STUDIEORDNING

for

Erhvervsakademiuddannelse i Operationel cybersikkerhed

Gældende fra 01.08.2025

Indhold

1. Uddannelsens mål for læringsudbytte 3
2. Uddannelsen indeholder 7 nationale fagelementer 3
   2.1. Forretningsforståelse 3
   2.2. Programmering 4
   2.3. Computerarkitektur 5
   2.4. Kommunikation og rapportering 7
   2.5. Automatisering og scripting 8
   2.6. Datasikkerhed 9
   2.7. Netværksarkitektur 10
3. Praktik 11
4. Krav til det afsluttende eksamensprojekt. 12
5. Regler om merit 12
6. Ikrafttrædelse 13

Denne nationale del af studieordningen for Erhvervsakademiuddannelsen i operationel cybersikkerhed er udstedt i henhold til § 21, stk. 1 i bekendtgørelse om tekniske og merkantile erhvervsakademiuddannelser og professionsbacheloruddannelser. Denne studieordning suppleres af institutionsdelen af studieordningen, som er fastsat af den enkelte institution, der udbyder uddannelsen.

Den nationale del er udarbejdet af uddannelsesnetværket for Professionsbachelor i Cybersikkerhed og godkendt af alle de udbydende institutioner.

1. Uddannelsens mål for læringsudbytte

Viden
Den uddannede har:

- viden om erhvervets praksis og central anvendt teori og metode inden for forebyggelse, identificering af og reaktion på cybersikkerhedstrusler, herunder governance og sikkerhedsprocedurer
- viden om erhvervets praksis og central anvendt teori og metode inden for organisationskultur og kommunikation samt designprincipper for strukturer, der fremmer cybersikkerhed
- forståelse for praksis og central anvendt teori og metode inden for cybersikkerhed samt forståelse for erhvervets anvendelse af teori og metode og de forskellige roller i en cybersikkerhedsorganisation

Færdigheder
Den uddannede kan:

- anvende centrale metoder og redskaber inden for forebyggelse, identificering af og reaktion på cybersikkerhedstrusler, og anvende de færdigheder, der knytter sig til beskæftigelse inden for cybersikkerhed
- vurdere praksisnære problemstillinger inden for cybersikkerhed samt opstille og vælge løsningsmuligheder
- formidle praksisnære problemstillinger og løsningsmuligheder inden for cybersikkerhed til samarbejdspartnere og brugere

Kompetencer
Den uddannede kan:

- håndtere udviklingsorienterede situationer inden for opsætning og drift af IT-systemer og strukturer, der fremmer cybersikkerhed i en organisation, samt implementering af foranstaltninger til at sikre data
- deltage i fagligt og tværfagligt samarbejde i forbindelse med udvikling, drift og compliance inden for cybersikkerhed med en professionel tilgang
- i en struktureret sammenhæng tilegne sig ny viden, færdigheder og kompetencer inden for cybersikkerhed

2. Uddannelsen indeholder 7 nationale fagelementer

2.1. Forretningsforståelse

Indhold
Fagelementet beskæftiger sig med generel virksomhedsforståelse og værdiskabelse i forretningen, herunder forskellige virksomhedstyper og deres værdikæder. Fagelementet arbejder med sammenhængen mellem forretning, informationsteknologi og cybersikkerhed.
Fagelementet introducerer til cybersikkerhedsmodenhed, inkl. governance og risikostyring, samt den cybersikkerhedsansvarliges rolle i organisationen.

Læringsmål for Forretningsforståelse

Viden
Den studerende har:

- udviklingsbaseret viden om organisationstyper og deres værdikæder, og hvordan cybersikkerhed påvirker virksomhedens økonomi og forretningsprocesser
- roller og ansvar i en organisation i relation til cybersikkerhed
- udviklingsbaseret viden om centrale begreber inden for risikostyring knyttet til arbejdet med cybersikkerhed i en organisation
- projektmodeller
- forståelse for praksis og anvendt teori og metode inden for forandringsledelse og kan reflektere over sikkerhedsmæssige problemstillinger i virksomheden.

