Uddannelses- og Forskningsministeriet

Prækvalifikation af videregående uddannelser - cybersikkerhed

Udskrevet 22. december 2024

Kandidat - cybersikkerhed - Aalborg Universitet

Institutionsnavn: Aalborg Universitet
Indsendt: 16/09-2019 08:43
Ansøgningsrunde: 2019-2
Status på ansøgning: Godkendt
Afgørelsesbilag
Download den samlede ansøgning
Læs hele ansøgningen

Ansøgningstype
Ny uddannelse

Udbudssted
København

Kontaktperson for ansøgningen på uddannelsesinstitutionen
Sebastian Bue Rakov Chefkonsulent | Strategi og Kvalitet | Studieservice Tlf.: 9940 9681 Mail: sbr@adm.aau.dk

Er institutionen institutionsakkrediteret?
Ja

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

Uddannelsestype
Kandidat

Uddannelsens fagbetegnelse på dansk fx. kemi
cybersikkerhed

Uddannelsens fagbetegnelse på engelsk fx. chemistry
Cyber Security

Den uddannedes titel på dansk
Civilingeniør, cand.polyt. i cybersikkerhed

Den uddannedes titel på engelsk
Master of Science (MSc) in Engineering (Cyber Security)

Hvilket hovedområde hører uddannelsen under?

Teknisk videnskab

Hvilke adgangskrav gælder til uddannelsen?

Der er ikke tilknyttet nogen bacheloruddannelser med retskrav til denne kandidatuddannelse.

Følgende bacheloruddannelser giver adgang til kandidatuddannelsen i cybersikkerhed (uden retskrav):

● AAU: Bachelor i IT, kommunikations- og medieteknologi, Bachelor i computerteknologi, Bachelor i elektronik og IT, Diplomingeniør i elektronik, Bachelor i datalogi, Bachelor i software, Bachelor i informationsteknologi

●DTU: Bachelor i elektroteknologi, Diplomingeniør i elektroteknologi, Bachelor i netværksteknologi og IT, Bachelor i softwareteknologi, Diplomingeniør i softwareteknologi.

- KU: Bachelor i datalogi
- ITU: Bachelor i softwareudvikling
- AU: Bachelor i datalogi, Bachelor i computerteknologi, Bachelor i elektronik
- SDU: Bachelor i electronics, Bachelor i software engineering, Bachelor i datalogi

Optagelse på kandidatuddannelsen i cybersikkerhed forudsætter engelsk på minimum B-niveau, da uddannelsen udbydes på engelsk.

Er det et internationalt uddannelsessamarbejde, herunder Erasmus, fællesuddannelse og lign.?

Nej

Hvis ja, hvilket samarbejde?

Hvilket sprog udbydes uddannelsen på?

Engelsk

Er uddannelsen primært baseret på e-læring?

Nej

ECTS-omfang

120

Beskrivelse af uddannelsens formål og erhvervssigte

Formålet med kandidatuddannelsen i cybersikkerhed er at give en dyb faglig indsigt i metoder og værktøjer inden for fagområdet. Uddannelsen tager udgangspunkt i tre centrale søjler: Sikkerhed i netværk og distribuerede systemer; udvikling, test og verifikation af sikker software samt en række centrale anvendelsesområder som IoT- og Cloud-sikkerhed, identity and access management, sikker håndtering af persondata, virksomheders IT- og service-arkitekturer og security governance.De uddannede kandidater får en stærk teknisk profil og en god forståelse for den kontekst, den tekniske faglighed indgår i. Gennem kurser og projektarbejde får de viden om væsentlige anvendelsesområder og erfaring med at omsætte den tekniske viden til udvikling af løsninger, f.eks. inden for analyse, design og implementering af sikre systemer og software, analyse og håndtering af cybertrusler og forebyggelse, detektion og mitigering af cyberangreb på forskellige typer af systemer. De kan også vælge at dygtiggøre sig inden for privacy engineering, adgangskontrol og håndtering af beskyttede ressourcer, IoT- og cloud-baserede systemer og arkitekturer og security governance.

De færdige kandidater ventes at bidrage til at imødegå den store efterspørgsel på kompetencer i cybersikkerhed i en verden, som i stadig stigende grad udsættes for cyberangreb. Alle virksomheder og organisationer har i dag et akut behov for at beskytte deres ressourcer, systemer og arkitekturer, overvåge trusselsbilledet og løbende iværksætte nye tiltag for at forebygge og mitigere cyberangreb. På samfundsplan vurderes trusselsniveauet som “meget højt” inden for områder som cyberspionage og cyberkriminalitet, og der er især fokus på kritisk infrastruktur og strategiske områder som sundheds-, energi-, finans-, tele-, søfarts- og transportsektorerne (se “Trusselsvurdering – Cybertruslen mod Danmark”, Center for Cybersikkerhed, marts 2019, https://fe-ddis.dk/cfcs/publikationer/Documents/Cybertruslen-mod-Danmark-2019.pdf)

En række bachelor- og kandidatuddannelser indeholder elementer af cybersikkerhed i form af enkeltkurser og fagprofiler, men de danske universiteter tilbyder for nærværende ikke nogen kandidatuddannelse, der har cybersikkerhed som det centrale omdrejningspunkt. Uden for AAU’s regi findes f.eks. en professionsbachelor i IT-sikkerhed på KEA og en kommende efteruddannelse i cybersikkerhed på DTU. Desuden tilbydes efteruddannelse i form af enkeltkurser på bl.a. Teknologisk Institut.

Fælles for disse uddannelser er, at de ikke har cybersikkerhed som det centrale emneområde, og at uddannelserne på erhvervsakademierne primært behandler cybersikkerhed på et operationelt niveau. Aftagervirksomhederne efterspørger i stigende grad medarbejdere, der ikke alene kan løse specifikke cybersikkerhedsproblemer, men som også er fortrolige med deres kontekst, f.eks. igennem forretningsforståelse, viden på tværs af de tekniske discipliner og viden om regulering (se Bilag 1, s. 8-9). Denne bredere kompetence kan kun opnås gennem en kandidatuddannelse, der har cybersikkerhed som det centrale omdrejningspunkt. Strukturen i kandidatuddannelsen i cybersikkerhed med fagkombinerende semesterprojekter muliggør opnåelse af kompetencer, der forbinder tekniske problemstillinger med kontekstuelle forretnings- og reguleringsmæssige problemstillinger. Den stærke forbindelse mellem faglig og kontekstuel viden er et kendetegn for AAUs problem-baserede læringsform.

Uddannelsens struktur og konstituerende faglige elementer

Uddannelsen er tilrettelagt som en sammenhængende uddannelse med en naturlig faglig progression, som kan gennemføres inden for den fastsatte tidsramme på 2 år. Uddannelsen består af 120 ECTS-point, der er fordelt på fire semestre med hver 30 ECTS-point. Hvert semester består af et projektmodul og på 1.-3. semester desuden af kursusmoduler. Uddannelsen har en faglig progression, der bevæger sig fra det specifikke mod det komplekse. De kontekstuelle elementer af cybersikkerhed bliver derfor mere markante i 3. semester, der tilbyder valg mellem to projektmoduler: ”Security governance” og ”Secure Systems Development”. På 4. semester udformer den studerende et kandidatspeciale under vejledning. Uddannelsens struktur tilbyder en række valgmuligheder, som gør det muligt for de studerende at specialisere sig i forskellige retninger. De fire semestre indeholder kurser og projekter, der samlet set bidrager til uddannelsens kompetenceprofil. Kursusmodulerne bidrager med viden, færdigheder og kompetencer for den studerende til at arbejde med metode og teori inden for et afgrænset fagområde, mens projektmodulerne vil sætte et tværfaglig fokus i en problemorienteret kontekst, hvor viden, færdigheder og kompetencer anvendes. Industrielt relevante problemstillinger vil udgøre grundlaget for projekterne, som vil blive udført i tæt samarbejde med både danske og internationale virksomheder. Dette bidrager til at sikre en tæt kobling mellem dimittendernes kompetencer og aftagernes behov samt til en glat overgang til beskæftigelse for dimittenderne.

SEMESTER 1:

Distributed systems security (Projektmodul 10 ECTS-point)

Projektmodulet sætter de studerende i stand til at løse en virkelighedsnær problemstilling relateret til sikkerhed i distribuerede systemer. Med udgangspunkt i PBL og videnskabelige metoder skal de studerende identificere og beskrive problemer fra den virkelige verden.

Network security (Kursusmodul 5 ECTS-point)

Kurset giver deltagerne en grundig introduktion til netværkssikkerhed, herunder både passive metoder til netværksovervågning og netværksanalyse samt aktive metoder som netværksscanning. Deltagerne opnår viden om netværksbaserede IT-sikkerhedstrusler, botnets og sikkerhedsprotokoller generelt.

Secure software development (Kursusmodul 5 ECTS-point)

Kurset gør det muligt at vurdere potentielle sikkerhedsrisici og sårbarheder i en typisk software-applikation, foretage en trusselsvurdering, opstille relevante sikkerhedsmål samt vurdere, anbefale og implementere relevante sikkerhedsmekanismer med henblik på at reducere antallet af sårbarheder.

Security in IoT and cloud architectures (Kursusmodul 5 ECTS-point)

I dette kursus lærer de studerende om de grundlæggende praktiske og teoretiske aspekter af sikkerhed i IoT-enheder og cloud-teknologier med fokus på de sikkerhedsmæssige aspekter. Kurset dækker også virtualiseringsteknologier, herunder i cloud-arkitekturer og deres sikkerhedskarakteristika.

Fundamentals of security and cryptography (Kursusmodul 5 ECTS-point)

I dette modul opnår de studerende fundamental viden om en række områder indenfor cybersikkerhed og kryptografi med henblik på at give de studerende et fælles udgangspunkt for de fortsatte studier. Kurset dækker områder indenfor netværkssikkerhed såvel som områder indenfor kryptografi.

SEMESTER 2:

Secure systems: Attack and defense (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 angriber" får de studerende en bedre forståelse for, hvordan systemer kan sikres mod angreb, og hvordan angreb detekteres. Det er muligt at arbejde på tværs af grupper, så én gruppe f.eks. angriber det system, som en anden gruppe beskytter.

Hacker space (Kursusmodul 5 ECTS-point)

Kurset giver deltagerne teoretisk viden om og praktisk erfaring med test og eksperimenter med såvel netværksbaserede angreb som malware. Det giver praktisk erfaring både fra angrebs- og forsvarsvinkler og tillader deltagerne at afprøve forskellige angrebs- og forsvarsstrategier i et sikkert og lukket testmiljø.

Advanced software security (Kursusmodul 5 ECTS-point)

Kurset giver deltagerne indsigt i og viden om et udvalg af avancerede "state-of-the-art" teorier, teknikker og værktøjer inden for software-sikkerhed, såsom statisk/dynamisk programanalyse, fuzzing, sprogbaseret sikkerhed, verificeret/certificeret programmering og andre formelle metoder samt den underliggende teori.

Machine learning (Kursusmodul 5 ECTS-point) (Valgfag)

De studerende opnår indsigt i de væsentligste aspekter af maskinlæring med henblik på at sætte dem i stand til at løse praktiske problemer. Samtidigt får de forståelse for den bagvedliggende teori, der gør dem i stand til at forstå styrker og muligheder samt antagelser, svagheder og begrænsninger.

Identity and access management (Kursusmodul 5 ECTS-point) (Valgfag)

I kurset lærer de studerende at forstå digitale identiteter og begreber som persondata, attributter, claims, assertions, credentials, privacy samt “privacy by design” og “privacy by default” (inkl. GDPR-principper). Endvidere fås en dyb forståelse af identifikation, autentifikation, autorisation og assurance levels.

SEMESTER 3:

På dette semester skal de studerende vælge mellem to projektmoduler: Security governance og Secure Systems Development og to af de følgende kurser: “Secure Systems Development”, “Privacy engineering”, “Sikkerhedsmodeller”, “IT security regulation” og “Enterprise security and compliance”. Kurset “Advanced topics of cyber security” er obligatorisk for alle.

Security governance (Projektmodul 15 ECTS-point) (Valgfag)

I dette projektmodul lærer de studerende om sammenhængen mellem tekniske, økonomiske, politisk-reguleringsmæssige og kulturelle aspekter af cybersikkerhedstrusler for enkeltpersoner, virksomheder, organisationer eller nationer.

Secure systems development (Projektmodul 15 ECTS-point) (Valgfag)

I dette projektmodul lærer de studerende at designe og udvikle et sikkert system baseret på en grundig analyse af trusler og risici. De studerende sættes desuden i stand til at teste og verificere sikkerheden af det system, der udvikles løbende gennem de forskellige udviklingsfaser.

Advanced topics of cyber security (Kursusmodul 5 ECTS-point)

Kurset giver de studerende viden om den nyeste forskning inden for cybersikkerhed. Det konkrete indhold opdateres løbende og inkluderer emner som detektion og omgåelse af sikkerhedsmekanismer, specialiserede angreb på protokoller og systemer og kollaborative forsvarsmekanismer.

Privacy engineering (Kursusmodul 5 ECTS-point) (Valgfag)

I kurset opnås en forståelse af privacy som koncept, og hvordan man som udvikler af software og systemer integrerer privacy i designprocessen. Disse løsninger bidrager til at sikre virksomheders brug af data og til at give kunder/brugere mulighed for at kontrollere hvilke data, som anvendes og gemmes.

Models of security (Kursusmodul 5 ECTS-point) (Valgfag)

Dette kursus giver den studerende en dybere indsigt i et udvalg af de formelle modeller og teorier, der udgør det teoretiske fundament for den formelle del af forskningen inden for IT-sikkerhed. De anvendes til formel certificering/validering af sikkerheden i de mest udsatte/sikkerhedskritiske systemer.

IT security regulation (Kursusmodul 5 ECTS-point) (Valgfag)

Formålet med kurset er at give de studerende et overblik over de lovgivningsmæssige og institutionelle rammer for cybersikkerhed og dens anvendelser. Kurset vil gennemgå relevant national og international regulering og lovgivning inden for området, herunder EU's direktiver og reguleringer.

Enterprise security and compliance (Kursusmodul 5 ECTS-point) (Valgfag)

Kurset bibringer de studerende en struktureret metode til identifikation og håndtering af risici i et større IT-systemlandskab, forslag til brug af sikkerhedsforanstaltninger og compliance-målinger. De vigtigste standarder relateret til compliance gennemgås, herunder specielt ISO 2700x.

SEMESTER 4:

Kandidatspeciale (Projektmodul 30 ECTS)

I det sidste semester udarbejder den studerende et speciale, der afspejler det højeste niveau af international viden inden for en problemstilling, som den studerende sammen med en vejleder har identificeret.

Valgmuligheder på 3. og 4. semester:

Der er endvidere mulighed at vælge et “Projektorienteret forløb i en virksomhed” på 25 ECTS på 3. semester, tage på udlandsophold på 3. semester eller afslutte med et langt kandidatspeciale på 45 eller 50 ECTS fordelt over 3. og 4. semester.

Begrundet forslag til taxameterindplacering

Takst 3: Den foreslåede uddannelse er en teknisk-videnskabelig civilingeniøruddannelse.

Forslag til censorkorps

Censorkorps for ingeniøruddannelserne og de tekniske diplomuddannelser (Elektronik, IT og Energi) og enkelte censorer fra censorkorpset for datalogi.

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

Dokumentationsrapport_KA_Cybersikkerhed_inkl.bilag.pdf

Kort redegørelse for det nationale og regionale behov for den nye uddannelse

Som det bl.a. konstateres i Finansministeriets rapport fra 2018, er truslen mod danske virksomheder og offentlige institutioner fra cyber-attacks stærkt stigende samtidig med, at implikationerne af angreb og nedbrud bliver større(se "Danish Cyber and Information Security Strategy", Finansministeriet, maj 2018, https://digst.dk/media/16943/danish_cyber_and_information_security_strategy_pdfa.pdf)

Den overordnede mangel på ingeniører, naturvidenskabelige kandidater og andre IKT-specialister fremgår af tre grundige analyser foretaget i de seneste år (se dokumentationsrapport). Undervisnings- og Forskningsministeriet har løbende udarbejdet udbudsfremskrivninger bl.a. til udvalget vedrørende kvalitet i uddannelsessystemet. DI og IDA har for Engineering the Future fremskrevet manglen på ingeniører og naturvidenskabelige kandidater. Endelig leverede en omfattende analyse af behovet for digitale kompetencer udarbejdet af Erhvervsstyrelsen, UFM og UVM detaljerede langfristede fremskrivninger for IKT-kandidater. Ifølge tal fra IDA og DI vil der i 2020 være en mangel på ingeniører og naturvidenskabelige kandidater på 7000 personer, mens antallet i 2025 forventes at stige til 10.000 personer (se dokumentationsrapport s.13).

Da cyberssikkerhedsproblematikken ikke begrænser sig til en dansk kontekst, er der også internationalt stor efterspørgsel på kvalificerede kandidater. Danske virksomheder kan derfor kun i begrænset omfang få dækket deres behov ved at rekruttere i udlandet, og danske universiteter er således nødt til at opruste på uddannelsesfronten i cybersikkerhed for at kunne dække arbejdsmarkedets behov. I 2018 gennemførte $(ISC)^2$ en undersøgelse blandt 1.500 respondenter i Nordamerika, Latinamerika, Asien-Stillehavsregionen og Europa og anslår på den baggrund, at der på globalt plan mangler 2,93 mio. cybersikkerhedseksperter – heraf 142.000 i Europa (se “Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens”, $(ISC)^2$ CYBERSECURITY WORKFORCE STUDY, 2018. https://www.isc2.org/Research/Workforce-Study). Respondenterne peger desuden på, at manglen på kvalificeret arbejdskraft er den væsentligste jobmæssige udfordring. 48% forventer, at deres organisation vil øge antallet af ansatte med fokus på cybersikkerhed i det kommende år, mens kun 5% forventes at reducere antallet.

Der findes som tidligere nævnt imidlertid ingen kandidatuddannelse i Danmark, der har cybersikkerhed som det centrale omdrejningspunkt. Kriterium 2 nedenfor indeholder en detaljeret beskrivelse af beslægtede uddannelser, og ledighedstal for beslægtede kandidatuddannelser er beskrevet i dokumentationsrapporten s. 14-15. Som det beskrives, findes der professionsbachelor- og efteruddannelser i IT- og cybersikkerhed, og en række kandidatuddannelser indeholder relevante kurser og studieforløb, men det er ikke i et omfang eller på et niveau, der opfylder behovet på arbejdsmarkedet. For de tekniske kandidatuddannelser, der indeholder elementer af cybersikkerhed, er ledigheden lav, men antallet af færdiguddannede kandidater er også relativt lavt. Eksempelvis har Datalogi på KU og AU i årene 2011-2016 uddannet hhv, mellem 38 og 63 kandidater pr. år og mellem 33 og 64 kandidater pr. år. ITUs Softwareudvikling har uddannet mellem 53 og 108 kandidater. Disse og lignende kandidatuddannelser betjener imidlertid et bredt behov for datalogisk arbejdskraft og fokuserer ikke specifikt på cybersikkerhed.

Kandidater med specialiserede tekniske kompetencer er efterspurgte, men mange virksomheder ønsker disse kompetencer forbundne med en forretnings- og organisationsforståelse. Der er brug for 'brede specialister' med en dyb teknisk faglighed kombineret med den fornødne helhedsforståelse af cybersikkerhed. AAUs aftagerdialog og den gennemførte behovsundersøgelse viser, at en sammenhængende kandidatuddannelse med cybersikkerhed som centralt tema er en forudsætning for imødekommelse af aftagernes stigende behov for ansatte med cybersikkerhedskompetencer, der forbinder operationelle lag med de system-, arkitektur- og forretningsrelaterede lag i cybersikkerhedsproblematikker. Den foreslåede kandidatuddannelse adresserer dette behov ved hjælp af AAUs problem-baserede læringstilgang.

På baggrund af nøje overvejelser har AAU valgt at ansøge om at udbyde uddannelsen på AAUs campus København. Dette er sket ud fra følgende hensyn:

- Mange væsentlige aftagervirksomheder og aktører er placeret i hovedstadsområdet. Det gælder eksempelvis myndigheder som rigspolitiet (NC3), forsvaret (Center for Cybersikkerhed) og store virksomheder/organisationer inden for kritiske sektorer som finans, tele og energi samt konsulentbranchen. Dette vil give gode muligheder for f.eks. gæsteforelæsninger og projektsamarbejde i semesterprojekter i løbet af studietiden samt gode jobmuligheder for kandidaterne efterfølgende.

- Uddannelsen vil bidrage til og have gavn af det miljø inden for cybersikkerhed, der er under kraftig udvikling i Københavnsområdet. Det drejer sig bl.a. om en række af de projekter, der er finansieret af Industriens Fond (Danish Cyber Security Hub på DTU, hvor AAU er repræsenteret i bestyrelsen, det nyligt etablerede Center for Information Security and Trust på ITU, samt Cyber Range på CBS Executive, hvor AAU også er partner) og innovationsmiljøerne omkring FinansIT, Smart City løsninger og kunstig intelligens.

- AAU øger pt. forskningsaktiviteterne inden for cybersikkerhed på AAU Campus København. Dette er drevet af en kombination af interne forskningsmidler og ansættelser af forskere på højt internationalt niveau, samt eksternt finansierede projekter, bl.a. EU-projekter og projekter finansieret af danske bevillinger.

- Det forventes de fleste studerende at komme fra uddannelser, der udbydes i hovedstadsområdet, herunder fra AAU campus København.

Endeligt skal det fremhæves, at ansøgning om prækvalifikation af bacheloruddannelsen i software samt kandidatuddannelserne i hhv. software og cybersikkerhed indgår i en samlet strategi for Det Tekniske Fakultet for IT og Design med fokus på at fremme digitalisering og bæredygtighed. På campus København bærer den eksisterende uddannelsesportefølje allerede markant præg af uddannelser med fokus på bæredygtighed, og ansøgningerne om uddannelserne inden for software og cybersikkerhed er dermed en udvikling inden for digitaliseringssporet og derfor også et led i fakultetets strategiske satsning for at udvikle campus København i takt med den overordnede strategi.

På campus Aalborg er fakultetet repræsenteret med fire institutter som indbyrdes komplimenterer komplementerer og styrker hinanden. Her er IT-området et horisontalt område, som indgår som afsæt for de øvrige fagdiscipliner, og AAU kan konstatere, at der er synergi mellem IT-området og fakultetets øvrige fagområder. Med erfaringen fra AAU campus Aalborg kan det konkluderes, at tilstedeværelsen af et forsknings- og undervisningsmiljø i IT, styrker de øvrige forskningsmiljøer, hvilket også ligger til grund for, at fakultetet ønsker at udvide sit forskningsmiljø og sin uddannelsesportefølje inden for IT-området i København.

Med udvikling af campus København og sigtet mod øget digitalisering adresserer alle tre uddannelser, der søges udbudt, et behov i hovedstadsområdet og skaber sammenhæng med den overordnede strategi for Det Tekniske Fakultet for IT og Design. De tre uddannelser bidrager dog med hvert sit fokus inden for hhv. cybersikkerhed og softwareudvikling.

På baggrund af massive opfordringer fra aftagerpanelerne i Aalborg og København og de øvrige drøftelser med erhvervslivet, ønskes uddannelsen udbudt på engelsk. Begrundelserne er som følger:

- Fagterminologien og litteraturen er på engelsk. Hovedparten af de værktøjer de studerende skal anvende findes kun på engelsk. Det er derfor væsentligt, at kandidaterne udvikler en stærk engelsk fagterminologi. Engelsk er en forudsætning for efter endt studie at kunne følge den teknologiske udvikling og erhverve sig ny viden.

- Cybersikkerhed er et internationalt område, hvor kandidaterne vil samarbejde med udenlandske aktører på daglig basis - kunder, leverandører og myndigheder. Disse relationer foregår alt overvejende på engelsk. Det bemærkes, at der ikke blot er tale om behov for et snævert fagligt/teknisk engelsk, da cybersikkerhed involverer mange discipliner, og der er behov for at samarbejde tæt på tværs af traditionelle faglige skel. Der er derfor brug for, at kandidaterne opnår træning i at bruge engelsk som arbejdssprog.

- Som det også fremgår af bemærkningerne fra aftagerpanelerne, har de fleste danske virksomheder, der beskæftiger højtuddannede IT-ansatte engelsk (og evt. dansk) som arbejdsprog. Det er således nødvendigt, at de uddannede kandidater kan begå sig i et internationalt miljø.

- Et uddannelsesudbud på engelsk gør det muligt at tiltrække internationale studerende, og dermed bidrage til, at efterspørgslen på kandidater imødekommes. AAU er særligt opmærksomme på en høj grad af fastholdelse af såvel danske studerende som studerende fra andre europæiske lande på det danske arbejdsmarked. Dette sker ved at facilitere gode relationer mellem studerende og erhvervsliv via projekt-arbejde og studiejobs.

