



Uddannelses- og Forskningsministeriet

Bredgade 38

DK-1269 København K

Ansøgning om prækvalifikation af ny uddannelse

På vegne af Danmarks Tekniske Universitet (DTU) fremsendes hermed ansøgning om oprettelse af en ny masteruddannelse, Master i Cybersikkerhed, på engelsk Master in Cybersecurity.

31. januar 2019

Journal nr. 19/00505

kbjer

Ansøgningen er udarbejdet i henhold til vejledning om prækvalifikation af nye uddannelser og er baseret på en konsulent rapport for afdækning af efteruddannelsespotentialet inden for computer science og en omfattende aftagerdialog (jf. ansøgningens afdækning af kriterium 1 og tilhørende bilag). Herunder er både DTU's Aftagerpanel, Advisory Board på DTU Compute, DTU's Cybersecurity netværk samt en række private virksomheder og offentlige institutioner inddraget.

Uddannelsen adressere et aktuelt behov på arbejdsmarkedet, som afspejler den teknologiske og samfundsmæssige udvikling og som i mindre grad imødekommes af eksisterende uddannelser (jf. ansøgningens afdækning af kriterium 2). Således understøtter ansøgningen DTU's mission om at udvikle og nyttiggøre naturvidenskab og teknisk videnskab til gavn for samfundet.

Ansøgningen er en udfyldelse af ministeriets ansøgningsskema samt bilagsmateriale. Såfremt der er behov for yderligere oplysninger, vil vi naturligvis tilvejebringe dem.

Med venlig hilsen

Anders O. Bjarklev

Rektor, DTU

Bilag 1: Aftagerundersøgelse

1. Oversigt over aftagere

Dato	Navn	Stilling	Virksomhed
24-08-2018	Ray Stanton	Group Chief Security Office	TDC Group
14-10-2018	Rikke Hvilshøj	Direktør	Dansk IT
15-10-2019	Johs Sterlie	Beretter om politiets muligheder for efteruddannelse	Tidligere NC3 (Nationalt Center for Cyber Crime)
18-10-2018	Bjarke Alling	Formand for IT Branchens sikkerhedsudvalg	IT-Branchen
18-10-2018	<i>Anonymiseret</i>		Novo Nordisk A/S
25-10-2018	Anders Kleinstруп Møller		Dansk IT
04-11-2018	Henning Mortensen	CISO/CPO/IT-sikkerhedschef	Brødrene A&O Johansen A/S
05-11-2018	Ole Kjeldsen	Teknologi og sikkerheds direktør	Microsoft
15-11-2018	IT sikkerhedsfagrådet	Fagrådets medlemmer	Dansk IT
03-12-2018	Emil Andersen	Head of HQ HR	A.P. Møller-Mærsk
17-12-2018	Svar fra IT-Branchens medlemmer. Spørgeskema sendt til IT-sikkerhedsudvalg (anonym besvarelse).	It-leverandører der har en forretningsmæssig interesse i it-sikkerhed.	Både store systemhuse og små it-sikkerhedskonsulenter iblandt.
14-12-2018	Rasmus Lisby Fruergaard-Pedersen	Software Security Engineer	Kamstrup
31-10-2018	Martin Jensen Buch	Chefkonsulent	IT-Branchen
03-01-2019	Mads Syska Hasling	CISO	Saxobank
03-01-2019	Kristian Kristensen	Director	F-Secure
03-01-2019	Jacob Herbst	CTO	Dubex
03-01-2019	Thomas Lund Sørensen	Chef for Center for Cybersikkerhed	Forsvarets Efterretningstjeneste
03-01-2019	Bo Danielsen	CIO	IDA
03-01-2019	Troels Langkjaer	Owner	Langkjaer Cyber Defence
08-01-2019	Uwe Hermann	Senior Director	Oticon, Eriksholm Research Centre
08-01-2019	Tina Moe	Professionelt bestyrelsesmedlem, Ledelsesrådgiver	Bl.a. Hedeselskabet, IPU, Alectia UK, Wemind, NNE Pharmaplan
08-01-2019	Kristian Johnsen	Faglig direktør	Diabetes foreningen
08-01-2019	Bodil Bruun	Fagkonsulent i matematik	Undervisningsministeriet
08-01-2019	Michael Nielsen	Cofounder and Partner and Manager	ForNAV and Microsoft
09-01-2019	Thomas Fænø Hansen	IT-Chef	Banedanmark
09-01-2019	Rune Domsten	Co-owner, co-founder	Domsten.dk og 3D Visionlab
09-01-2019	Hans Gottberg Rømer	Senior Director	Ørsted
15-01-2019	Henning Mortensen's Netværk	CISO/CPO/IT-sikkerhedschef, Formand	Brødrene A&O Johansen A/S, Rådet for Digital Sikkerhed

Aktivitetslog

Dato	Kommunikation med	Beskrivelse
2017.10.22	Lars Ramkilde Knudsen, DTU Compute Per Rhein Hansen, tidligere it-sikkerhedschef	Opfordrer LRK til at starte et initiativ vedr. Cyber Security uddannelse. Positiv modtagelse og startmøde aftales
2017.11.30	Lars Ramkilde Knudsen, DTU Compute, Per Rhein Hansen (hyres af DTU Compute)	Aftale om konsulentbistand til en analyseproces, hvorved der skal skabes overblik over hvilke udviklingsmuligheder inden for området cybersikkerhed, det kan anbefales DTU Compute at satse på i årene fremover. DTU Compute er i øjeblikket meget stærk på kryptologi området, men ønsker at komme til at dække cybersikkerhedsområdet bredere.
Januar- februar 2018	Konsulentopgave gennemført i samarbejde med Lars Ramkilde Knudsen og Christian D. Jensen	Skaber oversigt over cybersikkerhedsuddannelser i Danmark, identificere deres (inkl. DTU's) styrker og svagheder, og udarbejder en plan for, hvad der bør ske. Der tages delvis udgangspunkt i Deloitte rapporten fra 2015 om "Kortlægning af viden- og uddannelsesaktiviteter inden for cyber- og informationssikkerhed på danske uddannelses- og forskningsinstitutioner", som giver et billede af <i>spredte</i> satsninger på området. Dette betyder, at visse sikkerhedsområder slet ikke er dækket, hverken forskningsmæssigt eller uddannelsesmæssigt. Der må søges tilbage til de grundlæggende definitioner på Informationssikkerhed og Cybersikkerhed, for at finde ud af hvad sikkerhed handler om, og hvad der er vigtigst. Vi har valgt at tage afsæt i de klare og gode definitioner fra "Danmarks nationale cybersikkerhedsstrategi – 2018-2021".
2018.02.14	Afsluttende notat m. bilag	Der gives en gennemgang af de sikkerhedsområder, der er svagest dækket på danske universiteter, og det kan konstateres, at der er emner inden for Informationssikkerhed som endnu ingen undervisere/forskere har taget under seriøs behandling – endsige har udbudt kurser i. Det drejer sig om 8 ud af 14 hovedområder i standarden for Informationssikkerhed ISO 27001, som regeringen for flere år siden har krævet at alle offentlige institutioner skal følge! Dette betyder at det ikke vil være rimeligt at udbyde en cybersikkerhedsuddannelse uden en passende mængde af emner medtaget fra det bredere begreb informationssikkerhed. Aftagerne af en "Masteruddannelse i cybersikkerhed" vil givet vis forvente at få sikkerhed bredt dækket (ikke mindst pga. begrebsforvirringen på området, idet cybersikkerhed ofte opfattes synonymt med informationssikkerhed og it-sikkerhed)
2018.05.05	Møde mellem DTU Compute Efteruddannelse og DTU Efteruddannelse	Aase Grundtvig efterspørger master uddannelser der kan tages af e.g. DTU Diplom kandidater i IT.