Færdigheder
Den studerende kan:

- anvende metoder og redskaber til simpel modenhedsvurdering af en organisation og mestre en struktureret og risikobaseret tilgang til cybersikkerhed
- vurdere praksisnære og teoretiske problemstillinger relateret til risici samt begrunde og vælge relevante løsningsmodeller inden for risikohåndtering
- formidle praksisnære og faglige problemstillinger og løsninger vedrørende cybersikkerhed i en organisatorisk kontekst til samarbejdspartnere, brugere og interessenter

Kompetencer
Den studerende kan:

- håndtere komplekse og udviklingsorienterede situationer i forhold til at indgå i samspillet mellem IT-sikkerhed, politikker og IT-systemer i en organisation.
- selvstændigt indgå i fagligt og tværfagligt samarbejde og påtage sig ansvar inden for rammerne af en professionel etik i forhold til cybersikkerhedsarbejdet i en organisation
- identificere egne læringsbehov og udvikle egen viden, færdigheder og kompetencer i relation til den faglige sikkerhedsprofession i virksomheden

ECTS-omfang
Forretningsforståelse har et omfang på 10 ECTS-point

2.2. Programmering

Indhold:
Fagelementet beskæftiger sig med grundlæggende programmering i et programmeringssprog, som lever op til industriens standard indenfor scripting med et særligt henblik på cybersikkerhed. Herunder datatyper, datastrukturer, teori om fx operatorer, betingelser og kontrol-flow. Et yderligere fokus vil være på funktioner, parametre og inputvalidering. I fagelementet vil der desuden blive arbejdet med data fra f.eks. logfiler og databaser samt anvendelse af prædefinerede moduler og tredjepartsbiblioteker til løsning af specifikke problemstillinger. Der vil også være

fokus på selvstændig udvikling af værktøjer og programmer til analyse og håndtering af sådanne data. I fagelementet indgår dokumentation, der formidler funktionalitet og overleverer viden.

Læringsmål for Programmering

Viden
Den studerende har:

- udviklingsbaseret viden om grundlæggende datatyper og datastrukturer og forskelle på disse
- udviklingsbaseret viden om teori inden for programmering med fokus på scripting
- udviklingsbaseret viden om IT-udviklingsmiljøer og brug af disse
- forståelse for praksis og anvendt teori og metode inden for programmering, og kan reflektere over teknikker til at finde information til alternative løsninger

Færdigheder
Den studerende kan:

- anvende metoder og redskaber til behandling af I/O fra såvel lokale filer som eksterne databaser og forbindelser og mestre programmering og tilhørende værktøjer til bearbejdelse af data fra forskellige kilder
- anvende metoder og redskaber i programmeringssprog og mestre validering af input og håndtering af fejl
- vurdere praksisnære og teoretiske problemstillinger inden for valg af datatyper og moduler til en given problemstilling og begrunde og vælge relevante løsningsmodeller inden for programmering
- formidle og dokumentere praksisnære og faglige problemstillinger og løsninger vedrørende egne programmer og deres funktionalitet til samarbejdspartnere og brugere

Kompetencer
Den studerende kan:

- håndtere komplekse og udviklingsorienterede situationer i forhold til at udvikle og håndtere basale programmer.
- selvstændigt indgå i fagligt og tværfagligt samarbejde og påtage sig ansvar inden for rammerne af en professionel etik i forhold til udvikling af programmer og moduler, som kan anvendes af andre.
- identificere egne læringsbehov og udvikle egen viden, færdigheder og kompetencer i relation til at fremsøge og anvende relevante moduler i programmeringssprog

ECTS-omfang
Programmering har et omfang på 10 ECTS-point.

2.3. Computerarkitektur

Indhold:
Fagområdet beskæftiger sig med, hvordan de enkelte elementer i en computer, i form af hardware, operativsystem og software, interagerer med hinanden, samt deres funktioner og den betydning, funktionerne har på cybersikkerhed.

