



**Uddannelses- og
Forskningsministeriet**

Prækvalifikation af videregående uddannelser - Cybersikkerhed

Udskrevet 7. april 2026

Professionsbachelor - Cybersikkerhed - Zealand - Sjællands Erhvervsakademi

Institutionsnavn: Zealand - Sjællands Erhvervsakademi

Indsendt: 01/02-2026 11:08

Ansøgningsrunde: 2026-1

Status på ansøgning: Indsendt

[Download den samlede ansøgning](#)

[Læs hele ansøgningen](#)

Ansøgningstype

Ny uddannelse

Udbudssted

Næstved

Informationer på kontaktperson for ansøgningen (navn, email og telefonnummer)

Navn: Stine Rohde Frederiksen Email: stfr@zealand.dk Telefon: 5076 2781

Er institutionen institutionsakkrediteret?

Ja

Er der tidligere søgt om godkendelse af uddannelsen eller udbuddet?

Nej

Uddannelsestype

Professionsbachelor

Uddannelsens fagbetegnelse på dansk

Cybersikkerhed

Uddannelsens fagbetegnelse på engelsk

Cyber Security

Angiv den officielle danske titel, som institutionen forventer at bruge til den nye uddannelse

Professionsbachelor i cybersikkerhed

Angiv den officielle engelske titel, som institutionen forventer at bruge til den nye uddannelse

Bachelor of Cyber Security

Hvilket hovedområde hører uddannelsen under?

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, herunder Erasmus, fællesuddannelse el. lign.?

Nej

Hvis ja, hvilket samarbejde?

Hvilket sprog udbydes uddannelsen på?

Engelsk

Er uddannelsen primært baseret på e-læring?

Nej, undervisningen foregår slet ikke eller i mindre grad på nettet.

ECTS-omfang

210

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

Det skal indledningsvist bemærkes, at denne ansøgning bygger på uddannelsesansøgningen udarbejdet af Erhvervsakademi København, godkendt ved ansøgningsrunden i 2024. Da uddannelsen fortsat er under implementering og endnu ikke har genereret tilstrækkelige erfarings- og datagrundlag, vurderes det, at det på nuværende tidspunkt ikke vil være fagligt eller metodisk meningsfuldt at foretage selvstændige ændringer eller suppleringer i forhold til den allerede godkendte uddannelsesmodel.

Formålet med den engelsksprogede uddannelse er at uddanne internationale studerende til at håndtere tekniske og organisatoriske udfordringer inden for cybersikkerhed i både offentlige og private organisationer. Uddannelsen giver kompetencer til at udvikle, implementere og vedligeholde løsninger og processer, der forebygger, identificerer og afbøder cybertrusler i komplekse it-miljøer.

Undervisningen foregår på engelsk og kombinerer praksisnær erfaring med teoretisk indsigt gennem anvendelse af relevante metoder, værktøjer og systemer. Case-baseret undervisning, virksomheds-samarbejde og praktikforløb sikrer, at dimittenderne opnår konkret erfaring og hurtigt kan skabe værdi i internationale arbejdsmiljøer.

Uddannelses struktur og konstituerende faglige elementer

Den engelsksprogede professionsbacheloruddannelse i Cybersikkerhed er struktureret i overensstemmelse med den eksisterende danske uddannelse, som Zealand udbyder. Uddannelsens faglige indhold, opbygning og læringsmål er således identiske, mens undervisningssproget er engelsk og uddannelsen har en tydelig international profil målrettet internationale studerende.

Uddannelsen er tilrettelagt som et fuldtidsstudium over 3½ år (210 ECTS) og kombinerer teoretisk undervisning, praksisnære øvelser, projektarbejde og et obligatorisk praktikophold.

Fra gældende BEK nr 445 af 07/05/2025, bilag 1 om PBA i cybersikkerhed indsættes:

Formål og erhvervsigte: Formålet med professionsbachelor i cybersikkerhed er at kvalificere den uddannede til at kunne fungere selvstændigt som cybersikkerhedsspecialist med fokus på at arbejde med fortrolighed, integritet og tilgængelighed i forbindelse med udvikling, drift og sikkerhedsledelse af it-systemer i såvel private som offentlige virksomheder og organisationer.

Normering: Uddannelsen er normeret til 210 ECTS-point, der omfatter:

- 1) Uddannelseselementer med et samlet omfang på 160 ECTS-point, der tilrettelægges inden for uddannelsens faglige områder.
- 2) Praktik med et samlet omfang på 30 ECTS-point.

3) Bachelorprojekt på 20 ECTS-point.

Fagområder: Uddannelseselementerne tilrettelægges inden for følgende fagområder, der samlet set omfatter 160 ECTS-point, og som er indbyrdes vægtet i forholdet 1:1:1.

1) Cybersikkerhedsledelse, -governance og -processer: Fagområdet indeholder viden om governance, ledelsesværktøj og processer til at forhindre, overvåge, detektere og reagere over for trusler mod fortrolighed, integritet og tilgængelighed af systemer og applikationer. Fagområdet omhandler selvstændig organisering og ledelse af sikkerhedsarbejdet i organisationer og virksomheder samt principper, standarder og best practices i cybersikkerhed, herunder etiske, juridiske, politiske og ledelsesmæssige aspekter af cybersikkerhedsarbejde.

2) Netværkssikkerhed, detektering og arkitektur: Fagområdet indeholder netværksarkitekturer, medier og protokoller samt redskaber til at forhindre, overvåge, detektere og reagere over for trusler mod fortrolighed, integritet og tilgængelighed af netværkss kommunikation. Fagområdet indeholder de tekniske komponenter, som udgør de forskellige IT-systemer.

3) Software- og datasikkerhed og automation: Fagområdet indeholder sikkerhedsperspektivet i software, blandt andet programkvalitet og betydning af fejl- og datahåndtering for en software-arkitekturs sårbarheder. Fagområdet indeholder sikkerhedsdesignprincipper. Desuden indeholder fagområdet tiltag til kryptering og lagring samt automatisering, basal scripting og programmering.

Nationale og lokale uddannelseselementer: Uddannelseselementerne tilrettelægges som

1) Nationale fagelementer med et samlet omfang på 100 ECTS-point, der er fælles for uddannelsens studerende og fastsættes i den nationale del af studieordningen.

2) Lokale fagelementer med samlet omfang på 60 ECTS-point, der tilrettelægges under hensyntagen til lokale og regionale behov og fastsættes i institutionsdelen af studieordningen. De lokale fagelementer skal omfatte valgfag i et omfang, der mindst svarer til 5 ECTS-point.

Afstigning til:

Erhvervsakademiuddannelse i operationel cybersikkerhed

Uddannelsens navn: Erhvervsakademiuddannelse inden for operationel cybersikkerhed (Academy Profession Degree Programme in Operational Cyber Security)

Betegnelse: Uddannelsen giver den uddannede ret til at anvende betegnelsen AK i operationel cybersikkerhed (AP Graduate in Operational Cyber Security)

Formål og erhvervsigte: Formålet med uddannelsen er at kvalificere den uddannede til at kunne indgå i samarbejde om cybersikkerhedsopgaver med fokus på at arbejde med fortrolighed, integritet og tilgængelighed i forbindelse med udvikling, drift og support af it-systemer i såvel private som offentlige virksomheder og organisationer.

Normering: Uddannelsen er normeret til 120 ECTS-point, der omfatter:

- 1) Uddannelseselementer med et samlet omfang på 90 ECTS-point, der tilrettelægges inden for uddannelsens faglige områder.
- 2) Praktik med et samlet omfang på 20 ECTS-point.
- 3) Afsluttende eksamensprojekt på 10 ECTS-point.

Fagområder: Uddannelseselementerne tilrettelægges inden for følgende fagområder, der samlet set omfatter 90 ECTS-point, og som er indbyrdes vægtet i forholdet 1:1:1. →1) Forretningsforståelse, governance og kommunikation: Fagområdet omhandler kommunikation og tilrettelæggelse af sikkerhedsarbejdet i organisationer og virksomheder samt principper og best practice i cybersikkerhed, herunder etiske, juridiske, politiske og forretningsmæssige aspekter af cybersikkerhedsarbejde.

2) Netværkssikkerhed og arkitektur: Fagområdet indeholder netværksarkitekturer, medier og protokoller samt redskaber til at forhindre, detektere og reagere over for trusler mod fortrolighed, integritet og tilgængelighed af netværksskommunikation. Fagområdet indeholder de tekniske komponenter, som udgør de forskellige IT-systemer. →3) Programmering, datasikkerhed og automation: Fagområdet indeholder sikkerhedsperspektivet i datahåndtering, blandt andet fejlhåndtering og lagringsstrategier. Desuden indeholder fagområdet tiltag til kryptering samt automatisering, basal scripting og programmering.

Nationale og lokale uddannelseselementer: Uddannelseselementerne tilrettelægges som

- 1) Nationale fagelementer med et samlet omfang på 60 ECTS-point, der er fælles for uddannelsens studerende og fastsættes i den nationale del af studieordningen.
- 2) Lokale fagelementer med samlet omfang på 30 ECTS-point, der tilrettelægges under hensyntagen til lokale og regionale behov og fastsættes i institutionsdelen af studieordningen. De lokale fagelementer skal omfatte valgfag i et omfang, der mindst svarer til 5 ECTS-point.

