

Oplysninger fra CVR

CVR-nummer

45360644

Virksomhedens navn

Erhvervsakademi København S/I

Virksomhedens adresse

Nansensgade 19, 1366 København K

Grundoplysninger

Ansøgningstype

- ☐ Ny uddannelse
- ☐ Nyt udbud af ny uddannelse
- ☒ Nyt udbud af eksisterende uddannelse
- ☐ Dublering af udbud af uddannelse
- ☐ Flytning
- ☐ Ny uddannelsesfilial

Navn på institution

Erhvervsakademi København S/I

Postnummer

3400

Udbudssted

3400 Hillerød

Bynavn

Hillerød

Supplerende bynavn

Er institutionen institutionsakkrediteret?

- ☒ Ja
- ☐ Nej

Er der tidligere søgt om godkendelse af uddannelsen eller udbuddet?

- ☐ Ja
- ☒ Nej

Uddannelsestype

Professionsbacheloruddannelse

Uddannelsens fagbetegnelse dansk

Cybersikkerhed

Uddannelsens fagbetegnelse engelsk

Cyber Security

Uddannelsens officielle titel på dansk

Professionsbachelor i cybersikkerhed

Uddannelsens officielle titel på engelsk

Bachelor of Cyber Security

Hvilket fagområde hører uddannelsen under?

Det tekniske område

Hvilke adgangskrav gælder til uddannelsen?

Adgang via Gymnasial eksamen

Specifikke adgangskrav: Matematik B, Engelsk B

Adgang via 3-årig erhvervsuddannelse

Fuldført erhvervsuddannelse med en normeret varighed på 3 år eller mere

Specifikke adgangskrav: Matematik B, Engelsk B

Anden adgang

Adgangseksamen til ingeniøruddannelserne Specifikke adgangskrav: Matematik B, Engelsk B

Er det et internationalt samarbejde

- ☐ Ja
- ☒ Nej

Hvilket sprog udbydes uddannelsen på?

- ☒ Dansk
☐ Engelsk

Er uddannelsen primært baseret på e-læring?

- ☐ Ja
☒ Nej
☐ Andet

Uddannelsens omfang i antal ECTS-point?

195

Dokumentation af efterspørgsel på uddannelsesprofil

Bilag 1 - Behovsundersøgelse til dansk og engelsk udbud i Hillerød. pdf 435.9 KB

Behov og relevans for det nye udbud

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

Behovsanalysen viser, at der er et betydeligt behov for dimittender med kompetencer inden for cybersikkerhed. Dette understøttes af tidligere nationale og regionale behovsanalyser, EK's jobopslagsanalyse samt interviews med virksomheder og organisationer i Hillerød og Nordsjælland.

Samlet peger dokumentationen på en vedvarende og stigende efterspørgsel efter medar-bejdere, der kan kombinere tekniske cybersikkerhedskompetencer med forretningsforståelse, kommunikation og evnen til at omsætte regulatoriske krav til praksis.

Udviklingen drives af fortsat digitalisering, et mere komplekst trusselsbillede, skærpede regulatoriske krav og stigende krav til digital robusthed i både den offentlige og private sektor.

På den baggrund vurderer Erhvervsakademi København, at der er et klart og veldokumenteret behov for at etablere et udbud af professionsbacheloruddannelsen i cybersikkerhed på både dansk og engelsk i Hillerød.

Udbuddene vil styrke kompetenceforsyningen i Nordsjælland, som forventes at komme til at stå svagere i fremtiden med en øget efter-spørgsel i København, og vil bidrage til at understøtte virksomhedernes og myndighedernes arbejde med cybersikkerhed.

Underbygget skøn over det nationale og regionale behov for dimittender

Erhvervsakademi København forventer et årligt optag på 45 studerende på både det danske og det engelske udbud. Dette vurderes samlet at kunne bidrage med 65-70 dimittender årligt til arbejdsmarkedet.

Dette er baseret på KEAs oprindelige behovsanalyse fra 2024 som henviser til HBS Economis analyse fra 2019, som vurderer, at Danmark frem mod 2030 vil få behov for 130.000 flere medarbejdere indenfor informations- og cybersikkerhed.

De dansksprogede dimittender forventes primært at understøtte arbejdsmarkedet i Nordsjælland, som oplever vanskeligheder med at tiltrække kvalificeret arbejdskraft. Den stigende efterspørgsel efter cybersikkerhedsprofiler i København forventes at øge konkurrencen om arbejdskraften, hvilket vil vanskeliggøre rekruttering for nordsjællandske virksomheder.

De engelsksprogede dimittender forventes både at understøtte kompetenceforsyningen i Nordsjælland og hovedstadsområdet, hvor mange virksomheder arbejder internationalt og anvender engelsk som arbejdssprog.

Da der ikke findes andre engelsksprogede udbud af uddannelsen i hovedstadsområdet, vurderes der at være grundlag for de planlagte 90 studiepladser årligt.

Hvilke aftagere har været inddraget i behovsundersøgelsen?

Behovsafdækningen bygger på både tidligere og nye undersøgelser.

Den oprindelige behovsanalyse, som dannede grundlag for uddannelsens etablering i 2024, omfattede en spørgeskemaundersøgelse med 118 besvarelser samt interviews og dialog med mere end 30 aftagere og interessenter fra private virksomheder, offentlige myndigheder, brancheorganisationer og uddannelsesinstitutioner. Analysen blev suppleret med nationale analyser, arbejdsmarkedsdata og dialog med relevante brancheaktører.

Som led i den aktuelle behovsafdækning har Erhvervsakademi København gennemført kvalitative interviews med centrale aftagere i Hillerød og Nordsjælland, herunder ATP, Hillerød Kommune, VELUX og Region Hovedstaden.

Derudover er der gennemført en regional spørgeskemaundersøgelse blandt virksomheder og organisationer i Nordsjælland.

Behovsafdækningen bygger endvidere på dokumentation vedrørende efterspørgslen efter engelsksprogede cybersikkerhedsuddannelser samt på en analyse af udviklingen i jobopslag inden for cybersikkerhed.

Samlet giver dette et bredt billede af det lokale, regionale og nationale kompetencebehov.

Sammenhæng i uddannelsessystemet

Beskriv ligheder og forskelle til beslægtede uddannelser, herunder beskæftigelse og eventuel dimensionering

Siden EK (tidl. KEA) fik godkendt uddannelsen ved ansøgningsrunden september 2024, er en række andre erhvervsakademier begyndt at udbyde uddannelsen/fået godkendt udbud af uddannelsen. Zealand og Dania har fået godkendt det engelske udbud af uddannelsen. Der er endnu ikke ledighedstal på nogen udbud af uddannelsen.

Institutioner med godkendt udbud af cybersikkerhed:

Dansk uddannelse: EK, Erhvervsakademi Sydvest, Erhvervakademi Midt-Vest, Erhvervsakademi Dania, UCL, EAAA, Erhvervsakademi Kolding, UCN, Zealand

Engelsk uddannelse: Zealand, Erhvervakademi Dania

Uddannelsen er beslægtet med datamatiker, IT-teknolog og top-up i IT-sikkerhed (afvikles jf. reform), som alle har lav ledighed. Fra årgange der dimitterede i 2022 var ledigheden for dimittender 4-7 kvartal efter uddannelse:

IT-sikkerhed. Nationalt: 6,1%, på tidl. KEA 3,8%.