Tilbagemeldingerne fra aftagerpanelerne bekræfter, at virksomhederne har så stort et behov for medarbejdere med specifikke kompetencer, at de orienterer sig mod udlandet. I sådanne tilfælde er det udelukkende kompetencerne hos den ansatte, der er afgørende. I dokumentationsrapporten (s. 11) er det ligeledes beskrevet, at 64% af virksomehederne svarer, at de i nogen eller høj grad er interesserede i at ansætte engelsksprogede ingeniører i fremtiden, og kun 12% er slet ikke interesseret i dette.

Underbygget skøn over det nationale og regionale behov for dimittender

På vegne af AAU har analysevirksomheden Epinion gennemført en behovsundersøgelse i maj-juni 2019 (vedlagt som bilag 1 til dokumentationsrapporten). Der er gennemført en kombineret web- og telefonisk spørgerunde blandt 120 virksomheder i udvalgte brancher. 91 virksomheder har besvaret undersøgelsen via web, mens 29 virksomheder har besvaret over telefon, hvor interviewene er gennemført af Epinion. Data er vægtet på baggrund af virksomhedernes størrelse og branchetilhørsforhold med udgangspunkt i populationen for de udvalgte branchekoder. Derudover er der gennemført 10 kvalitative dybdeinterviews af Epinion med potentielle aftagervirksomheder. De potentielle aftagervirksomheder har blandt andet vurderet kompetenceprofilens relevans som en del af behovsundersøgelsen.

Epinions behovsundersøgelse peger på et stigende behov for medarbejdere med længerevarende tekniske uddannelser med kompetencer inden for cybersikkerhed. Det er karakteristisk, at kompetencebehovet ændrer sig dynamisk. 50% af de 120 adspurgte virksomheder forventer "I høj grad" et større behov for ingeniører, dataloger eller andre med længerevarende IT-uddannelser med kompetencer inden for cybersikkerhed om 3 år (2019 til 2022), mens 43% forventer det "I nogen grad" (se dokumentationrapporten s.15). Der forventes at være en stigning på 157% i behovet for ingeniører med kompetencer i cybersikkerhed frem mod 2022, mens behovet for ingeniørfaglige medarbejdere generelt stiger med 58%. Dybdeinterviews med aftagerne bekræfter ligeledes, at antallet af profiler specialiseret inden for cybersikkerhed hidtil har været meget begrænset, og fortsat er det, samtidig med, at efterspørgslen efter dem er stigende grundet den øgede digitalisering og krav til cybersikkerhed i både offentlige og private virksomheder.

I absolutte tal angiver undersøgelsen, at efterspørgslen efter ingeniører specialiseret i cybersikkerhed i 2020 forventes at være på 1.600 mod et forventet udbud på 1.500 dimittender fra de uddannelser, der pt. eksisterer og berører cybersikkerhed. Denne mangel vokser frem mod 2025, hvor efterspørgslen forventes at være på 3.400, mens udbuddet vil være på 3.000. Dette beregningseksempel viser således en mangel på 100 af disse ingeniører i 2020, stigende til 400 i 2025. Tallene tager højde for horisontal substitution mellem ingeniører, dataloger og andre med lange IT-uddannelser, ligesom udbuddet også inkluderer ingeniører, der har videreuddannet sig inden for cybersikkerhed, og som ikke nødvendigvis har det niveau og den hedhedsforståelse, som kandidaterne fra den foreslåede kandidatuddannelse vil have.

I forhold til muligheden for substitution bemærkes endvidere, at ledigheden på området generelt er lav. En prognose fra DI Digital konkluderede i 2015, at IT- og elektronikområdet i 2020 vil mangle 3.000 specialister på trods af fordobling i universiteternes optag af studerende (Engineer the Future (2015) Prognose for STEM-mangel 2025. https://engineerthefuture.dk/media/1520/prognose_for_stem-mangel_2025_endelig_med_forside.pdf). En rapport udarbejdet af regeringen i 2016 fastslår, at der i 2030 vil mangle 19.000 IT-specialister i Danmark (Erhvervs- og Vækstministeriet (2016) Redegørelse om Danmarks digitale vækst 2016). Manglen på specialister er imidlertid særlig høj inden for cybersikkerhed, hvor der ifølge den af Epinion gennemførte behovsundersøgelse i dag er ansat 249 ingeniører, dataloger eller andre med længerevarende IT-uddannelser med kompetencer inden for cybersikkerhed. Dette forventer virksomhederne vil stige til 639 om tre år.

Virksomhederne efterspørger i høj grad medarbejdere med kompetencer inden for cybersikkerhed. Flere af de virksomheder, der oplever udfordringer med at rekruttere ingeniører, dataloger eller andre med lange IT-uddannelser med kompetencer inden for cybersikkerhed forklarer, at der er meget lille udbud på markedet, men stor efterspørgsel efter de få kompetente medarbejdere (se Bilag 1).

Det betyder også, at flere mindre virksomheder og offentlige organisationer er presset af det høje lønniveau på området. Den store efterspørgsel udtrykkes dertil også ved, at 20% (24) af de adspurgte virksomheder aktuelt har ubesatte stillinger, som vil kunne varetages af en ingeniør med kompetencer inden for cybersikkerhed. Samlet set har disse 24 virksomheder 57 aktuelt ubesatte stillinger, der kunne varetages af en cybersikkerhedsingeniør.

Samtidig beskriver de adspurgte virksomheder, hvilke kompetencer inden for cybersikkerhed de forventer at få brug for samt behovet for kandidaternes organisatoriske og forretningsmæssige forståelse af konteksten. Epinions behovsundersøgelse viser, at virksomhederne har svært ved at rekruttere profiler med den rette kompetenceprofil inden for cybersikkerhed. 64% af virksomhederne svarer, at det enten er svært eller meget svært, mens kun 3% vurderer det som let eller meget let. Virksomhederne påpeger, at det særligt er medarbejdere med erfaring samt kompetencer over det tekniske niveau (arkitektoniske og strategiske), der er er mangel på. 76% af de 120 adspurgte virksomheder svarer, at de i høj grad eller i nogen grad vurderer, at civilingeniører i cybersikkerhed fra AAU vil være relevante at ansætte i virksomheden nu eller i fremtiden.

AAU forventer, at kandidatuddannelsen i cybersikkerhed vil uddanne 25 dimittender pr. år. Det bemærkes i den forbindelse, at ovennævnte fremskrivning af behovet på 400 i 2022 også omfatter efteruddannelse.

Hvilke aftagere har været inddraget i behovsundersøgelsen?

De potentielle aftagere for kandidaterne fra uddannelsen har været inddraget i form af

- tidlig involvering i arbejdet med udvikling af efteruddannelser og forslag til en kandidatuddannelse i IT-sikkerhed i 2013-2015
- løbende dialog med branchen, både gennem forsknings- og undervisningsrelateret samarbejde, gennem uformelle kontakter og via samarbejdsprojekter.
- netværksmøder i forbindelse med projektet “Fremtidens talenter inden for IT-sikkerhed”, der er et AAU-koordineret projekt finansieret af Industriens Fond (se dokumentationsrapport s. 5 og https://www.industriensfond.dk/IT_sikkerhed).
- behovsundersøgelsen foretaget af Epinion
- formelle aftagerpanelmøder i København og Aalborg

Analysevirksomheden Epinion fik til opgave at foretage en behovsundersøgelse for uddannelsen baseret på en opgaveforståelse udarbejdet i samråd med AAU. En liste af ca. 4-6 nøglepersoner hos virksomheder inden for hvert af flg. områder: telekommunikation, energi, finans og forsikring, konsulentfirmaer, produktion, sikkerhed/forsvar, softwareudvikling samt offentlige myndigheder, interesseorganisationer og råd blev identificeret. En kort beskrivelse af uddannelsen og dens kompetenceprofil (se Bilag 1) samt listen over nøglepersoner (Bilag 2) blev indleveret til Epinion, som efterfølgende supplerede med relevante virksomheder fra deres database og udarbejdede en interviewguide i samråd med AAU. Interviewguiden var inddelt i en introduktion, spørgsmål om brugen af ingeniørfaglige medarbejdere på arbejdspladsen, match med kompetencer inden for cybersikkerhed, match med kompetenceprofilen samt afsluttende spørgsmål. Undersøgelsen omfattede i alt 120 potentielle aftagervirksomheder for kandidater i cybersikkerhed, fordelt på 1) **Private IT-virksomheder,** der udelukkende beskæftiger sig med sikkerhedsløsninger eller specifikke områder af cybersikkerhed, 2) **Private virksomheder**, der beskæftiger sig med et andet forretningsområde end sikkerhed som sådan, og 3) **Offentlige organisationer**, hvor typiske jobfunktioner omfatter drift, specialiseret teknik, compliance, arkitektur og konsulentbistand / rådgivning.

Derudover har AAU været i dialog med instituttets aftagerpaneler i hhv. Aalborg og København. Aftagerpanelerne har modtaget information om uddannelserne i form af beskrivelser, den generelle kompetenceprofil, udkast til studieordninger og mundtlige præsentationer og diskussion med aftagerpanelerne har bl.a. medført en række justeringer i studieordningerne.

Aftagernes kommentarer centrerer sig omkring uddannelsens balance mellem tekniske og kontekstuelle elementer ved virksomhedernes cybersikkerhedsproblemer. De tekniske omfatter eksempelvis konkrete løsninger og trusselsproblematikker, mens de kontekstuelle omfatter forretningsforståelse, forståelse af reguleringsmæssige krav til cybersikkerhed og privacy samt computer- og data-etik. Der er blandt aftagerne efterspørgsel på begge typer kompetencer. Uddannelsens kurser tilgodeser primært de tekniske elementer, mens projektarbejdet giver mulighed for at adressere såvel tekniske som kontekstuelle elementer.

Hvordan er det konkret sikret, at den nye uddannelse matcher det påviste behov?

Udviklingen af uddannelsen er sket i tæt dialog med aftagervirksomhederne. Dette afspejler sig i matchet mellem virksomhedernes behov og uddannelsens indhold, som beskrevet i dette afsnit. I Epinions behovsundersøgelse er 120 virksomheder blevet bedt om at angive, hvilke områder de beskæftiger sig med i relation til cybersikkerhed. Nedenfor er områderne sammenholdt med uddannelsens kurser og projekter.

- **Design og udvikling af sikre systemer og software (59% af virksomhederne er beskæftiget med dette)**: Området er en kernekomponent i uddannelsen, og kandidaterne tilegner sig progressivt kompetencer gennem kurserne "Secure software development" og "Advanced software security" samt projektmodulet "Secure systems: Attack and defense". Studerende med særlig interesse for området har mulighed for at vælge at fordybe sig i området gennem kurset "Models of security" samt projektmodulet "Secure systems development".

- **GDPR - Sikker håndtering af persondata (51% af virksomhederne er beskæftiget med dette):** Datahåndtering er ligeledes en væsentlig komponent i uddannelsen. De studerende undervises både i sikker håndtering af data generelt og mere specifikt i forhold til persondata. Uddannelsen sigter dog på at give de studerende en mere generel metodisk indsigt i problemstillingerne end blot den nuværende persondataforordning (GDPR). Efter den grundlæggende introduktion i "Fundamentals of security and cryptography" på 1. semester har de studerende, der har interesse for det, mulighed for at følge kurset "Identity and access management" på 2. semester. Der er mulighed for at fortsætte fordybelsen på 3. semester med kurserne "Privacy Engineering" og/eller de mere regulatoriske aspekter i "IT security regulation" og "Enterprise security and compliance". Ligeledes giver projektmodulet på 3. semester mulighed for at fordybe sig i "Security Governance".

- **Netværkssikkerhed - forebyggelse og detektion af cyberangreb (32% af virksomhederne er beskæftiget med dette):** Netværkssikkerhed er også en kernekomponent i uddannelsen, hvor kandidaterne ligesom med sikker software vil opleve en progression gennem studiet. I kurset "Fundamentals of security and cryptography" får de studerende de grundlæggende forudsætninger, der skal til for at arbejde videre med sikkerhed i netværk og distribuerede systemer i samme semesters projektmodul "Distributed systems security". På 2. semester fortsætter progressionen med kurset "Hacker space", der også understøtter semestrets projektmodul "Secure Systems: attack and defense", hvor der fokuseres på både netværkssikkerhed og sikker software. De studerende, der ønsker det, kan allerede på 2. semester vælge at fokusere på maskinlæringsbaserede værktøjer. Emner relateret til den nyeste forskning inden for netværkssikkerhed er væsentlige i kurset "Advanced topics in cyber security" på 3. semester.

- **IoT- og Cloud-sikkerhed (29% af virksomhederne er beskæftiget med dette):** IoT- og Cloud-sikkerhed dækkes fra starten af uddannelsen i kurset "Security in IoT and Cloud architectures". Derudover indgår aspekter af IoT- og Cloud-sikkerhed naturligt i kurser og projekter, der omhandler netværk og distribuerede systemer, herunder projektmoduelt på 1. og 2. semester samt kurset i "Advanced topics in cyber security" på 3. semester.

- **Kritisk infrastruktur (18% af virksomhederne er beskæftiget med dette):** Rent metodisk adskiller beskyttelse af kritisk infrastruktur sig ikke fra øvrige systemer, men da konsekvenserne af angreb kan være voldsomme, vil der oftest vælges en tilgang, hvor sikkerhed prioriteres højt i forhold til f.eks. økonomi og brugeroplevelse. Området dækkes derfor i en kombination af ovenstående tekniske discipliner (netværkssikkerhed og udvikling af sikre systemer/software), kurserne i reguleringsmæssige aspekter ("IT security regulation" og "Enterprise security and compliance") samt projektmodulet på især 3. semester, hvor de studerende får mulighed for løse mere komplekse problemstillinger ved at kombinere viden fra disse forskellige områder.

- **Risikovurdering (17% af virksomhederne er beskæftiget med dette):** Risikovurdering indgår i mange af uddannelsens elementer, da det er et væsentligt aspekt i at analysere en problemstilling med henblik på at udvikle løsninger. Risikovurdering er således explicit fremhævet i læringsmålene for en række af uddannelsens elementer på den sidste del af uddannelsen - herunder “secure systems development”, “Security governance”, “IT security regulation”, “Enterprise security and compliance” og “Privacy engineering”.

Tilbagemeldingerne fra de potentielle aftagervirksomheder på kompetenceprofilen for den nye uddannelse er positive. De fleste virksomheder foretrækker en kandidat, der primært har dækket de tekniske kompetencer, men som også har forståelse for de mere “bløde” områder og på den måde har en holistisk forståelse for sikkerhed. Aftagervirksomhedernes forslag til bl.a. øget fokus på hardware og embeddede systemer samt integration af forretningsforståelse i projektmodulerne er indarbejdet i nærværende forslag til uddannelsesstruktur, kompetenceprofil og vil blive indarbejdet i den endelige studieordning.

AAU konkluderer på ovenstående baggrund, at uddannelsens indhold matcher aftagernes behov, og at der er sammenhæng mellem uddannelsens kompetenceprofil og uddannelsens erhvervssigte.

Beskriv ligheder og forskelle til beslægtede uddannelser, herunder beskæftigelse og eventual dimensionering.
Kandidatuddannelsen i cybersikkerhed henvender sig til teknisk-videnskabelige eller naturvidenskabelige bachelorer samt diplomingeniører med IT-faglige uddannelser. En solid IT-faglig basis er en forudsætning for at specialisere sig og opnå den krævede forskningsbaserede dybde og helhedsforståelse inden for cybersikkerhed. Hensigten er således at tilbyde en attraktiv kandidatuddannelse, som kan rekruttere bredt.

Som anført i studieordningen vil følgende bacheloruddannelser give adgang til kandidatuddannelsen i cybersikkerhed (uden retskrav):

- Fra AAU: Bachelor i IT, kommunikations- og medieteknologi; Computerteknologi; Elektronik og IT; Datalogi; Software; Informationsteknologi; samt Diplomingeniør i Elektronik

- Fra DTU: Bachelor i Elektroteknologi; Netværksteknologi og IT; Softwareteknologi; samt Diplomingeniør i Elektroteknologi og Softwareteknologi

- Fra KU: Bachelor i Datalogi

- Fra ITU: Bachelor i Softwareudvikling
- Fra AU: Bachelor i Datalogi; Computerteknologi; Elektronik
- Fra SDU: Bachelor i Electronics; Software Engineering; Datalogi

Nogle af disse uddannelser indeholder ikke specifikke kurser eller elementer af sikkerhed. Derfor indledes 1. semester på den foreslåede kandidatuddannelse med, at kurset “Fundamentals of security and cryptography” gennemføres i et koncentreret forløb, så alle deltagere hurtigt opnår et fælles fundament for projektarbejdet og de øvrige kurser.

Kandidatuddannelsen vil være den første i cybersikkerhed i Danmark, og den vil tilbyde studerende med en af ovennævnte bacheloruddannelser en ny valgmulighed for at videreuddanne sig inden for et område med gode jobmuligheder. De mest oplagte muligheder for videreuddannelse er på det private marked gennem certificeringer. Hvilke certificeringer, der er relevante for den enkelte, afhænger af vedkommendes jobfunktion og interesser og kan gå fra meget tekniske certificeringer som f.eks. Offensive Security Certified Professionel (OSCP) til mere compliance-orienterede certificeringer som Certified Information Systems Security Professional (CISSP) eller Certified Ethical Hacker (CEH). Disse certificeringer er ofte stærkt fokuseret på færdigheder og værktøjer, men qua dimittendernes teoretiske og metodiske kompetencer inden for såvel netværkssikkerhed, sikker software og sikkerhedstestning vil de være godt klædt på til at følge disse certificeringer. Derudover tilbyder mange virksomheder yderligere træningsforløb for nyansatte.

Endelig vil kandidaterne have mulighed for at søge mod forskeruddannelser (PhD). Det er AAUs erfaring - også baseret på dialoger med DTU - at det hidtil har været meget vanskeligt at rekruttere PhD-studerende inden for cybersikkerhed. Dette er dels en begrænsende faktor for offentlig dansk forskning på området, men det gør det også svært at imødekomme virksomhedernes behov for disse kandidater.

AAU har i udviklingen af uddannelsen gennemført en analyse af en række eksisterende uddannelser baseret pa■ deres indhold og erhvervssigte for at sikre, at den ansøgte uddannelse dels bidrager til øget sammenhæng i det danske uddannelsessystem, dels ikke vil resultere i forringelser af vilka■rene for de beslægtede uddannelser. Som tidligere nævnt, findes der ikke andre uddannelser på kandidatniveau, som er dedikeret til cybersikkerhed, men uddannelsen vil indgå i et spektrum af uddannelser på forskellige niveauer og med forskellige sigter. Derfor har analysen omfattet beslægtede professionsbacheloruddannelser, efteruddannelser og relaterede kandidatuddannelser inden for teknisk IT med særlig fokus på deres indhold af cybersikkerhed.

I det følgende omtales de 3 typer af uddannelser: 1) professionsbachelorer, 2) efteruddannelser, og 3) kandidatuddannelser.

1) Professionsbachelor (1 ½ år, 90 ECTS):

Disse uddannelser er korte videregående uddannelser, der henvender sig til studerende med en ungdomsuddannelse, og de skaber ikke en forskningsniveau-mæssig dybde i de studerendes faglighed. Selvom der elementvis er sammenfald mellem fagligheden på erhvervsuddannelserne i IT-sikkerhed og kandidatuddannelsen i cybersikkerhed, uddanner de dimittender med forskellige kompetencesæt. Kandidatuddannelsen i cybersikkerhed retter sig imod universitetsbachelorer og bygger på faglig dannelse til forskningsmæssig dybde. En professionsbachelor giver ikke samme kvalifikationer som en teknisk-videnskabelig bachelorgrad fra et universitet, og disse professionsbachelorer kan ikke optages på en civilingeniøruddannelse på kandidatniveau.

KEA og EA udbyder top-up uddannelser i IT-sikkerhed som overbygning til en AP degree som datamatiker eller IT-teknolog:

- IT-sikkerhed, top-up professionsbachelor, Københavns Erhvervsakademi (KEA)

- IT-sikkerhed, top-up professionsbachelor, Erhvervsakademi Aarhus (EA)

Det faglige indhold består på KEA af introduktion til IT-sikkerhed, IT-governance, system sikkerhed, netværks- og kommunikationssikkerhed, videregående IT-governance og software sikkerhed, mens det på EA består af system- og applikationssikkerhed, netværks- og kommunikationssikkerhed, design af sikre systemer og sikkerhedsledelse (IT-governance). KEA uddanner ca. 50 af disse professionsbachelorer pr. år.

2) Efteruddannelse (1 år, 60 ECTS):

Efter- og videreuddannelser er rettet imod erhvervsaktive bachelorer og kandidater og kan ikke danne grundlag for en efterfølgende forskningskarriere. Disse uddannelser indeholder sammenlignelige faglige elementer, men uden samme faglige dybde som den foreslåede kandidatuddannelse vil tilbyde.

- *Master i it, specialisering i IT-sikkerhed, IT-Vest (samarbejde mellem AAU og AU)*

AAU udbyder i regi af IT-Vest en masteruddannelse i IT-sikkerhed, hvortil der eksisterer fagpakker på 15 ECTS-point i henholdsvis netværkssikkerhed, IT-sikkerhed og kryptologi, IT-sikkerhed i organisationer, og sikker softwareudvikling.

- *Master in Information and Communication Technologies, specialisering i ICT Cyber and Information Security, AAU København*

Uddannelsen indeholder tre specialiseringer: ICT Services and Platforms, Management of ICT Innovations og ICT Cyber and Information Security. På den sidstnævnte specialisering indgår kurser og projekter i Cybercrime and Information Security Law, Enterprises Cyber Security, Cyber security and trust, Privacy & Security frameworks in Organizations, og Identity and Access Management.

- *Master i cybersikkerhed, 60 ECTS, DTU*

DTU har i april 2019 fået godkendt prækvalifikation til åbning af en ny masteruddannelse i cybersikkerhed, som tilbyder sammenlignelige faglige elementer. Den består af fire semestre med temaerne IT-sikkerhedsledelse og governance, IT-sikkerhedsinfrastruktur, sikre applikationer og systemer, og masterafhandlingsprojekt. Indholdet af denne uddannelse har et betydeligt overlap med den foreslåede kandidatuddannelse, men målgrupperne er forskellige, da der her er tale om efteruddannelse med brugerbetaling, og master-uddannelser kun har et omfang på 60 ECTS.

Endvidere har ITU i foråret 2019 etableret et Center for Information Security and Trust, som vil starte projekter for at hjælpe danske virksomheder til at opruste på IT-sikkerhed. I første omgang satses der på at udbyde kurser i IT-sikkerhed for små og mellemstore virksomheder i form af efteruddannelse (https://www.industriensfond.dk/UddannelsesprojektSMV).

3) Kandidat (2 år, 120 ECTS):

På kandidatniveau udbyder danske universiteter en bred vifte af tekniske IT-faglige uddannelser, og listen herunder er en bruttoliste af beslægtede civilingeniør- og datalogi-orienterede kandidatuddannelser:

- AAU: Communication Technology, Innovative Communication Technologies and Entrepreneurship, Datalogi, Software, Computer Science (IT)
- DTU: Computer Science and Engineering, Digitale medieteknologier, Informationsteknologi, Matematisk modellering og computing, Telekommunikation
- ITU: Datalogi, Softwaredesign
- KU: Datalogi
- SDU: Software engineering, data science, datalogi
- RUC: Computer science (Datalogi) + Informatik
- AU: Datalogi, Cognitive Science (Kognitionsvidenskab), Computerteknologi, Elektroteknologi, Informationsteknologi - IT, kommunikation og organisation, IT-produktudvikling (EN)

Blandt disse er der efterfølgende udvalgt de nærmest beslægtede uddannelser, hvor der indgår elementer af sikkerhed i uddannelserne.

AAU: *Communication Technology (CT) (tidligere Networks and Distributed Systems) og Innovative Communication Technologies and Entrepreneurship (ICTE)*

Disse uddannelser er de nærmest beslægtede ingeniøruddannelser på AAU (se dokumentationsrapporten s. 1). For CT berøres cybersikkerhed i et enkelt kursus på uddannelsen. På baggrund af den store interesse fra såvel som studerende som aftagere har der i de senere år været afviklet en del projekter med fokus på cybersikkerhed fra et netværksperspektiv. Uddannelsen dækker således kun en snæver del af cybersikkerhedsområdet, hvor bl.a. områderne sikker software og governance ikke berøres eller kun berøres helt perifert. ICTE indeholder to dedikerede kurser i cybersikkerhed, “Identity and access management” og “Enterprise security and compliance”. Derudover er kurset “Machine learning” relevant, og der er mulighed for at vælge semesterprojekter på 2. og 3. semester i relation til disse. De tre nævnte kurser foreslås samlæst med uddannelsen i cybersikkerhed.