Begrundet forslag til takstindplacering af uddannelsen

Som det danske udbud.

Forslag til censorkorps

Eksisterende censorkorps for uddannelsen

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

Bilag 1, Cybersikkerhed.pdf

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

En rapport fra den sikkerhedspolitiske analysegruppe viser, at der på nationalt plan vil mangle op mod 20.000 fuldtidsressourcer inden for cybersikkerhed i 2030. Samtidig viser It-Branchens medlemsundersøgelse for 2025, at halvdelen af it-virksomhederne i Region Sjælland efterspørger kompetencer inden for it-sikkerhed og compliance. Den nye uddannelse vil afhjælpe manglen på disse kompetencer. Det er dokumenteret at internationale medarbejdere er de rette kompetencematch for virksomhederne. Dette er afdækket af Dansk Erhverv, der i 2024 udgav en analyse, som viser, at internationale medarbejdere er en betydelig gevinst for Danmarks økonomi arbejdsmarked for virksomheder.

Zealand vil med et nyt udbud uddanne kandidater, der kan afhjælpe den manglende specialiseret arbejdskraft nationalt, men også regionalt, da professionsbacheloren i cybersikkerhed ikke findes på engelsk. Zealands behovsanalyse, som er baseret på en spørgeskemaundersøgelse og interviews til aftagere med 32 besvarelser, understøtter, at både offentlige og private virksomheder og organisationer i Region Sjælland og Hovedstaden har et behov for cybersikkerhedskompetencer fra engelsksprogede med en international profil.

Zealands aftagere udtrykker rekrutteringsudfordringer med cybersikkerhedsspecialister med internationale baggrunde og har et kritisk behov for at ansætte studerende og dimittender, blandt andet grundet kravene fra NIS 2 og mødet med det globale marked og internationale kunder. De studerende med en PBA i Cybersikkerhed på engelsk vil hermed særligt kunne bidrage med tværkulturel og sproglig forståelse inden for fagområdet.

Se herudover også bilag 1, behovsanalyse, for uddybende redegørelse.

Uddybende bemærkninger

Se bilag 1, behovsanalyse, for uddybende redegørelse.

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

Som tidligere nævnt er uddannelsen ny, og har kun haft et enkelt optag i sommeren 2025 på det danske udbud af uddannelsen på landsplan. Der henvises derfor til uddannelsesansøgningen for den nye uddannelse PBA i cybersikkerhed ved prækvalifikationen i september 2024, der vurderer det nationale behov for dimittender fra uddannelsen. Her vurderes det, at der er et endog meget højt behov for dimittender, og at behovet ikke dækkes af de eksisterende uddannelser.

Det skal hertil tilføjes, at der ikke er noget der tyder på, at behovet for cybersikkerhedskompetencer er ændret siden da - snarere tværtimod. Det antages derfor, at behovet for dimittender for på det internationale udbud af PBA i Cybersikkerhed er mindst lige så højt.

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

Behovsundersøgelsen er gennemført som en kombination af spørgeskemaundersøgelse, interviews og desk research. Zealand har i vinteren 2026 haft dialog med i alt 32 virksomheder og organisationer i Region Sjælland, udvalgt på baggrund af branche, virksomhedsstørrelse og geografisk placering samt via sneboldmetoden. Aftagerne omfatter både private og offentlige organisationer inden for cybersikkerhed, IT-drift, software, industri, medico og offentlig IT. Blandt de inddragede aftagere er bl.a. cybersikkerhedsvirksomheder (fx CSIS, Cyber Nordic), større internationale virksomheder (fx Novo Nordisk), IT-service- og softwarevirksomheder, offentlige myndigheder (fx Vurderingsstyrelsen og Koncern IT Region Sjælland) samt brancheorganisationen IT-Branchen. Virksomhederne har bidraget via skriftlige og telefoniske besvarelser, hvor de er blevet spurgt ind til behovet for internationale dimittender, relevante kompetencer samt villighed til at aftage praktikanter. Heraf har 16 aftagere eksplicit tilkendegivet støtte til etableringen af en engelsksproget PBA i Cybersikkerhed. Undersøgelsen er suppleret med nationale og regionale analyser fra bl.a. IT-Branchen, Erhvervsstyrelsen og Dansk Erhverv.

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

Sammenhængen mellem det påviste behov og uddannelsen er sikret gennem inddragelse af aftagere i behovsanalysen samt ved, at uddannelsens kompetenceprofil og faglige indhold direkte adresserer de efterspurgte kompetencer.

Det efterspurgte kompetencebehov er afspejlet i uddannelsens fagområder, som kombinerer cybersikkerhedsledelse, governance og processer med netværks-, software- og datasikkerhed samt automation. Undervisningen gennemføres på engelsk og tilrettelægges praksisnært med cases, virksomhedsinddragelse og praktik, hvilket aftagerne specifikt har efterspurgt.

Herudover er uddannelsens indhold identisk med den allerede godkendte danske PBA i Cybersikkerhed, som er udviklet på baggrund af nationale kompetencekrav, men suppleres med en international profil, der matcher virksomhedernes behov for engelsksprogede specialister. Aftagernes tilkendegivelse af villighed til både at ansætte dimittender og aftage praktikanter understøtter, at uddannelsen matcher et reelt og aktuelt arbejdsmarkedsbehov.

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

PBA i cybersikkerhed adskiller sig fra beslægtede uddannelser ved at være målrettet cybersikkerhed som selvstændigt fagområde og ved at kombinere tekniske, organisatoriske og governance-mæssige kompetencer i én sammenhængende uddannelse.

Beslægtede erhvervsakademi- og professionsbacheloruddannelser, herunder datamatiker, IT-teknolog og top-up-uddannelser inden for IT-sikkerhed, har primært fokus på enten programmering, IT-drift eller teknisk IT-sikkerhed og indeholder ikke en tilsvarende helhedsorienteret tilgang til cybersikkerhed.

Det engelsksprogede udbud vurderes ikke at have negative beskæftigelsesmæssige eller dimensioneringsmæssige konsekvenser for beslægtede uddannelser, idet rekrutteringsgrundlaget primært vil være internationale studerende, som i dag ikke har adgang til sammenlignelige uddannelsesudbud på professionsbachelorniveau i Danmark. Udbuddet forventes dermed at supplere det eksisterende uddannelseslandskab og bidrage til at dække et dokumenteret kompetencebehov uden at fortrænge eksisterende udbud.

Uddybende bemærkninger

Se også afdækning fra uddannelsesansøgningen på det danske udbud af PBA i cybersikkerhed for uddybning.

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

Rekrutteringen vil primært ske blandt internationale studerende, der i øjeblikket ikke har mulighed at søge ind på andre engelsksprogede udbud af andre erhvervsakademi-/professionsbacheloruddannelser i Danmark. Det vurderes derfor ikke, at dette udbud vil påvirke andre udbud hos hverken Zealand eller andre uddannelsesudbydere i landet.

Herudover ser det, at der til det danske udbud af uddannelsen er en massiv søgning. Fx oplevede KEA (nu EK) at få 197 førsteprioritetsansøgninger og 431 ansøgninger i alt til 80 studiepladser i sommeren 2025 (<https://www.ek.dk/om-os/nyheder/cybersikkerhed-stormer-ind-rekordmange-ansoegere>). Antagelsen er derfor, at enkelte dygtige, danske studerende også vil overveje at søge ind på det engelsksprogede udbud.

Beskriv kort mulighederne for videreuddannelse

Dimittender fra professionsbacheloruddannelsen i cybersikkerhed vil være kvalificerede til umiddelbart at indgå på arbejdsmarkedet og varetage centrale opgaver inden for cybersikkerhedsområdet.

Ønsker dimittenderne på et senere tidspunkt at videreuddanne sig, vil det være muligt at kigge på muligheder for en kandidatuddannelse.

Det vurderes dog ikke, at denne mulighed vil være relevant for langt de fleste dimittender.

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

2027: 65 studerende

2028: 65 studerende

2029: 65 studerende

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

Der er allerede etableret dialog med relevante aftagere inden for både offentlige og private organisationer, herunder virksomheder og institutioner med behov for kompetencer inden for it-drift, informationssikkerhed og cybersikkerhed. Aftagerne har generelt givet udtryk for interesse i at indgå i praktiksamarbejder, da praktikopholdene understøtter deres rekrutteringsbehov og bidrager med konkrete, anvendelsesorienterede kompetencer.

Zealand har gode kontakter til erhvervslivet, og disse vil ligeledes indgå i det videre udviklingsarbejde med dette udbud. Det vurderes derfor, at der også fremadrettet vil kunne indgås et tilstrækkeligt antal praktikaftaler til at understøtte uddannelsens praktikforløb. Udbuddet forventes ikke at få negative konsekvenser for beslægtede uddannelser, idet praktikopholdene i vid udstrækning vil rette sig mod aftagere med specifikt fokus på cybersikkerhed, og da der i forvejen er betydelig efterspørgsel efter studerende inden for området.

