Uddannelses- og Forskningsministeriet

Prækvalifikation af videregående uddannelser - Cybersikkerhed

Udskrevet 18. januar 2026

Professionsbachelor - Cybersikkerhed - Københavns Erhvervsakademi

Institutionsnavn: Københavns Erhvervsakademi
Indsendt: 13/09-2024 10:57
Ansøgningsrunde: 2024-2
Status på ansøgning: Godkendt
Afgørelsesbilag
Download den samlede ansøgning
Læs hele ansøgningen

Ansøgningstype

Ny uddannelse

Udbudssted

København

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

Kvalitetskonsulent, Iben Rehling, iber@kea.dk, 20770977

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?

Dansk

Er uddannelsen primært baseret på e-læring?

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

ECTS-omfang

210

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

Formålet med professionsbacheloruddannelsen i cybersikkerhed er at kvalificere den uddannede til at arbejde med både tekniske og forretningsmæssige aspekter af cybersikkerhed i offentlig og privat sektor.

På uddannelsen vil de studerende blive undervist i at opbygge og vedligeholde tekniske og forretningsmæssige strukturer til at forebygge, opdage og afbøde cyberangreb herunder governance og compliance relateret til cybersikkerhed. Uddannelsen vil være praksisnær og bygge på anvendt metode og teori samt værktøjer og systemer, der gør den uddannede i stand til at skabe værdi i en organisation fra dag et. Der vil i høj grad indgå cases og virksomhedssamarbejde, ligesom praktik er et centralt element.

Uddannelsen er opbygget således, at den studerende kan afslutte uddannelsen efter 2 år og opnå en erhvervsakademiuddannelse i cybersikkerhed. De erhvervsakademiuddannede kan udføre drift- og supportopgaver inden for cybersikkerhed i større private og offentlige organisationer, samt SMV-segmentet. Professionsbachelorerne vil finde beskæftigelse som cybersikkerhedsspecialister i en bred vifte af roller i større organisationer og organisationer, der er specialiserede i cybersikkerhed.

Uddannelses struktur og konstituerende faglige elementer

Læringsmål, professionsbacheloruddannelsen

Viden
Den uddannede har

- udviklingsbaseret viden om erhvervets praksis og anvendt teori og metode inden for forebyggelse, identificering af og reaktion på cybersikkerhedstrusler i en kompleks organisatorisk sammenhæng
- udviklingsbaseret viden om erhvervets praksis og anvendt teori og metode inden for analyse af organisationskulturers påvirkning af cybersikkerhed samt designprincipper for strukturer, der fremmer cybersikkerhed
- forståelse for praksis og anvendt teori og metode inden for nationale og internationale sikkerhedsstandarder og kan reflektere over cybersikkerhedsprincipper

Færdigheder
Den uddannede kan

- anvende metoder og redskaber inden for forebyggelse, identificering af og reaktion på cybersikkerhedstrusler og mestre analyse af mulige angreb
- anvende metoder og redskaber inden for nationale og internationale standarder til design og udvikling af cybersikkerhedssystemer, herunder mestre implementering af kryptografiske tiltag
- anvende metoder og redskaber inden for udvikling, drift og governance af IT-systemer og strukturer, der fremmer cybersikkerhed i en kompleks organisatorisk sammenhæng, herunder mestre automatisering af cybersikkerhedsopgaver

- vurdere praksisnære og teoretiske problemstillinger inden for cybersikkerhed samt begrunde og vælge relevante løsningsmodeller for cybersikkerhedstiltag i en kompleks organisatorisk sammenhæng
- formidle praksisnære og teoretiske problemstillinger og løsninger inden for cybersikkerhed til samarbejdspartnere, interessenter og brugere

Kompetencer
Den uddannede kan

- håndtere komplekse og udviklingsorienterede situationer i forhold til udvikling, drift og governance af IT-systemer, der fremmer cybersikkerhed i en organisation, samt udvikling og implementering af foranstaltninger til at sikre kritisk data
- håndtere komplekse og udviklingsorienterede situationer i arbejds- eller studiesammenhænge i forhold til udvikling og implementering af compliance og sikkerhedskultur i en kompleks organisatorisk sammenhæng
- selvstændigt indgå i fagligt og tværfagligt samarbejde og påtage sig ansvar inden for rammerne af en professionel etik i forhold til at rådgive om samt udvikle og drifte cybersikkerhedsforanstaltninger
- identificere egne læringsbehov og udvikle egen viden, færdigheder og kompetencer i relation til cybersikkerhed, herunder nationale og internationale trusselsbilleder og sikkerhedsstandarder

Uddannelsen vil blive tilrettelagt med udgangspunkt i følgende 3 fagområder, som vægtes 1:1:1 (se uddybning af fagområder i bilag)

- Cybersikkerhedsledelse, governance og processer
- Netværkssikkerhed og arkitektur
- Software-, datasikkerhed og automation

Læringsmål, erhvervsakademiuddannelsen

Viden
Den uddannede har

- viden om erhvervets praksis og central anvendt teori og metode inden for forebyggelse, identificering af og reaktion på cybersikkerhedstrusler, herunder governance og sikkerhedsprocedurer
- viden om erhvervets praksis og central anvendt teori og metode inden for organisationskultur og kommunikation samt designprincipper for strukturer, der fremmer cybersikkerhed
- forståelse for praksis og central anvendt teori og metode inden for cybersikkerhed samt forståelse for erhvervets anvendelse af teori og metode og de forskellige roller i en cybersikkerhedsorganisation

Færdigheder
Den uddannede kan

- anvende centrale metoder og redskaber inden for forebyggelse, identificering af og reaktion på cybersikkerhedstrusler samt governance af cybersikkerhedsstrukturer, og anvende de færdigheder, der knytter sig til beskæftigelse inden for cybersikkerhed
- vurdere praksisnære problemstillinger inden for cybersikkerhed samt opstille og vælge løsningsmuligheder
- formidle praksisnære problemstillinger og løsningsmuligheder inden for cybersikkerhed til samarbejdspartnere og brugere

Kompetencer
Den uddannede kan

- håndtere udviklingsorienterede situationer inden for opsætning og drift af IT-systemer og strukturer, der fremmer cybersikkerhed i en organisation, samt implementering af foranstaltninger til at sikre kritisk data
- deltage i fagligt og tværfagligt samarbejde i forbindelse med udvikling, drift og compliance inden for cybersikkerhed med en professionel tilgang
- i en struktureret sammenhæng tilegne sig ny viden, færdigheder og kompetencer inden for cybersikkerhed

Uddannelsen vil blive tilrettelagt med udgangspunkt i følgende 3 fagområder, som vægtes 1:1:1 (se uddybning af fagområder i bilag).

- Forretningsforståelse, governance og kommunikation
- Netværkssikkerhed og arkitektur
- Software-, datasikkerhed og automation

Uddannelsen indeholder flg. fagelementer fælles for PBA- og EAK-uddannelsen på de første 3 semestre:

Forretningsforståelse (10 ECTS) 1.-3. semester
Fagelementets formål er at kvalificere den studerende til at kunne forstå sammenhængen mellem forretning, informationsteknologi og cybersikkerhed. Den studerende får kompetencer til at arbejde med strategiske problemstillinger relateret til forskellige interessenters roller og ansvar i forhold til cybersikkerhed i en organisatorisk kontekst.

Programmering (10 ECTS) 1.-3. semester
Formålet med fagelementet er at sætte den studerende i stand til at løse konkrete problemstillinger inden for cybersikkerhed gennem udarbejdelsen af mindre scripts.
Den studerende bliver i stand til på egen hånd at arbejde med algoritmer, opskrifter og programmering af computere.

Computerarkitektur (10 ECTS) 1.-3. semester
Fagelementets formål er at kvalificere den studerende til at forstå og arbejde med computer- og cloud-arkitektur, inkl. hardware, software, styresystemer og cloud-modeller. Den studerende får kompetencer til at identificere og beskrive, hvor og hvordan sikkerhedssårbarheder kan opstå i denne arkitektur.

Kommunikation og rapportering (10 ECTS) 1.-3. semester
Fagelementets formål er at kvalificere den studerende til at løse skriftlig og mundtlige kommunikationsopgaver inden for cybersikkerhed i en organisation. Den studerende får kompetencer til at udtrække, behandle og præsentere data fra sikkerhedsværktøjer til fagfolk og ikke-fagfolk, såvel internt som eksternt.

Automatisering og scripting (5 ECTS) 1.-3. semester
Fagelementets formål er at kvalificere den studerende til at automatisere sikkerhedsopgaver ved anvendelse af scriptingsprog. Den studerende får kompetencer til at anvende biblioteker af funktioner og programmer i deres egne programmer med særligt fokus på at parse logs fra organisationens sikkerhedssystemer.

Datasikkerhed (5 ECTS) 1.-3. semester
Fagelementets formål er at kvalificere den studerende til at anvende metoder til lokal og skybaseret datalagring samt anvende principper for sikkerhedsdesign. Den studerende får kompetencer til at sikre data gennem adgangskontrol og kryptering.

Netværksarkitektur (10 ECTS) 1.-3. semester
Fagelementets formål er at kvalificere den studerende til at forstå netværksdesign og –strukturer i et sikkerhedsperspektiv. Den studerende får kompetencer til at planlægge og implementere effektive netværksløsninger.

IT-sikkerhedsdrift (10 ECTS) 1.-3. semester
Fagelementets formål er at kvalificere den studerende til at forstå principper og praksis for IT-drift med fokus på sikkerhed. Den studerende får kompetencer til at implementere og vedligeholde sikkerhedsforanstaltninger, risikostyring, trusselsvurderinger og sikre kontinuerlig drift i en IT-infrastruktur.

