ERHVERVSAKADEMI
AARHUS

STUDIEORDNING

for

Professionsbachelor it-sikkerhed

Del III: Valgfagskatalog

Ikrafttrædelse: 25.01.2023

Indhold

Denne studieordning skal læses i sammenhæng med den nationale del af studieordningen og den lokale del af studieordningen. Den nationale del af studieordningen er fælles for alle udbydere, mens den lokale del af studieordningen samt valgfagskataloget er fastlagt af Erhvervsakademi Aarhus.

1. Valgfagskatalog

På uddannelsen er der 15 ECTS valgfag. Valgfag, læringsmål og bedømmelseskriterier for de udbudte fag er beskrevet i dette valgfagskatalog.

Følgende valgfag udbydes:

- Netværkspenetrationstest (5 ECTS)
- Data science for it-sikkerhed (5 ECTS)
- SIEM og loganalyse (5 ECTS)
- Hændelses- og trusselshåndtering (5 ECTS)
- Industriel informationssikkerhed (5 ECTS)

De studerende kan følge valgfag på andre institutioner mod selv at afholde udgifter til transport, overnatning mv.

Sommerskole og vinterskole
Det er også muligt at vælge sommerskole eller vinterskole som valgfag. Den valgte sommer- eller vinterskole skal godkendes af uddannelsesledelsen på uddannelsen inden afrejse, hvorved forhåndsmerit kan opnås. Ved godkendelse af forhåndsmerit anses uddannelseselementet for gennemført, hvis det er bestået efter reglerne om uddannelsen.

Internationalt kontor kan kontaktes for yderligere information.

2. Prøver i valgfag

Ved begyndelse på et uddannelseselement, semester mv. er det samtidig automatisk tilmelding til de tilhørende prøver. Ved tilmelding bruges en prøvegang. Dette gælder dog ikke, hvor den studerende bliver forhindret i at deltage i prøven på grund af dokumenteret sygdom og barsel.

Det er altid den studerendes ansvar at sikre sig internetadgang i eksamenssituationen, og at den studerendes pc er funktionsdygtig.

Prøverne er altid på dansk, medmindre det er en del af den enkelte prøves formål at dokumentere færdigheder i fremmedsprog. Prøverne kan aflægges på svensk eller norsk i stedet for dansk, medmindre prøvens formål er at dokumentere den studerendes færdigheder i dansk.

2.1. Fuldførelse af prøver

Generelt for prøverne på uddannelsen gælder nedenstående i forhold til, hvornår en eksamen er fuldført, eller der er brugt et eksamensforsøg. Hvis der er afvigelser for en bestemt prøve, vil det fremgå af den enkelte beskrivelse af prøven nedenfor.

Ikke-bestået eksamen
Hvis en studerende ikke har opnået karakteren 02 eller derover til en mundtlig eller skriftlig prøve eller en kombination heraf, er prøven ikke bestået, og der er brugt et prøveforsøg.

Hvis eksamensprojektet er udarbejdet af en enkelt studerende og ikke bestås, kan den studerende vælge at arbejde videre på det eksisterende projekt eller udarbejde et nyt projekt.

Er der tale om en studerende, der har deltaget i et gruppeprojekt, og som ikke opnår karakteren 02 eller derover, kan den studerende skrive de afsnit om, som den studerende har udarbejdet af det fælles projekt, hvis det er individualiseret. Den studerende kan også vælge at skrive et nyt projekt alene, hvor reglerne for omfang, krav og retningslinjer for individuelt udarbejdede projekter gælder.

Ikke afleveret projekt/skriftlig besvarelse
Hvis den studerende ikke har afleveret sit eksamensprojekt eller skriftlige besvarelse, er der brugt et prøveforsøg.

Den studerende kan vælge at arbejde videre på det eksisterende projekt eller udarbejde et nyt projekt.

Ikke deltaget i eksamen/eksamination
Hvis den studerende har afleveret sit eksamensprojekt eller skriftlige besvarelse, men ikke har deltaget i den mundtlige eksamination, er der brugt et prøveforsøg.