***DTU:** Computer Science and Engineering og andre kandidatuddannelser*

Kandidatuddannelser på DTU indeholder typisk "study lines" (anbefalede studieforløb) med op til 30 ECTS "teknologiske liniefag", som kan vælges ud af en anbefalet liste af kurser. "Computer science and engineering" indeholder seks "study lines", deriblandt "Computer security" og "Safe and secure by design", og specielt "computer security" indeholder mange kurser i sikkerhed. Resten af de 120 ECTS i uddannelsen handler mere bredt om computer science and engineering (ikke IT-sikkerhed). "Informationsteknologi" indeholder det samme studieforløb i "computer security". "Mathematical modelling and computing" indeholder et anbefalet studieforløb om "Secure and reliable computing", som bl.a. indeholder to kurser i kryptografi. De øvrige kandidatuddannelser på DTU, der er nævnt ovenfor, indeholder enkelte sikkerhedsrelaterede kurser i f.eks. data security og biometric systems.

Øvrige universiteter og beslægtede kandidatuddannelser:

ITU: Datalogi indeholder en specialisering på 22,5 ECTS om "Information security" med to kurser i "Security 2" og "Advanced security". "Software design" indeholder et kursus om "Applied Information Security".

KU: Datalogi indeholder et kursus om "Proactive Computer Security".

SDU: Data science indeholder et enkelt kursus i "IT-sikkerhed, IT-etik og privathed". "Datalogi" indeholder et kursus om "Netværk og sikkerhed".

AU: Tilbyder bl.a. en række kurser inden for kryptografi og et kursus i "Identity and privacy", der kan vælges på "Datalogi" og "IT-produktudvikling".

Kandidatuddannelsen i cybersikkerhed på AAU adskiller sig fra ovennævnte uddannelser ved at skabe et dybt, bredt og sammenhængende fagligt fundament i metoder og værktøjer inden for fagområdet. Dette fundament udgøres af tre centrale søjler inden for fagligheden:

1. Sikkerhed i netværk og distribuerede systemer
2. Udvikling, test og verifikation af sikker software samt
3. En række centrale anvendelsesområder som IoT- og Cloud-sikkerhed, identity and access management, sikker håndtering af persondata, virksomheders IT- og service-arkitekturer og security governance.

Dimittender fra den foreslåede kandidatuddannelse i cybersikkerhed vil besidde kompetencer til at udforme dybdegående strategiske udviklings- og designmæssige analyser og træffe sikkerhedsmæssige beslutninger på den baggrund. Dertil opnår de studerende en dyb og konkret forståelse for sikkerhedsmæssige risici i organisationer med kritisk infrastruktur og lærer om forebyggelse, detektion og inddæmning af angreb.

Mere konkret vil den studerende på den foreslåede nye kandidatuddannelse i cybersikkerhed opnå omfattende viden, færdigheder og kompetencer inden for følgende internationalt anerkendte kernefagligheder for cybersikkerhed som videnskabeligt felt:

- Forståelse for de unikke karakteristika ved det heterogene og ustabile landskab af cybertrusler
- Velovervejet kommunikation, strategisk planlægning og design af løsninger til udvikling, test og verifikation af sikker software
- Udarbejdelse af kritiske risiko- og trusselsanalyser, som kan danne grundlag for sikkerhedsvurderinger i konkrete problemstillinger med kritisk infrastruktur
- Forebyggelse, detektion og inddæmning af angreb
- Designe og opgradere IT system arkitektur til at overholde nye reguleringer og juridiske bindinger (ISO2700x, GDPR, NIS, PSD2)

Denne faglige dybde og bredde understøttes af stærke faglige miljøer. Gennem kurser og projektarbejde sættes fokus på problembaseret læring, hvor de studerende opnår viden om væsentlige anvendelsesområder og erfaring med at omsætte teknisk viden til udvikling af konkrete løsninger. Et fokuseret uddannelsesforløb centreret omkring problembaserede læring afspejler et virkelighedsnært arbejdsmiljø, som sikrer, at de studerende besidder kompetencer af høj relevans og direkte anvendelighed for arbejdsmarkedet.

Som det fremgår af den sammenlignende analyse ovenfor, udbydes der kandidatuddannelser med relevante kurser og studieforløb i forhold til det faglige indhold af den foreslåede kandidatuddannelse i cybersikkerhed, men ikke i et omfang/niveau, der opfylder behovet på arbejdsmarkedet. Derfor fremstår den foreslåede kandidatuddannelse ikke blot som en modifikation af eksisterende tilbud, men vil adskille sig ved at udbyde et sammenhængende uddannelsesforløb på 120 ECTS-point med cybersikkerhed i centrum.

Den foreslåede nye kandidatuddannelse i cybersikkerhed på AAU vil således bidrage med en ny profil, som ikke overlapper med kompetenceprofiler for eksisterende uddannelser eller med disses erhvervssigte.

Afslutningsvist er forskningsmiljøet bag uddannelsen opmærksomt på og deltager aktivt i arbejdet i Danish Cyber Security Hub, der sigter efter at styrke og koordinere dansk uddannelse og forskning inden for cybersikkerhed. I forbindelse med projektet er der ikke identificeret relevante initiativer ud over de allerede beskrevne.

Rekrutteringsgrundlag og videreuddannelsesmuligheder

Kandidatuddannelsen forventes primært at rekruttere bachelorer fra universiteter i hovedstadsområdet. En væsentlig kilde vil være bachelor i IT, kommunikations- og medieteknologi (ITCOM) og evt. bachelor i software, som begge udbydes på AAU campus København. Bacheloruddannelserne i hhv. computerteknologi, elektronik og IT, datalogi, informationsteknologi samt diplomingeniør i elektronik (AAU) vil også udgøre rekrutteringsgrundlaget. Fra DTU kan der rekrutteres fra bacheloruddannelserne i hhv. softwareteknologi, elektroteknologi, netværksteknologi og IT samt diplomingeniør i elektroteknologi og softwareteknologi, og endelig kan der fra KU rekrutteres bachelorer i datalogi og fra ITU bachelorer i softwareudvikling.

Der vil således være et stort antal bachelorer især fra AAU campus København, ITU, DTU og KU, som er kvalificerede til at søge ind på den foreslåede kandidatuddannelse. Disse studerende kan i forvejen vælge blandt en bred vifte af kandidatuddannelser i hovedstadsområdet, som den nye uddannelse vil indgå i. Med et stigende nationalt behov for ingeniører, der overstiger antallet af dimittender samt et behov for kompetencer inden for cybersikkerhed, der er markant højere end behovet for ingeniører generelt, er der en volumen i efterspørgslen, der giver plads til en ny uddannelse i cybersikkerhed, uden at dette fa■r negativ virkning pa■ eksisterende uddannelser (se dokumentationsrapport, s. 15).

Forventet optag på de første 3 år af uddannelsen

Uddannelsen forventes at optage ca. 30 ansøgere pr. år. Ansøgere forventes dels rekrutteret fra AAUs adgangsgivende bacheloruddannelser i København, dels de øvrige adgangsgivende uddannelser i hovedstadsområdet. Endelig kan der forventes nogle ansøgere fra de øvrige adgangsgivende uddannelser i Danmark.

Hvis relevant: forventede praktikaftaler

Ikke relevant.

Øvrige bemærkninger til ansøgningen

Ingen.

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

Ja

Status på ansøgningen

Godkendt

Ansøgningsrunde

2019-2

Afgørelsesbilag - Upload PDF-fil

A3 - Godkendelse - KA i cybersikkerhed - AAU (København)(justeret).pdf

Samlet godkendelsesbrev - Upload PDF-fil

AALBORG UNIVERSITET

Rektoratet
Fredrik Bajers Vej 5
Postboks 159
9100 Aalborg

Prorektor
Inger Askehave
www.aau.dk

Dato: 02-07-2019
Sagsnr.: xxxx-xxx-xxxxx

Dokumentation af efterspørgsel på uddannelsesprofil

Baggrund for ansøgningen

Cyberangreb udgør i dag en alvorlig trussel mod vigtige samfundsfunktioner og mod virksomheders og enkeltpersoners data og ressourcer. Der er et stigende behov for altid at være forbundet til internettet for at kunne tilgå services og information, men samtidig øges vores sårbarhed og eksponering over for cybertrusler. Truslerne har resulteret i øgede krav til virksomhederne via EU og national lovgivning, herunder skrappe krav til håndtering af følsomme persondata og indrapportering af sikkerhedshændelser. Der er behov for bedre IT-arkitekturer, øget netværkssikkerhed, bedre softwareudvikling med fokus på sikkerhed og en øget bevågenhed på alle niveauer af, hvor sårbarhederne er hvilke ressourcer, der skal beskyttes, og hvilken betydning truslerne har for organisatoriske og forretningsmæssige processer.

Det overordnede formål med kandidatuddannelsen er at give den studerende en dyb teknisk faglighed kombineret med en helhedsforståelse af cybersikkerhed, idet udbuddet af uddannelser i Danmark, der giver kompetencer inden for cybersikkerhed, stadig er ret begrænset. Aalborg Universitet (AAU) har siden 2014 udbudt fagpakker i IT-sikkerhed sammen med IT-Vest og fra 2015 en specialisering i "Cyber and Information Security" på den eksisterende masteruddannelse i information and communication Technologies (mICT) i København. Derudover findes der professionsbacheloruddannelser i IT-sikkerhed på Københavns Erhvervsøkonomi (KEA) og Erhvervsakademi Aarhus, og Danmarks Tekniske Universitet (DTU) har i 2019 fået godkendt en efteruddannelse i cybersikkerhed. Desuden tilbydes efteruddannelse i form af enkeltkurser på bl.a. Teknologisk Institut. På kandidatniveau indgår elementer af sikkerhed i flere uddannelser både på AAU og andre danske universiteter, men der findes for nærværende ikke en ingeniøruddannelse på kandidatniveau, der har cybersikkerhed som det centrale omdrejningspunkt.

Uddannelsen og dens dimittender vil opfylde rekrutteringsudfordringer hos både specialiserede IT- og cybersikkerhedsvirksomheder, almindelige virksomheder samt offentlige organisationer, som alle oplever et stadigt voksende rekrutteringsproblem. Kandidater med specialiserede tekniske kompetencer er efterspurgte, men mange virksomheder ønsker disse kompetencer forbundne med en forretnings- og organisationsforståelse. Der er brug for 'brede specialister' med en dyb teknisk faglighed kombineret med den fornødne helhedsforståelse af cybersikkerhed, som kun vil kunne opnås med en forskningsbaseret uddannelse på kandidatniveau, der er fuldt dedikeret til fagområdet. Den foreslåede kandidatuddannelse adresserer dette behov ved hjælp af AAU's problembaserede læringstilgang.

Vurdering af hvorvidt kompetenceprofilen kan opnås via toning af en eksisterende uddannelse

AAU har afsøgt muligheder for toning af allerede eksisterende kandidatuddannelser på AAU med henblik på at opfylde aftagernes behov uden prækvalifikation og oprettelse af en ny kandidatuddannelse. AAU udbyder flere tekniske kandidatuddannelser, som indeholder elementer af IT-sikkerhed, og de nærmest beslægtede vurderes at være kandidatuddannelsen i communication technology (CT) på AAU campus Aalborg og kandidatuddannelsen i innovative communication technologies and entrepreneurship (ICTE) på AAU campus København. Begge udbydes af Institut for Elektroniske Systemer under Det Tekniske Fakultet for IT og Design. Konklusionen er imidlertid, at de beslægtede uddannelser på AAU ikke giver mulighed for den flerfaglighed, der er nødvendig for at dimittendernes kompetencer kan opfylde industriens behov for civilingeniører i cybersikkerhed.

CT fokuserer på netværk og distribuerede systemer. Uddannelsen går i dybden med teknologier i forhold til kommunikation (herunder trådløs kommunikation, antenner og modulering), netværksplanlægning, netværksperformance og realtidssystemer. Cybersikkerhed berøres i et enkelt kursus på uddannelsen. På baggrund af den store interesse fra såvel som studerende som aftagere har der i de senere år været afviklet en del projekter med fokus på cybersikkerhed fra et netværksperspektiv. Uddannelsen dækker således kun en snæver del af cybersikkerhedsområdet, hvor bl.a. områderne omkring sikker software og governance ikke berøres eller kun berøres helt perifert. En toning af uddannelsen for at dække disse områder ville kræve en så stor udskiftning i de udbudte kurser og projektmoduler, at der reelt ville være tale om en ny uddannelse (CT er en ny uddannelse, der afløser kandidatuddannelse i networks and distributed systems, men bemærkningerne ovenfor er fortsat gældende).

ICTE fokuserer på udvikling af nye services og løsninger baseret på informations- og kommunikationsteknologier (IKT), og hvordan IKT kan udnyttes til at skabe værdi, løse konkrete brugerbehov og generere nye forretningsmuligheder. De studerende får en generel forståelse af, hvordan de nyeste netværksteknologier (5G, cloud, Internet of Things) og state-of-the-art frameworks for service- og dataarkitekturer fungerer, og hvordan de kan skabe værdi i en given kontekst. De konkrete anvendelser omfatter analyse af brugerbehov, specifikke anvendelsesscenarier, stakeholder-analyse og udvikling af nye forretningsmodeller eller tilpasning af eksisterende. Den centrale præmis er, at nye services og løsninger har større chancer for at kunne realiseres, når bruger- og forretningsforståelse indgår som en integreret del af udviklingsprocessen. Sikkerhedsaspekter indgår i uddannelsen i relation til håndtering af persondata, adgangskontrol til beskyttede ressourcer og sikkerhed i virksomheder. De centrale kurser i "Identity and access management", "Machine learning" og "Enterprise security and compliance" vil kunne følges af studerende på både ICTE og den foreslåede uddannelse i cybersikkerhed.

Det har således været diskuteret og vurderet, om uddannelsens kompetenceprofil kunne opnås via en toning af en eksisterende uddannelse. Selv om der er elementer af cybersikkerhed i begge uddannelser, vil en toning af disse uddannelser efter AAUs opfattelse ikke kunne afhjælpe aftagernes ønsker om cybersikkerhedsspecialister på et højt teknisk niveau, der samtidig har organisations- og forretningsforståelse. En ændring af fagudbuddet med tilstrækkeligt indhold af cybersikkerhed vil ikke kunne rummes inden for disse uddannelser og vil i for høj grad ændre deres kompetenceprofiler og overordnede sigte.

Udviklingsprocessen (herunder aftagerinvolvering)

Kandidatuddannelsen er udviklet gennem en lang dialog med aftagere, der startede tilbage i 2013, hvor Aalborg Universitet udarbejdede et forslag til en masteruddannelse i informationssikkerhed og en kandidatuddannelse i IT-sikkerhed, som skulle udbydes på AAU campus i Aalborg. De involverede aftagere var dengang bl.a.

- Adser Leick (DI ITEK)
- Henrik Vinstrup (DI ITEK)
- Henning Mortensen (DI ITEK)
- Peter Kruse (CSIS Security Group A/S)
- Klaus Kongsted Andersen (Dubex A/S)
- Anders Pall Skött (CFIR)
- Rene Hedegaard Hansen (Terma)
- Poul Thorlacius-Ussing (Center for Cybersikkerhed, FE)
- Birgitte Kofod Olsen (Rådet for Digital Sikkerhed)
- Claus Hjorth (Medierådet for Børn og Unge)
- Mette Lindskov (Konsulent hos Rigspolitiet)
- Johnny Lundberg (National IT-Efterforskningssektion, Rigspolitiet)
- Anne Louise Capion (Center for Cybersikkerhed, FE).

For mange deltagere har de organisatoriske tilknytninger ændret sig siden, men de fleste er stadig aktive i det danske community inden for cybersikkerhed, og mange af dem har deltaget i løbende dialoger om udviklingen af kandidatuddannelsen helt frem til i dag.

I slutningen af 2018 iværksatte dekanen for TECH-fakultetet på AAU en proces med henblik på at lancere nye IT-uddannelser på campus i København, herunder nærværende kandidatuddannelse i cybersikkerhed. Der blev nedsat en arbejdsgruppe med repræsentanter fra tre forskningsgrupper på Institut for Elektroniske Systemer (Aalborg og København) og Institut for Datalogi (Aalborg), som fik til opgave at udvikle uddannelsen med udgangspunkt i det tidligere forslag som nævnt ovenfor. En adjunkt i cybersikkerhed blev ansat på CMI, Institut for Elektroniske Systemer i København pr. 1. feb. 2019 og inddraget i arbejdsgruppen. I 1. halvår 2019 blev der udarbejdet et oplysningsskema med struktur af uddannelsen, en generel kompetenceprofil og en studieordning for uddannelsen. I denne periode bidrog forskellige virksomheder med forslag og ønsker til indholdet, f.eks. Terma, PwC og Strand Consult.

Analysevirksomheden Epinion fik til opgave at foretage en behovsundersøgelse for uddannelsen udarbejdet i samråd med AAU (se bilag 1). Formålet var at kortlægge det nationale og regionale behov for højtuddannede med kompetencer inden for cybersikkerhed, afdække hvorvidt der er et match mellem kompetenceprofilen for den foreslåede kandidatuddannelse og industriens behov for højtuddannede med kompetence inden for cybersikkerhed samt at afdække potentielle aftagervirksomheders holdning til ansættelse af ikke-dansktalende kandidater med kompetence inden for cybersikkerhed.

Arbejdsgruppen udarbejdede en liste af ca. 4-6 nøglepersoner hos virksomheder inden for hvert af flg. områder: telekommunikation, energi, finans og forsikring, konsulentfirmaer, produktion, sikkerhed/forsvar, softwareudvikling samt offentlige myndigheder, interesseorganisationer og råd. En kort beskrivelse af uddannelsen og dens kompetenceprofil[1] samt listen over nøglepersoner blev indleveret til Epinion (se bilag 2), som efterfølgende supplerede med relevante virksomheder fra deres database og udarbejdede en interviewguide i samråd med AAU. Brancher og aftagervirksomheder er udvalgt ud fra en vurdering af uddannelsens erhvervssigte og centrale mulige aftagere, regionalt og nationalt. Interviewguiden var inddelt i en introduktion, spørgsmål om brugen af ingeniørfaglige medarbejdere på arbejdspladsen, match med kompetencer inden for cybersikkerhed, match med kompetenceprofilen samt afsluttende spørgsmål.

Behovsundersøgelsen er gennemført fra maj til juni 2019. Der er gennemført en kombineret web- og telefonisk spørgerunde blandt 120 virksomheder i udvalgte brancher. 91 virksomheder har besvaret undersøgelsen via web, mens 29 virksomheder har besvaret over telefon, hvor interviewene er gennemført af konsulenter fra Epinion. Data er vægtet på baggrund af virksomhedernes størrelse og branchetilhørsforhold med udgangspunkt i populationen for de udvalgte branchekoder. Derudover er der gennemført ti kvalitative dybdeinterviews med potentielle aftagervirksomheder af Epinion. Endelig er der gennemført en grundig desk research af relevante analyser og andre kilder vedrørende udbud og efterspørgsel på ingeniører. Behovsundersøgelsen blev afsluttet med en rapport til AAU juni 2019[2].

De potentielle aftagervirksomheder for kandidater i cybersikkerhed inddeles i Epinions undersøgelse i tre grupper:

1. **Private IT-virksomheder,** der udelukkende beskæftiger sig med sikkerhedsløsninger eller specifikke områder af cybersikkerhed, f.eks. udvikling af sikre systemer eller konsulentydelser på området. De har derfor brug for meget specialiserede medarbejdere, der eksempelvis kan udvikle nye sikre systemer eller lave analyser og test af virksomheders eksisterende sikkerhedsløsninger. Denne type virksomhed vil således primært efterspørge medarbejdere med dybe, specialiserede tekniske kompetencer på området.
2. **Private virksomheder**, der beskæftiger sig med et andet forretningsområde end sikkerhed som sådan. Det kan f.eks. være produktion af forskellige produkter eller levering af serviceydelser. Når disse virksomheder opnår en vis størrelse, vil der være behov for medarbejdere, der kan håndtere cybersikkerheden i virksomheden, det vil sige drift, herunder vedligeholde og overvåge sikkerhedssystemerne for at undgå angreb og nedbrud. Disse virksomheder vil som regel købe sig nogle sikkerhedsløsninger og har derfor brug for medarbejdere til at implementere og vedligeholde disse. Desuden kan der i sådanne virksomheder også ofte være brug for medarbejdere med viden om sikkerhed på et højere, strategisk plan, der kan sikre koblingen af sikkerheden og systemerne til forretningen og den strategiske udvikling. Endeligt vil der også i visse virksomheder være behov for medarbejdere, der har viden om lovgivning, krav og reguleringer på sikkerhedsområdet, og som kan anvende denne viden til at sikre, at virksomheden lever op til disse. Hos store virksomheder kan man også vælge at udvikle sin egen mere specialiserede sikkerhedsenhed, der f.eks. udvikler deres egne systemer, selv tester systemerne eller foretager analyser på eget data, hvilket kræver mere dybe, specialiserede medarbejdere.
3. **Offentlige organisationer**, der oftest vil efterspørge den samme type medarbejdere som private IT-virksomheder. Her er også der brug for medarbejdere med en dyb, specialiseret teknisk viden, der kan kode, hacke mv. Der er således primært konkurrence om denne type medarbejdere mellem konsulentvirksomhederne og de offentlige institutioner.

Der er afholdt møder med instituttets aftagerpaneler i København (18. juni) og Aalborg (1. juli), hvor uddannelsens kompetenceprofil og resultaterne fra behovsundersøgelsen blev drøftet[3].

Hos AAUs ledelse er processen med udvikling og ansøgning om prækvalifikation af nye uddannelser forankret hos prorektor Inger Askehave, dekan og prodekan for Det Tekniske Fakultet for IT og Design samt enheden Strategi og Kvalitet. Uddannelsens indhold og struktur har været drøftet i Studienævnet for Elektronik og IT, og det er studienævnets opgave at godkende studieordningen for uddannelsen. Arbejdsgruppen har udarbejdet ansøgningen

[1] Beskrivelse af uddannelsen og dens kompetenceprofil kan fremsendes, hvis dette ønskes.

[2] "Behovsundersøgelse for ingeniører med kompetencer inden for cybersikkerhed", Epinion, juni 2019

[3] Referater fra møder i aftagerpanel kan fremsendes, hvis dette ønskes.

om prækvalifikation i samarbejde med viceinstitutleder Ove Andersen, prodekan Jakob Stoustrup og medarbejdere fra Strategi og Kvalitet.

Studieordningen for uddannelsen blev sideløbende opdateret, og den blev godkendt af Studienævnet for Elektronik og IT på møde d. 21. aug. 2019. Denne indeholder en beskrivelse af uddannelsens kompetenceprofil samt udførlige beskrivelser af læringsmål for de enkelte kursus- og projektmoduler[4].

Ansøgningen har efterfølgende været forelagt og er godkendt af AAUs prorektor for uddannelse i september 2019.

Udviklingen af uddannelsens indhold i dialog med aftagere

Interessenterne har fået information om uddannelsens formål, profil, indhold og erhvervssigte på flere niveauer. Da nærværende uddannelse er den eneste kandidatuddannelse, der har cybersikkerhed som det centrale omdrejningspunkt, er der ikke drøftet konkret materiale om beslægtede uddannelser med aftagere.

Som tidligere nævnt har der været en tæt dialog med virksomheder allerede i 2013 og 2014 om udvikling af en masteruddannelse og en kandidatuddannelse i IT-sikkerhed. Det faglige indhold på masteruddannelsen i IT med specialisering i IT-sikkerhed i fagpakkerne "Netværkssikkerhed", "Sikker softwareudvikling" og "IT-sikkerhed i organisationer" blev udviklet og defineret i samarbejde mellem Institut for Datalogi, Juridisk Institut og Institut for Elektroniske Systemer (herunder sektionen CMI fra AAU København). Samme struktur dannede grundlag for det notat, der blev udarbejdet for kandidatuddannelsen i cybersikkerhed. Arbejdet skete i tæt samarbejde med potentielle aftagere, herunder både virksomheder, der indtænker cybersikkerhed i deres produktion, virksomheder, der har behov for at sikre deres systemer mod cyberangreb, virksomheder, der forvalter kritisk infrastruktur som f.eks. tele, energi og finans samt relevante myndigheder herunder repræsentanter fra politiet og forsvaret. Specialiseringen i "Cyber and Information Security" blev ligeledes udformet i dialog med de virksomheder, som er nævnt ovenfor.

