Uddannelses- og Forskningsministeriet

Prækvalifikation af videregående uddannelser - cybersikkerhed

Udskrevet 13. november 2026

Professionsbachelor - cybersikkerhed - Aalborg Universitet

Institutionsnavn: Aalborg Universitet
Indsendt: 13/09-2024 10:58
Ansøgningsrunde: 2024-2
Status på ansøgning: Godkendt
Afgørelsesbilag
Download den samlede ansøgning
Læs hele ansøgningen

Ansøgningstype
Ny uddannelse

Udbudssted
København.

Informationer på kontaktperson for ansøgningen (navn, email og telefonnummer)
Elisabeth Frederiksen, elba@adm.aau.dk, 99407377

Er institutionen institutionsakkrediteret?
Ja

Er der tidligere søgt om godkendelse af uddannelsen eller udbuddet?
Nej

Uddannelsestype
Professionsbachelor

Uddannelsens fagbetegnelse på dansk
cybersikkerhed

Uddannelsens fagbetegnelse på engelsk
Cyber security

Angiv den officielle danske titel, som institutionen forventer at bruge til den nye uddannelse
Diplomingeniør i cybersikkerhed; Professionsbachelor i ingeniørvirksomhed

Angiv den officielle engelske titel, som institutionen forventer at bruge til den nye uddannelse
Bachelor of Engineering in Cyber Security

Hvilket hovedområde hører uddannelsen under?
Tekniske område

Hvilke adgangskrav gælder til uddannelsen?
Optagelse pa■ diplomingeniøruddannelsen i cybersikkerhed forudsætter en gymnasial uddannelse med de specifikke adgangskrav:

- Matematik A (karakterkrav på mindst 4,0)
- Engelsk B
- Fysik B eller geovidenskab A

jf. Adgangsbekendtgørelsen, BEK nr. 36 af 13/01/2022, Bilag 1.

Uddannelsen giver adgang til kandidatuddannelsen i cybersikkerhed, AAU.

Er det et internationalt samarbejde, herunder Erasmus, fællesuddannelse el. lign.?
Nej

Hvis ja, hvilket samarbejde?

Hvilket sprog udbydes uddannelsen på?
Dansk

Er uddannelsen primært baseret på e-læring?
Nej, undervisningen foregår slet ikke eller i mindre grad på nettet.

ECTS-omfang
210

Beskrivelse af uddannelsens formål og erhvervssigte. Beskrivelsen må maks. fylde 1200 anslag

Uddannelsens adresserer et stigende behov for ingeniører med kompetencer i cybersikkerhed. Der uddannes langtfra tilstrækkeligt mange, og virksomhederne oplever i stigende grad problemer med rekruttering. De efterspørger kompetencer inden for databeskyttelse, risikohåndtering, lovgivning og compliance og beskyttelse af kritisk infrastruktur, og især mindre virksomheder (SMV'er) er under pres for at kunne modstå cybertrusler. I Danmark udbyder universiteter og erhvervsakademier uddannelser på forskellige niveauer inden for it og cybersikkerhed. Den foreslåede uddannelse fokuserer på tre søjler: (1) grundlæggende færdigheder i matematik og programmering, (2) viden og praktiske færdigheder inden for cybersikkerhed, der omfatter datasikkerhed, netværkssikkerhed, trusselsanalyse og etisk hacking, cloud-sikkerhed og AI, samt (3) sikkerhed i organisationer i form af risikostyring, databeskyttelse, compliance, lovkrav og forretningsforståelse. Denne kompetenceprofil dækkes ikke af beslægtede uddannelser. Uddannelsen udbydes i København grundet høj koncentration af aftagervirksomheder, eksisterende forskningsaktivitet samt ønske om videreudvikling af AAU's uddannelsesporteføljе i København

Uddannelses struktur og konstituerende faglige elementer

Uddannelsen er tilrettelagt som et sammenhængende program med en naturlig akademisk progression, som kan gennemføres inden for en tidsramme på 3½ år. Uddannelsen består af 210 ECTS-points, der er fordelt på syv semestre med hver 30 ECTS-point. Bortset fra 6. semester, består hvert semester af kursusmoduler og et projektmodul, der alle afsluttes med eksamener.

Uddannelsen starter med generel viden på 1.-2. semester og fortsætter derefter med mere avancerede cybersikkerhedskurser fra 3. semester, herunder kurser i "Etisk hacking", "Datasikkerhed og privatlivsbeskyttelse" og "Risikohåndtering". Uddannelsens struktur tilbyder en række valgmuligheder, som gør det muligt for de studerende at specialisere sig i forskellige retninger. Kursusmodulerne er brancheorienterede og giver de studerende den grundlæggende viden, færdigheder og evner til at forstå metode og teori bag et bestemt fagområde. Projektmodulerne lægger vægt på en tværfaglig tilgang, hvor de studerende arbejder i grupper og skal anvende deres viden ved at løse virksomhedsrelevante problemer i en praktisk sammenhæng.

Nedenfor beskrives titel, mål, indhold samt ECTS- point for de enkelte moduler. Uddannelsens endelige kompetenceprofil findes i Bilag 1 i dokumentationsrapporten. På alle semestre anvendes kompetencer og læring fra kursusmodulerne i projektmodulet.

1. SEMESTER:

P0 projekt: Teknologisk projektarbejde (Projektmodul 5 ECTS-point): Den studerende skal gennem projektmodulet opnå viden om den problemorienterede læringsmetode (PBL). P0 gennemføres i grupper, og de studerende sættes i stand til at løse en virkelighedsnær problemstilling ved at analysere cybertrusler og udføre trusselsmodellering i en realistisk brugssituation.

P1 projekt: Cybertrusler og cyberangreb (Projektmodul 10 ECTS-point): I P1-projektet skal de studerende tilegne sig viden inden for cybersikkerhed gennem teoretisk og praktisk arbejde. Der tages udgangspunkt i en samfunds- eller erhvervsrelevant problemstilling, der kan løses ved hjælp af teorier og metoder inden for feltet. I projektet arbejder de studerende med at designe og implementere en sikker applikation baseret på forskellige sikkerhedsprincipper.

Introduktion til cybersikkerhed (Kursusmodul 5 ECTS-point): Kursusmodulet giver et fundament i koncepter, terminologi og best practice for cybersikkerhed. De studerende udforsker cybertrusselslandskabet, angrebsmetoder, sårbarheder og sikkerhedsløsninger og udvikler færdigheder i kritisk tænkning og problemløsning for at kunne træffe informerede beslutninger i forbindelse med brancherelaterede scenarier.

Imperativ programmering (Kursusmodul 5 ECTS-point): Studerende opna■r pa■ dette kursus grundlæggende færdigheder i imperativ programmering og forsta■else for specifikke begreber som kontrolstrukturer, abstraktion med procedurer og funktioner, datastrukturer, fil input-output og simple algoritmer.

Problembaseret læring (Kursusmodul 5 ECTS-point): Kurset giver deltagerne en grundig introduktion til centrale tilgange, begreber og teknikker i problembaseret læring. Deltagerne opnår viden om at identificere, analysere og formulere et åbent og komplekst problem i en samfundsmæssig kontekst.

2. SEMESTER:

P2 projekt: Netværkssikkerhed (Projektmodul 15 ECTS-point): De studerende designer og implementerer en cybersikkerhedsløsning til at sikre datatransmission over et netværk og simulerer et scenarie i den virkelige verden, hvor sikkerheden er kritisk. Projektet involverer client-server kommunikation og overvejelser om sikker dataudveksling mellem klienter og servere.

Sikkerhed i computersystemer (Kursusmodul 5 ECTS-point): Kursusmodulet introducerer de studerende til centrale koncepter og metoder for netværkssikkerhed. På dette kursus får de studerende viden og praktiske færdigheder i forhold til at kunne beskytte systemer mod angreb og opdage, hvis systemer er blevet kompromitteret, men også til at konstruere sikre systemer.

Computernetværk (Kursusmodul 5 ECTS-point): Kursusmodulet introducerer konceptet computernetværk og internettet samt tilknyttede teknologier. Kurset giver en grundig indføring i TCP/IP referencemodellen, og hvordan kommunikation håndteres på internettet.

Matematik for cybersikkerhed (Kursusmodul 5 ECTS-point) Dette kursus handler om det matematiske grundlag, der er afgørende for cybersikkerhed. De studerende får viden om mængdeteori, algoritmer, kompleksitetsanalyse, logaritmer, kombinatorik, lineær algebra og vektorrum.

3. SEMESTER:

Sikkerhed i applikationsudvikling (Projektmodul 15 ECTS-point): I projektmodulet får de studerende kompetencer i udvikling af en sikkerhedsløsning til en applikation, et netværk eller et indlejret system (eller en kombination af disse) ud fra de nyest tilgængelige teknologier.

Etisk hacking (Kursusmodul 5 ECTS-point): Dette kursus handler om metoder til penetrationstest, herunder rekognoscering, sårbarhedsanalyse og teknikker til at identificere og adressere sikkerhedssvagheder i systemer før og efter et sikkerhedsbrud. Gennem praktiske øvelser vil de studerende lære om etisk udnyttelse af systemer at opdage sårbarheder, og at udvikle strategier til at sikre netværk.

Web-programmering og databaser (Kursusmodul 5 ECTS-point): Dette kursus giver de studerende færdigheder inden for webprogrammering og grundlæggende viden om databaser. De studerende lærer at udvikle dynamiske webapplikationer, analysere sårbarheder og designe sikre løsninger ved hjælp af client- og server-side teknikker.

Computerarkitekturer og operativsystemer (Kursusmodul 5 ECTS-point): Dette kursus dykker ned i den grundlæggende struktur af computerarkitekturer, udforsker datastier, hukommelseshierarkier og pipelining. Herudover undersøges operativsystemer, inkl. processtyring, hukommelsesstyring (virtuel hukommelse), filsystemer og I/O-systemer.

4. SEMESTER:

Cyberangreb og -forsvar (Projektmodul 15 ECTS-point): I dette projektmodul arbejder de studerende med et konkret system og lærer, hvordan det kan angribes og/eller forsvares. Ved at lære at "tænke som en angriber" får de studerende en bedre forståelse af, hvordan systemer kan sikres mod angreb, og hvordan angreb opdages.

Risikohåndtering (Kursusmodul 5 ECTS-point): Dette kursus handler om metoder til at identificere, analysere og prioritere cybersikkerhedstrusler i samspil med risikohåndtering, business continuity-planer og omkostningseffektive sikkerhedsløsninger.

Datasikkerhed og privatlivsbeskyttelse (Kursusmodul 5 ECTS-point): Dette kursus dækker teknikker til at beskytte dataintegritet, fortrolighed og tilgængelighed. De studerende udforsker kryptering, adgangskontrol og sikre kommunikationsmetoder for at beskytte følsomme oplysninger mod cybertrusler.

Sandsynlighedsregning og statistik (Kursusmodul 5 ECTS-point): Dette kursusmodul giver studerende kompetencer i at anvende dataanalyse og processering i forståelsen af ingeniørmæssige opgaver. Kursusenheden introducerer fundamentale begreber og metoder for sandsynlighedsregning og statistik.

5. SEMESTER:

Cybersikkerhed i distribuerede systemer (Projektmodul 15 ECTS-point) (valgfrit): I dette projekt designer og implementerer de studerende et sikkert distribueret system. Systemet kan inkludere IoT-, OT- og edge-enheder og en cloud-server. Studerende kan bruge machine learning og AI til at sikre deres system.

Cybersikkerhed og governance (Projektmodul 15 ECTS-point) (valgfrit): Dette projekt handler om at designe "security awareness" kampagner, udføre risikovurderinger og foreslå afværgestrategier for cybersikkerhedstrusler. Derudover vil de studerende udforske de juridiske og regulatoriske rammer for cybersikkerhed og governance i Europa.

Cloud-sikkerhed (Kursusmodul 5 ECTS-point): Dette kursus udstyrer de studerende med viden og kompetencer til at bygge sikre distribuerede systemer i skyen, udforske cloud-implementering og cloudservice modeller sammen med aktuelle trends og sikkerhedsovervejelser for cloud, virtualisering og edge computing.

Sikkerhed i IoT- og OT-miljøer (Kursusmodul 5 ECTS-point): Dette kursus gør de studerende i stand til at navigere i sikkerhedsudfordringerne ved sammenkoblede IoT- og OT-miljøer. Ved at udforske nye teknologier og forskellige IoT- og OT-enheder vil deltagerne få grundlæggende viden om sikkerhedskoncepter og best practice for sikring af disse komplekse systemer.

Machine Learning og AI i cybersikkerhed (Kursusmodul 5 ECTS-point) (valgfag): Kursusmodulet introducerer koncepter som statistisk interferens og data mining-algoritmer og beskriver, hvordan machine learning og kunstig intelligens anvender disse algoritmer til forbedring og løsning af problemstillinger inden for cybersikkerhed.

Sikkerhed i organisationer (Kursusmodul 5 ECTS-point) (valgfag): Dette kursus giver de studerende viden og færdigheder til at sikre virksomhedens data, aktiver og infrastruktur. Ved at udforske sikkerhedspolitikker, procedurer, incident response og nye trusler lærer deltagerne at udvikle og implementere effektive sikkerhedsstrategier. Dette kursus dækker også forståelse af menneskelige faktorer, der påvirker onlineadfærd og cybersikkerhed i organisationer.

6. SEMESTER:

Ingeniørpraktik (Projektmodul 30 ECTS-point): Praktikforløbet giver de studerende mulighed for at anvende deres akademiske viden på cybersikkerhedsudfordringer i den virkelige verden, samtidig med at de udvikler værdifulde professionelle kompetencer. Ved at integrere praktikanter i igangværende projekter kan virksomheder styrke deres rekrutteringsmuligheder og få adgang til nye perspektiver og potentielt samarbejde om den studerendes afsluttende projekt. Til gengæld for deres bidrag opnår praktikanterne et godt fundament for en fremtidig karriere inden for cybersikkerhed.

7. SEMESTER:

Bachelorprojekt (Projektmodul 20 ECTS-point): I det sidste semester arbejder de studerende på færdiggørelsen af bacheloropgaven, som giver dem mulighed for at anvende teoretisk viden og praktiske færdigheder, som de har lært under deres studie. Projekt skal desuden demonstrere deres generelle færdigheder inden for problemanalyse og ingeniørvidenskab.

Projektledelse og forretningsforståelse (Kursusmodul 5 ECTS-point): Dette kursus udstyrer de studerende med væsentlige færdigheder i at planlægge, udføre og styre ingeniørprojekter effektivt. De studerende lærer om projekters livscyklus, risikostyring og ledelsesteknikker, der kan sikre en succesfuld projektgennemførelse i tekniske miljøer, og de får indsigt i projekternes forretningsmæssige kontekst.

Malware-analyse (Kursusmodul 5 ECTS-point) (valgfag): Dette kursus dækker teknikker til at identificere, dissekere og eliminere skadelig software. Det inkluderer avancerede reverse engineering-teknikker og software security practices, der giver de studerende ekspertise i at analysere og beskytte systemer mod cybertrusler.

Cybersikkerhed lovgivning (Kursusmodul 5 ECTS-point) (valgfag): Dette kursus handler om global cybersikkerhedslovgivning med fokus på EU-direktiver og forordninger. Studerende lærer, hvordan disse regler påvirker organisationer og vigtigheden af compliance for opretholdelse af sikre digitale miljøer.

Begrundet forslag til takstindplacering af uddannelsen

Takst 3: Den foreslåede uddannelse er en professionsbacheloruddannelse under det teknisk-videnskabelige hovedområde.

Forslag til censorkorps

Diplomingeniøruddannelsernes censorkorps

Dokumentation af efterspørgsel på uddannelsesprofil - Upload PDF-fil på max 30 sider. Der kan kun uploades én fil

Dokumentationsrapport PBA cybersikkerhed.pdf

Kort redegørelse for det nationale og regionale behov for den nye uddannelse. Besvarelsen må maks. fylde 1800 anslag

Cybertrusler og -angreb udgør et stigende problem for alle dele af samfundet. Det er ressourcekrævende for virksomheder og organisationer, der må leve op til lovgivningen om cybersikkerhed fx GDPR, NIS2-direktivet og Cyber Resilience Act, og krav om compliance (ISO, IEC, m.fl.). De har svært ved at rekruttere medarbejdere med de rette kompetencer, og samlet set uddannes der ikke tilstrækkeligt mange ingeniører og it-kyndige. I behovsundersøgelsen angiver 85% af virksomhederne, at de i nogen eller høj grad har et behov for ingeniører med kompetencer inden for cybersikkerhed i dag, og 69% forventer, at behovet vil stige de kommende år. Dansk Industri (DI Digital) advarede i 2022 om, at Danmark i 2030 vil mangle 15-20.000 fagfolk inden for cyber- og informationssikkerhed. Som det fremgår af dokumentationen, er der ikke mange uddannelser i Danmark, som giver de nødvendige kompetencer, og universiteter og erhvervsakademier leverer ikke nok dimittender. Behovsafdækningen viser, at der i 2022 kun blev uddannet 183 bachelor-dimittender med en cybersikkerhedsprofil samt 62 professionsbachelorer (estimeret) med en cybersikkerheds top-up uddannelse, hvilket ialt giver 245 dimittender. Behovet for flere dimittender inden for it-området kan kun dækkes ved at udvide det samlede bachelor-/professionsbacheloroptag i Danmark. I behovsundersøgelsen er det tydeliggjort, at det største behov er i hovedstadsområdet. Den gennemsnitlige ledighed for beslægtede uddannelser for dimittendårgang 2021 er på 1,6%, mens beskæftigelsesprocenten ligger mellem 97-100% i 2021 (UFM's datavarehus). Der er således et behov for den nye uddannelse pa■ arbejdsmarkedet. Dels pa■ grund af den aktuelle og fremtidige store mangel pa■ ingeniører inden for området, dels pa■ grund af det identificerede kompetencegab

Uddybende bemærkninger

I september 2022 beskrev en rapport udarbejdet af regeringens sikkerhedspolitiske analysegruppe udfordringerne for dansk sikkerhed og forsvar frem mod 2035 (se dokumentationsrapporten s. 1). DI Digital, Rådet for Digital Sikkerhed og en række andre organisationer fremsendte d. 30. jan. 2023 et "bekymringsbrev" til regeringen, hvori de understregede behovet for en samlet indsats og beskrev 11 konkrete forslag til at fremme opbygningen af cyber-kompetencer i Danmark, herunder et øget optag på uddannelser i cybersikkerhed.

Ovennævnte rapport understregede, at der er kritisk mangel på cybersikkerhedskompetencer i danske virksomheder, og at det gør Danmark sårbar. Mere end hver 3. it-virksomhed efterspørger kompetencer inden for it og cybersikkerhed, og det vurderes, at der i 2030 vil mangle mellem 15.000-20.000 fuldtidsansatte. IDA vurderede i 2023 (se dokumentationsrapporten s. 10), at der i Danmark er et stort behov for kompetencer inden for cybersikkerhed: Ca. 40% af alle SMV'er mangler kompetencer inden for it- og cybersikkerhed, og i den offentlige sektor har kun 54% af de samfundskritiske it-systemer et tilstrækkeligt sikkerhedsniveau. Det konkluderes i samme rapport, at der skal være langt flere uddannede inden for cybersikkerhed, og at det som minimum skal sikres, at der på eksisterende uddannelser kan udbydes flere kurser inden for cybersikkerhed. Rapporten vurderer, at der i 2030, med den nuværende uddannelsesporteføljе, vil blive uddannet 8.000 flere inden for it- og cybersikkerhedsuddannelserne sammenlignet med 2021, men at der alligevel vil mangle 22.000 it-folk, hvoraf ca. 15.000 af disse skal it-uddannes i mellemlange og lange videregående uddannelser. Ekspertgruppen vurderer i samme publikation, at der er et væsentligt udækket behov for specialister i cybersikkerhed.

Dette er på linje med, hvad Epinions behovsundersøgelse fandt. En af behovsundersøgelsens hovedkonklusioner (Epinion, side 3) er, at virksomhederne efterspørger både faglige og organisatoriske kompetencer blandt ingeniører inden for cybersikkerhed. 85 pct. af virksomhederne i undersøgelsen angiver, at de i nogen eller høj grad har et behov for ingeniører med kompetencer inden for cybersikkerhed i dag. De forventer desuden, at behovet vokser de kommende år - blandt andet som følge af et øget trusselsbillede og ny lovgivning på området. 69 pct. af virksomhederne forventer, at behovet for denne typer af ingeniører vil være større om tre år, end det er i dag, mens 28 pct. forventer, at behovet vil være det samme. 52 pct. af virksomhederne synes, at rekrutteringen i dag er svær eller meget svær, og 27 pct. har aktuelt ledige stillinger på området. I fremtiden forventer 30 pct. af virksomhederne, at rekrutteringssituationen vil være den samme som nu, mens 42 pct. tror, at det vil være endnu sværere at rekruttere om tre år, end det er i dag.

Ansøgningen om diplomingeniøruddannelsen i cybersikkerhed indgår i en samlet strategi for Det Tekniske Fakultet for IT og Design, hvor AAUs uddannelsesportefølje på campus København fremover vil være koncentreret inden for STEM-området. Udbygningen skal desuden ses i sammenhæng med AAU's Digitaliseringsstrategi, som sigter mod at styrke udviklingen af digitale teknologier inden for forskning, uddannelse og videnssamarbejde. Siden 2020 er der på AAU's Campus København lanceret bacheloruddannelser i software og cyber- og computerteknologi samt kandidatuddannelser i cybersikkerhed og software. Kandidatuddannelsen i cybersikkerhed på AAU er den første og hidtil eneste i Danmark, som udelukkende fokuserer på dette område. På andre kandidatuddannelser på andre universiteter indgår det som et delelement sammen med andre områder. Uddannelsen havde sit første optag i september 2020, og de første kandidater dimitterede i juni 2022. Der har været en betydelig vækst i optaget fra ca. 30 ved 1. optag til ca. 80 ved optaget i 2024 og tilsvarende i antallet af færdiguddannede. I 2024 ansøgte 334 om optag.