2018.06	Møde mellem Line Clemmensen, Christian D. Jensen og DTU Compute's ledelse	Velvilje for at gå videre med at udarbejde Masteren, og enighed om at Christian D. Jensen skal være studieleder.
2018.08.24	Meeting between Christian D. Jensen and Ray Stanton, TDC Group	The possibility of a part time Master in cyber security was discussed, Ray expressed the need for a Master in the field, and the fact that continuing education within the IT-security field is valued highly in the TDC group.
2018.08.30	Møde med Compute's institutleder, forskere og undervisere fra DTU Compute, Security DTU og DTU Diplom	Der var en bred enighed om at det er en god ide med en Master indenfor cybersikkerhed og de første program-ideer bliver udarbejdet.
2018.09.07	Møde i DTU's Cybersecurity koordinerings netværk	Diverse forskningsansøgninger gennemgås, samt en diskussion af udviklingen af en master. Der er flere der gerne vil bidrage til udviklingen og undervisningen.
2018.10.03	Lars Henneberg, Mærsk Personlig samtale samt mail	Center for Corporate Governance accepterer min tilmelding til Risk Management seminar på CBS, hvor jeg skal høre Lars Hennebergs indlæg mhp. at få kontakt vedr. interview med Mærsk om den påtænkte masteruddannelse. Positiv respons; medarbejder blive bedt om at tage action
2018.10.09	Mail til Birgitte Hass, direktør for IT Brancheforeningen [ITB].	Per Rhein anmoder om møde; får tilsagn
2018.10.14	Rikke Hvilshøj, direktør for Dansk IT [DIT].	Tilsagn om møde med IT-sikkerhedsfagrådet
2018.10.15	Mail til tidl. medarbejder i NC3 . [Nationalt Center for Cyber Crime (NC3), i Rigspolitiet, arbejder med efterforskning og forebyggelse af it-kriminalitet]	Søger information om Politiets behov for efteruddannelse. Svaret er, at man benytter sig af Norsk politi's efteruddannelse, som er økonomisk gunstig, fordi Dansk politi selv bidrager med lærerkræfter. Masteruddannelsen vil derfor ikke være attraktiv, men enkeltstående kurser vil muligvis blive benyttet.
2018.10.18	Kasper Maltte Larsen Chief Technology Architect Manufacturing IT systems Global IT Novo Nordisk A/S	Første kontakt til Novo Nordisk . Videregiver henvendelsen til sikkerhedsafdelingen i hovedkontoret, som ikke ønsker at tage sig tid til et møde. Jeg svarer med at gå ind på NN's forslag om i stedet at skabe kontakt til Virksomhedsrådet for IT-sikkerhed , uden at der kommer en reaktion.
2018.10.18	Martin Jensen Buch ITB	Indkalder til møde hos ITB den 31.oktober. Deltagere: Bjarke Alling, Formand for ITB's sikkerhedsudvalg, og Martin Jensen Buch, som er sekretær for udvalget
2018.10.25	Anders Kleinstrup Møller [DIT]	Vender tilbage vedr. et møde med IT sikkerhedsfagrådet d. 15. november. Den 26. oktober får jeg mail om fagrådets medlemmer. PRH noter fra mødet: Alle deltagere virkede meget interesserede i en Masteruddannelse i Cybersikkerhed, men ingen mente at de havde mandat til at udtale sig på deres respektive firmaers vegne. Der fremkom

		dog nogle ret nyttige oplysninger. Søges fortsat dialog med fagrådets medlemmer skal det gå via formanden. Ikke lige hvad jeg havde brug for.
2018.10.31	Møde hos ITB	Konstruktivt møde, hvor ITB lovede at bistå med udformning og udsendelse af spørgeskema til deres medlemmer. I øvrigt særdeles positiv over for DTU's initiativ
xx	Dialog med Mads Syska Haslign fra Saxobank	Kontakter Mads via LinkedIn og han svarer positivt tilbage at han gerne vil deltage i følgegruppen for masteren.
2018.11.05	Mail fra Ole Kjeldsen, Microsoft	Ole vender tilbage på forespørgsel vedrørende følgegruppe til den nye Master. Han svarer positivt og vil gerne være med i følgegruppen.
2018.11.07	Mail til ITB	Svar til ITB efter mødet. Med forklaring om uddannelsens formål, samt første udkast til spørgeskema (2 vedhæftede bilag]
2018.11.20	Møde i DTU's Cybersecurity netværk	Forberedelse til workshop med Center for Cybersecurity. Et af punkterne er masteren og en poster udarbejdes til workshopen.
2018.11.22	Møde med Dekan Philip Binning	Dekanen synes forarbejdet ser fint ud og beder os om at arbejde videre med tiltaget samt han vil tage det op hos Direktionen.
2018.11.28	Mail fra Dekan Philip Binning	Dekanen meddeler at DTU's direktion har godkendt vores forslag om en ny Master i Cybersikkerhed.
2018.12.03	Mail fra Mærsk ved Emil Andersen	Påskønner initiativet, men ingen ressourcer til rådighed p.t. Vi kan evt. vende tilbage om et års tid.
2018.12.04	Rykker-mail til Novo Nordisk	Rykker 4. december med forslag om i det mindste at svare på et uforpligtende mini-spørgeskema.
2018.12.07	Svar fra Novo Nordisk	Udfyldt mini-spørgeskema
2018.12.11	Svar mail fra Jacob Herbst, Dubex	Jacob svarer positivt tilbage at han gerne vil deltage i følgegruppen for Masteren
2018.12.11	Svar mail fra Troels Langkjaer	Trols svarer positivt tilbage at han gerne vil deltage i følgegruppen for masteren
2018.12.11	Svar mail fra Bo Danielsen, Cerius	Bo svarer tilbage at han meget gerne vil støtte op om initiativet og deltage i en følgegruppe for masteren.
2018.12.11	Svar mail fra Rikke Hougaard Zeberd, Digitaliseringsstyrelsen	Rikke svarer positivt at et er godt vi tager dette initiativ på DTU og hun vil gerne være med i følgegruppen for Masteren.
2018.12.11	Svar mail Kristian Kristensen, F-Secure	Kristian er positiv og vil gerne være med i følgegruppen for Masteren. Desuden udtrykker Kristian at der er behov for den.
2018.12.11	Svar mail fra Ray Stanton, TDC Group	Ray er meget positiv og vil gerne være med i følgegruppen for Masteren.
2018.12.13	Svar mail fra Thomas Lund Sørensen, CfC	Thomas vil gerne deltage i følgegruppen for Masteren.
2018.12.14	Svar mail fra Bjørn Borup, IDA	Bjørn deltager gerne i følgegruppen for Masteren.
2018.12.14	Christian D. Jensen og Rasmus Lisby Fruergaard-Pedersen, Kamstrup	Møde med Michael Lisanti, fra CyLab på CMU i USA, arrangeret af Alexandra Instituttet og CenSec. Efter mødet diskuterede jeg behovet for en master i cybersikkerhed med

		Software Security Engineer Rasmus Lisby Fruergaard-Pedersen fra Kamstrup, der laver smarte målere. Rasmus udtrykte enighed i behovet for en master indenfor cybersikkerhed, men nævnte samtidigt at "det er ikke alle softwareudviklere hos Kamstrup der har behov for en så lang uddannelse". Udover behovet for eksperter med en bred forståelse af cybersikkerhed, mente han også at der er behov for kortere kurser der fokuserer på enkelte områder indenfor cybersikkerhed.
2018.12.17	Svarmail fra ITB	Udfyldte spørgeskemaer med kommentarer
2019.01.03	Følgegruppemøde på DTU	Til stede: Kristian Kristensen (F-Secure), Jacob Herbst (Dubex), Mads Syska Hasling (Saxobank), Thomas Lund Sørensen (CFCS), Bjørn Borup (IDA), Bo Danielsen (Cerius), Troels Langkjaer (Langkjaer), Per Rhein (DTU), Alberto Lluch Lafuente (DTU), Christian D Jensen (DTU), Line Clemmensen (DTU) Masteren præsenteres og følgegruppen kommenterer. De er positive over at der kommer efteruddannelse på området og har flere konkrete forslag til forbedring af Masteren.
2019.01.04	Arbejdsgruppen på Compute samt Per Rhein	Baseret på input fra følgegruppen vælger arbejdsgruppen at tilrette målgruppen og indholdet til at ramme ledere og dem med ansvar indenfor cybersikkerhed. Derudover tilpasses alle kursusmoduler således at de kan udbydes individuelt.
2019.01.08	Møde med DTU Compute's Advisory Board	Masteren præsenteres og advisory board giver feedback på forslaget. Advisory Board er positivt stemt overfor tiltaget om en deltidsmaster indenfor området. De påskønner initiativet, og kan se et behov for uddannelsen, og tilføjer at også bestyrelsesmedlemmer er en aftagergruppe for en sådan Master.
2019.01.09	Møde med DTU's aftagerpanel	Aftagerpanelet er glade for det præsenterede forslag og mener at der er et behov for videreuddannelse indenfor området. Målgruppe og indhold hænger godt sammen. De påskønner at kurserne kan udbydes individuelt også, da behovet er stort, og nogle aftagere vil gå efter korte kurser og ikke har et sigt på to år.
2019.01.09	Mail fra BaneDanmark	Spørgeramme udfyldt og sendt retur med positiv feedback om at organisationen vil have aftagere for en Master
2019.01.09	Mail fra Rune Domsten	Spørgeramme udfyldt med positiv feedback
2019.01.09	Samtale med Hans Rømer fra Ørsted	I forbindelse med Compute's Advisory board møde talte vi med Hans, som mente at Masteren vil have aftagere hos Ørsted.
2019.01.15	Svarmail fra Henning Mortensen	Fra hans bagland har han fået feedback om at det er et godt tiltag, og så en række særlig gode ting ved forslaget samt konkrete punkter vi vil tage op til overvejelse.