Der vil hurtigst muligt blive planlagt en ny mundtlig eksamination for den studerende, hvor den studerende vil blive eksamineret i det allerede afleverede projekt.

Syge- og omprøver
De konkrete frister fremgår under den enkelte prøvebeskrivelse.

Orientering om tid og sted for syge- og omprøver findes på Studieupdate. Tidspunktet kan være identisk med næste ordinære prøve. Den studerende skal selv orientere sig om, hvornår syge- og omprøve afholdes.

Sygeprøve
En studerende, der har været forhindret i at gennemføre en prøve på grund af dokumenteret sygdom eller af anden uforudseelig grund, får mulighed for at aflægge (syge)prøven snarest muligt. Er det en prøve, der er placeret i uddannelsens sidste eksamenstermin, får den studerende mulighed for at aflægge prøven i samme eksamenstermin eller i umiddelbar forlængelse heraf.

Sygdom skal dokumenteres ved lægeerklæring. Institutionen skal senest have modtaget lægeerklæring tre hverdage efter prøvens afholdelse. Studerende, der bliver akut syge under en prøves afvikling, skal dokumentere at vedkommende har været syg på den pågældende dag.

Dokumenteres sygdom ikke efter ovenstående regler, har den studerende brugt et prøveforsøg. Den studerende skal selv betale udgifter til en lægeerklæring. Krav til udformning af lægeerklæring findes på hjemmesiden under 'Værd at vide om eksamen'.

Omprøve

Ved en ikke-bestået prøve eller et manglende fremmøde ved en prøve, er den studerende automatisk tilmeldt omprøve, så længe der resterer prøveforsøg. Den studerende er tilmeldt den førstkommende afholdelse af prøven. Omprøven kan være identisk med næste ordinære prøve.

Uddannelsen kan dispensere fra den fortsatte tilmelding til en eksamen, når det er begrundet i usædvanlige forhold, herunder dokumenteret handicap.

3. Valgfag på uddannelsen

3.1. Netværkspenetrationstest

Indhold

Netværkspenetrationstest omhandler hele processen med at indsamle viden om målet, som skal testes for sikkerhedshuller, til udførelsen af selve testen og afrapportering af resultaterne heraf. Der arbejdes med klassiske såvel som nyere sårbarheder, og hvordan disse kan udnyttes af trusselsaktører. Derudover arbejdes der med etiske spørgsmål omkring indtrængen i systemer, samt hvordan en organisation kan bruge resultaterne fra en penetrationstest.

Læringsmål

Viden

Den studerende har:

- Udviklingsbaseret viden om forskellige typer af angreb, og hvordan disse kan mitigeres i praksis, samt anvendt teori og metoder i forhold til scanning af netværk og systemer, og udnyttelse af sårbarheder til at trænge ind i et system.
- Forståelse for praksis og anvendt teori om kontraktuelle forhold ved en penetrationstest.

Færdigheder

Den studerende kan:

- Anvende fagområdets metoder og redskaber og mestre de færdigheder, der knytter sig til beskæftigelse inden for professionen som penetrationstester, herunder indsamling af data om et givent mål, finde sårbarheder i et givet system, udarbejdning af en angrebsplan ud fra indsamlede oplysninger om et mål og udførelse af penetrationstests.

- Vurdere praksisnære og teoretiske problemstillinger omkring identificerede sårbarheder, samt begrunde og vælge relevante løsningsmodeller for mitigering af fundne sårbarheder.
- Formidle praksisnære og faglige problemstillinger til samarbejdspartnere og kunder gennem dokumentation og afrapportering.

Kompetencer
Den studerende kan:

- Håndtere komplekse og udviklingsorienterede situationer i forbindelse med planlægning og eksekvering af penetrationstests.
- Selvstændigt indgå i fagligt og tværfagligt samarbejde og påtage sig ansvar inden for rammerne af en professionel etik.
- Identificere egne læringsbehov og udvikle egen viden, færdigheder og kompetencer i relation til professionen.