Datamatiker. Nationalt: 8,2%, tidl. KEA: 4,7%, tidl. Cphbusiness: 4,4%.

IT-teknolog. Nationalt: 5,7%, på tidl. KEA: 3,7%.

Hverken PBA i cybersikkerhed eller top-up i IT-sikkerhed er dimensioneret.

Erhvervsakademiuddannelser 2-2 ½ år

- Datamatiker, 2 ½ år (EK, EAAA, Erhvervsakademi SydVest, Dania, Erhvervsakademi MidtVest, Zealand, UCN, UCL)
- IT-teknolog, 2 år (EK, EAAA, Erhvervsakademi Dania, UCL, UCN, Zealand)

Top-up uddannelser, professionsbachelor 1 ½ år (udfases jf. reformen)

- IT-sikkerhed
- Softwareudvikling

Professionsbacheloruddannelser

- Cybersikkerhed (diplomingeniør) (AAU, København)

Bacheloruddannelser

- Cyberteknologi (DTU, Lyngby)
- Cyber- og computerteknologi (AAU, København)

Kandidatuddannelser

- Cybersecurity (AAU, Aalborg og København)
- Computer science and engineering (DTU, Lyngby)

Beskriv rekrutteringsgrundlaget for ansøgte, herunder eventuelle konsekvenser for eksisterende beslægtede udbud

Rekrutteringsgrundlaget vil være de gymnasiale uddannelser og relevante erhvervsuddannelser, [f.eks.](#) data- og kommunikationsuddannelsen.

Uddannelsen differentierer sig fra beslægtede ingeniøruddannelser på AAU og DTU, hvor der er krav om bl.a. matematik på A-niveau.

Professionsbachelor i cybersikkerhed stiller krav om matematik på B-niveau.

På baggrund af adgangskrav og uddannelsens kombination af teknik- og forretningsfag kan uddannelsen tiltrække et bredere udsnit af profiler end beslægtede uddannelser.

Det forventes umiddelbart ikke, at udbuddet har konsekvenser for beslægtede udbud.

Beskriv kort mulighederne for videreuddannelse

En dimittend fra professionsbacheloruddannelsen eller erhvervsakademiuddannelsen i cybersikkerhed vil kunne træde direkte ud på arbejdsmarkedet og varetage vigtige funktioner inden for cybersikkerhed.

Dimittender vil derudover kunne tage relevant efter- og videreuddannelse inden for et bredere felt af IT-uddannelser.

Forventet år for første optag på uddannelsen

EK forventer at optage 45 studerende på uddannelsen. EK anser mindst 40 studerende pr. hold for rentabelt.

Forventet optag på de første 3 år af uddannelsen

1. år

45

2. år

45

3. år

45

Hvis relevant: forventede praktikaftaler

EK er en stor institution, der hvert år sender mange i praktik. Vi har ikke udfordringer med at finde praktikpladser til vores studerende - og dette forventes heller ikke at være en udfordring ift. professionsbacheloruddannelsen i cybersikkerhed. I spørgeskemaundersøgelsen angiver en stor del af virksomhederne i Nordsjælland, at de ønsker at have praktikanter fra uddannelsen.

Godkend og send ansøgningen

Øvrige bemærkninger til ansøgningen

EK søger både et dansk og et engelsk udbud af cybersikkerhed i Hillerød. Dette gøres ud fra tre vigtige hensyn:

- 1) Dels vurderer vi, at der er et udækket behov dimittender med kompetencer indenfor cybersikkerhed i Nordsjælland, hvilket er godtgjort i ansøgningen.
- 2) Herudover er det en vigtig prioritet for EK, at vi ikke vil have for små fagmiljøer, da vi mener, at det ikke er hensigtsmæssigt i forhold til de studerendes læring og undervisningens kvalitet. Etablering af både et dansk- og et engelsksproget udbud vi give grundlag for at etablere et sundt og stærkt fagmiljø.
- 3) Endelig vurderer vi, at etablering af både et dansk og et engelsk udbud, vil styrke integrationen af særligt de engelsksprogede studerende, som ofte mangler netværk i Danmark. Her vil flere danske medstuderende være medvirkende til at skabe et større netværk blandt danske studerende i Danmark, hvilket efter vores overbevisning også vil øge sandsynligheden for, at de engelsksprogede studerende vælger at søge job i Danmark efter endt uddannelse.

Det bekræftes hermed at ansøgningen er godkendt af Rektor

- ☒ Ja
☐ Nej

Kontaktperson og kontaktoplysninger

Navn

Jon Allix Olsen

Email

joao@ek.dk

Telefonnummer

30548874

Bilag 1 - Behovsundersøgelse for dansk- og engelsksproget udbud af professionsbacheloruddannelsen i cybersikkerhed i Hillerød

Indledning og metode

Uddannelsen PBA i Cybersikkerhed blev etableret på KEA i sommeren 2025 på baggrund af en behovsundersøgelse, som blev gennemført i foråret/sommeren 2024. I denne behovsundersøgelse påviste KEA et stort behov for at uddanne dimittender med kompetencer indenfor cybersikkerhed på professionsbachelorniveau. Dette behov blev igen dokumenteret i 2026 af Zealand, som her ud over også dokumenterede et behov for at udbyde uddannelsen på engelsk.

I dag udbydes uddannelsen i København på dansk, men Erhvervsakademi København (Tidligere KEA og Cphbusiness) vurderer, at der er et særligt behov for at udvide optaget udenfor København både på dansk og på engelsk. På Erhvervsakademi København (EK) vurderer vi, at den oprindelige ansøgning om uddannelse og udbud fra KEA 2024 samt ansøgningen om den engelske uddannelse og udbuddet på både dansk og engelsk fra Zealand i 2026 dokumenterer, at der fortsat er et behov for at uddanne personer indenfor cybersikkerhed på dansk og engelsk i hovedstadsområdet. For at underbygge dette, samt at underbygge behovet for at etablere disse udbud i Hillerød, har vi foretaget en mindre undersøgelse om de specifikke forhold i Hillerød og Sjælland nord for Hillerød.

Således bygger denne ansøgning samt behovsundersøgelsen på Erhvervsakademi Københavns (tidl. KEA) ansøgning om professionsbacheloruddannelsen i cybersikkerhed fra 2024 (dansk) samt Zealands ansøgning om ny professionsbachelor i Cyber Security fra 2026. I begge ansøgninger vises behovet for medarbejdere med kompetencer inden for cybersikkerhed.

Herudover har vi i forhold til denne specifikke ansøgning gennemført fem kvalitative interviews med repræsentanter for virksomheder i Hillerød og Nordsjælland samt gennemført en mindre spørgeskemaundersøgelse med ca. 20 besvarelser.

Hvilke aftagere har været inddraget i behovsundersøgelsen?

Behovsafdækningen bygger på både tidligere og nye undersøgelser gennemført i forbindelse med udviklingen af professionsbacheloruddannelsen i cybersikkerhed. Den oprindelige behovsanalyse, som dannede grundlag for uddannelsens etablering i 2024, omfattede en spørgeskemaundersøgelse med 118 besvarelser samt interviews og dialogaktiviteter med mere end 30 aftagere og interessenter fra private virksomheder, offentlige myndigheder, brancheorganisationer og uddannelsesinstitutioner. Analysen blev desuden understøttet af nationale analyser, arbejdsmarkedsdata og løbende dialog med relevante brancheaktører.

