn på slike bakdører
6. Diamantbanken sender IOC-er som også inkluderer andre IP-adresser fra kontornettet. Dette gjelder smarte møteromsskilt.
7. Analyse tyder på at det er et kompromittert default SSH-passord på møteromsskiltene som er misbrukt, og at det kommer innlogginger fra de billige kameraene.
 |