Øvelse 47 – Vurdering af CIS18-implementeringsgruppe (IG)

Information

Formålet med denne øvelse er at give dig en grundlæggende forståelse for, hvordan CIS18-kontroller kan bruges til at vurdere en virksomheds sikkerhedsmodenhed. Du skal i denne casebaserede øvelsen arbejde med begrebet implementeringsgrupper (IG) og anvende det til at analysere en virksomheds aktuelle praksis og fremtidige behov.

Baggrund

CIS Controls v8 indeholder 18 kontroller, som er struktureret til at hjælpe organisationer med at opbygge et effektivt sikkerhedsprogram. For at sikre, at anbefalingerne er realistiske og tilpasset forskellige typer organisationer, arbejder CIS med tre implementeringsgrupper (IG1 – IG3), der svarer til stigende modenhed og risikoprofil.

Ved at analysere en virksomheds sikkerhedspraksis kan man vurdere, hvilken IG der passer bedst – og hvordan virksomheden kan bevæge sig mod et højere niveau.

Case: BS Consulting A/S

BS Consulting A/S er en mellemstor virksomhed i teknologibranchen. De udvikler softwareløsninger til internationale kunder og opbevarer følsomme persondata. Virksomheden er bekymret for deres cybersikkerhed og ønsker en vurdering af deres nuværende situation og modenhedsniveau i forhold til CIS18.

Nuværende situation:

1. Har en etableret IT-afdeling med ansvar for cybersikkerhed.
2. Har antivirus og antimalware installeret og opdateret.
3. Har rollebaseret adgangskontrol.
4. Har en sikkerhedspolitik, men den er forældet, og medarbejdere er ikke trænet i den.
5. Har en reaktiv tilgang til sikkerhed (reagerer på hændelser, men forebygger ikke proaktivt).

Instruktioner

Som gruppe skal I analysere casen og vurdere:

1. Hvilken implementeringsgruppe (IG1, IG2 eller IG3) passer BS Consulting A/S bedst til i deres nuværende tilstand?
2. Hvilke dele af deres praksis trækker i retning af lav/moderat/høj modenhed?
3. Hvad skal der til for at hæve modenheden til næste IG?

Skriv jeres vurdering og begrund den med henvisning til CIS18 rammeværket.

Løsning

1. Implementeringsgruppe
   - CIS kontroller
     - 1 = IG 2
     - 2 = IG 0 → 1
     - 3 = IG 0 → 1
     - 4 = IG 0
     - 5 = IG 0
     - Scope = Data Protection (3) + Application Software Security (16)
       - Security Awareness and Skills Training (14)
     - Generelt er det svært at placere dem i IG1, IG2 eller IG3, da de ikke aktivt arbejder med sikkerheden.
2. Modenhed
   - Det meste trækker i retning af lav modenhed.
   - Mangel på information
   - De burde være på IG2, men er knap nok på IG 1.
3. Hævelse af modenhed
   - Der skal forbedres på stort set alle parametre.

Refleksionsspørgsmål

- Hvad er sammenhængen med IG og risikoprofil?
- Hvad er den største forskel mellem reaktiv og proaktiv cybersikkerhed?
  - **Reaktiv**: Gør noget, når skaden er sket.
  - **Proaktiv**: Gør noget før, at skaden indtræffer.
- Hvilke indsatser ville give mest værdi for BS Consulting A/S lige nu?

- Hvordan kan en virksomhed bruge IG-opdelingen til at prioritere sikkerhedsindsatser?

Ressourcer

- https://www.cisecurity.org/white-papers/cis-controls-v8

2026-02-19 12:04:53