Lokale fagelementer (20 ECTS) 1.-3. semester
Der vil være et udbud af aktuelle lokale, herunder valgfrie, fagelementer på 20 ECTS.

GÆLDER KUN ERHVERVSAKADEMIUDDANNELSEN:
På 4. semester er der praktik på 15 ECTS og afsluttende opgave på 15 ECTS.

Uddannelsen indeholder flg. fagelementer på PBA-uddannelsen på de sidste 4 semestre:

Cybersikkerhedsgovernance (10 ECTS) 4.-7. semester
Fagelementets formål er at kvalificere den studerende til at håndtere fundamentale opgaver som sikkerhedsansvarlig. Den studerende får kompetencer til at udføre risikoanalyse og inddrage relevant lovgivning i en organisations sikkerhedspolitikker og –praktikker.

Netværks- og kommunikationssikkerhed (10 ECTS) 4.-7. semester
Fagelementets formål er at kvalificere den studerende til at identificere og håndtere sårbarheder i netværk. Den studerende får kompetencer til at overvåge netværkssikkerhedstrusler samt implementere og konfigurere udstyr til monitorering og mitigering af angreb.

Softwaresikkerhed (10 ECTS) 4.-7. semester
Fagelementets formål er at kvalificere den studerende til at sikkerhedsvurdere software og softwarearkitektur. Den studerende får kompetencer til at opdage trusler mod software og forhindre sårbarheder i programkoder

Systemsikkerhed (10 ECTS) 4.-7. semester
Fagelementets formål er at kvalificere den studerende til at anvende sikkerhedsprincipper til systemsikkerhed og forensic processer. Den studerende får kompetencer til at udføre, udvælge, anvende og implementere praktiske tiltag til sikring af organisationens udstyr.

Lokale fagelementer (30 ECTS) 4.-7. semester
Der vil være et udbud af aktuelle lokale, herunder valgfrie, fagelementer på 30 ECTS.

På 4.-7. semester indlægges et semester med praktik på 30 ECTS og bachelorprojekt på 20 ECTS.

Uddybende beskrivelser kan rekvireres.

Begrundet forslag til takstindplacering af uddannelsen

Som professionsbachelor i IT-sikkerhed. Professionsbacheloruddannelsen i cybersikkerhed har brug for udstyr og licenser svarende til det niveau, som professionsbacheloren i IT-sikkerhed har.

Forslag til censorkorps

Censorkorpset for IT- og softwareudvikling. Indeholder i dag følgende andre uddannelser: Datamatiker, IT-teknolog, PBA i softwareudvikling, PBA i webudvikling, PBA i økonomi og IT, PBA i IT-sikkerhed, PBA i IT-arkitektur.

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

Bilag 1 - behovsanalyse - PBA i cybersikkerhed.pdf

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

I forbindelse med udviklingen af den nye uddannelse har KEA kortlagt det nuværende kompetencegab inden for cybersikkerhed i offentlige og private organisationer. Analysen viser, at der er behov for flere cybersikkerhedsuddannede, og at de skal have bredere og dybere kompetencer. Eksisterende uddannelser inden for cybersikkerhed uddanner i høj grad tekniske og akademiske specialister. Der er behov for flere medarbejdere med en hands-on tilgang, der har et solidt teknisk og forretningsmæssigt fundament. Der er også et behov for kortere uddannede medarbejdere til cybersikkerhedsdrift og –support, hvilket i dag ikke dækkes.

KEAs behovsanalyse er baseret på en spørgeskemaundersøgelse til aftagere med 118 besvarelser. 55% af aftagerne har forsøgt at rekruttere inden for cybersikkerhed de seneste 2 år. 68% har oplevet udfordringer med rekruttering. Af disse har 48% ansat en medarbejder, der matchede delvist, mens 18% har opgivet at rekruttere. Dette understøtter, at der er en generel mangel på cybersikkerhedsuddannede.

Interessenterne har givet udtryk for, at det er nødvendigt med en bred forståelse for cybersikkerhedsområdet kombineret med en specialisering. Behovet er derfor en uddannelse med en profil, hvor en bred uddannelse i cybersikkerhed kombineres med en specialisering i enten tekniske eller forretningsrelaterede fag. Denne uddannelse findes ikke i dag.

97% af respondenterne forventer et stigende behov for cybersikkerhedsmedarbejdere inden for de næste 5 år. Dette understøttes af regeringens strategi for cyber-og informationssikkerhed samt af tal fra Rambøll og Dansk IT m.fl.

“Særligt folk med god teknisk og rimelig forretningsforståelse kan være svære at finde. Ikke kun for os, men for alle i Danmark”
Rasmus Vedel, Chef for Cyberservices, KOMBIT

Uddybende bemærkninger

Udvalgte støtteerklæringer fra aftagere:

”HK Stat bakker fuldt ud op, omkring etableringen af en ny IT-sikkerheds uddannelse, med særligt fokus på cybersikkerhed. Kritisk infrastruktur, demokratiske institutioner og private virksomheder er i stigende grad truet af cyberangreb og senest i juni har CFCS advaret om et øget trusselsniveau mod det danske samfund. Behovet for at få etableret en uddannelse der er målrettet cybersikkerhedsområdet på PBA/KVU-niveau kan derfor ikke undervurderes. Det gælder både inden for Forsvaret, den offentlige forvaltning samt ude i de mange private virksomheder, som skal forebygge og håndtere de mange cyberangreb de oplever. Vi skal kunne rekruttere bredere til feltet og har brug for flere veje ind i faget. Derfor mener vi at denne nye uddannelse understøtter en vigtig samfundsinteresse.”
Heidi Juhl Pedersen, Sektorformand, HK Stat

“En af de helst store udfordringer er, at det er svært at skaffe mennesker med de rette kompetencer. Der er simpelthen ikke nok på markedet der har den fornødne viden.
[...] Særligt folk med god teknisk og rimelig forretnings-forståelse, kan være svære at finde. Ikke kun for os, men for alle i Danmark”
Rasmus Vedel, Chef for Cyberservices, KOMBIT

“Vi har i høj grad brug for medarbejdere med hybride kompetencer, der kombinerer forretningsforståelse og teknik. Derfor synes vi, at det er interessant, at Københavns Erhvervsakademi søger om at oprette en ny professionsbachelor i cybersikkerhed, som introducerer til sikkerhed fra første dag. [...] Den to-årige uddannelse i cybersikkerhed er der også et klart behov for – både i Københavns Kommune, hvor de kan indgå i first line support, og i de mindre kommuner, hvor de kan blive bindeled mellem forretning, IT og eksterne specialister.”
Lisa Hartmann Jensen,Teamkoordinator, Sikkerhed, Københavns Kommune

“Koblingen mellem virksomhedsforståelsen, governance og kommunikation er særlig vigtig og ofte noget, som der er mangel på. Vi har et stort behov for dygtige unge mennesker i Danmark indenfor Cyber området. Ikke mindst for at have kompetencerne i DK. Hos ISS f.eks. har vi langt de fleste cyber medarbejdere ansat i udlandet da der ikke er nok i DK og dem der er har enten ikke rette kompetencer eller er økonomisk ikke interessante da man nærmest kun kan finde folk med erfaring (der er alt for få ny-uddannede at tage fra).”
Martin Petersen, Chief Information Security Officer, ISS A/S

“Der er behov for tunge specialister på it-sikkerhedsområdet, men der er også brug for sikkerhedsfolk med en mere operationelt og praktisk adgang til sikkerhed. Vi har både brug for det teoretiske lag, og for en gruppe medarbejdere, der forstår, hvordan systemer, applikationer m.v. konfigureres i forhold til sikkerhed i det daglige arbejde.”
Jacob Behrend, IT-chef, Lyngby Taarbæk Forsyning

“Man skal evne at kombinere både teknisk og forretningsforståelse for at lykkedes i en storpolitisk organisation som fx SDU. Det er et stor behov både nu og i fremtiden for at sikre både viden, teknik og mennesker mod de stigende cybertrusler. KEAs og EAAAs ny uddannelse kan være med til at sikre dygtige medarbejde til fremtiden - medarbejdere som men de rette kompetencer formår at binde teknologi og mennesker sammen i et bedre sikret IT-landskab.”
Lasse Birnbaum Jensen, Teamleder for Infrastruktur, SDU IT, Region Syddanmark

“Som direktør i en mindre softwarevirksomhed er jeg meget bevist om behovet for, at der skal være stor fokus på cybersikkerhed - generelt i samfundet og specifikt i min virksomhed. I dag er det ofte specialiserede virksomheder, der leverer konsulentydelser indenfor cybersikkerhed. Ydelserne ligger på et prisniveau, der ikke er muligt at være med på for mindre virksomheder. Uddannes der fremadrettet flere, der har kendskab til både den tekniske og forretningsmæssige del af cybersecurity, vil det forhåbentlig medføre, at det bliver mere "tilgængeligt" for mindre virksomheder at ansatte medarbejdere, der kan løfte opgaven.”
Ann Christina Rindom Sørensen, Direktør, SafeJournal ApS

“Vi har hos [vores virksomhed] hvert år min. 3 datamatikerpraktikanter fra KEA, hvoraf flere tilbydes job efter endt praktikforløb hos os. Det er dog tydeligt, at der savnes en større viden om og forståelse for informations- og cybersikkerhed generelt på uddannelsen, da dette ikke er en obligatorisk del af uddannelsen. Dem som tager en valgfag i it-sikkerhed, når ikke langt nok ned i materien, og har derfor kun en overfladisk/begrænset viden herom.”
Legal & Compliance Consultant, privat virksomhed, 10-49 ansatte, Region H