I dokumentationsrapporten (s. 7-8) er der identificeret ni efterspurgte kompetenceområder på baggrund af aftagervirksomhedernes aktuelle såvel som fremtidige behov. Disse er (1) Datasikkerhed, herunder sikker håndtering af persondata (GDPR m.m.), (2) Risikovurdering og -håndtering, (3) Design og udvikling af sikre systemer og software, (4) Compliance (f.eks. NIS2, D-Mærket, relevante standarder som ISO 270xx mm.), (5) Forebyggelse og detektion af cyberangreb, (6) Sikkerhed i computersystemer, (7) Netværkssikkerhed, (8) Kritisk infrastruktur, (9) IoT-, OT og Cloud-sikkerhed. I dokumentationsrapporten er sammenhængen mellem uddannelsesstrukturen og virksomhedernes behov præsenteret. Både fag og projektmoduler giver kompetencer i bl.a. de digitale kompetenceområder, der er efterspurgt ovenfor. I undersøgelsen blev virksomhederne præsenteret for en kort beskrivelse af den nye uddannelse, og på baggrund heraf vurderer 69 pct. af virksomhederne, at det i høj eller nogen grad vil være relevant for dem at ansætte en sådan diplomingeniør i deres virksomhed i fremtiden.

For at forstå behovet for en ny uddannelse er 17 beslægtede uddannelser analyseret i forhold til tilgangen til - og kapaciteten på - uddannelserne (se dokumentationsrapporten s. 15). De uddannelser, som er tættest beslægtet med diplomingeniøruddannelsen i cybersikkerhed, er bacheloruddannelserne i hhv. cyber- og computerteknologi (AAU) og computerteknologi (AAU), hvor der er flere overlappende kompetencer, men hvor virksomhedstilknytningen ikke er så stærk. Bacheloruddannelserne i software (AAU) og cyberteknologi (DTU) har overlappende kompetencer inden for matematik og programmering samt netværk, men ingen af disse uddannelser har fokus på kompetencer inden for cybersikkerhed og har ikke tæt virksomhedstilknytning. Bachelor- og diplomingeniøruddannelserne i softwareteknologi (begge SDU) og softwareudvikling (ITU) har få overlappende kompetencer mest inden for programmering. Professionsbacheloruddannelserne fra KEA, Zealand og Erhvervsakademi Aarhus har overlappende kompetencer i programmering samt i cybersikkerhed (for de studerende, der vælger top-up muligheden) og virksomhedstilknytning, men mangler fokus på matematik og netværk. Det kan derfor konkluderes, at den foreslåede diplomingeniøruddannelse i cybersikkerhed har en unik opbygning og kompetenceprofil, som ikke kan genfindes i andre uddannelser i Danmark.

Behovsundersøgelsen har omfattet aftagere fra forskellige grupper inden for it og cybersikkerhed, herunder private it-virksomheder, som efterspørger medarbejdere med specifikke tekniske kompetencer inden for cybersikkerhed og private virksomheder, som beskæftiger sig med produktion og serviceydelser (både små, mellemstore og store virksomheder), som mere generelt har brug for øgede kompetencer inden for cybersikkerhed. Alle grupper har ubesatte stillinger inden for cybersikkerhed. Blandt mindre virksomheder er der 23%, som har ubesatte stillinger, for mellemstore og store virksomheder er tallene hhv. 38% og 26%, som har ubesatte stillinger (se dokumentationsrapporten, s. 20).

Idet repræsentanter fra hver af disse grupper har været inddraget i udviklingen af uddannelsen, og de har udtalt, at de gerne vil ansætte dimittender fra uddannelsen, kan det konkluderes, at dimittender fra diplomingeniøruddannelsen i cybersikkerhed har et relevant og godt erhvervssigte, som der er behov for. Set i lyset af den nuværende og fremtidige mangel på it-specialister med cybersikkerhedskompetencer, bidrager den ansøgte uddannelse med en kompetenceprofil, som virksomhederne efterspørger, og som er unik i forhold til beslægtede uddannelser.

Underbygget skøn over det nationale og regionale behov for dimittender. Besvarelsen må maks. fylde 1200 anslag

Diplomingeniøruddannelsen vil være adgangsbegrænset til 30 studerende i 2025, hvormed den vil kunne bidrage til at reducere det udækkede behov, der eksisterer for it-uddannelserne både nationalt og regionalt. Uddannelsens første dimittender forventes at dimittere i 2028. Dermed vil udbuddet af uddannelsen langtfra dække det nationale og regionale behov, men den vil udfylde et identificeret kompetencebehov hos aftagerne.

Tal fra UFM over antal ansøgere og optagne ansøgere til de beslægtede uddannelser viser, at de ikke har kapacitet til at optage alle kvalificerede ansøgere, og der var således 264 studerende i 2023, der fik afslag på deres 1. prioritet (s. 12). Det uudnyttede optagelsespotentiale er hovedsageligt i hovedstadsregionen, hvor der var 106 ansøgere i 2023, der ikke blev optaget på deres 1. prioritet.

Som beskrevet i dokumentationsrapporten (s. 19) estimerer Epinion, at der i foråret 2024 er ca. 27% af virksomhederne i undersøgelsen på tværs af landet, der har en eller flere ubesatte stillinger inden for cybersikkerhed. Det svarer til ca. 58 ledige stillinger. Virksomhederne med ledige stillinger ligger primært i Region Hovedstaden og Region Midtjylland.

Hvilke aftagere har været inddraget i behovsundersøgelsen? Besvarelsen må maks. fylde 1200 anslag

Epinion har udarbejdet en behovsundersøgelse for at afdække behovet for uddannelsen. I alt 118 aftagere deltog i spørgeskemaundersøgelse og 8 personer i interviews (se Bilag 2). Aftagerne kom fra store og små virksomheder inden for bl.a. softwareudvikling, it, cybersikkerhed, telekommunikation, finanssektoren og forsikringsselskaber samt offentlige virksomheder.

AAU har desuden været i dialog med instituttets aftagerpanel og enkelte andre repræsentanter fra industrien. I alt 14 har deltaget i møder, hvor uddannelsen er præsenteret, og som det fremgår af dokumentationsrapporten, er deres input brugt til at udvikle uddannelsens curriculum.

Både i den kvantitative og kvalitative undersøgelser indikerede aftagerne et stort behov for uddannelsen og specielt for kompetencerne i datasikkerhed, risikovurdering og -håndtering, design og udvikling af sikre systemer og software, compliance, detektion og forebyggelse af cyberangreb og sikkerhed i computersystemer og netværk.

AAU har udsendt høringsbrev om uddannelsen til DTU, ITU, AU, SDU, KU samt KEA for at skabe god informationsdeling og sikre et godt fremtidigt samarbejde i København.

Hvordan er det konkret sikret, at den nye uddannelse matcher det påviste behov? Besvarelsen må maks. fylde 1200 anslag

På baggrund af aftagernes input er der foretaget justeringer af uddannelsen for at sikre, at dennes kompetenceprofil matcher aftagernes behov. Det har resulteret i den endelige kompetenceprofil (Bilag 1). Fx er der lagt mere vægt på risikohåndtering med et nyt fag på 4. semester og for at få hele semesteret mere fokuseret på risikohåndtering blev det besluttet, at det oprindelige kursus på 6. semester i ”Privatlivsbeskyttelse og etik” skulle handle mere om databeskyttelse og flyttes til 4. semester. I dokumentationsrapporten er der en detaljeret gennemgang af, hvordan de påviste behov er dækket af kurser og semesterprojekter i det endelige curriculum.

Behovsundersøgelsen viser, at virksomhederne er positive over for uddannelsen, og de adspurgte virksomheder har et stort behov for uddannede inden for it- og cybersikkerhed: 85% af virksomhederne har i høj eller nogen grad behov for cybersikkerhedskompetencer lige nu. Dette tal øges, når man ser på behovet om 3 år, hvor 69% af virksomhederne forventer, at behovet vil stige. Aftagermøderne understøtter også dette behov (Bilag 4)

Det er således AAU’s vurdering, at uddannelsens indhold matcher aftagernes behov.

Beskriv ligheder og forskelle til beslægtede uddannelser, herunder beskæftigelse og eventuel dimensionering. Besvarelsen må maks. fylde 1200 anslag

I dokumentationsrapporten (Tabel 3) er der identificeret 5 kompetenceområder, som efterspørges af aftagerne og er indeholdt i den nye uddannelse: Matematik, programmering, netværk, cybersikkerhed samt virksomhedstilknytning. Disse er sammenlignet med 17 beslægtede uddannelser inden for it og cybersikkerhed. Den foreslåede uddannelse ligger tættest på AAU's bacheloruddannelse i cyber- og computerteknologi, men denne indeholder ikke det tætte samarbejde med industrien og det obligatoriske praktikforløb, som den foreslåede uddannelse gør. Erhvervsakademiernes uddannelser har et tæt samarbejde med erhvervslivet, men indeholder ikke matematik og netværksforståelse. Blandt disse er kombinationen af datamatiker eller it-teknolog og en 1½-årig top-up i cybersikkerhed nærest beslægtet. Diplomingeniøruddannelsen i cybersikkerhed er den eneste uddannelse, som samlet kan levere de kernekompetencer, der efterspørges af aftagerne.

Opgørelsen viser, at ledigheden er meget lav (1,6%). Tallene viser, at udbuddet ikke står mål med efterspørgslen. Dimittenderne kan varetage jobs, hvor de kan omsætte kompetencer i matematik, programmering og netværksviden og en indgående forståelse af cybersikkerhed.

Uddybende bemærkninger

Som nævnt ovenfor har AAU undervejs i udviklingen af uddannelsen gennemført en analyse af en række eksisterende uddannelser baseret på deres indhold og erhvervssigte for at sikre, at den ansøgte uddannelse vil bidrage med øget erhvervssigte, sammenhæng i det danske uddannelsessystem og ikke vil resultere i forringelser af vilkårene for de beslægtede uddannelser.

De beslægtede uddannelser på danske universiteter og erhvervsakademier er udvalgt ud fra andelen af indhold, der relaterer sig til cybersikkerhed (minimum 5 ECTS) og deres dækning af 5 centrale kompetenceområder: Matematik, programmering, netværk, cybersikkerhed og virksomhedstilknytning. Disse områder er fremkommet i dialog med aftagerne (møde med instituttets aftagerpanel, Epinions behovsundersøgelsen og mindre møder med udvalgte virksomheder). I dokumentationsrapporten (Tabel 3) vises en sammenligning af beslægtede uddannelser med kompetenceområderne samt i hvilken grad disse har sammenfaldende kernekompetencer med diplomingeniøruddannelsen i cybersikkerhed.

Følgende eksisterende uddannelser har været inddraget i analysen:

AAU

- Computerteknologi, Software (bachelor i teknisk videnskab) (Aalborg)
- Software, Cyber- og Computerteknologi (bachelor i teknisk videnskab) (København)

DTU:

- Cyberteknologi, Softwareteknologi (bachelor i teknisk videnskab)
- Softwareteknologi (diplomingeniør)

ITU:

- Softwareudvikling (bachelor i IT)

SDU:

- Softwareteknologi (diplomingeniør)

KEA, Zealand og EA Aarhus:

- Datamatiker (grundforløb) plus top-up i cybersikkerhed
- It-teknolog (grundforløb) plus top-up i cybersikkerhed

De beslægtede uddannelser falder i tre forskellige grupper: universitetsbachelorer (uden virksomhedspraktik), diplomingeniøruddannelser (med virksomhedspraktik og ingeniørfokus) samt professionsbacheloruddannelser (med virksomhedspraktik, men uden ingeniørfokus).

Analysen viser, at bacheloruddannelsen i softwareudvikling (ITU) kun har sammenfaldende kompetenceelementer med den foreslåede diplomingeniøruddannelse i cybersikkerhed inden for programmering og med mulighed for at tage et enkelt kursus som valgfag i cybersikkerhed. Dermed kan man konkludere, at den uddannelse har et meget lille sammenfald med den foreslåede diplomingeniøruddannelse.

Diplomingeniøruddannelserne i softwareteknologi (DTU og SDU) har sammenfaldende kompetenceområder på matematik, programmering samt virksomhedstilknytning (som praktik). Derudover tilbyder begge uddannelser cybersikkerhedskurser som valgfag, som studerende kan tage på et semester. Dog er der ikke fokus på netværk og en dybere forståelse for cybersikkerhed, som er identificeret som kompetenceområder for den foreslåede diplomuddannelse i cybersikkerhed. Det kan derfor konkluderes, at de eksisterende diplomingeniøruddannelser ikke dækker de samme kompetenceområder som den foreslåede uddannelse i cybersikkerhed.

Bacheloruddannelserne i hhv. computerteknologi (AAU), software (AAU, Aalborg og København), cyber- og computerteknologi (AAU) samt cyberteknologi (DTU) er alle ingeniøruddannelser inden for IT-området, og de har sammenfaldende kompetenceområder inden for matematik, programmering, netværk og med et eller flere fag i cybersikkerhed. Ingen af de nævnte bacheloruddannelser har dog en tæt virksomhedstilknytning. De studerende på universitetsbachelorer har en vis mulighed for tilknytning til virksomhederne via projektarbejde eller gæsteforelæsninger, men ikke som et planlagt semester i praktik, som det er tilfældet for den foreslåede diplomingeniøruddannelse i cybersikkerhed.

For uddannelsesforløbene på erhvervsakademierne KEA, ZEALAND og Erhvervsakademi Aarhus, datamatiker eller it-teknolog med top-up på cybersikkerhed, er der overlappende kompetenceområder på henholdsvis programmering, cybersikkerhed og virksomhedstilkytning, men ingen af disse uddannelser giver kompetencer inden for matematik og netværk.

Analysen viser således, at ingen af de beslægtede uddannelser uddanner dimittender med de samme kompetencer som den foreslåede diplomingeniøruddannelse i cybersikkerhed. Alle uddannelser har it-kompetencer som programmering, nogle har fokus på netværk, andre på matematik og igen andre på virksomhedstilknytning. Men ingen af dem dækker alle de nævnte kompetenceområder, og derfor kan diplomingeniøruddannelsen i cybersikkerhed betegnes som en ny profil, der for nuværende ikke findes i det danske uddannelsessystem.

I forhold til den organisatoriske kompetenceprofil, der omtales i dokumentationsrapporten (s. 7-8), adskiller diplomingeniøruddannelsen i cybersikkerhed sig også fra de beslægtede uddannelser. Uddannelses opbygning med problembaseret læring giver dimittender fra AAU særligt stærke kompetencer inden for problemløsende, praktiske tilgange til at samarbejde i teams, til at kommunikere mundtligt og skriftligt, projektledelse mm. Det er alle kompetencer, som virksomhederne i Epinions undersøgelse gav udtryk for, at deres ansatte bør have.

I det udsendte høringsbrev (Bilag 5) er de relevante uddannelsesinstitutioner (DTU, ITU, SDU, AU, KU og KEA) blevet informeret om indholdet i og kompetenceprofilen for den foreslåede uddannelse. Der er modtaget svar fra KEA, som ingen bemærkninger havde vedr. opbygning af AAU's foreslåede uddannelse, men som adresserer en eventuel udfordring med rekruttering til KEA's egne udbud på cybersikkerhedsområdet, idet KEA ønsker at få det eksisterende udbud i IT-Sikkerhed udvidet til en fuld professionsbacheloruddannelse.

AAU's afdækning af behovet for den nye diplomingeniøruddannelse viser klart, at der er 1) et uudnyttet og kvalificeret optagelsespotentiale, idet studerende i Københavnsområdet afvises fra deres 1. prioritetsansøgninger, og 2) så stor en efterspørgsel på dimittender inden for cybersikkerhedsområdet, at de eksisterende uddannelser og de to nye uddannelser samlet set ikke kan matche efterspørgslen.

Fagmiljøerne på hhv. KEA og AAU har gennem hele forløbet været bekendte med den parallelle udvikling af de to udbud, og det er i processen blevet tydeliggjort, at KEA og AAU sigter mod forskellige målgrupper. Ansøgerne til AAUs uddannelse tilhører en målgruppe, som gerne vil blive ingeniører og har interesse for de ingeniørfaglige discipliner med høje krav til matematik og avancerede tekniske fag.

Derfor vurderer AAU, at de to uddannelser kan sameksistere uden at forringe vilkårene for dimittenders beskæftigelse efter endt uddannelse.

Beskriv rekrutteringsgrundlaget for ansøgte, herunder eventuelle konsekvenser for eksisterende beslægtede udbud. Besvarelsen må maks. fylde 1200 anslag

Det forventes, at uddannelsen vil rekruttere studerende med interesse inden for teknologi og ingeniørkundskab samt for it og cybersikkerhed. De studerende forventes at komme med en baggrund i tek.-nat., STX- eller HTX uddannelser (eller tilsvarende) og vil derfor ligne ansøgerne til beslægtede uddannelser.

På de beslægtede uddannelser viser tallene et samlet optag på 642 i 2019 og 659 i 2022, mens tallene for COVID-perioden i 2020 og 2021 var højere. Det samlede antal dimittender er estimeret til ca. 245 i 2022. En rapport fra IDA fra 2023 beskriver dog, at mange kvalificerede ansøgere afvises fra universiteternes STEM- og it-uddannelser (se dokumentationsrapporten s. 13). Specifikt vurderes det, at antallet af afviste ansøgere er steget med i alt 19% fra 2022 til 2023, hvilket svarer til 1400 flere afviste ansøgere. En analyse fra DI Digital viser, at der i 2022 er afvist 576 ansøgere til STEM-uddannelser.

Det viser, at der på beslægtede uddannelser et uudnyttet og kvalificeret optagelsespotentiale, som i dag ikke bliver optaget. Der vil derfor være grundlag for optag af 30-40 kvalificerede ansøgere uden negativ indflydelse på optaget på beslægtede uddannelser.

Beskriv kort mulighederne for videreuddannelse

Uddannelsen er som udgangspunkt rettet mod erhvervslivet, da der er tale om en praksisnær diplomingeniøruddannelse med obligatorisk virksomhedspraktik. Hensigten er, at det skal være let for dimittenderne at finde relevante jobs og varetage konkrete jobfunktioner inden for cybersikkerhed, hvor de kan udnytte deres kompetencer.

Såfremt dimittender skulle ønske at videreuddanne sig inden for området, vil uddannelsen give adgang til AAU's kandidatuddannelse i cybersikkerhed og andre kandidatuddannelser inden for it og cybersikkerhed. Det vil også være muligt at supplere med kurser i certificering, fx Certified Hacker o.lign. (Microsoft, Teknologisk Institut m.fl.).

Forventet optag på de første 3 år af uddannelsen. Besvarelsen må maks. fylde 200 anslag

Uddannelsen forventes udbudt fra september 2025, hvor den er begrænset til at optage 30 ansøgere. I 2026-2028 forventes tallet at stige til 40 ansøgere.

Hvis relevant: forventede praktikaftaler. Besvarelsen må maks. fylde 1200 anslag

Et centralt element i uddannelsen er den obligatoriske virksomhedspraktik på 6. semester, hvor den studerende er lønnet af virksomheden. Virksomheden og den studerende opnår et godt kendskab til hinanden, og virksomhederne kan direkte anvende de opnåede resultater, hvis de måtte ønske det, da den studerende er i et ansættelsesforhold med virksomheden.

I behovsundersøgelsen fra Epinion er virksomhederne blevet spurgt, om det vil være relevant for dem at modtage praktikanter i et semester og give dem IDA's vejledende praktikløn på 16.200 kr./måned. Et flertal af virksomhederne er positivt stemte herfor, mens et mindretal enten er mindre positivt stemte eller i tvivl om, hvorvidt det vil være relevant. 55 pct. af virksomhederne svarer, at det i nogen eller høj grad vil være relevant, mens 32 pct. af virksomhederne svarer, at det i lav grad eller slet ikke vil være relevant.

Samlet set forventes der at være et bredt spektrum af virksomheder og organisationer på tværs af sektorer, som gerne vil modtage studerende i praktik. Der kan dog være visse typer af virksomheder, som ikke har ressourcer til eller tradition for at modtage praktikanter.

Øvrige bemærkninger til ansøgningen

Ingen øvrige bemærkninger.

Hermed erklæres, at ansøgning om prækvalifikation er godkendt af institutionens rektor

Ja

Status på ansøgningen

Godkendt

Ansøgningsrunde

2024-2

Afgørelsesbilag - Upload PDF-fil

Afgørelsesbrev A14 Professionsbachelor (diplomingeniør) cybersikkerhed AAU.pdf

Samlet godkendelsesbrev - Upload PDF-fil

AALBORG UNIVERSITET

Rektoratet
Fredrik Bajers Vej 7K
9220 Aalborg Ø

Prorektor
Anne Marie Kanstrup
Telefon: +45 9940 7380
E-mail: prorektor@aau.dk
www.aau.dk

Dato: 11-09-2024
Sagsnr.: 2024-415-00091

Dokumentation af efterspørgsel på uddannelsesprofil

Baggrund for ansøgningen

Danske virksomheder og organisationer udsættes i stadig stigende grad for cybertrusler og cyberangreb. Næsten dagligt høres om distributed denial-of-service (DDoS) attacks, ransomware attacks og brud på datasikkerheden, som ofte medfører lækage af fortrolige data i form af forretningshemmeligheder og persondata. Den tilspidsede geopolitiske situation fører ligeledes til trusler mod nationalstater, myndigheder og politikere, samt at borgere udsættes for snyd og bedrageri i form af falske e-mails og SMS'er, som forsøger at franarre personlige informationer og penge.

EU er særdeles opmærksom på dette trusselsbillede og behovet for regulering i forhold til cybersikkerhed, og en lang række direktiver og forordninger er allerede vedtaget eller under udarbejdelse. Eksempler er GDPR, NIS2 (Network and Information Security Directive, version 2), Digital AI Act og Cyber Resilience Act. EU stiller krav til alle medlemslande om implementering på nationalt niveau, og der kan udstedes store bøder til virksomheder, der ikke lever op til lovgivningen. Desuden er der et stigende pres på virksomheder om at leve op til compliance og certificeringskrav (ISO 27000-familien, D-Mærket, IEC, m.m.). Det er ressourcekrævende, ikke mindst for små og mellemstore virksomheder (SMV'er), og det betyder, at danske virksomheder og organisationer har behov for en væsentlig opgradering af viden og kompetencer inden for disse områder.

Den danske regering udgav i december 2021 en "National strategi for cyber- og informationssikkerhed"[1], hvoraf det fremgår, at *"efterspørgslen på cyber- og informationssikkerhedskompetencer skal imødekommes ved at uddanne flere specialister og opbygge stærkere kapacitet på tværs af samfundet".* Det nævnes bl.a., at der er behov for, at *"samfundets adgang til kompetencer inden for cyber- og informationssikkerhed styrkes gennem de videregående uddannelser bl.a. inden for ordinære uddannelser og videregående voksen-, efter- og videreuddannelse".* Strategien lægger ligeledes op til en *"styrkelse af det offentligt-private samarbejde for herved at blive "bedre til at dele viden og erfaringer"*.

