Uge 11 – Logning, sporbarhed og sikkerhedshændelser

I denne uge skifter fokus fra *forebyggelse* til *observation og sporbarhed*.
I introduceres til logning som en **grundlæggende sikkerhedsmekanisme**, der understøtter governance, compliance, hændelseshåndtering og efterforskning.

Ugen danner det teoretiske og begrebsmæssige fundament for de kommende uger med **systemlogning, audit og SIEM/XDR**.

Forberedelse

- Se kolonen *Forberedelse og pædagogisk tilrettelæggelse* i planen på It's learning

♂ Øvelser

- Alle øvelser i denne uge gennemføres som **gruppeøvelser og diskussioner baseret på slides**

Læringsmål der arbejdes med i faget denne uge

Overordnede læringsmål fra studieordningen

Viden

Den studerende har viden om:

- Generelle governanceprincipper
- Relevante it-trusler
- Relevante sikkerhedsprincipper til systemsikkerhed

Færdigheder

Den studerende kan:

- Implementere systematisk logning og monitorering af enheder *(påbegyndt)*
- Analysere logs for incidents og følge et revisionsspor *(påbegyndt)*

Kompetencer

Den studerende kan:

- Udvælge og anvende praktiske mekanismer til detektion af it-sikkerhedsmæssige hændelser *(påbegyndt)*

Praktiske mål for ugen

- Den studerende kan redegøre for, hvornår der som minimum bør oprettes en loglinje
- Den studerende har en grundlæggende forståelse for log management

---

Afleveringer

- Ingen.

Skema

Tirsdag

Tid	Aktivitet
08:15	Introduktion til dagen
08:25	Gruppeøvelse: Hvad er sikkerhed?
08:35	Opsamling på gruppeøvelse
08:40	Oplæg: Hvornår skal der altid logges?
09:00	Gruppeøvelse: Sikkerhedskrav i en generisk webshop

Tid	Aktivitet
09:35	Opsamling på gruppeøvelse
09:45	Pause
10:00	Oplæg: Grundlæggende introduktion til log management
10:15	Gruppeøvelse: Log management
10:50	Opsamling på gruppeøvelse
11:00	Oplæg: CIA-T, Gold standards og logformater
11:30	Undervisning slut

Kommentarer

- Ugen fokuserer på **forståelse og vurdering**, ikke implementering.
- Begreber og krav fra denne uge anvendes direkte i de kommende uger med rsyslog, auditd og Wazuh.

Last update: 2026-03-20 13:58:28