Øvrige bemærkninger til ansøgningen

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

Ja

Status på ansøgningen

Indsendt

Ansøgningsrunde

2026-1

Afgørelsesbilag - Upload PDF-fil

Samlet godkendelsesbrev - Upload PDF-fil

Behovsanalyse

Prækvalifikation af engelsk udbud af PBA Cybersikkerhed

Indhold

Introduktion	2
Behovsanalysens hovedkonklusioner	3
Anvendte metoder	4
Udvælgelse af virksomheder og organisationer	4
Spørgeskema og interviews	4
Desk-research	7
Behovsanalysen	7
Nationalt behov for arbejdskraft	7
Regionale perspektiver på manglende arbejdskraft.....	9
Stort behov for specialister hos virksomheder med internationalt fokus	12
Rekrutteringsudfordringer blandt virksomhederne	14
Mangel på for arbejdskraft fra internationale.....	19
Praktikmuligheder for studerende med en international profil.....	20
Uddannelsens kompetenceprofil.....	22
Uddannelsens indhold	22
Konklusion.....	26
Støtteerklæring	27
Kilder	28

Introduktion

“En international profil er ikke blot at foretrække, men også i høj grad nødvendig.” Sådan lyder det fra Novo Nordisk, én af de aftagere i indeværende behovsanalyse, som støtter oprettelsen af et engelsk udbud af PBA i Cybersikkerhed. Manglen på specialiseret arbejdskraft inden for cybersikkerhed i Danmark er allerede i dag markant og forventes at tiltage yderligere i de kommende år.

Som led i udmøntning af reform af professions- og erhvervsrettede uddannelser har Zealand fået mulighed for at oprette op til 100 internationale uddannelsespladser. Zealand ønsker at udmønte 65 af disse engelsksprogede pladser med henblik på at imødekomme et veldokumenteret regionalt og nationalt behov for internationale dimittender inden for cybersikkerhed.

Det skal indledningsvist bemærkes, at denne prækvalifikationsansøgning helt grundlæggende bygger på uddannelsesansøgningen udarbejdet af Erhvervsakademi København, godkendt ved ansøgningsrunden i september 2024. Da uddannelsen fortsat er under implementering og endnu ikke har genereret tilstrækkelige erfarings- og datagrundlag, vurderes det, at det på nuværende tidspunkt ikke vil være fagligt eller metodisk meningsfuldt at foretage selvstændige ændringer eller suppleringer i forhold til den allerede godkendte uddannelsesmodel.

Efterspørgslen efter dimittender med kompetencer indenfor cybersikkerhed kan ikke imødekommes af danske dimittender alene. Virksomheder og offentlige organisationer i og omkring Region Sjælland peger på udfordringer med både rekruttering og fastholdelse af kvalificerede medarbejdere, hvilket nødvendiggør adgang til et bredere og mere internationalt rekrutteringsgrundlag.

Danmark rummer en bred vifte af private virksomheder og offentlige institutioner, som i stigende grad er afhængige af sikre digitale løsninger og robust it-infrastruktur. Implementeringen af blandt andet NIS 2-direktivet, øget digitalisering samt et voksende trusselsbillede skaber et presserende behov for højt specialiserede kompetencer inden for it-sikkerhed, risikostyring, compliance og beskyttelse af kritiske systemer og data.

Zealand ønsker på denne baggrund at udbyde professionsbacheloren i cybersikkerhed på engelsk for at tiltrække internationale studerende, som kan bidrage til at dække arbejdsmarkedets behov i og omkring Region Sjælland. Et engelsksproget udbud vurderes samtidig at styrke uddannelsens faglige miljø og relevans, idet cybersikkerhed er et globalt fagområde, hvor trusler, standarder og løsninger i vid udstrækning er internationale.

Dialogen med aftagere viser, at der er stor opbakning til en international uddannelse i cybersikkerhed, og at virksomhederne gerne vil ansætte internationale dimittender. Dimittender fra den internationale professionsbachelor forventes derfor at have særdeles gode beskæftigelsesmuligheder i Region Sjælland.

Behovsanalysens hovedkonklusioner

- Der er et stort og stigende nationalt og regionalt behov for cybersikkerhedsspecialister, som ikke imødekommes af danske dimittender alene.
- Behovsanalysen viser et meget stort behov for cybersikkerhedskompetencer fra internationale dimittender med en PBA i Cybersikkerhed hos virksomheder og organisationer i og omkring Region Sjælland.
- Der er betydelige rekrutterings- og fastholdelsesudfordringer inden for cybersikkerhed i Region Sjælland og på landsplan.
- Heraf har internationale medarbejdere i høj grad indflydelse på at afhjælpe beskæftigelsesvæksten og kompetencebehovene hos virksomhederne.
- Efterspørgslen retter sig i stigende grad mod engelsksprogede medarbejdere, som kan arbejde professionelt i internationale og tværkulturelle sammenhænge.
- Internationale medarbejdere vurderes som centrale for implementering og efterlevelse af internationale krav og reguleringer, herunder NIS2, ISO-standarder og GDPR.
- Dialogen med Zealands aftagere viser bred opbakning til etableringen af en engelsksproget PBA i Cybersikkerhed, herunder villighed til at ansætte dimittender og modtage praktikanter.

Anvendte metoder

For bedst muligt at kunne afdække behovet for uddannelsen i Region Sjælland har Zealand udarbejdet en analyse baseret på en spørgeskemaundersøgelse, kvalitative interviews og desk-research.

Udvælgelse af virksomheder og organisationer

I vinteren 2026 fik Zealand kontakt til 32 virksomheder og organisationer på tværs af Region Sjælland og Hovedstaden, som alle fandt det relevant at bidrage til et projekt om behovet for en engelsksproget PBA i Cybersikkerhed hos Zealand. Deltagerne blev udvalgt fra det offentlige CVR-register ud fra virksomhedsstørrelse, branche og geografisk placering samt gennem sneboldmetoden, hvor eksisterende kontakter henviste til yderligere virksomheder. Zealand har inddraget både store virksomheder samt SMV'er fra IT-sektoren, da begge virksomhedstyper har betydelig risiko for at blive udsat for cybertrusler. Herunder har op imod 40% af de store virksomheder oplever udfordringer med at øge deres it-sikkerhedsniveau.¹

Zealand har også været i dialog med en chefkonsulent i brancheorganisationen IT-Branchen. Brancheorganisationen, der har ca. 800 medlemsvirksomheder inden for IT- og cybersikkerhedssektoren understøtter behovet for at oprette cybersikkerhedsuddannelsen på engelsk i Zealand og har udarbejdet en støtteerklæring i denne forbindelse (se nederst i materialet).

Spørgeskema og interviews

De virksomheder, Zealand rakt ud til fik tilsendt spørgsmål gennem mail, som tog udgangspunkt i behovet for relevant arbejdskraft fra engelsksprogede studerende og dimittender med en PBA i Cybersikkerhed. Virksomhedernes besvarelser på de tilsendte spørgsmål fungerede som tilkendegivelser af, at de støtter op om at udbyde uddannelsen på Zealand. Mens nogle af virksomhederne svarede skriftligt, var der andre som besvarede spørgsmålene telefonisk. Et overblik over spørgsmålene ses i tabellen nedenfor.

¹Erhvervsstyrelsen (2024): "Digital Sikkerhed i danske SMV'er", Styrelsen for Samfundssikkerhed December (2024): " Digital sikkerhed i danske SMV'er 2024"

Spørgsmål
Har din virksomhed behov for professionsbachelorer i cybersikkerhed med en international profil?
Hvad vurderer du en professionsbachelor i cybersikkerhed med en international profil vil kunne bidrage med i virksomheden?
Hvordan vurderer du behovet for denne type kompetencer i Region Sjælland generelt ?
Vil din virksomhed være interesseret i at aftage praktikanter fra uddannelsen?

I forlængelse af tabellen blev deltagerne spurgt ind til cybersikkerhedsuddannelsens internationale profil og dens relevans for virksomheden samt hvilke kompetencer, som de efterspørger hos deres internationale medarbejdere. I forlængelse af forrige afsnit repræsenterer deltagerne mulige brancher, som professionsbachelorerne i cybersikkerhed, som er engelsksprogede, potentielt kan arbejde og komme i praktik i. Blandt de interviewede er der både inddraget private og offentlige arbejdspladser.