I september 2022 beskrev en rapport udarbejdet af regeringens sikkerhedspolitiske analysegruppe[2] udfordringerne for dansk sikkerhed og forsvar frem mod 2035. Med udgangspunkt i denne advarede Dansk Industri (DI Digital) om, at Danmark i 2030 vil mangle 15-20.000 fagfolk inden for cyber- og informationssikkerhed. DI Digital, Rådet for Digital Sikkerhed og en række andre organisationer fremsendte d. 30. jan. 2023 et "bekymringsbrev" til regeringen[3], hvori de understreger behovet for en samlet indsats og beskriver 11 konkrete forslag til at fremme opbygningen af cyber-kompetencer i Danmark, herunder et øget optag på uddannelser i cybersikkerhed.

[1] https://fm.dk/media/25359/national-strategi-for-cyber-og-informationssikkerhed_web-a.pdf
[2] https://www.forsvaret.dk/globalassets/fmn/dokumenter/nyheder/2022/-dansk-sikkerhed-og-forsvar-mod-2035-den-sikkerhedspolitiske-analyserapport-.pdf
[3] https://www.digitalsikkerhed.dk/wp-content/uploads/2023/01/Manglende-cyber-og-informationssikkerhedskompetencer.pdf

Udbuddet af ingeniører med kompetencer inden for cybersikkerhed dækker langtfra den efterspørgsel, som virksomheder har i dag og i de kommende år. The International Information System Security Certification Consortium (ISC) anslår i rapporten "Cybersecurity Workforce Study" fra 2022[4], at der mangler 3,4 mio. IT Security Professionals på verdensplan.

Den foreslåede diplomingeniøruddannelse i cybersikkerhed vil bidrage til at opfylde dette behov og samtidigt understøtte den nationale strategi om et tæt samarbejde med erhvervslivet om cybersikkerhed. Uddannelsen vil komplementere det bestående udbud med en ny type af ingeniører, som hurtigere kan komme ud på arbejdsmarkedet og har et særligt erhvervsfokus. Det obligatoriske semester med praktikforløb vil give de studerende et væsentligt indblik i praktiske problemer og opgaver, som der arbejdes med i virksomhederne og styrke mulighederne for ansættelse, når uddannelsen er afsluttet. I hovedstadsområdet er det indtil nu kun DTU, som udbyder diplomingeniøruddannelser, mens AAU ikke har udbudt denne type af uddannelse i København. AAU har dog en lang erfaring med diplomingeniøruddannelser på campus Aalborg.

Strategi for udvikling af uddannelsesporteføljen
Ansøgningen om diplomingeniøruddannelsen i cybersikkerhed indgår i en samlet strategi for Det Tekniske Fakultet for IT og Design, hvor AAUs uddannelsesportefølje på campus København fremover vil være koncentreret inden for STEM-området. Udbygningen skal desuden ses i sammenhæng med AAU's Digitaliseringsstrategi, som sigter mod at styrke udviklingen af digitale teknologier inden for forskning, uddannelse og videnssamarbejde.

Siden 2020 er der på AAU's Campus København lanceret bacheloruddannelser (teknisk videnskab) i **software** og **cyber- og computerteknologi** samt kandidatuddannelser i **cybersikkerhed** og **software**. Sideløbende med nærværende ansøgning søges der om godkendelse af en ny kandidatuddannelse i **computer engineering**, som skal erstatte den nuværende kandidatuddannelse i innovativ kommunikationsteknik og entreprenørskab (sidste optag 2024).

Kandidatuddannelsen i cybersikkerhed på AAU er den første og hidtil eneste i Danmark, som udelukkende fokuserer på dette område. I andre kandidatuddannelser (på andre universiteter) indgår det som et delelement sammen med andre områder. Uddannelsen havde sit første optag i september 2020, og de første kandidater dimitterede i juni 2022. Der har været en betydelig vækst i optaget fra ca. 30 ved 1. optag til ca. 80 ved optaget i 2024 og tilsvarende i antallet af færdiguddannede. I 2024 ansøgte 334 om optagelse. Uddannelsen bidrager væsentligt til at imødekomme den stigende efterspørgsel fra virksomhederne, og kandidaterne finder hurtigt beskæftigelse.

I tilknytning til kandidatuddannelsen er der opbygget et omfattende netværk med virksomheder og organisationer inden for området. Mange studerende samarbejder med virksomheder i form af projektorienterede forløb i virksomheden, semesterprojekter og det afsluttende kandidatspeciale. Der arrangeres hacker-events, foredrag og konferencer. Der gøres en stor indsats for at gøre unge interesserede i feltet og tiltrække dem til studiet, bl.a. i to projekter finansieret af Industriens Fond: "Unge – Community for Cybersikkerhed (Cyberskills)" (2020-2023) og "Fast track til kompetencer i cybersikkerhed" (2023-2025).

Professor Jens Myrup Pedersen, AAU, er leder af AAUs forskningsgruppe i cybersikkerhed på campus København og har været en central drivkraft i opbygningen af det faglige miljø, der ligger til grund for både den eksisterende kandidatuddannelse og den nye diplomingeniøruddannelse, Han står desuden i spidsen for det danske cyberlandshold, som i 2022 opnåede at blive europamestre i cybersikkerhed. Forud for mesterskaberne pågår en omfattende udvælgelsesprocedure blandt unge mennesker i hele Danmark for at finde frem til de dygtigste talenter. Jens Myrup er også en hyppig gæst i medierne, når der er behov for ekspertvurderinger af konkrete hændelser. De mange aktiviteter har skabt stor synlighed og udgør en god basis for lancering af den nye uddannelse.

AAU har således valgt at udbyde den nye uddannelse på campus København ud fra flg. hensyn:

- Der eksisterer allerede et stærkt fagligt miljø med forskning og undervisning i cybersikkerhed på campus København.
- Diplomingeniøruddannelsen vil supplere og understøtte den eksisterende kandidatuddannelse, så der fremover kan uddannes begge typer af ingeniører i det samme faglige miljø.

[4] https://isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx

- Der er udviklet et stort netværk omkring cybersikkerhed med virksomheder og organisationer i hovedstadsområdet, og mange væsentlige aftagervirksomheder og aktører er placeret her. Det gælder fx virksomheder som Microsoft, Dubex, PwC, Terma, Novo Nordisk, Mærsk, TDC, m.fl. Det giver gode muligheder for praktikforløb og projektsamarbejde i løbet af studietiden samt gode jobmuligheder for kandidaterne efterfølgende.
- Behovsundersøgelsen viser, at virksomhederne med ledige stillinger primært ligger i Region Hovedstaden og Region Midtjylland.
- Tal fra Danmarks Statistik[5] understøtter, at rekrutteringsproblemerne for it-specialister er klart størst i hovedstadsområdet.

Ledelsens rolle i processen omkring udvikling af uddannelsen
Arbejdet med udvikling af diplomingeniøruddannelsen blev påbegyndt i slutningen af 2023. Der blev nedsat en udviklingsgruppe på Institut for Elektroniske Systemer, bestående af viceinstitutleder, studienævnsformand, sektionsleder og VIP'er fra fagmiljøet, og der blev udpeget en kontaktperson i dekansekretariatet for det Tekniske Fakultet for IT og Design. Der blev desuden afholdt et møde med instituttets aftagerpanel, hvor uddannelsens struktur og indhold blev drøftet (se nedenfor).

Der blev udarbejdet et oplysningsskema med strukturen for uddannelsen og en generel kompetenceprofil (se Bilag 1), og AAU's strategiske uddannelsesråd (DSUR) gav grønt lys til at gå videre med ansøgningen.

I forbindelse med udarbejdelsen af ansøgningen har dekanatet på Det Tekniske Fakultet for IT og Design informeret en række universiteter og centrale samarbejdspartnere om AAU's arbejde vedrørende den nye uddannelse. Det er afgørende for AAU at skabe en god dialog og rum for fremtidigt samarbejde om uddannelser, der omhandler cybersikkerhed, så behovet for øgede kompetencer kan understøttes bedst muligt.

Prodekanen har d. 19. juni 2024 udsendt høringsskrivelser til DTU, ITU, AU, SDU, KU samt KEA med svarfrist d. 5. juli. Der er modtaget svar fra KEA (se Bilag 5), mere om dette senere i ansøgningen.

Evt. toning af eksisterende uddannelse
Typen og varigheden af uddannelsen gør, at det ikke er muligt at opnå det ønskede indhold ved en toning af de eksisterende uddannelser. En sammenligning med nuværende beslægtede uddannelser (se nedenfor) viser, at den nye uddannelse er en meget praksisnær uddannelse med tæt erhvervstilknytning, bl.a. i kraft af det obligatoriske praktikforløb. Dette kan ikke i samme grad opnås i de eksisterende 3-årige bacheloruddannelser i teknisk videnskab på AAU. De indeholder dog sammenfaldende kompetencer i matematik, programmering og netværk.

Udviklingen af uddannelsens indhold i dialog med aftagere
Dialogen med aftagere og interessenter tog udgangspunkt i instituttets aftagerpanel og det eksisterende netværk af virksomheder og organisationer, der blev omtalt ovenfor. Efterfølgende blev en større kreds af potentielle aftagere inddraget i Epinions behovsundersøgelse.

Uddannelsen blev fremlagt for instituttets aftagerpanel den 30. november 2023 (Bilag 3). Mødedeltagerne havde forinden modtaget en oversigt over uddannelsens struktur og en foreløbig kompetenceprofil. Som det fremgår af mødereferatet, består panelet af repræsentanter fra virksomheder og organisationer, hvoraf især Microsoft og Center for Cybersikkerhed er centrale aktører.

I februar-marts 2024 fik analysevirksomheden Epinion til opgave at foretage en behovsundersøgelse sammen med AAU. Det overordnede formål med behovsundersøgelsen var at undersøge behovet hos potentielle aftagervirksomheder for uddannelsen som helhed og for de centrale fagelementer, som var planlagt i kompetenceprofilen samt at forstå det reelle behov for ingeniører inden for cybersikkerhed. En spørge- og interviewguide blev udarbejdet i samarbejde mellem Epinion og arbejdsgruppen. Den indeholdt bl.a.:
- Oplysninger om virksomheden (branche, primære aktiviteter, antal ansatte, lokation) og interviewpersonen
- Brugen af ingeniører og andre medarbejdere med viden om cybersikkerhed på arbejdspladsen, deres baggrund, arbejdsopgaver og jobfunktioner

[5] https://www.dst.dk/da/Statistik/nyheder-analyser-publ/nyt/NytHtml?cid=40866.

- Virksomhedens kompetencebehov inden for cybersikkerhed og udfordringer med at rekruttere i dag og de næste 3 år. Hvilke specifikke kompetencer er vigtige?
- Hvordan matcher kompetenceprofilen for den påtænkte uddannelse disse behov hos virksomheden?

Virksomhederne blev indledningsvis inddelt i nogle hovedgrupper for at sikre, at alle relevante sektorer blev inddraget, f.eks.:

- Store virksomheder (så som Microsoft, Novo Nordisk, Maersk)
- Virksomheder med cybersikkerhed som kerneforretning (så som Dubex, Seculyze, CSIS Security Group, Arbit CDS)
- Små og mellemstore virksomheder (SMV'er)
- Konsulentvirksomheder (så som PWC, Ernest & Young)
- Brancheorganisationer og råd (DI Digital, Rådet for Digital Sikkerhed, IT-Branchen)
- Offentlige myndigheder og styrelser (så som Center for Cybersikkerhed, Sundhedsdatastyrelsen, Rigspolitiet, Aarhus Kommune)
- Kritisk infrastruktur (TDC, Norlys, SektorCERT)
- Finanssektoren (Bankdata, Danske Bank, e-Nettet)
- Forsikringsselskaber (TopDanmark, Tryg)

En prioriteret bruttoliste af modtagere blev sendt til Epinion, som efterfølgende udvalgte en delmængde af disse. De udvalgte virksomheder modtog information om uddannelsens kompetenceprofil og indhold.

Behovsundersøgelsen blev gennemført i marts-april 2024. Af de potentielle aftagervirksomheder har 118 virksomheder besvaret spørgeskemaundersøgelsen. Derudover har konsulenter fra Epinion udført otte kvalitative telefoninterviews med potentielle aftagervirksomheder (se Bilag 2). Behovsundersøgelsen blev afsluttet med en rapport, som blev afleveret til AAU i starten af maj 2024. Rapporten indeholder dokumentation for:

- Virksomhedernes behov for medarbejdere med kompetencer inden for cybersikkerhed
- Efterspurgte kompetencer hos virksomhederne
- Rekruttering af medarbejdere med kompetencer inden for cybersikkerhed
- Virksomhedernes vurdering af diplomingeniøruddannelsen.

For at supplere behovsundersøgelsen og gå mere i dybden med aftagernes ønsker og kompetencebehov blev der i april-maj 2024 arrangeret mindre møder af ½ - 2 timers varighed med udvalgte aftagere:

- 11. apr. 2024: Møde med PWC (Benjamin Vanggaard) og Dubex (Jim Bauer)
- 12. apr. 2024: Teams-møde med Arbit CDS (Rasmus Borch)
- 7. maj 2024: Teams-møde med Maersk (Camilla Bonde)
- 23. maj 2024: Teams-møde med Novo Nordisk (Ingrid Colding-Jørgensen)

Deltagerne fik ligeledes tilsendt information om uddannelsens struktur og kompetenceprofil på forhånd. Mødereferater er vedhæftet i Bilag 4.

Aftagernes bidrag til udvikling af uddannelsen

Dialogen med aftagerne har resulteret i vigtige kommentarer og tilkendegivelser, som er indarbejdet i uddannelsens konkrete indhold, opbygning og kompetenceprofil (se Bilag 1).

Fra **instituttets aftagerpanel** var der fuld opbakning til at udbyde uddannelsen (Bilag 3). De udtrykte begejstring og bekræftede, at der var stort behov for kompetencerne hos aftagerne. Mht. indhold og struktur var der nogle vigtige kommentarer:

- Nødvendigheden af kompetencer inden for *ressourcebegrænsning* ift. lavenergi- og ressourcesvage systemer. Det indgår i kurset "Sikkerhed i IoT- og OT-miljøer" samt semesterprojektet om "Cybersikkerhed i distribuerede systemer".
- *Kryptering*, som indgår i kurset "Sikkerhed i computersystemer"
- *Quantum computing og kvantesikre systemer* blev nævnt som et relevant område at forholde sig til. Det betragtes i første omgang som et område for kandidatuddannelsen, men fagmiljøet ser på, hvordan elementerne kan inkluderes i diplomingeniøruddannelsen.

- *Lovgivning, beredskabsagenda, og "cyber security levels"* blev nævnt som områder, de studerende skal have kendskab til. I det nuværende curriculum er det en del af kurset "Sikkerhed i organisationer" og 'privacy'.
- Der var opbakning om nødvendigheden af kurset "Machine learning og AI i cybersikkerhed", men det blev pointeret, at *cybersikkerhed i ML og AI systemer* er også vigtigt og bør behandles i uddannelsen. Det vil blive inddraget i udvikling af det nævnte kursus.
- Herudover var der en kommentar om, hvordan det sikres, at *alle får både 'bløde' og 'hårde' kompetencer*, og at nogle studerende ikke gemmer sig i grupper. Denne er en valid kommentar, der relaterer sig til projektarbejde, men som det fremgår af curriculum, er der en del kurser, som den studerende skal bestå individuelt, og i øvrigt har underviserne stor erfaring i at holde øje med dette problem i deres vejledning af semesterprojektgrupper.

De adspurgte virksomheder i **behovsundersøgelsen** er samlet set positivt indstillede over for en ny diplomingeniøruddannelse i cybersikkerhed på Aalborg Universitet i København. I undersøgelsen blev virksomhederne præsenteret for en kort beskrivelse af den nye uddannelse, og på baggrund heraf vurderer 69 pct. af virksomhederne, at det i høj eller nogen grad vil være relevant for dem at ansætte en sådan diplomingeniør i deres virksomhed i fremtiden. 20 pct. mener, at kandidaterne i lav grad vil være relevant for dem, mens 3 pct. vurderer, at de slet ikke vil være relevante for deres virksomhed. *(Epinion, s. 12-13)*

Virksomhedsrepræsentanterne i de kvalitative interviews er også meget positive over for forslaget om en diplomingeniøruddannelse i cybersikkerhed. Den samlede uddannelse beskrives som ambitiøs på den positive måde, og som en god introduktion til de vigtigste koncepter inden for cybersikkerhed. Uddannelsen vil ifølge virksomhedsrepræsentanterne være et godt fundament, som man kan bygge ovenpå enten med en kandidat, erhvervserfaring eller efteruddannelse.

> *I think that this is a good broad-spectrum introduction to cybersecurity concepts and as such, I think it looks perfectly fine to me. I think the intent of this degree just from looking at it is they're trying to create a substrate, a set of foundational skills that are going to serve you well no matter which way you pivot in security. (Epinion, s. 12)*

Virksomhedsrepræsentanterne lægger særligt vægt på vigtigheden af dels bachelorprojekter og dels praktikperioden. De to elementer er vigtige, fordi bachelorprojektet giver den studerende mulighed for at gå i dybden med et emne, mens erhvervserfaringen er essentiel for virksomhederne ift. potentiel ansættelse.

> *Jeg kan rigtig godt lide den her del med bachelorprojektet og så selvfølgelig praktikken. Det er noget af det allervigtigste, at man kommer ud i praktik. Det giver virkelig også virksomheden mulighed for dels at se den person an, men også den studerende mulighed for ansættelse efterfølgende (Epinion, s. 13).*

Repræsentanterne i de kvalitative interviews mener imidlertid, at uddannelsen også har sine mangler. Flest nævner, at der bør bruges mere tid på kunstig intelligens givet den eksponentielle udvikling på området. Mange lægger vægt på, at compliance bør være mere fremtrædende i uddannelsen, da det er relevant for alle virksomheder og kun forventes at blive det i stigende grad. Andre nævner datakvalitet, kvantekryptering, arkitektur og incident response som emner, der bør sikres et tilstrækkeligt fokus på i løbet af uddannelsen.

> *Hvis jeg skal komme med et bud på noget, jeg mangler, så er det mere AI og især offensive AI. Det fylder meget nu, og inden uddannelsen bliver godkendt, og de kommer ud, så går der fire år, og der er der ikke nok AI (Epinion, s. 13).*
>
> *There could be more focus on compliance, because when we talk about industry then compliance is very important. I think everything revolves around compliance whether it's ISO list or OT compliant and so on. (Epinion, s. 13).*

I **de mindre aftagermøder** blev uddannelsens curriculum præsenteret, og der blev åbnet for en diskussion af uddannelsens relevans, curriculums sammensætning og behovet for kandidater fra uddannelsen hos aftagervirksomheder (Bilag 4).

Der var en enstemmig opbakning for nødvendigheden af uddannelsen hos aftagervirksomhederne. Mht. til curriculum var hovedinput fra fleste af aftagere behov for mere *matematik*, *programmering* og *netværksviden* i uddannelsen. Herudover var behov for *AI* og *machine learning* fremhævet, som også understregede behov for matematik og programmering som forudsætning for AI og anvendt AI. Herudover blev andre emner fremhævet, som: *1) behov for risikovurdering, -håndtering og -styring, 2) forståelse af*

computer- arkitekturer og systemer, og 3) kendskab til standarder og reguleringsinitiativer som ISO, NIST, CIS og AI Act. Nogle aftagere var ikke overbevist om nødvendigheden af at inkludere "cybersikkerheds awareness og behaviour" i uddannelsen med det argument, at "virksomhederne selv kan lære deres ansatte om disse emner".

Ud over input til curriculum var der et ønske om at tiltrække flere kvinder i uddannelsen. I forhold til samarbejde med industri og praktikpladser blev det nævnt, at det vil være vigtigt at skabe bedre samarbejde med SMV'er og at identificere klare og tydelige læringsmål for praktikopholdet, så de studerende er praktikklare. Brugen af industrisamarbejde til at definere praktiske cases i forbindelse med semesterprojekter og bidrag fra industrien som gæsteoplæg til kurserne blev ligeledes nævnt som vigtige tiltag for at gøre uddannelsen mere praksisnær. Endelig nævnte nogle aftagere relevansen af samarbejde med certificeringsvirksomheder.

Samlet set peger aftagerne på, at den foreslåede uddannelse i cybersikkerhed skal være sammensat af kernekompetencer inden for matematik, programmering og netværksviden og en indgående forståelse af cybersikkerhed.

Hvordan er aftagernes bidrag indarbejdet i tilrettelæggelsen af uddannelsen?
I dialogen med aftagerne er der blevet fjernet kurser, tilføjet nye kurser og sat mere fokus på projektemnerne.

På semestrene 1.-3. er der ikke foretaget nogen ændringer. Aftagerne har generelt været tilfredse med disse og har set dem som opbygning af viden for de studerende.

På 4. semester var der oprindeligt foreslået 3 kurser, 2 obligatoriske og 1 valgfag. De obligatoriske fag var "Sikkerhed i organisationer" og "Sandsynlighedsregning og statistik", og valgfaget var enten "Brugerbevidsthed og -adfærd" eller "Risikovurdering". Flere gange under aftagermøderne blev det nævnt, at et fag som "Brugerbevidsthed og -adfærd" ikke passede til uddannelsen. Derfor blev det bestemt at fjerne dette kursus. I stedet blev det nævnt, at "Risikohåndtering" er meget vigtigt, og derfor er dette kursus blevet et kursus, alle studerende skal have. For at få semesteret til at være mere fokuseret om risikohåndtering blev det besluttet, at det oprindelige kursus på 6. semester i "Privatlivsbeskyttelse og etik skulle handle mere om datasikkerhed og flyttes til 4. semester. Det resulterede i kurset "Datasikkerhed og privatlivsbeskyttelse", som også er et kursus, som alle studerende skal tage. "Sandsynlighedsregning og statistik" kurset ændres ikke, da det skal anvendes på det følgende semester på kurser i fx "Machine Learning og AI". Semesterprojektet på 4. semester var oprindeligt et valg mellem projekt i "Cybersikkerhed og brugeradfærd" eller projekt i "Cybersikkerhed og governance". Da aftagerne har sagt, at det vil være relevant at arbejde mere fokuseret på risikohåndtering, er det besluttet, at der på 4. semester blot skal være en projektmulighed med tema i "Cyberangreb og -forsvar". Dette åbner op for, at studerende kan lave nogle "red- og blue team"-øvelser, som flere af aftagerne efterspørger i undervisningen.