Den foreliggende behovsafdækning bygger herudover på den dokumentation af behovet for engelsksprogede dimittender inden for cybersikkerhed, som blev udarbejdet i forbindelse med EA Zealands ansøgning om et engelsksproget udbud af uddannelsen i 2026.

Her ud over har vi til denne ansøgning suppleret med fem kvalitative interviews med relevante aftagere i Nordsjælland samt en mindre spørgeskemaundersøgelse med 20 besvarelser.

Af navngivne virksomheder som vi har gennemført interviews med kan nævnes Hillerød Kommune, ATP, Velux og Region Hovedstaden. En af de virksomheder, der deltog i kvalitative interviews, har ikke ønsket at indgå med navn. Af

virksomheder, som deltog i spørgeskemaundersøgelsen var både store og små, offentlige og private virksomheder herunder eksempelvis FC Nordsjælland, DLF Seeds, Furesø Kommune, Bravida og SanSteel.

Behov og relevans for det nye udbud

Behovet for medarbejdere med kompetencer inden for cybersikkerhed er i dag omfattende og stigende. Cybersikkerhed er blevet et strategisk samfundsanliggende, hvor både offentlige myndigheder, private virksomheder og organisationer i stigende grad er afhængige af sikre digitale systemer, data og infrastrukturer. Samtidig er trusselsbilledet blevet mere komplekst som følge af øget digitalisering, voksende regulatoriske krav og et stigende antal cyberangreb. Der er derfor et betydeligt behov for medarbejdere, som kan forebygge, identificere, håndtere og afbøde cybersikkerhedshændelser samt understøtte organisationers arbejde med compliance, governance, risikostyring og sikkerhedskultur. Dette behov er dokumenteret gennem både nationale analyser, brancheundersøgelser og behovsanalyser gennemført i forbindelse med etableringen af professionsbacheloruddannelsen i cybersikkerhed.

I forbindelse med udviklingen af professionsbacheloruddannelsen i cybersikkerhed gennemførte KEA i 2024 en omfattende behovsanalyse blandt virksomheder, offentlige organisationer, brancheorganisationer og myndigheder. Analysen viste en bred enighed om, at der er mangel på kvalificeret arbejdskraft inden for cybersikkerhed, og at manglen forventes at vokse i de kommende år. Blandt de adspurgte aftagere forventede 97 % et stigende behov for cybersikkerhedsmedarbejdere inden for de næste fem år. Samtidig havde over halvdelen af virksomhederne forsøgt at rekruttere medarbejdere inden for cybersikkerhed de seneste år, og blandt disse havde mere end to tredjedele oplevet væsentlige udfordringer med at finde kandidater med de nødvendige kompetencer. Mange virksomheder havde måttet nøjes med delvist kvalificerede kandidater eller helt opgive at besætte stillingerne.

Behovet understøttes af nationale analyser af arbejdsmarkedet. I den dokumentation, som lå til grund for uddannelsens etablering, vurderes det, at Danmark frem mod 2030 vil mangle op mod 13.000 medarbejdere med kompetencer inden for informations- og cybersikkerhed. Samtidig viste data indsamlet i forbindelse med behovsanalysen et meget stort antal stillingsopslag, hvor cybersikkerhed eller IT-sikkerhed indgik som centrale kompetencekrav. Samlet peger analyserne på, at efterspørgslen efter cybersikkerhedskompetencer allerede i dag overstiger udbuddet af kvalificeret arbejdskraft, og at denne ubalance forventes at vokse yderligere i takt med digitaliseringen af samfundet.

De gennemførte analyser peger samtidig på, at arbejdsmarkedet ikke alene efterspørger tekniske specialister. Tværtimod fremhæver arbejdsgivere på tværs af sektorer et stort behov for medarbejdere, der kan kombinere tekniske kompetencer med forståelse for forretning, governance, compliance, risikostyring og kommunikation. Moderne cybersikkerhed handler ikke alene om teknologi, men i lige så høj grad om kommunikation, organisatoriske processer, ledelse, regulering og implementering i komplekse organisationer. Virksomheder og myndigheder efterspørger derfor medarbejdere, som kan fungere i spændingsfeltet mellem teknik og forretning og omsætte sikkerhedshændelser- og krav til konkrete løsninger i praksis. Dette behov blev fremhævet af både offentlige myndigheder, kommuner, brancheorganisationer og private virksomheder i forbindelse med udviklingen af uddannelsen.

Behovet for cybersikkerhedskompetencer forstærkes yderligere af et stigende cybertrusselsniveau og skærpede regulatoriske krav. Dansk Erhverv peger i udspillet *Sådan styrker vi Danmarks digitale sikkerhed* (2025) på, at cybertruslernes voksende omfang og kompleksitet stiller nye krav til både den offentlige og den private sektors digitale robusthed. Organisationen fremhæver, at virksomheder i stigende grad skal kunne håndtere krav relateret til blandt andet cybersikkerhed, governance, compliance og risikostyring, og at dette kræver adgang til kvalificeret

arbejdskraft med relevante kompetencer. Særligt små og mellemstore virksomheder har blandt andet behov for medarbejdere, som kan omsætte komplekse sikkerheds- og compliancekrav til konkrete løsninger i den daglige drift.

Digitaliseringen af samfundskritiske funktioner, produktionsapparater, forsyningskæder og serviceydelser har samtidig gjort cybersikkerhed til et grundvilkår for en bred kreds af virksomheder og organisationer. Kompetencebehovet handler derfor ikke alene om teknisk specialisering, men også om evnen til at forstå regulatoriske krav og organisatoriske processer samt omsætte disse til praksis i konkrete drifts- og udviklingsmiljøer. Dette skaber et tydeligt sammenfald mellem arbejdsmarkedets efterspørgsel og professionsbacheloruddannelsens kompetenceprofil, der netop kombinerer tekniske cybersikkerhedskompetencer med governance, compliance, kommunikation og forretningsforståelse.

I 2026 gennemførte Zealand en supplerende behovsanalyse med særligt fokus på den engelsksprogede professionsbacheloruddannelse i cybersikkerhed. Analysen bekræfter de konklusioner, der blev identificeret i forbindelse med den oprindelige uddannelsesansøgning, og viser samtidig, at virksomheder og organisationer i Region Sjælland og Hovedstadsregionen i stigende grad efterspørger medarbejdere med internationale kompetencer. Zealands analyse peger på betydelige rekrutteringsudfordringer inden for cybersikkerhed og dokumenterer, at mange virksomheder oplever et behov for engelsksprogede medarbejdere, som kan arbejde i internationale miljøer, håndtere internationale kunder og leverandører samt understøtte efterlevelsen af internationale standarder og reguleringer.

Siden KEA gennemførte behovsanalysen i 2024, er den geopolitiske situation blevet yderligere præget af øget ustabilitet og skærpet stormagtskonkurrence. Europas sikkerhedspolitiske virkelighed er i stigende grad påvirket af Ruslands fortsatte aggression mod Ukraine, en mere kompleks relation til Kina samt en voksende usikkerhed om de fremtidige transatlantiske relationer og Europas strategiske afhængigheder. Denne udvikling har medført et øget fokus på forsyningsikkerhed, beskyttelse af kritisk infrastruktur, teknologisk suverænitæt og digital robusthed på både europæisk og nationalt niveau.