Et overblik over Zealands aftagere og deres karakteristika ses nedenfor:

Virksomhed	Virksomhedstype	Navn	Stilling
Cyber Nordic	Cybersikkerhedsvirksomhed	Morten Holm Gregeresen	Direktør og stifter
LS Control	Industrielektronikvirksomhed	Per Nielsen	CEO
SeeSafe	Sikkerhedsteknologivirksomhed	Henrik Sjøberg	COO
Searine	Maritim teknologivirksomhed (søtransport)	Anders Hovmøller	CEO
TD-K	IT- og servicevirksomhed	Ibrahim Ramku	CTO
Safepay Nordic	Fintech-virksomhed	Jesper Malmberg	Partner

CSIS	Cybersikkerhedsvirksomhed	Christiane Hjerrild	Direktør
Novo Nordisk	Medicinalvirksomhed	Lorena Ronquillo	Sikkerhedsarkitekt
Koncern IT Region Sjælland	Offentlig IT-organisation	Emma Brix Jørgensen	HR-konsulent
SimpleGroup	IT- og digitaliseringskoncern	Allan Bo Christiansen	CCO
Triple Arm Technique	Softwarevirksomhed	Lahib Youssef	CEO /Senior Software Developer
Vurderingsstyrelsen	Offentlig myndighed	Lars Blomgaard	IT-Security Arkitekt
KeepIT	IT-servicevirksomhed	Itamar Lokzinsky	Security Operation Center Manager
Connexa A/S	IT-drifts- og cybersikkerhedsvirksomhed	Thomas Schmidt	Direktør og partner
Nesp.ONE ApS	Computerkonsulent- og it-servicefirma	Martin Schulze	Direktør

Nedenfor ses brancheorganisationen IT-branchen, som også støtter op om at åbne en PBA i cybersikkerhed med en international profil hos Zealand:

Brancheorganisation	Stilling
IT-Branchen	Chefkonsulent

Som tidligere nævnt har Zealand i alt 32 fået besvarelser. Heraf har 16 af disse virksomheder og organisationer nået at vende tilbage og tilkendegive, at de støtter op om åbningen af den engelsksprogede PBA i Cybersikkerhed i Zealand. Det vil sige, at der er et betydeligt behov for internationale medarbejdere blandt virksomhederne og organisationer, idet halvdelen af de adspurgte støtter op om etableringen af den engelsksprogede PBA i Cybersikkerhed på Zealand.

Desk-research

Regionale og nationale undersøgelser, rapporter og statistikker er inddraget for at tydeliggøre udviklingen af behovet for cybersikkerhedskompetencer fra engelsktalende studerende og dimittender. Dokumenterne er produceret af statslige styrelser og brancheorganisationer (se sidst i analysen for kildehenvisninger).

Behovsanalysen

Nationalt behov for arbejdskraft

I 2022 udgav Den Sikkerhedspolitiske Analysegruppe en rapport, som vurderer, at Danmark frem mod 2030 vil komme til at mangle op mod 20.000 medarbejdere med kompetencer inden for cybersikkerhed. I forlængelse heraf peger brancheorganisationen IT-Branchen på udfordringerne med at rekruttere kvalificeret arbejdskraft på området:

”Allerede i 2030 vurderes Danmark at mangle op mod 20.000 fuldtidsressourcer inden for cyber- og informationssikkerhed. Derfor bør strategien indeholde en samlet plan for, hvordan optaget på cybersikkerhedsuddannelserne øges, nye uddannelser oprettes, og hvordan cybersikkerhed i højere grad integreres i øvrige, relevante (it-)uddannelser.”²

Udtalelsen understreger, at det stadig mere komplekse og alvorlige trusselsbillede har skabt betydelige rekrutteringsudfordringer inden for cybersikkerhed. Samtidig viser en rapport fra Erhvervsstyrelsen, at 40 % af små og mellemstore virksomheder har et utilstrækkeligt cybersikkerhedsniveau, hvilket yderligere tydeliggør behovet for flere uddannede specialister på området.³

IRIS-group (mfl.) har derudover udarbejdet en omfattende analyse, der sætter fokus på den nuværende overefterspørgsel efter personer med mellemlange videregående uddannelser (MVU) og it-baggrund mod 2030.⁴ Rapporten indeholder vigtige konklusioner for nærværende behovsanalyse.

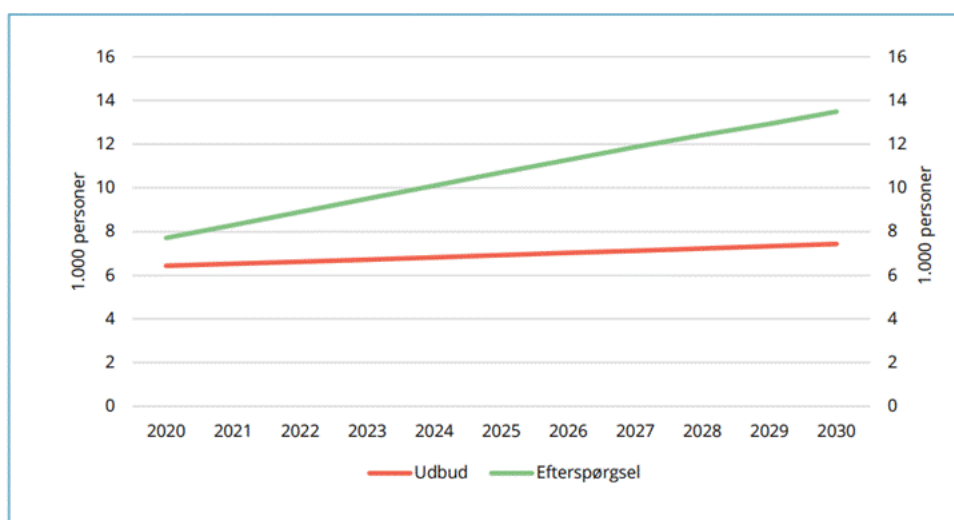
²IT-Branchen (2025): ”Det bør Danmarks kommende cybersikkerhedsstrategi indeholde”

³Erhvervsstyrelsen (2022): ”Digital Sikkerhed i danske SMV’er”

⁴IRIS-group (2021): ”Mismatch på det danske arbejdsmarked i 2030”

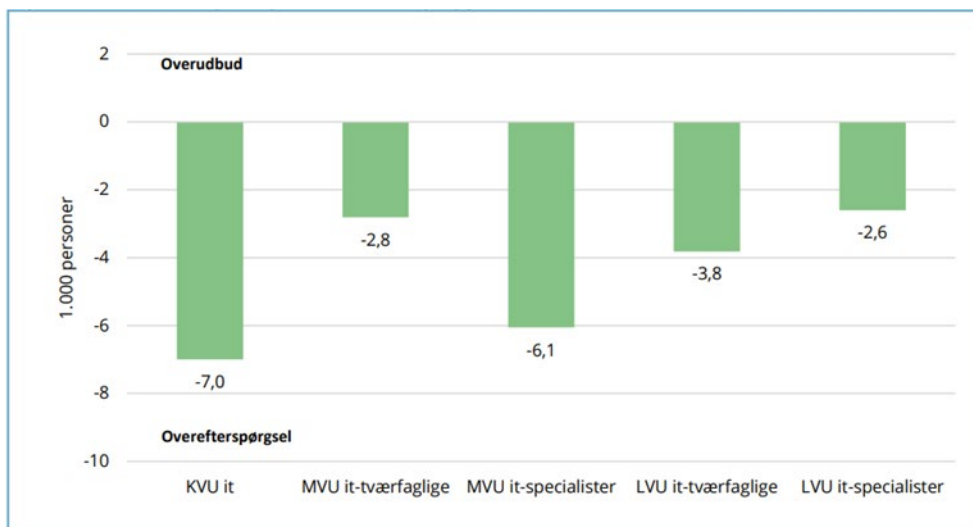
Mellemlangt videregående uddannede it-specialister kan blandt andet defineres som specialister med kompetence inden for cybersikkerhed. Som Figur 1 illustrerer, vil der frem mod 2030 være en kløft mellem udbud og efterspørgsel efter MVU it-specialister, som vil være stigende. Det vil sige, at der fortsat være en overefterspørgsel efter it-specialister, hvis ikke antallet af MVU it-specialister stiger.

Figur 1. Udviklingen i arbejdsudbuddet og efterspørgslen efter MVU it-specialister, 2020-30



Udover, at der viser sig at være en stigning i de positive beskæftigelsesmuligheder for it-specialister med en MVU, som inkluderer personer med en professionsbachelor i cybersikkerhed, er en bemærkelsesværdig pointe, at overefterspørgslen i 2030 er størst blandt MVU it-specialister og personer med korte videregående it-uddannelser sammenlignet med øvrige it-uddannelser (se Figur 2).

Figur 2. Mismatch opdelt på uddannelsesgrupper, 2030



Der er altså et klart stigende nationalt behov for it-specialister, og konsekvenserne heraf vil kun vokse, hvis ikke flere personer uddannes til at løse udfordringer. Manglen på it-specialister kan være afgørende for Danmarks cybersikkerhed, og netop denne uddannelsesgruppe er særligt efterspurgt, blandt andet i Region Sjælland, hvor både kvantitative og kvalitative data afspejler behovet for arbejdskraft.

Manglen på arbejdskraft fra internationale cybersikkerhedsspecialister kommer til udtryk blandt Zealands aftagere. Direktøren hos Nesp.ONE ApS giver udtryk for følgende:

”Cybersikkerhed er i dag en afgørende forudsætning for både private virksomheder og offentlige organisationer, og behovet for veluddannede specialister vil kun vokse i takt med øgede regulatoriske krav, digitalisering og et mere komplekst trusselsbillede.”

