STUDIEORDNING

Diplomuddannelsen i it-sikkerhed

Januar 2024

1. Indledning

Diplomuddannelsen i it-sikkerhed er en erhvervsrettet videregående uddannelse målrettet ansatte i virksomheder og organisationer med en væsentlig anvendelse af it.

Uddannelsen er omfattet af reglerne i Bekendtgørelse om diplomuddannelser nr. 933 af 13/06/2022 og hører under fagområdet IT og teknik. Uddannelsen udbydes efter lov om erhvervsrettet grunduddannelse og videregående uddannelse (videreuddannelsessystemet) for voksne (VFV-loven) og efter bestemmelserne om tilrettelæggelse af deltidsuddannelser i lov om åben uddannelse (erhvervsrettet voksenuddannelse) m.v.

Studieordningen er udarbejdet i fællesskab af de institutioner, som er godkendt af Styrelsen for Videregående Uddannelser til udbud af denne uddannelse jf. § 16 i Bekendtgørelse om diplomuddannelser BEK nr. 933 af 13/06/2022. Studieordningen finder anvendelse for alle godkendte udbud af uddannelsen, og ændringer i studieordningen kan kun foretages i et samarbejde mellem de udbydende institutioner.

Følgende uddannelsesinstitutioner er ved denne studieordnings ikrafttræden godkendt til udbud af diplomuddannelsen i it-sikkerhed:

- Erhvervsakademi Aarhus
- Københavns Erhvervsakademi
- UCL Erhvervsakademi og Professionshøjskole
- Professionshøjskolen UCN

Ved udarbejdelse af den fælles studieordning og væsentlige ændringer afledt heraf tager institutionerne kontakt til aftagerne og øvrige interessenter samt indhenter en udtalelse fra censorformandskabet, jf. BEK nr. 18 af 09/01/2020 om prøver i erhvervsrettede videregående uddannelser (eksamensbekendtgørelsen) og Bekendtgørelsen for diplomuddannelser nr. 933 af 13/06/2022.

Studieordningen og væsentlige ændringer afledt heraf træder i kraft ved et studieårs begyndelse og skal indeholde den fornødne overgangsordning.

Studieordningen træder i kraft den 01/01/2024.

2. Uddannelsens formål

Diplomuddannelsen i it-sikkerhed har til formål at kvalificere nuværende og kommende ansatte til at kunne fungere selvstændigt som it-sikkerhedsspecialist med fokus på at arbejde med fortrolighed, integritet og tilgængelighed i forbindelse med udvikling og drift af it-systemer i såvel private som offentlige virksomheder og organisationer, herunder at indgå i tværfaglige og tværgående samarbejder samt selvstændigt udvikle egen sikkerhedspraksis. Dimittenden skal kunne analysere, planlægge, vurdere og anvende elementer, der indgår i it-sikkerhedsprocesser på et såvel strategisk, taktisk som operativt niveau på en reflekterende og

handlingsorienteret måde.

3. Uddannelsens varighed

Uddannelsen er normeret til 1 studenterårsværk og svarer til 60 ECTS-point (European Credit Transfer System). ECTS-point er en måleenhed for en studerendes arbejdsbelastning. Det samlede antal ECTS-point er en talmæssig angivelse for den totale arbejdsbelastning, som gennemførelsen af en uddannelse eller et modul er normeret til. I studenterårsværket er indregnet arbejdsbelastningen ved alle former for uddannelsesaktiviteter, der knytter sig til uddannelsen eller modulet, herunder skemalagt undervisning, selvstudie, projektarbejde, udarbejdelse af skriftlige opgaver, øvelser og cases mv. samt eksaminer og andre bedømmelser.

Uddannelsen skal være afsluttet senest 6 år efter, at den studerende er begyndt på uddannelsen. Institutionen kan i særlige tilfælde dispensere herfra.

4. Uddannelsens titel

Uddannelsen giver den uddannede ret til at anvende betegnelsen: Diplom i it-sikkerhed. Den engelske betegnelse er: Diploma of IT-Security.

5. Adgangskrav

For at blive optaget på Diplomuddannelsen i it-sikkerhed skal du have en af følgende uddannelser:

- En relevant uddannelse mindst på niveau med en erhvervsakademiuddannelse, fx datamatiker, it-teknolog eller tilsvarende
- En relevant akademiuddannelse
- Desuden skal du have mindst 2 års erhvervserfaring efter din adgangsgivende uddannelse.