“Jeg tror at IT-verdenen er på vej ind i en meget sårbar periode. De ældre, "der var der fra starten", og primært var verdensmestre i et felt, er så småt på vej ud af den tekniske funktion. Området er vokset (f.eks. Cloud). Det kræver mere viden (antal trusler, angreb og potentielle angribere vokser stødt). Kravene og arbejdsbyrden omkring funktionerne bliver flere (F.eks. NIS2/DORA). [...]En sund drift, compliance, udvikling, risk management og incident response af et system, er en stor opgave, ofte placeret på for få hænder. Min erfaring er, at cyber-sikkerhed delen ofte er det første der bliver nedprioriteret, eller mangler. Så ja. Vi mangler fagfolk på området. Og vi mangler værdifuld og dedikeret uddannelse til dem.
Simon N Jensen, IT-sikkerhedskonsulent, Industriens Pension

“Den voksende digitalisering af samfundet stiller større og større krav til vores cybersikkerhed. Derfor er der behov for flere typer profiler med en grundig baggrund både i det tekniske og de mere bløde processer.”
Morten Sørensen, CEO, Omnisec

”Center for Cybersikkerhed bifalder generelt udbredelsen af uddannelsestilbud, der styrker det samfundsmæssige fokus på og faglige kompetencer inden for cybersikkerhed. Københavns Erhvervsakademis uddannelsesforslag er et væsentligt bidrag hertil.”
Center for Cybersikkerhed

“DI Digital støtter på kraftigeste oprettelsen af en PBA i Cybersikkerhed og afstigningsmuligheden, behovet for cyberkompetencer på alle niveauer stiger voldsomt på grund af den øgede digitalisering og det ændrede trusselbillede.”
Jeppe Engell, Chefkonsulent, DI Digital

”Jeg vil gerne udtrykke min støtte til oprettelsen af Professionsbachelor i Cybersikkerhed. I vores virksomhed, og i branchen generelt, er der et stigende behov for specialister, der kan håndtere komplekse cybersikkerhedsudfordringer. En målrettet uddannelse inden for dette område vil være afgørende for at sikre, at vi har de nødvendige kompetencer til at beskytte
vores digitale infrastruktur og data mod trusler. Det vil ikke kun styrke vores virksomhed, men også bidrage til branchens samlede robusthed og innovation.”
Alexandru Gheorghiasa, Senior IT Security Architect, Novo Nordisk

Oversigt over navngivne (ikke anonyme) respondenter i spørgeskemaundersøgelsen

Klaus Petersen, CTO, Alpha Solutions

John Talchow, Direktør og co-founder, CyberNordic

Erik Lindstam, Direktør, DataConsult ApS

Sanne Wiborg, HR og Regnskabschef, KIMO Consult ApS

Frederik Linderberg, Co-founder og Partner, ZRM

Ronnie Pedersen, Senior Manager Network & Security, Atea Professional services

Morten Sørensen, CEO, Omnisec

Ali Al-Alak, CEO, SPEDA

Mathias Nielsen, Cyber Security Team Lead, CURAit A/S

Morten Olsen, Projektchef SW, DI-Teknik A/S

Bo Ellehave, Partner, Northtech ApS

Steen Jensen, Ejer, ip-support

Søren Bank Greenfield, Afdelingschef (Cyber- og informationssikkerhed), Sundhedsdatastyrelsen

Simon Kramme, Enhedsleder Oversvømmelse & Hydrologi, DMI

Heidi Schwartz, Engineering Manager, Monta aps.

Kenneth Bülow, Chef for Cyber- & informationssikkerhed, DR (Danmarks Radio)

Martin Andersen, Director of Engineering, BLAST

Sebastian Brøndum, Senior Cloud Engineer, Raw Power Games

Kristian de Lichtenberg, CTO, Costbits Aps

John Schmidt, Head of IT, Lederne

Simon N Jensen, IT-sikkerhedskonsulent , Industriens Pension

Peter Hansen, Direktør og godkendt revisor, øernes revision

Ann Christina Rindom Sørensen, Direktør, SafeJournal ApS

Jesper Stæhr Mikkelsen, Kontorchef, Klimadatastyrelsen

Benjamin Irani, Director, Software Engineering, Infrastructure, Cyber Security and Cloud Solutions, Eywa Systems

Mikkel Mandrup, Operations Manager, Netcompany A/S

Michael Bræmer Roune, Delivery Director, Fellowmind

Ralph Olsen, Consultant Manager, Conscia Danmark A/S

Simon Juul, Operations Manager, Dataexpert

Morten Bøgh, Lead Engineer, the LEGO Group

Simon Thyregod, CISO, Nykredit

Eske Jakobsen, Politikommissær (sektionsleder) , National enhed for Særlig Kriminalitet - National Cyber Crime Center

Tomasz Otap, IT-Partner, Move On Career

Markus Priess, Dagligt leder, Currus Connect ApS

Andrius Bendikas, CEO, Twentyfour

Jacob Behrend, IT-chef, Lyngby Taarbæk Forsyning

Lars Bøgelund Sørensen, Cloud Architect, GN Store Nord A/S - GN Group - GN IT

Mikkel Jon Larssen, Partner, Chef for Risk Assurance i BDO (It-revisorer og cyberspecialister), BDO Statsautoriseret Revisionsaktieselskab

Michael Blom Vedel, Team Lead, IT Security & Network, Banking Circle

Jonas Donbæk, Director, Head of Group IT, s360

Line Hansen, Head of People & Culture.io, CyberPilot.io

Ask Risom Bøge, Områdeleder, Sikkerhed & Compliance , Digitalisering og It , Region Midtjylland

Claus Glavind, Director, Cloud Operations, DynamicWeb Software A/S

Dan Ellehuus Nielsen, Team lead Cybersecurity OTSOC 24-7, Siemens Gamesa Renewable Energy A/S

Nicolai, Co-Founder, Klimakampen ApS

Oliver Albertsen, IT Security Consultant, Banshie

Kasper Jensen, IT-Sikkerhedsspecialist, GEUS

Alexandru Gheorghiasa, Senior IT Security Architect, Novo Nordisk

Ulla Malling, Projektchef, Forbrugerrådet Tænk

Justin Strangeways, Senior Security Manager, GlobalConnect A/S

Bjarke Alling, Principal Advisor, Epical Group

Christian Wiese Svanberg, Advokat & Partner, CO:PLAY advokatfirma

Lasse Birnbaum Jensen, Teamleder for Infrastruktur , SDU IT

Mathias Ytte Lindberg Droob, Datasikkerhedkonsulent, Aalborg forsyning

Chris Kjølbo, Systemadministrator, ZBC // Avirus

Martin Petersen, Chief Information Security Officer, ISS A/S

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

HBS Economics konkluderer at efterspørgslen på arbejdskraft med cybersikkerhedskompetencer vil stige og der frem mod 2030 i Danmark være behov for at besætte 13.000 flere stillinger inden for cybersikkerhed.

I KEAs behovsanalyse angiver 74% af aftagerne, at de vil være interesserede i at ansætte en eller flere dimittender fra den nye uddannelse. 97 aftagere er fra Region Hovedstaden og de har angivet en interesse i årligt at ansætte mellem 48-67 dimittender. De 97 organisationer udgør anslået 2% af aftagerne inden for relevante brancher i Region Hovedstaden, så det reelle behov for dimittender vil være større.

Data fra LinkedIn viser, at der i september 2024 var 12.653 stillingsopslag på LinkedIn i hele landet, hvor ordene ‘cybersikkerhed’ eller ‘IT-sikkerhed’ indgik, og at der lokalt i København var 4381 stillingsopslag med ordet ‘cybersikkerhed’ og 7231 med ordet ‘IT-sikkerhed’.

“Vi har et stort behov for dygtige unge mennesker i Danmark indenfor Cyberområdet. Ikke mindst for at have kompetencerne i DK. Hos ISS f.eks. har vi langt de fleste cybermedarbejdere ansat i udlandet da der ikke er nok i DK ”
Martin Petersen, CISO, ISS

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

Deltagerne i behovsundersøgelsen inkluderer private og offentlige aftagere fra relevante brancher, rekrutteret gennem KEAs virksomhedssamarbejde. KEAs uddannelsesudvalg for de digitale uddannelser har ligeledes været inddraget i processen.

Respondenternes jobfunktion
Øverste ledelse i større organisationer: 27
Områdeledelse: 40
IT-og cybersikkerhedsspecialister: 25
Leder eller ejer af mindre IT-org.: 21
Anden ledelse: 5

84 aftagere har udtrykt støtte til ansøgningen, herunder Novo Nordisk, ISS, Netcompany, GN Store Nord, Lyngby Taarbæk Forsyning, Nykredit, Københavns Kommune, Kombit, Dubex og Sundhedsdatastyrelsen.

Følgende interesseorganisationer har lavet en støtteerklæring til uddannelsen:

- DI Digital
- Industriens Fond
- Center for Cybersikkerhed
- HK Stat
- KL

Der har desuden været afholdt møder og interviews med over 30 deltagere fra DI Digital, Dansk Erhvervs CISO Netværk, HK Stat, KL, Dubex, Københavns Kommune, Forsvaret, Industriens Fond og Center for Cybersikkerhed.

Hvordan er det konkret sikret, at den nye uddannelse matcher det påviste behov? Besvarelsen må maks. fylde 1200 anslag
Uddannelsen er udviklet af nuværende undervisere på PBA i IT-sikkerhed i dialog med praktikvirksomheder og gennem deltagelse i netværk og på konferencer.