Siden 2018 er der arbejdet på videreudvikling af notatet om kandidatuddannelsen i cybersikkerhed i dialog med aktører fra både myndigheder og virksomheder, der dengang var involveret i at skabe forløbet. Dog blev det på ledelsesplan besluttet, at de juridiske aspekter skulle erstattes af andre, som kunne dækkes af faggrupperne på Institut for Elektroniske Systemer og Institut for Datalogi. Det har givet plads til emner som IoT - og cloud-sikkerhed, identity and access management, compliance og privacy engineering for at tilgodese nogle af de aftagerbehov, der også fremhæves i behovsundersøgelsen og på aftagerpanelmøderne. Det detaljerede forslag til uddannelsens struktur og faglige indhold blev således defineret i begyndelsen af 2019, og det er med mindre tilretninger blevet vel modtaget hos aftagerne, som beskrevet nedenfor. Efterfølgende blev der udarbejdet en studieordning og kompetenceprofil i foråret 2019, og kompetenceprofilen indgik i den korte beskrivelse, som Epinion har givet videre til aftagerne i forbindelse med behovsundersøgelsen.

Via Epinions behovsundersøgelsen blev aftagerne præsenteret for uddannelsens kompetenceprofil. De enkelte virksomheder har hver især forslag til mindre justeringer, der kan gøre uddannelsen mere relevant for netop deres virksomhed, f.eks. øget fokus på machine learning eller operations technology. Overordnet set er det dog primært forretningsforståelse, der efterspørges på tværs af virksomhederne. Det påpeges, at det giver virksomhederne stor værdi, når deres IT-medarbejdere har forståelse for, hvordan forretningen fungerer, og hvordan sikkerhed skal spille ind som et understøttende element i virksomhedens primære formål. Desuden fremhæves det, at de tekniske færdigheder dækkes tilfredsstillende i kompetenceprofilen, men at også de personlige kompetencer hos den enkelte kandidat er vigtige og vægtes højt, når virksomhederne skal ansætte nye medarbejdere inden for dette område. Tilbagemeldingerne fra de potentielle aftagervirksomheder på kompetenceprofilen for den nye uddannelse er positive.

Efterfølgende har to aftagerpaneler diskuteret Epinions behovsundersøgelsen på to aftagerpanelmøder i hhv. København og Aalborg. Herudover har aftagerpanelerne modtaget udkast til studieordninger og mundtlige præsentationer. Diskussionen med aftagerpanelerne har medført en række justeringer i studieordningerne, hvilket er beskrevet i detaljer herunder.

Tilbagemeldingerne fra de potentielle aftagervirksomheder på kompetenceprofilen for den nye uddannelse er positive. Aftagernes bemærkninger centrerer sig om uddannelsens balance mellem tekniske og kontekstuelle elementer ved virksomhedernes cybersikkerhedsproblemer. De tekniske elementer omfatter f.eks. konkrete løsninger og trusselsproblematikker, mens de kontekstuelle omfatter forretningsforståelse, forståelse af reguleringsmæssige krav til cybersikkerhed og privacy samt computer- og data-etik. Der er blandt aftagerne efterspørgsel på begge typer kompetencer. De kontekstuelle elementer i cybersikkerhed tilgodeses i uddannelsens projekter, jvf. AAUs problem-baserede læringsform.

[4] Uddannelsens struktur og kompetenceprofil kan fremsendes, hvis dette ønskes.

Aftagerpanelerne fremhæver vigtigheden af en kandidatuddannelse frem for eksempelvis en masteruddannelse. Kandidatuddannelsen i cybersikkerhed giver de studerende de rette metodiske og teoretiske kompetencer, og de adspurgte aftagerne kan forestille sig at ansætte kandidater fra den i den nærmeste fremtid. De understreger også, at engelsk er arbejdssproget i industrien inden for området, ligesom de lægger stor vægt på vigtigheden af at kunne tiltrække internationale studerende for at dække behovet for kandidater. Aftagerne opfordrede derfor til at uddannelsen udbydes på engelsk. Virksomhederne er ikke tilbageholdende med at ansætte engelsksprogede medarbejdere og bl.a. konstateredes det på et af møderne med aftagerne, at "der i forvejen ikke er mange tekniske virksomheder i Danmark, der ikke har engelsksprogede ansatte".

Øvrige dialoger med aftagere
I 2019 har der også været afholdt syv såkaldte meet-ups, som er uformelle møder med deltagelse af industrien og uddannelsens tilrettelæggere. Disse møder er en del af projektet **"**Fremtidens Talenter inden for IT-sikkerhed", der ledes af AAU og finansieret af Industriens fond. Virksomhederne har præsenteret deres syn på uddannelse, talentudvikling og rekruttering inden for cybersikkerhed. Input fra disse arrangementer er indgået i arbejdet med uddannelsen, ikke mindst i forhold til vægtningen mellem teknik og kontekst samt prioriteringen af de forskellige tekniske elementer i uddannelsen.

Der har været afholdt meet-ups med følgende fokus og deltagelse:

- D. 18. februar 2019 i Aarhus. Fokus: People, processes and technology. Deltagelse af Alexandra Instituttet, Jyske Bank og 2600 Security.
- D. 5. marts 2019 i København. Fokus: Fintech. Deltagelse af PII Guard, IBM og JN Data.
- D. 19. marts 2019 i København. Fokus: Maritim og transport. Deltagelse: DSB, Mærsk, DTU.
- D. 10. april 2019 i Aarhus. Fokus: Energisektoren. Deltagelse: Siemens, Vestas, AAU.
- D. 7. maj 2019 i København. Fokus: Konsulent og myndigheder. Deltagelse: Deloitte, NC3 (Rigspolitiet), Center for Cybersikkerhed (Forsvaret).
- D. 8. maj 2019 i Aarhus. Fokus: Informationssikkerhed i organisationer. Deltagelse: Dansk IT, eCrime Labs, Jens Heyn Roed Andersen (konsulent).
- D: 14. maj 2019 i Aalborg. Fokus: Energi og Tele. Deltagelse: TDC, Telenor og SE (Syd Energi).

Udover disse meet-ups har der været afholdt et mere specifikt dialogmøde med henblik på at diskutere virksomhedernes ønsker til uddannelsesinstitutionerne (og uddannelserne) samt få en dialog om, hvordan samarbejdet og mellem virksomheder og universiteter kan øges på cybersikkerhedsområdet. Mødet blev holdt på Aarhus Universitet d. 27. maj 2019 med deltagelse af følgende virksomheder og uddannelsesinstitutioner: Bestseller, Siemens, Salling Group, TDC, Combitech, Vestas, SE, Cyberpilot, JN Data, Devoteam, PwC, Aarhus Universitet, AAU, Erhvervsakademi Dania, Århus Erhvervsakademi og Professionshøjskolen University College Nordjylland.

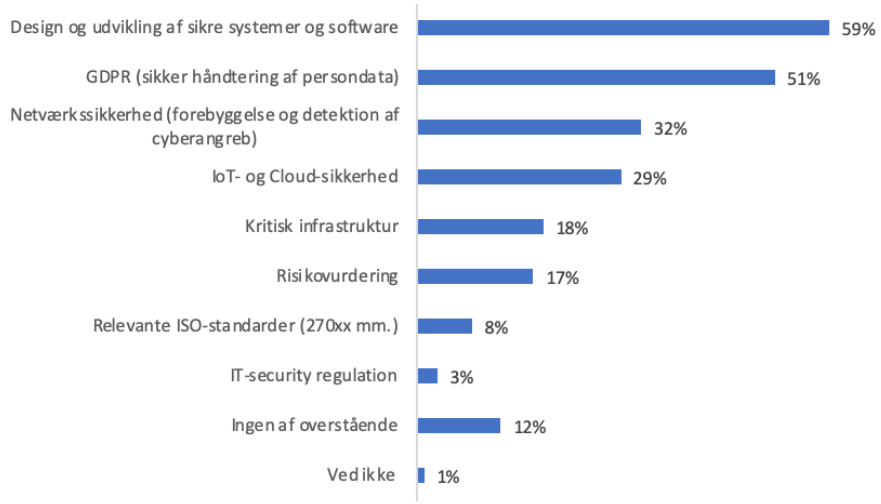
Der har således i arbejdet med udviklingen af kandidatuddannelsen i cybersikkerhed har været en høj grad af involvering fra potentielle aftagere. De er løbende blevet præsenteret for og har forholdt sig aktiv til uddannelsens indhold og formål, og uddannelsens er blevet tilpasset på baggrund af aftagerbidragene, så den modsvarer behovene hos aftagerne.

Sammenhængen mellem uddannelsens kompetenceprofil og uddannelsens erhvervssigte

De uddannede kandidater får en stærk teknisk profil, men også en god forståelse for den kontekst, den tekniske faglighed indgår i. De har således kompetencerne til at omsætte den tekniske viden til udvikling af konkrete løsninger, f.eks. inden for analyse, design og implementering af sikre systemer og software, analyse og håndtering af cybertrusler og forebyggelse, detektion og mitigering af cyberangreb på forskellige typer af såvel simple som komplekse systemer. Derudover vil de kunne arbejde med privacy engineering, adgangskontrol og håndtering af beskyttede ressourcer, IoT- og cloud-baserede systemer og arkitekturer og security governance. Dimittendernes jobfunktioner kan således både omfatte operationelle, analytiske og planlægningsmæssige opgaver.

I det følgende beskrives først, hvilke områder virksomhederne typisk beskæftiger sig med i relation til cybersikkerhed, og hvordan de vigtigste områder understøttes af det faglige indhold i uddannelsen. Efterfølgende gennemgås typiske jobfunktioner i virksomhederne, og hvordan uddannelsen gør det muligt at sigte mod disse med de rette valg af fag projekter.

Arbejdsområder
I Epinions behovsundersøgelse (Bilag 1, s. 8) er virksomhederne er blevet bedt om at angive, hvilke områder de beskæftiger sig med i relation til cybersikkerhed. Nedenstående figur viser en række af de vigtigste områder og andelen af virksomhederne, som beskæftiger sig med disse.



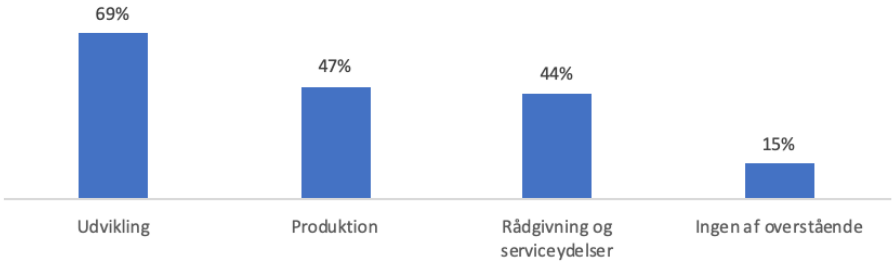
Figur 1: Er din virksomhed beskæftiget med et eller flere af følgende områder? N=120. Kilde: Epinion, s. 8.

I det følgende er der kort redegjort for sammenhængen mellem uddannelsens struktur og virksomhedernes behov som afdækket i figur 1. Der tages udgangspunkt i de seks væsentligste områder, da de øvrige områder kun er nævnt af mindre end 10% af virksomhederne.

- **Design og udvikling af sikre systemer og software**: Dette er en kernekomponent i uddannelsen, og kandidaterne tilegner sig progressivt kompetencer gennem kurset "Secure software development" (1. semester), kurset " Advanced Software Security" (2. semester) samt projektmoduler "Secure systems: Attack and defense" (2 semester). Studerende med særlig interesse for området har mulighed for at vælge at fordybe sig i området gennem kurset "Models of security" (3. semester) samt projektmoduler "Secure systems development" (3. semester).
- **GDPR (Sikker håndtering af persondata):** Datahåndtering er ligeledes en væsentlig komponent i uddannelsen. De studerende undervises både i sikker håndtering af data generelt og mere specifikt i forhold til persondata. Uddannelsen sigter dog på at give de studerende en mere generel metodisk indsigt i problemstillingerne end blot den nuværende persondataforordning (GDPR). Efter den grundlæggende introduktion i "Foundations of security and cryptography" (1. semester) har de studerende, der har interesse for det, mulighed for at følge kurset "Identity and access management" (2. semester). Der er mulighed for at fortsætte fordybelsen på 3. semester med kurserne "Privacy engineering" og/eller de reguleringsmæssige aspekter i "IT security regulation" og "Enterprise security and compliance". Ligeledes giver projektmoduler på 3. semester mulighed for at fordybe sig i "Security Governance".
- **Netværkssikkerhed (forebyggelse og detektion af cyberangreb):** Dette er også en kernekomponent i uddannelsen, hvor kandidaterne ligesom med sikker software vil opleve en progression gennem studiet. I kurset "Foundations of security and cryptography" (1. semester) får de studerende de grundlæggende forudsætninger, der skal til for at arbejde videre med sikkerhed i netværk og distribuerede systemer i samme semesters projekt "Distributed systems security". På 2. semester fortsætter progressionen med kurset "Hacker space", der også understøtter semestrets projektmoduler "Secure systems: Attack and defense", hvor der fokuseres på både netværkssikkerhed og sikker software. De studerende, der ønsker det, kan allerede på 2. semester vælge at fokusere på maskinlæringsbaserede værktøjer. Emner relateret til den nyeste forskning inden for netværkssikkerhed er væsentlige i kurset "Advanced topics in cyber security" på 3. semester.
- **IoT- og Cloud-sikkerhed:** Dette dækkes fra starten af uddannelsen i kurset "Security in IoT and cloud architectures". Derudover indgår aspekter af IoT- og cloud-sikkerhed naturligt i kurser og projekter der omhandler netværk og distribuerede systemer, herunder projektmodul på 1. og 2. semester samt kurset i "Advanced topics in cyber security" på 3. semester.
- **Kritisk infrastruktur:** Rent metodisk adskiller beskyttelse af kritisk infrastruktur sig ikke fra øvrige systemer, men da konsekvenserne af angreb kan være voldsomme vil der oftest vælges en tilgang, hvor sikkerhed prioriteres højt i forhold til f.eks. økonomi og brugeroplevelse. Området dækkes derfor i en kombination af ovenstående tekniske discipliner (netværkssikkerhed og udvikling af sikre systemer/software), kurserne i reguleringsmæssige aspekter ("IT security regulation" og "Enterprise Security and Compliance") samt projektmodulerne på især 3. semester, hvor de studerende får mulighed for løse mere komplekse problemstillinger ved at kombinere viden fra disse forskellige områder (enten med et teknisk fokus, eller med et governance-fokus).
- **Risikovurdering:** Risikovurdering indgår i mange af uddannelsens elementer, da det er et væsentligt aspekt i at analysere en problemstilling med henblik på at udvikle løsninger. Risikovurdering er således eksplicit fremhævet i læringsmålene for en række af uddannelsens elementer på den sidste del af uddannelsen -

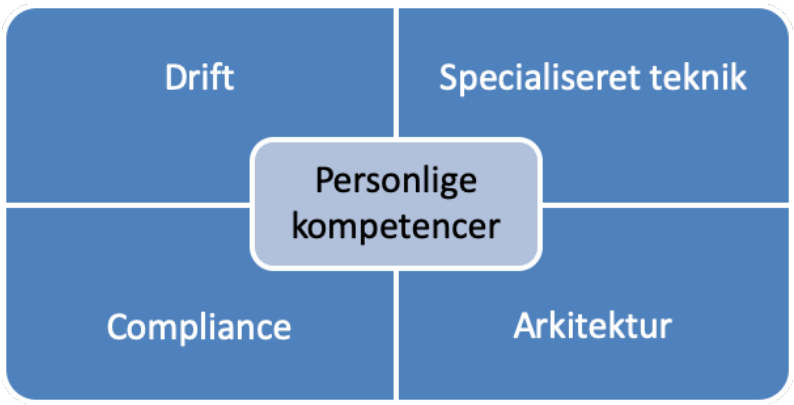
herunder “Secure systems developement”, “Security Governance”, “IT security regulation”, “Enterprise Security and Compliance” og “Privacy Engineering”.

Jobfunktioner
Cybersikkerhed indgår oftest i udviklingsområderne i virksomhederne, men også i produktion og som en del af rådgivning eller serviceydelser som vist i Figur 2, (se Bilag 1, s.9). Hertil udspørges virksomhederne om erhvervslivets aktuelle og fremtidige behov for ingeniører eller andre med længerevarende IT-uddannelser med stærke kompetencer inden for cybersikkerhed til at varetage ovenstående arbejdsområder.



Figur 2: Indgår cybersikkerhed i et eller flere af følgende områder i virksomhedens arbejde? N=120. Kilde: Epinion, s. 9

Epinions rapport identificerer fire forskellige typer arbejdsfunktioner inden for cybersikkerhed som vist i Figur 3 (Bilag 1, s. 14) Gennemgående for alle typer funktioner er dog, at virksomhederne samtidig efterspørger visse personlige kompetencer, der ikke knytter sig specifikt til det faglige.



Figur 3: Funktioner for medarbejdere med kompetencer inden for cybersikkerhed. Kilde: Epinions, s.14

De fire jobfunktioner karakteriseres som følger:

- Profiler, der arbejder med **drift**, skal overordnet set sørge for, at virksomheden fungerer i dagligdagen. De skal sørge for den daglige drift af systemerne og f.eks. implementere nye systemer, der er udviklet af andre, som købes til virksomheden. Vigtige kompetencer i denne funktion er f.eks netværksovervågning og drift af servere. Det er typisk større private virksomheder, der har brug for denne type medarbejdere.
- Profiler, der arbejder med **specialiseret teknik**, er 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, der varetages af disse medarbejdere. Medarbejdere af denne type er oftest eftertragtede af private IT-virksomheder eller offentlige organisationer, der beskæftiger sig med sikkerhed.
- Profiler, der arbejder med **compliance**, skal overordnet sørge for, at virksomhedens cybersikkerhed lever op til de krav, love og reguleringer, der er gældende for virksomhedens produkter og services. Denne type medarbejdere skal have en vis juridisk viden samt forståelse for de relevante krav og reguleringer og mulighederne for at kunne leve op til disse. Denne type medarbejder efterspørges primært af større og sommetider internationale private virksomheder, der har behov for in-house viden om dette område, idet de ofte arbejder i flere lande, hvor der er mange forskellige reguleringer. Niveauet af reguleringer er dertil stærkt stigende i løbet af de seneste år, hvilket øger behovet for denne type medarbejdere.
- Profiler, der arbejder med **arkitektur**, arbejder på et mere overordnet niveau, hvor de skal koble sikkerheden i virksomhederne med forretningens behov og strategi. Disse medarbejdere skal have 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 har brug for denne type medarbejdere, der kan arbejde et niveau "højere" end de tekniske specialister eller driftsmedarbejdere og være tættere på det strategiske niveau i virksomheden.

På tværs af de fire typer funktioner gælder det, at virksomhederne efterspørger personlige kompetencer hos medarbejderen. Dette kan være kompetencer som omgængelighed, positiv indstilling, kommunikative evner mv. Virksomhederne ser således ikke kun på de faglige færdigheder hos medarbejderen, men også hvordan det personlige aspekt vil passe ind i virksomheden eller den pågældende afdeling. Der er således et præcist forhold mellem uddannelsens kombination af teknisk specialiserede kurser, de valgfrie kurser samt de dybtgående projekter, og aftagernes behov for kandidater, der med en dyb teknisk viden har blik for dén forretningsmæssige kontekst, som cybersikkerhed indgår i.

Udover de af Epinion identificerede fire arbejdsfunktioner, kan en femte arbejdsfunktion identificeres.

- Dialogen med aftagere og netværk, bl.a. de tidligere omtalte møder i forbindelse med projektet "Fremtidens Talenter inden for IT-sikkerhed", har afdækket **konsulentrollen** som endnu en væsentlig jobprofil. Konsulentrollen findes i flere formater, herunder både generalist og specialist, og i både små og store konsulenthuse. For konsulenterne fremhæves særligt viden om kommunikation, forretningsforståelse og compliance, hvilket er afdækket i uddannelsens læringsmål. Konsulenterne har brug for en dyb teknisk viden om cybersikkerhed for at kunne foretage risikovurderinger og identificere kritiske sårbarheder inden for områder som f.eks. virksomhedens it-arkitektur, samspil med cloud-leverandører og forretningspartnere, forretningsprocesser og håndtering af kundeinformation. PwC, Omada og NNIT er eksempler på aftagere, der efterspørger disse kompetencer.

De fem typer arbejdsfunktioner afspejles i uddannelsens kompetenceprofil. Nedenstående liste giver et overblik over hvilke kompetencer, der knytter sig til de fem identificerede arbejdsfunktioner (Bilag 1, s. 14). Det bemærkes dels, at alle fem arbejdsfunktioner er vel understøttet af uddannelsens kompetenceprofil, og at hvert element fra kompetenceprofilen understøtter mindst en af nedenstående jobfunktioner.

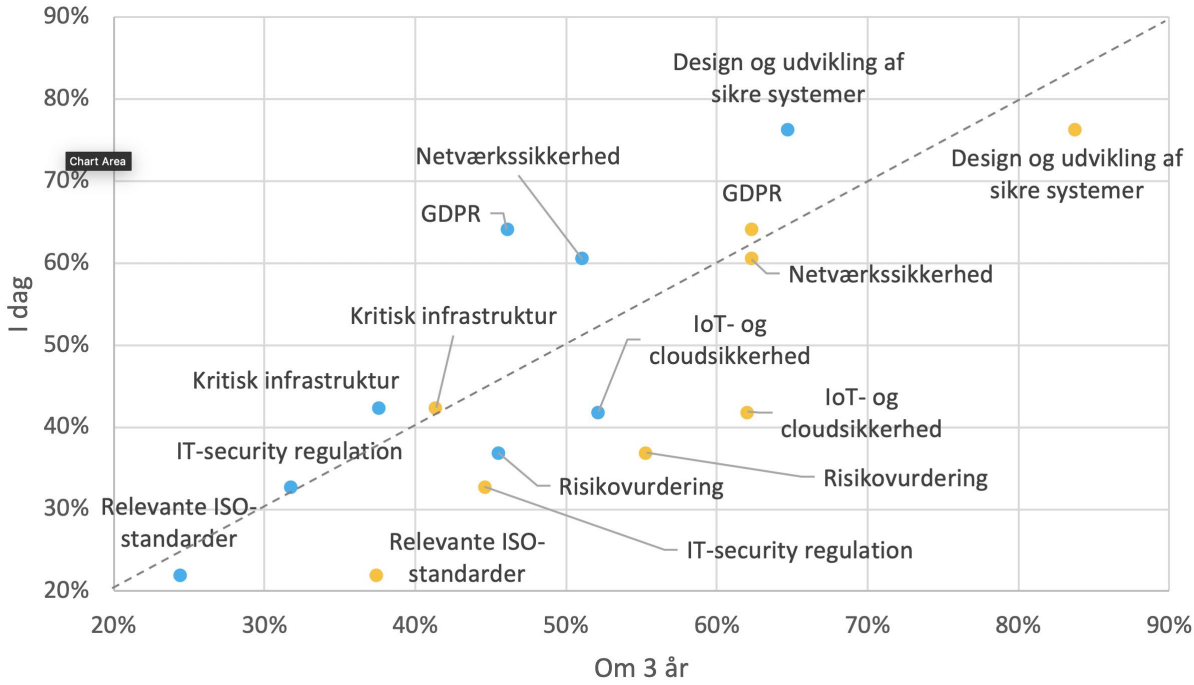
- Arbejdsfunktion **Drift:**
  Denne jobfunktion understøttes i særlig grad af de elementer fra kompetenceprofilen, der omhandler risikovurderinger, risikoanalyse, analyse af komplekse sikkerhedsproblemstillinger, netværkssikkerhed, enterprise security, monitorering og analyse af netværkstrafik, sikkerhedsanalyse- og evaluering, identity- and access management, identifikation af angribere samt evnerne til at analysere og forstå organisationers behov i forhold til cybersikkerhed.
- Arbejdsfunktion **Specialiseret teknik:**
  Følgende elementer fra kompetenceprofilen understøtter i særlig grad denne jobfunktion: Analyse af komplekse problemer i relation til sikkerheden i systemer (IoT, Cloud, distribuerede systemer, embeddede systemer) og design af sikre distribuerede løsninger, forskningsbaseret viden inden for en række centrale tekniske områder (netværkssikkerhed, design af sikre systemer og sikker software, sikkerhed i IoT og Cloud, modeller for softwaresikkerhed), monitorering og analyse af netværkstrafik, konfiguration og operation af sikre testmiljøer, forstå, analysere, vurdere, udvælge og evaluere teknologier. Det vurderes også for denne arbejdsfunktion særligt relevant selvstændigt at kunne tilegne sig og forstå den nyeste forskningsmæssige viden, og at kunne omsætte denne viden til konkrete løsninger.
- Arbejdsfunktion **Compliance:**
  Følgende elementer fra kompetenceprofilen understøtter i særlig grad denne jobfunktion: Risikovurderinger, sikkerhed i IoT og Cloud arkitektur, privacy engineering, enterprise security, IT security regulation and governance, identity and access management, authentication og adgangskontrol samt analyse af cybersikkerhedsbehov i organisationer.
- Arbejdsfunktion **Arkitektur:**
  Følgende elementer fra kompetenceprofilen understøtter i særlig grad denne jobfunktion: Design af sikre distribuerede løsninger, implementering af distribuerede systemer med fokus på sikkerhed, sikkerhed i IoT- og Cloud-arkitekturer, design af sikre systemer og software, privacy engineering, enterprise security, modeller af softwaresikkerhed, sikkerhedsanalyse og evalueringer, analysere cyber-risici, kombinere viden om forskellige teknologier og enheder samt kompetencer i at vurdere, udvælge og anvende relevante metoder til at sikre systemer.
- Arbejdsfunktion **Konsulent:**
  Konsulentrollen kan som nævnt være både generalist og specialist og afhængigt heraf gøre brug af forskellige kompetencer. Ud over de allerede nævnte arbejdsfunktioner efterspørges, der kompetencer relateret til hhv. dyb specialistviden og kommunikation, forretningsforståelse og compliance. Dermed vil følgende elementer fra kompetenceprofilen i særlig grad understøtte denne funktion: Forskningsbaseret viden om netværkssikkerhed, design af sikre systemer og sikker software, sikkerhed i IoT og Cloud-arkitekturer og risikoanalyse, viden om teorier og modeller til at udføre sikkerhedsanalyser og evalueringer, viden om forsknings- og udviklingsmæssige udfordringer i forhold til cybersikkerhed, kompetencer inden for

sikkerhedstesting af systemer - samt Enterprise Security, risikovurdering og IT-sikkerhedsregulering og governance. Forretningsforståelse afdækkes af kompetencebeskrivelsens elementer om at analysere cyberrisiko og identificere cybersikkerhedsbehovet i organisationer, og kommunikationsaspektet dækkes gennem formidling af projektarbejdet.