Læringsmål for Computerarkitektur

Viden
Den studerende har:

- udviklingsbaseret viden om arkitektur i IT-kontekst
- udviklingsbaseret viden om forskellige hardwaretyper, herunder CPU, hukommelse, lagring, og input output udstyr
- udviklingsbaseret viden om OS arkitektur, herunder kernel, shell, processer og services samt filsystemer
- viden om forskellige talsystemer
- forståelse for praksis og anvendt teori og metode inden for forskellige applikationstyper og deres arkitektur og kan reflektere over, hvilke behov de opfylder, og hvilke sikkerhedsudfordringer, de kan udgøre
- forståelse for praksis og anvendt teori og metode inden for Cloud arkitektur, herunder IaaS, PaaS og SaaS, og kan reflektere over de overvejelser, der gør sig gældende i et sikkerhedsperspektiv

Færdigheder
Den studerende kan:

- anvende metoder og redskaber til opsætning og anvendelse af operativsystemer og udvalgte applikationer i et virtuelt miljø og mestre installation af forskellige operativsystemer
- anvende metoder og redskaber til grundlæggende tiltag til autentificering og brugerstyring
- anvende metoder og redskaber til cloudløsning og mestre implementering af basale sikkerhedsforanstaltninger i forbindelse med løsningen
- vurdere praksisnære og teoretiske problemstillinger inden for arkitektur i relation til cybersikkerhed samt begrunde og vælge relevante løsningsmodeller inden for cloud eller andre typer af arkitektur
- formidle praksisnære og faglige problemstillinger og løsninger til samarbejdspartnere og brugere vedrørende cybersikkerhed i forbindelse med forskellige arkitekturelementer i operativsystemer, application deployment models samt proceskommunikation og -handlinger

Kompetencer
Den studerende kan:

- håndtere komplekse og udviklingsorienterede situationer i forhold til at opsætte et labmiljø til undersøgelse af relevante cybersikkerhedsmæssige problemstillinger.

- selvstændigt indgå i fagligt og tværfagligt samarbejde og påtage sig ansvar inden for rammerne af en professionel etik i forbindelse med udvælgelse og opbygning af relevant systemarkitektur
- identificere egne læringsbehov og udvikle egen viden, færdigheder og kompetencer i relation til computerarkitekturer i et cybersikkerhedsperspektiv

ECTS-omfang
Computerarkitektur har et omfang på 10 ECTS-point.

2.4. Kommunikation og rapportering

Indhold
Fagelementet beskæftiger sig med, hvordan man kommunikerer effektivt i en virksomhed om cybersikkerhed, både gennem opbygning af en cybersikkerhedskultur og cybersikkerhedstræning og gennem krisekommunikation. Fagelementet indeholder desuden dataindsamling, metrikker, visualisering, formidling og præsentation af cybersikkerhedsrapporter i en organisation, både mundtligt og skriftligt.

Læringsmål for Kommunikation og rapportering

Viden
Den studerende har:

- udviklingsbaseret viden om sikkerhedskommunikation og -rapportering i en virksomhed
- udviklingsbaseret viden om intern og ekstern hændelsesrapportering og krisekommunikation
- forståelse for praksis og anvendt teori og metode inden for indsamling og anvendelse af trusselsvurderinger og kan reflektere over kommunikative virkemidler og kanaler i relation til en virksomheds kultur og værdier

Færdigheder
Den studerende kan:

- anvende metoder og redskaber til data-drevet cybersikkerhed baseret på risici og trusler og mestre opbygning af hændelsesrapportering og krisekommunikation
- vurdere praksisnære og teoretiske problemstillinger relateret til at udarbejde og orientere om trusselsanalyse samt begrunde og vælge relevante løsningsmodeller inden for sikkerhedstiltag
- formidle praksisnære og faglige problemstillinger og løsninger vedrørende cybersikkerhed til relevante interne og eksterne målgrupper i mundtlige præsentationer og skriftlige rapporter