ECTS-omfang
Fagelementet Netværkspenetrationstest har et omfang på 5 ECTS-point.

Prøveform og tilrettelæggelse
Prøven er en individuel mundtlig prøve med afsæt i en individuel skriftlig rapport på baggrund af en individuel praktisk prøve.

Den skriftlige rapport
Den første del af prøven består af en individuel praktisk prøve i netværkspenetrationstest, hvori den studerendes resultater dokumenteres i en rapport på maksimalt 10 normalsider. Den praktiske prøve foregår 1 - 2 uger før eksamen, og udføres individuelt uden observation

Den individuelle mundtlige prøve
Den individuelle mundtlige prøve har et omfang af 25 minutter, som fordeles som følger:

- Ca. 10-12 minutter hvor den studerende præsenterer hovedpunkter i rapporten
- ca. 8-10 minutters eksamination
- 5 minutter votering.

Forudsætninger for at gå til eksamen– deltagelsespligt og aflevering
For at gå til den mundtlige del af prøven skal indholdet af den individuelle skriftlige opgave være redeligt. Opgaven skal opfylde formkrav samt være korrekt og rettidig afleveret (se Canvas).

Bedømmelseskriterier og censurtype

Bedømmelseskriterierne for prøven er lig med læringsmålene for valgfaget. Bedømmelse sker på baggrund af en helhedsvurdering af den individuelle skriftlige opgave og mundtlige præstation ved eksamen. Bedømmelse sker efter 7-trinsskalaen, og der er intern censur.

3.2. Data Science for IT-sikkerhed

Indhold
Data science for it-sikkerhed handler om, hvordan man udvælger og forbereder data til *machine learning*-modeller samt anvendelsen af disse modeller. Modellerne afprøves i praksis på datasæt som relaterer sig til forskellige grene af it-sikkerhed, såsom mail og netværkstrafik. Der arbejdes med, hvordan modeller kan klassificere f.eks. spam-mail og ondsindet trafik på netværket. Fagelementet har fokus på, hvordan man kan evaluere, udvælge og anvende metoder inden for data science på IT-sikkerhedsmæssige områder, herunder netværks intrusion detection system (NIDS).

Læringsmål
Viden
Den studerende har:

- Udviklingsbaseret viden til dataforberedelse, dataanalyse og datavisualisering samt anvendt teori og metoder hertil.
- Forståelse for praksis, anvendt teori og metode i relation til modeller til kategorisering, herunder machine learning, og kan reflektere over professionens praksis og anvendelse af teori og metode.

Færdigheder
Den studerende kan:

- Anvende fagområdets metoder og redskaber til at forberede data til machine learning, analysere og visualisere data og anvende et konkret machine learning framework på praktiske problemstillinger inden for it-sikkerhed.
- Vurdere praksisnære og teoretiske problemstillinger inden for brugen af machine learning til it-sikkerhed samt begrunde og vælge relevante løsningsmodeller hertil.
- Formidle praksisnære og faglige problemstillinger og løsninger til samarbejdspartnere og brugere.

Kompetencer
Den studerende kan:

- Håndtere komplekse og udviklingsorienterede situationer i forhold til udvælgelse og anvendelse af passende machine learning-modeller til løsninger af konkrete problemstillinger inden for it-sikkerhed.

- Selvstændigt indgå i fagligt og tværfagligt samarbejde og påtage sig ansvar for valg af machine learning til it-sikkerhed inden for rammerne af en professionel etik.
- Identificere egne læringsbehov og udvikle egen viden, færdigheder og kompetencer i relation til professionelt arbejde i spændingsfeltet mellem machine learning og it-sikkerhed.

ECTS-omfang
Fagelementet Data Science i IT-sikkerhed har et omfang på 5 ECTS-point.

Prøveform og tilrettelæggelse herunder evt. formkrav
Prøven er en individuel mundtlig prøve med afsæt i en individuel praktisk prøve, hvor den studerende skal dokumentere sine resultater i en individuelt udarbejdet rapport på maksimalt 10 normalsider.