På 5. semester er der ændret i valgfriheden i forhold til kurser og projektet. I forhold til det oprindelige har feedback fra aftagerne forårsaget, at kursus i "Machine Learning og AI i Cybersikkerhed" nu bliver et valgfrit kursus, og at kurset i "Sikkerhed i organisationer" bliver et andet valgfrit kursus. Det åbner op for, at de studerende kan vælge mellem at lave projekt i "Cybersikkerhed i distribuerede systemer" eller "Cybersikkerhed og governance", afhængig af interesser. Flere aftagere har nævnt, at governance-aspektet er vigtigt at få med i en uddannelse på en eller anden måde, og på denne måde kan de studerende selv vælge, om de ønsker at gå den vej eller den mere tekniske vej. På 6. semester har aftagerdialogen resulteret i, at det oprindelige kursus i "Privatlivsbeskyttelse og etik" nu er flyttet til 4. semester og har fået nyt navn (som allerede nævnt), og der er blevet identificeret to valgfag, som aftagerne mener er vigtige at vide noget om, nemlig "Cybersikkerhed og lovgivning" og "Malware-analyse". Bachelorprojektet er derfor reduceret fra 25 ECTS til 20 ECTS for at give plads til et valgfag, idet kurset i "Projektledelse og forretningsforståelse" skal tages af alle studerende.

Det er vigtigt at tiltrække flere kvinder til cybersikkerhed, og AAU har et særligt fokus på dette i relation til at øge diversiteten på uddannelserne. Fx har der været arbejdet med ordvalg i curriculum og muligheder for forskellige typer af projekter (i valgfri moduler). AAU deltager bl.a. i et samarbejde med DTU, NTNU og IDA[6] om "Empowering Diversity in Engineering".

[6] https://ida.dk/arrangementer-og-kurser/arrangementer/empowering-diversity-in-engineering-insights-initiatives-and-innovation-355788.

Samlet set har dialogen med aftagerne bidraget med mange væsentlige forslag og ændringer og haft en signifikant indflydelse på uddannelsens fagelementer, kursuselementer og projektelementer. Det har styrket uddannelsens kvalitet og er med til at sikre, at uddannelsen er tilpasset industriens behov.

Sammenhængen mellem uddannelsens kompetenceprofil og uddannelsens erhvervssigte

Uddannelsens kompetenceprofil

I Bilag 1 beskrives uddannelsens struktur og kompetenceprofil, som den har været diskuteret med aftagere via Epinions behovsundersøgelse.

Uddannelsen giver de studerende et omfattende fundament inden for cybersikkerhed, der omfatter både teoretisk viden og praktiske kompetencer, der er vigtige for at kunne navigere i udfordringerne i det meget dynamiske landskab for cybersikkerhed. Virksomheder på tværs af alle sektorer har brug for ingeniører med ekspertise til at beskytte kritiske systemer og data mod cyberangreb. Denne efterspørgsel forventes at stige eksponentielt i de kommende år, hvilket gør dimittender fra denne uddannelse meget attraktive på jobmarkedet.

Uddannelsen sigter mod at imødekomme den stigende efterspørgsel efter cybersikkerhedsfolk ved at fokusere på tre centrale søjler: (i) grundlæggende viden om generelle tekniske emner, herunder matematik, programmering og computerarkitekturer, (ii) viden og praktiske færdigheder inden for flere cybersikkerhedsdomæner, der spænder fra trusselsanalyse og etisk hacking til cloud-sikkerhed og maskinlæring, og (iii) ekspertise i håndtering af data og tjenester i virksomheder, herunder risikostyring, databeskyttelse og cybersikkerhedsregler.

Efterspurgte kompetencer

En af behovsundersøgelsens hovedkonklusioner (Epinion, side 3) er, at virksomhederne efterspørger både faglige og organisatoriske kompetencer blandt ingeniører inden for cybersikkerhed. Når det gælder faglige kompetencer, efterspørger virksomhederne især ingeniører med kompetencer inden for datasikkerhed og risikovurdering og -håndtering. Med hensyn til de mere organisatoriske og personlige kompetencer efterspørger næsten alle virksomheder ingeniører, der har en problemløsende tilgang, og som både kan samarbejde med andre (også på tværs af fagligheder) samt arbejde selvstændigt.

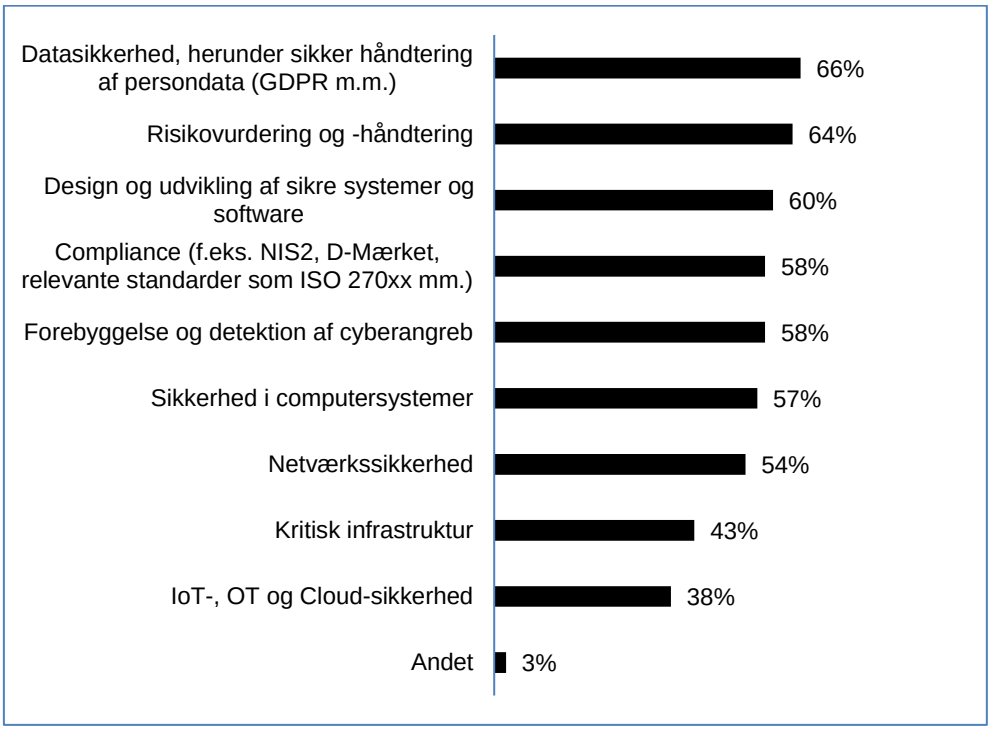
Ifølge interviewpersonerne har der historisk været mangel på ingeniørfaglige uddannelser med speciale i cybersikkerhed, hvilket reflekteres i udbuddet af profiler med de kompetencer i dag. Derfor har mange virksomheder ikke ansat ingeniører med kompetencer inden for kun cybersikkerhed, men snarere medarbejdere, der har tillært sig viden og kompetencer inden for området som tillæg til deres uddannelse inden for et andet område. I alle virksomhederne indgår de ansatte desuden i mere eller mindre omfattende uddannelsesprogrammer suppleret med sidemandsoplæring. Her vil det være en fordel for virksomhederne at ansætte ingeniører, som allerede har tilegnet sig de rette kompetencer under uddannelsen. Derudover nævner mange, at de har ansatte fra fx datalogi, og de større virksomheder har dertil udenlandske ansatte med kompetencer i cybersikkerhed.

> *Det er primært inden for teknologi, at folk har en ingeniørmæssig baggrund eller anden anden IT-baggrund. (Epinion, s. 5)*

I Epinions behovsundersøgelse er virksomhederne er blevet bedt om at angive, hvilke faglige og tekniske kompetencer og kvalifikationer de efterspørger, og resultatet er vist i Figur 1.

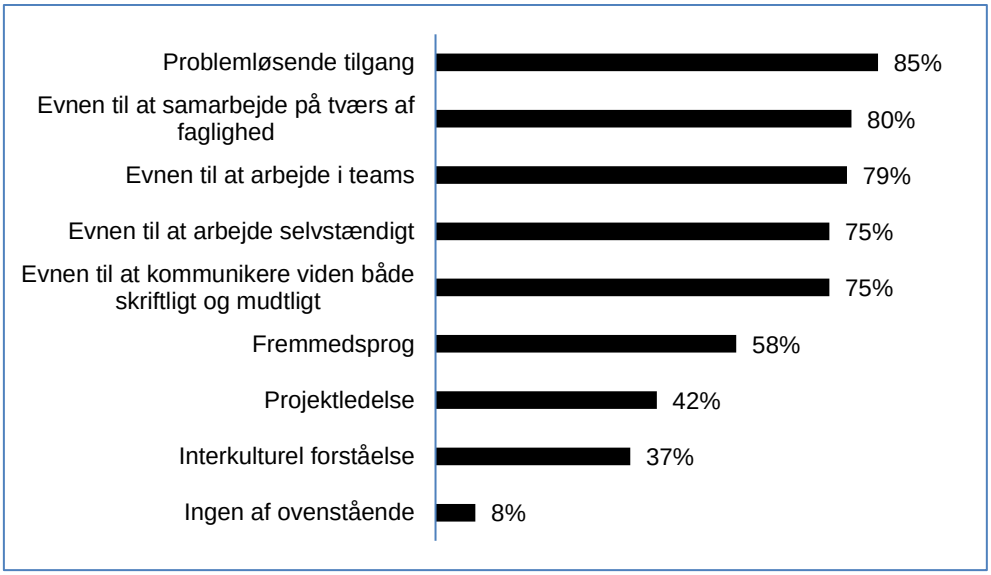
I de kvalitative interviews er der efterspørgsel på en lang række forskellige kompetencer afhængigt af virksomhedernes størrelse og område. Der nævnes blandt andet behov for kompetencer inden for governance, standarder, blueprints, cloud-teknologier, AI-relaterede teknologier, sikker kodning, risikostyring, awareness og sikkerhedsledelse. Flere interviewdeltagere nævner dertil, at der særligt er et behov for profiler med kompetencer inden for cybersikkerhed *kombineret* med kompetencer inden for udvikling og/eller forretningsforståelse.

> *I'm heading a department of specialists coming from different clubs of cybersecurity, covering risk management, governance, penetration testing, system engineering, software development and so on. So, most of my guys are with some sort of cybersecurity background (Epinion, s. 8)*



Figur 1: Hvilke faglige og tekniske kompetencer og kvalifikationer efterspørger I hos ingeniører, der har kompetencer inden for cybersikkerhed? N=118. Kilde: Epinion, side 7.

Virksomhederne har ligeledes høje krav til ingeniørernes organisatoriske kompetencer og kvalifikationer. Det gælder især en problemløsende tilgang samt evnen til både at kunne arbejde tværfagligt og i teams men også individuelt. Derudover er skriftlig og mundtlig kommunikation også vigtigt for mange virksomheder, hvilket kan ses i Figur 2, mens en kompetence som projektledelse er mindre efterspurgt (dog stadig af 42 pct.).



Figur 2: Hvilke organisatoriske kompetencer og kvalifikationer efterspørger I hos ingeniører, der har kompetencer inden for cybersikkerhed? N=118. Kilde: Epinion, side 8.

Erhvervssigte

I det følgende beskrives det, hvordan de efterspurgte kompetencer fra aftagerne er indarbejdet i uddannelsens kurser og projekter, primært med udgangspunkt i ovennævnte kompetencebehov. Referencerne til kurser og projektenheder er relateret til den endelige uddannelsesprofil, se Bilag 1.

- **Datasikkerhed, herunder sikker håndtering af persondata (GDPR m.m.):** Dette område dækkes primært af kurset "Datasikkerhed og privatlivsbeskyttelse" samt semesterprojektet "Cyberangreb og -forsvar på 4. semester, men vil også indgå i andre semesterprojekter.

- **Risikovurdering og -håndtering:** Dækkes af kurset "Risikohåndtering" og semesterprojektet "Cyberangreb og forsvar" på 4. semester samt videregående kurser på de flg. semestre. Emnet bliver også berørt indledningsvist allerede i P1-projektet på 1. semester.
- **Design og udvikling af sikre systemer og software:** Behandles især på 3. semester, hvor semesterprojektet handler om "Sikkerhed i applikationsudvikling". Det understøttes af kurser i "Web-programmering og databaser" og "Computerarkitekturer og operativsystemer" samt valgfaget "Malware-analyse" på 7. semester.
- **Compliance (f.eks. NIS2, D-Mærket, relevante standarder som ISO 270xx mm.):** Understøttes af kurset "Sikkerhed i organisationer" og projektet "Cybersikkerhed og governance" på 5. semester samt valgfaget "Cybersikkerhed og lovgivning" på 7. semester.
- **Forebyggelse og detektion af cyberangreb:** Et gennemgående element i uddannelsen. Dækkes af kurserne "Introduktion til cybersikkerhed" (1. semester), "Etisk hacking" (3. semester), "Cloud-sikkerhed" og "Sikkerhed i IoT- og OT-miljøer" (5. semester)
- **Sikkerhed i computersystemer:** Dækkes primært af kurset af samme navn på 2. semester samt det videregående projekt i "Cybersikkerhed i distribuerede systemer" (5. semester)
- **Netværkssikkerhed:** Dækkes af kurset "Sikkerhed i computersystemer" og semesterprojektet "Netværkssikkerhed" på 2. semester. Semesterprojektet på 5. semester "Cybersikkerhed i distribuerede systemer' vil også indhold elementer fra netværkssikkerhed.
- **Kritisk infrastruktur:** Understøttes af adskillige kurser og projekter på 4. og 5. semester. Herudover dækker det valgfri kurset "Cybersikkerhed og lovgivning" de regulatoriske og lovgivningsmæssige rammer for kritiske infrastrukturer.
- **IoT-, OT og Cloud-sikkerhed:** Dækkes af kurserne "Cloud-sikkerhed" og "Sikkerhed i IoT- og OT-miljøer" (5. semester).

Virksomhedspraktik på 6. semester og det afsluttende bachelorprojekt vil ligeledes dække minimum et og typisk flere af disse kompetenceområder.

De organisatoriske kompetencer og kvalifikationer, der efterspørges i Fig. 2, trænes specielt på AAU, hvor alle studerende undervises efter den problembaserende læringstilgang. Alle studerende arbejder problem- og projektbaseret gennem hele uddannelsen, hvorigennem de opnår kompetencer i individuel problemløsning og arbejde ved fx individuel opgaveløsning på kurser, mens der opnås teamkompetencer på projektenheder, fx i tværfaglige samarbejder med virksomheder eller eksterne organisationer. I alle projekter skal de studerende på diplomingeniøruddannelsen håndtere komplekse og udviklingsorienterede situationer og kommunikere både skriftligt og mundtligt med andre studerende, vejledere og eventuelt andre samarbejdspartnere (fx fra industrien). Det udtrykte behov for organisatoriske kompetencer indgår således også i uddannelsen.

Jobfunktioner
De ovennævnte kompetencer relaterer sig til typiske jobfunktioner i virksomhederne, som en diplomingeniør i cybersikkerhed vil kunne varetage. I forbindelse med AAUs ansøgning om kandidatuddannelsen i cybersikkerhed fra 2019 blev følgende fem jobfunktioner eller jobprofiler identificeret:

- **Drift:** Sørger for den daglige drift af systemer og implementerer nye systemer, der er udviklet af andre, som købes til virksomheden. Vigtige kompetencer er f.eks netværksovervågning og drift af servere. Typisk større private virksomheder.
- **Specialiseret teknik:** De mere specialiserede, dybe teknikere, som arbejder med mere avancerede og tekniske opgaver. Det kan være opgaver som kodning, udvikling af sikre systemer, hacking og lignende. Typisk private IT-virksomheder eller offentlige organisationer, der beskæftiger sig med sikkerhed.
- **Compliance:** Skal overordnet sørge for, at virksomhedens cybersikkerhed lever op til de krav, love og reguleringer, der er gældende for virksomhedens produkter og services. Kræver en vis juridisk viden samt forståelse for de relevante krav og reguleringer og mulighederne for at kunne leve op til disse. Tidligere lå dette behov primært hos større og sommetider internationale private virksomheder, der opererer i flere lande med mange forskellige reguleringer, men i dag efterspørger også SMVer uddannede, som skal arbejde med compliance, pga. de øgede lovkrav.
- **Arkitektur**: Arbejder på et mere overordnet niveau, hvor de skal koble sikkerheden i virksomhederne med forretningens behov og strategi og er tættere på det strategiske niveau i virksomheden. Kræver en mere overordnet forretningsforståelse, så de kan se, hvordan virksomhedernes sikkerhedssystemer kan spille ind i virksomhedens andre forretningsområder, samt hvilken udvikling der er nødvendig fremadrettet. Særligt større private virksomheder.

- **Konsulent**: Findes i flere formater, herunder både generalist og specialist, og i både små og store konsulenthuse. Kræver viden om kommunikation, forretningsforståelse og compliance. Har brug for en dyb teknisk viden om cybersikkerhed for at kunne foretage risikovurderinger og identificere kritiske sårbarheder inden for f.eks. virksomhedens it-arkitektur, samspil med cloud-leverandører og forretningspartnere, forretningsprocesser og håndtering af kundeinformation. Eksempler er PwC, Omada og NNIT.

Det er AAUs vurdering, at ovenstående jobfunktioner kan varetages af diplom- og civilingeniører. Behovsundersøgelsen viser, at nogle virksomheder vil foretrække diplomingeniører pga. deres mere praksisnære tilgang (Epinion, s. 13-14), da diplomingeniører bliver hurtigere arbejdsklare (time to market) og kan være attraktive for SMVer, hvor dimittender fra kandidatuddannelsen i cybersikkerhed kan være mere attraktive for større virksomheder. Samlet set konkluderer AAU, at uddannelsen dækker de kompetenceområder og jobprofiler, der efterspørges af virksomhederne.

Vurdering af det samfundsmæssige behov for uddannelsen

I det efterfølgende redegøres for, hvordan AAU har vurderet det samfundsmæssige behov for uddannelsen ved at balancere arbejdsmarkedets behov for kompetencer, der ligger i diplomingeniøruddannelsen i cybersikkerhed med udbuddet af eksisterende beslægtede uddannelser.

Mangel på dimittender inden for cybersikkerhed i forhold til erhvervslivets behov

En analyse fra Deloitte[7] viser, at der er kritisk mangel på cybersikkerhedskompetencer i danske virksomheder, og at det gør Danmark sårbar. Mere end hver 3. it-virksomhed efterspørger kompetencer inden for it og cybersikkerhed, og det vurderes, at der i 2030 vil mangle mellem 15.000-20.000 fuldtidsansatte.

IDA vurderede i 2023[8], at der i Danmark er et stort behov for kompetencer inden for cybersikkerhed: Ca. 40% af alle SMV'er mangler kompetencer inden for it- og cybersikkerhed, og i den offentlige sektor har kun 54% af samfundskritiske it-systemer et tilstrækkeligt sikkerhedsniveau. Det konkluderes i samme rapport, at der skal være langt flere uddannede inden for cybersikkerhed, og at det som minimum skal sikres, at der på eksisterende uddannelser kan udbydes flere kurser inden for cybersikkerhed. Rapporten vurderer, at der i 2030, med den nuværende uddannelsesportefølje, vil blive uddannet 8.000 flere inden for it- og cybersikkerhedsuddannelserne sammenlignet med 2021, men at der alligevel vil mangle 22.000 it-folk, hvoraf ca. 15.000 af disse skal it-uddannes i mellemlange og lange videregående uddannelser. Ekspertgruppen vurderer i samme publikation, at der er et "*væsentligt udækket behov for specialister i cybersikkerhed. Efterspørgslen på disse kompetencer er steget hurtigt og er fortsat i vækst. Virksomhederne oplever stor rekrutteringsbyrde: Det tager lang tid at besætte ledige stillinger og der skal gives en høj løn. Ofte må man opgive at få specifikke kompetencekrav opfyldt, fordi man ikke kan finde kandidater, som mestrer f.eks. sikker systemarkitektur og kodning*".

Søgningen til uddannelserne

I IDA-rapporten[6] fra 2023 beskrives tendenser for optagelsen på videregående uddannelser. Rapporten beskriver, at der er stigninger på hhv. 10% i tilgangen til ingeniøruddannelser og 5% til it-uddannelser sammenlignet med 2022. I samme publikation undersøges de afviste kvalificerede ansøgere. Det vurderes, at antallet af afviste ansøgere steget med i alt 19% fra 2022 til 2023, hvilket svarer til 1400 flere afviste ansøgere. Ved optagelsen i 2023 havde 47% af de afviste kvalificerede ansøgere kun markeret én prioritet i ansøgningen.

En DI analyse[9] viser, at der i 2022 blev afvist 300 første prioritetsansøgere på universiteterne. Analysen viser også, at kun hver 5. afviste kvalificerede førsteprioritetsansøger til en it-uddannelse bliver optaget på en anden it-uddannelse. Det er således et tal, som ikke umiddelbart kan findes i KOT, men som er vigtigt at forholde sig til, når virksomhederne mangler så mange uddannede. Analysen viser, at der generelt afvises 576 ansøgere til en STEM-uddannelse i 2022, hvoraf 224 afvises fra DTU, 94 fra ITU samt 41 fra Aalborg Universitet. AAU ser dette som en signifikant faktor og mener, at alle potentielle it-

[7] https://www.altinget.dk/digital/artikel/deloitte-kritisk-mangel-paa-medarbejdere-med-cyberkompetencer-goer-nationen-saarbar

[8] https://ida.dk/media/14371/ida-ekspertgruppe-rapport_cybersikkerhed_a4.pdf

[9] https://www.danskindustri.dk/arkiv/analyser/2023/7/mange-kvalificerede-ansogere-afvises-fra-universiteternes-stem--og-it-uddannelser/

og cybersikkerheds-interesserede skal kunne finde en it- og cybersikkerhedsuddannelse, som de kan optages på via 1. prioritet.