Kompetencer
Den studerende kan:

- håndtere komplekse og udviklingsorienterede situationer i forhold til at planlægge og gennemføre awareness aktiviteter, herunder udbrede en risikomodel i en organisation
- selvstændigt indgå i fagligt og tværfagligt samarbejde og påtage sig ansvar inden for rammerne af en professionel etik i forhold til at fremme en cybersikkerhedskultur i en organisation
- identificere egne læringsbehov og udvikle egen viden, færdigheder og kompetencer i relation til kommunikation og rapportering af cybersikkerhed

ECTS-omfang
Kommunikation og rapportering har et omfang på 10 ECTS-point.

2.5. Automatisering og scripting

Indhold:
Fagelementet har et fokus på indlæring og forståelse af programmeringsdelen af automatisering i et cybersikkerhedsperspektiv. Herunder indgår opbygning af services i forskellige operativsystemer, til f.eks. monitorering eller gentagne operationer, som man gerne vil sikre kører uden brugerinput. I dette fagelement vil der ydermere være et fokus på brug af terminalværktøjer, såsom shell, PowerShell og lignende, for at skabe fortrolighed i denne interaktion mellem terminal og operativsystem. Der vil også være et område af fagelementet, der beskæftiger sig med dokumentationen af disse automatiseringsløsninger.

Læringsmål for Automatisering og scripting

Viden
Den studerende har:

- udviklingsbaseret viden om terminalværktøjer i forskellige operativsystemer
- udviklingsbaseret viden om indbyggede værktøjer til automatisering i operativsystemer
- udviklingsbaseret viden om serialisering
- forståelse for praksis og anvendt teori og metode inden for opbygning af services i et operativsystem og kan reflektere over manuelle løsningers egnethed til automatisering i et sikkerhedsperspektiv

Færdigheder
Den studerende kan:

- anvende metoder, redskaber og relevante moduler til automatisering af sikkerhedstiltag og mestre løsning af problemstillinger inden for domænet ved anvendelsen af en terminal
- vurdere praksisnære og teoretiske problemstillinger vedrørende tredjepartsmoduler samt begrunde og vælge relevante løsningsmodeller inden for scripting og automatisering
- formidle og dokumentere praksisnære og faglige problemstillinger og løsninger vedrørende automatiseringstiltag til samarbejdspartnere og brugere

Kompetencer
Den studerende kan:

- håndtere komplekse og udviklingsorienterede situationer i forhold til at benytte terminalværktøjer i gængse operativsystemer
- håndtere komplekse og udviklingsorienterede situationer i forhold til udvikling og konfiguration af nye automatiseringsforslag til gængse operativsystemer
- selvstændigt indgå i fagligt og tværfagligt samarbejde og påtage sig ansvar inden for rammerne af en professionel etik ved udvikling af automatiseringsforslag, som kan anvendes af andre
- identificere egne læringsbehov og udvikle egen viden, færdigheder og kompetencer i relation til at fremsøge og anvende relevante automatiseringsløsninger

ECTS-omfang
Automatisering og scripting har et omfang på 5 ECTS-point.

2.6. Datasikkerhed

Indhold:
Fagelementet beskæftiger sig med lokale og eksterne datalagringssystemer såsom cloud. Der vil i dette fagelement være et fokus på forskellige tiltag og værktøjer man kommer i berøring med i forbindelse med sikring af data samt vurdering af konsekvensen ved brug af disse. Dette indebærer blandt andet et fokus på sikkerhedsparadigmer og sikkerhedsprincipper - herunder CIA-triaden, som er et gennemgående sikkerhedsparadigme på hele uddannelsen – men også principper såsom Least Privilege og Defense In Depth. Der vil i fagelementet ydermere indgå teori om kryptografi, såsom forskellen på hashing og kryptering, og best practices indenfor krypteringsstandarder, samt relevante sårbarheder i forbindelse med backup og databaseløsninger som fx injection.