Følgende elementer har været anvendt:

- Løbende kvalitetsarbejde med relevans for cybersikkerhed
- Uddannelsesudvalg

- Kvalitative dialoger med fagforbund, netværk samt aftager- og praktikvirksomheder
- Spørgeskemaundersøgelse
- Interessetilkendegivelse
- Høring af relevante uddannelsesorganisationer

Herefter er der udført desk research, hvor vi bl.a. har inddraget disse analyser:

- Regeringens nationale strategi for cyber- og informationssikkerhed 2022-2024
- Analyse fra HBS Economics
- Rapporten ’IT i praksis 2023-24’ fra Rambøll og Dansk IT
- LinkedIn Talent, søgning på Cybersikkerhed og IT-sikkerhed

Der er afholdt interviews og møder med mere end 30 interessenter og aftagere, som har givet feedback på indhold og dimittendprofiler.

Der er gennemført en spørgeskemaundersøgelse via mail og på LinkedIn med 118 respondenter, der har givet input til uddannelsens indhold og behov for praktikanter og dimittender.
Der har desuden været dialog med Erhvervsakademi Aarhus om indhold, og der er opnået enighed om uddannelsesbeskrivelsen.

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

KEA har lavet en oversigt over beslægtede uddannelser inden for fagområdet. Oversigten viser, at der ikke findes andre praksisnære videregående uddannelser på erhvervsakademi- og professionsbachelorniveau, som giver generelle cybersikkerhedskompetencer med mulighed for specialisering i forretning eller teknik. Datamatiker og IT-Teknolog uddannelserne giver adgang til top-up i IT-sikkerhed, men cybersikkerhed indgår ikke i fagene. Top-up i IT-sikkerhed giver primært tekniske kompetencer, mens ingeniøruddannelser har højere adgangskrav og ingen forretningsrettede fag.

Den nye uddannelse i cybersikkerhed vil være beslægtet med datamatiker, IT-teknolog og top-up i IT-sikkerhed, som alle har lav ledighed. I 2021 var ledigheden for dimittender 4-7 kvartal efter uddannelse: **IT-sikkerhed** 6,4%, på KEA 3,9%. **Datamatiker** 7,4%, på KEA 2,8%. **IT-teknolog** 7,4%, på KEA 5,4%. Den nye uddannelse er primært beslægtet med top-up i IT-sikkerhed, som ikke er dimensioneret.

KEA vil udfase sit udbud af top-up i IT-sikkerhed. Udfasningen afhænger af opstarten af den nye uddannelse, for at sikre, at der overordnet set vil blive uddannet flere med kompetencer inden for cybersikkerhed eller IT-sikkerhed.

Uddybende bemærkninger

Oversigt over beslægtede uddannelser:

Erhvervsakademiuddannelser 2-2 ½ år

Datamatiker, 2 ½ år
Udbud: KEA, EAAA, Erhvervsakademi SydVest, Dania, Erhvervsakademi MidtVest, Copenhagen Business Academy, Zealand, UCN, UCL
Link til studieplan: https://studieordninger.kea.dk/2024/31/196 Kort beskrivelse: På uddannelsen lærer du at programmere, analysere og dermed at udvikle og optimere IT-systemer.
Forskel: Der er mere vægt på programmering og systemudvikling, men begrænset indhold af netværk. Der er ingen kommunikation eller cybersikkerhed.

IT-teknolog, 2 år
Udbud: KEA, EAAA, Erhvervsakademi Dania, UCL, UCN
Link til studieplan: https://studieordninger.kea.dk/2024/31/181
Kort beskrivelse: På IT-teknologuddannelsen lærer du at designe og opbygge netværk, som indeholder fx routere, switche, firewalls og servere samt elektronikudvikling og programmering af mikroprocessorsystemer i forbindelse med IoT.
Forskel: Der er mere vægt på netværk og praktisk elektronikudvikling, men begrænset indhold af programmering og IT-sikkerhed. Der er ingen kommunikation eller cybersikkerhed.

Top-up uddannelser, Professionsbachelor 1 ½ år

IT-sikkerhed
Udbud: KEA, EAAA, Zealand, UCN, UCL
Link til studieplan: https://studieordninger.kea.dk/2024/33/183 Kort beskrivelse: Du bliver ekspert i bekæmpelsen af hackere, ransomware og DDOS-angreb, og du får kompetencer indenfor governance – altså de gode procedurer for at undgå angreb.
Forskel: Der er vægt på teknisk IT-sikkerhed, men begrænset indhold af forretningsrettede cybersikkerhedsfag. Uddannelsen bygger oven på enten Datamatiker eller IT-teknolog, som ikke har læringsmål inden for cybersikkerhed.

Softwareudvikling
Udbud: KEA, EAAA, Copenhagen Business Academy, Erhvervsakademi Dania, Erhvervsakademi SydVest, UCN, UCL
Link til studieplan: https://studieordninger.kea.dk/2024/33/192
Kort beskrivelse: På top-up uddannelsen i Softwareudvikling lærer du, hvordan du designer og programmerer store distribuerede datatunge systemer.
Forskel: Uddannelsen indeholder programmering, softwareudvikling og systemudvikling. Cybersikkerhed indgår ikke i uddannelsen.

Bacheloruddannelser

Cyberteknologi (civilingeniør)
Udbud: DTU, Lyngby
Link til studieplan: https://www.dtu.dk/uddannelse/bachelor/uddannelsesretninger/cyberteknologi
Kort beskrivelse: Uddannelsesretningen kombinerer software med hardware – kabler med teori – for at give dig den bedste forståelse af de usynlige teknologier, der hele tiden ændrer vores verden.
Forskel: Uddannelsen har fokus på software, hardware og netværk. Forretningsrettede cybersikkerhedsfag indgår ikke i uddannelsen. Kræver Matematik A, Dansk A samt to STEM fag på A, B eller C niveau. Sigter mod kandidatuddannelse som civilingeniør.

Cyber- og computerteknologi
Udbud: Aalborg Universitet, København
Link til studieplan: https://www.aau.dk/uddannelser/bachelor/cyber-computerteknologi
Kort beskrivelse: På uddannelsen i Cyber- og computerteknologi har du fokus på programmering, internetteknologier, agil softwareudvikling, sikkerhed og bæredygtighed.
Forskel: Uddannelsen har fokus på programmering, softwareudvikling og internetteknologier. Der er få tekniske sikkerhedsfag, men ingen forretningsrettede. Kræver Matematik A, Dansk A samt et STEM fag på A eller B niveau. Sigter mod kandidatuddannelse som civilingeniør.

Kandidatuddannelser

Cybersecurity (civilingeniør)
Udbud: Aalborg Universitet, Aalborg og København
Link til studieplan: https://www.aau.dk/uddannelser/kandidat/cyber-security
Kort beskrivelse: På uddannelsen lærer du om netværkssikkerhed, software og privacy, og du bliver kvalificeret til at hjælpe virksomheder og offentlige institutioner til at modstå fremtidige cyberangreb.
Forskel: Kræver ingeniørbachelor. Uddannelsen har fokus på tekniske sikkerhedsfag, men ingen forretningsrettede.

Computer science and engineering (civilingeniør)
Udbud: DTU, Lyngby
Link til studieplan: https://www.dtu.dk/english/education/graduate/msc-programmes/computer-science-and-engineering
Kort beskrivelse: Bred uddannelse inden for datalogi og ingeniørvidenskab med enkelte kurser i cybersikkerhed.
Forskel: Kræver bachelor inden for ingeniørfaget. Uddannelsen har fokus på datalogi, software og hardware med enkelte fag inden for teknisk cybersikkerhed.

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

Rekrutteringsgrundlaget vil være de gymnasiale uddannelser og relevante erhvervsuddannelser, f.eks. data- og kommunikationsuddannelsen. I 2023 var der her 14.956 studenter, der fuldførte deres gymnasieuddannelse (danmarks statistik). Tal fra Børne- og Undervisningsministeriet viser, at der i de kommende år vil blive flere unge i København trods generelt faldende ungdomsårgange. De fremskriver at antallet af unge på ungdomsuddannelserne i København og i Københavns omegn vil stige med ca. 3300 fra 2018-2030.

Uddannelsen forventes at differentiere 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 forventer KEA at kunne tiltrække et bredere udsnit af profiler end beslægtede uddannelser.

På IT-teknologuddannelsen har KEA oplevet en kraftig stigning i søgningen og har i år optaget 160 studerende. Ca. 67% af de optagne ønsker at studere videre på PBA i IT-sikkerhed. Vi forventer, at en del af disse studerende fremover vil søge ind på PBA i cybersikkerhed.

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. Hvis dimittenderne ønsker yderligere uddannelse senere, vil der være forskellige muligheder.

De erhvervsakademiuddannede i cybersikkerhed kan opnå en professionsbachelorgrad ved at tage de sidste to år af PBA-uddannelsen eller tage en diplomuddannelse i IT-sikkerhed eller andre IT-uddannelser på deltid.

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

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

KEA anser mindst 40 studerende pr. hold for rentabelt. Første hold: 40 studerende (sommer + vinter). Herefter: 80 studerende sommer, 40 studerende vinter.

2025/26: 80
2026/27: 120
2027/28: 120

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

I behovsanalysen angiver 83% af aftagerne, at de vil være interesserede i at have studerende i praktik. Her er der spurgt til, hvor mange praktikanter de kunne være interesserede i at tage pr. år. Her har 97 aftagere i Region Hovedstaden angivet en interesse for at tage mellem 94 og 141 praktikanter årligt. De 97 organisationer udgør anslået 2% af aftagerne inden for relevante brancher i Region Hovedstaden, så det reelle antal praktikvirksomheder vil være større.