IDA[6] viser, at der i perioden fra 2022-2023 er sket en stigning i søgning til it-uddannelser generelt på 8000 ansøgere. Ser man over en længere periode, så er optagelsestallene dog nu 2% lavere end de var i 2019. Dette kan skyldes, at regeringen har besluttet, at universiteterne i de store byer skal reducere optaget af studerende. Bl.a. har DTU optaget 2% færre it-studerende i 2023, selvom antallet af ansøgere har været større.

Tal fra Jobindex og Computerworld viser, at der i første halvår af 2023 var 1395 jobannoncer inden for it- og cybersikkerhed[10]. Samtidig konstateres det, at omkring 48% af it-virksomheder opgiver at besætte stillinger, idet der ikke er ansøgere til dem. Mette Lundberg, IT-Branchen, udtaler[11], at der ligger et stort paradoks i, at flere er interesserede i it-uddannelser, og at industrien efterspørger uddannede, og der samtidig afvises kvalificerede ansøgere til uddannelserne. Hun henviser til, at der i alt blev afvist 1.732 ansøgere på it-uddannelser i 2023 på grund af pladsmangel, hvilket har betydet, at 46,8% af danske virksomheder har måtte opgive at besætte ledige it-stillinger, da der ikke var ansøgere til dem.

Beslægtede uddannelser

Diplomingeniøruddannelser kan udbydes af både universiteter og erhvervsakademier (professionshøjskoler). I Danmark findes en række beslægtede bachelor-, professionsbachelor- og diplomingeniøruddannelser. Universiteterne AAU, DTU, ITU og SDU har alle it-bacheloruddannelser, hvor fokus er tekniske kompetencer inden for programmering og softwareudvikling, med enkelte fag inden for cybersikkerhed. Erhvervsakademierne udbyder alle en top-up uddannelse i it-sikkerhed på 1 1/2 år, der bygger oven på 2-årige forløb (AP degree) som datamatiker eller it-teknolog. De identificerede, beslægtede uddannelser indeholder alle elementer af it-teknologi som fagprofil og med en eller flere kurser form af enkeltkurser og dele af fagprofiler.

Tabel 1 viser en oversigt over de identificerede beslægtede it-uddannelser med mindst 5 ECTS inden for cybersikkerhed. Det udelukker uddannelser som Cyberværnepligten og Forsvarets Efterretningstjenestes Cyberakademi. Ydermere er efteruddannelser, som indeholder enkelte eller samlede uddannelsesforløb ikke medtaget.

Tabel 1: Oversigt over beslægtede uddannelser på universiteter og erhvervsakademier.

Beslægtede uddannelser	
AAU	**KEA**
01 Computerteknologi, bach. i tekn. videnskab (Aal)	09 Datamatiker (grundforløb)
02 Software, bach. i tekn. videnskab (Aal)	10 It-teknolog (grundforløb)
02a Software, bach. i tekn. videnskab (Kbh)	11 It-sikkerhed (top-up)
03 Cyber- og computerteknologi, bach. i tekn. videnskab (Kbh)	
DTU	**Erhvervsakademi Zealand**
04 Cyberteknologi, bach. i tekn. videnskab	12 Datamatiker (grundforløb)
05 Softwareteknologi, bach. i tekn. videnskab	13 It-teknolog (grundforløb)
06 Softwareteknologi, diplomingeniør	14 It-sikkerhed (top-up)
ITU	**Erhvervsakademi Aarhus**
07 Softwareudvikling, bach. I IT	15 Datamatiker (grundforløb)
SDU	16 It-teknolog (grundforløb)
08 Softwareteknologi, diplomingeniør	17 It-sikkerhed (top-up)

Bacheloruddannelserne i computerteknologi og software (AAU, Aalborg) indeholder et enkelt kursus i sikkerhed sent på uddannelserne. Bacheloruddannelsen i cyber- og computerteknologi (AAU, København) har i alt to kursusmoduler samt to projektmoduler (i alt 40 ECTS), hvori de studerende kan arbejde med cybersikkerhed. DTU's bacheloruddannelser i cyberteknologi samt softwareteknologi kombinerer teknologiudvikling med et enkelt kursus i cybersikkerhed. DTU's diplomingeniøruddannelse i softwareteknologi har ikke som udgangspunkt cybersikkerhedskurser, men de kan tilvælges som valgfag. ITU's bacheloruddannelse i softwareudvikling har fokus på softwareudviklingskompetencer. Studerende har også her mulighed for at vælge sikkerhed som et valgfag. Det samme er tilfældet med SDU's diplomingeniøruddannelse i softwareteknologi, hvor sikkerhed kan vælges som valgfag, men ikke er en integreret del af uddannelsen.

[10] https://itb.dk/maerkesager/digitale-kompetencer/fremtidens-rekrutteringshul-bliver-kun-stoerre/
[11] https://itb.dk/branchen-generelt/selvom-ansoegningstallet-skyder-i-vejret-sakker-kvinderne-bagud/

På top-up uddannelserne i IT-sikkerhed på erhvervsakademierne KEA, Zealand og EA Aarhus kan der vælges mellem kompetencer inden for videregående sikkerhed i IT-governance, softwaresikkerhed, penetrationstest samt SIEM og log-analyse. Det skal dog samtidig nævnes, at der ikke er krav til matematikkompetencer til forskel fra universitetsuddannelsernes krav til ingeniørbachelorer og diplomingeniører.

Optagelsespotentiale

I forbindelse med udvikling af diplomingeniøruddannelsen i cybersikkerhed er det undersøgt, om der er et uudnyttet kvalificeret optagelsespotentiale. Data for beslægtede uddannelser (beskrives i næste afsnit) og antallet af ansøgere med en af disse som deres 1. prioritet, sammenholdt med det reelle optagelsestal, kan give en indikation af behovet for uddannelsen.

Tabel 2 viser antal ansøgere på 1. prioritet og optagne på de udvalgte beslægtede uddannelser. Det har ikke været muligt at finde nøgletal for alle professionsbacheloruddannelserne samt top-up uddannelserne i it-sikkerhed. Alligevel er de medtaget her for at give et mere fuldstændigt billede.

Tabel 2: Antal ansøgere i 2022 og 2023 på 1. prioritet og antal optagne på beslægtede uddannelser. Data: KOT. Diplomuddannelser er markeret med (diplom), andre uddannelser er bacheloruddannelser. Det har ikke været muligt at finde tal for top-up uddannelserne på erhvervsakademierne KEA, Zealand og Aarhus vedr. optag, dimission osv.

	2022	2022	2023	2023
	Ansøgere, 1. prio.	**Optagne**	**Ansøgere, 1. prio.**	**Optagne**
Aalborg Universitet				
01 Computerteknologi, bach. i tekn. videnskab (Aal)	35	33	20	17
02 Software, bach. i tekn. videnskab (Aal)	138	145	135	127
02a Software, bach. i tekn. videnskab (Kbh)	71	58	71	82
03 Cyber- og computerteknologi, bach. i tekn. videnskab (Kbh)	31	31	45	42
Danmarks Tekniske Universitet				
04 Cyberteknologi, bach. i tekn. videnskab	27	30	30	30
05 Softwareteknologi, bach. i tekn. videnskab	98	112	123	90
06 Softwareteknologi, diplomingeniør	120	157	147	120
IT-Universitetet i Kobenhavn				
07 Softwareudvikling, bach. I IT	176	251	231	185
Syddansk Universitet				
08 Softwareteknologi, diplomingeniør	58	55	59	61
KEA				
09 Datamatiker, grundforløb	236	175	227	175
10 It-teknolog, grundforløb	122	120	157	130
11 It-sikkerhed, top-up udd.*		19		31
Erhvervsakademi Zealand				
12 Datamatiker, grundforløb	138	145	155	169
13 It-teknolog, grundforløb	0	0	35	38
14 It-sikkerhed, top-up udd.**				
Erhvervsakademi Aarhus				
15 Datamatiker, grundforløb	113	73	133	68
16 it-teknolog, grundforløb	47	36	52	36
17 it-sikkerhed, top-up udd.**				
* disse tal er fra KEA's egen årsrapport				
** der er ikke fundet tal for denne uddannelse				

I det efterfølgende redegøres der for, hvorledes den foreslåede diplomingeniøruddannelse kan bidrage til at udfylde behovet for it- og cybersikkerhedsuddannede.

På baggrund af tabellen kan det udledes, at der i 2023 i alt var 264 studerende, som ikke blev optaget på deres 1. prioritet. Specielt på uddannelser i Københavnsområdet var der på DTU og ITU i alt 106 afviste 1. prioritetsansøgere. Uddannelserne på KEA, Zealand og Erhvervsakademiet Aarhus har ydermere 147 afviste 1. prioritetsansøgere. Sammenligner man afviste ansøgere i 2022 (i alt 155, 85 fra universiteter og 70 fra erhvervsakademier) med 2023, kan der ses en 70% stigning i antallet af afviste første prioritetsansøgere til de beslægtede uddannelser.

På grund af regeringens beslutning om udflytning af uddannelser er det tydeligt, at der har været en effekt på optagelsespotentialet på de beslægtede uddannelser. DTU er i den forbindelse blevet pålagt at optage 5-10% færre studerende, mens ITU har været fritaget fra nedskæring af optag. Øvrige beslægtede uddannelser har ikke skåret ned på IT-relaterede uddannelser[12]. AAU konkluderer hermed, at der er et kvalificeret optagelsespotentiale for uddannede med cybersikkerheds- og it-kompetencer.

I forbindelse med udarbejdelsen af ansøgningen om nærværende uddannelse har dekanatet på Det Tekniske Fakultet for IT og Design informeret en række universiteter om AAU's arbejde vedrørende den nye uddannelse. Således er der fremsendt en orientering til DTU, KEA, ITU, SDU. Ingen af de adspurgte universiteter havde kommentarer ang. uddannelsens opbygning og kompetenceprofil, hvorfor høringssvarene ikke har givet anledning til justering i uddannelsens opbygning. KEA har dog fremsendt bemærkninger til AAU med bekymring for, om AAUs foreslåede uddannelse til forringe vilkårene for deres aktiviteter inden for cybersikkerhed. KEA er i tillæg selv ved at ansøge om ny professionsbacheloruddannelse i cybersikkerhed.

AAU har reflekteret over KEAs input og vurderer med ovenstående redegørelse, at det er tydeligt, at der er et tilstrækkeligt stor og kvalificeret optagelsespotentiale i Hovedstadsområdet, hvorfor de to udbud kan sameksistere uden, at dette forringer vilkårene eller skabe uhensigtsmæssige mellem udbuddene.
I nedenstående afsnit redegøres derfor sammenhængen mellem den foreslåede uddannelse samt beslægtede uddannelser. Ud fra analysen er det ligeledes tydeliggjort, at de to udbud har overlappende kernekompetencer, men også at de adskiller sig på fx matematik og netværk, som AAUs foreslåede diplomingeniøruddannelse indeholder. Dermed er målgruppen for de to uddannelser også forskellig fra hinanden. De potentielle studerende, der søger om optagelse på AAUs diplomingeniøruddannelse i cybersikkerhed, er den målgruppe, som gerne vil blive ingeniører og har kvaliteter og interesse for de ingeniørfaglige discipliner med høje krav til matematik og avancerede tekniske fag. Herudover kan AAUs målgruppe have intentioner og overvejelser, om at de på sigt kan tage en kandidatuddannelse, hvilket ikke er en mulighed for de studerende, som optages på KEAs udbud.

I Tabel 3 vises det, hvordan beslægtede uddannelser har overlappende kompetenceområder med den foreslåede diplomingeniøruddannelse i cybersikkerhed samt fordelingen af kompetencer inden for matematik, programmering, netværk og cybersikkerhed. Ud fra aftagermøderne er det vurderet, at særligt disse kompetenceområder bør være centrale for den foreslåede uddannelse i cybersikkerhed, og de er derfor anvendt i screeningen for kompetencer i Tabel 3. Diplomingeniøruddannelserne og erhvervsakademiernes uddannelser understøtter i højere grad virksomhedstilknytning.

[12] https://dm.dk/akademikerbladet/aktuelt/2022/marts/overblik-saadan-bliver-universiteterne-ramt-af-udflytningsplanen/

Tabel 3: Overblik over beslægtede uddannelser og deres kompetenceområder[13]. "X" betyder, at kompetencen er til stede, mens "(X)" betyder, at dele af kompetencen er til stede (og kun er opfyldt ved valgfag).

Uddannelse	Matematik	Program-mering	Net-værk	Cyber-sikkerhed	Virksomheds-tilknytning
Aalborg Universitet					
01 Computerteknologi, bach. i tekn. videnskab (Aal)	X	X	X	X	
02 Software, bach. i tekn. videnskab (Aal)	X	X	(X)	X	
02a Software, bach. i tekn. videnskab (Kbh)	X	X	(X)	X	
03 Cyber- og computerteknologi, bach. i tekn. videnskab (Kbh)	X	X	X	X	
Danmarks Tekniske Universitet					
04 Cyberteknologi, bach. i tekn. videnskab	X	X	X	(X)	
05 Softwareteknologi, bach. i tekn. videnskab	X	X		(X)	
06 Softwareteknologi, diplomingeniør	X	X		(X)	X
IT-Universitetet i Kobenhavn					
07 Softwareudvikling, bach. I IT		X		(X)	
Syddansk Universitet					
08 Softwareteknologi, diplomingeniør	X			(X)	X
KEA					
09 Datamatiker, grundforløb		X			
10 It-teknolog, grundforløb		X			
11 It-sikkerhed, top-up udd.*		X		X	X
Erhvervsakademi Zealand					
12 Datamatiker, grundforløb		X			
13 It-teknolog, grundforløb		X			
14 It-sikkerhed, top-up udd.**		X		X	X
Erhvervsakademi Aarhus					
15 Datamatiker, grundforløb		X			
16 it-teknolog, grundforløb		X			
17 it-sikkerhed, top-up udd.**		X		X	X

Af tabellen ses det, at de uddannelser, som er tættest beslægtet med diplomuddannelsen i cybersikkerhed, er bacheloruddannelserne i hhv. cyber- og computerteknologi (AAU) og computerteknologi (AAU), hvor der er flere overlappende kompetencer, men hvor virksomhedstilknytningen ikke er så stærk. Bacheloruddannelserne i software (AAU) og cyberteknologi (DTU) har overlappende kompetencer inden for matematik og programmering samt netværk, men ingen af disse uddannelser har fokus på kompetencer inden for cybersikkerhed og har ikke tæt virksomhedstilknytning. Bachelor- og diplomingeniøruddannelsen i softwareteknologi (begge SDU), og bacheloruddannelsen i softwareudvikling (ITU) har få overlappende kompetencer mest inden for programmering. Professionsbacheloruddannelserne fra KEA, Zealand og Erhvervsakademi Aarhus har overlappende kompetencer i programmering samt i cybersikkerhed (for de studerende, der tager top-up muligheden) samt virksomhedstilknytning, men mangler fokus på matematik og netværk.

Den foreslåede diplomingeniøruddannelse i cybersikkerhed er kompetencegivende inden for alle områder i Tabel 3 og giver dermed en samlet kompetenceprofil inden for it- og cybersikkerhed, som ikke eksisterer i det danske uddannelseslandskab.

Idet den foreslåede uddannelse potentielt vil blive en del af undervisningstilbuddet, er det relevant at se på, hvorledes de beslægtede uddannelser ser ud mht. optag og beskæftigelse. I Tabel 4 angives de beslægtede uddannelser pr. institution samt nøgletal som optag (tilgang) og dimittendtal baseret på udtræk fra Uddannelses- og Forskningsministeriets datavarehus.

Tabel 4 viser desværre ikke tal for bacheloruddannelserne i software og cyber- og computerteknologi (AAU, Kbh), idet disse uddannelser er nyere uddannelser med første studiestart i henholdsvis 2020 og 2021. Ligeledes har det ikke været muligt i at finde tal for professionsbacheloruddannelserne KEA, Zealand og Erhvervsakademi Aarhus i Uddannelses- og Forskningsministeriets datavarehus, som er sammenlignelige med de andre uddannelsestal. Der er derfor foretaget et estimat baseret på tallene fra Tabel 1, hvoraf det fremgår, at på KEA går ca. 10% af de optagne studerende på datamatiker og it-teknologuddannelsen videre på top-up uddannelsen i it-sikkerhed i 2023. Hvis man antager, at det også er gældende for Zealand og Erhvervsakademi Aarhus, så har man et samlet tal på (31, 21 og 10), i alt 62 optagne studerende i 2023.

[13] Vurderingen er foretaget efter gennemgang af studieordninger fra de beslægtede uddannelser. Der er lidt usikkerhed forbundet med vurderingen, da nogen uddannelser har en række valgfri kursus-elementer, som kan give uddannelsen en lidt anden karakter dog uden at helhedsbilledet bliver ændret.

Tabel 4: Oversigt over beslægtede uddannelser samt nøgletal som optag (tilgang) og dimittendtal fra årene 2019-2022. Kilde: Udtræk fra Uddannelses- og Forskningsministeriets Datavarehus.

	Tilgang				Dimittender			
	TG 2019	TG 2020	TG 2021	TG 2022	DM 2019	DM 2020	DM 2021	DM 2022
Aalborg Universitet								
01 Computerteknologi, bach. i tekn. videnskab (Aal)	23	23	18	25	7	0	16	21
02 Software, bach. i tekn. videnskab (Aal)	161	206	231	192	59	83	103	95
02a Software, bach. i tekn. videnskab (Kbh)								
03 Cyber- og computerteknologi, bach. i tekn. videnskab (Kbh)	0	0	0	0				
Danmarks Tekniske Universitet								
04 Cyberteknologi, bach. i tekn. videnskab	39	47	37	31	19	8	17	15
05 Softwareteknologi, bach. i tekn. videnskab	85	120	98	94	58	59	59	52
06 Softwareteknologi, diplomingeniør	90	110	117	114	64	62	46	58
IT-Universitetet i Kobenhavn								
07 Softwareudvikling, bach. i IT	161	194	164	153	71	97	97	100
Syddansk Universitet								
08 Softwareteknologi, diplomingeniør	83	64	56	50	10	15	22	32
KEA								
09 Datamatiker, grundforløb								
10 It-teknolog, grundforløb								
11 It-sikkerhed, top-up udd.*								
Erhvervsakademi Zealand								
12 Datamatiker, grundforløb								
13 It-teknolog, grundforløb								
14 It-sikkerhed, top-up udd.**								
Erhvervsakademi Aarhus								
15 Datamatiker, grundforløb								
16 it-teknolog, grundforløb								
17 it-sikkerhed, top-up udd.**								
I alt	642	764	721	659	288	324	360	373

Af Tabel 4 fremgår det, at der i alt kun er sket en stigning på optaget på ganske få studerende fra 642 i 2019 til 659 i 2022. i årene 2021 og 2022 har der dog været så mange som 764 og 721 studerende på uddannelserne. Fluktuationen skal ses som et resultat af Covid-perioden i 2020 og 2021, hvor flere studerende søgte ind på en uddannelse, mens årene fra 2019 og 2022 viser det normale niveau.[14]

For alle de beslægtede uddannelser sker der et vist frafald i løbet af studietiden, så antallet af dimittender er ca. 350-380 hvert år. Reelt er der dog et mindre antal dimittender med de efterspurgte kompetencer. Hvis der alene kigges på de tættest beslægtede uddannelser fra Tabel 3 (uddannelserne 1-5), kom der i 2022 kun 183 dimittender med en cybersikkerhedsprofil samt 62 professionsbachelorer (estimeret) med en cybersikkerheds top-up uddannelse, hvilket i alt giver 245 dimittender inden for cybersikkerhed. Som tidligere nævnt, er der et betydeligt større behov for studerende med disse profiler, og at der skal uddannes betydeligt flere dimittender for at imødekomme nuværende og kommende behov.

Det kan på ovenstående baggrund konkluderes, at der er et klart behov for og plads i det danske uddannelseslandskab til diplomingeniøruddannelsen i cybersikkerhed. Dette dels på grund af den store aktuelle mangel på kompetencer inden for it- og cybersikkerhed, der yderligere vil stige i de kommende år, og dels fordi der eksisterer et kompetencegab inden for matematik, programmering, netværk og cybersikkerhed, hvor alle de efterspurgte kompetencer ikke kan genfindes på nogen af de eksisterende uddannelser. Som det er vist tidligere, efterspørges de specifikke kompetencer, uddannelsen vil give inden for diplomuddannelsen i cybersikkerhed af aftagervirksomheder, både nu og fremover.

Ledighedsfrekvens på beslægtede uddannelser

I afdækningen af det samfundsmæssige behov for diplomingeniøruddannelsen i cybersikkerhed er ledighedsfrekvensen for de beslægtede uddannelser blevet undersøgt via udtræk fra Uddannelses- og Forskningsministeriets datavarehus. Tabel 5 viser oversigten over ledighedsfrekvensen samt antal fuldførte studerende for beslægtede uddannelser i perioden 2019-2021. Ledigheden er opgjort som den gennemsnitlige ledighedsgrad i 4-7. kvartal efter dimission. Det er ikke alle beslægtede uddannelser, der har tal for ledighedsfrekvens i perioden fra 2019-2021.

[14] https://ufm.dk/aktuelt/pressemeddelelser/2023/kvote-2-sogningen-stiger-tallene-tyder-pa-gradvis-normalisering-efter-covid-19

Tabel 5: Beslægtede uddannelser antal fuldførte (FF) samt ledighedsfrekvens i % (LF) for perioden 2019-2021. Kilde: Uddannelses- og Forskningsministeriets Datavarehus. Databasen indeholder ikke sammenlignelige data for professionsbacheloruddannelserne 9-17.