Opfylder du ikke de nævnte krav men har andre tilsvarende kompetencer, kan den enkelte institution dispensere efter en individuel kompetencevurdering. Kontakt uddannelsesinstitutionen for yderligere herom.

6. Uddannelsens mål for læringsudbytte og struktur

6.1 Uddannelsens mål for læringsudbyttet

Målene for læringsudbyttet på Diplomuddannelsen i it-sikkerhed beskrives ud fra Kvalifikationsrammen for de videregående uddannelser således:

Viden og forståelse

Dimittenden har viden om og forståelse for:

1) Gængse internationale standarder og normer vedr. it-sikkerhed
2) Risk Management ift. it-sikkerhed
3) Gængse it-sikkerhedstrusler
4) Krypteringsalgoritmer, deres egenskaber og anvendelse
5) It-sikkerhedsprincipper til design af sikre systemer
6) Sikringsmekanismer som indgår i sikre systemer
7) It-sikkerhedstiltag og kan reflektere over forretningsbehov i forhold hertil.

Færdigheder

Dimittenden kan:

1) Anvende, vurdere og formidle it-sikkerhedsstandarder ift. Forretningsbehov
2) Vælge, begrunde og formidle velegnede it-sikkerhedstiltag ift. givne forretningsmæssige scenarier
3) Identificere og argumentere for velegnede valg af relevante mekanismer til at imødegå identificerede it-sikkerhedstrusler
4) Mestre relevante designprincipper i forbindelse med udvikling af sikre systemer.

Kompetencer

Dimittenden kan:

1) Med udgangspunkt i bl.a. gængse it-sikkerhedsstandarder håndtere udarbejdelse af målrettede it-sikkerhedspolitikker og -procedurer ift. forretningsbehov
2) Håndtere udviklingsorienterede situationer herunder: i. Sikre it-systemer vha. relevante krypteringstiltag ii. Designe, konstruere, implementere og teste it-sikkerhedsforanstaltninger med inddragelse af velegnede tekniske elementer iii. Gennemføre metoder til efterforskning af it-sikkerhedshændelser
3) Håndtere komplekse situationer indenfor professionen
4) Selvstændigt tilegne sig viden, færdigheder og kompetencer indenfor it-sikkerhed
5) Påtage sig ansvar indenfor professionen samt indgå professionelt i tværfagligt samarbejde

6.2 Struktur

Diplomuddannelsen i it-sikkerhed består af tre obligatoriske moduler, et antal valgfrie moduler samt et obligatorisk afgangsprojekt. Alle moduler inden afgangsprojektet er på enten 5 eller 10 ECTS-point, mens afgangsprojektet, der afslutter uddannelsen som en syntese af de foregående moduler, er på 15 ECTS-point.

Afgangsprojektet (15 ECTS)	
Der udvikles løbende nye valgfag til Diplom i it-sikkerhed. Disse vil løbende blive beskrevet i en allonge (bilag 2) til studieordningen.	
Sikkerhed i it-governance (it-sikkerhedsledelse) (5 ECTS)	Softwaresikkerhed (10 ECTS)
Videregående sikkerhed i it-governance (Videregående sikkerhedsledelse) (5 ECTS)	
Systemsikkerhed (10 ECTS)	
Netværks- og kommunikationssikkerhed (10 ECTS)	

Obligatoriske moduler jf. bilag 1:

Uddannelsens obligatoriske moduler, der er fælles for alle studerende, omfatter 3 moduler, i alt 25 ECTS-point. De obligatoriske moduler er konstituerende for uddannelsen.

For uddybning af læringsmål, indhold og omfang af de obligatoriske moduler henvises til bilag 1.

Valgfrie moduler jf. bilag 2:

Uddannelsen omfatter valgfrie moduler, der for den enkelte studerende skal udgøre i alt 20 ECTS-point. De valgfrie moduler er understøttende i forhold til uddannelsens mål for læringsudbytte. Den studerende kan vælge at tage et eller to valgmoduler i en anden diplomuddannelse under samme bekendtgørelse uden for fagområdet for it-sikkerhed, dog højst 10 ECTS-point (jf. bilag 1, Bekendtgørelsen om diplomuddannelser BEK nr. 1008 af 29/06/2016). Således skal mindst ét valgmodul á 5 ECTS-point tages inden for uddannelsens faglige område.