Læringsmål for Datasikkerhed

Viden
Den studerende har:

- udviklingsbaseret viden om grundlæggende sikkerhedsparadigmer
- udviklingsbaseret viden om forskelle mellem lokal og ekstern lagring
- udviklingsbaseret viden om sikkerhedsdesign-principper
- udviklingsbaseret viden om sårbarheder i forbindelse med lagring og sikring af data
- forståelse for praksis og anvendt teori og metode inden for datasikkerhed og kan reflektere over best practices indenfor sikring af data som kryptering og hashing

Færdigheder
Den studerende kan:

- anvende metoder og redskaber til ekstern lagring af data og mestre tiltag til adgangskontrol, både lokalt og i cloud

- vurdere praksisnære og teoretiske problemstillinger i relation til CIA eller lignende samt begrunde og vælge relevante løsningsmodeller inden for krypteringstiltag til sikring af data
- formidle praksisnære og faglige problemstillinger og løsninger vedrørende datasikkerhed og tilhørende valg af tiltag til samarbejdspartnere og brugere

Kompetencer
Den studerende kan:

- håndtere komplekse og udviklingsorienterede situationer i forhold til at vurdere og udvælge metoder til sikring af data i et givent system, herunder værktøjer til adgangskontrol både lokalt og i cloud
- selvstændigt indgå i fagligt og tværfagligt samarbejde og påtage sig ansvar inden for rammerne af en professionel etik i forbindelse med sikring af data
- identificere egne læringsbehov og udvikle egen viden, færdigheder og kompetencer i relation til best practice inden for datasikkerhed.

ECTS-omfang
Datasikkerhed har et omfang på 5 ECTS-point.

2.7. Netværksarkitektur

Indhold:

Fagelementet beskæftiger sig med netværksudstyr og komponenter og de forskellige udfordringer i netværk knyttet til cybersikkerhed, herunder specificering af relevante sikkerhedskrav til en netværksløsning i cloud- og hybridmiljø. Fagelementet beskæftiger sig med praktisk opsætning, drift og sikring af mindre netværk.

Læringsmål for Netværksarkitektur

Viden

Den studerende har:

- udviklingsbaseret viden om OSI modellen eller tilsvarende reference model
- udviklingsbaseret viden om adressering i de forskellige lag
- udviklingsbaseret viden om relevante netværksprotokoller
- udviklingsbaseret viden om subnetting og routing/segmentering
- udviklingsbaseret viden om netværksudstyr og komponenter
- forståelse for praksis og anvendt teori og metode inden for netværksanalyse og kan reflektere over forskellige sikkerhedsudfordringer i netværk

Færdigheder

Den studerende kan:

- anvende metoder og redskaber til netværksanalyse og mestre opsætning, fejlfinding og tiltag til sikring af mindre netværk

- vurdere praksisnære og teoretiske problemstillinger i forhold til sikkerhedskrav til netværk samt begrunde og vælge relevante løsningsmodeller inden for specificering og deployment af netværksløsninger, herunder i cloud- og hybridmiljø
- formidle praksisnære og faglige problemstillinger og løsninger vedrørende specifikation og dokumentation af sikkerhedskrav til samarbejdspartnere og brugere

Kompetencer

Den studerende kan:

- håndtere komplekse og udviklingsorienterede situationer i forhold til at designe, herunder opdele, simple netværk i segmenter ved brug af netværksudstyr
- håndtere komplekse og udviklingsorienterede situationer i forbindelse med analyse af netværkstrafik med henblik på at forebygge eller afbøde angreb
- selvstændigt indgå i fagligt og tværfagligt samarbejde og påtage sig ansvar inden for rammerne af en professionel etik i forhold til design, opsætning og konfigurering af simple netværk
- identificere egne læringsbehov og udvikle egen viden, færdigheder og kompetencer i relation til protokoller og netværksarkitekturer

ECTS-omfang
Netværksarkitektur har et omfang på 10 ECTS-point.