Hvilke af følgende emner bør en masteruddannelse fokusere på? Vælg op til 7

	BESVARELSER-	
Styring af informationssikkerhedsbrud	11	79%
Overensstemmelse [compliance], bl.a. GDPR	9	64%
Organisering af informations-sikkerhed	9	64%
Kommunikationssikkerhed	8	57%
Driftssikkerhed	7	50%
Adgangsstyring	7	50%
Ledelse & ledelsessystem	6	43%
Nød-, beredskabs- og reetablerings-styring	6	43%
Softwareudvikling m.m., dvs. anskaffelse, udvikling og vedligeholdelse af systemer	5	36%
Leverandørforhold	5	36%
Kryptografi	5	36%
Personalesikkerhed	3	21%
Fysisk sikring og miljøsikring	2	14%
Styring af aktiver	1	7%
Andet (angiv venligst)		

Hvordan foretrækkes masteren gennemført?

	BESVARELSER-	
Deltids over 3 år	7	50%
Halvtids over 2 år	5	36%
Fuldtids på 1 år	2	14%

Vil du som arbejdsgiver være villig til at betale for følgende i forbindelse med dine medarbejderes gennemførelse?

	BESVARELSER-	
Kursusafgiften	11	79%
Bøger og andet studiemateriale	7	50%
Evt. kortvarige studie-rejser/-ture (virksomhedsbesøg, eksterne kursussteder)	6	43%
En del af den anvendte arbejdstid	6	43%
Hele den anvendte arbejdstid	3	21%
Intet af ovenstående	1	7%

15. januar 2019

Udtalelse fra DTU Compute's Advisory Board vedr. Master i Cybersikkerhed

I forbindelse med den planlagte ansøgning om prækvalifikation af en ny deltidsmasteruddannelse i cybersikkerhed er DTU Compute's Advisory Board blevet orienteret om uddannelsen. Efterfølgende har man drøftet behovet for uddannelsen gennem en mundtlig høring af det materiale prækvalifikationsansøgningen baseres på (foranalysen).

Samtlige medlemmer af Advisory Board har kommenteret materialet detaljeret og konklusionen er, at Advisory Board samstemmende bifalder uddannelsesinitiativet, som beskrives som nødvendigt. Vurderingen er, at uddannelsen udfylder et hul for efteruddannelse, om end behovet er meget bredere end en enkelt masteruddannelse kan dække. Der er et stigende behov for it-sikkerhedsfolk såvel som ledere med ansvar og strategisk indsigt i håndtering af IT-sikkerhed i Danmark og Advisory Board ser uddannelsen som et vigtigt instrument til at kompetenceløfte folk ikke bare i industrien men i høj grad også i offentlige organisationer til at varetage disse sikkerhedsroller.

Flere af medlemmerne i Advisory Board understreger, at de værdsætter at kurserne i Masteren også kan tages enkeltvis.

Advisory Board har også kommenteret på uddannelsens samlede kursusportefølje og tilhørende læringsmål, og påskønner særligt læringsmålet om de studerende efterfølgende kan udarbejde beredskabsplaner for cyberangreb. Arbejdsgruppen har efterfølgende gennemarbejdet alle forslag og har desuden taget mere specifikke ønsker som f.eks. at kigge på ansøgninger til sponsorater, således at mindre virksomheder også kan få glæde af uddannelsen til efterretning.

Advisory Board anbefaler på denne baggrund uddannelsen prækvalificeret og ser frem til at følge udviklingen fremover.

På vegne af Advisory Board for DTU Compute

Rune Domsten, Uwe Hermann, Tina Moe, Kristian Johnsen, Bodil Bruun, Per Tejs Knudsen, Michael Nielsen



Uwe Hermann

MINUTES

Fremlæggelse for DTU Compute's Advisory Board

Enclosed 'ForanalyseMasterCybersikkerhed-20190107' og
'Spørgeramme'

8 January 2019

LKHC

Til stede

Tina Moe (Ledelsesrådgiver), Uwe Hermann (Oticon), Rune Domsten (3D Visionlab og Domsten.dk), Bodil Bruun (Fagkonsulent i matematik stx/hf, Undervisningsministeriet), Kristian Johnsen (faglig direktør i Diabetesforeningen), Michael Nielsen (ForNAV), Per B Brockhoff (DTU), Line Clemmensen (DTU)

Fraværende

Per Tejs Knudsen (cBrain)

Mødereferat

Line Clemmensen præsenterer deltids masteren i cybersikkerhed.

- i. Behov for masteruddannelse i cybersikkerhed
- ii. Målgruppe: 1. Eksisterende IT-sikkerheds ledere, fremtidige IT-sikkerheds ledere, IT-medarbejdere med ansvar for produkter, systemer og infrastruktur.
- iii. Optagelsesberettigede
- iv. Formål og erhvervssigte
- v. Uddannelsesstruktur
- vi. Kursusindhold
- vii. Projektindhold
- viii. Kursusafgift
- ix. Aftagere vi har haft kontakt til indtil nu

Feedback fra Advisory Board:

Der er ingen tvivl om at der er brug for videreuddannelse i cybersikkerhed, spørgsmålet er formatet, da behovsomfanget er bredere end hvad en enkelt uddannelse kan rumme.

Kurser skal kunne tages individuelt da der således vil være endnu flere der kan drage nytte af udbuddet. Det vil have en større målgruppe, da overvejelser omkring tidshorisonten på 2 år således kan omgås.

Ad ii – Målgruppen: Målgruppen er pind 2 men også pind 1, dog stryges titlerne (CIO, etc).

Ad vi – Det blev pointeret at det er vigtigt at uddannelsen har et objektiv om at de studerende efterfølgende kan udarbejde beredskabsplaner for cyberangreb [dette er et af de overordnede læringsmål for uddannelsen]

Ad ix – Aftager: Produkt/industri virksomheder mangler som aftagere. Disse vil være interessante at kontakte da de vil være en del af målgruppen.

Ad viii – Prissætning svarer til en leders uddannelsesbudget (ok i fht målgruppe). Evt skal studierejse slettes så uddannelsen kan ramme bredere ved en sænket afgift. I fht. Mindre virksomheder vil det være nyttigt at kigge på sponsorater fra f.eks. Industriens Fond for at kunne ramme denne målgruppe også (der ses et behov).

MINUTES

Møde i følgegruppe for Master i Cybersikkerhed ved DTU

Enclosed 'Foranalyse vedr deltidsmaster i cybersikkerhed' og
'Spørgeramme'

3 January 2019

LKHC

Til stede

Kristian Kristensen (F-Secure), Jacob Herbst (Dubex), Mads Syska Hasling (Saxobank), Thomas Lund Sørensen (CFCS), Bjørn Borup (IDA), Bo Danielsen (Cerius), Troels Langkjaer (Langkjaer), Per Rhein (DTU), Alberto Lluch Lafuente (DTU), Christian D Jensen (DTU), Line Clemmensen (DTU)

Fraværende

Ole Kjeldsen (Microsoft), Rikke Hougaard Zeberg (Digitaliseringsstyrelsen), Michael Lind Mortensen (Rådet for Digital Sikkerhed og Bankdata), Ray Stanton (TDC), Nicola Dragoni (DTU)

Mødereferat

Agenda

1. Præsentationsrunde
2. Præsentation af den foreslåede Master
3. Feedback på forslaget fra Advisory board (aftagerpanel)
4. AOB

Line byder velkommen og præsenterer agendaen. Agendaen godkendes.

Punkt 1. Præsentationsrunde

Christian D Jensen, Sektionsleder Cybersikkerhed, DTU

Bo Danielsen, Cerius. Tidligere samarbejdet med DTU gennem studenterprojekter.

Line Clemmensen, Lektor, Studieleder for efteruddannelse, DTU.

Mads Syska Hasling, Saxobank. Uddannet ved DTU

Thomas Lund Sørensen, CFCS, Fra KU oprindeligt

Alberto Lafuente, Head of Section for Formal Methods, DTU.