Afgangsprojekt

Afgangsprojektet på 15 ECTS-point afslutter uddannelsen. Afgangsprojektet skal dokumentere, at uddannelsens mål for læringsudbytte er opnået. Afgangsprojektets emne skal ligge inden for uddannelsens faglige område og formuleres, så eventuelle valgmoduler uden for uddannelsens faglige område inddrages.

Samtlige obligatoriske moduler og det nødvendige antal valgfrie og retningsspecifikke moduler på et samlet omfang af 45 ECTS-point skal være bestået før den studerende kan afslutte afgangsprojektet (jf. § 15 stk. 2 i Bekendtgørelsen om diplomuddannelser).

7. Afgangsprojekt

I afgangsprojektet skal den studerende dokumentere evnen til på et analytisk og metodisk grundlag at kunne bearbejde en kompleks og praksisnær problemstilling i relation til en konkret opgave inden for it-sikkerhed området. Afgangsprojektet skal omfatte centrale emner i uddannelsen. Ved løsningen af den opstillede problemstilling er det vigtigt, at den studerende kan anvende centrale teorier og metoder. Afgangsprojektet skal endvidere medvirke til at dokumentere, at diplomuddannelsen samlede læringsmål er opnået.

7.1 Læringsmål for afgangsprojektet

Mål for læringsudbytte

Viden og forståelse

Den studerende har viden om og forståelse af:

- Teorier og metoder i forhold til egen IT-sikkerhedsmæssig praksis og den valgte problemstilling samt kan reflektere over praksis indenfor området.

Færdigheder

Den studerende har færdigheder til at:

- Begrunde og vælge relevante løsningsmodeller samt foretage analyse af den valgte problemstilling med anvendelse af teori og undersøgelsesmetode inden for IT-sikkerhed.
- Vurdere og formidle komplekse problemstillinger, analyseresultater og itsikkerhedsmæssige beslutninger til relevante interessenter i og uden for organisation.

Kompetence

Den studerende kan:

- På reflekteret baggrund udvikle og begrunde valg af løsninger og handlinger for komplekse IT-sikkerhedsmæssige problemstillinger
- håndtere komplekse problemstillinger inden for specialiseringen
- identificere egne læringsbehov i forhold til projektet og specialiseringen
- tilpasse metoder og teknikker i forhold til de konkrete problemstillinger i projektet.
- sætte sig ind i nye teorier, metoder og teknikker i det omfang, det er relevant for projektet
- reflektere over og udvikle sin arbejdsproces i forhold til projektet og specialiseringen
- indgå i fagligt og tværfagligt samarbejde i forhold til projektets interessenter.

7.2 Udarbejdelse af afgangsprojekt

Den studerende skal have bestået alle tidligere prøver for at kunne indstilles til afgangsprojekt. Problemformuleringen til afgangsprojekt udarbejdes af den studerende i samarbejde med en

virksomhed. Problemformuleringen skal godkendes af uddannelsesinstitutionen. Institutionen stiller vejleder til rådighed under udarbejdelsen af afgangsprojektet. Uddannelsesinstitutionen udarbejder nærmere retningslinjer med de formelle krav til afgangsprojektet, dokumentation og vejledning.

8. Undervisnings- og arbejdsformer

På uddannelsen anvendes en bred vifte af undervisningsformer, som til sammen skal understøtte ovenstående og fremme opnåelsen af de læringsmål, som er beskrevet i denne studieordning.

De gennemgående undervisningsformer er dialogbaseret holdundervisning, arbejde i studiegrupper, selvstudie, individuelle opgaver og miniprojekter.

For at medvirke til uddannelsens faglighed og internationalisering vil dele af undervisningen foregå på engelsk og mange materialer er på engelsk.

Fælles for alle disse aktiviteter er, at der opstilles klare mål for læringsaktiviteterne. Endvidere tilbydes forskellige aktiviteter som kan medvirke til at fremme den enkeltes læring; herunder individuel vejledning og coaching.

For at studiets undervisningsformer kan fungere, kræves aktivitet og tilstedeværelse, samt aktiv deltagelse i de stillede obligatoriske opgaver og projektarbejder.

Der kan være bundne forudsætninger, som er studieaktiviteter, der skal afleveres for at deltage i uddannelsens prøver.

8.1 Evaluering

Som et led i kvalitetssikringen af uddannelsen og de enkelte moduler anvendes institutionens modulevalueringssystem.