3. Praktik

Læringsmål for praktikken på uddannelsen

Viden

Den studerende har:

- udviklingsbaseret viden om praktikvirksomhedens praksis samt central anvendt teori og metode inden for praktikfunktionen og operationel cybersikkerhed forståelse for erhvervets og operationel cybersikkerheds anvendelse af teori, metode og redskaber i forhold til praksis i relation til praktikopholdet.

Færdigheder

Den studerende kan:

- anvende alsidige tekniske og analytiske arbejdsmetoder, der knytter sig til beskæftigelse inden for erhvervet i relation til praktikopholdet
- vurdere praksisnære problemstillinger og opstilling af løsningsmuligheder i relation til praktikopholdet
- formidle praksisnære problemstillinger og begrundede løsningsforslag inden for operation cybersikkerhed i relation til praktikopholdet

Kompetencer

Den studerende kan:

- varetage udviklingsorienterede situationer og planlægning af daglige arbejdsopgaver i relation til praktikopholdet inden for operationel cybersikkerhed
- deltage i fagligt og tværfagligt samarbejde med en professionel tilgang i relation til praktikopholdet
- tilegne sig ny viden, færdigheder og kompetencer i relation til praktikopholdets opgaver inden for operationel cybersikkerhed

ECTS-omfang
Praktikken har et omfang på 20 ECTS-point.

Antal prøver
Praktikken afsluttes med 1 prøve.

4. Krav til det afsluttende eksamensprojekt.

Det afsluttende eksamensprojekt dokumenterer sammen med uddannelsens øvrige prøver og praktikprøven, at uddannelsens mål for læringsudbytte er opnået.

Det afsluttende eksamensprojekt skal endvidere dokumentere den studerendes forståelse af praksis og central anvendt teori og metode i relation til en praksisnær problemstilling. Problemstillingen skal tage udgangspunkt i en konkret opgave inden for uddannelsens område. Problemstillingen, der skal være central for uddannelsen og erhvervet, formuleres af den studerende, eventuelt i samarbejde med en privat eller offentlig virksomhed. Institutionen skal godkende problemstillingen.

Prøven i det afsluttende eksamensprojekt
Eksamensprojektet afslutter uddannelsen, når alle forudgående prøver er bestået.

ECTS-omfang
Det afsluttende eksamensprojekt har et omfang på 10 ECTS-point.

Prøveform
Prøven består af et projekt og en mundtlig del. Prøven er med ekstern censur, og der gives en samlet individuel karakter efter 7-trin skalaen for projektet og den mundtlige del.

5. Regler om merit

Beståede uddannelseselementer ækvivalerer de tilsvarende uddannelseselementer ved andre uddannelsesinstitutioner, der udbyder uddannelsen.

Den studerende har pligt til at oplyse om gennemførte uddannelseselementer fra en anden dansk eller udenlandsk videregående uddannelse og om beskæftigelse, der må antages at kunne give merit.

Uddannelsesinstitutionen godkender i hvert enkelt tilfælde merit på baggrund af gennemførte uddannelseselementer og beskæftigelse, der står mål med fag, uddannelsesdele og praktikdele.

Afgørelsen træffes på grundlag af en faglig vurdering.

Den studerende har ved forhåndsgodkendelse af studieophold i Danmark eller udlandet pligt til efter endt studieophold at dokumentere det godkendte studieopholds gennemførte uddannelseselementer.

Den studerende skal i forbindelse med forhåndsgodkendelsen give samtykke til, at institutionen efter endt studieophold kan indhente de nødvendige oplysninger.

Ved godkendelse efter ovenstående anses uddannelseselementet for gennemført, hvis det er bestået efter reglerne om den pågældende uddannelse.

6. Ikrafttrædelse

Denne nationale del af studieordningen træder i kraft den 01.08.2025

Studieordningen gælder for alle studerende på uddannelsen fra ikrafttrædelsesdatoen.