Jacob Herbst, teknisk chef for Dubex, medlem af Sikkerhedsrådet. Civ. Ing. Dengang uden studieretning.

Kristian Kristensen, Delivery Director, F-Secure. Arbejder med at finde talenter og der er stærkt brug for dem så påskønner initiativet.

Per Rhein, konsulent, lang karriere indenfor IT-sikkerhed.

Troels Langkjaer, Novo, Mærsk og Forsvaret, Langkjaer Cyberdefense, opr. datalog.

Bjørn Borup, CIO IDA.

Punkt 2. Præsentation af den foreslåede Master

Christian D. Jensen præsenterer deltidsmasteren med baggrund i 'Foranalysen'.

- i. Behov for Masteruddannelse i cybersikkerhed. Hvordan ser det ud i danske tal?
- ii. Målgruppen for masteren beskrives (opkvalificering/karriereskifte)
- iii. Formål og erhvervssigte: Tekniske kompetencer og forretningsindsigt. Stærk faglig teknisk kerne samt governance elementer, plus tre specialiseringer.
- iv. Kursusprogrammets struktur præsenteres (4 semestre, 60 ECTS). 2x2 undervisningsdage samt praktiske opgaver. Konsulentopgave og Masterprojekt linket til firmaernes problemstillinger.

- v. Kernefaglige kurser: 10 elementer.
- vi. Specialisering i softwaresikkerhed
- vii. Specialisering i netværkssikkerhed
- viii. Specialisering i systemsikkerhed
- ix. Nationale og regionale behov. Ved søgning på JobIndex er der i dag i omegnen af 40 ledige stillinger i hovedstadsområdet.

Punkt 3. Feedback fra aftagerpanelet

Ad v: Der mangler et punkt med forståelse for trusler – hvorfor skal vi gøre alt dette? Hvilke modstandere står vi overfor? Generel enighed (patchning, operativniveau – er det dækket i fht områderne der nævnes?). [De grundlæggende principper dækker dette].

Hiv det op på organisations og forretningsniveau når vi skal forstå truslerne. Vi mangler ledelses/forretningsniveau – og dette må gerne komme først i en form.

Vi skal have en introduktionsforelæsnings – trussel, og brugere (zero-trust paradigme).

Ryk kryptologi længere ned i rækken af kurser, tænk oppefra.

Hygiejne og opbygning af infrastruktur er vigtig.

Awareness og soft-skills del i fht brugere er nødvendig.

Uddannelsen er for bred.

Optone ledelsesdelen og nedtone hands-on.

Der mangler compliance og GDPR hvis vi stiler efter ledelsesniveauet.

Lav et kursus for trends og tendenser. Der er rivende udvikling.

Ad ii: Målgruppe – er det teknikere eller er det folk med erfaring i infosek der skal kunne tale sammen med bestyrelse mm vi vil ramme?

[Vi ligger os i det præsenterede mest op af det tekniske.]

IT-folk der skal ind og arbejde med sikkerhed generelt og skal op og arbejde som chef senere.

Der er brug fore bredden i compliance i større virksomheder (men måske mindre og anderledes marked end det vi vil sende specialister ind i).

Aime efter CISO'er dem der vil derover eller dem der skal opkvalificeres. Klæde stærke tekniske baggrunde på til at begå sig på ledelsesgange.

Netværkschef, klædes på til at kommunikere med CISO'er mm.

Det er ikke en software udvikler vi har fat i her.

Udviklingschef, netværkschef, mm – rettet mod ledelsesniveau både i prisklasse og tidsindsats.

Teknikere der vil ledelse.

Med bredden er det en generalist rolle – og det vi har brug for er at kunne tage generelle IT-folk og få dem over i IT-sikkerhed hvor der mangler folk.

Der er brug for at kunne udfordre konsulenter og leverandører – ved ikke om markedet er stort nok for så lang en uddannelse.

Vi savner folk med en bredde, lidt ligesom der er lagt op til her. Men pris og måske tidsomkostning er for høj.

Det her er relevant for IT-chefer, mellemledere, programledere, CISO'er, bestyrelsesmedlemmer, mm.

Der er brug for dette i Danmark når vi ramper op på cybersikkerhed. Der er det meget relevant.

Tekniske specialister – sendes på 2 ugers CENS kurser

Privacy by design mm vil også være en god differentiator som universitet i fht videreuddannelse af softwareudviklere.

Enkelte kurser for softwareudviklere? Det er der brug for, 3-6 dage op til et halvårsforløb (3-6 måneder). Der er mange konkurrenter, e.g. Microsoft (internt) og diverse certificeringer. Evt. kombineret med online learning.

Alle tre specialiseringsretninger er interessante for erhvervslivet som enkeltkurser og her skal teorien blandes med hands-on og konsulentopgave. CENS-kurser er dyre og kun en uge intensivt og inkl rejseudgifter. Der vil en udspreddning til 3-6 måneder og en opgave være en differentiator (som beskrevet i oplægget).

Ad i: Konkurrence med certificeringer kommer hvis det bliver for teknisk.

Det er et meget langt sigt – det taler måske imod en master på 2 år. Men grundkompetencerne mangler. Dette kommer tilbage til målgruppen.

Ad vi: Er det overhovedet relevant at have en master for softwaresikkerhed for softwareudviklere? Det der efterspørges i forbindelse med opkvalificering af softwareudviklere er korte kurser, online kurser og lign. Det er relevant, men det kommer ikke til at ske i praksis. Der er brug for dybe kompetencer for softwareudviklere og ikke bredde. Lav i stedet en der er mere organisatorisk rettet – f.eks. en i risiko. Kobling mellem ledelse og teknik er en stor mangel.

Ad ii: Softwareudviklere og netværksfolk er meget forskellige – kan det virkelig samles i en uddannelse? Bliver uddannelsen for bred?

Ad ix: Der er en stigende efterspørgsel. Der er væsentligt over 40 IT-sikkerheds stillinger i Hovedstadsområdet i dag, mange bliver ikke slået op. Det er nok nærmere 400.

Der mangler kvalificerede CISO'er – der findes ikke mange med erfaringer (af naturlige årsager).

Disse stillinger slås ikke op og der et kæmpe samt stigende behov.

Hvor mange kan I sende på en master der er orienteret ledelsesniveauet? 1-2 stykker per firma.

Konsulentvirksomheder har mere brug for specialiseringskurserne eller et grundforløb (et crash kursus på 3 måneder fuld tid til nye folk).

Ministerierne skal opgraderes med nye funktioner – 50 styks. Dette kunne også være relevant for kommuner og andre ikke-IT virksomheder.

1-årig fuldtidsmaster er måske relevant? Tid er meget vigtig. Skills er ofte vigtigere end papir.

Engelsk sprog? Det er klart en fordel at uddannelsen er på engelsk. Det vil ikke forhindre nogen i at søge da engelsk er fagsproget indenfor IT-sikkerhed.

Opsummering:

Gentænk specialiseringer og få mere governance ind

Gentænk målgruppen – ledelsesniveau

Prisen og længden er svær – vi skal fokusere på ledelsesniveau og evt tænke på sponsorater

Start 2020 vil være bedre pga uddannelsesbudgetter for 2019 vil være fastsat inden da.

Hvis vi kan vinkle med Industriens Fond – så kan det måske lade sig gøre i industrien men ikke i det offentlige

Punkt 4. AOB

Der mangler en MSc i Cybersikkerhed. Kompetencerne findes på DTU men der mangler sikkerhedsvinklen. Godt med hackerlab mv. Generelt fokus på sikkerhed i uddannelserne på DTU er vigtige.

Fwd: spørgeramme

Christian D. Jensen

Wed 1/9/2019 3:25 PM

To:Line Katrine Harder Clemmensen <lkhc@dtu.dk>;

 1 attachments (52 KB)

Spørgeramme.docx;

Input fra [REDACTED]

Chr.

----- Forwarded Message -----

Subject:spørgeramme

Date:Wed, 9 Jan 2019 08:23:59 +0000

From:[REDACTED]

To:Christian Damsgaard Jensen <cdje@dtu.dk>

Kære Christian

Som aftalt et udfyldt skema

I mit område vil der være 1-2 kandidater og 1-2 kandidater i divisionen "Signal", som vil have glæde af at tage en master inden for Informationssikkerhed

Med venlig hilsen

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Fra: Line Katrine Harder Clemmensen <lkhc@dtu.dk>

Sendt: 2. november 2018 14:40:10

[REDACTED]

Cc: Christian D. Jensen; Anders Pall Skött

Emne: Master in Cyber Security (continuing education)

Dear [REDACTED],

We are in the process of developing a new continuing education (1 year) Master in Cyber Security at DTU. Anders Pall Skött has recommended you for the advisory board on the new Master. Would you be interested in joining such an advisory board?