I denne sammenhæng indtager cybersikkerhed en stadig større og mere central rolle. Cyberangreb anvendes i stigende grad som et strategisk redskab i internationale konflikter og rammer ikke alene myndigheder og forsvarsrelaterede aktiviteter, men også virksomheder, forsyningsvirksomheder, sundhedssektoren, produktionsvirksomheder og andre samfundskritiske funktioner. Samtidig er moderne organisationer blevet mere afhængige af digitale systemer, cloudløsninger og globale værdikæder, hvilket øger sårbarheden over for både statslige og ikke statslige aktører.

Udviklingen har medført et markant politisk og regulatorisk fokus på cybersikkerhed i Europa. Implementeringen af blandt andet NIS2-direktivet, Cyber- og informationssikkerhedsstrategien, skærpede krav til informationssikkerhed og øgede krav til dokumentation, risikostyring og compliance betyder, at et stigende antal organisationer skal opbygge interne kompetencer inden for cybersikkerhed. Behovet omfatter ikke alene højt specialiserede eksperter, men i høj grad også praksisnært uddannede medarbejdere, som kan omsætte tekniske, organisatoriske og regulatoriske krav til konkrete løsninger i organisationernes daglige drift.

Denne udvikling understøtter de konklusioner, som allerede blev dokumenteret i forbindelse med KEAs behovsanalyse fra 2024 og Zealands behovsanalyse fra 2026, hvor både virksomheder, offentlige myndigheder og brancheorganisationer pegede på betydelige rekrutteringsudfordringer og et voksende behov for medarbejdere med cybersikkerhedskompetencer. Den geopolitiske udvikling siden den første behovsundersøgelse for denne uddannelse i 2024 giver således ikke anledning til at antage, at behovet for dimittender fra professionsbacheloruddannelsen i cybersikkerhed er aftaget. Tværtimod peger udviklingen på, at behovet for medarbejdere, der kan styrke danske virksomheders og myndigheders digitale robusthed og modstandsdygtighed, er blevet yderligere forstærket.

Nordsjælland er kendetegnet ved et højt aktivitetsniveau inden for produktion, life science, offentlig drift, kritisk infrastruktur og teknologibaserede servicevirksomheder. Det er sektorer, der i stigende grad er afhængige af digitale systemer og data og derfor også særligt eksponerede over for cybertrusler. Dialogen med relevante virksomheder og

organisationer i Hillerød peger på, at både private og offentlige arbejdsgivere fortsat efterspørger medarbejdere inden for cybersikkerhed, som kan kombinere tekniske kompetencer med praktisk anvendelse i produktion, drift og organisatorisk forankring. Behovet knytter sig ikke alene til specialistfunktioner, men også til medarbejdere, der kan bidrage til at implementere og vedligeholde sikkerhedsforanstaltninger på tværs af organisationens daglige aktiviteter.

Professionsbacheloruddannelsen i cybersikkerhed er fortsat en ny uddannelse og har kun haft optag siden sommeren 2025. Det eksisterende dokumentationsgrundlag fra Erhvervsakademi Københavns ansøgning om uddannelsen i 2024 samt Zealands ansøgning om et engelsksproget udbud i 2026 viser imidlertid et betydeligt og veldokumenteret behov for dimittender med uddannelsens kompetenceprofil. Samtidig er der ikke identificeret forhold, der indikerer, at det nationale eller regionale behov for cybersikkerhedskompetencer er blevet mindre siden de oprindelige analyser blev gennemført. Tværtimod peger både digitaliseringsudviklingen, det aktuelle trusselsbillede og de stigende regulatoriske krav på, at behovet fortsat er voksende.

På den baggrund vurderer Erhvervsakademi København, at der fortsat er et væsentligt og dokumenteret behov for at udvide kapaciteten inden for cybersikkerhedsuddannelser i hovedstadsområdet. Etableringen af et udbud af professionsbacheloruddannelsen i cybersikkerhed på både dansk og engelsk i Hillerød vil bidrage til at imødekomme arbejdsmarkedets behov for kvalificeret arbejdskraft, styrke virksomhedernes og myndighedernes adgang til relevante kompetencer og understøtte den digitale robusthed i Nordsjælland og det øvrige Sjælland.

Regulatorisk pres og regionalt kompetencebehov i Nordsjælland

Nordsjælland er kendetegnet ved en høj koncentration af life science-, medico- og lægemiddelvirksomheder, sundhed samt virksomheder, der indgår i kritiske forsynings- og værdikæder. Denne erhvervsprofil betyder, at regionen i særlig grad påvirkes af nye nationale og europæiske krav til cyber- og informationssikkerhed.

Implementeringen af NIS2 og Cyber- og informationssikkerhedsstrategien medfører, at et langt større antal virksomheder og offentlige organisationer nu er omfattet af krav til risikostyring, sikkerhedsforanstaltninger, hændeshåndtering og ledelsesansvar. Kravene omfatter blandt andet sundhedssektoren, digital infrastruktur, fremstillingsindustri og offentlige myndigheder, som alle er stærkt repræsenteret i Nordsjælland. Cybersikkerhed er derfor ikke længere alene en teknisk disciplin, men en integreret del af organisationers governance, compliance, drift og modstandsdygtighed.

Samtidig er mange virksomheder i regionen underlagt reguleringer, der stiller omfattende krav til sikkerhed, dataintegritet, sporbarhed og dokumentation. I disse miljøer kan cyberhændelser få alvorlige konsekvenser for drift, myndighedsgodkendelser og patientsikkerhed. Det skaber behov for medarbejdere, der kan arbejde i krydsfeltet mellem teknologi, kvalitet, regulering og forretning.

Det samlede regulatoriske pres øger efterspørgslen efter praksisnære cybersikkerhedskompetencer. Virksomheder og offentlige organisationer har behov for medarbejdere, der kan omsætte krav fra NIS2, DORA, ISO27001, sikkerhedsloven og lov om informationssikkerhed til konkrete sikkerhedstiltag og complianceprocesser. Behovet kan ikke alene dækkes af højt specialiserede kandidater, men kræver også professionsrettede dimittender, som kan indgå direkte i overvågnings-, drifts-, udviklings- og kvalitetsopgaver.

EK har bl.a. haft dialog med en større produktionsvirksomhed (anonym) med ca. 2000 medarbejdere og med hovedsæde i Hillerød. Virksomhedens Head of Information Security beskriver, at de oplever et behov for at øge antallet af medarbejdere inden for cybersikkerhed de næste år. Han beskriver samtidig, hvordan det kan være svært at rekruttere de rigtige profiler til Nordsjælland, da de mister mange pga. transporten til fra København til Nordsjælland.

Et udbud af professionsbacheloruddannelsen i cybersikkerhed i Hillerød vil bidrage til at dække dette kompetencebehov og styrke adgangen til kvalificeret arbejdskraft i Nordsjælland. Uddannelsen vil understøtte

virksomhedernes og de offentlige aktørers arbejde med at efterleve regulatoriske krav og sikre robuste cyber- og informationssikkerhedsmiljøer.