29% af aftagerne er kun interesserede i praktikforløb på 20 uger, hvilket indikerer, at vi med en længere praktik på professionsbacheloruddannelsen kan udvide antallet af praktiksteder.

Det forventes, at praktikanterne fra den nye uddannelse i cybersikkerhed vil komme i praktik i mange af de samme virksomheder som de beslægtede uddannelser i IT-teknologi og IT-sikkerhed på KEA. I perioden 2020-2024 var der på disse uddannelser samlet 513 praktikforløb i København og 549 praktikforløb i hele Danmark.

Øvrige bemærkninger til ansøgningen

Den stigende digitalisering af samfundet stiller større og større krav til virksomheder, organisationer og medarbejderens kompetencer inden for cybersikkerhed. Cybersikkerhed tænkes i stigende grad ind i alle dele af vores samfund, og det er nødvendigt med dygtige medarbejdere for at afværge cyberangreb og udtænke løsninger, som beskytter samfundet. De videregående uddannelser skal løbende tilpasse sig den aktuelle virkelighed, og her er cybersikkerhedsdagsordenen ingen undtagelse. KEA har kompetencerne og viljen til at bidrage til, at den danske sikkerhed og konkurrenceevne styrkes, ved at udbyde en ny professionsbacheloruddannelse indenfor cybersikkerhed.

På baggrund af behovsanalysen har vi dokumenteret behovet for en professionsbachelor i cybersikkerhed med mulighed for afstigning på en erhvervsakademiuddannelse. KEAs samarbejdspartnere i erhvervslivet udtrykker et stort ønske og behov for den nye uddannelse for at imødekomme det voksende behov for cybersikkerhedskompetencer. Ved at etablere en ny professionsbacheloruddannelse i cybersikkerhed med afstigningsmulighed på erhvervsakademiniveau får danske virksomheder adgang til medarbejdere med de nødvendige kompetencer, så de kan beskytte fysisk og digital infrastruktur og afbøde følgerne af angreb, der er en konsekvens af et stigende trusselsniveau.

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

Ja

Status på ansøgningen

Godkendt

Ansøgningsrunde

2024-2

Afgørelsesbilag - Upload PDF-fil

Afgørelsesbrev A13 Professionsbachelor Cybersikkerhed KEA.pdf

Samlet godkendelsesbrev - Upload PDF-fil

KEA KVALITET OG ANALYSE

GULDBERGSGADE 29 E
2200 KØBENHAVN N

TEL +45 46 46 00 00

CVR: 31656206

WWW.KEA.DK

BEHOVSANALYSE

Behov og relevans for professionsbachelor i cybersikkerhed

Indhold

1. Indledning 2
1.1 Metode 2
2. Kompetenceefterspørgsel generelt 3
3. Behovsanalyse 4
3.1 Interviews med aftagere og interesseorganisationer 5
3.2 Spørgeskemaundersøgelse blandt aftagere 7
3.3 Aftagernes holdning til behovet for uddannelsen 9
3.4 Aftagernes holdning til fagligt indhold på uddannelsen 10
3.5 Afrunding 13
4. Uddannelsens indhold 14
4.1 Uddannelsens formål og erhvervssigte 14
4.2 Uddannelsens overordnede mål for læringsudbytte 14
4.3 Uddannelsens indhold og tilrettelæggelse 17
4.4 Beslægtede uddannelser 19
4.5 Videreuddannelsesmuligheder 23
4.6 Rekruttering til uddannelsen 23
5. Interessetilkendegivelser 23
5.1 Udpluk af støtteerklæringer 24
6. Konklusion 25
7. Høringssvar fra andre uddannelsesinstitutioner 26
7.1 Opsummering af høringssvar 26
7.2 Høringssvar vedlagt 27

1. INDLEDNING

Behovet for kompetencer til at imødekommende den stigende trussel inden for cybersikkerhed fremgår blandt andet af regeringens nationale strategi for cyber-og informationssikkerhed (regeringen, 2021) samt af tal fra Rambøll og Dansk IT. Deres rapport 'IT i praksis 2023-24' viser, 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).

KEAs samarbejdspartnere i erhvervslivet udtrykker et stort ønske og behov for den nye professionsbacheloruddannelse i cybersikkerhed for at imødekomme det voksende behov for cybersikkerhedskompetencer. Den nye uddannelse vil kvalificere dimittender til at varetage opgaver inden for cybersikkerhed i den offentlige og den private sektor til at arbejde med både tekniske og forretningsmæssige aspekter af cybersikkerhed.

På uddannelsen vil de studerende lære at opbygge og vedligeholde tekniske og forretningsmæssige strukturer til at forebygge, opdage og afbøde cyberangreb samt governance og compliance relateret til cybersikkerhed. Uddannelsen vil være praksisnær og bygge på anvendt metode og teori samt værktøjer og systemer, der gør den uddannede i stand til at skabe værdi i en organisation fra dag et. Der vil i høj grad indgå cases og virksomhedssamarbejde, ligesom praktik er et centralt element.

Uddannelsen er opbygget således at den studerende kan afslutte uddannelsen efter 2 år og opnå en erhvervsakademiuddannelse i cybersikkerhed. De erhvervsakademiuddannede kan udføre drift- og supportopgaver inden for cybersikkerhed i større private og offentlige organisationer, samt SMV-segmentet.

Professionsbachelorerne vil finde beskæftigelse som cybersikkerhedsspecialister i en bred vifte af roller i større organisationer og organisationer, der er specialiserede i cybersikkerhed.

1.1 METODE

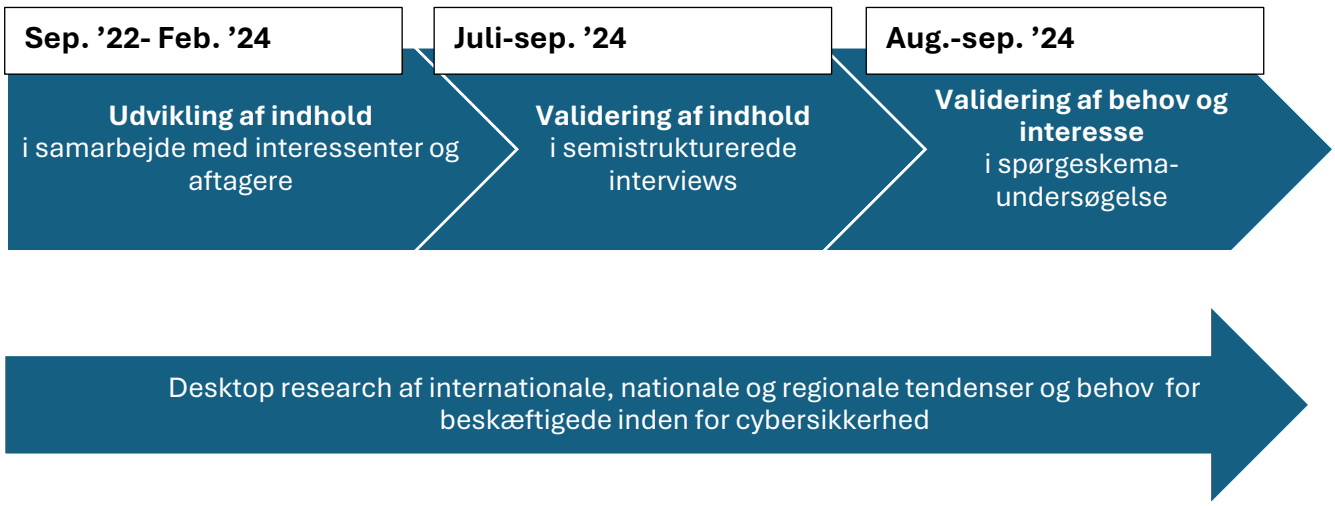
Behovsanalysen er inddelt i to dele.

Den første del er en analyse af aftagernes behov baseret på kvantitative og kvalitative data indsamlet af KEA samt løbende desk research. Den fulde analyse kan rekvireres via uddannelseschef Merete Hess, mhes@kea.dk.

Den anden del beskriver uddannelsens indhold og tilrettelæggelse.

Aftagernes behov i dækningsområdet er et centralt omdrejningspunkt. KEA har et stort netværk af relevante praktik-og aftagervirksomheder fra beslægtede uddannelser i dækningsområdet, som behovsafdækningen har taget udgangspunkt i.

Oversigt over udvikling af fagindhold og validering af indhold og behov:



2. KOMPETENCEEFTERSPØRGSEL GENERELT

"Cybertruslen er i dag en af de mest alvorlige trusler mod Danmark. Den er blevet et grundvilkår, som vi alle sammen må agere efter – i vores privatliv, vores arbejdsliv og i samfundet som helhed" (regeringen, 2021). Regeringens nationale strategi for cyber- og informationssikkerhed 2022-2024, sigter efter at styrke Danmarks digitale sikkerhed, fordi der er en markant cybersikkerhedstrussel og ikke nok uddannede med relevante kompetencer.

Tal fra Rambøll og Dansk IT's rapport ' IT i praksis 2023-24' viser, 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).

22 % af de virksomheder og myndigheder, der har forsøgt at rekruttere medarbejdere inden for informationssikkerhed, har enten ikke kunnet ansætte eller har måttet ansætte en profil uden alle de ønskede kompetencer (regeringen, 2021).

Efterspørgslen på arbejdskraft med informationssikkerhedskompetencer vil stige fremover (HBS Economics, 2019). HBS Economics konkluderer i analysen, at hvis den nuværende udvikling fortsætter vil der frem mod 2030 være behov for at besætte 13.000 flere stillinger inden for IT-sikkerhed i Danmark end i dag (HBS Economics, 2019).