Den individuelle mundtlige prøve har et omfang af 25 minutter, som fordeles som følger:

- Ca. 10-12 minutter hvor den studerende præsenterer hovedpunkter i rapporten
- ca. 8-10 minutters eksamination
- 5 minutter votering.

Forudsætninger for at gå til eksamen – deltagelsespligt og aflevering
For at gå til den mundtlige del af prøven skal indholdet af den individuelle skriftlige opgave være redeligt. Opgaven skal opfylde formkrav samt være korrekt og rettidig afleveret (se Canvas).

Bedømmelseskriterier og censurtype
Bedømmelseskriterierne for prøven er lig med læringsmålene for valgfaget. Bedømmelse sker på baggrund af en helhedsvurdering af den individuelle skriftlige opgave og mundtlige præstation ved eksamen. Bedømmelse sker efter 7-trinsskalaen, og der er intern censur.

3.3. SIEM og loganalyse

Indhold
SIEM og loganalyse omhandler indsamling, administration, håndtering og søgning i logdata i gængse IT-systemer til overvågning, proaktiv håndtering og fejlfinding i forhold til at imødegå sikkerhedstrusler og hændelser.

Læringsmål for SIEM og Loganalyse

Viden
Den studerende har:

- Udviklingsbaseret viden om typiske arkitekturer og værktøjer til logning og Security Information and Event Management (SIEM), samt logformater og -typer til standardsystemer og juridiske krav til logning og bevarelse af data i forbindelse med forensic analyse.
- Forståelse for praksis, anvendt teori og metode om SIEM og loganalyse og kan reflektere over professionens praksis og anvendelse af metode og teori.

Færdigheder
Den studerende kan:

- Anvende fagområdets metoder og redskaber til at lave en baseline-analyse af en infrastruktur, bruge logdata til at identificere infrastrukturkomponenter og analysere logdata og netværkstrafik til at finde sikkerhedshændelser.
- Vurdere praksisnære og teoretiske problemstillinger omkring auditering og logning af data samt begrunde og vælge relevante løsninger.
- Formidle praksisnære og faglige problemstillinger og løsninger til samarbejdspartnere og brugere.

Kompetencer
Den studerende kan:

- Håndtere komplekse og udviklingsorienterede situationer omkring opsætning af SIEM-løsninger på tværs af produkter, herunder udvikling af dashboards, der viser tegn på hændelser.
- Selvstændigt indgå i fagligt og tværfagligt samarbejde, herunder påtage sig ansvaret for SIEM-løsninger og træffe beslutninger om. hvilke data der skal indsamles i en given situation inden for rammerne af en professionel etik.
- Identificere egne læringsbehov indenfor SIEM og loganalyse og udvikle egen viden, færdigheder og kompetencer i relation til professionen.

ECTS-omfang
Fagelementet SIEM og loganalyse har et omfang på 5 ECTS-point.

Prøveform og tilrettelæggelse
Prøven består af en individuel mundtlig eksamen som tager udgangspunkt i en individuelt udarbejdet skriftlig synopsis på baggrund af en udleveret case samt et trækspørgsmål uden forberedelse til eksamen.

Den skriftlige synopsis
Synopsen udarbejdes på baggrund af en udleveret case. Synopsen må maksimalt fylde 4 normalsider og skal udarbejdes individuelt.

Den individuelle mundtlige prøve
Den individuelle mundtlige eksamen har et omfang af i alt ca. 30 minutter, som fordeles som følger:

- 5-7 minutter, hvor den studerende præsenterer synopsen
- 8-10 minutters diskussion og spørgsmål vedrørende indhold i den studerendes oplæg.
- 10-12 minutter: Den studerende trækker et spørgsmål vedr. fagelementets læringsmål.
- 5 minutters votering.

Forudsætninger for at gå til eksamen– deltagelsespligt og aflevering
For at gå til den mundtlige del af prøve skal indholdet af den skriftlige opgave være redeligt. Opgaven skal opfylde formkrav samt være korrekt og rettidig afleveret (se Canvas).