9. Prøver og bedømmelse

I løbet af uddannelsen skal den studerende stifte bekendtskab med flere forskellige former for bedømmelse. Alle former har som centralt omdrejningspunkt at bringe den anvendte teori i spil med den virkelighed, den studerende er en del af, for at fastholde fokus på udviklingen af den personlige handlekompetence.

Eksamensform og bedømmelse skal afspejle den tilstræbte kompetenceudvikling i de enkelte moduler. Hvert modul afsluttes med en bedømmelse. Bedømmelsesformen vælges af den enkelte udbyderinstitution blandt de forslag, som fremgår af prøveallongens mulige formater. Dette skal fremgå af den enkelte uddannelsesudbyders studie- og eksamensvejledning. Prøven skal være tilrettelagt, så det er muligt at udprøve modulets læringsmål.

Mindst 30 ECTS-point udprøves med ekstern censur, heraf 15 ECTS-point på afgangsprojektet og min. 10 ECTS-point på de obligatoriske moduler.

9.1 Eksamensbeviser

Institutionen udsteder modulbeviser for hvert bestået modul samt uddannelsesbevis og Diploma Supplement ved afslutningen af uddannelsen. Er uddannelsen gennemført ved flere institutioner, udstedes uddannelsesbeviset af den institution, hvor afgangsprojektet er bestået.

I beviset angives:

- Resultatet af bedømmelserne i de enkelte udprøvninger.
- Karaktervægtene, hvormed disse indgår i gennemsnittet.
- Den opnåede gennemsnitskarakterer for studiet som helhed.

10. Merit

Beståede moduler ved en af institutionerne ækvivalerer samme modul ved de andre institutioner. Institutionen kan godkende, at gennemførte og beståede uddannelseselementer, eller dele heraf, fra en dansk eller udenlandsk it-sikkerhedsuddannelse træder i stedet for moduler, der er omfattet af denne studieordning såfremt uddannelseselementerne svarer til diplomniveauet i Den danske kvalifikationsramme for livslang læring.

Ved meritoverførsel fra anden uddannelse medregnes opnået karakter ikke, men overføres som bestået.

Det påhviler den studerende at sætte sig ind i mål for læringsudbyttet i studieordningen for det eller de moduler, der søges merit for, og at dokumentere meritgrundlaget i forhold til disse mål.

Det er ikke muligt at søge merit for afgangsprojektet.

Realkompetencevurdering kan gennemføres i henhold til Bekendtgørelse om individuel kompetencevurdering (Realkompetencevurdering) nr. 8 af 10/01/2008.

Meritstuderende
Institutionen kan godkende, at studerende fra andre videregående uddannelser følger dele af uddannelsen og aflægger prøve efter gældende retningslinjer. Det er en forudsætning, at det er et godkendt led i deres egen uddannelse.

11. Orlov

En studerende kan få orlov fra uddannelsen begrundet i personlige forhold. Om de nærmere regler for at få orlov samt de bestemmelser, der er gældende for studerende på orlov, henvises til institutionens retningslinjer.

12. Censorkorps

Diplomuddannelsen i IT-sikkerhed benytter det af Styrelsen for Videregående Uddannelser godkendte censorkorps for IT og teknik.

13. Studievejledning

Hver institution udarbejder studievejledning, undervisningsplan samt eksamensvejledning for hvert modul. Nærværende studieordning, samt andre dokumenter og regler af betydning for de studerende på uddannelsen fremgår af institutionens hjemmeside.

14. Klager og dispensation

14.1 Klager

Klager over prøver behandles efter reglerne i Bekendtgørelse om prøver og eksamener i erhvervsrettede uddannelser, BEK nr. 1500 af 02/12/2016 (Eksamensbekendtgørelsen).

Alle klager over prøver kan indgives til institutionen senest 2 uger fra den dag, afgørelsen er meddelt den studerende.

Klager over forhold ved prøver indgives individuelt af eksaminanden til uddannelsesinstitutionen.

Hver udbyderinstitution udarbejder et eksamensreglement indeholdende klagevejledning.

Klager over øvrige forhold behandles efter reglerne i BEK nr. 18 af 09/01/2020 om prøver i erhvervsrettede videregående uddannelser (eksamensbekendtgørelsen) og BEK nr. 933 af 13/06/2022 om diplomuddannelser.