Et engelsksproget udbud af uddannelsen

Cybersikkerhedsområdet er karakteriseret ved et arbejdsmarked, hvor mange virksomheder opererer internationalt, samarbejder på tværs af landegrænser og anvender engelsk som koncernsprog eller dagligt arbejdssprog. I mange virksomheder foregår samarbejdet med kunder, leverandører, udviklingsmiljøer og sikkerhedsleverandører i forvejen på engelsk, og cybersikkerhedsarbejdet tager i vid udstrækning udgangspunkt i internationale standarder, værktøjer, dokumentation og reguleringer.

Et engelsksproget udbud vil samtidig gøre det muligt at tiltrække en bredere og delvist anderledes gruppe af studerende end et rent dansksproget udbud. Dermed udvides rekrutteringsgrundlaget til uddannelsen, samtidig med at arbejdsmarkedet får adgang til flere dimittender med relevante cybersikkerhedskompetencer. Dette er særligt relevant i en situation, hvor både tidligere behovsanalyser og dialogen med aftagere peger på vedvarende udfordringer med at rekruttere kvalificerede medarbejdere inden for cybersikkerhed. Et engelsksproget udbud kan derfor bidrage til at afhjælpe eksisterende mangel på arbejdskraft ved at tiltrække internationale studerende, som efter endt uddannelse kan indgå på det danske arbejdsmarked.

Dialogen med virksomheder og organisationer i forbindelse med etableringen af uddannelsen understøtter denne vurdering. Flere aftagere har fremhævet værdien af medarbejdere, der kan indgå i internationale samarbejder og arbejde i engelsksprogede miljøer. Samtidig har ingen af de virksomheder og organisationer, der har bidraget til behovsafdækningen, peget på engelsksprogede kompetencer som en udfordring i relation til ansættelse af dimittender. Tværtimod vurderes engelskkundskaber i mange tilfælde som en fordel eller som et neutralt forhold, fordi engelsk allerede indgår som en naturlig del af virksomhedernes daglige arbejde.

Mens det dansksprogede udbud i Hillerød primært forventes at understøtte kompetencebehovet i Hillerød og det øvrige Nordsjælland, vurderes det engelsksprogede udbud at have et større geografisk dækningsområde. Da der ikke findes andre engelsksprogede professionsbachelorudbud i cybersikkerhed i hovedstadsområdet, vil dimittender fra et engelsksproget udbud i Hillerød kunne bidrage til at dække virksomhedernes behov for cybersikkerhedskompetencer på tværs af hele hovedstadsregionen. Et sådant udbud vil derfor både styrke virksomhedernes adgang til kvalificeret arbejdskraft og bidrage til at sikre et større samlet udbud af cybersikkerhedskompetencer i regionen.

Kvalitative interviews med virksomhedsrepræsentanter

For at belyse det konkrete arbejdsmarkedsbehov i Hillerød og Nordsjælland har EK gennemført fem kvalitative interviews med repræsentanter fra både offentlige og private organisationer i området, herunder kommunal sektor, sundhedssektoren, større produktionsvirksomheder og samfundskritiske organisationer.

Interviewpersonerne kommer fra følgende virksomheder:

- ATP
- Region Hovedstaden
- Velux
- Hillerød Kommune
- En større dansk virksomhed, som ønsker at være anonym

Interviewene bekræfter de konklusioner, der fremgår af de nationale og regionale behovsanalyser, og peger samlet set på et fortsat stort behov for medarbejdere med kompetencer inden for cybersikkerhed.

Virksomhederne beskriver et arbejdsmarked, hvor cybersikkerhed i stigende grad er blevet en integreret del af organisationernes drift og udvikling. En repræsentant fra en større IT-afdeling i en nordsjællandsk kommune udtrykker dette meget klart ved at sige at "alle mine folk arbejder med cybersikkerhed som en del af lige præcis deres kompetencer, men jeg tror at vi bare må erkende at behovet for cybersikkerhedsfolk er stigende."

Tilsvarende beskriver en større produktionsvirksomhed med hovedsæde i Hillerød, at behovet for medarbejdere inden for cybersikkerhed er voksende: "Der er et stigende behov. Vi skal opruste."

Interviewene viser samtidig, at cybersikkerhedsopgaver i praksis løses gennem en kombination af interne medarbejdere og eksterne leverandører. Flere organisationer beskriver, hvordan governance, compliance, risikostyring og sikkerhedsledelse i høj grad håndteres internt, mens mere specialiserede eller overvågningsintensive opgaver løses af eksterne samarbejdspartnere. Dermed vil dimittender fra uddannelsen både kunne understøtte virksomheders egne cybersikkerhedsfunktioner og indgå i de specialiserede virksomheder, som leverer cybersikkerhedsydelser til andre organisationer.

Flere af de interviewede virksomheder peger desuden på konkrete udfordringer med at rekruttere medarbejdere inden for cybersikkerhed. Den kommunale repræsentant fortæller, at organisationen måtte slå den samme stilling op flere gange, før rekrutteringen lykkedes: "Vi brugte 3 opslag før vi var i mål, reelt er lønforskel på privat og offentlig her en udfordring."

En anden større privat virksomhed beskriver tilsvarende udfordringer med at tiltrække kvalificerede kandidater til Nordsjælland: "Det er svært at rekruttere gode profiler til Nordsjælland, vi mister mange på transporten fra København, samtidigt er de dygtige dyre."

Også ATP, som har hovedkontor i Hillerød og omkring 3.000 medarbejdere, beskriver betydelige udfordringer med rekruttering af cybersikkerhedsprofiler. Organisationen har de seneste år rekrutteret blandt andet sikkerhedsspecialister, sikkerhedsarkitekter og medarbejdere til Security Operations-funktioner, men peger på både geografiske og markedsmæssige udfordringer: "Rekrutteringen har dog været udfordrende. ATPs hovedkontor er placeret i Hillerød, hvilket kan gøre transporten fra Københavnsområdet relativt tidskrævende." og videre: "Der er stor efterspørgsel på erfarne cybersikkerhedsprofiler, [og] det har været en udfordring at tiltrække og rekruttere de rette kandidater til de stillinger, vi har besat gennem de seneste to år."

Interviewene viser samtidig, at virksomhederne efterspørger kompetencer, der går ud over rent tekniske færdigheder. Der lægges stor vægt på medarbejdere, som kan kombinere teknisk forståelse med forretningsforståelse, kommunikation og organisatorisk indsigt. ATP fremhæver eksempelvis, at uddannelsens kompetenceprofil er relevant, fordi organisationen arbejder bredt med blandt andet governance, sikkerhedsstrategi, compliance, sikkerhedsarkitektur, Security Operations og beskyttelse af kritisk digital infrastruktur. Virksomheden fremhæver: "Særligt evnen til at omsætte tekniske problemstillinger til målrettet kommunikation over for både interne og eksterne interessenter er en væsentlig kompetence i vores daglige arbejde."

Samme tendens ses hos de øvrige aftagere. En kommune understreger vigtigheden af, at cybersikkerhedsmedarbejdere kan kommunikere med både ledelse og medarbejdere: "Jeg tror det er enormt vigtigt, at der undervises i kompetencer til at være forståelige både overfor topledelse, men også for den enkelte medarbejder."