I arbejdet med at afdække behovet for medarbejdere inden for cybersikkerhed har KEA været i dialog med LinkedIn ang. data på ledige stillinger inden for området. LinkedIn har trukket data på opslåede stillinger i hele landet og i København, hvor 'cybersikkerhed' eller 'IT-sikkerhed' nævnes. Data viser, at der i september 2024 var 12.653 ledige stillinger på LinkedIn i hele landet og at der lokalt i København var 4381 ledige stillinger, hvor ordet 'cybersikkerhed' indgår samt 7231 stillinger, hvor ordet 'IT-sikkerhed' indgår.

I undersøgelsen fremgår det samtidig, at kompetencer inden for IT Compliance og IT Governance er blandt særligt efterspurgte i jobopslagene inden for søgeordene. Disse temaer er i høj grad en del af den forretningsmæssige del af cybersikkerhedsområdet på den nye uddannelse.

3. BEHOVSANALYSE

I KEAs arbejde med sikring og udvikling af kvaliteten af uddannelserne indgår der løbende kontakt til virksomheder og relevante interessenter. Det er blandt andet i dette arbejde, KEA har fået input til, hvilke behov aftagerne for den nye uddannelse i cybersikkerhed har. Projektgruppen, der har arbejdet med at udvikle uddannelsen, består af nuværende undervisere på professionsbacheloruddannelsen i IT-sikkerhed. Gruppen har gennem udviklingsprocessen fået feedback på struktur og indhold fra praktiksteder, virksomhedskontakter og organisationer og justeret indholdet løbende. Herefter er dialogen blevet formaliseret gennem semistrukturerede interviews, hvor fagoversigten og fag er blevet gennemgået og informanterne har givet feedback. Ligeledes har der løbende være dialog med Erhvervsakademi Aarhus om indholdet, og der er opnået enighed om uddannelsesbeskrivelsen.

I alt har mere end 150 aftagere og interessenter været inddraget i arbejdet med at udvikle uddannelsen.

Af tabel 1 fremgår en ikke-udtømmende liste over aftagere og interessenter, der har været inddraget:

Tabel 1

Interviews og dialog	**Spørgeskemaundersøgelse**
Jeppe Engell – HK Privat (senere DI Digital) Formand for KEAs Uddannelsesudvalg for de digitale uddannelser frem til foråret 2024	Klaus Petersen, Alpha Solutions John Talchow, CyberNordic Erik Lindstam, DataConsult ApS Sanne Wiborg, KIMO Consult ApS
Rasmus Vedel, chef for Cyberservices, Kombit	Frederik Linderberg, ZRM Ronnie Pedersen, Atea Professional services
Gorm Mandsberg, CEO Dubex	Morten Sørensen, Omnisec Ali Al-Alak, SPEDA
Programchef i Industriens Fond	Mathias Nielsen, CURAit A/S Morten Olsen, DI-Teknik A/S
Programleder, KL	Bo Ellehave, Northtech ApS Steen JEnsen , ip-support
Lisa Hartmann Jensen, Teamkoordinator Sikkerhed, Københavns Kommune møde i foråret '24 samt 26/8 '24	Søren Bank Greenfield, Sundhedsdatastyrelsen Simon Kramme, DMI Heidi Schwartz, Monta aps. Kenneth Bülow, DR (Danmarks Radio)
Center for cybersikkerhed, to afdelingsledere	Martin Andersen, BLAST Sebastian Brøndum, Raw Power Games
Erhvervsakademi Århus, Uddannelseschef Gert Simonsen m.fl.	Kristian de Lichtenberg, Costbits Aps John Schmidt, Lederne Simon N Jensen, Industriens Pension
Dansk Erhverv, CISO Netværk (Chief Information Security Officers)	Peter Hansen, ørnes revision Ann Christina Rindom Sørensen, SafeJournal ApS

Patrick Terman-Andreasen, HK Stat KEAs uddannelsesudvalg for de digitale uddannelser, se medlemmer her: https://kea.dk/images/DA/Files/Om-KEA/KEA-uddannelsesudvalg-2022-2026.pdf	Jesper Stæhr Mikkelsen, Klimadatastyrelsen Benjamin Irani, Eywa Systems Mikkel Mandrup, Netcompany A/S Michael Bræmer Roune, Fellowmind Ralph Olsen, Conscia Danmark A/S Simon Juul, Dataexpert Morten Bøgh, the LEGO Group Simon Thyregod, Nykredit Eske Jakobsen, National enhed for Særlig Kriminalitet - National Cyber Crime Center Tomasz Otap, Move On Career Markus Priess, Currus Connect ApS Andrius Bendikas, Twentyfour Jacob Behrend, Lyngby Taarbæk Forsyning Lars Bøgelund Sørensen, GN Store Nord A/S - GN Group - GN IT Mikkel Jon Larssen, BDO Statsautoriseret Revisionsaktieselskab Michael Blom Vedel, Banking Circle Jonas Donbæk, s360 Line Hansen, People & Culture.io, CyberPilot.io Ask Risom Bøge, Digitalisering og It , Region Midtjylland Claus Glavind, DynamicWeb Software A/S Dan Ellehuus Nielsen, Siemens Gamesa Renewable Energy A/S Nicolai, Klimakampen ApS Oliver Albertsen, Banshie Kasper Jensen, GEUS Alexandru Gheorghiasa, Novo Nordisk Ulla Malling, Forbrugerrådet Tænk Justin Strangeways, GlobalConnect A/S Bjarke Alling, Epical Group Christian Wiese Svanberg, CO:PLAY advokatfirma Lasse Birnbaum Jensen, SDU IT Mathias Ytte Lindberg Droob, Aalborg forsyning Chris Kjølbo, ZBC // Avirus

3.1 INTERVIEWS MED AFTAGERE OG INTERESSEORGANISATIONER

Informanterne er blevet præsenteret for uddannelsens opbygning og fagelementernes indhold. Herefter har der været en dialog om indhold og hvor dimittendprofilerne kunne finde beskæftigelse, hvor vi særligt har været nysgerrige på de nyskabende elementer i uddannelsen, nemlig:

- Hvordan informanten vurderede indhold i den 2-årige erhvervsakademiuddannelse og behov for de uddannede
- Hvordan informanten så på kombinationen af teknik- og forretningskompetencer

Endelig har vi vendt behovet for cybersikkerhedsuddannede i informantens egen organisation og generelt på samfundsplan.

De vigtigste pointer fra interviews fremgår af tabel 2.

Tabel 2

Jeppe Engell, Chefkonsulent, DI Digital (tidl. HK Digital og formand for KEAs	Forretning/teknik: Det er vigtigt med en bredde i fagene i starten af uddannelsen, så både de forretningsmindede og teknikmindede har en passende læringskurve.

uddannelsesudvalg for de digitale uddannelser)	EAK vs. PBA: Vi er nødt til at skabe kompetencer på flere niveauer og uddanne både generalister og specialister. Særligt SMV'er har ikke brug for fuldtidsspecialist.
Rasmus Vedel, chef for Cyberservices, Kombit (Kombit hjælper kommuner med at løfte cybersikkerhed.)	Forretning/teknik: Kombinationen er vigtig. Der mangler tekniske profiler, der forstår forretningen. EAK vs. PBA: Kombit kan ansætte PBA'erne i deres Security Operations Center. EAK kan ansættes som firstlinesupportere. Behovet for EAK vil være stort ude i kommunerne. En PBA vil give kommunerne mere, end de har brug for.
Gorm Mandsberg, CEO Dubex (Løbende dialog om behov under udarbejdelsen af fag og struktur samt interview i aug. '24)	Cybersikkerhed/It-sikkerhed: Godt at brede fokus for uddannelsen ud fra IT-sikkerhed til cybersikkerhed. IT-sikkerhedsbegrebet indikerer, at det kun handler om IT, og at man kan købe sig til sikkerhed hos sin IT-leverandør. Cybersikkerhed er meget bredere og handler bl.a. om governance, beredskab og info-sec. IT er en lille del af det. Det er også et plus i forhold til den nuværende IT-sikkerhedsoverbygning, at sikkerhed tænkes ind i alle fag fra starten. Behov: 17 nuværende eller tidligere ansatte i Dubex er fra KEA. Behov for i størrelsesorden 4 praktikanter og 5-7 ansatte pr. år, heraf 1-2 kortuddannede.
Programchef i Industriens Fond	Fagfordeling på PBA: Det virker som en rigtig god og holistisk tilgang til cybersikkerhed. Det er en stor styrke, at man både har de tekniske, de organisatoriske og de mere menneskelige aspekter med. Kommentar til fagfordeling på EAK: Virker som en fin blanding af de forskellige cybersikkerhedsaspekter.
Programleder, KL	Eksempler på udfordringer blandt medlemmer af KL: Ubesatte stillinger. Overbelastning af eksisterende medarbejdere. Formentlig opgaver der ikke løftes tilstrækkeligt kvalificeret. Kommentar til fagfordeling EAK/PBA: Alle uddannelser der leverer kvalificerede kandidater på området er velkomne. De 2-årige kan vise sig at blive lige så efterspurgte som dem med den lange uddannelse, både i løn/kvalifikations gap - men også set i forhold til at kunne rekruttere og fastholde kandidater.
Center for cybersikkerhed, to afdelingsledere	Kommentar til fagfordeling EAK/PBA: KEAs forslag til en ny uddannelse i cybersikkerhed ser rigtig spændende ud. I et bredt samfundsmæssigt perspektiv er det vigtigt at styrke forebyggelse af angreb, da mange angreb på virksomheder skyldes mangelfuld IT-sikkerhed. Uddannelsens nationale fag giver en bred forståelse for hele sikkerhedsområdet, og de lokale fag og valgfag giver den studerende mulighed for tidligt at identificere sin interesse og sit talent. Praksisnærhed:

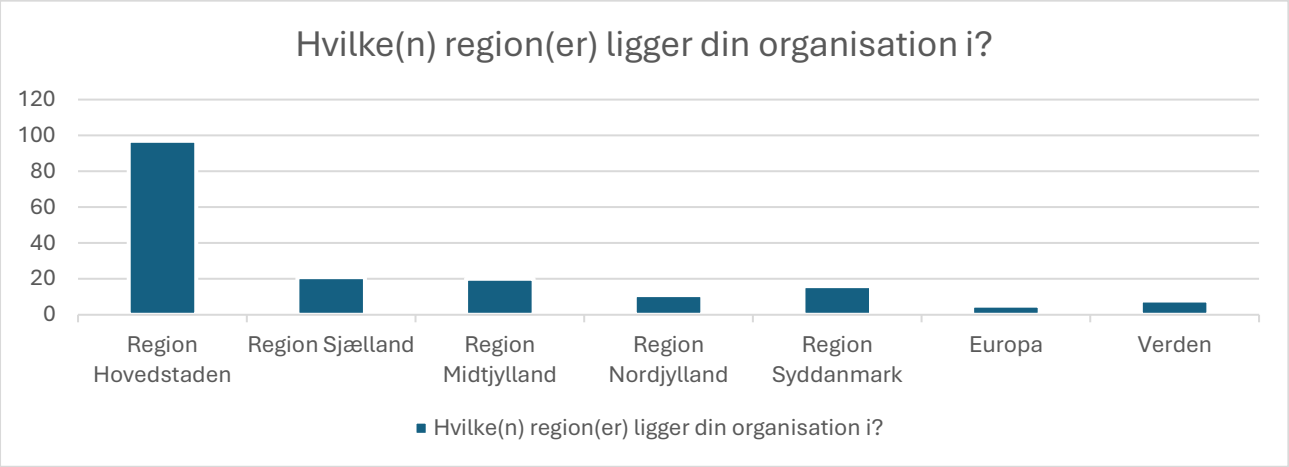
	Det er positivt, at de studerende får en hands-on tilgang gennem konkrete cases og at sikkerhed er et gennemgående tema på uddannelsen. Praktik og bachelor: I forhold til vores specifikke behov i CFCS synes vi, det er positivt, at praktikken forløber over et helt semester med mulighed for at fortsætte samarbejdet med den studerende i et bachelorprojekt. Det tager ofte noget tid at sikkerhedsgodkende en praktikant og give adgang til systemer og processer, og her er et langt forløb en fordel. Specialisering: Valgfag, lokale fag, praktik og bachelorprojekt vil give den studerende mulighed for specialisering i detektion, analyse og incidence response af cyberangreb. Sammen med den brede indføring i cybersikkerhed vil det give nogle profiler, der vil være attraktive for os, men også for andre offentlige myndigheder og private cybersikkerhedsfirmaer.
Lisa Hartmann Jensen, Teamkoordinator Sikkerhed, Københavns Kommune, møde i foråret '24 samt aug. '24	Forretning/teknik: Vi har i høj grad brug for medarbejdere med hybride kompetencer, der kombinerer forretningsforståelse og teknik. Om EAK-profiler: Den to-årige uddannelse i cybersikkerhed er der også et klart behov for – både i Københavns Kommune, hvor de kan indgå i first line support, og i de mindre kommuner, hvor de kan blive bindeled mellem forretning, IT og eksterne specialister. Behov: I Københavns Kommune er vi glade for bachelorerne i IT-sikkerhed, og de kommer næsten altid til samtale, hvis de søger job hos os, fordi kvaliteten af dimittenderne er så høj. Vi forventer at kunne aftage praktikanter og dimittender fra både EAK- og PBA-uddannelsen.

3.2 SPØRGESKEMAUNDERSØGELSE BLANDT AFTAGERE

Som del af KEAs behovsanalyse er der sendt en spørgeskemaundersøgelse til relevante praktik- og aftagervirksomheder. 118 aftagere har besvaret KEAs spørgeskema om den nye uddannelse i cybersikkerhed.

Det fremgår af figur 1 at størstedelen af respondenterne er fra Region Hovedstaden, som KEA også primært uddanner til.

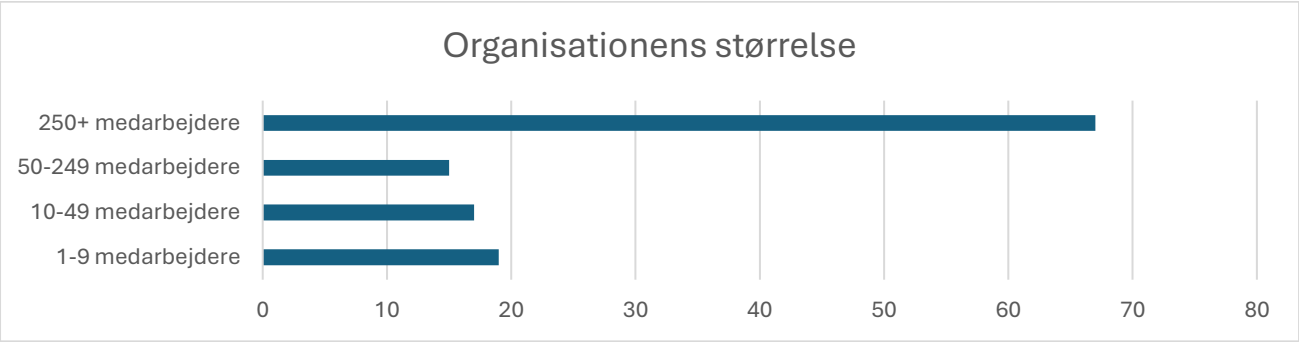
Figur 1



Respondenterne fordeler sig med 97 private, 19 offentlige og 2 andre typer organisationer.

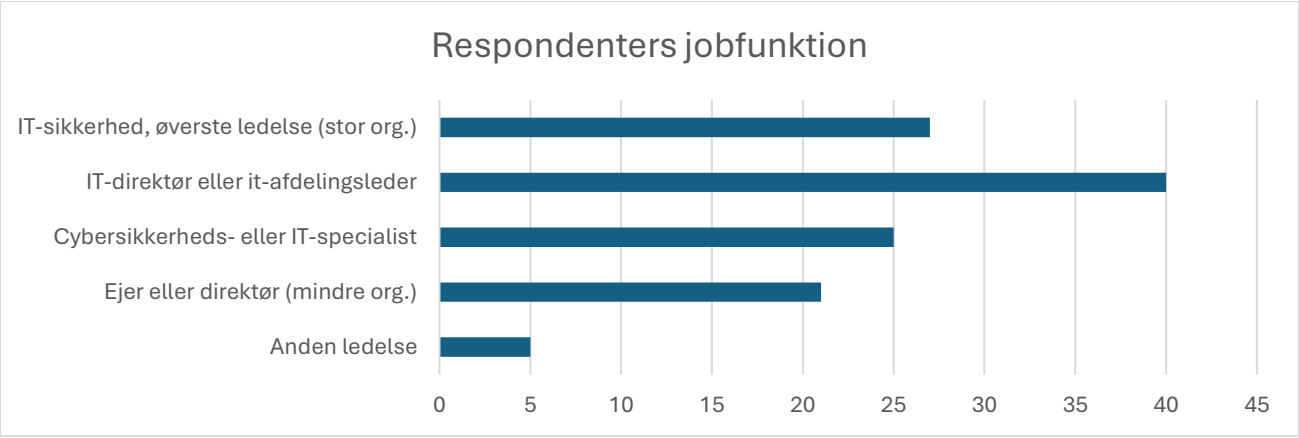
Jf. Figur 2 er der er flest respondenter fra store organisationer (over 250 medarbejdere),erunder 9 globale fondsejede eller C25 virksomheder og 19 offentlige organisationer.

Figur 2



Af figur 3 fremgår respondenternes stillingsbetegnelser inddelt i kategorier. Respondenterne er enten topledere inden for cybersikkerhed, IT-ledere, specialister eller en anden type ledere.

Figur 3



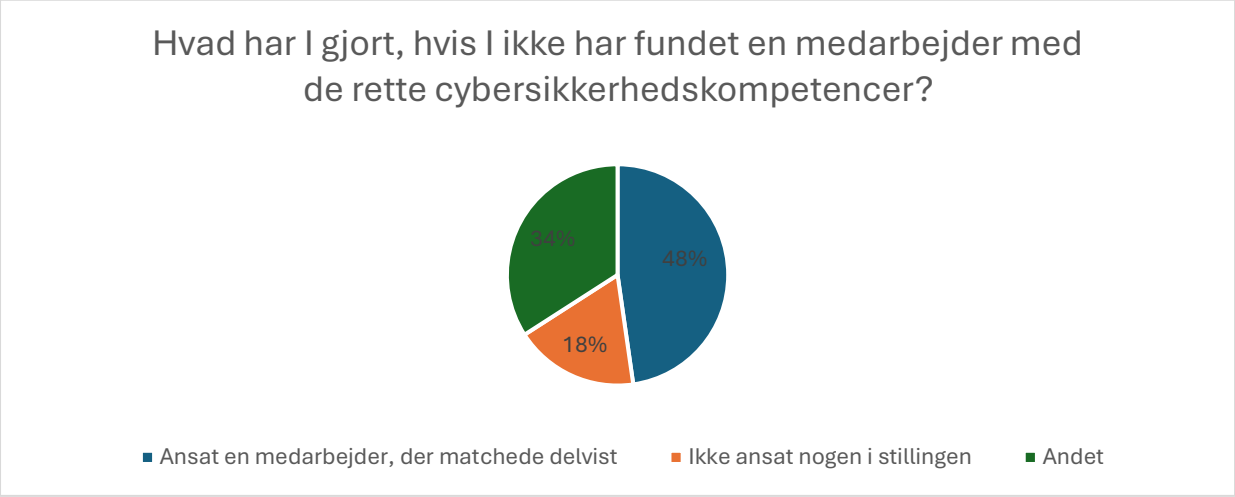
3.3 AFTAGERNES HOLDNING TIL BEHOVET FOR UDDANNELSEN

97% af respondenterne angiver, at behovet for cybersikkerhedsmedarbejdere de næste 5 år vil være stigende. Allerede i dag har mange virksomheder dog svært ved at rekruttere kvalificeret arbejdskraft.

