Øvelse 1 – Fagets læringsmål

Information

Når vi påbegynder et nyt projekt eller en arbejdsøvelse, er det vigtigt først at forstå det overordnede formål. Det samme gør sig gældende for studerende, når de starter et nyt fag. Det vil sige: Hvad forventes det, at den studerende kan, når faget afsluttes?

Dette giver samtidig den studerende mulighed for at afgrænse sig, da et 10 ECTS-fag inden for IT-sikkerhed ofte har en stor faglig bredde. Hertil kommer, at de studieordninger, som beskriver de enkelte fag og deres læringsmål, ofte er skrevet abstrakt og ukonkret. Derfor skal den enkelte studerende selv tolke, hvad der menes, og sætte det i kontekst i forhold til den konkrete undervisning.

Dette kan skabe usikkerhed og tvivl om, hvad den studerende skal fokusere på i sit arbejde uden for øvelsestimerne, som kun udgør ca. 24 % af det forventede arbejde i faget.

I de følgende øvelser skal I arbejde med jeres **forståelse af studieordningens læringsmål**. Da læringsmålene kan være abstrakte og åbne for fortolkning, er det vigtigt, at I arbejder med dem i jeres teams, og at alle medlemmer bidrager med deres perspektiv.

Ved at anvende en struktureret tilgang sikrer I, at alle synspunkter bliver inddraget, og at der opnås en fælles og nuanceret forståelse af læringsmålene.

Den nationale studieordning kan findes på mitucl.dk

Instruktioner

1. Læs og reflekter over læringsmålene individuelt

Tidsestimat: 20 minutter

Hvert teammedlem skal individuelt læse og reflektere over studieordningens læringsmål for faget System sikkerhed.

2. Notér et konkret eksempel på hvert læringsmål

Tidsestimat: 20 minutter

Hvert teammedlem skal individuelt notere ét eller flere konkrete eksempler, der relaterer sig til hvert læringsmål.

Som 1. semester-studerende kan dette være svært. Der er ikke noget rigtigt eller forkert – det handler om, hvad du allerede ved, eller kan finde frem til.

3. Skab en fælles forståelse i gruppen

Tidsestimat: 30 minutter

Benyt en struktur, der sikrer, at alle gruppemedlemmers synspunkter bliver hørt. Del og diskuter de konkrete eksempler, der relaterer sig til hvert læringsmål – gerne flere eksempler pr. læringsmål.

4. Efter pausen: Del i Padlet

Tidsestimat: 15 minutter

Gruppen skal nu skrive udvalgte læringsmål og tilhørende konkrete eksempler ind i den fælles Padlet.

Herefter laver vi en fælles opsamling, hvor hvert team præsenterer deres eksempler i plenum.

Løsning

Viden

Den studerende:

- **Har viden om generelle governance-principper og sikkerhedsprocedurer**
  - Ansvarsfordeling, gennemsigtighed, risikostyring, compliance, kontrol og opfølgning
  - Standarder og rammeværk: ISO 27001, NIS2, GDPR, CIS18
  - Adgangsprocedurer
- **Har viden om metode og praksis inden for væsentlige forensic-processer**
  - Analyse af IT-udstyr som drives eller RAM
  - Identificering af en hændelse
  - Indsamling af data (sørge for, at det er sikkert)
  - Bevarelse af data (sørge for, at det ikke kan ændres)
  - Analyse af hændelsen (find spor og evt. sammenhænge)
  - Rapportering af alt ovenstående
- **Kan forstå og reflektere over relevante IT-trusler**
  - Kendskab til forskellige IT-trusler, fx phishing, malware, DDoS-angreb, insidertrusler osv.
- **Har kendskab til teorier, metode og praksis inden for sikkerhedsprincipper til systemsikkerhed**
  - CIA-triaden, Defense in Depth, Least Privilege

- **Kan forstå og reflektere over sikkerhedsprincipper til systemsikkerhed, herunder adgangskontrol**
  - Authentication, Authorization, Accounting (AAA)
- **Har viden om teorier, metode og praksis i forhold til sikkerhedsadministration i DBMS**
  - SQL Injection, backup, kryptering og rettigheder

Færdigheder

Den studerende:

- **Kan anvende metoder og redskaber til at implementere systematisk logning og monitorering af enheder**
  - Følge et benchmark for at sikre korrekt opsætning af enhederne
  - Analysere logs for hændelser
  - Udnytte modforanstaltninger til sikring af systemer
  - Hvordan logs indsamles, hvordan enheder konfigureres sikkert
  - Etablering af monitorering og alarmer
  - Forebyggelse og styrkelse af sikkerheden
- **Kan analysere logs for incidents og følge et revisionsspor**
  - Bruge SIEM-værktøjer
- **Kan anvende metoder og redskaber til at identificere forskellige typer af endpoint-trusler**
  - Vælge relevante løsningsmodeller for at fjerne eller afbøde trusler mod systemer
  - Genoprette systemer efter en hændelse
  - Opfange trusler på netværket og bestemme den bedste løsning for at undgå angreb
- **Kan formidle praksisnære problemstillinger og løsningsmuligheder til samarbejdspartnere og brugere**
  - Kunne kommunikere på et niveau, så alle kan være med
  - Arbejde på et højt abstraktionsniveau

Kompetencer

Den studerende:

- **Kan håndtere komplekse og udviklingsorienterede situationer i forhold til håndtering af enheder på command line-niveau**
  - Lære at bruge Linux command line til IT-sikkerhed

- **Kan selvstændigt indgå i fagligt og tværfagligt samarbejde og påtage sig ansvar inden for rammerne af professionel etik**
  - Udvælge, anvende og implementere praktiske mekanismer til at forhindre, detektere og reagere på specifikke IT-sikkerhedshændelser
  - Arbejde med og implementere SIEM-værktøjer
- **Kan håndtere værktøjer til at identificere og fjerne/afbøde forskellige typer af endpoint-trusler**
  - Anvende værktøjer som ThreatLocker eller andre Endpoint Protection-løsninger
- **Kan identificere egne læringsbehov og udvikle egen viden, færdigheder og kompetencer i relation til systemsikkerhed**
  - Arbejde selvstændigt og sikre egen læring

Ressourcer

- https://www.mitucl.dk/

2026-02-20 08:38:27