Regionale perspektiver på manglende arbejdskraft

I 2024 udgav Dansk Erhverv en analyse, der viser, at internationale medarbejdere er en betydelig gevinst for Danmarks økonomi og har stor betydning for det danske arbejdsmarked. Dette gælder især i Region Sjælland, hvor udenlandsk arbejdskraft står for mindst halvdelen

af den samlede beskæftigelsesvækst i flere kommuner. Dansk Erhverv meddeler herunder, at "udenlandsk arbejdskraft driver beskæftigelsesvæksten i Region Sjælland".⁵

Oprettelsen af en international linje i cybersikkerhed på Zealand vil kunne bidrage direkte til at imødekomme regionens behov for kvalificeret arbejdskraft ved både at tiltrække internationale studerende og fastholde dem på det regionale arbejdsmarked efter endt uddannelse.

Da cybersikkerhed er et område med dokumenteret mangel på arbejdskraft og samtidig er afgørende for både private og offentlige organisationers digitale drift, vil en engelsksproget uddannelse fungere som et strategisk redskab til at understøtte den fortsatte beskæftigelsesvækst i Region Sjælland og på landsplan. Samtidig vil uddannelsen styrke virksomhedernes adgang til kompetencer, der kan arbejde i internationale og flerkulturelle sammenhænge, hvilket er særligt relevant i en region præget af globaliserede virksomheder og internationale værdikæder.

Zealand udarbejdede i 2025 en behovsanalyse ifm. prækvalifikationsansøgningen til det danske udbud, der viste et tydeligt behov for cybersikkerhedskompetencer blandt virksomheder og organisationer i Region Sjælland. Virksomhederne der indgik i analysen, omfattede både store, små og mellemstore og omfattede nogle af de mest kritiske virksomheder i det cybersikkerhedstruede felt. I analysen samarbejdede Zealand blandt andet med IT-branchen, som indhentede data, der belyste, at mere end 40% af it-virksomheder i Region Sjælland efterspørger kompetencer inden for it-sikkerhed og compliance. De regionale arbejdsmarkedstal fra Styrelsen for Arbejdsmarked og Rekruttering (STAR), understøtter at der allerede i det første halvår af 2025 er *gode jobmuligheder og mangel på arbejdskraft* på Sjælland for IT-sikkerhedskonsulenter, som er en mulig titel for uddannelsens dimittender.⁶

De cybersikkerhedskompetencer, der er behov for i regionen, er for virksomhederne vigtige at opnå, men for flere virksomheder er det ikke nok bare at have de rette faglige kompeten-

⁵ Dansk Erhverv (2024): "Over halvdelen af beskæftigelsesvæksten i Region Sjælland skyldes udenlandsk arbejdskraft"

⁶ Arbejdsmarkedsbalancen Styrelsen for Arbejdsmarked og Rekruttering – Historik (2025)

cer. Sproget og den kulturelle forståelse for det globale marked, som flere og flere virksomheder i Region Sjælland har behov for at opnå, gør at der er en betydelig efterspørgsel på engeltalende medarbejdere.

Erhvervshus Sjælland, der indgik i Zealands behovsanalyse i 2025, og på baggrund af regionens kompetencebehov vurderede, at der er et betydeligt behov for cybersikkerhedsuddannelsen, understøtter herunder behovet for, at virksomhederne tilpasser sig det globale konkurrerende marked, hvor internationaliseringen er i fokus. Jimmy Faustin Andersen, der er projektleder i Erhvervshus Sjælland, har udtalt sig om erhvervshusets indsats, BSR, der har til formål at hjælpe virksomheder fra Østersøregionen ud på det globale marked. Han fremhæver, hvor vigtigt det er, at virksomhederne ansætter internationale medarbejdere for at klare sig godt på markedet:

“Erhvervshus Sjælland hjælper blandt andet små og mellemstore virksomheder med at stå stærkere på deres internationale ben ved at åbne deres øjne for markedspotentialer. Vi er glade for, at vi med den nye indsats kan give dem endnu flere muligheder og gøre dem mere modstandsdygtige, når de skal ud på det globale marked.”⁷

Erhvervshuset som har blik for, hvilke kompetencebehov, der er relevante i erhvervslivet i Region Sjælland, vurderer altså, at der er et klart behov for en større grad af internationale medarbejdere og engelsksprogede. Jimmy uddyber herunder:

“Verden bliver mere og mere international, og det kan vi også mærke hos os; særligt [...] Vi kender virksomhederne i vores område rigtig godt og følger dem tæt. De trygge rammer og den tætte relation gør, at vi kan tale direkte ind i deres ofte lokale hverdag og ud i den globale kontekst.”

Citatet beskriver, hvordan internationaliseringen i stigende grad påvirker virksomhederne i regionen. Erhvervshuset oplever, at lokale virksomheder i højere grad skal agere i en global

⁷ Erhvervshus Sjælland (2024): “Små lokale virksomheder, store globale muligheder: Ny indsats baner vejen”

sammenhæng, og at deres behov derfor rækker ud over det lokale marked. Samtidig fremhæves værdien af det tætte kendskab til virksomhederne og den nære relation, som gør det muligt at støtte dem i at navigere mellem en lokal hverdag og internationale krav og muligheder.

Zealand har i samarbejde med IT-Branchen undersøgt behovet for oprettelsen af PBA'en i Cybersikkerhed på engelsk i Zealand. Chefkonsulenten i brancheorganisationen giver udtryk for et betydeligt behov blandt deres medlemmer:

"Jeg kan bekræfte, at der også er efterspørgsel efter internationale/engelsktalende cybersikkerhedsprofessionelle blandt vores medlemmer."

Ovenstående citat tydeliggør, at IT-Branchen ser et klart behov for internationale og engelsktalende cybersikkerhedsprofessionelle. Det understøtter oprettelsen af en PBA i Cybersikkerhed på Zealand, da en international uddannelse kan imødekomme virksomhedernes efterspørgsel og bidrage til at dække manglen på kvalificeret arbejdskraft i branchen.

Stort behov for specialister hos virksomheder med internationalt fokus

Novo Nordisk ligeledes er en af Zealands aftagere, der ser en markant relevans i at oprette den engelsksprogede cybersikkerhedsuddannelse i Zealand. Sikkerhedsarkitekt i Novo Nordisk nævner i den forbindelse følgende: *"En international profil er ikke blot at foretrække, men også i høj grad nødvendig."*

Derudover støtter CEO fra virksomheden Searine op om, at Zealand åbner en PBA i Cybersikkerhed i engelsk, da virksomheden sigter efter et globalt marked:

"Vi har behov for trygheden og vores sprog er engelsk her, fordi vi sigter efter et globalt marked, så det vil være mere oplagt for os at ansætte en engelsktalende, der kan hjælpe med at fremme Cybersikkerhed for ikke at ændre på vores procedure."

HR-konsulent fra Digital Konzern finder det ligeledes relevant at ansætte en international medarbejder med en professionsbachelor i Cybersikkerhed, da disse medarbejdere især har blik for internationale procedurer og tendenser inden for cybersikkerhed:

“Den internationale profil kan potentielt bidrage med viden om internationale standarder, tendenser og trusselsbilleder inden for cybersikkerhed, som også kan have relevans i en regional kontekst. Samtidig kan det give et bredere perspektiv på informationssikkerhed og beredskab.”

Hos IT-servicevirksomheden KeepIT er der det afgørende, at deres medarbejdere kan arbejde på tværs af nationaliteter. Derfor er det en ekstra fordel for virksomheden at ansætte en professionsbachelor i Cybersikkerhed med en international profil. Virksomhedens SOC-manager nævner følgende:

“Vi er et internationalt team, og vi forventer, at alle i teamet kan arbejde på tværs af nationaliteter, ellers er de ikke et match. Jeg kan derfor godt se, at det ville være en fordel, hvis man blev uddannet i et miljø, hvor mange arbejder sammen med andre internationale profiler og får en god forståelse for at arbejde på tværs af nationaliteter og kulturer.”

IT- og cybersikkerhedsvirksomheden Connexa A/S er en af Zealands aftagere, der udtrykker et stort behov for uddannelsen. Virksomhedens direktør tydeliggør ønsket om at aftage dimittender fra uddannelsen:

“En sådan uddannelse vil efter vores vurdering være et væsentligt bidrag til at imødekomme branchens behov og samtidig styrke både erhvervslivet på Sjælland og Danmarks samlede position i fremtidens cybersikkerhedslandskab. Hos Connexa vil vi fortsat meget gerne overveje dimittender fra Zealand til relevante stillinger fremover.”

Direktør i IT-virksomheden LS Control er ligeledes meget positive i forhold til at åbne en PBA i Cybersikkerhed på engelsk, da mange af deres kunder er internationale:

“Vi vil se positivt på det, hvis der også er en international linje. Når alt kommer til alt, så vil det kunne bidrage til at øge tilflytningen og tilknytning til området af kvalificeret arbejdskraft, og da mange af vores kunder er internationale, så vil det blot være et plus med en international linje.”

Ovenstående citat peger altså på, at en international linje ses som en klar fordel, da den både kan bidrage til at tiltrække og fastholde kvalificeret arbejdskraft i området og samtidig matche virksomhedernes internationale kundegrundlag.