14.2 Dispensation fra studieordningen

Institutionen kan, når særlige forhold begrunder det, dispensere fra de bestemmelser i studieordningen, der ikke er bundet i bekendtgørelsesgrundlaget. Klager over afgørelser i henhold til denne studieordning indgives til institutionen. Fristen for indgivelse af klager er 2 uger fra den dag, afgørelsen er meddelt den pågældende. Institutionens afgørelser efter denne studieordning kan af studerende indbringes for Styrelsen for Videregående Uddannelser, når klagen vedrører retlige spørgsmål. Fristen for at indgivelse af klagen er 2 uger fra den dag, afgørelsen er meddelt den pågældende.

Klagen stiles til Undervisningsministeriet, men afleveres til institutionen. Denne afgiver en udtalelse, som klageren har lejlighed til inden for en frist af én arbejdsuge at kommentere.

15. Overgangsordninger

I henhold til BEK nr. 933 af 13/06/2022 om diplomuddannelser §20 stk. 2 skal institutionerne i forbindelse med udarbejdelse af studieordningsrevisioner sikre de nødvendige overgangsordninger. Derfor vil studerende, der er påbegyndt uddannelsen før den 1. januar 2024 og som har bestået de tidligere obligatoriske moduler; *Netværks- og kommunikationssikkerhed*, *Softwaresikkerhed* samt

Videregående sikkerhed i it-governance kan færdiggøre uddannelsen under den nye studieordning uafhængigt af, om modulerne er bestået med intern eller ekstern censur.

16. Retsgrundlag

Studieordningens retsgrundlag udgøres af:

1) BEK nr. 933 af 13/06/2022 om diplomuddannelser.
2) Bekendtgørelse af lov om erhvervsrettet grunduddannelse og videregående uddannelse (videreuddannelsessystemet) for voksne LBK nr. 578 af 01/06/2014
3) Bekendtgørelse af lov om åben uddannelse (erhvervsrettet voksenuddannelse) m.v. LBK nr. 315 af 05/04/2017
4) BEK nr. 18 af 09/01/2020 om prøver i erhvervsrettede videregående uddannelser (eksamensbekendtgørelsen)
5) Bekendtgørelse om karakterskala og anden bedømmelse ved uddannelser på Uddannelses- og Forskningsministeriets område nr. 114 af 03/02/2015
6) Bekendtgørelse om fleksible forløb inden for videregående uddannelse for voksne nr. 1348 af 29/11/2013

Retsgrundlaget kan læses på adressen www.retsinfo.dk

Bilag 1: Obligatoriske moduler

OB1 Netværks- og kommunikationssikkerhed (10 ECTS)

Indhold

Modulet sætter den studerende i stand til at forstå og håndtere netværkssikkerhedstrusler samt implementere og konfigurere udstyr til samme.

Modulet omhandler forskelligt sikkerhedsudstyr, herunder Intrusion Detection System (IDS) til monitorering. Derudover vurdering af sikkerheden i et netværk, udarbejdelse af plan til at lukke eventuelle sårbarheder i netværket samt gennemgang af forskellige VPN teknologier.

Læringsmål

Viden

Den studerende har viden om og forståelse for:

- Netværkstrusler
- Trådløs sikkerhed
- Sikkerhed i TCP/IP
- Adressering i de forskellige lag
- Dybdegående kendskab til flere af de mest anvendte internet protokoller (ssl)
- Hvilke enheder, der anvender hvilke protokoller
- Forskellige sniffing strategier og teknikker
- Netværk management (overvågning/logning, snmp)
- Forskellige Virtual Private Network (VPN) setups
- Gængse netværksenheder der bruges ifm. sikkerhed (firewall, Intrusion Detection System (IDS) / Intrusion Prevention System (IPS), honeypot, Deep Packet Inspection (DPI).

Færdigheder

Den studerende kan:

- Overvåge netværk samt netværkskomponenter, (f.eks. IDS eller IPS, honeypot)
- Teste netværk for angreb rettet mod de mest anvendte protokoller
- Identificere sårbarheder som et netværk kan have.

Kompetencer

Den studerende kan:

- Håndtere udviklingsorienterede situationer herunder:
  - designe, konstruere og implementere samt teste et sikkert netværk
  - monitorere og administrere et netværks komponenter mht. it-sikkerhed Studieordning for Diplom I IT-sikkerhed
  - Udfærdige en rapport om de sårbarheder et netværk eventuelt skulle have (red team report)
  - Opsætte og konfigurere et IDS eller IPS.
- Kan håndtere relevante krypteringstiltag til sikring af netværkskommunikation.