Bedømmelseskriterier og censurtype
Bedømmelseskriterier for prøven er lig med læringsmål for det valgfrie uddannelseselement. Bedømmelsen er en helhedsvurdering af den skriftlige synopsis samt den studerendes præstation ved den mundtlige eksamen, dvs. såvel præsentation, diskussion samt besvarelse af trækspørgsmål. Bedømmelse sker efter 7-trinsskalaen, og der er intern censur.

3.4. Hændelses- og trusselshåndtering

Indhold
Hændelses- og trusselshåndtering handler om, hvordan man opdager, efterforsker, inddæmmer og genopretter infrastrukturer efter en sikkerhedshændelse, samt hvordan man leder efter eventuelle nye trusler. Der er fokus på relevante værktøjer og metoder til at indsamle, bevare, bearbejde og analysere digitale beviser i forbindelse med afhjælpning af sikkerhedshændelser og til støtte for fremtidige undersøgelser.

Læringsmål for hændelses- og trusselshåndtering

Viden
Den studerende har:

- Udviklingsbaseret viden om taktikker, teknikker og procedurer som anvendes af nutidens trusselsaktører samt grundprincipper og processer i efterforskning på IT-udstyr og forbindelsen til hændelseshåndtering.
- Forståelse for praksis, anvendt teori og metode i forbindelse med hændelses- og trusselshåndtering, samt kan reflektere over professionens praksis og anvendelse af teori og metode.

Færdigheder
Den studerende kan:

- Anvende fagområdets metoder og redskaber til at søge efter indikatorer på, at der er sket et sikkerhedsbrud, samt kan identificere brugeraktivitet og analysere endpoints og netværkstrafik.
- Vurdere om der er sket sikkerhedsbrud samt begrunde og vælge relevante metoder til hændelseshåndtering.
- Formidle resultater af analysen i form af ekspertrapporter til kunder og relevante brugere.

Kompetencer
Den studerende kan:

- Håndtere komplekse og udviklingsorienterede situationer i relation til håndtering af hændelser og trusler inden for it-sikkerhed.
- Selvstændigt indgå i fagligt og tværfagligt samarbejde omkring håndtering af trusler og hændelser og påtage sig ansvar for løsninger inden for rammerne af en professionel etik.
- Identificere egne læringsbehov og udvikle egen viden, færdigheder og kompetencer i relation til trussels- og hændelseshåndtering.

ECTS-omfang
Fagelementet Hændelses- og trusselshåndtering et omfang på 5 ECTS-point.

Prøveform og tilrettelæggelse
Eksamen består af en individuel mundtlig eksamen med afsæt i en skriftlig rapport.

Den skriftlige rapport
Rapporten må have et omfang af max 10 normalsider. Rapporten skal udarbejdes individuelt af den studerende.

Den individuelle mundtlige eksamen
Den individuelle mundtlige eksamen har et omfang af 30 minutter, som fordeles som følger:

- 8-10 minutter: Den studerende præsenterer rapporten
- 15-17 minutter: Diskussion og eksamination vedrørende rapporten samt spørgsmål vedrørende fagets læringsmål
- 5 minutter: votering.

Forudsætninger for at gå til eksamen– deltagelsespligt og aflevering
For at gå til den mundtlige del af prøven skal indholdet af den skriftlige opgave være redeligt. Opgaven skal opfylde formkrav samt være korrekt og rettidig afleveret (se Canvas).

Bedømmelseskriterier og censurtype
Bedømmelseskriterier for prøven er lig med læringsmål for det valgfrie uddannelseselement. Bedømmelsen er en helhedsvurdering af den skriftlige opgave samt den mundtlige præstation ved eksamen. Bedømmelse sker efter 7-trinsskalaen, og der er intern censur.

3.5. Industriel informationssikkerhed

Indhold
Industriel informationssikkerhed omhandler arbejdet med at sikre og monitorere industrielle systemer (OT). Fagelementet arbejder med opbygning af industrielle netværk, sikkerhedsstandarder, samt hvordan disse adskiller sig fra it-sikkerhed i andre domæner. Dertil arbejdes der med konkrete modforanstaltninger til sikring af industrielle systemer og netværk.