Uddannelsen er inspireret af den internationale udvikling inden for området. I 2017 udgav Association for Computing Machinery (ACM) sammen med bl.a. IEEE Computer Society en rapport med anbefalinger til indholdet af nye uddannelser om cybersikkerhed[5]. Rapporten nævner en lang række vigtige "knowledge areas": data security, software security, component security, connection security, system security, human security, organizational security, og societal security. Disse områder berøres direkte eller indirekte i den nye uddannelse.

Fremtidige kompetencebehov

I den kvantitative undersøgelse fra Epinion blev de 120 virksomheder spurgt til hvilke konkrete, **tekniske kompetencer,** de anser som vigtige i dag og hvilke, der regnes for at være vigtige om tre år. Figur 4 illustrerer de anvendte kompetencer i dag (den lodrette akse) i forhold til kompetencebehovet om tre år (den vandrette akse) blandt virksomhederne. De kompetencer, som den foreslåede uddannelse giver kandidaterne, vil blive stadigt stigende efterspurgt (se Bilag 1, s. 15). Som det fremgår, vil kompetencer, der kombinerer specifik teknisk viden med generel forståelse, møde en stigende efterspørgsel. Disse vurderinger er kombineret i figuren nedenfor, hvor kompetencer i den nederste, højre halvdel forventes at være mere vigtige om tre år end nu.



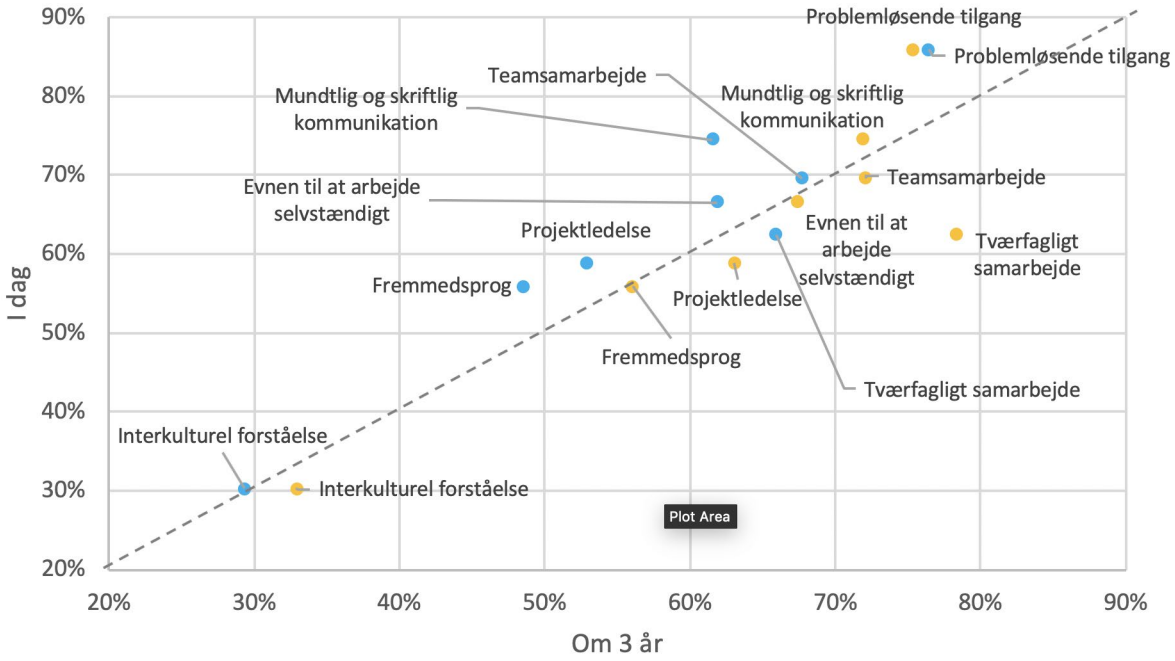
Figur 4: Faglige og tekniske kompetencer for cybersikkerhedsingeniører i dag og om tre år.
N: De gule prikker er baseret på besvarelser fra de 49 respondenter, der har angivet på nuværende tidspunkt at have en eller flere medarbejdere ansat med kompetencer inden for cybersikkerhed. De blå prikker er baseret på samme respondenters vurdering af kompetencebehovet i dag, men på alle virksomheders vurdering af behovet om tre år (N=49/120). Kilde: Epinion, s. 15.

De fleste kompetencer forventes at blive mere relevante inden for de næste tre år, end de allerede er i dag – i hvert fald hvis man ser på de virksomheder, der på nuværende tidspunkt har medarbejdere med kompetencer inden for cybersikkerhed ansat. Disse virksomheder ser både design og udvikling af sikre systemer, netværkssikkerhed, IoT- og Cloud-sikkerhed, risikovurdering, IT-security regulation samt relevante ISO-standarder som værende mere relevante om tre år end tilfældet er nu. Særligt IoT- og Cloud-sikkerhed og risikovurdering forventes at blive betydeligt mere vigtige fremadrettet, men design og udvikling af sikre systemer vurderes fortsat – både i dag og om tre år – som den vigtigste kompetence for disse virksomheder. Samlet set viser figuren således en generel forventning til, at langt de fleste faglige og tekniske kompetencer vil blive mere efterspurgte i fremtiden.

Når det kommer til de anvendte **organisatoriske kompetencer**, forventes de fleste kompetencer at være lige så relevante fremadrettet, som de er i dag. Behovet for de enkelte kompetencer er illustreret i Figur 5 nedenfor.

[5] "Cybersecurity curricula 2017", ACM Computing Curricula Series, Joint Task Force on Cybersecurity Educations, Dec. 2017. https://cybered.hosting.acm.org/wp/wp-content/uploads/2018/02/csec2017_web.pdf.

For alle virksomheder gælder det, at en problemløsende tilgang er den vigtigste organisatoriske kompetence at besidde både i dag og om tre år. At kunne samarbejde med andre fagligheder er desuden en kompetence, der forventes at blive betydeligt mere relevant om tre år, end den allerede er i dag, især hos de virksomheder, der allerede har ansatte inden for cybersikkerhed. Hos disse virksomheder er projektledelse også en kompetence, der fremadrettet forventes at blive større efterspørgsel efter. Der kan således med fordel arbejdes på at sikre, at kandidaterne i cybersikkerhed udvikler deres evner inden for dels tværfagligt samarbejde og teamsamarbejde samt projektledelse fremadrettet (se bilag 1, s.16).



Figur 5: Organisatoriske kompetencer for cybersikkerhedsingeniører i dag og om tre år.
N: De gule prikker er baseret på besvarelser fra de 49 respondenter, der har angivet på nuværende tidspunkt at have en eller flere medarbejdere ansat med kompetencer inden for cybersikkerhed. De blå prikker er baseret på samme respondenters vurdering af kompetencebehovet i dag, men på alle virksomheders vurdering af behovet om tre år (N=49/120). Klide: Epinion, s. 16.

Epinions behovsundersøgelse understøtter ligeledes behovet for en engelsksproget uddannelse, som også blev fremhævet på møderne med aftagerpanelerne (se Bilag 1, s. 17). 64% af virksomhederne er i nogen eller høj grad interesserede i at ansætte ingeniører med kompetencer i engelsk i virksomheden i fremtiden. Det er særligt virksomheder, der allerede har engelsksprogede ingeniørfaglige medarbejdere ansat, der er interesserede i at ansætte flere engelsksprogede medarbejdere. 91% af disse virksomheder er interesserede i at ansætte flere engelsksprogede medarbejdere, mens dette kun gør sig gældende for 46% af de virksomheder, der ikke har engelsksprogede ansat på nuværende tidspunkt.

Hvor attraktive er kandidaterne fra uddannelsen?

76% af de adspurgte virksomheder vurderer, at ingeniører i cybersikkerhed fra AAU enten i nogen eller i høj grad vil være relevante at ansætte i deres virksomhed nu eller i fremtiden (se Bilag 1, s.18). 13% af virksomhederne mener dette i lav grad, mens kun 1% angiver, at kandidater med uddannelsen slet ikke vil være relevante for deres virksomhed. Det tyder således på, at der er et stort antal virksomheder i de relevante brancher, som vil være interesserede i kandidater fra cybersikkerhedsuddannelsen. De store virksomheder er de mest positive overfor at ansætte kandidater med en uddannelse i cybersikkerhed fra AAU, mens de mellemstore (20-99 ansatte) er de mindst positive.

I dybdeinterviewene med potentielle aftagervirksomheder er der generelt stor tilfredshed med kompetenceprofilen og uddannelsens planlagte opbygning. Stort set alle virksomheder vurderer, at kandidater med en sådan profil kan være relevante i deres virksomhed og opfylde de behov, de overordnet set efterspørger. Det tyder således på, at en profil som denne vil være relevant for alle tre typer virksomheder tidligere præsenteret, men også for de fire forskellige funktioner beskrevet tidligere. Det påpeges dog, at hvis kandidaten skal sidde i en specialistrolle, vil yderligere specialisering formentlig være nødvendig.

I denne forbindelse giver uddannelsen mulighed for, at den studerende tidligt i forløbet kan sigte mod den mest attraktive jobfunktion ved at vælge fag og projekter på 2. og 3. semester, der i særlig grad understøtter denne.

Behovet for forretningsforståelse og blødere kompetencer

De fleste virksomheder, som omfatter otte større danske virksomheder, efterspørger desuden særligt mere forretningsforståelse hos kandidaterne. Der er således en opfattelse af, at kandidaterne bliver dækket ind på de fleste nødvendige tekniske og faglige kompetencer, men at de med fordel også kunne få bedre forståelse for, hvordan virksomheder og offentlige institutioner fungerer og cybersikkerhedens rolle i virksomheden.

Der skelnes generelt mellem to typer af kompetencer, når virksomhederne taler om kompetencer for cybersikkerhedsingeniører. Groft set er der de tekniske kompetencer, eksempelvis hacking og machine learning, og så er der de mere "bløde" kompetencer såsom håndtering af persondata og governance (se Bilag 1, s.19-20). De fleste virksomheder foretrækker en kandidat, der primært har dækket de tekniske kompetencer, men som også har forståelse for de mere "bløde" områder, og på den måde har en holistisk forståelse for sikkerhed, mens enkelte virksomheder foretrækker dog kandidater, hvor den bløde sikkerhed er nedtonet.

Flere virksomheder efterspørger mere fokus på de blødere emner både governance og persondatahåndtering, men også ledelse, etik og juridisk viden er områder, der ønskes viden om blandt kandidaterne. Disse kompetencer er særligt relevante for kandidater, der blandt andet skal arbejde med compliance, men også som en del af den holistiske forståelse for sikkerhed blandt andre typer profiler.

Overordnet set synes uddannelsens kompetencer at stemme godt overens med de relevante funktioner, som kandidaterne kan komme ud til på arbejdsmarkedet og hermed virksomhedernes behov. Kompetencerne taler dog umiddelbart bedst ind i en drift- eller arkitektfunktion, men kan med mindre justeringer eller yderligere specialisering i virksomhederne også varetage compliance- eller specialistroller (se Bilag 1, s. 21).

Opsummerende er der således ingen af de fire funktioner i Figur 3, som en kandidat i cybersikkerhed ikke forventes at kunne udfylde, men kompetenceprofilen lægger umiddelbart en lille smule bedre til drift- og arkitektur-medarbejdere ifølge de potentielle aftagervirksomheder. Idet der kun er tale om kandidatuddannelsen, kan den forudgående bacheloruddannelse også have indflydelse på kandidatens samlede profil, og dermed sagtens indgå i en funktion i forhold til compliance eller mere specialiserede arbejdsopgaver.

Adgangskravet til uddannelsen vil være en teknisk-videnskabelig bachelorgrad i software, datalogi, computerteknologi eller netværksteknologi. Sammen med en kandidatuddannelse i cybersikkerhed vil dimittenderne have opnået solide IT-kompetencer, som gør dem egnede til at varetage de krævede opgaver.

Aalborg Universitet vurderer således, at uddannelsens kompetenceprofil afspejler en balance i forhold til erhvervssigtet, og at der er sammenhæng mellem uddannelsens kompetenceprofil og uddannelsens erhvervssigte.

Vurdering af det samfundsmæssige behov for uddannelsen

I det følgende redegøres der for, hvordan AAU har vurderet det samfundsmæssige behov for uddannelsen, dvs. balancen mellem på den ene side arbejdsmarkedets behov for kompetencerne og på den anden side udbuddet af beslægtede eksisterende uddannelser og den nye uddannelse.

Cybersikkerhed er et kraftigt ekspanderende område både globalt og nationalt. Dette gælder ikke mindst inden for IoT, som mange virksomheder anvender i dag. Ifølge Gartner vurderes det, at markedet for IoT-sikkerhedsløsninger vil vokse fra 912 mill. $ i 2016 til 3.1 mia. $ i 2021 – dvs. med over 25% årlig vækst[6]. Ifølge det danske konsulentfirma Damvad vil det globale marked for IT-sikkerhed være vokset til 248 mia. $ i 2023[7].

I Danmark er der allerede i dag er 2.900 beskæftiget i selve den danske IT-sikkerhedsbranche fordelt på 263 virksomheder. Damvad vurderer, at branchen har et højt vækstpotentiale både i Danmark og i udlandet, men at branchens vækst er hæmmet af mangel på arbejdskraft. Det største behov for IKT-specialister med IT-sikkerhed som speciale ligger imidlertid uden for selve sikkerhedsbranchen. Ifølge Center for Cybersikkerhed vurderes truslen fra cyberspionage og cyberkriminalitet som værende meget høj[8]. Der er således et akut behov for, at myndigheder og virksomheder opruster deres sikkerhedsberedskab.

I behovsundersøgelsen fra Epinion (se Bilag 1) er der foretaget analyser af uddannelsesstatistiske kilder for at skabe et nationalt overblik over cybersikkerhed og beslægtede uddannelser. Den overordnede mangel på ingeniører og naturvidenskabelige kandidater og andre IKT-specialister fremgår af tre grundige analyser og fremskrivninger foretaget i de seneste år. Undervisnings-og Forskningsministeriet har løbende udarbejdet udbudsfremskrivninger bl.a.

[6] https://www.gartner.com/en/newsroom/press-releases/2018-03-21-gartner-says-worldwide-iot-security-spending-will-reach-1-point-5-billion-in-2018

[7] Damvad analytics (2019). "Den danske IT- sikkerhedsbranche".

[8] Center for Cybersikkerhed (2019). "Trusselsvurdering: Cybertruslen mod Danmark 2019". https://fe-ddis.dk/cfcs/publikationer/Documents/Cybertruslen-mod-Danmark-2019.pdf

til udvalget vedrørende kvalitet i uddannelsessystemet. DI og IDA har for Engineering the Future fremskrevet manglen på ingeniører og naturvidenskabelige kandidater. Endelig leverede en omfattende analyse af behovet for digitale kompetencer udarbejdet af Erhvervsstyrelsen, UFM og UVM detaljerede langfristede fremskrivninger for IKT-kandidater.

I nedenstående beregning er der taget højde for de nyeste optagelsestal i 2018, den nyeste studieadfærd mht. søgning, optag og fuldførelsesprocenter samt den seneste beskæftigelsesudvikling (se Bilag 1, s. 6).

	2020	2025
Efterspørgsel ingeniører og naturvidenskabelige kandidater	130.000	150.000
Udbud ingeniører og naturvidenskabelige kandidater	123.000	140.000
Mangel ingeniører og naturvidenskabelige kandidater	7.000	10.000

Tabel 1: Beregning af mangel på ingeniører og naturvidenskabelige kandidater på BSc- og MSc-niveau i 2020 og 2025. Kilde: Beregnet af Epinion på grundlag af data fra IDA og DI 2015 og 2018 s. 6

Der er med nedenstående tabel beregnet en stor mangel på civilingeniører med specialisering i cybersikkerhed også i Danmark. I udbuddet er inkluderet ingeniører eksempelvis fra DTU, som har taget efteruddannelse inden for cybersikkerhed.

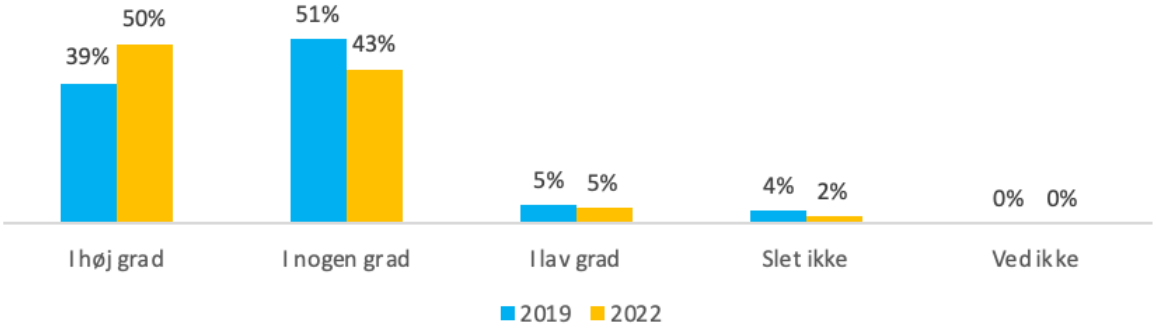
Det kan bemærkes, at der er betydelige substitutionsmuligheder mellem ingeniører, dataloger og andre. I nedenstående regneeksempel er indregnet horisontal substitution mellem de forskellige uddannelseskategorier: ingeniører, dataloger eller andre med længerevarende IT-uddannelser (se Bilag 1, s. 7).

	2020	2025
Efterspørgsel efter ingeniører spec. i cybersikkerhed	1.600	3.400
Udbud af ingeniører specialiseret i cybersikkerhed	1.500	3.000
Mangel	100	400

Tabel 1: Regneeksempel på udbud og efterspørgsel af civilingeniører med speicalisering i cybersikkerhed. Kilde: Epinions, 2.

I Tabel 4 vises det forventet behov hos de virksomheder, der er blevet spurgt i forbindelse med undersøgelsen af behovet for specialister i cybersikkerhed. Sammenholdes denne med overstående regneeksempel, som kun går på den type civilingeniører, AAU vil uddanne, er der ganske god overensstemmelse.

Epinions behovsundersøgelse peger også på et stigende behov for medarbejdere med længerevarende tekniske uddannelser med kompetencer inden for cybersikkerhed, som gengivet i figuren nedenfor (se Bilag 1, s. 10).



Figur 6: I hvilken grad vurderer du, at der i din virksomhed i dag/inden for de næste tre år vil være større behov for ingeniører, dataloger eller andre med længerevarende IT-uddannelser med kompetencer inden for cybersikkerhed? N=120. Kilde: Epinion, s. 10

Her ses det, at efterspørgslen på kandidater med en kompetenceprofil tilsvarende dimittender fra kandidatuddannelsen i cybersikkerhed, fra erhvervslivet, både aktuelt og fremtidigt, langt overvejende falder i kategorierne "I høj grad" eller "I nogen grad".

Beslægtede uddannelser
En række kandidatuddannelser indeholder elementer af cybersikkerhed i form af enkeltkurser og fagprofiler, men danske universiteter tilbyder for nærværende ikke nogen kandidatuddannelse, der har cybersikkerhed som det centrale omdrejningspunkt. Uden for AAU's regi findes f.eks. professionsbacheloruddannelser i IT-sikkerhed på KEA EA og en kommende efteruddannelse i cybersikkerhed på DTU. Desuden tilbydes efteruddannelse i form af enkeltkurser på Teknologisk Institut o. lign. En detaljeret analyse af disse uddannelser er gengivet i ansøgningen.

Ledighedsfrekvensen for dimittender fra beslægtede uddannelser

Som et led i afdækningen af det samfundsmæssige behov for en kandidatuddannelse i cybersikkerhed er ledighedsfrekvensen for dimittender fra beslægtede kandidatuddannelser blevet undersøgt via udtræk fra Uddannelses- og Forskningsministeriets datavarehus. Følgende kandidatuddannelser er blevet inddraget:

- **Aalborg Universitet (AAU):**
  Communication Technology, Innovative Communication Technologies and Entrepreneurship, Datalogi, Software, Computer Science (IT)
- **Danmarks Tekniske Universitet (DTU)**:
  Computer Science and Engineering, Digitale medieteknologier, Informationsteknologi, Matematisk modellering og computing, Telekommunikation
- **IT-Universitetet (ITU):**
  Datalogi, Softwaredesign
- **Københavns Universitet (KU):**
  Datalogi
- **Syddansk Universitet (SDU):**
  Software engineering, data science, datalogi
- **Roskilde Universitetscenter (RUC):**
  Computer science (Datalogi) + Informatik
- **Aarhus Universitet (AU):**
  Datalogi, Cognitive Science (Kognitionsvidenskab), Computerteknologi, Elektroteknologi, Informationsteknologi - it, kommunikation og organisation, it-produktudvikling (EN)

Blandt disse uddannelser er nogle dog så nye, at der endnu ikke findes ledighedstal herfor, men nedenstående Tabel 2 vises ledighedsfrekvens og antal dimittender for de fleste af uddannelserne i perioden 2011-2016.

Tallene understreger den meget lave ledighedsfrekvens blandt dimittender med beslægtede uddannelser.

	2011		2012		2013		2014		2015		2016	
	Ledighed	Fuldførte	Ledighed	Fuldførte	Ledighed	Fuldførte	Ledighed	Fuldførte	Ledighed	Fuldførte	Ledighed	Fuldførte
Datalogi (computer science). UDDkode: 8081												
KU	2,4 %	63	1,0 %	38	5,2 %	54	1,2 %	55	2,6 %	60	1,2 %	53
RUC			24,2 %	6	21,1 %	5						
SDU	5,1 %	7	0,0 %	7	0,8 %	11	0,4 %	10	2,9 %	17	0,0 %	17
AU	2,1 %	47	1,7 %	33	5,4 %	36	5,3 %	42	1,8 %	64	4,1 %	64
AAU Aalborg	4,9 %	22	3,5 %	16	0,4 %	13	5,9 %	18	1,2 %	22	2,7 %	32
Datalogi (IT) (computer science (IT)). UDD kode: 8073												
AAU Aalborg									0,0 %	5		
Digitale medioteknologier. UDD kode: 5242												
DTU									3,2 %	38	5,2 %	44
Matematisk Modellering og Computing. UDD kode: 8020												
DTU									2,5 %	68	1,1 %	76
Software Engineering. UDD kode: 5397												
SDU									1,0 %	8	0,0 %	11
ITU	14,9 %	53	3,2 %	59	6,7 %	64	4,7 %	86	3,8 %	93	1,8 %	108
Networks and distributed systems. UDD kode: 5214												
AAU Aalborg									0,0 %	9	0,2 %	8
ICTE. UDD kode: 8344												
AAU København									18,8 %	19	5,4 %	10
Software. UDD kode: 3106												
AAU Aalborg									1,0 %	34	5,5 %	36
Informationsteknologi. UDD kode: 3222												
DTU									0,1 %	83	0,8 %	101
Telekommunkation. UDD kode: 8308												
DTU							8,5 %	27	1,2 %	14	7,2 %	22
Computerteknologi. UDD kode: 5271												
AU	5,3 %	18	0,0 %	24	8,4 %	25	7,1 %	24	6,3 %	35		
Computerteknologi. UDD kode: 3340												
AU											5,4 %	31
Elektroteknologi. (cand.polyt). UDD kode: 6269												
AU									11,9 %	5	0,0 %	8
DTU									4,2 %	97	5,1 %	69
Elektroteknologi. (cand.scient.tech). UDD kode: 6270												
AU											16,3 %	6
It, Kommunikation og organisation. UDD kode: 8229												
AU, School of business and social sciences	9,7 %	27										
AU			9,0 %	63	8,4 %	53	8,3 %	85	2,4 %	75	6,9 %	99
IT-produktudvikling. UDD kode: 3347												
AU											16,7 %	39
IT-produktudvikling. UDD kode: 8349												
AU					0,0 %	5	7,7 %	17	10,4 %	31		
SDU							9,0 %	27				

Kilde: Uddannelses- og Forskningsministeriets datavarehus, dataudtræk fra kuben ElevLedighed d.10.07.2019, 12-08-2019 og 21.08.2019

Tabel 3: Ledighedsfrekvens i 4.-7. kvartal efter dimission og antal dimittender fra beslægtede kandidatuddannelser[9].