Christian Jensen (cc'ed) will be the Head of Studies for the new Master. We are looking at an accreditation in February and a start of the Master program in the Fall 2019, if all goes well. Thus we would invite the advisory board to a meeting already this fall.

Sincerely,
Line Clemmensen
Head of Continuing Education
DTU Compute

Sv: Master i Cyber Security (continuing education)

[Redacted]

Sun 11/4/2018 2:09 PM

Inbox

To: Line Katrine Harder Clemmensen <lkhc@dtu.dk>;

Cc: Christian D. Jensen <cdje@dtu.dk>; Anders Pall Skött <anps@dtu.dk>;

Kære alle tre

Det var en rigtig god nyhed. Det har været et ønske længe, og er noget jeg meget gerne vil være med til at promovere!

Også mange tak fordi i tænkte på mig til advisory boardet! Det er jeg naturligvis meget glad for. Jeg er i den situation, at kalenderen permanent er for fuld, og jeg kan ikke påtage mig flere aktiviteter - både henset til min familie og kvaliteten af mit arbejde.

Det er en vigtig sag, så jeg vil gerne foranlede at Rådet udpeger en deltager til advisory boardet, hvis i har interesse. SU.

Som sagt vil jeg også gerne bidrage kommunikationsmæssigt. Hvis i får brug for det med omtale på LinkedIn, citater om behov osv. så tag gerne fat i mig.

Fortsat god søndag.

Med venlig hilsen

[Redacted signature block]

Sv: SV: Hælp vedr akkreditering af Master i Cybersikkerhed

[Redacted]

Tue 1/15/2019 10:35 PM

To: Line Katrine Harder Clemmensen <lkhc@dtu.dk>;

Cc: Christian D. Jensen <cdje@dtu.dk>;

Kære Line

Ja, jeg nåede ikke at samle op i mandags og i morgen drager jeg udenlands til og med lørdag, så det bliver ikke helt så elegant en opsamling som jeg havde forestillet mig, da jeg oprindeligt tænkte, at jeg ville høre lidt rundt i baglandet. Du får lige de tilbagemeldinger jeg har modtaget opsummeret nedenfor:

Godt tiltag:

Deltid

Godt forbundet til erhvervslivet

OK forbindelse til informationssikkerhed

Forhold der bør afklares:

Adgangskrav er for mig uklare

Relativ stor fokus på sw development, hvor jeg har en klar forventning om at det allerede ER inkluderet i Datalogi o.lign. og derfor måske ikke behøves her

Og så er der igen (helt på linie med de øvrige danske strategier) stor/alene fokus på udefrakommende angreb (APT mv.)

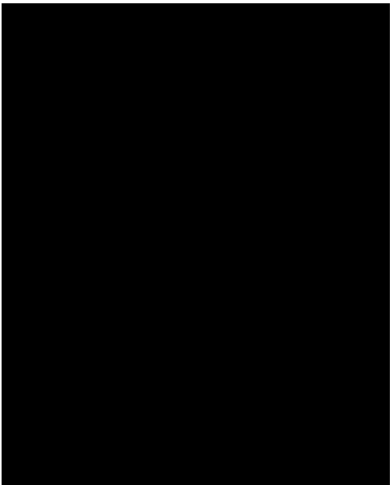
Med masterniveauet og prissætningen er det en relativ begrænset gruppe, de vil appellere til. De skiver selv it-sikkerhedsledere, og dette er nok korrekt vurderet. Jeg ser ikke denne masteruddannelse som et tilbud der har potentiale til at få en stor volumen, og dermed dække det store arbejdsmarkedsbehov for disse kompetencer. Det er et nicheprodukt. Jeg tror mere, at erhvervsakademiernes diplomuddannelse i it-sikkerhed kan appellere til en bredere skare, og har dermed også væsentligt større sandsynlighed for at kunne opbygge volumen.

Den rent indholdsmæssige del af uddannelsen er stærk på it-governance og infrastruktur, men relativt svag på udviklingssiden. Det bedste middel for it-sikkerhed, er at udvikle software og systemer der i designet er tænkt sikkert – både i forhold til udefra kommende angreb, såvel som privacyelementet – med andre ord privacy by design.

Med venlig hilsen

[Redacted]
[Redacted]
[Redacted]

[Redacted]



Fra: Line Katrine Harder Clemmensen <lkhc@dtu.dk>
Sendt: 15. januar 2019 22:10:20
Til: [REDACTED]
Cc: Christian D. Jensen
Emne: Re: SV: Hjælp vedr akkreditering af Master i Cybersikkerhed

Kære [REDACTED],

Er der noget nyt på denne tråd?

Tak
Line

From: Line Katrine Harder Clemmensen
Sent: Wednesday, January 9, 2019 3:22:33 PM
To: [REDACTED]
Cc: Christian D. Jensen
Subject: Re: SV: Hjælp vedr akkreditering af Master i Cybersikkerhed

Mange tak!
Line

Sendt fra min iPhone

Den 9. jan. 2019 kl. 15.21 skrev [REDACTED]:

Kære Line

Jeg har modtaget det og sendt det rundt i netværket. Jeg har bedt om kommentarer i denne uge og samler op på mandag.

Med venlig hilsen

[Redacted]
[Redacted]
[Redacted]

[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

[Redacted]

Fra: Line Katrine Harder Clemmensen <lkhc@dtu.dk>
Sendt: 8. januar 2019 21:54
Til: [Redacted]
Cc: Christian D. Jensen <cdje@dtu.dk>
Emne: Hjælp vedr. akkreditering af Master i Cybersikkerhed

Kære [Redacted],

Du tilkendegav tidligere at du kunne hjælpe os via dit netværk i forbindelse med opsætningen af en master i cybersikkerhed. Vil du have mulighed for at sende det foreslåede program til en master samt vedhæftede spørgeskema rundt i dit netværk?

Vi har brug for et bredt og veldokumenteret behov for masteren i denne form for at kunne få den akkrediteret.

Vi skal sende ansøgningen om akkreditering ind først i februar, så vi vil sætte pris på et få svar retur så hurtigt som muligt og helst senest 25/1 så vi kan nå at samle det hele.

På forhånd mange tak for hjælpen og godt nytår!

Mvh. Line

Studieleder for videreuddannelse

DTU Compute

RESUME

Møde i DTU's Aftagerpanel onsdag den 9. januar 2019

11. januar 2018

J.nr. 08/01140

chtra

Deltagere

Julie Helsted-Winkel for Jakob Holding Rasmussen (Novo Nordisk)

Michael Schulz Rasmussen (Cowi a/s)

Erik Bundgaard (Krüger A/S)

Inger Birgitte Kroon (Cowi a/s)

Claus Lundegaard (Intomics)

Hans-Aage Hjuler (Danish Power System)

Harrie Boonen (Lundbeck a/s)

Ib Enevoldsen (Rambøll)

Mette Juhl Jørgensen (Flexicon a/s)

Bo Vendelsø-Nielsen (Telia)

Kurt Agerbæk Christensen (Haldor Topsøe a/s)

Mikael Bundgaard-Nielsen (Novozymes)

Mogens Arentoft (MAN Energy Solutions)

Inge Sandholt (Sandholt Aps)

Hans Gottberg Rømer (Ørsted)

Steffen Frydendal Poulsen (Siemens Gamesa)

Fei Chen (Haldor Topsøe a/s)

Frank Nielsen (Radiometer)

Carsten Jensen (Dansk Dyrlægeforening)

Anne Lise Middelboe (DHI Group)

FRA AUS/DTU

Anders O. Bjarklev (rektor)

Philip Binning (Dekan)

Martin E. Vigild (Dekan)

Lars D. Christoffersen (Vicedekan, DTU Diplom)

Jørgen Jensen (Studiechef - Afdelingen for Uddannelse og Studerende)

Trine Eltang (Kontorchef – Afdelingen for Uddannelse og Studerende)

Mette Lilje (Chefkonsulent – Afdelingen for Uddannelse og Studerende)

Kit Bjerregård (Fuldmægtig, – Afdelingen for Uddannelse og Studerende)
Lone Hegelund (specialkonsulent - Rektoratet)
Christian D. Jensen (Lektor, DTU Compute)
Line Klemmensen (Lektor, DTU Compute)
Per Brockhoff (Institutdirektør, DTU Compute)
Helle Rootzén (Professor, DTU Compute)
Jan Madsen (Professor, DTU Compute)