	2019				2021	
	FF	LF	FF	LF	FF	LF
Aalborg Universitet						
01 Computerteknologi, bach. i tekn. videnskab (Aal)	7	1%			16	3%
02 Software, bach. i tekn. videnskab (Aal)	59	3%	83	1%	103	2%
02a Software, bach. i tekn. videnskab (Kbh)						
03 Cyber- og computerteknologi, bach. i tekn. videnskab (Kbh)						
Danmarks Tekniske Universitet						
04 Cyberteknologi, bach. i tekn. videnskab	19	0%	8	1%	17	3%
05 Softwareteknologi, bach. i tekn. videnskab	58	0%	59	0%	59	0%
06 Softwareteknologi, diplomingeniør	64	9%	61	3%	46	0%
IT-Universitetet i Kobenhavn						
07 Softwareudvikling, bach. I IT	71	1%	97	1%	97	0%
Syddansk Universitet						
08 Softwareteknologi, diplomingeniør	10	8%	15	9%	22	2%
KEA						
09 Datamatiker, grundforløb						
10 It-teknolog, grundforløb						
11 It-sikkerhed, top-up udd.*			47		82	
Erhvervsakademi Zealand						
12 Datamatiker, grundforløb						
13 It-teknolog, grundforløb						
14 It-sikkerhed, top-up udd.						
Erhvervsakademi Aarhus						
15 Datamatiker, grundforløb						
16 it-teknolog, grundforløb						
17 it-sikkerhed, top-up udd.						
* tal fra KEA's årsrapport						

Ledighedsprocenten for de i Tabel 5 sammenlignede tættest beslægtede bacheloruddannelser ligger mellem 0,2% (softwareudvikling ITU) og 3,1%, hhv. computerteknologi (AAU) og cyberteknologi (DTU). Der er dog ingen ledighedstal for software (AAU CPH), cyber- og computerteknologi (som er nye uddannelser) samt uddannelserne fra KEA, Zealand og Erhvervsakademi Aarhus. Hvis man ser generelt på alle uddannelserne for året 2021, er gennemsnittet af ledighedsprocenten 1,6%. Ifølge Uddannelses- og Forskningsministeriets datavarehus ligger beskæftigelsesprocenten for de beslægtede uddannelser mellem 97-100% i 2021. Beskæftigelsesprocenten for computerteknologi er for eksempel på 97%, for DTU's diplomingeniør i softwareteknologi 100% og for SDUs diplomingeniør i softwareteknologi 98%.

Den lave ledighedsprocent for beslægtede uddannelser indikerer, at dimittenderne enten kommer i job med det samme eller fortsætter på en kandidatuddannelse. I Tabel 6 er den gennemsnitlige ledighedsprocent i 4-7. kvartal efter dimission undersøgt for de tættest beslægtede kandidatuddannelser (cand.polyt.).

Gennemsnittet for den akkumulerede ledighed er på 2,2%. Disse gennemsnit ligger tæt på IDAs statistik[8] over total ledighed for ingeniører over tid, som er mellem 2,1% og 3,1% i perioden 2019-2022, mens ledighedsprocenten totalt over samme periode er 1,3%. På denne baggrund vurderer AAU, at diplomingeniører i cybersikkerhed hurtigt vil komme i beskæftigelse eller overgå til en relevant kandidatuddannelse. Ligeledes vurderer AAU, at dimittender fra tætbeslægtede uddannelser kommer hurtigt i beskæftigelse, hvilket yderligere understøtter konklusionen om, at der eksisterer stor efterspørgsel på dimittender med kompetencer inden for området.

Tabel 6: Oversigt over fuldførte og ledighedsgrad for kandidatuddannelser (cand.polyt.) i årene 2019-2021. Kilde: Undervisnings- og Forskningsministeriet Datavarehus.

Kandidatuddannelse	Antal fuldførte			Ledighedsgrad			Total	
(Civilingeniør, 2-årig)	2019	2020	2021	2019	2020	2021	Fuldførte	Ledighedsgrad
Innovativ kommunikationsteknik og entreprenørskab (AAU)	18	6	14	5,1%	7,0%	0,0%	38	4,0%
Software (AAU)	41	60	61	2,4%	1,9%	0,7%	162	1,7%
Informationsteknologi (DTU)	109	98	149	2,6%	2,3%	1,4%	356	2,1%
Kommunikationsteknologier og Systemdesign (DTU)	23	10	10	3,6%	0,0%	9,2%	43	4,3%
Computerteknologi (AU)	20	27	38	0,0%	1,4%	2,1%	85	1,2%
Software engineering (SDU)	37	26	36	2,8%	0,3%	0,1%	99	1,1%

Behovet for uddannelse på det fremtidige arbejdsmarked (behovsundersøgelsen)
Nogle af behovsundersøgelsens hovedkonklusioner (Epinion, side 3) er:

- ***Virksomhederne har allerede i dag et behov for ingeniører med kompetencer inden for cybersikkerhed og forventer, at behovet vil være stigende de kommende år***
  85 pct. af virksomhederne i undersøgelsen angiver, at de i nogen eller høj grad har et behov for ingeniører med kompetencer inden for cybersikkerhed i dag. De forventer desuden, at behovet vokser de kommende år - blandt andet som følge af et øget trusselsbillede og ny lovgivning på området. 69 pct. af virksomhederne forventer, at behovet for denne typer af ingeniører vil være større om tre år, end det er i dag, mens 28 pct. forventer, at behovet vil være det samme.
- ***Rekrutteringssituationen er udfordret af et lille udbud og en stor efterspørgsel***
  Virksomhederne i undersøgelsen oplever generelt en udfordrende rekrutteringssituation grundet et lille udbud af ingeniører med kompetencer inden for cybersikkerhed kombineret med en stor efterspørgsel. 52 pct. af virksomhederne synes, at rekrutteringen i dag er svær eller meget svær, og 27 pct. har aktuelt ledige stillinger på området. I fremtiden forventer 30 pct. af virksomhederne, at rekrutteringssituationen vil være den samme som nu, mens 42 pct. tror, at det vil være endnu sværere at rekruttere om tre år, end det er i dag.
- ***Virksomhederne er generelt positivt indstillet overfor en ny diplomingeniøruddannelse i cybersikkerhed***
  Efter at være blevet præsenteret for en kort beskrivelse af uddannelsen vurderer 69 pct. af virksomhederne, at det i høj eller nogen grad vil være relevant for dem at ansætte en diplomingeniør fra uddannelsen. Interviewpersonerne ser uddannelsen som et godt fundament, som dimittenderne kan bygge videre på med erhvervserfaring, en kandidatuddannelse eller efteruddannelse. Interviewpersonerne er særligt positive over, at de studerende kommer i praktik og skriver et praksisorienteret bachelorprojekt.

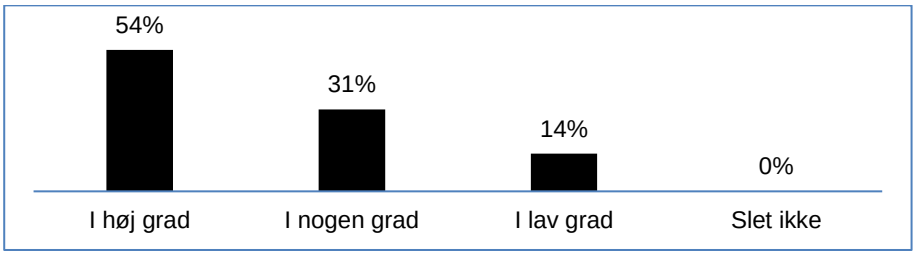
Der findes allerede en kandidatuddannelse i cybersikkerhed, hvorfra der uddannes civilingeniører, men virksomhederne frygter ikke, at diplomingeniøruddannelsen karambolerer med kandidatuddannelsen i cybersikkerhed. "Resultaterne af undersøgelsen tyder ikke på, at diplomuddannelsen vil konkurrere unødigt med kandidatuddannelsen i cybersikkerhed. 75 pct. af virksomhederne foretrækker ikke en civilingeniør over en diplomingeniør eller omvendt, når de skal ansætte. Interviewpersonerne fremhæver desuden, at man på mange andre ingeniørretninger har både et diplom- og et civilingeniørspor. De mener at diplomingeniørerne i modsætning til civilingeniører særligt vil være relevante for små og mellemstore virksomheder, der ikke i samme grad som store virksomheder har behov for en lige så høj grad af specialisering. Samtidig kommer diplomingeniørerne hurtigere ud på arbejdsmarkedet, som er i stor mangel på arbejdskraft." *(Epinion, s. 3).*

I undersøgelsen er virksomhederne derfor blevet spurgt om, hvorvidt de foretrækker en civilingeniør over en diplomingeniør (eller omvendt). 75 pct. af virksomhederne foretrækker dog ikke den ene profil frem for den anden, når de skal ansætte en ny medarbejder til at varetage opgaver inden for cybersikkerhed. Blandt de resterende virksomheder er der en lille tendens til, at virksomhederne foretrækker en civilingeniør, men 10 pct. af virksomhederne angiver omvendt, at de foretrækker en diplomingeniør.

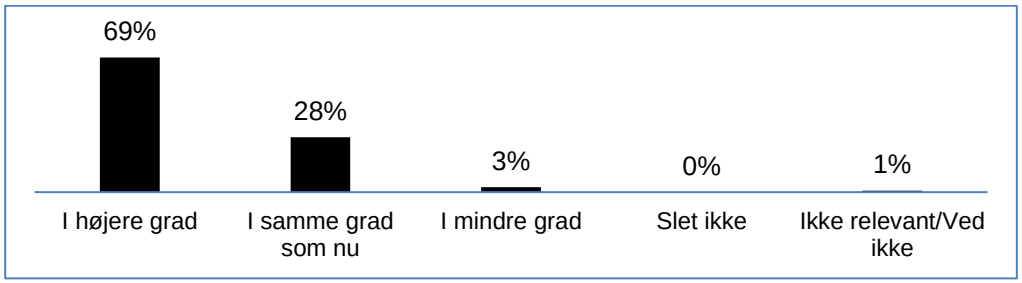
I interviewene fremgår det, at behovet for en diplomingeniøruddannelse i cybersikkerhed ikke bliver mindre i kraft af, at der allerede er en civilingeniøruddannelse i samme felt. Det skyldes, at de to uddannelser ses som grundlæggende forskellige og derfor supplerer hinanden. Flere nævner desuden, at den store fordel ved en diplomingeniøruddannelse er, at de studerende bliver arbejdsklar hurtigere, og det er der brug for givet den store mangel på folk med kompetencer inden for området. Nogle peger på, at der hvor de ser den største relevans for den type af kandidater er hos de små og mellemstore virksomheder, som ikke har behov for de samme specialiserede kompetencer som hos de store virksomheder.

Ja altså det at have begge uddannelser giver mening, bare fordi vi har behov for begge dele. Altså man kan jo vende den om og sige: Vi har jo også både diplom og kandidat på alle andre ingeniøruddannelser. Og du får hurtigere nogle folk ud, som kan arbejde med det, og som kan indgå i et team og eksekvere (Epinion, s. 14).

I behovsundersøgelsen er der blevet spurgt til, hvorvidt virksomhederne finder behov for kompetencerne, der er relaterer til diplomuddannelsen i cybersikkerhed nu og i fremtiden. Figur 3 og 4 viser behovet for kompetencer for cybersikkerhed i dag og om 3 år.

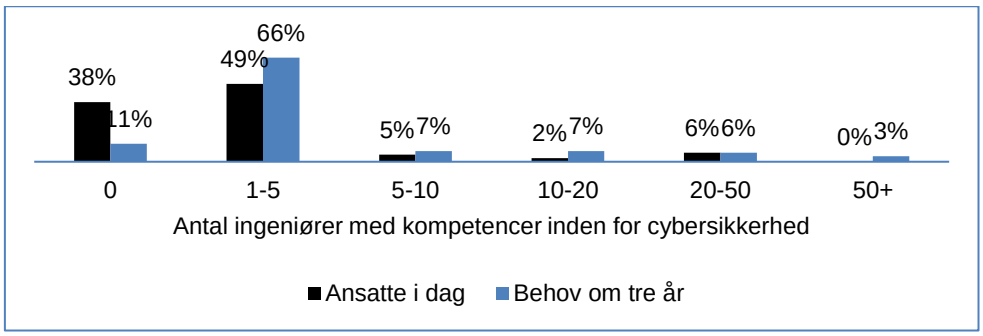


Figur 3: I hvilken grad vurderer du, at der i din virksomhed i dag er brug for ingeniører med kompetencer inden for cybersikkerhed? N=118. Kilde: Epinion (s. 4).



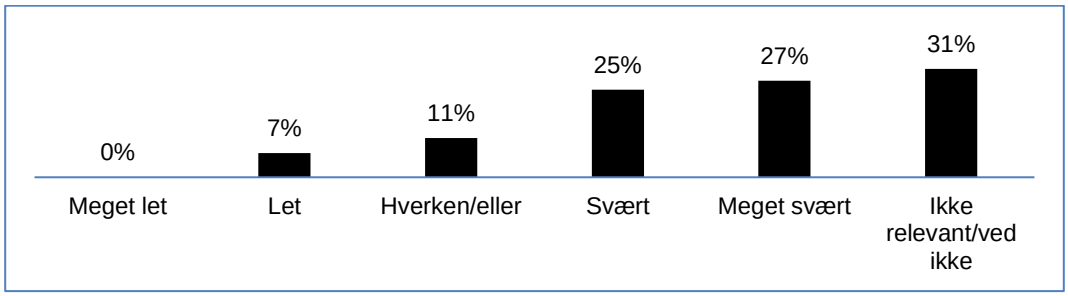
Figur 4: I hvilken grad vurderer du, at der om tre år vil være behov for ingeniører med kompetencer inden for cybersikkerhed? N=118. Kilde: Epinion (s. 6).

Sammenholdes figur 3 og 4, er det tydeligt, at de adspurgte virksomheder har et stort behov for uddannede inden for it- og cybersikkerhed: 85% af virksomhederne har i høj eller nogen grad behov for cybersikkerhedskompetencer lige nu. Dette tal øges dog, når man ser på behovet om 3 år, hvor 69% af virksomhederne forventer at behovet vil stige, mens 28% forventer, at det vil være på samme niveau som i dag. Disse tal understøttes af vurderingen af, at mange af virksomhederne forventer at ansætte flere personer i stillinger om 3 år (Figur 5).

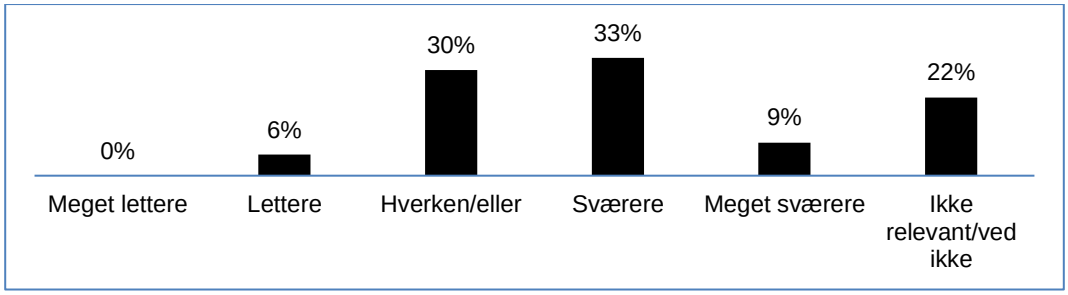


Figur 5: Hvor mange ingeniører har I ansat i dag med kompetencer inden for cybersikkerhed? og hvor mange ingeniører forventer I cirka, at I har behov for om tre år med kompetencer inden for cybersikkerhed? N=118. Kilde: Epinion (s.6).

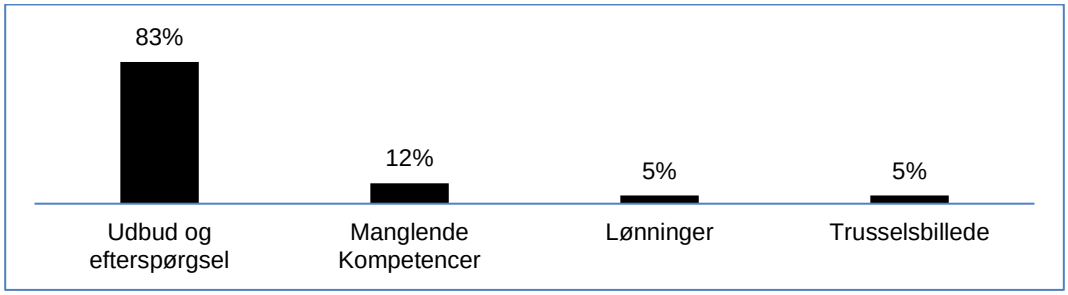
I behovsundersøgelsen er virksomhederne blevet adspurgt, hvor svært de oplever det at rekruttere ansatte med kompetencer inden for cybersikkerhed i dag (Figur 6), og hvordan de forventer situationen vil være om 3 år (Figur 7). Det ses, at 52% af virksomhederne vurderer, at det i dag er svært eller meget svært at rekruttere ingeniører med kompetencer inden for cybersikkerhed. 42% af de adspurgte virksomheder vurderer, at det også vil være svært eller meget svært om 3 år, mens 30% mener, det vil være på samme niveau som nu (hverken eller). Det lave udbud i forhold til efterspørgslen angives af 83% som den væsentligste årsag (Figur 8).



Figur 6: Hvor let eller svært oplever du, at det er for din virksomhed at rekruttere ingeniører med kompetencer inden for cybersikkerhed? N=118. Kilde: Epinion (s.9).



Figur 7: Forventer du, at det vil blive lettere eller sværere for din virksomhed at rekruttere ingeniører med kompetencer inden for cybersikkerhed inden for de næste tre år? N=118. Kilde: Epinion (s.11).



Figur 8: Beskriv gerne hvorfor du forventer, at det inden for de kommende år vil blive sværere for din virksomhed at rekruttere ingeniører, der har kompetencer inden for cybersikkerhed. N=42, der summeres til mere end 100, da nogle virksomheder har angivet flere svar. Kilde: Epinion (s. 11).

Interviewpersonerne fra Epinion's behovsundersøgelse mener, at der ikke uddannes nok dimittender med kompetencer inden for cybersikkerhed, og at det gør, at de ikke er optimistiske over for den fremtidige rekrutteringssituation: *"Der uddannes ikke nok. Det er nok 15 år siden, at vi startede med at efterlyse, at flere på cybersikkerhedsområdet blev uddannet. Der er lavet den ene rapport efter den anden, der peger på, at vi mangler medarbejdere på det her område". (Epinion, s. 12)*

Dette underbygges med, at en anden interviewperson fortæller om det stigende behov for uddannede inden for it- og cybersikkerhed i takt med, at nye teknologier udvikles og bruges og den stigende mængde af krav fra lovgivningen: *"Behovet er stigende. Det her område bliver ikke mindre vigtigt, og vi har i mange år haft et underskud af folk, som kan noget med cybersikkerhed. Der kommer jo de næste år en masse lovgivning, som man skal arbejde med som virksomhed, så det betyder, at virksomheder som ikke har forholdt sig til det tidligere bliver mødt af lovkrav. Det givet et øget pres på organisationer - der skal ansættes flere folk og flere rådgivere. (Epinion, s. 6)*

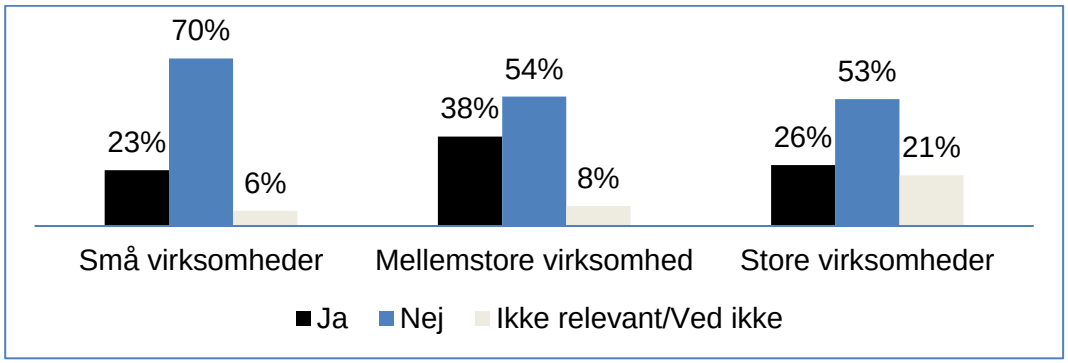
Ligeledes beskrives, at det er et konkurrencepræget marked, der er drevet af et for lille udbud og for stor efterspørgsel efter medarbejdere med kompetencer inden for cybersikkerhed:

> *"Det er et svært marked at rekruttere i. Jeg tror, at efterspørgslen overgår udbuddet, og derfor kunne jeg godt tænke mig, der var et større udbud af folk at vælge imellem i denne her verden" (Epinion, s. 9).*
>
> *"Det er et kompetitivt marked i forhold til at få rekrutteret. Vi bruger et eksternt konsulent-bureau til at hjælpe os med at finde de rigtige. Specielt når søger de specialiserede profiler. Vi har også nogle tiltag for at rekruttere kvinder (Epinion, s. 10).*

Epinion har derudover estimeret, at der på tværs af landet er ca. 27% af virksomhederne i undersøgelsen, som på tidspunktet for undersøgelsen har en eller flere ubesatte stillinger. Det svarer til ca. 58

ledige stillinger, som kunne besættes af en ingeniør inden for cybersikkerhed. Virksomhederne med ledige stillinger ligger primært i Region Hovedstaden og Region Midtjylland. Som vist på Figur 9 angiver 38% af de mellemstore virksomheder, at de har ubesatte stillinger, mens tallene for små og store virksomheder ligger på hhv. 23% og 26%.

AAU vurderer hermed, at virksomheder i høj grad har brug for uddannelsens kompetencer både nu og i fremtiden. Diplomingeniører fra den nye uddannelse i cybersikkerhed vil kunne gå direkte ud i erhvervslivet, men de vil også have mulighed for at fortsætte på kandidatuddannelsen i cybersikkerhed. Beslægtede uddannelser har lav ledighed, hvilket betyder, at der er stor chance for, at diplomingeniørerne kommer i job med det samme. Med et forventet optag på 30-40 diplomingeniører i cybersikkerhed kan det konkluderes, at der er behov for og plads til uddannelsen på det nuværende uddannelsesmarked.



Figur 9: Har virksomheden aktuelt ubesatte stillinger, der vil kunne varetages af en ingeniør med kompetencer inden for cybersikkerhed? (opdelt på virksomhedsstørrelse) N=118. Kilde: Epinion (s.10).