Forklaring til Tabel 3:

'Ledighed' angiver den gennemsnitlige ledighedsgrad i 4.-7. kvartal efter fuldførelse. De nyeste tal er fra 2016 (dimittendårgang).

'Fuldførte' angiver antallet af fuldførte per år (dimittendår). Der tages udgangspunkt i fuldførte i perioden 1. oktober året før til 30. september i året.

Der tages udgangspunkt i bruttoledigheden. For at blive defineret som bruttoledig skal den fuldførte være uden arbejde og stå til rådighed for arbejdsmarkedet og modtage dagpenge, kontanthjælp eller starthjælp. Fuldførte, der er i gang med en ny uddannelse eller udvandret, regnes som ikke-ledige.

Hvis antallet af fuldførte i en celle er 4 individer eller derunder, vises antallet ikke. Dette gælder også for beregninger pba. heraf.

På denne baggrund vurderer AAU, at dimittender fra en kandidatuddannelse i IT-sikkerhed hurtigt vil komme i beskæftigelse.

Behovet for uddannelsen på det fremtidige arbejdsmarked

I maj 2018 udgav Finansministeriet en rapport om regeringens nationale strategi for cyber- og informationssikkerhed[10]. Heri konkluderer man, at forbedret informations- og cybersikkerhed er essentiel både for Danmarks konkurrenceevne og for samfundets stabilitet. Med den høje grad af digitalisering i samfundet kommer imidlertid også en øget risiko for cyberangreb. Samtidigt bliver de samfundsmæssige implikationer af angreb og nedbrud større. Ifølge rapporten kan sårbarhederne for danske virksomheder og offentlige myndigheder især tilskrives flg. faktorer:

[9] Note til Tabel 2: Der forefindes ingen oplysninger om ledighedsgrad eller antal dimittender i kuben ElevLedighed i Datavarehuset for Softwareudvikling. UDD kode: 6265 (Softwareudvikling (design). Dog forefindes data på Softwareudvikling, som er indsat i denne tabel).

[10] "Danish Cyber and Information Security Strategy", Finansministeriet, maj 2018, https://digst.dk/media/16943/danish_cyber_and_information_security_strategy_pdfa.pdf.

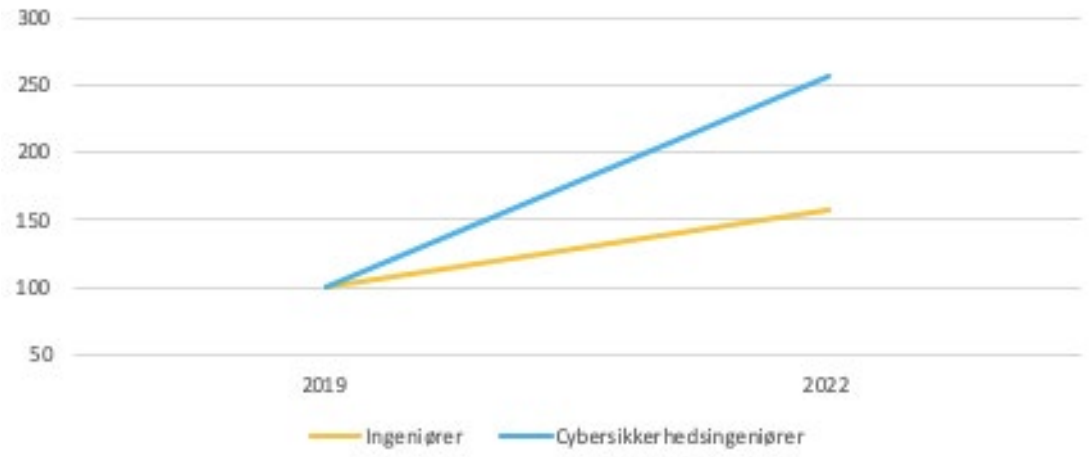
1. en utilstrækkelig sikkerhedskultur,
2. en høj afhængighed af digital infrastruktur,
3. et stigende antal forbundne enheder (f.eks. IoT devices),
4. en høj kompleksitet i porteføljen af digitale services, der anvendes, i kombination med forældede IT-systemer og
5. cyberangreb kan gennemføres nemt og billigt via værktøjer på internettet.

Cyberangreb kan ramme alle dele af samfundet, og konsekvenserne kan række fra økonomiske tab til - i værste fald - tab af menneskeliv.

Der er imidlertid kraftig mangel på veluddannet kvalificeret arbejdskraft inden for området. Både specialiserede IT- og cybersikkerhedsvirksomheder, almindelige virksomheder og offentlige organisationer oplever et stadigt voksende rekrutteringsproblem. Kandidater med specialiserede tekniske kompetencer er efterspurgte, men mange virksomheder ønsker også disse kompetencer forbundet med en forretnings- og organisationsforståelse. Der er brug for 'brede specialister'.

AAU er forpligtet til at sikre, at det uddanner studerende til fremtidens samfund. Dette indebærer, at det bidrager til at imødegå behovet for ingeniører med en flerfaglig forståelse af cybersikkerhed og dermed medvirker til at fremme en positiv udvikling hos regionens virksomheder og i Danmark generelt.

I behovsundersøgelsen vurderer 93% af de adspurgte virksomheder, at der i nogen eller høj grad vil være større efterspørgsel efter medarbejdere med kompetencer inden for cybersikkerhed i deres virksomhed fremadrettet (se Bilag 1, s. 4). Der forventes at være en stigning på 157% i behovet for ingeniører med kompetencer i cybersikkerhed, mens behovet for ingeniørfaglige medarbejdere generelt stiger med 58% i løbet af de næste tre år (jf. figur 7 nedenfor). 64% af virksomheder oplever dertil, at det er svært eller meget svært at rekruttere medarbejdere med kompetencer inden for cybersikkerhed, som markedet ser ud i dag (se Bilag 1, s. 11).



Figur 7: Indekseret udvikling af behov for ingeniører generelt og cybersikkerhedsingeniører. Kilde: Epinion, s.11, N=112/103.

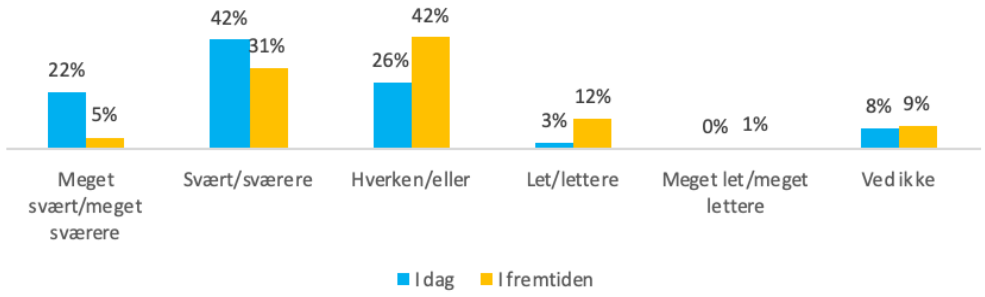
Som det fremgår af Tabel 4, er manglen på IKT-specialister særlig høj inden for cybersikkerhed, Her udgør den ifølge Epinion 11,9% i dag, stigende til 19,2% om tre år (se Bilag 1, s.10)

	2019	2022
Antal ingeniører, dataloger eller andre med længerevarende IT-uddannelse i dag og forventet antal om 3 år	2.098	3.320
Ingeniører, dataloger eller andre med længerevarende IT-uddannelser med kompetencer inden for cybersikkerhed i dag og forventet antal om 3 år	249	639
Andel ingeniører, dataloger eller andre med længerevarende IT-uddannelse med kompetencer inden for cybersikkerhed	11,9 %	19,2 %

Tabel 4: Hvor mange ingeniører, dataloger eller andre med længerevarende IT-uddannelser med kompetencer inden for cybersikkerhed er der ansat i virksomheden i dag, og hvor mange forventer I cirka, der er behov for om tre år? Kilde: Epinion, s. 10

64% af de adspurgte virksomheder er i nogen eller høj grad interesserede i at ansætte engelsksprogede ingeniører i virksomheden i fremtiden. Derimod er 12% slet ikke interesserede i dette. Det er særligt virksomheder, der allerede har engelsksprogede ingeniørfaglige medarbejdere ansat, der er interesserede i at ansætte flere engelsksprogede ingeniører (se Bilag 1, s. 17).

I dybdeinterviewene med potentielle aftagervirksomheder fremgår det også, at virksomhederne i høj grad efterspørger medarbejdere med kompetencer inden for cybersikkerhed. Ligeledes vurderes det, at udbuddet af denne type profiler hidtil har været meget begrænset og fortsat er det, samtidig med at efterspørgslen efter dem er stigende grundet den øgede digitalisering og krav til cybersikkerhed i både offentlige og private virksomheder.



Figur 8: Hvor let eller svært oplever du, at det er i dag for din virksomhed at rekruttere ingeniører eller andre med de rette kompetencer inden for cybersikkerhed? & Forventer du, at det vil blive lettere eller sværere for din virksomhed at rekruttere ingeniører eller andre med de rette kompetencer inden for cybersikkerhed i de kommende år? N=86/120. Kilde Epinion.

Virksomheder, der arbejder med produktion, er dem, der udtrykker at have sværest ved at rekruttere medarbejdere med kompetencer inden for cybersikkerhed på nuværende tidspunkt, mens det er lettest for de virksomheder, der beskæftiger sig med rådgivning og serviceydelser. I fremtiden er det også virksomheder, der benytter cybersikkerhed i deres produktion, der i højeste grad forventer, at det bliver sværere at rekruttere denne type medarbejder, mens virksomheder, der benytter cybersikkerhed i deres rådgivning og serviceydelser, er de mest fortrøstningsfulde.

Flere af de virksomheder, der oplever udfordringer med at rekruttere ingeniører, dataloger eller andre med lange IT-uddannelser med kompetencer inden for cybersikkerhed forklarer, at der er meget lille udbud på markedet, men stor efterspørgsel efter de få kompetente medarbejdere. Det betyder også, at flere mindre virksomheder og offentlige organisationer er presset af det høje lønniveau, der gør sig gældende på området. Den store efterspørgsel udtrykkes dertil også i, at 20% (24) af de adspurgte virksomheder aktuelt har ubesatte stillinger, som vil kunne varetages af en ingeniør med kompetencer inden for cybersikkerhed. Samlet set har disse 24 virksomheder 57 aktuelt ubesatte stillinger, der kunne varetages af en ingeniør med kompetencer indenfor cybersikkerhed.

De af adspurgte virksomheder i behovsundersøgelsen fra Epinion frygter, at det vil tage flere år før udbuddet matcher efterspørgslen. Virksomhederne fremhæver at de ofte kun får få ansøgere til deres opslåede stillinger.

> *Det er smalt på tværs af lande. Hvis vi bare slår stilling op, synes jeg det kan være svært at tiltrække. Der er langt imellem de dygtige. (Chief Security Architect, stor virksomhed)*(se Bilag 1, s.19*)*

Det er særligt medarbejdere med erfaring samt kompetencer over det tekniske niveau (arkitektoniske og strategiske), der er svære at rekruttere. Nogle virksomheder arbejder derfor med at koble junior- og seniorprofiler for at veje op for den manglende erfaring hos de nyansatte, men der er fortsat efterspørgsel efter mere erfarne medarbejdere (se Bilag 1, s.12). Denne mangel adresseres i den her foreslåede kandidatuddannelse, hvor de arkitektoniske og strategiske kompetencer opnås dels gennem fag-kombinerende semester gruppeprojekter på 15 ECTS-point, dels ved uddannelsens fokus på koblingen mellem de tekniske og kontekstuelle elementer i cybersikkerhedsproblematikkerne.

I dag uddannes der således kandidater, der delvist opfylder arbejdsmarkedets behov, men antallet er færre end det forventede behov. Samtidigt påpeger virksomhederne særligt deres behov for medarbejdere, der har kompetencer ud over snævre problemstillinger. Dette imødekommes med den foreslåede kandidatuddannelse, der dels giver kandidaterne en forståelse af cybersikkerhed, som går på tværs af de enkelte discipliner (bl.a. netværk, distribuerede systemer, software, IoT/Cloud, standarder og regulering), dels giver kandidaterne en stærk teoretisk forståelse, der sætter dem i stand til at løse komplekse problemstillinger og reflektere over egen praksis.

Med en kompetenceprofil svarende til den ansøgte uddannelse, vurderes det, at arbejdsmarkedssituationen for dimittenderne fra uddannelsen i cybersikkerhed vil være favorabel.

3. UDBUD OG EFTERSPØRGSEL – PERSPEKTIVANALYSE OM KANDIDATUDDANNELSEN INDEN FOR CYBERSIKKERHED

Den overordnede mangel på ingeniører og naturvidenskabelige kandidater og andre IKT-specialister fremgår af tre mere grundige analyser og fremskrivninger foretaget i de seneste år. Undervisnings- og Forskningsministeriet har løbende udarbejdet udbudsfremskrivninger, bl.a til udvalget vedrørende kvalitet i uddannelsesssystemet. DI og IDA har for Engineering the Future fremskrevet manglen på ingeniører og naturvidenskabelige kandidater. Endelig leverede en omfattende analyse af behovet for digitale komptencer udarbejdet af Erhvervsstyrelsen, UFM og UVM detaljerede langfristede fremskrivninger for IKT-kandidater.

I nedenstående beregning er der taget højde for de nyeste optagelsestal i 2018, den nyeste studieadfærd mht. søgning, optag og fuldførelsesprocenter samt den seneste beskæftigelsesudvikling.

Tabel 1: Beregning af mangel på ingeniører og naturvidenskabelige kandidater på BSc- og MSc-niveau i 2020 og 2025

	2020	2025
Efterspørgsel ingeniører og naturvidenskabelige kandidater	130.000	150.000
Udbud ingeniører og naturvidenskabelige kandidater	123.000	140.000
Mangel ingeniører og naturvidenskabelige kandidater	7.000	10.000

Kilde: IDA og DI 2015 og 2018 og egne beregninger 2019.

På trods af et stigende udbud af IKT-arbejdskraft viste grundscenariet i analysen fra UFM og Erhvervstyrelsen, at der vil være et udækket efterspørgselspotentiale på 19.000 IKT-specialister i 2030. Det vil sige en situation, hvor efterspørgslen ikke dækkes af arbejdskraftudbuddet af IKT-uddannede. Det kan risikere at medføre produktionsbegrænsninger og lavere produktivitet, da jobbene risikerer at forsvinde eller blive besat af personer med et lavere kompetenceniveau.

Særlig stor ville manglen blive på IKT-specialister med lange videregående uddannelser. Det samlede udækkede efterspørgselspotentiale på 19.000 i 2030 dækker over betydelige forskelle mellem uddannelsesgrupperne. Fremskrivningen viser et underudbud af IKT-arbejdskraft med lange videregående uddannelser på ca. 13.000. Dette på trods af, at der forventedes en markant stigning i antallet af personer med lange videregående uddannelser frem mod 2030. Derimod pegede fremskrivning på et mindre overudbud af IKT-specialister med erhvervsuddannelser og korte videregående uddannelser.

Det stigende optag på IKT-uddannelser efter 2016 vil ifølge Epinions beregninger reducere manglen lidt, men den vil stadig være tæt på de 10.000.

Hvad kan vi sige specielt om kandidater i cybersikkerhed, som skal bygge videre på en bacheloruddannelse i software?

Vi taler om et metodologisk vanskeligt område. Man skelner mellem underudbud (under-supply) og mangelfulde delkompetencer hos færdiguddannede (under-skilling). Der er ofte manglende konsistens i analyserne, og det gør det også vanskeligt at sammenligne forskellige landes uddannelsespolitikker med henblik på at imødegå mangelsituationer.

Skal man med hensyn til cybersikkerhed satse på en ny formel uddannelse eller udbygge eksisterende efteruddannelser? Det klare svar er, at både underudbud og manglende delkompetencer hos færdiguddannede IKT-kandidater mv. skal adresseres. På trods af problemet med sammenlignelighed kan vi udtale os med rimelig sikkerhed for Danmarks vedkommende. Der er et meget stort behov flere cybersecurity specialister. I USA er det et af de områder, som har størst beskæftigelsesvækst overhovedet. Baseret på øgningen i antal jobs inden for cyber security fra 2017 til 2018 voksede behovet med 50 % på bare et år.

Der er med nedenstående tabel beregnet en stor mangel på civilingeniører med specialisering i cybersikkerhed også i Danmark. I udbuddet er inkluderet ingeniører fx fra DTU, som har taget videreuddannelse inden for cybersikkerhed.

Det kan bemærkes, at der er betydelige substitutionsmuligheder mellem ingeniører, dataloger og andre. I nedenstående regneeksempel er indregnet horisontal substitution mellem de forskellige uddannelseskategorier: ingeniører, dataloger eller andre med længerevarende IT-uddannelser.

Tabel 2: Regneeksempel på udbud og efterspørgsel af civilingeniører med speicalisering i cybersikkerhed

	2020	2025
Efterspørgsel efter ingeniører spec. i cybersikkerhed	1.600	3.400
Udbud af ingeniører specialiseret i cybersikkerhed	1.500	3.000
Mangel	100	400

I tabel 3 i efterfølgende kapitel vises forventet behov hos de virksomheder, der er blevet spurgt i forbindelse med undersøgelsen af behovet for specialister i cybersikkerhed. Sammenholdes denne med overstående regneeksempel, som kun går på den type civilingeniører, AAU vil uddanne, er der ganske god overensstemmelse.

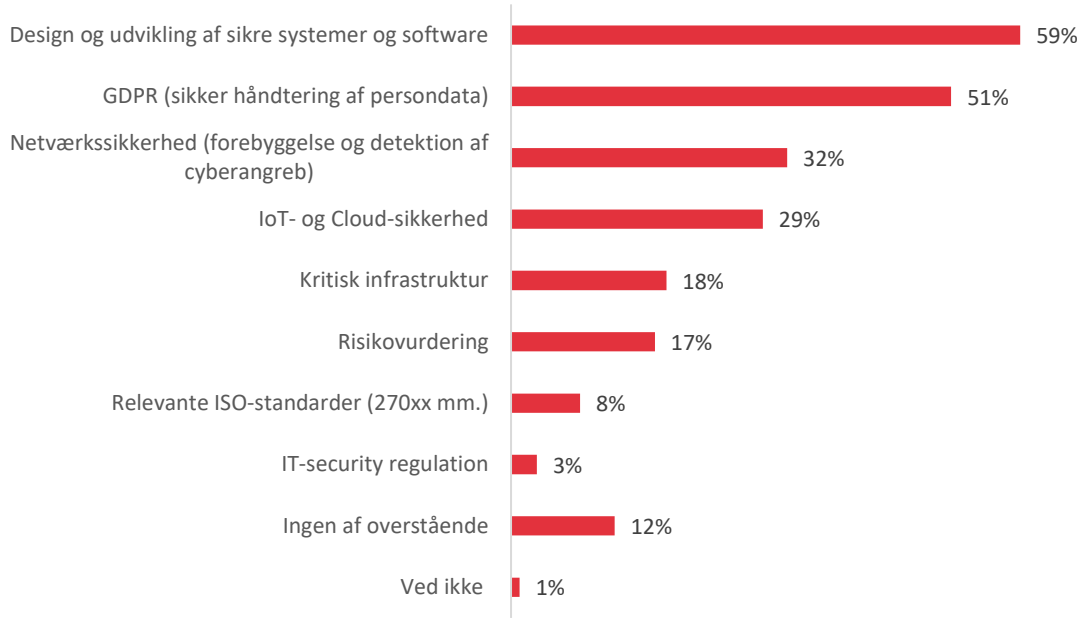
4. AFTAGERVIRKSOMHEDERNES BEHOV

4.1 CYBERSIKKERHEDS ROLLE I VIRKSOMHEDERNE

I dette afsnit afdækkes cybersikkerheds rolle i de virksomheder, der har deltaget i spørgeskema-undersøgelsen. Det vil sige andelen af virksomheder, som beskæftiger sig indenfor områder der vedrører information eller kommunikation samt andre brancher, hvor der er behov for cybersikkerhed eksempelvis grundet virksomhedens størrelse.

Blandt virksomhederne beskæftiger 59% sig med design og udvikling af sikre systemer og software. Halvdelen (51%) beskæftiger sig også med sikker håndtering af persondata, mens 32% beskæftiger sig med henholdsvis netværkssikkerhed. 12% af virksomhederne beskæftiger sig ikke med nogen af de oplistede områder.

Figur 1: Er din virksomhed beskæftiget med et eller flere af følgende områder?



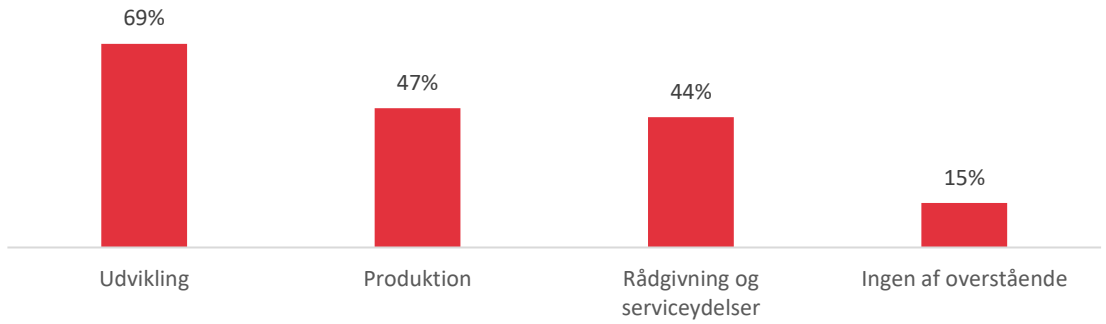
N=120

Det er overvejende små (0-20 ansatte) og mellemstore virksomheder (20-99 ansatte) i informations- og kommunikationsbranchen, der designer og udvikler sikre systemer og software. Relevante ISO-standarder, netværkssikkerhed og risikovurdering benyttes omvendt primært i større virksomheder (100+ ansatte) i andre brancher end informations- og kommunikationsbranchen. For de resterende områder er der ikke tydelige forskelle mellem brancher og virksomhedsstørrelser.

Cybersikkerhed indgår oftest i udviklingsområderne i virksomhederne. Blandt 69% af virksomhederne indgår cybersikkerhed således i udviklingsområdet i virksomheden. Hos 47% indgår

cybersikkerheden i produktionen, mens den indgår som en del af rådgivning eller serviceydelser blandt 44% af de adspurgte virksomheder. Hos 15% af de adspurgte virksomheder indgår cybersikkerhed ikke i nogle af de tre områder.

Figur 2: Indgår cybersikkerhed i et eller flere af følgende områder i virksomhedens arbejde?