En større international produktionsvirksomhed efterspørger tilsvarende dimittender med forretningsforståelse og evnen til at arbejde risikobaseret: "Det er vigtigt for os, at de nyuddannede [...] er forberedt på en risikobaseret virkelighed, hvor det ikke handler om blindt at forfølge best practice, men derimod at vælge de bedste løsninger på de udfordringer som forretningen har." og konkluderer: "Altså er basal forretningsforståelse en nødvendighed."

Endelig viser interviewene, at virksomhederne generelt er positive over for et engelsksproget uddannelsesudbud. Flere virksomheder arbejder allerede helt eller delvist på engelsk, og ingen af de interviewede vurderer, at engelsksprogede dimittender udgør en udfordring. En international produktionsvirksomhed fremhæver, at

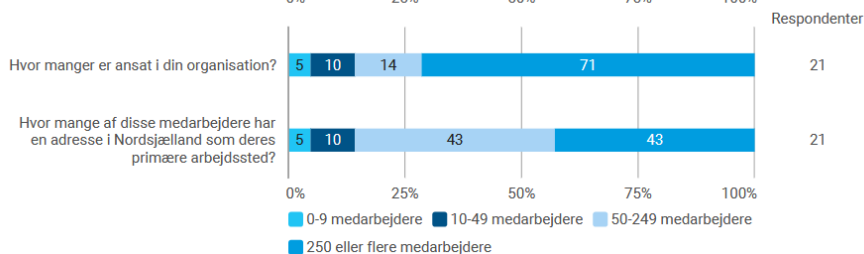
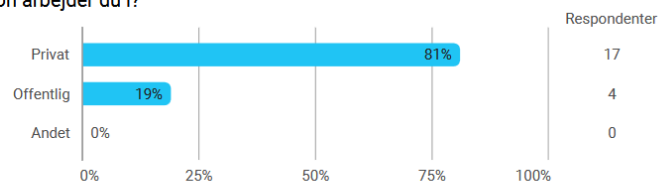
"koncernsproget er engelsk", mens en anden virksomhed understreger, at "den generelle lingo i sikkerhed er på engelsk". Andre organisationer peger på, at engelskkundskaber ikke udgør et problem i sig selv, så længe dimittenderne kan begå sig i organisationen.

Samlet peger interviewene på et arbejdsmarked i Nordsjælland, hvor efterspørgslen efter cybersikkerhedskompetencer fortsat er høj, hvor virksomheder og offentlige organisationer oplever konkrete rekrutteringsudfordringer, og hvor der er behov for dimittender, som kan kombinere tekniske cybersikkerhedskompetencer med forretningsforståelse, kommunikation og praktisk anvendelse. Interviewene understøtter dermed vurderingen af, at der er et væsentligt regionalt behov for et udbud af professionsbacheloruddannelsen i cybersikkerhed i Hillerød.

Spørgeskemaundersøgelse blandt virksomheder i Nordsjælland

Som supplement til de kvalitative interviews har vi gennemført en mindre spørgeskemaundersøgelse blandt virksomheder og offentlige organisationer i Nordsjælland. I alt blev 24 besvarelser påbegyndt, hvoraf 18 blev gennemført. Respondenterne repræsenterer både private og offentlige organisationer inden for blandt andet industri, rådgivning, kommunal sektor, IT, service og produktion, og størstedelen af de deltagende organisationer har en betydelig del af deres medarbejdere placeret i Nordsjælland.

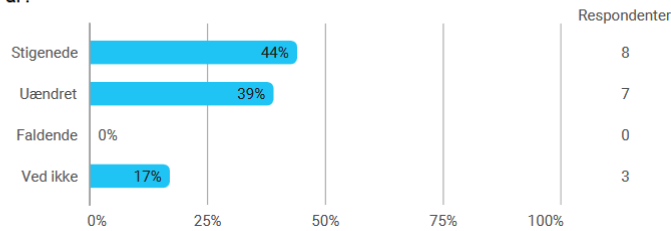
Hvilken type organisation arbejder du i?



Undersøgelsen skal ses som et supplement til den øvrige behovsafdækning, og datagrundlaget er relativt begrænset. Resultaterne giver derfor ikke grundlag for stærke statistiske konklusioner. Til gengæld bidrager undersøgelsen med interessante indikationer af, hvordan cybersikkerhedsområdet opfattes blandt virksomheder og organisationer i Nordsjælland.

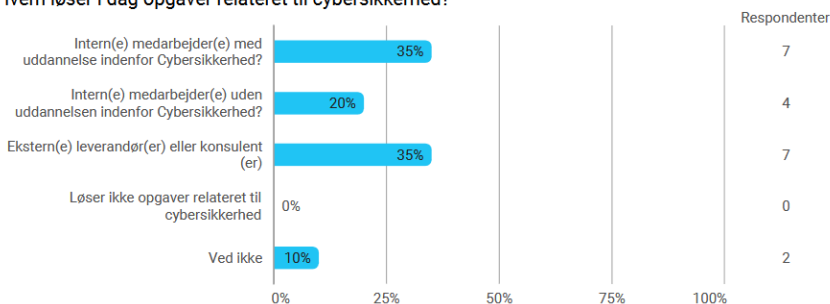
En af de mest markante observationer er, at ingen af respondenterne forventer et faldende behov for medarbejdere med cybersikkerhedskompetencer inden for de kommende fem år. Tværtimod vurderer 44 % af respondenterne, at behovet vil være stigende, mens 39 % forventer et uændret behov. Samlet peger dette på en forventning om, at cybersikkerhed også fremover vil være et vigtigt og vedvarende kompetenceområde for virksomhederne i regionen.

Hvordan ser du behovet for at rekruttere medarbejdere, der kan arbejde med cybersikkerhed, indenfor de næste fem år?



Undersøgelsen viser samtidig, at cybersikkerhedsopgaver allerede i dag spiller en væsentlig rolle i mange organisationer. Blandt respondenterne angiver 35 %, at cybersikkerhedsopgaver varetages af medarbejdere med formel uddannelse inden for området, mens 20 % anvender interne medarbejdere uden specifik cybersikkerhedsuddannelse. Hertil kommer, at 35 % får løst opgaverne gennem eksterne leverandører eller konsulenter. Ingen respondenter angiver, at de ikke arbejder med cybersikkerhed. Resultaterne understreger således, at cybersikkerhed er et relevant arbejdsområde for hovedparten af de deltagende virksomheder og organisationer.

Hvem løser i dag opgaver relateret til cybersikkerhed?



Ved første øjekast fremstår virksomhedernes umiddelbare interesse for at ansætte dimittender fra uddannelsen mere afdæmpet. 34 % vurderer, at det i høj eller meget høj grad vil være relevant at ansætte en dimittend fra uddannelsen, mens 39 % vurderer, at det i mindre grad eller slet ikke vil være relevant. De åbne kommentarer peger imidlertid på, at disse svar i flere tilfælde ikke skyldes manglende behov for cybersikkerhedskompetencer, men snarere virksomhedernes størrelse eller organisering. Flere respondenter angiver eksempelvis, at cybersikkerhed håndteres af eksterne specialister eller af centrale koncernfunktioner. En virksomhed skriver:

”Dimittender vil ikke være relevante for vores virksomhed, da vores størrelse gør, at cybersikkerhed altid vil blive løst af eksterne partnere.” En anden respondent anfører: ”Vi er nok for lille en virksomhed til at have en med så specifikt et ansvarsområde.” Mens en tredje bemærker: ”Vi har alt med cybersikkerhed kommende fra vores amerikanske HQ, derfor denne besvarelse. Havde vi ikke haft det, ville jeg have svaret at det var vigtigt for os at rekruttere med denne uddannelse.”