Afbud Jesper Lomborg Manigoff (3shape)
Dorthe Lybye (Rockwool International)
Paw Allan Tinghus Petersen (Oxyguard a/s)
Anne-Lise Høgh Lejre (Teknologisk Institut)
Laila Grahl-Madsen (IRD Fuel Cells)
Esben Laulund (Chr. Hansen)
Niels Degn (Foss)
Michael Knørr Skov (Cowi)

Referent: Christa Trandum (Chefkonsulent – Afdelingen for Uddannelse og Studerende)

Dagsorden

1. **Velkomst**
Ved dekan dekan Martin E. Vigild og Philip Binning
2. **Siden sidst**
Ved dekan Philip J. Binning
3. **Præsentation af proces og foreløbige rammer for udviklingen af en ny DTU-strategi**
Ved rektor Anders O. Bjarklev
4. **Temadrøftelse: Digitalisering – hvordan forbereder vi de studerende til fremtidens digitale arbejdsmarked?**
Korte oplæg ved professor Helle Rootzén og professor Jan Madsen (DTU Compute) og efterfølgende diskussion
5. **Ny deltidsmasteruddannelse (efteruddannelse) i Cyber Security**
Ved lektor Christian D. Jensen (DTU Compute)
6. **Meddelelsepunkter**
Ved dekan Martin E. Vigild
7. **Evt**

[Af pladshensyn inkluderer dette referat kun pkt. 5]

5. Ny deltidsmasteruddannelse (efteruddannelse) i Cyber Security

Philip J. Binning gav en kort beskrivelse af de lovmæssige rammer for deltidsmasteruddannelser, at DTU søger om prækvalifikation af en ny deltidsmasteruddannelse i Cyber Security i Uddannelses- og Forskningsministeriet i dette forår, med henblik på at kunne udbyde uddannelsen fra efteråret 2019. Han gav herefter ordet til lektor Christian D. Jensen fra DTU Compute, der skal stå i spidsen for udviklingen af uddannelsen.

Christian D. Jensen orienterede om, at uddannelsen henvender sig til Masteruddannelsen kan med fordel følges af enhver med en IT baggrund, som ønsker en bred indføring og solid faglig fundering indenfor cybersikkerhed, men den retter sig især mod at styrke den faglige profil blandt medarbejdere der allerede varetager eller ønsker at kvalificere sig til IT-sikkerhedsledelsesopgaver i organisationer. Han uddybede også, at DTU med cybersikkerhed mener beskyttelse af data og trusler mod viden, enkeltpersoner eller virksomheder ligger inde med.

Adgangskravene følger retningslinjerne for DTU's masteruddannelser, dvs. der kræves en relevant bacheloruddannelse og minimum to års relevant erhvervserfaring efter gennemført adgangsgivende uddannelse. Omfanget af masteruddannelsen er 60 ECTS point, hvoraf 40 ECTS optjenes gennem kurser, 5 ECTS points gennem et midtvejsprojekt kursus (konsulent projekt) og 15 ECTS gennem et afsluttende masterprojekt. Uddannelsen tilrettelægges som deltidsundervisning inden for en tidsramme på normalt to år, idet størstedelen af aftagerne forventes at tage uddannelsen sideløbende med at de er i job.

Masteruddannelsen i Cybersikkerhed vil omfatte klasseundervisning i teoretiske-, teknologiske, organisatoriske, og menneskelige aspekter af cybersikkerhed, samt praktisk arbejde gennem praktiske øvelser der typisk tager udgangspunkt i den studerendes egen virksomhed, en konsulentopgave, og en afsluttende opgave der normalt tager udgangspunkt i en sikkerhedsproblemstilling i den studerendes egen virksomhed. Klasseundervisningen vil i hvert semester have et overordnet tema. I det første semester er dette tema IT-sikkerhedsledelse og governance, i det andet semester gennemgås de teknologier og systemer der udgør IT-sikkerhedsinfrastrukturen, i det tredje semester vil der være fokus på udvikling og drift af sikre applikationer og systemer, mens den studerende hovedsageligt vil arbejde med sit masterafhandlingsprojekt i fjerde semester.

Medlemmer af aftagerpanelet gav udtryk for, at det er overbevisningen, at DTU rammer et område, hvor de fleste virksomheder har en stigende opmærksomhed på, at der er et udækket behov. Det blev nævnt at netop ny teknologi stiller større og større krav til sikkerhed, og det blev også nævnt at æn på sikkerhed. Kunsten bliver at sammensætte et program der dækker behovet i erhvervslivet. En umiddelbar kommentar fra panelet var, at der er et behov for "hands on viden", der i praksis kan lukke huller hos virksomhederne. Hertil svarede Christian Jensen, at uddannelsen primært har fokus på ledelsesaspektet inden for cybersikkerhed, og ikke på at give konkrete værktøjer til øget sikkerhed.

Panelets medlemmer spurgte også mere konkret til antallet af studiepladser og om det vil være muligt at tage enkeltmoduler. Hertil svarede lektor Line Clemmensen, at der baseret på den foreløbige behovsundersøgelse, vil blive udbudt ca. 20 studiepladser årligt, men at der vil være mulighed for et let-

tere øget optag om nødvendigt. Virksomheder, der måske kun har brug for delelementer i uddannelsen vil også få mulighed for at sende enkeltfagskursister. Blandt aftagerpanelets medlemmer var der interesse for dette. Flere gav udtryk for, at det kunne vise sig praktisk at kunne shoppe enkeltkurser, både fra et ledelsesmæssige perspektiv, men også at kunne sende medarbejdere, der efterfølgende vil kunne lappe huller. Line Clemmensen informerede i forlængelse heraf om, at virksomheder, der har meget specifikke behov altid er velkomne til at kontakte DTU Compute med henblik på at få skræddersyede forløb.

Endelig spurgte panelet til, om der findes lignende tilbud i Danmark. Hertil forklarede Christian Jensen, at der ikke er lignende uddannelser i Københavns-området, men at der som en studielinje under IT-uddannelsen på IT Vest er et lignende spor. Her ud over er der en række private udbydere af kortere certificeringskurser, men ikke kurser der tilsammen bliver gradsgivende. Der er desuden professionsbachelorer på KEA og Århus Erhvervsakademi, men ingen efteruddannelsesmuligheder.

Dekan Philip J. Binning rundede punktet af med at konkludere, at Aftagerpanelet udtrykker fuld opbakning til DTU's ansøgning om prækvalifikation af uddannelsen.

Master i Cybersikkerhed

Introduktion

Efter spektakulære angreb mod Mærsk i 2017 og WannaCry ransomware-angrebet, der lammede dele af det britiske sundhedsvæsen tidligere samme år, er der kommet øget fokus på IT-sikkerhed og de risici danske virksomheder, myndigheder og borgere står overfor, som konsekvens af den stigende digitalisering af det danske samfund. Denne tendens er global og forventes at fortsætte i den forudseelige fremtid; IT-sikkerhedsorganisationen (ISC)² anslår at der netop nu mangler omkring 3 millioner IT-sikkerhedsmedarbejdere, heraf 142.000 medarbejdere i Europa [1], og en rapport fra den amerikanske IT-sikkerhedsvirksomhed Cybersecurity Ventures anslår at dette vil være 3,5 millioner ledige job indenfor cybersikkerhed i 2021 [2].

Vi har valgt at tage afsæt i de klare og gode definitioner fra Danmarks nationale cybersikkerhedsstrategi – 2018-2021:

”Cybersikkerhed omfatter beskyttelse imod de sikkerhedsbrud, der opstår som følge af angreb mod data eller systemer via en forbindelse til et eksternt net eller system. Arbejdet med cybersikkerhed fokuserer således på sårbarheder ved sammenkoblingen mellem systemer, herunder forbindelser til internettet” [3].

Der uddannes i dag få IT-specialister med kompetencer indenfor IT-sikkerhed i Danmark, hvor DTU Computes studielinie i Computersikkerhed på Informationsteknologi så vidt vides er den eneste danske kandidatuddannelse med hovedvægt indenfor IT-sikkerhed. Der findes desuden en specialisering indenfor Informationssikkerhed (med et mere begrænset kursusudbud) på datalogiuddannelsen på ITU, samt professionsbachelor uddannelser på erhvervsakademierne i København og Århus. Det samlede antal af nyuddannede fra DTU, ITU og erhvervsakademierne dækker dog langt fra de danske behov.

