Statens Digitaliseringsakademi

Teknisk it-sikkerhed i staten

Teknisk it-sikkerhed i staten

Få dyb it-sikkerhedsteknisk viden via kontekstnære case-øvelser og eksempler fra en statslig virkelighed

Hvem er kurset for?

Kurset er for dig, der er sikkerhedsmedarbejder i en statslig myndighed. Du har erfaring med ISO 27001-området, og har dermed stiftet bekendtskab med fx risikostyring, beredskabsstyring og leverandørstyring.

Du har behov for mere it-sikkerhedsteknisk dybde i forhold til bl.a. sikkerhedsforanstaltninger og tekniske minimumskrav.

Varighed: 2 dage
Afholdelse: Fysisk i København
Pris: 3.300 kr. inkl. forplejning

I kan også bestille kurset til jeres kontor eller team for op til 25 medarbejdere til 67.175 kr.

Læs mere på digitaliseringsakademi.dk

Det får du på kurset

1. Evnen til at vurdere, udfordre og kvalitetssikre den konkrete implementering af de obligatoriske tekniske minimumskrav
2. Styrkelse af din forståelse for trusselsbilledet og de relevante aktører gennem arbejde med threat modelling
3. Forståelse for grundlæggende elementer og komponenter i sikkerhedsarkitekturen
4. Rustes til at indgå i et sikkerhedsteknisk leverandørsamarbejde og kunne stille de nødvendige krav
5. Indsigt i sikkerhedsforhold, udfordringer og muligheder når det kommer til brug af cloud
6. Styrkelse af din kommunikation med forretningen ved implementering af tekniske sikkerhedsforanstaltninger