Bilag 1: Uddannelsens kompetenceprofil og modulopbygning

Uddannelsens kompetenceprofil (dec. 2023)

Viden

- Har viden om centrale teorier, metoder og praksis inden for fagområdet cybersikkerhed
- Kan forstå og reflektere over teorier, metoder og praksis inden for fagområdet cybersikkerhed
- Har indsigt i fagområdets matematiske grundlag
- Har viden om agile principper og metoder, som anvendes inden for professionen til udvikling
- Har viden om distribuerede systemer og kommunikationsnetværk
- Har forståelse for og viden om udvikling af software, herunder samspil med hardware
- Har viden om grundlæggende begreber og løsninger i forhold til netværks- og systemsikkerhed
- Har indsigt i professionens praksis
- Kan systematisk gennemføre og dokumentere forsøg/test og på baggrund heraf drage konklusioner
- Har indsigt i etiske og regulatoriske aspekter af cybersikkerhed
- Har indsigt i betydningen af cybersikkerhed for samfund, virksomheder, organisationer og individ
- Har viden om og forståelse af praksiskrav inden for sikkerhed og kommunikationssystemer
- Har viden om metoder til planlægning og styring af teamorganiseret projektarbejde

Færdigheder

- Kan anvende tidssvarende metoder og redskaber til at beskrive, analysere, modellere, implementere, verificere og dokumentere cybersikkerhed
- Kan anvende principper og metoder inden for agil systemudvikling
- Kan vurdere teoretiske og praktiske problemstillinger samt begrunde og vælge relevante løsninger med udgangspunkt i litteraturstudier, modeller, analyser, simuleringer og/eller test
- Kan på videnskabeligt grundlag gennemføre forsøg og drage valide konklusioner.
- Kan formidle faglige problemstillinger og løsningsmodeller til fagfæller og ikke-specialister eller samarbejdspartnere eller brugere.
- Kan reflektere over erfaringsudveksling mellem uddannelse og professionens praksis
- Kan argumentere for og anvende teorier, metoder og værktøjer til at overvåge, analysere, designe og implementere løsninger til cybersikkerhed

Kompetencer

- Har en metodisk arbejdsform
- Har færdigheder i agil systemudvikling og forstår principper, fordele og ulemper
- Kan diskutere fagbegreber i forbindelse med cybersikkerhed i software og computernetværk
- Kan redegøre for menneskelige aspekter af cybersikkerhed
- Er i stand til at designe løsninger til ønsket funktionalitet ved analyse, simulering og implementering
- Kan forstå og diskutere løsninger relateret specielt til sikkerhed i software og netværk
- Kan håndtere komplekse og udviklingsorienterede situationer i studie- eller arbejdssammenhænge.
- Kan selvstændigt indgå i fagligt og tværfagligt samarbejde med en professionel tilgang
- Kan omsætte akademiske kundskaber og færdigheder til praktisk problemløsning
- Kan identificere egne læringsbehov og strukturere egen læring i forskellige læringsmiljøer

Modulopbygning af uddannelsen (juli 2024)

Semester	ECTS	Modul	Titel
1	5	Kursus	Introduktion til cybersikkerhed
	5	Kursus	Imperativ programmering
	5	Kursus	Problembaseret læring
	5	Projekt P0	Teknologisk projektarbejde

	10	Projekt P1	Cybertrusler og cyberangreb
2	5	Kursus	Sikkerhed i computersystemer
	5	Kursus	Computernetværk
	5	Kursus	Matematik for cybersikkerhed
	15	Projekt P2	Netværkssikkerhed
3	5	Kursus	Etisk hacking
	5	Kursus	Web-programmering og databaser
	5	Kursus	Computerarkitekturer og operativsystemer
	15	Projekt	Sikkerhed i applikationsudvikling
4	5	Kursus	Risikohåndtering
	5	Kursus	Datasikkerhed og privatlivsbeskyttelse
	5	Kursus	Sandsynlighedsregning og statistik
	15	Projekt	Cyberangreb og -forsvar
5	5	Kursus	Cloud-sikkerhed
	5	Kursus	Sikkerhed i IoT- og OT-miljøer
	5	Kursus	Valgfrihed mellem: - Machine learning og AI i cybersikkerhed - Sikkerhed i organisationer
	15	Projekt	Valgfrihed mellem: - Cybersikkerhed i distribuerede systemer - Cybersikkerhed og governance
6	30	Projekt	Ingeniørpraktik
7	5	Kursus	Projektledelse og forretningsforståelse
	5	Kursus	Valgfrihed mellem: - Cybersikkerhed og lovgivning - Malware-analyse
	20	Projekt	Bachelorprojekt

Bilag 2: Liste med virksomheder og kontaktpersoner

Medlemmer af aftagerpanelet for Institut for Elektroniske Systemer:

- Claus Siggaard Andersen, Telenor A/S
- Jakob Birk Filsø, Turf Tank
- Jan Harding Gliemann, DEIF A/S
- Jens Christian Lindof, RTX A/S
- Lars Finn Sloth Larsen, Danfoss
- Michael Bondo Andersen, Gatehouse Holding A/S
- Ole Kjeldsen, Microsoft Danmark & Island
- Pernille Iversen, Center for Cybersikkerhed
- Rune Domsten, Indesmatech ApS
- Tobias Piechowiak, Jabra

Virksomheder og personer, som Epinion har interviewet (baseret på vores bruttoliste):

Microsoft	Ole Kjeldsen	olek@microsoft.com
Bankdata	Michael Lind Mortensen	mim@bankdata.dk
EY	Mille Østerlund	milleoesterlund@gmail.com
Rådet for Digital Sikkerhed	Henning Mortensen	henning.mortensen@digitalsikkerhed.dk
CSIS Security Group	Jan Kaastrup	jka@csis.com

Force Technology	Christian Kloch	ckl@forcetechnology.com
NNIT	Nicholas Karlsen	nhka@nnit.com
Terma	Samant Khajuria	sakh@terma.com
SektorCERT (tidligere Energi-CERT)	Søren Maigaard	soren@Energicert.dk

Der er gennemført en webbaseret spørgeskemaundersøgelse blandt 118 virksomheder.

Derudover er der gennemført 8 kvalitative dybdeinterviews med potentielle aftagervirksomheder af konsulenter i Epinion.

Bilag 3: Referat af møde med aftagerpanel, Institut for Elektroniske Systemer

Dato: 30. oktober 2023, 9-13

Deltagere:

Eksterne medlemmer af aftagerpanelet: Claus Siggaard Andersen, Telenor A/S; Jakob Birk Filsø, Turf Tank; Jan Harding Gliemann, DEIF A/S; Jens Christian Lindof, RTX A/S; Lars Finn Sloth Larsen, Danfoss; Michael Bondo Andersen, Gatehouse Holding A/S; Ole Kjeldsen, Microsoft Danmark & Island; Pernille Iversen, Center for Cybersikkerhed; Rune Domsten, Indesmatech ApS; Tobias Piechowiak, Jabra;

Fra AAU, Institut for Elektroniske Systemer: Mads Græsbøll Christensen, institutleder; Ove Andersen, studieleder, viceinstitutleder; Tatiana K. Madsen, studienævnsforperson, Studienævn for Elektronik og IT; Reza Tadayoni, sektionsleder, CMI; Sokol Kosta, lektor, CMI.

Referenter: Charlotte Høeg og Mette Billeskov, Institut for Elektroniske Systemer.

Dagsorden

5. Drøftelse af forslag til nye uddannelser:
   a. Diplomingeniør i cybersikkerhed (Kbh.) v/ Reza Tadayoni

Reza Tadayoni, sektionsleder for instituttets sektion 'Communication, Media and Information Technologies' (CMI) i København præsenterede baggrunden for den nye diplomingeniøruddannelse i cybersikkerhed i København (jf. Rezas slides). Reza er medlem af uddannelsens udviklingsgruppe. Formand for gruppen, professor Jens Myrup Pedersen, kommer til at stå i spidsen for uddannelsen, der forskningsmæssigt vil blive understøttet af CMI-sektionen, hvis fagligheder sikrer, at undervisningen kan foregå forskningsbaseret og i tæt forbindelse med erhvervsliv og organisationer.

Baggrunden for uddannelsen er, at der i fremtiden vil være et stort behov for ingeniører med kompetencer inden for cybersikkerhed. Bl.a. vurderer DI, at der i Danmark i 2030 vil mangle mellem 15.000-20.000 fagfolk inden for cyber- og informationssikkerhed. Endvidere er et af målene i regeringens "National strategi for cyber- og informationssikkerhed" at imødekomme efterspørgslen på cyber- og informationssikkerhedskompetencer ved at uddanne flere specialister og opbygge stærkere kapacitet på tværs af samfundet. Der er for øjeblikket ikke et tilstrækkeligt antal uddannelser på bachelor/diplomniveau i Danmark inden for området, og der må hvert år afvises kvalificerede ansøgere.

Diplomingeniøruddannelsen vil være praksisnær og indeholde en stor grad af samarbejde med virksomheder. Uddannelsen vil blive udbudt på dansk og have en varighed på 3,5 år (7 semestre). Uddannelsen er opbygget således, at der på 1.-5. semester på hvert semester vil være kurser for 15 ECTS og projektarbejde for 15 ECTS. På 6. semester vil de studerende være i praktik for 30 ECTS, og på 7. semester skrives bachelorprojekt på 25 ECTS og tages kursus på 5 ECTS.

Uddannelsen vil give kompetencer inden for vigtige områder som:

- Netværks-, IoT- og cloud-sikkerhed
- Design af sikre systemer
- Sikker softwareudvikling
- Relevante ISO-standarder
- Risikovurdering
- Kritisk infrastruktur
- IT security regulation og GDPR, herunder sikker håndtering af persondata
- Privacy Engineering

På baggrund af præsentationen blev aftagerrepræsentanterne bedt om input ift., om man finder uddannelsen interessant og relevant, og der fremkom følgende kommentarer:

Rune spurgte til, om ressourcebegrænsning er tænkt ind ift. de lavenergi/ressourcesvage systemer i industrien, der ikke kan have ekstra latency og således ikke kan køre, hvis der inkluderes ressourcekrævende sikkerhedsrutiner. Reza takkede for den gode kommentar og oplyste, at studerende bl.a. vil arbejde med problemstillingen i forbindelse med IoT og distribuerede systemer.

Lars kommenterede, at han var enig i Runes betragtninger. Danfoss kigger også ind i controllere, som kommunikerer indbyrdes. I disse systemer er det vigtigt, at der i systemarkitekturen er taget højde for sikkerhed. Der er behov for medarbejdere på dette område. Det vil også være godt at få lovgivning og regulering på området med. Også denne relevante kommentar takkede Reza for.

Jan erklærede sig enig i det fremførte og nævnte også 'cyber security levels'. Der er givne niveauer, der vil ændre sig over tid, så man vil skulle være på forkant. Ville man måske kunne færdiggøre uddannelsen med en form for certificering og være aktør i den sammenhæng, så man kan være med til at etablere systemer, når det nu er en mere praktisk orienteret uddannelse?

Michael pointerede, at overblik over standarder, certificering, lovgivning og regulering er vigtig og bør fremgå af curriculum.

Jens Christian Lindof gav udtryk for at være enig og nævnte, at han gik ud fra, at uddannelsen også kommer omkring kvantesikre systemer, da der sandsynligvis vil være flere kvantecomputere, når studerende er færdige. Kvantesikre systemer vil også være et 'buzzword' ift. at tiltrække studerende. Til dette nævnte Ove, at instituttet for første gang i indeværende semester kører et kursus på nogle kandidatuddannelser inden for kvantecomputing, og at et sådant kursus måske også ville kunne inkluderes i denne uddannelse.

Reza kommenterede, at området også er under udvikling i forbindelse med nogle forskningsprojekter. Det skal overvejes, hvordan det kan inkluderes i uddannelsen, og det er en rigtig god kommentar, at det er vigtigt med viden om kvantesikkerhed, og at det vil være godt ift. rekruttering.

Pernille Iversen udtrykte stor begejstring for uddannelsen, og at man fra Center for Cybersikkerheds side er "all-in". Hun fremkom med følgende betragtninger:

- Vil uddannelsen indeholde forståelse for kryptering, som hun anser som et vigtigt element?
- Er der i studieordningen noget ift. beredskabsagendaen, så de studerende bliver klædt på ift. den?
- Peger kurset 'Machine learning og AI i cybersikkerhed' på 5. semester énvejs ift. anvendelse, eller omfatter det også, hvordan cybersikkerhed kan være en udfordring inden for machine learning og AI?
- Hvordan sikres det, at dimittenderne ikke kommer ud og er for "bløde" i projekterne ift. behovet? Pernille har haft en del studerende til jobsamtaler og har lagt mærke til, at de deler sig i to poler. Den ene del går den "bløde" kommunikationsvej og har måske "gemt sig" lidt i projektarbejdet og er ikke så nørdede. Den anden del er nørderne, som er dybt inde i de tekniske elementer i projekterne. Ove kommenterede, at det er velkendt, at der er faglige forskelle på studerende, og at ikke alle opnår samme dybe tekniske forståelse.

Ift. kvantecomputing nævnte Mads, at fagfælleudvikling også er hans ansvar som institutleder. Kvantecomputing er et nyt felt, vi er nødt til at udvikle os inden for. Instituttet rekrutterer i Kbh. på adjunktniveau, og vi er nødt til at opbygge de faglige kompetencer, så vi kan udbyde forskningsbaseret undervisning. Ift. de nye uddannelser vil der være en afvejning af, hvilket indhold der skal være på diplomuddannelsen, og hvilket der skal være på kandidatuddannelsen. Vi ser også, at vi har en mulighed inden for dette område, da vi er nogen af de første, der arbejder med dette.

Tobias foreslog måske at indarbejde krypteringsteknologier i diplomuddannelsen og give mulighed for, at man også kan tage den som en efter-videreuddannelse.

Ift. uddannelsesforløbet kommenterede Claus Siggaard Andersen, at det ser ud til først at blive sjovt på 5. semester, og han appellerede til at give uddannelsen lidt sjovere indhold fra starten for at tiltrække studerende, men at der ellers er fuld opbakning til uddannelsen fra hans side. Ove kommenterede, at det måske er en generel problematik på vores bacheloruddannelser, at det skal være spændende tidligt, og at det er læring, vi skal tage med – også på andre uddannelser.

Afslutningsvist konkluderede Ove, at der er opbakning fra alle til denne professionsrettede uddannelse inden for cybersikkerhed. Der var fra panelets side fremkommet gode input, som vi skal være opmærksomme på og vil tage med i det videre arbejde. Vi kan ikke love, at alle input kommer med i den endelige udgave. Vi afventer nu accept længere oppe i systemet, men forventer at høre nyt inden for de nærmeste måneder. I givet fald skal behovet undersøges nærmere, og aftagerpanelet vil modtage materiale til høring, når det foreligger.

Bilag 4: Referater fra møder med virksomheder, arrangeret af arbejdsgruppen:

Der er afholdt flg. møder med aftagere:

- 11. apr. 2024: Møde med PWC (Benjamin Vanggaard) og Dubex (Jim Bauer)
- 12. apr. 2024: Teams-møde med Arbit (Rasmus Borch)
- 7. maj 2024: Teams-møde med Maersk (Camilla Bonde)
- 23. maj 2024: Teams-møde med Novo Nordisk (Ingrid Colding-Jørgensen)

Møde med PWC og Dubex, d. 11. april 2024

Til stede: Henning Olesen, Lene Sørensen, AAU; Benjamin Vanggaard, PWC; Jim Bauer, Dubex

Henning Olesen starter med at forklare, hvorfor mødet afholdes og fortæller om at undersøge behovet for uddannelsen. Uddannelsen beskrives med kurser og projektmoduler, kompetenceprofil, og det gøres klart, hvad der er elementer i en diplomuddannelse i forhold til eksisterende bachelor- og kandidatuddannelser.

Det blev kommenteret fra aftagernes side, at de opfatter, at projekterne ofte tager mere tid studiemæssigt, og at man ikke skal undervurdere, hvor meget arbejde der ligger i dem.

Aftagerne var enige om, at markedet for potentielle man kan ansætte inden for området it-sikkerhed, er tømt. Folk skifter job og det er vanskeligt at rekruttere. Det er ikke kun i Danmark men et generelt problem. En uddannelse er dog ikke ensbetydende med at man kan få et særligt job. Det hænger sammen med, hvad it-sikkerhedsbranchen er interesseret i.

Aftagerne syntes, at det var vanskeligt at svare på, om disse diplomuddannede er nogle de gerne vil have, men nævner at de er sikre på, at der er behov for dem.

Der blev talt om at det er vigtigt på uddannelsen af have fundamentet i orden inden for programmering og matematik. Begge dele skal anvendes når der skal analyseres i virksomhederne. Man behøver ikke at være en super haj til det, men fundamentet skal være i orden. Begge aftagere sagde, at man ikke regner med, at nogen de ansætter, kan alting. Der skal investeres i oplæring mm. så derfor skal være meget fokus på, at ballasten er i orden, for den kan man ikke lige sådan lære.

De sagde begge, at der er brug for cyber-kompetencer. Denne uddannelse kan nok ikke selv give anledning til at lukke behovet for flere uddannede. Uddannelser med cyber kompetencer foregår andre steder også på DTU og professionshøjskolerne og top-up uddannelserne. Det er derfor meget vigtigt at denne uddannelse kan vise præcist, hvad der kommer ud af den. Det kunne være en tanke at samarbejde med certifikeringsvirksomheder. Der er mange SMV'er som vil have brug for disse kompetencer. Man skal have tydeligt fokus på hands-on på uddannelsen, da det vil være en stor fordel. De studerende skal kunne forstå teknologien inden noget som helst andet, og certificering kan hjælpe på forståelsen af teknologien (for eksempel CIS, COMSIA osv.).

Det blev bemærket, at det kunne være godt at tone uddannelsen på en måde. En måde var at øge linket til forretningsdelen, som allerede er hintet lidt i uddannelsen. Aftagerne syntes, at der er et teknisk ambitiøst niveau i uddannelsen, men ikke nødvendigvis at man kan snakke forretningssprog – og det er spørgsmålet, om det kunne være en vej.

Der blev nævnt, at risiko er centralt og at det kunne være godt at behandle i kurser og projekter.

Det blev understreget at det er vigtigt at de studerende har en god forståelse for netværk og programmering da, det er hvad der skal bygges videre på i virksomhederne. Hvis tingene er for teoretiske, kan studerende springe fra. Man skal kunne tilbyde noget, som er anderledes end KEA, DTU osv. og det skal man brande sig på.

Uddannelsen fremstår som fagligt ambitiøs på IT-sikkerhed.

Aftagerne blev herefter bedt om at se på kursus og projektsammensætningen på uddannelsen.

Aftagerne kunne ikke lide kursustitlen i web-programmering, da den reflekterede noget med web-side udvikling. De understregede, at det er nødvendigt og afgørende, at der er noget om programmering og databaser og de forslog den titel i stedet. De sagde, at hvis man arbejder med IT-sikkerhed så skal man lære mange programmeringssprog og de ting kan man ikke altid bruge tid på at lære de studerende når de ansættes.

Det blev foreslået, at studerende i projekter eller kurser kunne kikke på eksisterende værktøjer og så forsøge at ændre dem. De mente at det kunne være en god øvelse.

De var begge enige om, at kursus i Computerarkitektur og computersystemer absolut skal være på uddannelsen. De snakkede også om, at den skulle indeholde noget om cloud.

På uddannelsen kunne man også involvere direkte virksomheder, som sikkerhedsleverandører og de kunne vise hvad de havde fundet osv. De studerende kunne grave i logs og forsøge at forstå, hvad systemerne har gjort. Det vil hjælpe IT-afdelingen virkeligt meget. Der blev spurgt hvor det kunne ligge på uddannelsen.

Henning spurgte, hvor de største problemer ligger.
Der blev svaret, at der var flere. Der blev spurgt om, hvorfor etisk hacking skal fylde så meget? Det er interessant men der er mange andre emner, som for eksempel den offensive og defensive del i stedet. Der skal jo ikke uddannes en hacker.
Hvis der skal være noget om hacking anbefales kurset at det bliver lagt til allersidst (6. semester) efter de studerende har lært om systemerne. Så kan man sætte et red og blue team op, lave øvelsesscenarier, hacke og rapportere om det. Nogen unge tror, at de skal være hackere, men man er nødt til at have det faglige element rigtigt.

Aftagerne håbede også, at de studerende ville have et vist kendskab til ISO, NIST, CIS osv. Det er der brug for i virksomhederne. Det skal dog nok først komme lidt senere på uddannelsen.

Det blev nævnt, at kurset i Governance/compliance er på uddannelsen og det var aftagerne enige i skulle være. De nævnte at det er vigtigt at lære om ISO 27000 og det skal være i uddannelsen. Hvor det ligger, er det ok. ISO 27000 er vigtig.

Aftagerne forstod ikke kursusmodulet i sikkerhed og brugeradfærd. De syntes, at det blev for lavpraktisk og er et emne skal orienteres om på et andet kursus (man skal vide noget om det, men det skal ikke være centralt eller fylde så meget).

I stedet blev det foreslået, at der skal være et kursus i risikohåndtering og at man kan kikke på risk management og compliance/governance på det 4. semester. Efter lidt tid blev man dog mere enig om, at kursus skulle hedde noget med risikostyring, så det modsvarer det engelske udtryk risk management.

Det projekt på 4. semester (valgfri projekt) (som var knyttet til brugeradfærd) skal handle mere om teknisk incidence response med logs, og der kunne i projektet arbejdes konkret med logfiler fra en virksomhed.

Begge aftagere ser uddannelsen som en god mulighed for at sparre med erhvervslivet med praktiske cases. De er begge interesserede i at være gæsteforelæsere osv.

De foreslog også, at etisk hacking ville være mere relevant efter 4. semester, og at det måske skal kaldes red team/blue team hacking i stedet.

Det blev diskuteret om, der var nok fokus på cloud generelt. Og det blev nævnt, at det perspektiv og den læring burde ligge i netværk og arkitekturkurset. Og måske det skulle hedde netværk og cloud i stedet.

Aftagerne syntes også, at Machine Learning ikke behøvede at blive nævnt eksplicit som kursustitel på den måde. I stedet blev det foreslået, at det kunne hedde emerging technologies, og dermed også indeholde andre typer af centrale teknologier. I den forbindelse blev det diskuteret, at i mange virksomheder kunne man endnu ikke direkte anvende ML, men analyser vil ske mere gennem programmering. Specielt når der tales om fortrolige ting, der ikke skal være tilgængelige for andre. Kun meget robuste virksomheder anvender ML til det.

Det blev foreslået, at man kunne tale om kvanteteknologi, om hvor langt forskningen er og fremtidsperspektiverne, og det kunne være et emne under ”emerging technologies” kurset.

Derudover blev det også nævnt, at når de studerende er blevet gode til at programmere så lad dem kende OWASP programmering for at de kan gennemgå kode på en sikker måde.