I forlængelse af ovenstående vurderer en anden af Zealands aftagere, herunder COO fra SeeSafe, at det er afgørende med en cybersikkerhedsuddannelse med en international profil:

“Det er afgørende for vores ansatte, at de kan både dansk og engelsk i skrift og tale. Vi har både danske og internationale kunder. International profil er rigtig godt, men dansk er indtil videre et ”must”.”

Citatet understreger, at både dansk- og engelskkundskaber er vigtige for virksomhederne, da de arbejder med både danske og internationale kunder. Samtidig peges der på, at en international profil er positiv på trods af, at dansk fortsat er en forudsætning. Zealand har i forbindelse med de tidligere udbud af internationale uddannelser adresseret de sproglige udfordringer ved at indgå i samarbejde relevante udbydere af danskundervisning i kommunalt regi. Dette samarbejde tænkes videreført med Næstved kommune, som tilkendegiver i deres støtteerklæring, at de vil støtte de studerende med integrationen i det danske samfund. De nævner bl.a. Næstveds UngeCentrum, som er et samlingssted for unge, hvor de internationale studerende allerede under uddannelsen vil stifte bekendtskab med dansk sprog og kultur.

Rekrutteringsudfordringer blandt virksomhederne

IT-drifts- og cybersikkerhedsvirksomhed Connexa A/S oplever udfordringer med rekruttering af kvalificerede, engelsksprogede medarbejdere. Virksomhedens direktør beskriver dette:

“Som IT-drifts- og cybersikkerhedsvirksomhed hos Connexa A/S oplever vi i stigende grad, at adgangen til veluddannede cybersikkerhedsspecialister er begrænset. Samtidig ser vi en markant og voksende efterspørgsel i markedet efter bachelorer med stærke tekniske kompe-

tencer inden for IT-sikkerhed, drift og risikohåndtering [...] Vi ser et stort potentiale i en international profil, som både kan tiltrække talent fra udlandet og styrke det danske arbejdsmarked med højt kvalificerede cybersikkerhedsprofessionelle.”

Citatet udtrykker, at der er stor mangel på cybersikkerhedsspecialister, mens behovet i markedet vokser. Connexa A/S ser derfor en international uddannelsesprofil som en strategisk løsning til både at dække manglen på arbejdskraft og styrke Danmarks kompetencer inden for cybersikkerhed.

Virksomheden Nesp.ONE ApS har ligeledes rekrutteringsvanskeligheder, når det kommer til ansættelsen af engelsksprogede cybersikkerhedsspecialister. Direktøren nævner følgende:

”Som virksomhed med fokus på organisatorisk informationssikkerhed oplever vi i stigende grad, at adgangen til kvalificerede cybersikkerhedsspecialister er begrænset. Samtidig ser vi en markant voksende efterspørgsel i markedet efter medarbejdere med solide kompetencer inden for cybersikkerhed, risikostyring og beskyttelse af kritiske digitale infrastrukturer.”

Hos Nesp.ONE ApS er der ud fra ovenstående citat en mangel på kvalificeret arbejdskraft, der kan matche virksomhedens internationale profil. Dette er en generel tendens blandt virksomheder i Danmark. En engelsksproget PBA i Cybersikkerhed vil derfor kunne afhjælpe disse kompetenceproblemer. Direktøren uddyber følgende:

”En sådan uddannelse vil ikke blot kunne styrke rekrutteringsgrundlaget for virksomheder som vores, men også bidrage til at udvikle og professionalisere cybersikkerhedsbranchen i Danmark. Den internationale dimension vil samtidig kunne tiltrække talent og kompetencer, som er nødvendige i et globalt cybersikkerhedslandskab.”

Udover faglige kompetencer efterspørger virksomhederne altså også engelsksprogede medarbejdere med international forståelse, der kan navigere i globale markeder. En PBA i Cybersikkerhed med international profil vil derfor både styrke regionens tiltrækning og fastholdelse af kvalificeret arbejdskraft og matche virksomhedernes behov for medarbejdere, der

kan arbejde med både danske og internationale kunder og have forståelse for det internationale marked.

Den internationale kompetenceprofil og bidraget i virksomhederne

PBA i Cybersikkerhed på engelsk adskiller sig fra Zealands eksisterende PBA i Cybersikkerhed, idet uddannelsen bliver oprettet med henblik på at uddanne dimittender, der har en international profil. Cybersikkerhed er et globalt fagområde, hvor trusler, teknologier og standarder i høj grad er internationale. En uddannelse med internationalt fokus og undervisning på engelsk klæder dimittenderne på til at arbejde med internationale samarbejdspartnere, globale sikkerhedsstandarder og multinationale organisationer. Dette gælder både i større og mindre virksomheder.

Sikkerhedsarkitekt i Novo Nordisk beskriver, hvordan professionsbachelorerne med fordel kan bidrage til virksomheden:

“Jeg mener, at de kan bidrage med en meget stor strategisk værdi, især for globale organisationer som Novo Nordisk. For eksempel har disse fagfolk typisk en forståelse for, hvordan kultur, lokale normer og regionale risikovilligheder kan påvirke sikkerhedsbeslutninger, hvilket sikrer, at politikker fungerer i praksis på verdensplan – og ikke kun på papiret.”

Hos Novo Nordisk fremhæves det altså, at internationale cybersikkerhedsfolk ikke bare tænker i teorier og regler, men forstår, hvordan tingene faktisk fungerer i virkeligheden rundt om i verden. Virksomheden har netop behov for de kompetencer, fordi dimittenderne ved, at sikkerhed ikke er “one size fits all”, fordi kultur, arbejdsvaner og holdninger varierer fra land til land. Den forståelse gør, at sikkerhedspolitikker bliver brugbare og effektive globalt.

I forlængelse af ovenstående uddyber Novo Nordisk, at de har erfaring med, at internationale medarbejdere fremmer problemløsningen i virksomheden:

“Typisk er sikkerhedsprofessionelle med international profil også mere erfarne i at arbejde med distribuerede teams, leverandører og myndigheder i forskellige lande, hvilket reducerer

friktion og fremskynder problemløsning. Dette har vi især oplevet i forbindelse med håndtering af sikkerhedshændelser.”

På baggrund af citatet har de i Novo Nordisk altså erfaring med, sikkerhedsprofessionelle med international profil er vant til at samarbejde på tværs af lande og organisationer, hvilket mindsker misforståelser og gør det lettere at handle hurtigt og effektivt. Især når der opstår sikkerhedshændelser.

Zealands behovsanalyse fra 2025 afdækkede, hvordan alle aftagerne havde udfordringer med manglende kompetencer inden for Cybersikkerhed, hvilket specielt handlede om mangel på medarbejdere, der havde kompetencer til at implementere sikkerhedsløsninger, blandt andet med udgangspunkt i NIS 2-direktivet. Der bliver herunder stillet skærpede lovkrav til virksomheders evne til at beskytte netværk og informationssystemer. En af de mindre virksomheder, som har deltaget i Zealands projekt, nemlig Triple Arm Technique, beskriver deres behov for professionsbachelorerne er stort, idet de har mangel på viden inden for implementering af sikkerhedsløsninger:

“Professionsbachelorerne vil med fordel give os mere viden omkring Cybersikkerhed og ressourcer til at implementere nogle løsninger, der kan øge sikkerheden i vores systemer.”

I Vurderingsstyrelsen er der ligeledes et behov for både danske og engelske medarbejdere, der kan bidrage til at arbejde med governance i organisationen. IT-sikkerhedsartikelen nævner:

“Det vigtigste nysgerrigheden for at lære og forstå behov for virksomheden og governance. Denne disciplin skal smelte sammen med det praktiske og operationelle. Blandt andet forståelsen for SIEM, Firewalls, XDR /EDR, PAM/ adgangsstyring er vigtig. Forstå spændet mellem politikker, standarder og SOP i en virksomhed, og hvordan noget går fra at være teori til praksis.”

I Novo Nordisk er der ligeledes fokus på relevansen af internationale medarbejdere som led af sikkerhedslovgivningerne, som skal implementeres i virksomhederne:

“Hvis man antager, at en sikkerhedsprofessionel med international profil også har et solidt kendskab til internationale lovgivningsmæssige rammer (GDPR, ISO-standarder, regional cyberlovgivning, eksportkontrol m.m.), kan vedkommende hjælpe organisationen med at overholde regler på tværs af landegrænser og undgå fejl, som potentielt kan blive omkostnings-tunge.”

IT-sikkerhedsarkiteksten i Vurderingsstyrelsen betegner behovet for kompetencerne som høje:

“Baseret på vores trusselsvurdering, så er behovet højt. Det er baseret på den geopolitisk situation. Vi i Danmark og EU skal være mere selvforsynende fremadrettet og det rammer helt ned i mindre virksomheder i dag”.

HR-konsulent fra Digital Koncern kommer ligeledes ind på, hvordan engelsksprogede professionsbachelor i Cybersikkerhed vil kunne være til stor gavn for koncernens beredskab og informationssikkerhed:

“Professionsbacheloren vil kunne bidrage relevant til funktionen, særligt i forhold til informationssikkerhed og beredskab. Det lyder til, at uddannelsens indhold matcher de opgaver, som funktionen i forvejen varetager inden for informationssikkerhed og beredskab.”