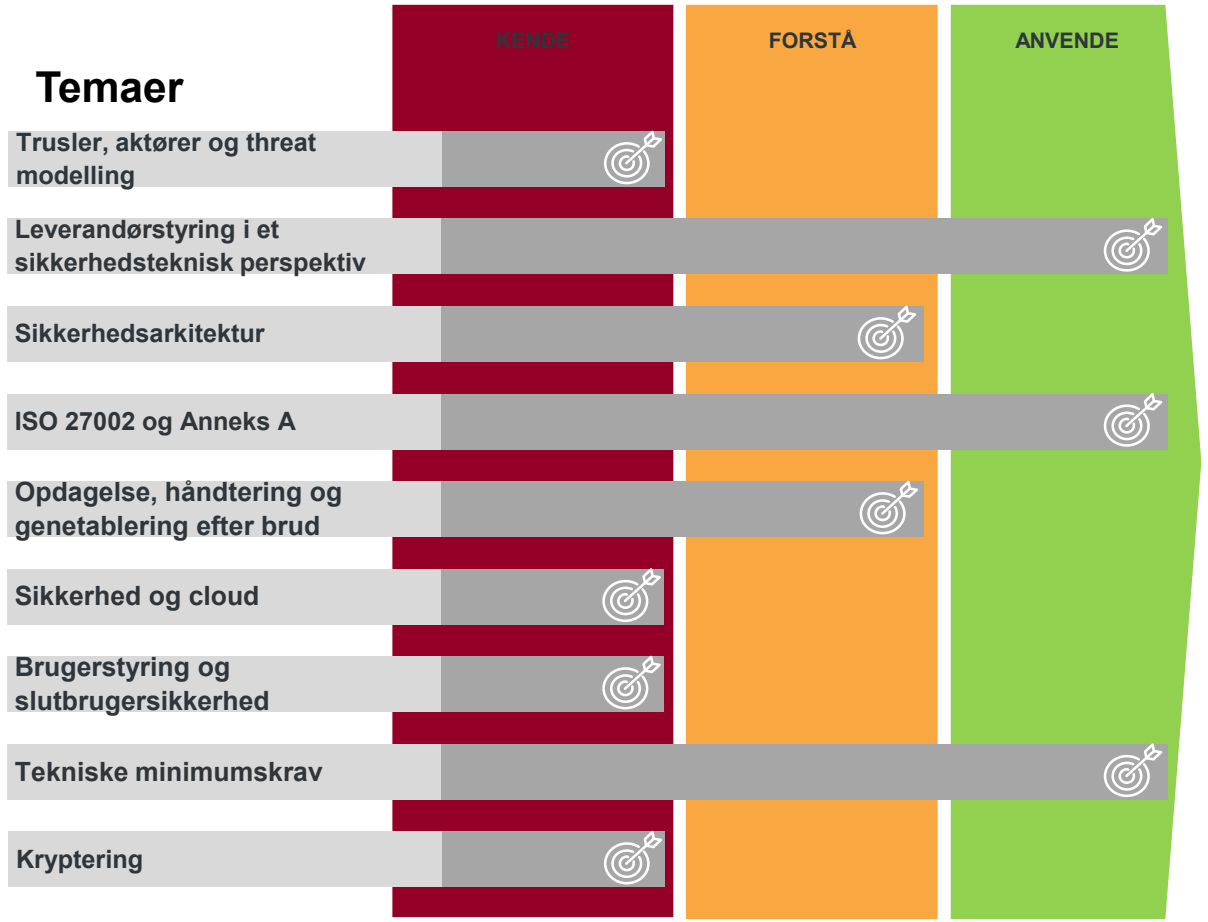
DIGITALISERINGSSTYRELSEN

Læringsmål og temaer

Overordnede læringsmål

- *Trusler og risikostyring*
  Kursusdeltagerne rustes til at forstå trusselsbilledet, inkl. aktørernes virkemidler. Deltagerne introduceres til og arbejder med metoder til threat modelling.
- *Teknisk it-sikkerhed i praksis*
  Kursusdeltagerne styrkes i at kunne løfte deres rolle og ansvar i arbejdet med teknisk it-sikkerhed i egen organisation. Deltagerne arbejder med bl.a. sikkerhedsarkitektur og kryptering.
- *Forberedelse og håndtering af krisesituationer*
  Kursusdeltagerne får en forståelse for organisering og nøgleaktiviteter inden for beredskabsplanlægning samt kendskab til de konkrete redskaber, til støtte af et samlet beredskab med særligt fokus på it-tekniske foranstaltninger, såsom brugerstyring og de 20 tekniske minimumskrav.

Læringstaksonomi



DIGITALISERINGSSTYRELSEN

Kursusprogram

Dag 1

01 Rammer for it-sikkerhed i staten
I første modul får deltagerne indsigt i de strategiske og lovgivningsmæssige rammer for it-sikkerhed i staten. Vi berører bl.a. ISO 27002, der er kommet i en dansk udgave i 2023 og kommer kort ind på NIS2 og dennes betydning.

02 Trusler, aktører og threat modelling
Her får deltagerne indsigt i den nyeste viden om trusler mod offentlige myndigheder. Der er særligt fokus på trusselsaktørerne og de virkemidler, de anvender gennem praktiske øvelser med threat modelling og Mitre ATTACK & DEFEND

03 Sikkerhedsarkitektur I
Efter frokost på dag 1 bliver deltagerne gennem forståelse for relevante sikkerhedsarkitekturer rustet til at være kravstillere og sparringspartnere til it-organisation og løsningsleverandør ved valg af sikkerhedsarkitekturer.

04 Opdagelse, håndtering & genetablering efter sikkerhedsbrud
Cybersikkerhedshændelser i kontinuerlig udvikling stiller nye og udvidede krav til deltagernes forståelse af den traditionelle håndtering af it-sikkerhedsbrud. Gennem praktiske og kontekstnære øvelser får deltagerne viden om kritiske processer og tekniske redskaber før, under og efter et sikkerhedsbrud uanset karakteren af sikkerhedsbruddet.

Dag 2

05 Brugerstyring og slutbrugersikkerhed
Vi bibringer i dette modul en forståelse for den traditionelle brugerlivscyklus og udvider den med håndtering af privilegerede adgange og multifaktorautentificering. Deltagerne arbejder videre med den fiktive statslige case-applikation fra dag 1 og designer brugerstyringen for denne.

06 Sikkerhedsarkitektur II: Kryptering
Deltagerne får her viden på højt niveau om, hvordan kryptering virker, og i hvilke situationer centrale krypteringsmetoder er effektive. Deltagerne bliver dermed i stand til at stille de rette krav til tekniske løsninger og infrastruktur.

07 Sikkerhedsarkitektur III: Cloud og sikkerhed
Gennem fortsat arbejde med den fiktive case-applikation, som nu er blevet flyttet til skyen, får deltagerne indsigt i cloud-sikkerhed i relation til sikkerhedsarkitektur, brugsmønstre og ikke mindst faldgruber.

08 Leverandørstyring i et sikkerhedsteknisk perspektiv
Som informationssikkerhedsmedarbejder i staten er det afgørende at kunne bidrage til en tilstrækkelig leverandørstyring på de tekniske områder – særligt på områder med stor innovation som fx cloud, IOT, virtualisering, containere og mobile løsninger.

09 Tekniske minimumskrav
Vi sætter deltagerne i stand til at evaluere og føre tilsyn med tilstrækkeligheden i opfyldelsen af de tekniske minimumskrav gennem en dyb og praktisk forståelse for kravene og implementeringen af dem.

DIGITALISERINGSSTYRELSEN

Kursusforløb

Overordnet opbygning

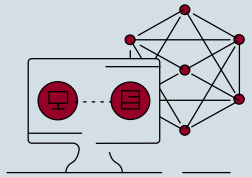
Før

Før første kursusdag forbereder deltagerne sig ved:

- Udfyldelse af læringskontrakt med egen leder og reflektere over målsætning ved at tage kurset
- Læse et par artikler med fagrelevante emner

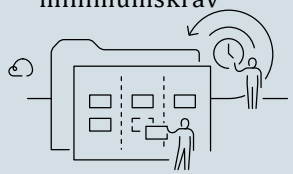
Dag 1

- Rammerne for it-sikkerhed i staten
- Trusler, aktører og threat modelling
- Sikkerhedsarkitektur
- Opdagelse, håndtering og genetablering efter sikkerhedsbrud



Dag 2

- Brugerstyring og slutbrugersikkerhed
- Kryptering
- Sikkerhed og cloud
- Leverandørstyring i et sikkerhedsteknisk perspektiv
- Tekniske minimumskrav



Efter

Efter kursusdagene understøttes det lærte igennem:

- Kursusbøger samt mail til deltagere med materialer
- Status på læringskontrakt med egen leder og refleksion om brug i egen organisation

DIGITALISERINGSSTYRELSEN