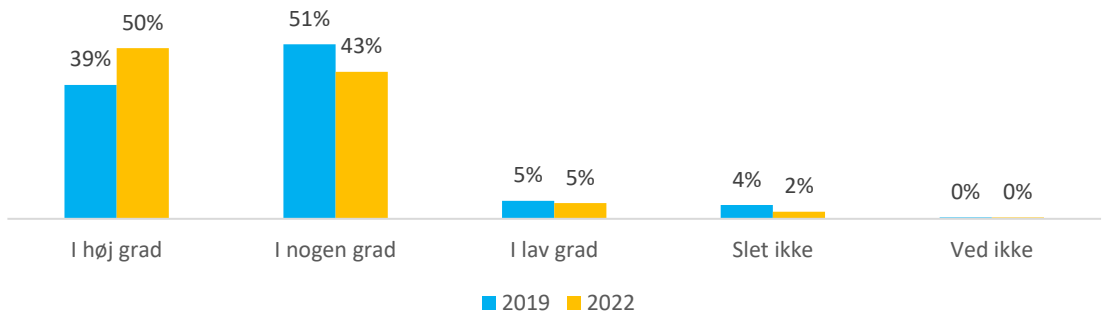
N=120

4.2 VIRKSOMHEDERNES AKTUELLE OG FREMTIDIGE BEHOV FOR INGENIØRER MED KOMPETENCER INDEN FOR CYBERSIKKERHED

I dette afsnit afdækkes virksomhedernes aktuelle og fremtidige behov for ingeniører med kompetencer inden for eksempelvis sikkerhed i netværk og distribuerede systemer; udvikling, test og verifikation af sikker software; samt en række centrale anvendelsesområder som IoT- og cloud-sikkerhed, identity and access management, sikker håndtering af persondata, virksomheders it- og service-arkitekturer og security governance.

Spørgeskemaundersøgelsen blandt aftagervirksomheder viser, at 90% af virksomhederne i høj eller nogen grad har et aktuelt behov for ingeniører, dataloger eller andre med en længere videregående IT-uddannelse med kompetencer inden for cybersikkerhed. Denne andel forventes at være stabil frem mod 2022 (om 3 år), dog med en tendens til, at behovet er en smule større fremadrettet jf. en større stigning i kategorien ”i høj grad” i modsætning til ”i nogen grad”. Kun 4% af de adspurgte virksomheder mener slet ikke at have behov for medarbejdere med kompetencer inden for cybersikkerhed i dag, og kun 2% forventer ikke at have behovet om tre år.

Figur 3: I hvilken grad vurderer du, at der i din virksomhed i dag/inden for de næste tre år vil være større behov for ingeniører, dataloger eller andre med længerevarende IT-uddannelser med kompetencer inden for cybersikkerhed?



N=120

Det er især de store virksomheder, der vurderer, at der vil være større behov for ingeniører med kompetencer inden for cybersikkerhed både i dag og i fremtiden, selvom de små og mellemstore virksomheder også i nogen grad vurderer, at behovet er stort og fortsat vil være det om tre år.

4.2.1 Virksomhedernes aktuelle og fremtidige behov for ingeniører med kompetencer inden for cybersikkerhed i tal

Alle adspurgte virksomheder i undersøgelsen har enten ingeniører, dataloger eller andre medarbejdere med en længerevarende uddannelse ansat. Til sammen har virksomhederne på nuværende tidspunkt ansat 2.098 af denne type medarbejdere, mens behovet anslås at være 3.320 medarbejdere om tre år (2022). Ser man på medarbejdere med særlige komptencer inden for cybersikkerhed, er der tale om en udtalt stigning i behovet. I dag udgør de medarbejdere, der har kompetencer inden for cybersikkerhed 11,9% ud af alle ingeniører, dataloger og andre med længerevarende IT-uddannelser ansat i de adspurgte virksomheder, mens virksomhederne i 2022 forventer, at de udgør over 19%. Behovet synes således at stige både for ingeniører, dataloger og andre med længerevarende IT-uddannelser generelt, men særligt for denne type medarbejdere med kompetencer inden for cybersikkerhed.

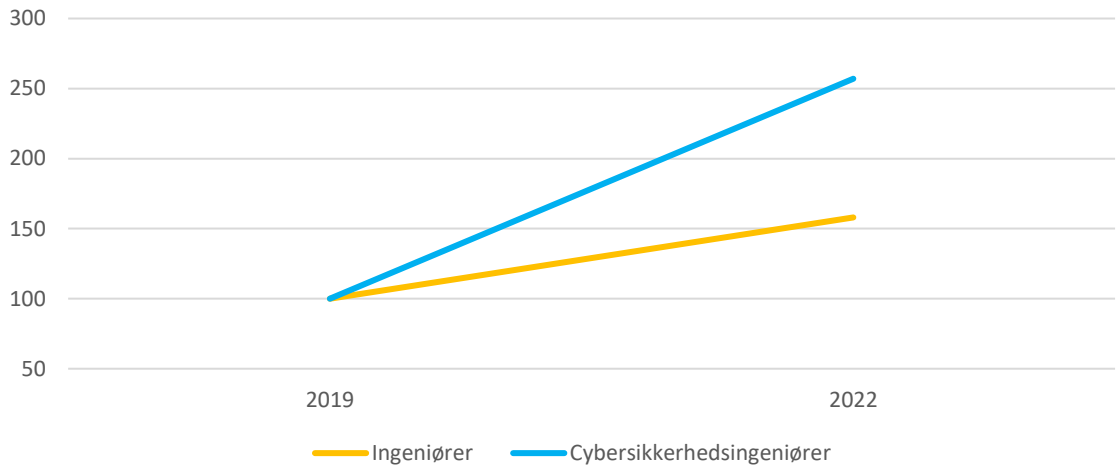
Tabel 3: Hvor mange ingeniører, dataloger eller andre med længerevarende IT-uddannelser med kompetencer inden for cybersikkerhed er der ansat i virksomheden i dag, og hvor mange forventer I cirka, der er behov for om tre år?

	2019	2022
Antal ingeniører, dataloger eller andre med længerevarende IT-uddannelse i dag og forventet antal om 3 år	2.098	3.320
Ingeniører, dataloger eller andre med længerevarende IT-uddannelser med kompetencer inden for cybersikkerhed i dag og forventet antal om 3 år	249	639
Andel ingeniører, dataloger eller andre med længerevarende IT-uddannelse med kompetencer inden for cybersikkerhed	11,9 %	19,2 %

N=112/103.

Stigningen i det forventede behov for ingeniører, dataloger eller andre med en lang IT-uddannelse med kompetencer inden for cybersikkerhed frem mod 2022 er således på 157%. I samme periode forventes en stigning i antallet af ingeniører på 58%. Nedenstående figur illustrerer denne udvikling ved brug af indeksering.

Figur 4: Indekseret udvikling af behov for ingeniører generelt og cybersikkerhedsingeniører

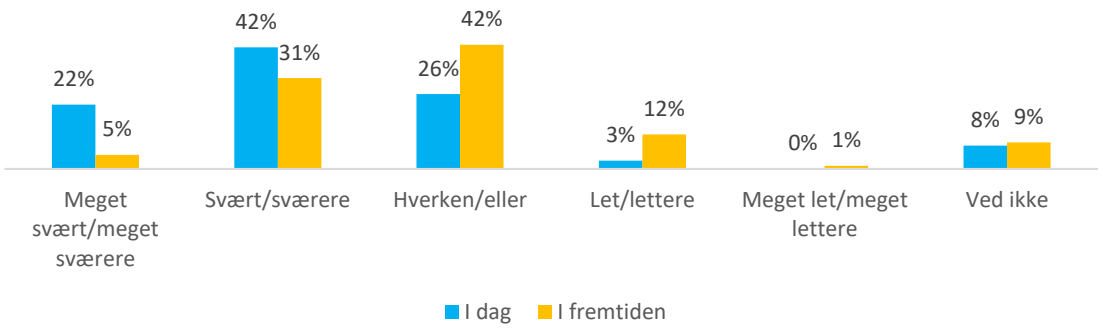


N=112/103.

4.2.2 Rekruttering af ingeniører med kompetencer inden for cybersikkerhed

I dag oplever 64% af de adspurgte virksomheder, at det er enten svært eller meget svært at rekruttere ingeniører eller andre medarbejdere med kompetencer inden for cybersikkerhed, mens kun 3% vurderer det som let eller meget let. Fremadrettet forventer virksomhederne dog, at det bliver en smule lettere end i dag, men dog fortsat kun 13%, der forventer, at rekrutteringen bliver let eller meget let.

Figur 5: Hvor let eller svært oplever du, at det er i dag for din virksomhed at rekruttere ingeniører eller andre med de rette kompetencer inden for cybersikkerhed? & Forventer du, at det vil blive lettere eller sværere for din virksomhed at rekruttere ingeniører eller andre med de rette kompetencer inden for cybersikkerhed i de kommende år?



N=86/120

Virksomheder, der arbejder med produktion, er dem, der udtrykker at have sværest ved at rekruttere medarbejdere med kompetencer inden for cybersikkerhed på nuværende tidspunkt, mens det er lettest for de virksomheder, der beskæftiger sig med rådgivning og serviceydelser. I fremtiden er det også virksomheder, der benytter cybersikkerhed i deres produktion, der i højeste grad forventer, at det bliver sværere at rekruttere denne type medarbejder, mens virksomheder, der benytter cybersikkerhed i deres rådgivning og serviceydelser, er de mest fortrøstningsfulde.

Flere af de virksomheder, der oplever udfordringer med at rekruttere ingeniører, dataloger eller andre med lange IT-uddannelser med kompetencer inden for cybersikkerhed forklarer, at der er meget lille udbud på markedet, men stor efterspørgsel efter de få kompetente medarbejdere. Det betyder også, at flere mindre virksomheder og offentlige organisationer er presset af det høje lønniveau, der gør sig gældende på området. Den store efterspørgsel udtrykkes dertil også i, at 20% (24) af de adspurgte virksomheder aktuelt har ubesatte stillinger, som vil kunne varetages af en ingeniør med kompetencer inden for cybersikkerhed. Samlet set har disse 24 virksomheder 57 aktuelt ubesatte stillinger, der kunne varetages af en cybersikkerhedsingeniør.

De virksomheder, der forventer, at det også inden for de kommende år vil blive svært at rekruttere ingeniører med kompetencer inden for cybersikkerhed fremhæver primært, at konkurrencen om de få kompetente medarbejdere er for stor grundet et for lille udbud, og at der uddannes for få profiler med kompetencer inden for sikkerhed. I det der allerede nu er underskud af arbejdskraft, vil det tage flere år før udbuddet matcher efterspørgslen, hvorfor det også inden for den næste årrække vil være en udfordring at rekruttere denne type medarbejdere. Denne oplevelse af udfordringer i rekrutteringen og manglende udbud genfindes også i de kvalitative dybdeinterviews. Her fremhæver aftagervirksomhederne, at de ofte kun får få ansøgere til deres opslåede stillinger, og at det også ofte er de samme få kandidater, der går igen indenfor området.

> *Det er smalt på tværs af lande. Hvis vi bare slår stilling op, synes jeg det kan være svært at tiltrække. Der er langt imellem de dygtige*. (Chief Security Architect, stor virksomhed)

Det er særligt medarbejdere med erfaring samt kompetencer over det tekniske niveau (arkitektoniske og strategiske), der er svære at få fat i. Nogle virksomheder arbejder derfor med at koble junior- og seniorprofiler, for at veje op for den manglende erfaring hos de nyansatte, men der er fortsat efterspørgsel efter mere erfarne medarbejdere.

4.2.3 Karakteristik af virksomhederne og deres behov

Baseret på de kvalitative dybdeinterviews kan de potentielle aftagervirksomheder for kandidater i cybersikkerhed groft set opdeles i tre overordnede grupper: 1) private IT-virksomheder, 2) private virksomheder og 3) offentlige organisationer.

1. **Private IT-virksomheder** beskæftiger sig som regel udelukkende med sikkerhedsløsninger eller specifikke områder af cybersikkerhed fx udvikling af sikre systemer eller

konsulentydelser på området. De har derfor brug for meget specialiserede medarbejdere, der fx kan udvikle nye sikre systemer eller lave analyser og test af virksomheders eksisterende sikkerhedsløsninger. Denne type virksomhed vil således primært efterspørge medarbejdere med dybe, specialiserede tekniske kompetencer på området.

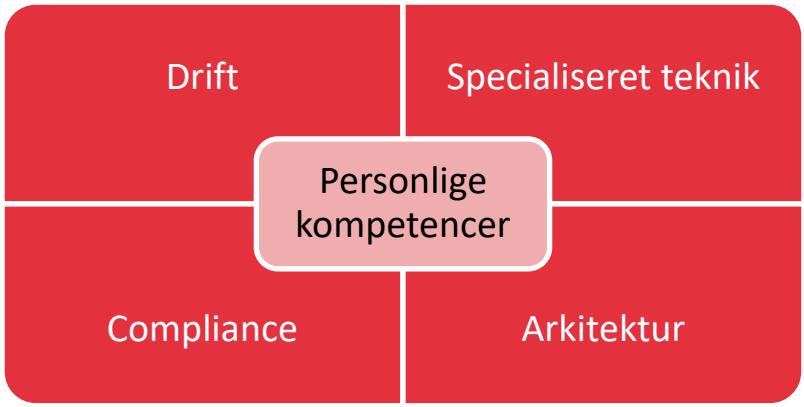
2. **Private virksomheder** beskriver virksomheder, der som udgangspunkt beskæftiger sig med et andet forretningsområde end sikkerhed som sådan. Det kan fx være produktion af forskellige produkter eller levering af serviceydelser. Når disse virksomheder opnår en vis størrelse, vil der være behov for medarbejdere, der kan håndtere cybersikkerheden i virksomheden, den såkaldte drift, fx vedligeholde og overvåge sikkerhedssystemerne for at undgå angreb og nedbrud. Disse virksomheder vil som regel købe sig nogle sikkerhedsløsninger, og har derfor brug for medarbejdere til at implementere og vedligeholde disse. Desuden kan der i denne størrelse virksomheder også ofte være brug for medarbejdere med viden om sikkerhed på et lidt højere, strategisk plan, der kan koble sikkerheden og systemerne hertil til forretningen og den strategiske udvikling. Endeligt vil der også i visse virksomheder være behov for medarbejdere, der har viden om lovgivning, krav og reguleringer på sikkerhedsområdet, og som kan anvende denne viden til at sikre, at virksomheden lever op til disse. Hos store virksomheder kan man også vælge at udvikle sin egen mere specialiserede sikkerhedsenhed, der eksempelvis udvikler deres egne systemer, selv tester systemerne eller foretager analyser på eget data, hvilket kræver mere dybe, specialiserede medarbejdere
3. **Offentlige organisationer** vil oftest efterspørge den samme type medarbejdere som private IT-virksomheder. Også her er der brug for medarbejdere med en dyb, specialiseret teknisk viden, der kan kode, hacke mv. Der er således primært konkurrence om denne type medarbejdere mellem konsulentvirksomhederne og de offentlige institutioner.

4.3 HVILKE KOMPETENCER EFTERSPØRGER VIRKSOMHEDER?

I dette afsnit undersøges det, hvilke tekniske og organisatoriske kompetencer ingeniørfaglige ansatte anvender i virksomhederne, samt hvilke kompetencer virksomhederne vurderer, der bliver større behov for frem mod 2022.

På baggrund af de kvalitative analyser kan medarbejdere med kompetencer indenfor cybersikkerhed generelt opdeles som siddende i fire forskellige typer af funktioner i virksomhederne. Alt afhængigt af virksomhedens størrelse og opgaver vil typerne sommetider overlappe, og der kan muligvis også identificeres yderligere funktioner. Gennemgående for alle typer funktioner er dog, at virksomhederne samtidig efterspørger visse personlige kompetencer, der ikke knytter sig specifikt til det faglige. De fire funktioner er præsenteret i figuren nedenfor.

Figur 6: Funktioner for medarbejdere med kompetencer inden for cybersikkerhed



Profiler, der arbejder med **drift**, skal overordnet set sørge for, at virksomheden fungerer i dagligdagen. De skal sørge for den daglige drift af systemerne og eksempelvis implementere nye systemer, der er udviklet af andre, som købes til virksomheden. Vigtige kompetencer i denne funktion er fx netværksovervågning og drift af servere. Det er typisk større private virksomheder, der har brug for denne type medarbejdere.

Profiler, der arbejder med **specialiseret teknik**, er 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, der varetages af disse medarbejdere. Medarbejdere af denne type er oftest eftertragtede af private IT-virksomheder eller offentlige organisationer, der beskæftiger sig med sikkerhed.

Profiler, der arbejder med **compliance**, skal overordnet sørge for, at virksomhedens cybersikkerhed lever op til de krav, love og reguleringer, der er gældende for virksomhedens produkter og services. Denne type medarbejdere skal have en vis juridisk viden samt forståelse for de relevante krav og reguleringer og mulighederne for at kunne leve op til disse. Denne type medarbejder efterspørges primært af større og sommetider internationale private virksomheder, der har behov for in-house viden om dette område, i det de ofte arbejder i flere lande, hvor der er mange forskellige reguleringer. Niveauet af reguleringer er dertil stærkt stigende i løbet af de seneste år, hvilket øger behovet for denne type medarbejdere.

Profiler, der arbejder med **arkitektur**, arbejder på et mere overordnet niveau, hvor de skal koble sikkerheden i virksomhederne med forretningens behov og strategi. Disse medarbejdere skal have 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 har brug for denne type medarbejdere, der kan arbejde et niveau "højere" end de tekniske specialister eller driftsmedarbejdere og være tættere på det strategiske niveau i virksomheden.

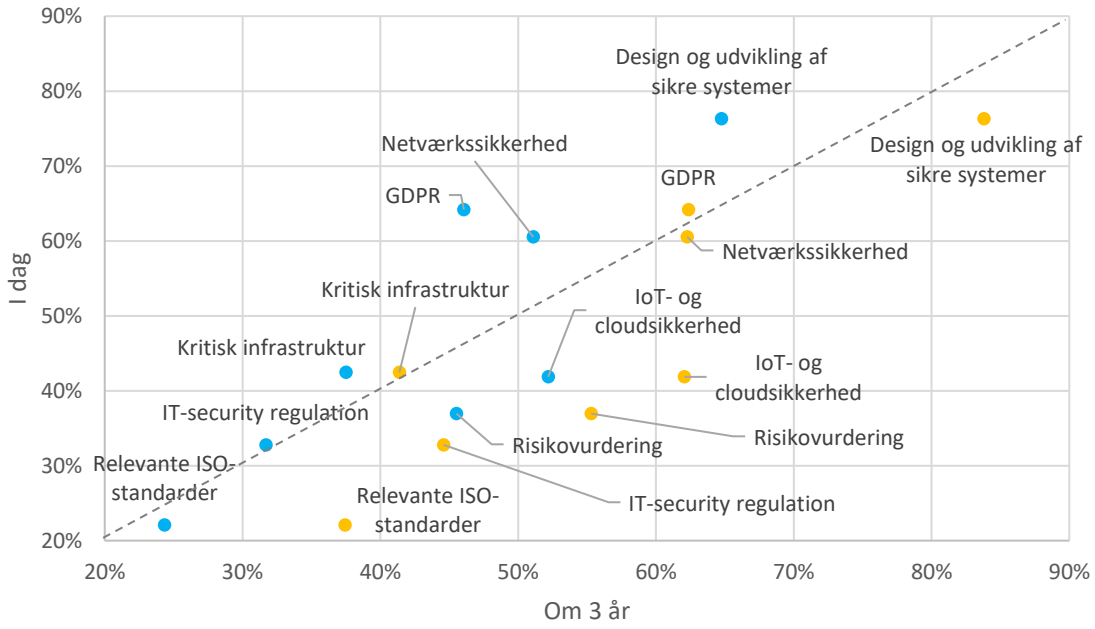
På tværs af de fire typer funktioner gælder det, at virksomhederne efterspørger **personlige kompetencer** hos medarbejderen. Dette kan være kompetencer som omgængelighed, positiv

indstilling, kommunikative evner mv. Virksomhederne ser således ikke kun på de faglige færdigheder hos medarbejderen, men også hvordan det personlige aspekt vil passe ind i virksomheden eller den pågældende afdeling. Her nævnes det også i de kvalitative dybdeinterviews, at behovet for personlige kompetencer afhænger af den givne stilling. Der kan eksempelvis være forskel på, hvor udadvendt en medarbejder har behov for at være, alt efter om han skal sidde med kundekontakt eller i teamsamarbejde, eller om der er tale om mere specialiserede opgaver (fx funktionen "specialiseret teknik" som beskrevet ovenfor).

> *Det kommer an på stillingen. Hvis det kræver meget dyb specialiseret viden, så behøver man ikke være ekstrovert, som hvis man skal have kontakt med kunder og kollegaer.* (Chief Security Architect, stor virksomhed)

Ser man på de mere konkrete, tekniske kompetencer, er de 120 virksomheder i den kvantitative undersøgelse blevet spurgt til, hvilke kompetencer, de ser som vigtige i dag, og hvilke der regnes for at være vigtige om tre år. Disse vurderinger er kombineret i figuren nedenfor, hvor kompetencer i den nederste, højre halvdel forventes at være mere vigtige om tre år end nu.

Figur 7: Faglige og tekniske kompetencer for cybersikkerhedsingeniører i dag og om tre år



N: De gule prikker er baseret på besvarelser fra de 49 respondenter, der har angivet på nuværende tidspunkt at have en eller flere medarbejdere ansat med kompetencer inden for cybersikkerhed. De blå prikker er baseret på samme respondenters vurdering af kompetencebehovet i dag, men på alle virksomheders vurdering af behovet om tre år (n=49/120).

Ifølge modellen ovenfor forventes de fleste kompetencer at blive mere relevante inden for de næste tre år, end de allerede er i dag – i hvert fald hvis man ser på de virksomheder, der på nuværende tidspunkt har medarbejdere med kompetencer inden for cybersikkerhed ansat. Disse virksomheder ser både design og udvikling af sikre systemer, netværkssikkerhed, IoT- og cloudsikkerhed,

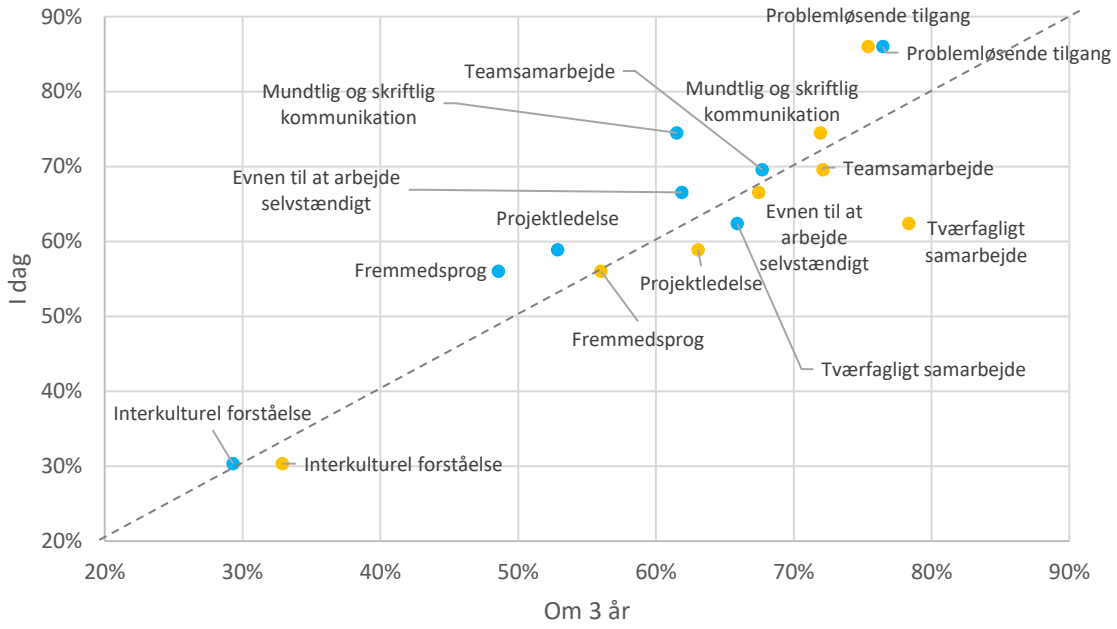
risikovurdering, IT-security regulation samt relevante ISO-standarder som værende mere relevante om tre år end tilfældet er nu. Særligt IoT- og cloudsikkerhed og risikovurdering forventes at blive betydeligt mere vigtige fremadrettet, men design og udvikling af sikre systemer vurderes fortsat – både i dag og om tre år – som den vigtigste kompetence for disse virksomheder. Blandt andet IoT- og cloudsikkerhed er vigtige elementer i driften af sikkerhed, som mange private virksomheder har behov for:

> *Det er vigtigt at man i det første semester kommer omkring mange forskellige dele af IT-sikkerhed. Det er præcis de her ting, som jeg tror den store efterspørgsel i det private erhvervsliv er på. Mange bruger cloud og arbejde med styring på internet of things.* (Grundlægger, mindre virksomhed)

Ser man på alle virksomheder, er det også særligt IoT- og cloudsikkerhed samt risikovurdering, der fremhæves som blivende vigtigere kompetencer fremadrettet. Samlet set viser figuren således en generel forventning til, at langt de fleste faglige og tekniske kompetencer vil blive mere efterspurgte i fremtiden, hvilket ligger i forlængelse af de andre resultater, der tyder på, at efterspørgslen efter medarbejdere med disse kompetencer allerede er stor og også vil stige i de kommende år.