På baggrund af ovenstående afsnit er der altså et tydeligt og veldokumenteret behov for professionsbachelor i cybersikkerhed med en international profil. Virksomheder og offentlige organisationer efterspørger medarbejdere, der kan omsætte internationale standarder, lovgivning og sikkerhedspolitikker til praksis og arbejde effektivt på tværs af landegrænser. En engelsksproget PBA i Cybersikkerhed vil imødekomme dette behov, styrke virksomhedernes evne til at håndtere globale sikkerhedstrusler og understøtte efterlevelse af skærpede lovkrav som NIS2. Uddannelsen vil dermed være et væsentligt bidrag til både erhvervslivets og samfundets digitale robusthed.

Mangel på for arbejdskraft fra internationale

Som fremhævet i Zealands behovsanalyse fra 2025 viser en rapport fra Iris Groups (mfl.) beskæftigelsestendensen hos it-specialister, som indebærer professionsbachelorere i Cybersikkerhed, frem mod 2030.⁸ Rapporten viser, at disse grupper beskæftiges med en årlig vækstrate på 8,1% som illustreret i tabellen nedenfor

Tekst	Beskæftigede 2011	Beskæftigede 2018	Gns. årlig vækstrate
MVU it-specialister	4.000	7.000	8,1 %
MVU øvrige	460.000	500.000	1,2 %

Data som Zealand indhentede i samarbejde med IT-Branchen viser i forlængelse heraf, at mere end 40% af it-virksomheder i Region Sjælland efterspørger kompetencer inden for it-sikkerhed og compliance. Der bliver ikke blot efterspurgt kompetencer efter dimittender og studerende tilknyttet den eksisterende PBA i Cybersikkerhed. Flere af de virksomheder i Region Sjælland, der har deltaget Zealands projekt fremhæver, at der specielt er et behov efter arbejdskraft fra medarbejdere med en international profil. En af de mellemstore IT-virksomheder, som har deltaget i Zealands projekt, nemlig Simple Agency Group beskriver deres behov for professionsbachelorerne, idet de er under pres og har mangel på arbejdskraft. Virksomhedens CCO nævner følgende:

“Da IT-jobmarkedet er under stort pres og mangel på arbejdskraft, især inden for et område som cybersikkerhed, så er det min vurdering af en professionsbachelor, inklusiv en med en international profil, i høj grad vil kunne bidrage til at vi i Simple Agency Group vil kunne øge sikkerheden hos vores kunder.”

Ifølge virksomheden vil der fremadrettet være et stigende behov efter cybersikkerhedsuddannede. Han fortsætter:

“Cybersikkerhed er et af de områder, der set i lyset af markedet og verdensudviklingen kommer til at være et endnu større behov for fremadrettet.”

⁸ Iris Group (2018): "Iris Group (2018) Vækst og vækstvilkår i Region Sjælland"

I større virksomheder som Novo Nordisk, der især har behov for internationale medarbejdere, viser der sig også at være en stor efterspørgsel på cybersikkerhed. Virksomhedens sikkerhedsarkitekt nævner:

“Der er en stor efterspørgsel inden for ingeniør- og IT-området, som ikke kan dækkes, og Region Sjælland rummer mange globaliserede virksomheder, der er afhængige af sikre digitale driftsmiljøer, og som kan få stor gavn af disse fagfolk.”

En rapport fra Dansk Industri fremhæver i forbindelse med den høje mangel på arbejdskraft blandt virksomheder frem mod 2030, at en større indsats for at hente flere internationale medarbejdere er blandt de mest populære tiltag til at forebygge den manglende arbejdskraft.

Praktikmuligheder for studerende med en international profil

Som det fremgår af de foregående afsnit, findes der i Region Sjælland en efterspørgsel af internationale cybersikkerhedsuddannedes kompetencer. Zealands interviewpersoner viser en klar villighed til ansættelse og praktik, såfremt der åbnes en uddannelse. Partner for SafePay Nordic udtrykker i denne forbindelse følgende:

“Ja, virksomheden vil være interesseret i at modtage praktikanter. Det vil kunne tilføre virksomheden ny viden og opdaterede kompetencer inden for cybersikkerhed.”

Direktøren for Cyber Nordic har ligeledes en positiv holdning over for af aftage praktikanter fra Zealand:

“Ja, der vil være supermeget behov for deres kompetencer som praktikanter, og det er vigtigt med det forretningsmæssige perspektiv.”

Direktør hos CSIS er også positiv over for at modtage praktikanter i virksomheden. I forlængelse af dette udtrykker hun følgende:

“Sådan en bachelor vil være fedt! Alt hvad der kan skabes af mere uddannelse i Cyber er godt. Og hvis det endda er på engelsk så supergodt.”

Direktøren for Nesp.ONE ApS giver udtryk for, at virksomheden har meget gode erfaringer med at aftage praktikanter fra Zealand. Dette har medført, at de både nu og fremadrettet finder det værdifuldt at aftage praktikanter, specielt studerende under en PBA i Cybersikkerhed på engelsk:

”Vi har tidligere haft gode erfaringer med at ansætte bachelorer Zealand. De har bidraget med værdifuld viden og praktiske kompetencer, som hurtigt har kunnet omsættes til konkrete opgaver i vores organisation. Vi vil også fremadrettet have stor interesse i at rekruttere dimittender med IT-baggrund.”

Hos Connexa A/S er der et stort ønske om at aftage praktikanter fra Zealand. Virksomheden har et ønske om at ansætte og fastholde praktikanter og har på nuværende tidspunkt en studerende ansat fra Zealand, som direktøren anser, har en *vigtig* rolle i virksomhedens arbejde med at omsætte teori til praksis:

”Vi har siden vi startede vores virksomhed haft et særdeles positivt samarbejde med Zealand – Sjællands Erhvervsakademi, og har blandt andet ansat kandidater med stor succes. En af vores medarbejdere er i gang med bachelor fra Zealand, og han har i dag en vigtig rolle i vores organisation. Hans faglige niveau, praktiske forståelse og evne til hurtigt at omsætte teori til virkelige kundescenarier er et klart resultat af den uddannelse, han har gennemført.”

Direktøren udtrykker, at virksomheden oplever et meget værdifuldt samarbejde med Zealand, og at Zealand leverer kandidater med stærke faglige og praksisnære kompetencer, som hurtigt skaber værdi i virksomheden. Denne erfaring, som gør især virksomheden modtagelig over for praktikanter og engageret i at støtte op om oprettelsen af en PBA i Cybersikkerhed på engelsk på Zealand.

Der er i Region Sjælland en tydelig efterspørgsel efter cybersikkerhedskompetencer med international profil. Zealands interview med virksomheder viser en klar villighed til både at ansætte dimittender og modtage praktikanter, hvis uddannelsen etableres. Virksomhederne fremhæver, at praktikanter kan bidrage med ny viden, opdaterede kompetencer og et vigtigt forretningsmæssigt perspektiv. Samtidig har virksomhederne tilkendegivet, at de vil

støtte uddannelsen gennem praktikophold, virksomhedsbesøg, cases og undervisningsbidrag. Dette understreger, at der er bred opbakning fra det regionale erhvervsliv til oprettelsen af en engelsksproget PBA i Cybersikkerhed.

Uddannelsens kompetenceprofil

Formålet med professionsbacheloruddannelsen i cybersikkerhed på engelsk er at uddanne internationale dimittender, der selvstændigt kan varetage rollen som cybersikkerhedsspecialist med fokus på at sikre fortrolighed, integritet og tilgængelighed i forbindelse med udvikling og drift af it-systemer i både private og offentlige organisationer. Alt undervisning vil foregå på engelsk, således at dimittenderne typisk vil komme til at arbejde i internationale og tværkulturelle sammenhænge, hvor cybersikkerhed reguleres og praktiseres på tværs af landegrænser.

Gennem undervisning opnår dimittenderne kompetencer til at anvende internationale standarder og lovgivning inden for cybersikkerhed samt til at kommunikere og samarbejde professionelt med internationale interessenter, leverandører og myndigheder. Formålet er således at klæde dimittenderne på til at kunne omsætte globale sikkerhedskrav og -politikker til praktiske og operationelle løsninger, der fungerer i forskellige organisatoriske og kulturelle kontekster, og dermed imødekomme arbejdsmarkedets behov for cybersikkerhedsspecialister med en stærk international kompetenceprofil.

Uddannelsens indhold

Uddannelsens faglige indhold vil være identisk med den eksisterende danske PBA i Cybersikkerhed, som Zealand udbyder fra 2026. Hentet direkte fra Bekendtgørelse om tekniske og merkantile erhvervsakademiuddannelser og professionsbacheloruddannelser, BEK nr 445 af 07/05/2025, bilag 1 vedr. PBA i cybersikkerhed:

Professionsbachelor i cybersikkerhed

Uddannelsens navn: Uddannelse til professionsbachelor i cybersikkerhed (Bachelor's Degree Programme in Cyber Security).

