Kompetenceudvikling er vital for Forsvarets evne til at løse tidens og fremtidens opgaver.

UDDANNELSESBESKRIVELSE

FORSVARETS CYBERVÆRNEPLIGT

Uddannelsesbeskrivelse

Formål
Uddannelsen har til formål at give deltagerne en bred forståelse for cybernetværksopbygning, cybersikkersikkerhed og de værktøjer, der anvendes til at sikre og optimere IT-systemer. Deltagerne vil lære at arbejde med praktiske cybersikkerhedsløsninger, herunder implementering og administration af teknologier og metoder til sikring af cyberinfrastruktur Uddannelsen sætter deltagerne til effektivt at forebygge, detektere og håndtere cybertrusler, samtidig med at de opnår indsigt i de nyeste tendenser og udfordringer inden for cybersikkerhed.

Forudsætninger
- Basisuddannelse (Hæren, Søværnet eller Flyvevåbnet)
- Bestået matematik niveau E
- Bestået engelsk niveau E

Læringsudbytte
Efter endt uddannelse vil deltageren:

Viden
- Have viden om grundlæggende netværksprotokoller som IP, TCP/IP, DNS og DHCP samt deres anvendelse i kommunikation og datadeling.
- Have forståelse for principperne for netværksopbygning og serveradministration, herunder virtualisering og sikkerhedsforanstaltninger.
- Have forståelse for sårbarheder og trusler mod IT-systemer samt hvordan adfærd kan påvirke sikkerheden.
- Have forståelse for etiske hacking-metoder og sikkerhedskoncepter for at kunne evaluere og imødegå trusler.
- Have forståelse for procedurer og metoder til sikring af data og systemer i både Forsvarets og private enheder.
- Have viden om signalordrer, kaldesignaler (KALSIG), legitimationssystemer samt anvendelsen af alternative signalmidler.

Praktiske oplysninger

Udgivelsesdato
JAN 2025

Målgruppe
Værnepligtige der skal gennemføre Forsvarets cyberværnepligt

Niveau
Niveau 4
jf. kvalifikationsrammen for livslang læring

ECTS
Uddannelsen giver ikke ECTS point

Varighed
6 måneder fuldtid

Tilmelding
Via Forsvarets dag

Uddannelsesudbyder
Føringsstøtteregimentet

Kursusansvarlig
FSR/ITU
FIIN: FSR-KTP-3B-ITU

Formidler Q
- Q - 4147605 Cyberværnepligt
- Q - 3926447 Netværk 1 modul 2
- Q - 3936842 IT-supporter klargøring

Færdigheder

- Kunne opsætte og konfigurere sikkerhedsindstillinger på sociale medier, browsere, mobile enheder, hjemmeroutere og IoT-enheder.
- Kunne vælge og anvende værktøjer til netværksovervågning, identificere trusler og foretage analyser af netværks-data.
- Kunne vælge og anvende passende metoder til at konfigurere netværksløsninger, herunder VLAN, DHCP og firewall-opsætning.
- Kunne anvende PowerShell til automatisering og fjernadministration af servere og klienter.
- Kunne vælge og anvende passende metoder til at løse problemer relateret til brud på IT-sikkerheden samt kommunikere løsninger opad og nedad i organisationen.
- Kunne vælge og anvende forskellige sikkerhedsformer, herunder korrekt brug af SPR-radioer med V60-audiobokse og X5-headset, i overensstemmelse med gældende signalordrer (SIGO). Endvidere kunne afsende præcise meldinger inden for taktiske rammer, anvende relevante troppetegn og signaturer samt følge væsentlige forvaltningsprocedurer relateret til udstyret.

Kompetencer

- Kunne tage ansvar for planlægning og opsætning af netværks- og serverløsninger, der opfylder sikkerhedsmæssige krav.
- Kunne indgå i et tværfagligt samarbejde med kollegaer og organisationer om at imødegå sikkerhedstrusler og sikre systemer.
- Kunne planlægge og tage ansvar for udvikling af procedurer og arbejdsgange for at øge cybersikkerheden i organisationen.
- Kunne opsøge og anvende ny viden om trusler, tendenser og teknologier for at understøtte egen læring og udvikling.
- Kunne planlægge og tage ansvar for formidling af komplekse tekniske problemstillinger i en forståelig og anvendelig kontekst.
- Kunne tage ansvar for egen forebyggende vedligeholdelse, forskriftsmæssig opbevaring og anvendelse af signalmateriel samt tage initiativ til at skride ind, hvis bestemmelser for opbevaring og brug overskrides.

Indhold

- Introduktion til netværksopbygning og protokoller (IP, TCP/IP, DNS, DHCP).
- Grundlæggende serveradministration og virtualisering.
- Etisk hacking og penetrationstests.
- Opsætning af sikkerhedsindstillinger (VLAN, firewall, IoT-sikkerhed).
- Automatisering og scripting med PowerShell.
- Netværksovervågning med værktøjer som Wireshark, Snort og ELK.

- Q - 2543255 TASO Terminal Area Security Officer
- Q - 3195704 IT- og Cybersikkerhed
- Q - 3220359 CIS-grunduddannelse
- Q - 1637842 Signaluddannelse II

- Håndtering af brud på cybersikkerhed og risikostyring.
- Implementering af sikkerhedsprocedurer i organisationer.
- Introduktion til faget med repetition af grundlæggende VHF/UHF-antenneteori
- Gennemgang af SPR, V60 og X5
- Alternative signalmidler
- Signalordrer, kodepunkter og legitimationssystemer, samt troppetegn og signaturer

Studie- og arbejdsformer
Uddannelsen gennemføres som tilstedeværelse.

Uddannelsen veksler mellem følgende undervisningsformer:
- Klasseundervisning
- Foredrag
- Gruppearbejde
- Cases
- Praktiske øvelser
- E-læring

Prøver/eksamen/certificering
Prøveform: Praktisk summativ
Varighed: 5 dage
Bedømmelsesform: bestået / ikke bestået.
Beståelses kriterium: Evaluering af samlet resultat ifbm øvelsen.
Efter endt uddannelse tildeles følgende Q'er:
- Q-nr.: 4147605 Cyberværnepligt
- Q-nr.: 3926447 Netværk 1 modul 2
- Q-nr.: 3936842 IT-supporter klargøring
- Q-nr.: 2543255 TASO Terminal Area Security Officer
- Q-nr.: 3195704 IT- og Cybersikkerhed
- Q-nr.: 3220359 CIS-grunduddannelse
- Q-nr.: 1637842 Signaluddannelse II

Bemærkninger
Når deltageren har gennemført og bestået uddannelsen, vil deltageren kunne godskrives for følgende fag på data- og kommunikationsuddannelsen, trin 1:
- 17678 Netværk 1
- 16859 Serverteknologi – Linux
- 16858 Server administration og sikkerhed
- 16862 Server automatisering
- 16856 Server teknologi - databaseserver