Når det kommer til de anvendte organisatoriske kompetencer, forventes de fleste kompetencer at være lige så relevante fremadrettet, som de er i dag. Behovet for de enkelte kompetencer er illustreret i figuren nedenfor.

Figur 8: Organisatoriske kompetencer for cybersikkerhedsingeniører i dag og om tre år



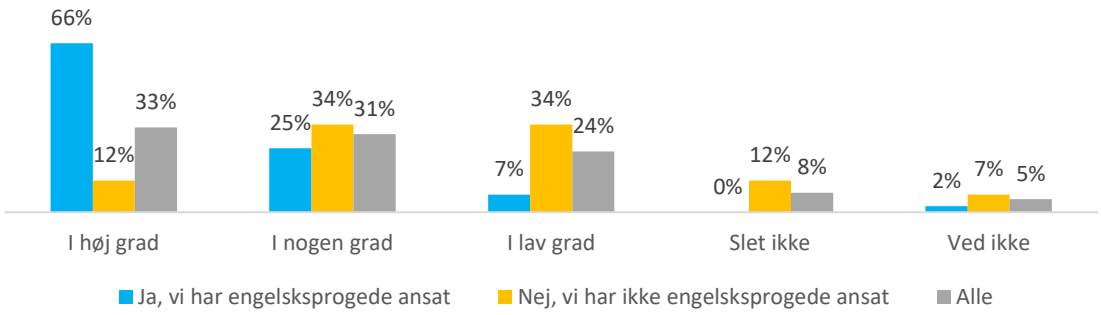
N: De gule prikker er baseret på besvarelser fra de 49 respondenter, der har angivet på nuværende tidspunkt at have en eller flere medarbejdere ansat med kompetencer inden for cybersikkerhed. De blå prikker er baseret på samme respondenters vurdering af kompetencebehovet i dag, men på alle virksomheders vurdering af behovet om tre år (n=49/120).

For alle virksomheder gælder det, at en problemløsende tilgang er den vigtigste organisatoriske kompetence at besidde både i dag og om tre år. At kunne samarbejde med andre fagligheder er desuden en kompetence, der forventes at blive betydeligt mere relevant om tre år, end den allerede er i dag, især hos de virksomheder, der allerede har ansatte inden for cybersikkerhed. Hos disse virksomheder er projektledelse også en kompetence, der fremadrettet forventes at blive større efterspørgsel efter. Der kan således med fordel arbejdes på at sikre, at kandidaterne i cybersikkerhed udvikler deres evner inden for dels tværfagligt samarbejde og teamsamarbejde samt projektledelse fremadrettet.

4.3.1 Ansættelse af engelsksprogede medarbejdere

Der er generelt tegn på villighed til at ansætte engelsksprogede medarbejdere i virksomhederne – særligt hos de virksomheder, der i forvejen har engelsksprogede ansat. 37% af de adspurgte virksomheder har på nuværende tidspunkt ansat engelsksprogede (dvs. ikke-dansktalende) ingeniørfaglige medarbejdere i virksomheden. Størstedelen, 61%, har ikke engelsksprogede ingeniørfaglige medarbejdere ansat.

64% af virksomhederne er i nogen eller høj grad interesserede i at ansætte engelsksprogede ingeniører i virksomheden i fremtiden. Derimod er 12% slet ikke interesserede i dette. Det er særligt virksomheder, der allerede har engelsksprogede ingeniørfaglige medarbejdere ansat, der er interesserede i at ansætte flere engelsksprogede medarbejdere. 91% af disse virksomheder er således i nogen grad eller høj grad interesserede i at ansætte flere engelsksprogede medarbejdere, mens dette kun gør sig gældende for 46% af de virksomheder, der på nuværende tidspunkt ikke har engelsksprogede ansat.



N=120

4.4 VURDERING AF KOMPETENCEPROFILEN

Dette afsnit afdækker matchet mellem virksomhedernes behov og kompetenceprofilen for den påtænkte kandidatuddannelse i cybersikkerhed. De potentielle aftagervirksomheder har blandt andet vurderet kompetenceprofilens relevans som en del af behovsundersøgelsen.

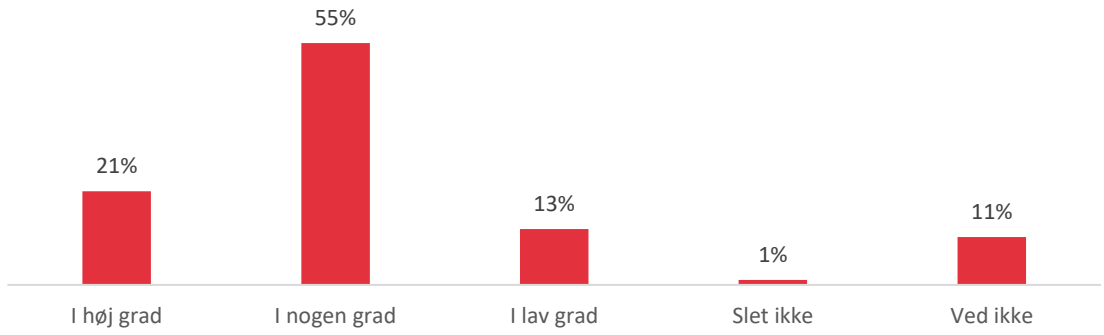
Kandidatuddannelsen i cybersikkerhed løber over fire semestre og har et omfang på 120 ECTS-point. Tabellen nedenfor viser uddannelsens opbygning opdelt på semestre. Tilføjet i bilaget er også kompetenceprofilen, der beskriver uddannelsens output ift. viden, færdigheder og kompetencer.

	Modul	Titel
1. sem.	Projekt (10 ECTS)	Sikkerhed i distribuerede systemer
	Kursus 1 (5 ECTS)	Netværkssikkerhed
	Kursus 2 (5 ECTS)	Sikker softwareudvikling
	Kursus 3 (5 ECTS)	Sikkerhed i IoT- og cloud-arkitekturer
	Kursus 4 (5 ECTS)	Grundlæggende sikkerhed og kryptografi
2. Sem	Projekt (15 ECTS)	Sikre systemer – Angreb og forsvar
	Kursus 1 (5 ECTS)	Hacker space
	Kursus 2 (5 ECTS)	Avanceret software-sikkerhed
	Kursus 3 (5 ECTS)	Valgmuligheder: Machine learning Identity and access management
3.-4. Sem	Der vælges blandt flg. muligheder: 3. sem.: 3 kurser + projekt, 4. sem.: Afgangsprojekt 3. sem.: Kursus 1 (se nedenfor) + Projektorienteret forløb i en virksomhed (25 ECTS), 4. sem.: Afgangsprojekt Kurser og langt afgangsprojekt: 3. sem.: Kursus 1 (se nedenfor) + 1-2 valgfag (5 el. 10 ECTS) 3.-4. sem.: Langt afgangsprojekt (hhv. 50 el. 45 ECTS).	
3. Sem	Projekt (15 ECTS)	Valgmuligheder: Security governance Udvikling af sikre systemer
	Kursus 1 (5 ECTS)	Avancerede emner inden for cybersikkerhed
	Kursus 2 & 3 (10 ECTS)	Valgmuligheder (2 ud af flg. 4 kurser): Privacy engineering Sikkerhedsmodeller Regulering af IT-sikkerhed Sikkerhed i virksomheder
4. Sem	Projekt (30 ECTS)	Afgangsprojekt

På baggrund af en kort beskrivelse af uddannelsen (baseret på kompetenceprofilen), vurderer 76% af de adspurgte virksomheder, at ingeniører i cybersikkerhed fra AAU vil enten i nogen eller i høj grad være relevante at ansætte i deres virksomhed nu eller i fremtiden. 13% af virksomhederne mener dette i lav grad, mens kun 1% angiver, at kandidater med uddannelsen slet ikke vil være relevante for deres virksomhed. Det tyder således på, at der er et stort antal virksomheder i de

relevante brancher, som vil være interesserede i kandidater fra cybersikkerhedsuddannelsen i København.

Figur 9: I hvilken grad vurderer du, at civiliingeniører i cybersikkerhed fra Aalborg Universitet i København vil være relevante at ansætte for din virksomhed nu eller i fremtiden?



N=120

De store virksomheder er de mest positive over for at ansætte kandidater med en uddannelse i cybersikkerhed fra AAU, mens de mellemstore (20-99 ansatte) er de mindst positive. Dette stemmer overens med de kvalitative fund, hvor de fleste typiske funktioner for denne type kandidat vil være mest relevante i store virksomheder, eller i små, meget specialiserede virksomheder på området.

I dybdeinterviewene med potentielle aftagervirksomheder er der generelt stor tilfredshed med kompetenceprofilen og uddannelsens planlagte opbygning. Stort set alle virksomheder vurderer, at kandidater med en sådan profil kan være relevante i deres virksomhed og opfylde de behov, de overordnet set efterspørger.

Det tyder således på, at en profil som denne vil være relevant for alle tre typer virksomheder tidligere præsenteret, men også for de fire forskellige funktioner beskrevet tidligere. Det påpeges dog, at hvis kandidaten skal sidde i en specialistrolle, vil yderligere specialisering formentlig være nødvendig. Specialiseringen kan dels foregå i virksomheden, men kan også begynde på universitetet, hvis der blev udbudt forskellige spor på kandidaten, så kandidaterne allerede tidligt i forløbet begynder at specialiserer sig:

> *Man kunne overveje at lave tre specialiseringer, for ellers bliver det rigtig meget på to år. Man kan strukturere det efter, hvad man gerne vil have ud af det. Overordnet set ser det fornuftigt ud.* (Chief Security Architect, stor virksomhed)

De fleste virksomheder, som omfatter otte større danske virksomheder, efterspørger desuden særligt mere forretningsforståelse hos kandidaterne. Der er således en opfattelse af, at kandidaterne bliver dækket ind på de fleste nødvendige tekniske og faglige kompetencer, men at de med fordel også kunne få bedre forståelse for, hvordan virksomheder og offentlige institutioner fungerer og cybersikkerhedens rolle i virksomheden.

> *…men det der giver os værdi, er når de har forretningsforståelse. Man skulle måske koble noget forretningsviden på også, så de har forståelse for, at det de laver, laver de, fordi forretningen har brug for det. En bredere forståelse for forretning kunne være super god.* (Chief Product Security & Solution Officer, stor virksomhed)

Der skelnes generelt mellem to typer af kompetencer, når virksomhederne taler om kompetencer for cybersikkerhedsingeniører. Groft set er der de tekniske kompetencer, eksempelvis hacking og machine learning, og så er der de mere "bløde" kompetencer såsom håndtering af persondata og governance. De fleste virksomheder foretrækker en kandidat, der primært har dækket de tekniske kompetencer, men som også har forståelse for de mere "bløde" områder og på den måde har en holistisk forståelse for sikkerhed. Enkelte virksomheder foretrækker dog kandidater, hvor den bløde sikkerhed er nedtonet:

> *Når man begynder at blande håndtering af persondata og andre ting ind i det er det det vi kalder blød sikkerhed. Jeg vil overveje om man vil lave uddannelsen mere hardcore og så samle de mere bløde ting som governance og den slags i et modul. Der er jo allerede jurister og mange andre, der fokuserer på persondata, så jeg tænker, at hvis det skal give mening at have en cand.polyt ud af det her, så skal det være en, der har lidt overordnet kendskab til de blødere ting, men fokus må altså være de mere langhårede ting.* (Chief Security Architect, stor virksomhed)

Til gengæld efterspørger flere virksomheder mere fokus på de blødere emner, både governance og persondatahåndtering, men også ledelse, etik og juridisk viden er områder, der ønskes viden om blandt kandidaterne. Disse kompetencer er særligt relevante for kandidater, der blandt andet skal arbejde med compliance, men også som en del af den holistiske forståelse for sikkerhed blandt andre typer profiler.

> *Der er også nogle af de blødere ting som governance, som mange af de større virksomheder skriger efter. Folk der kan lave politikker, etablere nogle processer, der gør at man kan styre sig ned igennem et meget komplekst system.* (Grundlægger, mindre virksomhed)

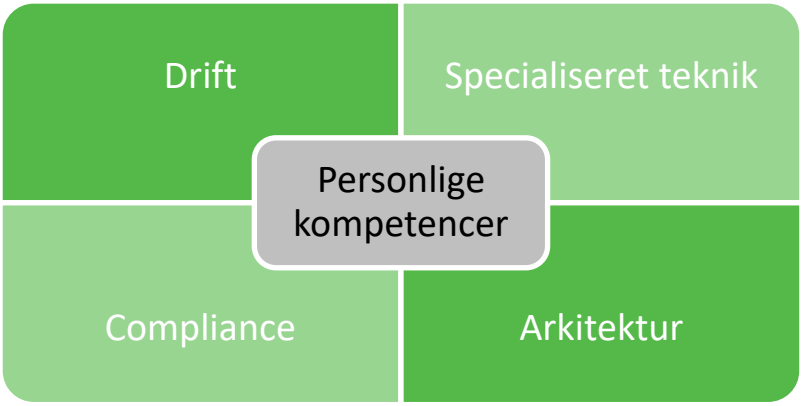
> *Den anden del, jeg efterspørg er lidt mindre teknisk. Jeg ønsker lidt mere jura og mere management. Det bliver på bekostning af det tekniske. Det er især pga. persondataretlige regler, vi skal efterleve. I den forbindelse er det meget nyttigt at have lidt politologisk eller etisk omkring overvågning. Hvis akademikerne også lige kan overveje noget etisk og juridisk – må vi overvåge, og er det rimeligt. Der er security governance, så det kunne selvfølgelig indeholde noget management, men det kan også handle om noget organisering. Det kunne være meget nyttigt at få nogle få elementer om ledelse og strategi, så de sikkerhedssystemer afspejler sin forretning og strategi.* (Chief Information Security Officer, stor virksomhed)

Overordnet set synes uddannelsens kompetencer at stemme godt overens med de relevante funktioner, som kandidaterne kan komme ud til på arbejdsmarkedet og hermed virksomhedernes behov. Kompetencerne taler dog umiddelbart bedst ind i en drift- eller arkitektfunktion, men kan

med mindre justeringer eller yderligere specialisering i virksomhederne også varetage compliance- eller specialistroller. Overensstemmelsen med kompetenceprofilen og funktionerne er opsummeret i figuren nedenfor.

> *Den er meget bred. Det er udmærket udgangspunkt for en, der skal ind og specialiseres i en særlig retning. Hvis jeg fik sådan en her foran mig, vil jeg spørge ham, hvad det lige præcis er, han vil… [kompetenceprofilen] vil typisk være en arkitekt med viden om processer. Er der en specialistrolle? Jo måske nok, men så skal vedkommende specialisere sig her.* (IT security Engineer, stor virksomhed)

Figur 10: Overensstemmelse mellem kompetenceprofil og kompetencer nødvendige i de fire funktioner



Opsummerende er der således ingen af de fire funktioner, som en kandidat i cybersikkerhed ikke forventes at kunne udfylde, men kompetenceprofilen lægger umiddelbart en lille smule bedre til drift- og arkitektur-medarbejdere ifølge de potentielle aftagervirksomheder. Idet der også kun er tale om kandidatuddannelsen i denne rapport, kan den forudgående bacheloruddannelse også have indflydelse på kandidatens samlede profil, og dermed sagtens indgå i en funktion i forhold til compliance eller mere specialiserede arbejdsopgaver. En lærenem kandidat vil formentligt også hurtigt tilegne sig de yderligere nødvendige kompetencer på en arbejdsplads, hvorfor det for flere virksomheder også er vigtigt, og sommetider næsten vigtigere end de egentlige tekniske kompetencer, at kandidaten er nysgerrig og besidder evnen til let at tillære sig ny viden og færdigheder.

Bilag 2: Liste med virksomheder og kontaktpersoner til Epinion

Liste med virksomheder og kontaktpersoner til kvalitative interviews. Vi foreslår at Epinion kontakter 1-2 virksomheder fra hver kategori. Virksomhederne er prioriterede inden for hver kategori. Dvs. Epinion starter med førstnævnte virksomhed inden for hver kategori.

Kommunikation:

- TDC - Kristian Kindtler - KRKI@tdc.dk
- Motorola Solutions - Christian Ritter - christian.ritter@motorolasolutions.com
- Telenor - Per Olsen - pol@telenor.dk
- TT-Netværket – René Skytte Christoffersen – rene.skytte.christoffersen@tt-network.dk
- Netic - Morten Bundgaard - morten@bndgrd.dk
- DK Hostmaster - Erwin Lansing - erwin@dk-hostmaster.dk

Energi:

- Vestas - Thomas Bonello - tobll@vestas.com
- SE - Kenneth Bjerregaard Jørgensen - kenj@se.dk
- NRGI - Michael Warrer - miwa@nrgi.dk
- Ørsted / RADIUS? (Ingen kontakter)

Finans og forsikring:

- Jyske Bank - Ba Duong Anders Le - bad@jyskebank.dk
- Danske Bank – Martin Clausen – cla@danskebank.dk
- e-Nettet – Nikolas Triantafyllidis – nit@e-nettet.dk
- TopDanmark – Mads Wijngaard – yk1@topdanmark.dk

Konsulentfirmaer:

- PwC - Claus Nørklit Roed - cnr@pwc.dk
- Strand Consult - John Strand – js@strandconsult.dk
- Omada - Stefan Buus - sbu@omada.dk
- NNIT – Ole Steen Brams – ostb@nnit.com
- Deloitte - Gorm Christiansen - gormchr@deloitte.dk

Produktion:

- Siemens - Peter Frøkjær - Formand@isaca.dk (også formand for ISACA)
- Lego - Søren Brandbyge - soeren.brandbyge@lego.com
- Grundfos - Jes Beirholm - (har vist kun hans linkedin)
- Intelligent Systems - Niki Nicolas Grigoriou - nng@intelligentsystems.dk
- DS Stålprofiler - Christian Erland Jensen - cej@ds-staalprofil.dk
- FOSS – Janick Elleholm Jensen – (kun LinkedIn)

Sikkerhed/forsvar:

- Terma - Jan Dorn Johansen - jaj@terma.com eller Samant Khajuria, sakh@terma.com
- CSIS - Peter Kruse - pkr@csis.dk

Softwareudvikling:

- Microsoft - Ole Kjeldsen - olek@microsoft.com
- Google Denmark - Christian Stahl - christianstahl@google.com
- Mediathand – Gert Skov Petersen – gert@mediathand.com
- Dencrypt – Søren Sennels (COO) – soren.sennels@dencrypt.dk
- Systematic?
- Agilic?
- Trifork
- DevoTeam
- Mjølner Informatics
- Cryptera – Bo Rosenkilde – bo.rosenkilde@cryptera.com
- NETS
- KMD
- Cisco

Offentlige myndigheder, interesseorganisationer og råd:

- Digitaliseringsstyrelsen – Mogens Rom Andersen – moran@digst.dk
- Rådet for Digital Sikkerhed – Henning Mortensen – henning.mortensen@digitalsikkerhed.dk

- Center for Cybersikkerhed - Mille Østerlund - milost@cfcs.dk
- Rigspolitiet (NC3) - Johnny Vestergaard - JVE004@politi.dk
- Liga - Bjarke Alling - ba@liga.com (formand for IT Branchens Udvalg for IT-Sikkerhed)
- Dansk Metal – Torben Andersen Lindhart – toalet@danskmetal.dk
- Tele Industri – Jakob Willer – jw@teleindu.dk

Uddannelses- og Forskningsministeriet

Aalborg Universitet

E-mail: aau@aau.dk

Godkendelse af ny uddannelse

5. februar 2020

Styrelsen for Forskning og Uddannelse
Forskning og Forskningsbaserede Uddannelser

Bredgade 40
1260 København K
Tel. 3544 6200

www.ufm.dk

CVR-nr. 1991 8440

Sagsbehandler
Britta Vegeberg
Tel. 72 31 84 25
bve@ufm.dk

Ref.-nr.
19/29773-6

Uddannelses- og forskningsministeren har på baggrund af gennemført prækvalifikation af Aalborg Universitets (AAU) ansøgning om godkendelse af ny uddannelse truffet følgende afgørelse:

Godkendelse af ny kandidatuddannelse i cybersikkerhed (København)

Afgørelsen er truffet i medfør af § 20, stk. 1, nr. 1, i bekendtgørelse nr. 853 af 12. august 2019 om akkreditering af videregående uddannelsesinstitutioner og godkendelse af videregående uddannelser

Det er en forudsætning for godkendelsen, at uddannelsen og dennes studieordning opfylder uddannelsesreglerne, herunder bekendtgørelse nr. 20 af 9. januar 2020 om universitetsuddannelser tilrettelagt på heltid (uddannelsesbekendtgørelsen).

Da AAU er positivt institutionsakkrediteret gives godkendelsen til umiddelbar oprettelse af uddannelsen.

Uddannelses- og forskningsministeren har i sin godkendelse lagt vægt på, at AAU har dokumenteret et behov for uddannelsen, som ikke kan dækkes af eksisterende uddannelser på området.

Hovedområde:
Uddannelsen hører under det teknisk-videnskabelige område.

Titel
Efter reglerne i uddannelsesbekendtgørelsens § 26 og nr. 6.2. i bilag 1, fastlægges uddannelsens titel til:

Dansk: Civilingeniør, cand.polyt. i cybersikkerhed
Engelsk: Master of Science (MSc) in Engineering (Cyber Security)

Udbudssted:
Uddannelsen udbydes på Aalborg Universitet i København.

Sprog:
Ministeriet har noteret sig, at uddannelsen udbydes på engelsk.

Ministeriet bemærker hertil, at det fremgår af § 31, stk. 1, i bekendtgørelse nr. 23 af 9. januar 2020 om adgang til universitetsuddannelser tilrettelagt på heltid (adgangsbekendtgørelsen), at hvis en uddannelse eller væsentlige dele heraf udbydes på engelsk, skal ansøgeren senest inden det tidspunkt, der er fastsat for studiestarten, dokumentere kundskaber i engelsk svarende til mindst engelsk B-niveau.

Normeret studietid:
Efter reglerne i uddannelsesbekendtgørelsens § 25 fastlægges uddannelsens normering til 120 ECTS-point.

Takstindplacering:
Uddannelsen indplaceres til: Heltidstakst 3
Aktivitetsgruppekode: 5360

Styrelsen for Forskning og Uddannelse

Koder – Danmarks Statistik:
UDD: 3168
AUDD: 3168

Censorkorps:
Ministeriet har noteret sig, at uddannelsen tilknyttes ingeniøruddannelsernes landsdækkende censorkorps, censorkorpset for de tekniske diplomuddannelser (Elektronik, IT og Energi) og enkelte censorer fra censorkorpset for datalogi. Det er muligt at supplere censorkorpset, således at det samlede korps bl.a. dækker alle de fag/fagelementer, der indgår i uddannelsen.

Adgangskrav:
Efter det oplyste er følgende uddannelser direkte adgangsgivende til kandidatuddannelsen, jf. § 23, stk. 1, i adgangsbekendtgørelsen:

Aalborg Universitet:
- Bacheloruddannelse i IT, kommunikation og medieteknologi
- Bacheloruddannelse i computerteknologi
- Bachelor i elektronik og IT
- Diplomingeniør i elektronik
- Bacheloruddannelse i datalogi
- Bacheloruddannelse i software
- Bachelor i informationsteknologi

Øvrige danske universiteter:
- Bachelor i elektroteknologi, DTU
- Diplomingeniør i elektroteknologi, DTU
- Bachelor i netværksteknologi og IT, DTU
- Bacheloruddannelse i softwareteknologi, DTU
- Diplomingeniør i softwareteknologi, DTU
- Bacheloruddannelse i softwareudvikling, ITU
- Bachelor i computerteknologi, AU
- Bachelor i elektronik, AU
- Bachelor i electronics, SDU
- Bacheloruddannelse i software engineering, SDU
- Bacheloruddannelse i datalogi, AU, KU og SDU

Herudover skal den studerende have sproglige færdigheder i engelsk svarende til gymnasialt B-niveau jf. ovenfor.

Ministeriet bemærker hertil, at det af hensyn til de studerendes retssikkerhed tydeligt skal fremgå af uddannelsens studieordning samt universitetets hjemmeside, såfremt der er andre uddannelser end de ovenfor nævnte, der anses som adgangsgivende til uddannelsen, jf. § 26, stk. 1, nr. 2, i adgangsbekendtgørelsen.

Ministeriet bemærker endvidere, at AAU, jf. § 26, stk. 2, i adgangsbekendtgørelsen skal fastsætte særlige adgangskrav i kandidatuddannelsernes studieordninger i forhold til optagelse af andre bachelorer.

Retskrav
Ministeriet noterer sig, at der ikke er bacheloruddannelser med retskrav på kandidatuddannelsen.

Styrelsen for Forskning og Uddannelse

Med venlig hilsen

J. Sørensen

Jørgen Prosper Sørensen
Chefkonsulent