Disse besvarelser peger på en vigtig pointe: Efterspørgslen efter cybersikkerhedskompetencer kommer ikke nødvendigvis til udtryk som et direkte behov hos den enkelte virksomhed for at ansætte egne specialister. For mange virksomheder dækkes behovet i stedet gennem eksterne cybersikkerhedsleverandører, konsulentbureau eller interne specialistfunktioner placeret andre steder i koncernen. Det betyder, at den samlede efterspørgsel efter cybersikkerhedskompetencer kan være større, end virksomhedernes direkte ansættelsesinteresse umiddelbart giver indtryk af.

Set i sammenhæng med, at næsten halvdelen af respondenterne forventer et stigende behov for cybersikkerhedskompetencer, kan undersøgelsen også indikere, at efterspørgslen efter specialiserede cybersikkerhedsleverandører og konsulenttydelser vil fortsætte med at vokse. Dette vil øge behovet for uddannede

cybersikkerhedsmedarbejdere både hos virksomheder, der ønsker egne kompetencer, og hos de specialiserede virksomheder, som leverer cybersikkerhedsydelser til erhvervslivet. Dermed understøtter undersøgelsen vurderingen af, at et øget udbud af dimittender med cybersikkerhedskompetencer vil kunne bidrage til at styrke den samlede kompetenceforsyning i regionen.

Samlet set understøtter spørgeskemaundersøgelsen således de øvrige resultater i behovsanalysen. Selvom datagrundlaget er begrænset, peger besvarelsene på et arbejdsmarked, hvor cybersikkerhed allerede er et væsentligt kompetenceområde, hvor behovet forventes at være stabilt eller stigende i de kommende år, og hvor efterspørgslen efter cybersikkerhedskompetencer både kommer til udtryk gennem virksomhedernes egne rekrutteringsbehov og gennem anvendelsen af eksterne specialister og leverandører.

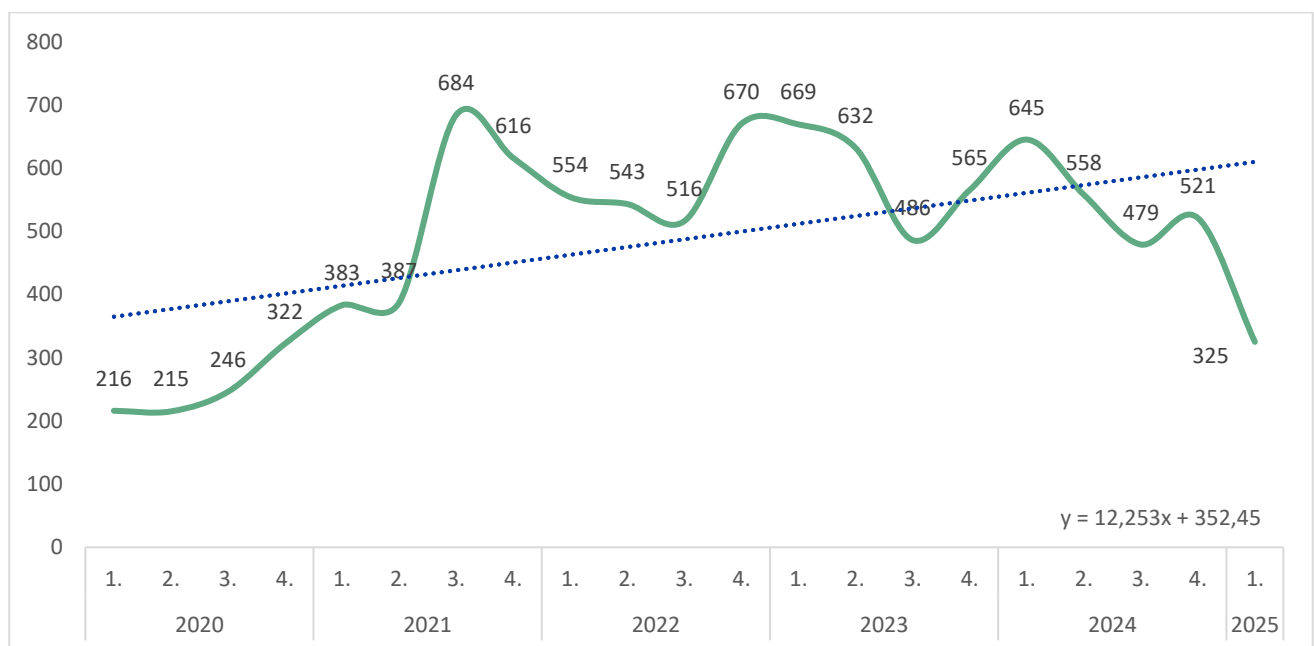
Jobopslagsanalyse

EK har via programmet Watson undersøgt jobopslag indenfor cybersikkerhed. Figur 1 viser den kvartalsvis udvikling i antallet af jobopslag indenfor cybersikkerhed i hele landet fra januar 2020 til og med marts 2025. Det ses på figuren, at der har været et større udsving i antallet af jobopslag med kompetencer indenfor cybersikkerhed fra 2. kvartal 2020 til 1. kvartal 2024. Det kan skyldes Covid19 og den stigende efterspørgsel af arbejdskraft, vi så på det danske arbejdsmarked i den efterfølgende periode. Derudover viser tal fra Rambøll og Dansk IT's rapport 'IT i praksis 2023-24', at cybersikkerhed er den absolut største bekymring i de danske virksomheder i 2023, men at halvdelen af de private virksomheder og 43 % af de offentlige organisationer ikke besidder kompetencerne til at håndtere det stigende trusselsniveau (Rambøll, 2023). Det kan dermed forklare den stigning, vi har set i antallet af jobopslag indenfor cybersikkerhed siden 2020.

På figuren kan vi se et fald i antallet af jobopslag siden 1. kvartal 2024. Vi har set samme udvikling for det samlede antal jobopslag i Danmark, der fortsat er på et højt niveau, men faldende.

Den lineære tendenslinje viser dog, at efterspørgslen af denne type dimittender er stigende. I hele perioden er den kvartalsvis stigning på ca. 12 jobopslag indenfor cybersikkerhed.