OB2 Systemsikkerhed (10 ECTS)

Indhold

System Security. Den studerende kan udføre, udvælge, anvende, og implementere praktiske tiltag til sikring af firmaets udstyr og har viden og færdigheder, der supportere dette.

Læringsmål

Viden

Den studerende har viden om:

- Generelle governance principper / sikkerhedsprocedurer
- Væsentlige forensic processer
- Relevante it-trusler
- Relevante sikkerhedsprincipper til systemsikkerhed
- OS roller ift. sikkerhedsovervejelser
- Sikkerhedsadministration i database - Database Management Systems (DBMS).

Færdigheder

Den studerende kan:

- Udnytte modforanstaltninger til sikring af systemer
- Følge et benchmark til at sikre opsætning af enhederne
- Implementere systematisk logning og monitering af enheder
- Analysere logs for incidents og følge et revisionsspor
- Kan genoprette systemer efter en hændelse.

Kompetencer

Den studerende kan:

- håndtere enheder på command line-niveau
- håndtere værktøjer til at identificere og fjerne/afbøde forskellige typer af endpoint trusler
- håndtere udvælgelse, anvendelse og implementering af praktiske mekanismer til at forhindre, detektere og reagere over for specifikke it-sikkerhedsmæssige hændelser.
- håndtere relevante krypteringstiltag.

OB3 Videregående sikkerhed i it-governance (Videregående sikkerhedsledelse) (5 ECTS)

Indhold

Den studerende skal kunne forstå og deltage i tilrettelæggelse af sikkerhedsarbejdet i organisationen. Den studerende skal have forståelse for, hvordan samfundsorganisationer påvirker sikkerhedsarbejdet.

Læringsmål

Viden

- Den studerende har viden om og forståelse for:
- Relevant jura indenfor it-sikkerhed
- Risikoanalyse indenfor it-sikkerhed
- It-sikkerhedsarbejde og kultur i organisationen
- Organisationsforståelse i et sikkerhedsperspektiv
- It-governance
- It-politikker og -praktikker
- Standarder og organisationer i it-sikkerhedsarbejdet
- Infrastrukturelt perspektiv på it-sikkerhed.

Færdigheder

Den studerende kan:

- Søge information og navigere i standarder og anvende det i de systemer, de benytter
- Navigere i og indhente oplysninger om gældende love og regler inden for it-sikkerhedsrelevante emner
- Bidrage til at udvikle en governance model for en given organisation.

Kompetencer

Den studerende kan:

- Udarbejde specifikke it-sikkerhedspolitikker for en given organisation
- Håndtere fundamentale opgaver som sikkerhedsansvarlig.

Bilag 2: Valgfrie moduler inden for uddannelsens faglige område

VF1 Softwaresikkerhed (10 ECTS)

Indhold

Modulet fokuserer på sikkerhedsperspektivet i software, blandt andet programkvalitet og fejlhåndterings samt datahåndterings betydning for en software arkitekturs sårbarheder. Elementet introducerer også til forskellige designprincipper, herunder ”security by design”.

Læringsmål

Viden
Den studerende har viden om:

Hvilken betydning programkvalitet har for it-sikkerhed ift.:

- Trusler mod software
- Kriterier for programkvalitet
- Fejlhåndtering i programmer
- Forståelse for security design principles, herunder:
    - security by design
    - privacy by design.

Færdigheder
Den studerende kan:

Tage højde for sikkerhedsaspekter ved at:

- Programmere håndtering af forventede og uventede fejl
- Definere lovlige og ikke-lovlige input data, bl.a. til test
- Bruge et Application Programming Interface (API) og/eller standard biblioteker
- Opdage og forhindre sårbarheder i programkoder
- Sikkerhedsvurdere et givet software arkitektur.

Kompetencer
Den studerende kan:

- Håndtere risikovurdering af programkode for sårbarheder.
- Håndtere udvalgte krypteringstiltag.

VF2 Sikkerhed i it-governance (it-sikkerhedsledelse) (5 ECTS)

Indhold

Etik og principper for it-sikkerhed samt introduktion til principper og begreber inden for it-sikkerhed.

Den studerende får en forståelse for grundlæggende principper og antagelser i it-sikkerhedsarbejde, og introduceres til etiske og politiske aspekter af samme.