Betegnelse: Uddannelsen giver den uddannede ret til at anvende betegnelsen Professionsbachelor i cybersikkerhed (Bachelor of Cyber Security)

Formål og erhvervsigte: Formålet med professionsbachelor i cybersikkerhed er at kvalificere den uddannede til at kunne fungere selvstændigt som cybersikkerhedsspecialist med fokus på at arbejde med fortrolighed, integritet og tilgængelighed i forbindelse med udvikling, drift og sikkerhedsledelse af it-systemer i såvel private som offentlige virksomheder og organisationer.

Normering: Uddannelsen er normeret til 210 ECTS-point, der omfatter:

- 1) Uddannelseselementer med et samlet omfang på 160 ECTS-point, der tilrettelægges inden for uddannelsens faglige områder.
- 2) Praktik med et samlet omfang på 30 ECTS-point.
- 3) Bachelorprojekt på 20 ECTS-point.

Fagområder: Uddannelseselementerne tilrettelægges inden for følgende fagområder, der samlet set omfatter 160 ECTS-point, og som er indbyrdes vægtet i forholdet 1:1:1.

- 1) Cybersikkerhedsledelse, -governance og -processer: Fagområdet indeholder viden om governance, ledelsesværktøj og processer til at forhindre, overvåge, detektere og reagere over for trusler mod fortrolighed, integritet og tilgængelighed af systemer og applikationer. Fagområdet omhandler selvstændig organisering og ledelse af sikkerhedsarbejdet i organisationer og virksomheder samt principper, standarder og best practices i cybersikkerhed, herunder etiske, juridiske, politiske og ledelsesmæssige aspekter af cybersikkerhedsarbejde.
- 2) Netværkssikkerhed, detektering og arkitektur: Fagområdet indeholder netværksarkitekturer, medier og protokoller samt redskaber til at forhindre, overvåge, detektere og reagere over for trusler mod fortrolighed, integritet og tilgængelighed af netværksskommunikation. Fagområdet indeholder de tekniske komponenter, som udgør de forskellige IT-systemer.
- 3) Software- og datasikkerhed og automation: Fagområdet indeholder sikkerhedsperspektivet i software, blandt andet programkvalitet og betydning af fejl- og datahånd-

tering for en software-arkitekturs sårbarheder. Fagområdet indeholder sikkerhedsdesignprincipper. Desuden indeholder fagområdet tiltag til kryptering og lagring samt automatisering, basal scripting og programmering.

Nationale og lokale uddannelseselementer: Uddannelseselementerne tilrettelægges som

- 1) Nationale fagelementer med et samlet omfang på 100 ECTS-point, der er fælles for uddannelsens studerende og fastsættes i den nationale del af studieordningen.
- 2) Lokale fagelementer med samlet omfang på 60 ECTS-point, der tilrettelægges under hensyntagen til lokale og regionale behov og fastsættes i institutionsdelen af studieordningen. De lokale fagelementer skal omfatte valgfag i et omfang, der mindst svarer til 5 ECTS-point.

Afstigning til:

Erhvervsakademiuddannelse i operationel cybersikkerhed

Uddannelsens navn: Erhvervsakademiuddannelse inden for operationel cybersikkerhed (Academy Profession Degree Programme in Operational Cyber Security)

Betegnelse: Uddannelsen giver den uddannede ret til at anvende betegnelsen AK i operationel cybersikkerhed (AP Graduate in Operational Cyber Security)

Formål og erhvervsigte: Formålet med uddannelsen er at kvalificere den uddannede til at kunne indgå i samarbejde om cybersikkerhedsopgaver med fokus på at arbejde med fortrolighed, integritet og tilgængelighed i forbindelse med udvikling, drift og support af it-systemer i såvel private som offentlige virksomheder og organisationer.

Normering: Uddannelsen er normeret til 120 ECTS-point, der omfatter:

- 1) Uddannelseselementer med et samlet omfang på 90 ECTS-point, der tilrettelægges inden for uddannelsens faglige områder.
- 2) Praktik med et samlet omfang på 20 ECTS-point.
- 3) Afsluttende eksamensprojekt på 10 ECTS-point.

Fagområder: Uddannelseselementerne tilrettelægges inden for følgende fagområder, der samlet set omfatter 90 ECTS-point, og som er indbyrdes vægtet i forholdet 1:1:1. --1) Forretningsforståelse, governance og kommunikation: Fagområdet omhandler kommunikation og tilrettelæggelse af sikkerhedsarbejdet i organisationer og virksomheder samt principper og best practice i cybersikkerhed, herunder etiske, juridiske, politiske og forretningsmæssige aspekter af cybersikkerhedsarbejde.

2) Netværkssikkerhed og arkitektur: Fagområdet indeholder netværksarkitekturer, medier og protokoller samt redskaber til at forhindre, detektere og reagere over for trusler mod fortrolighed, integritet og tilgængelighed af netværkskommunikation. Fagområdet indeholder de tekniske komponenter, som udgør de forskellige IT-systemer. --3) Programmering, datasikkerhed og automation: Fagområdet indeholder sikkerhedsperspektivet i datahåndtering, blandt andet fejlhåndtering og lagringsstrategier. Desuden indeholder fagområdet tiltag til kryptering samt automatisering, basal scripting og programmering.

Nationale og lokale uddannelseselementer: Uddannelseselementerne tilrettelægges som

- 1) Nationale fagelementer med et samlet omfang på 60 ECTS-point, der er fælles for uddannelsens studerende og fastsættes i den nationale del af studieordningen.
- 2) Lokale fagelementer med samlet omfang på 30 ECTS-point, der tilrettelægges under hensyntagen til lokale og regionale behov og fastsættes i institutionsdelen af studieordningen. De lokale fagelementer skal omfatte valgfag i et omfang, der mindst svarer til 5 ECTS-point.

Konklusion

Behovsanalysen viser et stort og voksende behov for cybersikkerhedsspecialister både nationalt og regionalt. Samtidig peger analysen tydeligt på, at efterspørgslen i stigende grad retter sig mod engelsksprogede medarbejdere med en international kompetenceprofil. Dette skyldes, at cybersikkerhed i sin natur er et globalt fagområde, hvor trusselsbilleder, teknologier, standarder og lovgivning udvikles og anvendes på tværs af landegrænser.

Virksomheder i og omkring Region Sjælland opererer i stigende grad på internationale markeder, samarbejder med udenlandske kunder og leverandører og anvender internationale standarder og rammeværk som ISO, NIS2 og GDPR, hvor arbejds sproget ofte er engelsk. Engelsksprogede medarbejdere vurderes derfor som afgørende for effektiv kommunikation, implementering af internationale sikkerhedskrav og håndtering af globale sikkerhedshændelser.

Derudover bidrager internationale medarbejdere med viden om globale "best practices", internationale procedurer og kulturelle forskelle, hvilket styrker organisationernes evne til at omsætte sikkerhedspolitikker til praksis i multinationale og tværkulturelle sammenhænge. Zealands behovsanalyse adresserer dermed ikke blot manglen på arbejdskraft, men også målrettet understøttelse af behov for medarbejdere, der har en engelsksproget PBA i Cybersikkerhed, som kan arbejde i en international cybersikkerhedskontekst og dermed styrke regional og national mangel på kvalificeret arbejdskraft.

Støtteerklæring

Støtteerklæring vedrørende en internationale professionsuddannelse (PBA) i Cybersikkerhed

IT-Branchen støtter initiativet om at udbyde en professionsbacheloruddannelse (PBA) i Cybersikkerhed på engelsk på Zealand – Sjællands Erhvervsakademi.

I hele landet, især i Region Sjælland og Hovedstaden, ser vi et betydeligt behov for dimittender, der har en international baggrund.

Der er gode beskæftigelsesmuligheder for internationale studerende fra Cybersikkerhedsuddannelsen i regionen og på landsplan. Behovet for cybersikkerhedsspecialister de seneste år været hurtigt voksende i medlemsvirksomhederne i IT-Branchen.

Efterspørgslen efter kvalificeret arbejdskraft i branchen er fortsat betydelig.

Med venlig hilsen



Troels Johansen

Chefkonsulent og ansvarlig for cybersikkerhed

Kilder

Arbejdsmarkedsbalancen Styrelsen for Arbejdsmarked og Rekruttering – Historik (2025): [historik](#)

Dansk Erhvervs (2024): [Over halvdelen af beskæftigelsesvæksten i Region Sjælland skyldes udenlandsk arbejdskraft](#)

Erhvervsstyrelsen (2022): https://erhvervsstyrelsen.dk/sites/default/files/2022-09/Digital-sikkerhed-i-Danske-SMVer_Erhvervsstyrelsen_Sep2022_WA.pdf

Iris Group (2018): Iris Group (2018) Vækst og vækstvilkår i Region Sjælland

Iris Group (2021): [Mismatch-paa-det-danske-arbejdsmarked-i-2030-1.pdf](#)

IT-Branchen (2025): [Det bør Danmarks kommende cybersikkerhedsstrategi indeholde - IT-Branchen](#)