Læringsmål for industriel informationssikkerhed

Viden
Den studerende har:

- Udviklingsbaseret viden om typiske sikkerhedstrusler, gængse protokoller og konfigurationer, samt sikkerhedsstandarder som er relevante for industriel sikkerhed.
- Forståelse for praksis, anvendt teori og metoder til at sikre industrielle netværk og kan reflektere over forskellige løsninger hertil.

Færdigheder
Den studerende kan:

- Anvende fagområdets metoder og værktøjer til at monitere og analysere industrielle systemers sikkerhedsmæssige tilstande.
- Vurdere praksisnære og teoretiske løsninger til opbygning af sikre industrielle systemer, samt begrunde og udvælge relevante løsningsmodeller.
- Formidle behovet for at implementere netværksopdeling i forbindelse med industrielle systemer til samarbejdspartnere og kunder.
- Analysere og beskrive relevante OT-systemarkitekturer i forhold til reelle krav
- Definere procedurer til risikovurdering og risikostyring i forbindelse med industrielle systemer.

Kompetencer
Den studerende kan:

- Håndtere komplekse og udviklingsorienterede situationer i forhold til implementering af relevante modforanstaltninger til sikring af industrielle systemer.
- Selvstændigt indgå i fagligt og tværfagligt samarbejde og påtage sig ansvar inden for rammerne af en professionel etik.
- Identificere egne læringsbehov og udvikle egen viden, færdigheder og kompetencer i relation til professionen.

ECTS-omfang
Fagelementet Industriel informationssikkerhed har et omfang på 5 ECTS-point.

Prøveform og tilrettelæggelse herunder evt. formkrav
Prøven består af en individuel mundtlig eksamen som tager udgangspunkt i en individuelt udarbejdet synopsis på baggrund af en udleveret case samt et trækspørgsmål uden forberedelse til eksamen.

Den skriftlige synopsis
Synopsen udarbejdes på baggrund af en udleveret case. Synopsen må have et omfang af højest 5 normalsider.

Den individuelle mundtlige prøve
Den individuelle mundtlige eksamen har et omfang af i alt ca. 30 minutter, som fordeles som følger:

- 5-7 minutter, hvor den studerende præsenterer synopsen
- 8-10 minutters diskussion og spørgsmål vedrørende indhold i den studerendes oplæg.
- 10-12 minutter: Den studerende trækker et spørgsmål vedr. fagelementets læringsmål.
- 5 minutters votering.

Forudsætninger for at gå til eksamen – deltagelsespligt og aflevering
For at gå til den mundtlige del af prøven skal indholdet af den individuelle skriftlige opgave være redeligt. Opgaven skal opfylde formkrav samt være korrekt og rettidig afleveret (se Canvas).

Bedømmelseskriterier og censurtype
Bedømmelseskriterier for prøven er lig med læringsmål for det valgfrie uddannelseselement.
Bedømmelsen er en helhedsvurdering af den skriftlige synopsis samt den studerendes præstation ved den mundtlige eksamen, dvs. såvel præsentation, diskussion samt besvarelse af trækspørgsmål.
Bedømmelse sker efter 7-trinsskalaen, og der er intern censur.

4. Anvendelse af hjælpemidler

Under prøverne er anvendelse af hjælpemidler, herunder elektroniske hjælpemidler, tilladt, medmindre der i bekendtgørelsen eller studieordningen for den enkelte uddannelse er fastsat begrænsninger i anvendelsen.

Eventuelle regler for indskrænkning af brug af hjælpemidler vil fremgå af beskrivelsen af den enkelte prøve.

5. Ikrafttrædelse

Valgfagskataloget træder i kraft den 25. januar 2023 og har virkning for de studerende, som skal vælge valgfag efter den 25. januar 2023.

Samtidig ophæves valgfagskataloget af 01.10.2020. Prøver påbegyndt før den 1. februar 2023 skal afsluttes efter den tidligere studieordning senest den 01.08.2023.