Henning spurgte, om virksomhederne ville være interesserede i at tage imod praktikanter. Begge aftagere svarede at det ville være vanskeligt og udfordrende, da man bruger tid på oplæring, og man ikke kan være sikker på at få det retur bagefter.

Det blev foreslået at indgå i samarbejde med SMV’er, idet de fleste store virksomheder har en lang onboarding proces, og man synes, at det skal være personer man kan investere i. Aftagerne synes heller ikke,,at det er tydeligt at der skulle være brug for praktik, med projektarbejdet og fast samarbejde med for eksempel virksomheder eller Dansk Industri eller Digitaliseringstyrelsen. De nævnte også, at forsvaret kunne have gavn af et samarbejde.

Aftagerne syntes, at uddannelsen er interessant fra et rekrutteringsperspektiv. De nævnte, at de hellere ville have en færdig uddannet studerende end en i praktik, da ingen uddannelse kan uddanne studerende som er helt præcist tilpassede til virksomhederne. De sagde, at studenterjobs er vigtige og at man gennem studenterjobs kan opnå samme erfaring og bedre erfaring end praktikken.

Man foreslog at kikke på virksomheden Systematic, der skaber ting, måske den kunne være vigtig for samarbejde.

Til sidst blev det nævnt, at aftagerne syntes, at det er essentielt, at der kommer flere kvinder på uddannelsen. Derfor skal man tænke grundigt over titlerne på kurser og projekter og hvordan man brander en sådan uddannelse.

Det blev også nævnt, at man kunne lave officielt samarbejde med Cyber4women organisationen.

Kort møde med Rasmus Borch, Arbit CDS, d. 12. april 2024 (Teams)

Deltagere: Henning Olesen, AAU; Rasmus Borch, Arbit CDS

Rasmus fortalte om, hvad virksomheden arbejder med, især produktudvikling. De betragter sig som en nichevirksomhed. Netværkssikkerhed er et vigtigt område. Arbit arbejder med Air gap løsninger, bl.a. nationale løsninger og trusler. Han understregede, at der er forskellige behov hos forskellige virksomheder, forskellige løsninger. Det kan være godt at skitsere forskellige profiler for uddannelsen.

Rasmus havde flg. bemærkninger til uddannelsen:

- Studerende bør lære om risikovurderinger, arbejde med defense in depth på nogle systemer og kunne tænke kontekstafhængigt.
- Rasmus understregede også værdien af certificeringer. Studerende kunne f.eks. lave noget og lade andre grupper teste det, Common Criteria, hw og sw, også NIS2, - det giver værdi!
- Overordnet om uddannelsen: Det ser fantastisk godt ud!
- Har haft en praktikant fra DTU. Det er vigtigt at praktikanter kommer fra et universitet.
- SW-udvikling er meget vigtigt for Arbit. Civ.ing. bør have en baggrund inden for dette.
- "Dem skal vi bare have flere af"!
- AI er vigtigt!
- Gode muligheder inden for politi og forsvar, men der kræves sikkerhedsgodkendelse.

Møde med Camilla Wilde Bonde (Maersk), d. 7. maj 2024 (Teams)

Deltagere fra AAU: Lene Sørensen, Reza Tadayoni, Edlira Dushku
Minutes: Charlotte Hoegh

There was a short Introduction to the participants and to the two existing educations within cyber security.

Intro to diploma education. It is an education of 3,5 year. In the education the students must spend 6 months within a company (with salary) at the 6. Semester and do their BA project at the 7. Semester. After that they are ready to go directly to a company or continue at a master.
Half of our education is projects – which give the students a possibility for a lot of practical experience.

Lene and Reza introduced the scheme as it looks now and asked Camilla, what her opinion was and if she would hire one of these students?

Camilla: It is a good profile – it is actually very good. We need some people with these skills – we have a whole new scene of new regulations. We are missing cross discipline-oriented staff, we have a lot of people who works in silos, and we need someone who can do it in a more holistic way/problems based. Camilla asked about the prevention part, what are the requirements from a data protection point of view, risk-based view. Do we have that in the education? If our department only have few resources, it is only high risk problems/threats that will be fixed – if we have more resources we can go deeper.

Risk management is very important – it should play a bigger role. It is something we all use/know of. It should not be an elective course. Other companies are hiring risk management personal – but these people also need to know of Cyber Security and privacy. That is what we are missing. Risk assessment is the most important right now, together with the other competences: AI act, risk assessment and off course GDPR.

I work closely with our cyber security team – what is lacking here is the ability to run muck exercises, where we can practice/simulate attacks. There are a lot of external consultants who are doing this, and they are super expensive. It would be great if we could learn these students to run these exercises.

We also have people in 3. parties' engagement. The students need to know about this subject as well. We have 70000 3. parties in Maersk. We are doing assessment on many of these. If we have a weak 3. parti it will hit Maersk hard. All your communication is run by a vender – they should run these vender audits/due dilligence.

Edlira: Good idea to put it as a model, difficult to have an entire course about this.

Camilla: Even though it is an education for engineering, they should know something about laws/regulations. For example, all the new laws for China, they have a large impact on our company. If you have critical information structure, you have to fulfill a lot of security requirements. It could be good to have an introduction to this.

Reza: Simulation of attacks – is this a part of ethical hacking – could this be included here?

Camilla: The risk management oversee this simulation. You gather all the state holders for this arrangement/cyber-attacks and decide what to do and make a plan B. It is a super good idea to run this – but I don't know who you could contact. We did this in Carlsberg.
Lene: Should we get rid of "Brugeradfærd"?

Camilla: No, it is also just as important /security in your organization. More than 50% of mistakes happens inside the company. So, it is still very important. Access management and access control and the governance set up, could be a part of the legal course.

What we do – we have developed a process for all new stuff. It could be a questionnaire, where we ask questions to staff in the beginning. If we don't have this, it could have huge consequences for the companies - it is hugely important. With all this data flowing (big data) – it is important that people know that there are different kinds of data and it is a huge risk if you don't put access control on it. It becomes super important if you want to use AI.

Lene: What do you think about the 7. semester with 2 elective courses?

Camilla: It is a good choice to do that. But I think that Machine Learning and AI should be on the 1. And/or the 2. Semester, we need the students to know this early on. We have 25 AI systems in use and we need to have people who can operate this.

Lene/Reza: They need to have some basic knowledge of mathematics etc. before they have courses in Machine Learning and AI, but we will make sure that they know this before they go to internship.

Camilla: If someone comes with this profile, you show here, I will hire him/her.

Møde med Ingrid Colding-Jørgensen (CISO, Novo Nordisk), d. 23. maj 2024 (Teams)

Deltager fra AAU: Lene Sørensen

På mødet blev baggrunden for uddannelsen gennemgået, hvorefter vi snakkede om det draft udkast til uddannelsen, som hun forinden havde haft mulighed til at kikke på.

Umiddelbart blev der peget på et par elementer, som hun syntes springer i øjnene:

- Uddannelsen ser ud til at ville for meget. Anbefalingen er at have fokus på om den er teknisk, governance fokuseret eller det leder videre til en it-sikkerhedsleder. Som dele af den fremstår, så synes den mere teknisk og det skal nok understreges mere. Der er brug for alle kompetencerne uanset om teknisk, governance eller it-sikkerhed.
- Privacy og Etik som kursus virker som om det ikke passer ind. Det er her specielt etik-delen som ikke giver mening
- Cybersikkerheds Awareness og Behaviour - er noget som virksomhederne selv kan lære sine ansatte. Det skal ikke være en del af uddannelsen, som ellers er teknisk.
- Virksomhederne kan selv uddanne dem i governance perspektiver, hvis det alligevel skal være på det her mindre niveau. Uddannelsen ser nemlig ellers ekstremt teknisk ud. Der er ingen grund til at gå ind på ITU/CBS områder med det.
- Risk Management er en måde at tænke på. Man skal her fokusere på sandsynligheder og konsekvenser og lære ikke at gå i panik, men sikre at de rigtige løsninger findes. Det er supervigtigt og særdeles mandatory som kursus.
- For mig er matematik ikke så vigtig.
- Andre udfordringer er cybersikkerhed i forbindelse med supply chains, og integrationer af API'er osv (interaktioner).
- Et kursus, der kunne være relevant kunne være noget med signaler og monitorering (automatisk), hvor man skal sætte det op og man skal kunne spore hvorfor alerts kommer og dermed sikre et relevant respons.

Novo har allerede en del studerende som intern. Hun mener ikke, at lønnen ville være afgørende, det er mere vigtigt hvorfor de studerende vil til Novo. De skal selv komme med en gennemarbejdet idé som de vil arbejde med. Novo har ikke ressourcer til at finde ud af det med dem, når de først er "inde". De studerende skal jo ind i de indre systemer og derfor skal der også foretages et baggrundstjek af de studerende inden de får lov.
En idé er måske at lave en workshop på uni, hvor de studerende kan identificere klare og tydelige læringsmål for deres praktik, så det er praktikklare. Det er helt essentielt.

Det blev aftalt, at man eventuelt senere i processen kan kontakte Ingrid igen for yderligere kommentarer til en eventuel modificering af kursus- og projektmoduler.

Bilag 5: Høringsbrev og -svar fra KEA

AALBORG UNIVERSITET

Aalborg Universitet
Fredrik Bajers Vej 7K
Postboks 159
9220 Aalborg Øst

Dato: 18.06.2024
Sagsnr.: 2023-043-00323

Høring ifm. prækvalifikation af ny diplomingeniøruddannelse i cybersikkerhed på AAU
Aalborg Universitet sender i efteråret 2024 ansøgning til Uddannelses- og Forskningsministeriet mhp. prækvalifikation af en ny diplomingeniøruddannelse i cybersikkerhed. Første optag forventes september 2025. Uddannelsen forankres på Institut for Elektroniske Systemer, Det Tekniske Fakultet for IT og Design.

Som en del af processen foretages en høring blandt universiteter med sammenlignelige fagligheder for bl.a. at sikre at vilkårene for eksisterende uddannelser ikke forringes (fx hvis der udbydes sammenlignelige uddannelser inden for umiddelbar nærhed). Indeværende uddannelse udbydes på AAUs campus i København. AAU vurderer ikke, at uddannelsen forringer vilkårene for eksisterende udbud, men adresserer den stigende efterspørgsel efter kompetencer inden for IT-branchen.

At der er behov for kompetenceopbygning inden for IT-sikkerhed, understreges af regeringens "National strategi for cyber- og informationssikkerhed". Ved sin udgivelse i 2021 fremsatte denne bl.a. et mål om at: "Efterspørgslen på cyber- og informationssikkerhedskompetencer skal imødekommes ved at uddanne flere specialister og opbygge stærkere kapacitet på tværs af samfundet". Dette behov støttes af tal fra DI, som vurderer at der i 2023 vil mangle mellem 15.000-20.000 fagfolk på området. Samtidig anslog ISC* i 2022, at der mangler 3,4 millioner IT Security Professionals på verdensplan. Formålet med denne uddannelse er således at adressere samfundsudviklingen ved at bidrage til uddannelse inden for IT-sikkerhedsområdet.

Uddannelsens indhold og tilrettelæggelse
Diplomingeniør i cybersikkerhed vil være en praksisnær uddannelse, hvor de studerende vil opleve et tæt samarbejde med virksomheder og organisationer.

Det overordnede mål med uddannelsen er, at de studerende opnår forståelse for de problemstillinger, som virksomheder, rådgivende ingeniører, serviceinstitutter og forskningsinstitutioner møder i forbindelse med cybersikkerhed, samt at de bliver i stand til at omsætte denne viden i professionel praksis.

De studerende opnår kompetencer til selvstændigt at varetage udviklings-, analyse-, og serviceopgaver i både private og offentlige virksomheder. Derudover forberedes den studerende på en erhvervsfunktion, der fordrer kommunikation og samarbejde med andre faggrupper om sådanne problemstillinger og opgaver.

Uddannelsen vil give kompetencer inden for vigtige anvendelsesområder som netværks-, IoT- og cloud-sikkerhed, design af sikre systemer, sikker softwareudvikling, relevante ISO-standarder m.m., risikovurdering, kritisk infrastruktur, IT security regulation og GDPR, sikker håndtering af persondata og privacy engineering.

Uddannelsen i cybersikkerhed er tilrettelagt som et problemorienteret studium, og der undervises og vejledes efter Aalborg Universitets metode for problembaseret læring gennem en kombination af projektarbejde og understøttende kurser.

Ved yderligere spørgsmål om uddannelsen kontakt viceinstitutleder og studieleder Ove Andersen: oa@es.aau.dk

Vi vil gerne anmode om at modtage eventuelle høringssvar senest den 5. juli 2024.

Med venlig hilsen
Louise Møller Haase
Prodekan for uddannelse, Det Tekniske Fakultet for IT og Design, AAU

* The International Information System Security Certification Consortium

Aalborg Universitet
Fredrik Bajers Vej 7K
Postboks 159
9220 Aalborg Øst

KEA DIGITAL

GULDBERGSGADE 29 N
2200 KØBENHAVN N

TEL +45 46 46 00 00
FAX +45 46 46 00 99

CVR: 31656206
EAN: 5798 000 560291

WWW.KEA.DK

8. august 2024

KEAs høringssvar vedr. prækvalifikation af ny diplom-ingeniøruddannelse i cybersikkerhed på AAU

Københavns Erhvervsakademi (KEA) er enige med AAU i ønsket om at vi i Danmarks skal uddanne flere med kompetencer indenfor IT- og cybersikkerhed.
Derfor vil KEA principielt gerne støtte AAUs ønske om at oprette en diplomuddannelse i cybersikkerhed.

KEA udbyder allerede en praksisorienteret uddannelse på IT sikkerhedsområdet i København, professionsbachelor i IT-Sikkerhed (top-up)[1], som er placeret i samme kvalifikationsramme (niveau 6) som den diplomingeniør som AAU søger. Uddannelsen har optag to gange årligt.

KEA vil samtidig med AAU's ansøgning i september 2024 søge om at få det eksisterende udbud i IT-Sikkerhed udvidet til en fuld PBA. Et udbud som der er stor efterspørgsel efter blandt KEAs samarbejdspartnere i erhvervslivet. KEA vil i sin prækvalifikationsansøgning for den fulde PBA i IT-Sikkerhed, bl.a. lægge vægt på uddannelsens praksisnærhed, erhvervsopkobling og sammenhæng til andre dele af uddannelsessektoren på alle niveauer jf. de politiske ønsker om åbne døre i uddannelsessektoren.

Erhvervsakademiernes udbud er landsdækkende, så hvis KEAs ansøgning bliver godkendt kan udbuddet søges af alle landets erhvervsakademier til udbud i deres geografiske dækningsområde. De enkelte udbud kan tilrettes lokale forhold med lokale fagelementer og valgfag i studieordningen, således at mindre og mellemstore virksomheder i hele landet, kan ansætte lokalt uddannede IT-medarbejder med IT-sikkerhedskompetencer.

I lyset af KEAs allerede eksisterende udbud på PBA-niveau i København og KEA's planer herfor mener KEA, at et nyt udbud af diplomingeniør i cybersikkerhed fra AAU i København kan risikere at forringe vilkårene for KEAs udbud. Såfremt AAU får godkendt og etablerer det foreslåede udbud, vil KEA gerne invitere til et samarbejde

[1] Se https://kea.dk/uddannelser/top-up/it-sikkerhed for yderligere oplysninger om KEAs uddannelse og på Uddannelsesguiden for overblik over de fire andre steder i landet, hvor uddannelsen udbydes. KEA udbyder derudover en diplomuddannelse (Åben Uddannelse) i it-sikkerhed, se https://kompetence.kea.dk/uddannelser/it/diplom-i-it-sikkerhed

om de to udbud, så der fx ikke opstår uhensigtsmæssig konkurrence.

KEA er – i modsætning til AAU – geografisk begrænset til at udbyde uddannelser i Region Hovedstaden, og en placering af AAUs planlagte udbud væk fra de eksisterende lignende udbud, vil give flere virksomheder og studerende geografisk nærhed til tilbud om en it-sikkerhedsuddannelse.

Uafhængigt at de aktuelle planer om udbud, foreslår KEA et samarbejde med AAU om at give adgang for professionsbachelorer i IT-Sikkerhed fra erhvervsakademierne adgang til AAUs kandidatuddannelse i Cyber Security, hvor der i dag i adgangskravene, er en generel henvisning til at studerende med en professionsbachelor ikke kan optages. Cyber Security - Aalborg Universitet (aau.dk)

KEA fremsender høringsbrev til AAU m.fl. om de ønskede ændringer til PBA i IT-Sikkerhed (top-up) inden ansøgning til ministeriet medio september.

KEA ser frem til et fortsat godt og om muligt tættere samarbejde om uddannelser med AAU inden for cybersikkerhed mv.

Med venlig hilsen

Merete Hess
Uddannelseschef, KEA Digital
Københavns Erhvervsakademi (KEA)

Uddannelses- og Forskningsministeriet

Kære Per Michael Johansen

På baggrund af gennemført prækvalifikation af Aalborg Universitets ansøgning om godkendelse af ny uddannelse er der truffet følgende afgørelse:

Godkendelse af ny diplomingeniøruddannelse i cybersikkerhed (København)

Afgørelsen er truffet i medfør af § 20, stk. 1, i bekendtgørelse om akkreditering af videregående uddannelsesinstitutioner og godkendelse af videregående uddannelser (nr. 1558 af 2. juli 2021 med senere ændringer), og § 3, stk. 3, i bekendtgørelse nr. 271 af 22. marts 2014 om særlige betingelser for godkendelse af udbud af erhvervsakademiuddannelser, professionsbacheloruddannelser, akademiuddannelser og diplomuddannelser.

Da Aalborg Universitet er positivt institutionsakkrediteret, gives godkendelsen til umiddelbar oprettelse af uddannelsen.

Ansøgningen er blevet vurderet af det rådgivende udvalg for vurdering af udbud af videregående uddannelser (RUVU). Vurderingen er vedlagt som bilag.

Vedlagt i bilag er desuden uddannelsens grundoplysninger. Ved spørgsmål til afgørelsen eller de vedlagte grundoplysninger kan Uddannelses- og Forskningsstyrelsen kontaktes på pkf@ufm.dk.

Med venlig hilsen

Christina Egelund

Bilag: 1 – RUVU's vurdering af ansøgningen
2 – Følgebrev fra Uddannelses- og Forskningsstyrelsen med uddannelsens grundoplysninger

3. december 2024

Uddannelses- og Forskningsministeriet

Bredgade 40-42
1260 København K

Tel. 3392 9700
ufm@ufm.dk
www.ufm.dk

CVR-nr. 1680 5408

Ref.-nr.
2024 - 52808

Bilag 1 – RUVU's vurdering af ansøgningen

Nr. A14– ny uddannelse (Efterår 2024)			**Status på ansøgningen:** Godkendt	
Ansøger og udbudssted:	Aalborg Universitet (København)			
Uddannelsestype:	Professionsbacheloruddannelse			
Uddannelsens navn (fagbetegnelse) på hhv. dansk/engelsk:	- Cybersikkerhed - Cyber Security			
Titel, som uddannelsen giver ret til at anvende:	- Diplomingeniør i cybersikkerhed - Bachelor of Engineering in Cyber Security			
Hovedområde:	Tekniske område		**Genansøgning:**	Nej
Sprog:	Dansk	**Antal ECTS:**	210 ECTS	
Link til ansøgning på pkf.ufm.dk:	https://pkf.ufm.dk/flows/aadb35d3332d543ee0388658815feddd			
RUVU's vurdering på møde d. 1. november 2024	RUVU vurderer, at ansøgningen opfylder kriterierne som fastsat i bilag 4 i bekendtgørelse om akkreditering af videregående uddannelsesinstitutioner og godkendelse af videregående uddannelser (nr. 1558 af 2. juli 2021 med senere ændringer). RUVU noterer sig, at ansøgningen dokumenterer et behov for dimittender med stærke ingeniørfaglige kompetencer inden for cybersikkerhed. Herunder påvises både et behov for specifikke tekniske kompetencer inden for cybersikkerhed i bl.a. it-virksomheder og et mere generelt behov for kompetencer inden for cybersikkerhed på tværs af virksomhedsstørrelse og brancher. RUVU vurderer, at uddannelsen med sine adgangskrav og sit fokus på avancerede tekniske fag vil tiltrække en anden målgruppe af studerende, og at uddannelsen er målrettet et andet arbejdsfelt end den anden ansøgte professionsbachelor i cybersikkerhed fra bl.a. Københavns Erhvervsakademi.			

Bilag 2 – Følgebrev fra Uddannelses- og Forskningsstyrelsen med uddannelsens grundoplysninger

Diplomingeniør i cybersikkerhed
Bachelor of Engineering in Cyber Security

Hovedområde:
Tekniske område

Titel:
Efter reglerne i § 3 i bekendtgørelse nr. 2674 af 28. december 2021 om Bekendtgørelse om uddannelserne til professionsbachelor som diplomingeniør (diplomingeniørbekendtgørelsen), giver uddannelsen ret til at anvende titlen:

- **Dansk:** Diplomingeniør i cybersikkerhed
- **Engelsk:** Bachelor of Engineering in Cyber Security

Udbudssted:
København.

Sprog:
Dansk.

Normeret studietid:
Efter reglerne i diplomingeniørbekendtgørelsens § 2, stk. 1, fastlægges uddannelsens normering til 210 ECTS-point.

Takstindplacering:
Uddannelsen indplaceres til: Heltidstakst 3
Aktivitetsgruppekode: 4052

Koder Danmarks Statistik:
UDD: 5930
AUDD: 5930

Censorkorps
Ministeriet har noteret sig, at uddannelsen tilknyttes Diplomingeniør-uddannelsernes censorkorps.

Adgangskrav:
Efter det oplyste kan der jf. § 4 i bekendtgørelse nr. 56 af 10. januar 2024 om adgang til erhvervsakademiuddannelser og professionsbacheloruddannelser (adgangsbekendtgørelsen) opnås adgang til uddannelsen via følgende:

Gymnasial adgang:
Specifikke adgangskrav:
- Matematik A,
- Engelsk B, og
- enten fysik B eller geovidenskab A

Anden adgang:

- Adgangseksamen til ingeniøruddannelserne
- *Ingen specifikke adgangskrav*

Eventuelle øvrige lokale adgangskrav, som for eksempel karakterkrav eller regler om adgangsprøver fastsættes i forbindelse med klargørelse af udbuddet på optagelsesportalen www.optagelse.dk.