Læringsmål

Viden
Den studerende har viden om og forståelse for:

- Praktiske etiske overvejelser ifm. arbejdet indenfor it-sikkerhed
- Principper indenfor it-sikkerhed
- Risikoanalyse
- Standarder og organisationer i sikkerhedsarbejdet
- Trusler og trusselsbilledet
- Operationelle overvejelser for it-sikkerhed
- Sikkerhedspolitikker og -procedurer (Business Continuity and Disaster Recovery).

Færdigheder
Den studerende kan:

- Foretage risikovurdering af mindre systemer/virksomheder, herunder datasikkerhed
- Vurdere hvilke sikkerhedsprincipper, der skal anvendes i forhold til en given kontekst.

Kompetencer
Den studerende kan:

- Håndtere analyser om, hvilke sikkerhedstrusler der aktuelt skal behandles i et konkret it-system.

VF3 Netværkspenetrationstest (5 ECTS)

Indhold

Den studerende lærer om hvordan en penetration test udføres, samt kan indhente oplysninger om de seneste sårbarheder, og kan benytte sig af de relevante værktøjer til dette formål.

Læringsmål

Viden
Den studerende viden om og forståelse for:

- Etiske samt kontraktuelle forhold omkring en penetrationstest.
- Standardiseringorganisationers og myndigheders krav til og om penetrationstesting

Færdigheder
Den studerende kan:
Tage højde for sikkerhedsaspekter ved at:

- Anvende relevante metoder ved udførsel af en penetrationstest
- Udarbejde en angrebsplan ud fra indsamlede oplysninger om et mål
- Finde sårbarheder i et givet system • Dokumentere og rapportere fundne sårbarheder

Kompetencer
Den studerende kan:

- Planlægge en penetration test, samt eksekvere den både ved brug af værktøjer og manuelt.

VF4 SIEM og log analyse (5 ECTS)

Indhold

Den studerende lærer om Security information and event management (SIEM), herunder hvordan man kan indsamle, administrere, og søge i sikkerhedshændelsesdata i et større it-system (komplekse systemer, Internet og Things (IoT), deployments, corporate IT).

Læringsmål

Viden
Den studerende har viden om og forståelse for:

- Typiske Security Information and Event Management (SIEM) arkitekturer
- Standard logformater og logtyper for standard systemer og komponenter
- Typiske SIEM produkter
- Juridiske krav til logning og bevarelse af data ifb. forensic analyse.

Færdigheder
Den studerende kan:

- Typiske SIEM arkitekturer
- Standard logformater og logtyper for standard systemer og komponenter
- Typiske SIEM produkter
- Juridiske krav til logning og bevarelse af data ifb. forensic analyse.

Kompetencer
Den studerende kan:

- Designe og implementere en SIEM løsning på tværs af diverse produkter Træffe beslutninger om hvilke data der skal indsamles i en givne situation
- Identificerer fejl i logopsamlingen
- Deltage i drøftelser på et praktisk og strategisk niveau i forhold til implementering af logmanagement/SIEM.

VF5 Data Science for IT-sikkerhed (5 ECTS)

Indhold

Data Science for IT-sikkerhed. Den studerende kan evaluere, udvælge og anvende metoder inden for data science på IT-sikkerhedsmæssige områder og har viden og færdigheder, der supporterer dette.

Læringsmål

Viden
Den studerende har viden om:

- Data forberedelse, herunder rensning, skalering og normalisering.
- Data analyse.
- Data visualisering.
- Modeller til kategorisering, herunder machine learning.

Færdigheder
Den studerende kan:

- Forberede data til machine learning.
- Analysere og visualisere data, både i form af input og resultater.
- Anvende et konkret machine learning framework på praktiske problemstillinger inden for IT-sikkerhed.
- Evaluere og sammenligne resultater fra machine learning algoritmer.

Kompetencer
Den studerende kan:

- Udvælge og anvende passende machine learning algoritmer til løsninger af konkrete problemer inden for IT-sikkerhed, samt evaluere disse.
- Selvstændigt tilegne sig viden, færdigheder og kompetencer inden for området.

VF6 Digital forensics og incident response (DFIR) (10 ECTS)

Indhold

Modulet fokuserer på opbygning af færdigheder og kompetencer hos den studerende til at kunne opstille og udarbejde en it-sikkerheds beredskabsplan på virksomheds- og/eller organisationsniveau.