Figur 1: Kvartalsvis antal jobopslag med kompetencer indenfor cybersikkerhed i Danmark



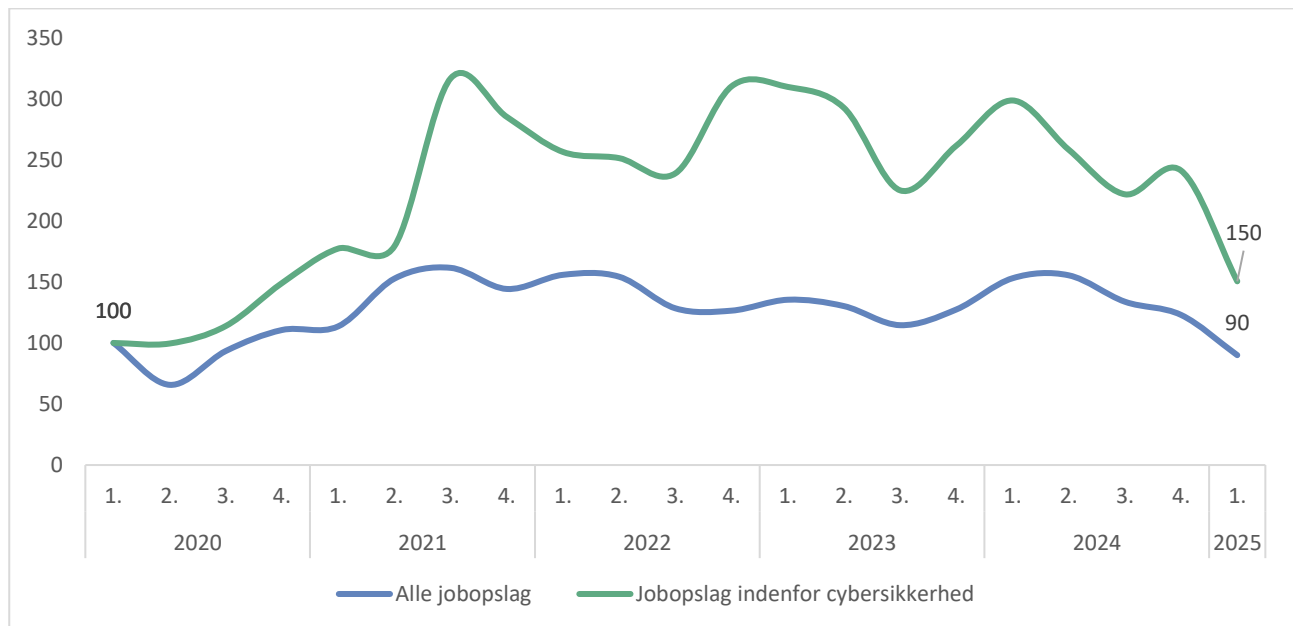
Kilde: Egen søgning i IBM Watson Explorer

Note: Data er opgivet på kvartalsniveau, og udviklingen inden for årene kan derfor være påvirket af sæsoneffekter. Datamærkaterne angiver antal jobopslag i kvartalet. Vi har søgt på jobopslag, der indeholder ordene cybersikkerhed, IT-sikkerhed, netværkssikkerhed, softwaresikkerhed, datasikkerhed, IT-security, Cyber security, IT compliance, IT Governance, IT security og network security.

Blandt disse jobopslag er det IT-sikkerhedsspecialister og softwareudviklere, der er særligt efterspurgt, og virksomhederne med flest opslag er Forsvaret, Forsvarets Efterretningstjeneste, Novo Nordisk, The Hub, Politiet, Graduateland og Banedanmark.

For at undersøge, om efterspørgslen blot følger den generelle udvikling i jobopslag i Danmark, har vi lavet en sammenligning af de indekserede udviklinger i samtlige jobopslag i hele landet og jobopslag inden for cybersikkerhed i hele landet.

Figur 2: Indekseret udvikling i jobopslag for hele landet (Basiskvartal = 2020)



Kilde: Egen søgning i IBM Watson Explorer

Note: Figuren viser det indekserede antal jobopslag. Indeks 100 viser antallet af jobopslag i 1. kvartal 2020. Data er opgivet på kvartalsniveau, og udviklingen inden for årene kan derfor være påvirket af sæsoneffekter. Datamærkaterne angiver det indekserede antal jobopslag i 1. kvartal 2020 og 1. kvartal 2025.

Figur 2 viser, at antallet af jobopslag inden for cybersikkerhed i hele landet er steget med 50% i perioden fra 1. kvartal 2020 til og med 1. kvartal 2025. I samme periode er samtlige antal jobopslag i hele landet faldet med 10%.

Det skal bemærkes, at der er markant færre jobopslag inden for cybersikkerhed end det samlede antal jobopslag i landet, og der skal derfor mere til for at vi ser udsving i den nationale udvikling.

Konklusion

Samlet set viser behovsanalysen, at der fortsat er et betydeligt og voksende behov for dimittender med kompetencer inden for cybersikkerhed.

De nationale og regionale analyser, som lå til grund for etableringen af professionsbacheloruddannelsen i cybersikkerhed i 2024, dokumenterede et omfattende kompetencebehov blandt både offentlige og private arbejdsgivere.

Dette billede understøttes af EK's jobopslagsanalyse, som viser, at antallet af jobopslag med krav om cybersikkerhedskompetencer er steget markant siden 2020 og har udviklet sig væsentligt mere positivt end arbejdsmarkedet generelt. Selvom antallet af opslag har varieret fra år til år, viser analysen en langsigtet stigende efterspørgsel efter cybersikkerhedskompetencer.

Der er ikke identificeret forhold, som siden har reduceret dette billede. Tværtimod peger den fortsatte digitalisering, implementeringen af nye regulatoriske krav, den geopolitiske udvikling samt et komplekst trusselsbillede med stigende hybride trusler, der kombinerer destruktive cyberangreb, des- og misinformation på, at efterspørgslen efter cybersikkerhedskompetencer er blevet yderligere forstærket.

De gennemførte interviews med virksomheder og organisationer i Hillerød og Nordsjælland bekræfter dette billede. Aftagerne beskriver konkrete rekrutteringsudfordringer, stigende behov for cybersikkerhedskompetencer og et ønske om medarbejdere, der kan kombinere teknisk indsigt med forretningsforståelse, kommunikation og praktisk anvendelse. Samtidig peger både interviewene og spørgeskemaundersøgelsen på, at cybersikkerhed i stigende grad er blevet en integreret del af virksomhedernes og de offentlige organisationers drift, og at behovet for kompetencer på området forventes at være stabilt eller stigende i de kommende år.

Nordsjælland rummer en høj koncentration af virksomheder og organisationer inden for blandt andet life science, produktion, kritisk infrastruktur, sundhed og offentlig administration. Disse sektorer er i særlig grad påvirket af de stigende krav til informations- og cybersikkerhed og har derfor behov for kvalificeret arbejdskraft, der kan omsætte tekniske, organisatoriske og regulatoriske krav til praksis. Et lokalt udbud i Hillerød vil styrke virksomhedernes adgang til relevante kompetencer og samtidig bidrage til at imødekomme de dokumenterede rekrutteringsudfordringer i området.

Der vurderes desuden at være et særskilt behov for et engelsksproget udbud. Et engelsksproget udbud vil udvide rekrutteringsgrundlaget til uddannelsen, tiltrække internationale studerende og styrke virksomhedernes adgang til arbejdskraft i et fagområde, hvor mange virksomheder arbejder internationalt og anvender engelsk som arbejdssprog. Da der ikke findes andre engelsksprogede professionsbachelorudbud i cybersikkerhed i hovedstadsområdet, vil et engelsksproget udbud i Hillerød kunne understøtte kompetenceforsyningen i hele hovedstadsregionen.

På denne baggrund vurderer Erhvervsakademi København, at der er et klart og veldokumenteret behov for at etablere et udbud af professionsbacheloruddannelsen i cybersikkerhed på både dansk og engelsk i Hillerød. Disse udbud vil bidrage til at styrke kompetenceforsyningen i Nordsjælland og hovedstadsområdet, understøtte virksomhedernes og myndighedernes arbejde med cybersikkerhed og bidrage til at styrke Danmarks digitale robusthed og modstandsdygtighed.