Der findes en række private kursusudbydere indenfor IT-sikkerhed, der tilbyder kurser (f.eks, CISSP, CISM og CEH), ligesom IT-Vest¹ udbyder en IT-Masteruddannelse med særlig fokus på IT-sikkerhed. Disse tilbud er generelt anerkendte og supplerer den traditionelle sidemandsoplæring i de danske virksomheder, men dette er ikke nok til at dække danske virksomheders behov for IT-sikkerhedsspecialister og -generalister.

DTUs masteruddannelse i Cybersikkerhed skal medvirke til at dække efterspørgslen på IT-sikkerheds-specialister med særlig fokus på de tekniske kompetencer, men samtidig med vægt på at se IT-sikkerhed i et bredere perspektiv, dvs. inddrage væsentlige emner vedr. ledelseskompetencer (der ellers håndteres under informationssikkerhedsområdet).

Målgruppe

Masteruddannelsen kan med fordel følges af enhver med en IT baggrund, som ønsker en bred indføring og solid faglig fundering indenfor cybersikkerhed, men den retter sig især mod at styrke den faglige profil blandt medarbejdere der allerede varetager eller ønsker at kvalificere sig til IT-sikkerhedsledelsesopgaver i organisationer. Det er således vigtigt at studerende på masteren bibringes en forståelse for de ledelses- og forretningsmæssige aspekter af cybersikkerhed, såvel som de teoretiske og teknologiske aspekter.

Målgruppe inkluderer således eksisterende IT-sikkerhedsledere som er blevet forfremmet til deres nuværende stilling på baggrund af en generel IT baggrund, enkelte certificeringskurser indenfor IT-sikkerhed og personlig interesse og erfaring, men ønsker en bredere teoretisk og teknologisk indsigt for at kunne indgå i en ligeværdig faglig dialog med specialiserede medarbejdere, konsulenter og leverandører.

¹ It-vest er et uddannelses- og forskningssamarbejde mellem Syddansk Universitet, Aalborg Universitet og Aarhus Universitet.

Med til målgruppen hører også den større gruppe af medarbejdere, der har ansvar for udvikling og/eller drift af centrale produkter, systemer og infrastruktur, hvor cybersikkerhed udgør et væsentligt element. Dette inkluderer produkt- og projektledere, IT-arkitekter, netværksarkitekter og –administratorer.

Uddannelsesprogrammet

Adgangskravene til deltidsmasterene følger retningslinjerne for DTU's masteruddannelser, dvs. der kræves en relevant bacheloruddannelse og minimum to års relevant erhvervserfaring efter gennemført adgangsgivende uddannelse. Vurdering af ansøgere til uddannelsen vil foregå i samarbejde med Afdelingen for Uddannelse og Studerende (AUS).

Omfanget af masteruddannelsen er 60 ECTS point, hvoraf 36 ECTS optjenes gennem kurser, 5 ECTS points gennem et midtvejsprojekt kursus (konsulent projekt) og 15 ECTS gennem et afsluttende masterprojekt. Uddannelsen tilrettelægges som deltidsundervisning inden for en tidsramme på normalt to år, idet størstedelen af aftagerne forventes at tage uddannelsen sideløbende med at de er i job. Kurserne og afgangsprojektet evalueres i overensstemmelse med 'Bekendtgørelse om eksamen og censur ved universitetsuddannelser'.

Masteruddannelsen i Cybersikkerhed vil omfatte klasseundervisning i teoretiske-, teknologiske, organisatoriske, og menneskelige aspekter af cybersikkerhed, samt praktisk arbejde gennem praktiske øvelser der typisk tager udgangspunkt i den studerendes egen virksomhed, en konsulentopgave², og en afsluttende opgave der normalt tager udgangspunkt i en sikkerhedsproblemstilling i den studerendes egen virksomhed. Klasseundervisningen (der også kan omfatte gruppearbejde) vil i hvert semester have et overordnet tema. I det første semester er dette tema IT-sikkerhedsledelse og governance, i det andet semester gennemgås de teknologier og systemer der udgør IT-sikkerhedsinfra-strukturen, i det tredje semester vil der være fokus på udvikling og drift af Sikre applikationer og systemer, mens den studerende hovedsageligt vil arbejde med sit masterafhandlings-projekt i fjerde semester. Den overordnede struktur er vist i Figur 1 og de overordnede temaer for hver af de tre kursussemestre forklares i det følgende, hvor de kurser der skal indgå i uddannelsen listes³.

Semester

Kursus Program

1	IT-sikkerhedsledelse og governance	
2	IT-sikkerhedsinfrastruktur	Konsulent projekt
3	Sikre applikationer og systemer	Tendenser & teknologier
4	Master afhandlings projekt	

Figur 1. Program for Master i Cybersikkerhed

² Konsulentopgaven er inspireret af konsulentopgaven på DTUs eMBA og tænkes gennemført ved at virksomheder kan foreslå projekter, som de studerende så vælger at arbejde på i mindre grupper.

³ Da uddannelsen tænkes udbudt på Engelsk, vil titlerne på de listede kurser være på Engelsk.

1. semester: IT-sikkerhedsledelse og governance

Det første semester giver en bred introduktion til de fundamentale begreber og principper indenfor cybersikkerhed, samt et solidt grundlag for god IT-sikkerhedsledelse og en risiko baseret tilgang til IT-sikkerhedsarbejdet, der tager højde for organisationens risikoprofil.

Der er identificeret følgende 5 ECTS kurser på første semester⁴:

1. Security principles (and their implementation in systems)
2. IT Security Governance (legislation/regulation/standards)
3. Risk Management

På baggrund af disse kurser vil masterstuderende have en solid forståelse af centrale begreber i cybersikkerhed og det teoretiske grundlag for hele studiet. Studerende vil også få en indføring i god praksis omkring IT-sikkerhedsarbejde, herunder hvordan politikker og kontroller afhænger af aktuelle trussels- og risikovurderinger (f.eks. forholdet mellem risiko-reduktion og omkostning ved at indføre en given kontrol; dette kaldes på Engelsk *risk leverage*). Studerende vil også have fået en introduktion til ledelsesmæssige discipliner som ledelsessystem, risiko styring, organisation, personalesikkerhed, styring af aktiver, fysisk sikkerhed og miljø sikkerhed, driftssikkerhed, leverandørforhold (herunder kravspecifikation og anskaffelser), nød-, beredskabs- og reetableringsstyring samt overholdelse af lovgivnings- og kontraktmæssige krav (jvf. ISO 27001 [4] og GDPR [5]).

2. Semester: IT-sikkerhedsinfrastruktur

Det andet semester fokuserer på sikkerheden i de systemer og den infrastruktur organisationer benytter til at opnå deres strategiske mål.

Der er identificeret følgende 5 ECTS kurser på andet semester:

1. Enterprise and Security Architectures
2. Identity and Access Management

På baggrund af disse kurser vil studerende forstå fundamentale principper omkring opbygning og drift af IT-systemer og -infrastrukturer og de værktøjer og teknologier der er nødvendige for at opnå den tilstrækkelige sikkerhed. Der vil være et særligt fokus på identitets og adgangskontrolsystemer, da disse spiller en central rolle i at regulere adgang til data og systemer.

3. Semester: Sikre applikationer og systemer

Det tredje semester fokuserer på fundamentale principper for udvikling, anskaffelse og drift af sikre IT-systemer, herunder applikationer og tjenester (Eng: *services*), samt beskyttelse af persondata i henhold til Persondataforordningen.

Der er identificeret følgende 5 ECTS kurser på tredje semester:

1. Application Security
2. Data Protection & Privacy
3. Trends and Technologies in Cybersecurity

På baggrund af disse kurser vil studerende kunne lede udvikling og/eller anskaffelse af IT-systemer, hvor der stilles krav til cybersikkerhed. Studerende vil desuden forstå den rolle systemets brugere spiller i det overordnede sikkerhedsbillede, samt hvordan de grundliggende sikkerhedsprincipper, der blev introduceret i det første kursus, realiseres i praksis. Studerende vil desuden have en forståelse af forskellige modeller for *privacy* og de teknikker og teknologier der kan benyttes for at optimere persondataskyttelsen og reducere risikoen for påtale og bøder i forbindelse med lækager. Endelig vil studerende få et overblik over de seneste trends og sikkerhedsteknologier indenfor centrale områder.