Modulet giver den studerende færdigheder og kompetencer til operativ og taktisk håndtering af hackerangreb i virksomheden. Den studerende lærer, hvad der sker i en virksomhed under et angreb, samt lærer at kunne håndtere hændelsen. Modulet giver den studerende kendskab til strategier og værktøjer, til at håndtere angreb.

Den studerende lærer at koble de beskrevne rammer for virksomhedens it-sikkerhed, herunder virksomhedens it-sikkerhedsdokument sammen med virksomhedens security incident response handlinger. På den måde tilfører modulet en udbygning af det den studerendes handlingsorienterede kompetenceopbygning.

Den studerende lærer at oprette en beredskabsplan og kunne agere igennem beredskabsplanens faser. Derudover lærer den studerende at kunne analysere de data, der indsamles, herunder analyse af netværks trafik, artefakter/filer og logs) samt online vs. offline analyse.

Endeligt lærer den studerende at udarbejde en SIR rapport.

Modulet indeholder således emner indenfor:

- Beredskabsplaner
- DFIR plan og de 6 faser
- Datasikring og validering
- Forensic analyse
- Malware analyse
- SIR rapport.

Læringsmål

Viden
Den studerende har viden om:

- "tools, tactics, and procedures (TTP)" der anvendes af nutidens angribere
- korrekt håndtering og sikring af beviset efter gældende lovgivning
- grundprincipper og processer i efterforskning på it-udstyr (digital forensics) og forbindelsen til hændelseshåndtering samt "Chain of Custody"

Færdigheder
Den studerende kan:

- søge i relevante filer, registreringsdatabaser, hukommelse og lignende for Indicators of Compromise (IoCs) analysere endpoints og netværkstrafik for tegn på sikkerhedshændelser
- identificere brugeraktivitet i bevismaterialet • anvende og udvikle processer til hændelseshåndtering i en organisation
- viderebringe resultater i form af ekspertrapporter og vidneerklæringer

Kompetencer
Den studerende kan:

- selvstændigt håndtere indsamling og analyse af data i forbindelse med en sikkerhedshændelse og bruge disse til at inddæmme og afhjælpe et brud
- anvende, udvikle, og dele threat intelligence, herunder anvende det til at finde flere brud
- indgå i et samarbejde omkring hændelseshåndtering
- selvstændigt tilegne sig viden, færdigheder og kompetencer inden for området.

VF7 It-sikkerhed i webapplikation (5 ECTS)

Indhold

Modulet består af en teoretisk forståelse af de sikkerhedsudfordringer, der findes i forbindelse med udvikling og vedligeholdelse af webapplikationer. For at skabe den bedste forståelse, vil der også være en del "hands-on", hvor den studerende vil komme til at afprøve og implementere teknologier til at skabe sikkerhed for webløsninger. Der vil blive taget udgangspunkt i aktuelle anerkendte sikkerhedsudfordringer.

For at skabe den bedste forståelse for disse, vil den studerende i bredt udfald, skulle udnytte sikkerhed hullerne, hvorefter den studerende vil skulle rette problemet, så sikkerhed hullerne ikke længere er tilgængelige.

Læringsmål

Viden
Den studerende har viden om:
- Anvendelse af sikkerhedsforanstaltninger til webteknologier.
- Sikkerhedsanalyse af webapplikationer.
- Risikovurdering i forhold til webløsninger.

Færdigheder
Den studerende kan:
- Foretage sikkerhedsforanstaltninger omkring webapplikationer.
- Teste sikkerheden af webløsninger.
- Vurdere om en webløsning er sikker i forhold til dens formål.

Kompetencer
Den studerende kan:
- Implementere sikkerhedsforanstaltninger i webløsninger.
- Genkende og løse sikkerhedshuller i webapplikationer.
- Vejlede om, samt anvende teknologier der afhjælper sikkerhedsmæssige udfordringer for webløsninger.

VF8 Industriel informationssikkerhed (5 ECTS)

Indhold

Industriel informationssikkerhed omhandler arbejdet med at sikre og monitorere industrielle systemer, Operational Technology (OT). Med henblik på dette introduceres de studerende til, hvordan industrielle netværk typisk er opbygget, hvilke sikkerhedsstandarder der gør sig gældende, samt hvordan disse adskiller sig fra it-sikkerhed i andre domæner.

Derudover arbejdes der med konkrete modforanstaltninger til sikring af industrielle systemer og netværk.

Læringsmål

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.