⁴ Det overvejes om der senere skal søges særskilt akkreditering af nogle (eller alle) 5 ECTS kurser på Master i Cybersikkerhed, således at der kan optages enkeltkursusstuderende på disse af masterprogrammets kurser.

4. Semester: Masterafhandlingsprojekt

Det fjerde og sidste semester er afsat til den afsluttende opgave, hvor den studerende vil demonstrere en samlet forståelse af de emner der er blevet gennemgået i kurserne, ved at løse en større IT-sikkerhedsopgave, typisk fra egen organisation.

Kursusstruktur

Kursusstrukturen vil typisk være 3 x 2 dages on site undervisning, med hjemmearbejde mellem de to kursusperioder, således at den studerende arbejder aktivt med kursusmaterialet mellem møderne og vha de intense moduler får et godt netværk gennem de andre studerende. Kurserne vil afsluttes med en eksamen eller en opgave der relaterer til problemstillinger i de organisationer de studerende rekrutteres fra. Denne struktur giver desuden større fleksibilitet i forhold til den studerendes normale arbejde. For at forøge netværksaspektet og synergien mellem de studerende på masteren vil der desuden være en studietur i forbindelse med et af kerne kurserne til et relevant cybersikkerheds miljø. Forslag er: Carnegie Mellon Universitetet i Pittsburgh som er hjemsted for SEI (med verdens første Computer Emergency Response Team – CERT) og CyLab med mere end 300 forskere tilknyttet.

Projektkurset med et konsulentprojekt giver firmaerne der har ladet en medarbejder deltage i uddannelsen mulighed for at fremlægge en case som studerende derefter kan vælge at løse som en konsulentopgave under vejledning af underviserne.

Forventet positivt udbytte

Ved at udbyde en Master i Cybersikkerhed, vil DTU bidrage til at dække et alvorligt behov for kompetencer i Danmark og danne grundlag for en succesfuld fortsat digitalisering af det danske samfund. Uddannelsen forventes i øvrigt at medvirke til synliggørelse af DTUs kompetencer indenfor IT-sikkerhed, både overfor de studerende på uddannelsen og den bredere danske offentlighed. Dette vil kunne danne grundlag for et styrket forskningssamarbejde mellem DTU og danske virksomheder og myndigheder.

På de indre linjer, vil samarbejdet omkring en Master i Cybersikkerhed, være med til at skabe øget synlighed og samarbejde på tværs af de institutter der tænkes at indgå i undervisning på uddannelsen; disse kunne omfatte DTU Compute, DTU Fotonik, DTU Diplom, samt DTU Management.

Faglig profil og mål for læringsudbytte

Det tilstræbes at udbyde en masteruddannelse, som berører alle de væsentligste aspekter af cybersikkerhed, samt vigtige elementer fra det overordnede begreb "informationssikkerhed". Målet er at skabe et fagligt overblik til nytte for de, der arbejder (eller vil arbejde) med IT-sikkerhed indenfor en af de tre specialiseringer defineret ovenfor: softwaresikkerhed, netværkssikkerhed og systemsikkerhed.

Kandidater der har gennemført uddannelsen forventes at kunne:

- Udarbejde **sikkerhedsplaner** for IT-systemer, herunder:
 - Gennemføre risikoanalyser af IT-systemer
 - Identificere sikkerhedsmål for et givet IT-system
 - Formulere sikkerhedspolitikker for et givet IT-system
 - Implementere sikkerhedsteknologier der understøtter de definerede sikkerhedspolitikker
- Udarbejde **beredskabsplaner** for IT-sikkerhedshændelser (incident response)
- Udarbejde **nødplaner** for katastrofeshændelser relateret til IT-anvendelsen med henblik på at opretholde virksomhedens funktioner, evt. inklusiv en genetablering af driftsfaciliteterne
- Forestå **udvikling af sikre IT-systemer**, herunder:
 - Udvikling af sikre software systemer
 - Udvikling af sikre kommunikationsprotokoller
 - Design og drift af sikre netværk

- Gennemføre **sikkerhedsanalyse** af IT-systemer (inkl. "ethical hacking" / penetration testing)

Prissætning

Post	Detaljer	ECTS	Pris (DKK)
Kurser	ECTS givende kurser	35	200.000
Konsulent opgave (projekt)	Vejledning og konsulentbistand	10	45.000
Afsluttende MS projekt	Vejledning og eksamen	15	55.000
Studietur	Rejseudgifter	-	50.000
Total			350.000

Figur 2. Prissætning for uddannelsen

Forskningsbaseret uddannelse

Uddannelsen giver en bred introduktion til emnet cybersikkerhed baseret på forskning i flere af DTU Computes sektioner samt på DTU Fotonik, DTU Diplom og DTU Management. Undervisningsformen giver mulighed for at mange forskellige undervisere med hver deres faglige specialviden kan bidrage til udviklingen af undervisningsmateriale samt til afholdelsen af kurser. I forbindelse med afgangsprojektet vil de studerende være i tæt kontakt med en vejleder, hvilket er en oplagt mulighed for at integrere forskning og uddannelse. Der lægges i øvrigt op til at undervisningsmateriale fra uddannelsen også inddrages i kandidatkurser på campus, i det omfang det er relevant, f.eks. på studielinen i Computersikkerhed.

Intern kvalitetssikring

I 2013 blev den nye akkrediteringslov indført i Danmark og de første universiteter, herunder DTU, blev i løbet af 2014 institutionsakkrediteret. En institutionsakkreditering er en vurdering af, om institutionens kvalitetssikringssystem er velbeskrevet og veldokumenteret og også fungerer i forbindelse med det daglige arbejde. Systemet skal sikre, at institutionen hele tiden har fokus på kvaliteten, udvikler den løbende og reagerer, når der er noget galt. Med en positiv institutionsakkreditering påhviler det universiteterne selv at sikre løbende og systematiske evalueringer af institutionens samlede undervisnings- og uddannelsesudbud.

Masteruddannelsen i cybersikkerhed vil således være omfattet af DTUs generelle kvalitetssystem. I lighed med uddannelser på campus vil der ske en løbende evaluering af hvert kursus samt af programmet som helhed.

Investeringsvurdering og evaluering

Oprettelse af en masteruddannelse i Cybersikkerhed kræver ingen særlige anlægsaktiver, idet uddannelsen ligger i forlængelse af eksisterende og planlagte aktiviteter indenfor cybersikkerhed på DTU.

Det primære behov for investering vil således vedrøre udvikling af nye og tilpasning af eksisterende kurser til uddannelsen. Denne investering afholdes i første omgang af de enkelte institutter der indgår i uddannelsen, men forventes tilbagebetalt, dels gennem indtjeningen på uddannelsen og dels gennem afledte effekter, såsom større synlighed og flere rentable industrikontakter indenfor området.

I forbindelse med afholdelse af de enkelte kurser vil der endvidere kunne opstå behov for særligt udstyr og licenser til særligt software, hvilket afhænger direkte af antallet af studerende og behovet skal derfor kunne dækkes af deltagernes kursusafgift.

Vigtige risici

De primære risici vedrører truslen fra eventuelle konkurrenter, samt et kompetencetab på DTU, som gør det umuligt at gennemføre uddannelsen.

Der er på nuværende tidspunkt kun en konkurrent i Danmark, nemlig masteruddannelsen på IT-Vest, men det anses for usandsynligt at det samlede behov for videre-/efteruddannelse på højt niveau indenfor cybersikkerhed i Danmark dækkes af det kombinerede udbud fra disse to uddannelser.

Masteruddannelsen i Cybersikkerhed udbydes i samarbejde mellem tre institutter på DTU: DTU Compute, DTU Fotonik og DTU Diplom (med mulighed for yderligere at samarbejde med DTU Management). På DTU Compute inddrages kompetencer fra mere end 10 medarbejdere i tre sektioner, så understøttelsen er særdeles robust og faren for et fatalt kompetencetab vurderes ikke eksisterende.

Referencer

- [1] (ISC)², »(ISC)² CYBERSECURITY WORKFORCE STUDY,« (ISC)², Clearwater, Florida, U.S.A., 2018.
- [2] S. Morgan, »Cybersecurity Jobs Report: 2017 edition,« Cybersecurity Ventures (sponsored by Herjavec Group), Northport, New York, U.S.A., 2017.
- [3] Regeringen, »National strategi for cyber- og informationssikkerhed,« Finansministeriet, København, 2018.
- [4] ISO/IEC JTC 1/SC 27, »ISO27001: Information Security Management System (ISMS) standard,« International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2013.
- [5] »Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),« *Official Journal of the European Union*, årg. L119, pp. 1-88, 2016.