55% af aftagerne har prøvet at rekruttere medarbejdere inden for cybersikkerhed inden for de seneste 2 år.

68% af aftagerne har oplevet udfordringer med rekruttering, heraf har 48% ansat en medarbejder, der matchede delvist, mens 18% har opgivet at ansætte jf. Figur 4. De resterende stillinger er bl.a. blevet besat i udlandet, via rekrutteringsbureau eller dækket af konsulenter.

Figur 4



Aftagernes interesse for praktikanter

I Region Hovedstaden har 80% af aftagerne i undersøgelsen interesse i at tage en eller flere praktikanter. Det drejer sig om 97 virksomheder. Disse virksomheder har angivet, at de er interesseret i at have mellem 88-135 praktikanter om året. De 97 organisationer udgør anslået 2% af aftagerne inden for relevante brancher i Region Hovedstaden, så det reelle behov for praktikanter vil være større.

Aftagernes interesse for dimittender

74% af aftagerne i Region Hovedstaden vil være interesserede i at ansætte en eller flere dimittender fra uddannelsen. De 97 virksomheder angiver, at de er interesserede i at ansætte mellem 48-67 dimittender om året. 18 virksomheder angiver ikke et konkret antal, men angiver at det vil afhænge af behov eller den konkrete profil på dimittenden. De 97 organisationer udgør som tidligere anført anslået 2% af aftagerne inden for relevante brancher i Region Hovedstaden, så det reelle behov for dimittender vil være større.

3.4 AFTAGERNES HOLDNING TIL FAGLIGT INDHOLD PÅ UDDANNELSEN

Respondenterne er blevet præsenteret for en fagoversigt for hhv. den 3 ½-årige professionsbacheloruddannelse og den 2-årige erhvervsakademiuddannelse. De er blevet spurgt, om de havde kommentarer til fagene. Der er efterfølgende lavet en tekstanalyse af kommentarerne med fokus på, hvad respondenterne forventer af fagligt indhold ud fra fagets navn.

12 respondenter skriver, at professionsbacheloruddannelsen ser fin, spændende eller fornuftig ud. 9 respondenter skriver det samme for erhvervsakademiuddannelsen. I undersøgelsen angives 26 specifikke ønsker til indhold, heraf 18 til de tekniske fagelementer og 8 ønsker til de fagelementer, der beskæftiger sig med forretning.

Respondenterne giver generelt udtryk for et behov for et bredt udsnit af emner inden for cybersikkerhed, hvilket understøtter uddannelsens opbygning hvor dimittenderne får en profil med en bred teknisk grundviden inden for cybersikkerhed kombineret med en dybere specialisering enten inden for teknik eller forretning.

Respondenternes ønsker til det tekniske indhold fordeler sig på 18 emner, nævnt af 1-6 respondenter hver, der spænder over IT-sikkerhedsdrift, programmering, system- og softwaresikkerhed, kryptografi, automatisering, fysisk udstyr og infrastruktur, trusselsanalyse, hacking, penetrationstest, datasikkerhed og håndtering af sikkerhedshændelser. Hands-on erfaring og produkterfaring nævnes også som vigtige elementer i uddannelsen.

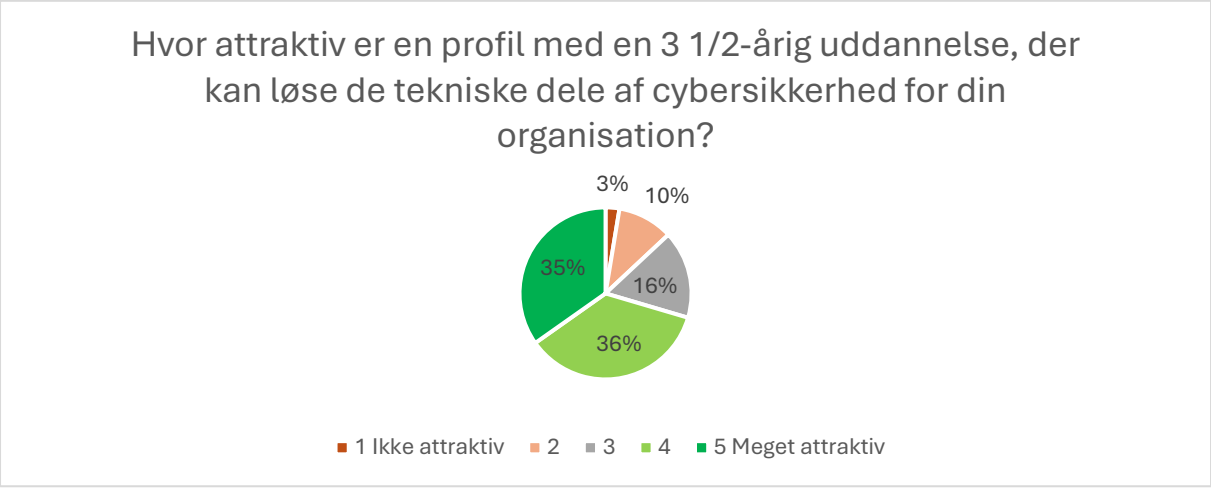
Ønsker til indhold inden for forretning er fordelt på lovgivning (16), compliance (13), kommunikation og rapportering (12) adfærd/awareness (11), governance (8), risikovurdering (8), virksomhedsforståelse (7) og projektledelse (1).

Alle emner berørt af respondenterne indgår i både professionsbacheloruddannelsen og erhvervsakademiuddannelsen med forskellig vægtning - med undtagelse af projektledelse. Ud fra dette vurderer KEA, at respondenterne ser et stort behov for en praksisrettet profil inden for cybersikkerhed, der kombinerer brede tekniske kompetencer med forretningsforståelse, kommunikation, governance og compliance, hvilket ikke findes i dag.

Behovet for profiler med teknisk eller forretningsmæssig specialisering

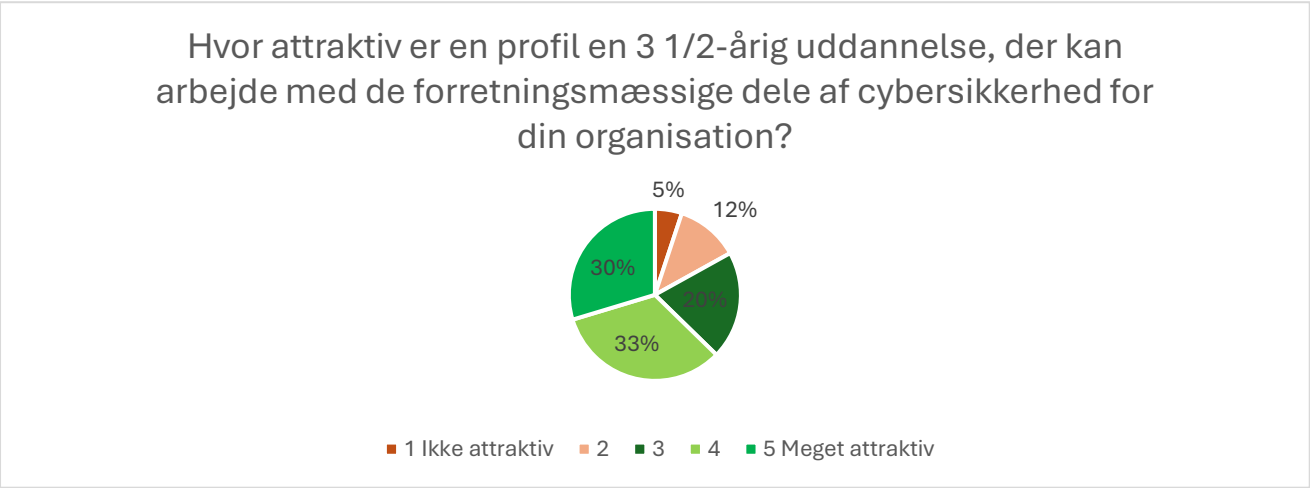
Af figur 5 fremgår det, at 71% af respondenterne bedømmer en professionsbacheloruddannelse med en teknisk specialisering til 4 eller 5 på en skala fra 1-5, hvor 1 er ikke attraktiv og 5 er meget attraktiv.

Figur 5



Af figur 6 fremgår det, at 63% af respondenterne bedømmer en professionsbacheloruddannelse med en forretningsspecialisering til 4 eller 5 på en skala fra 1-5, hvor 1 er ikke attraktiv og 5 er meget attraktiv.

Figur 6



Tre respondenter fra organisationer med over 250 ansatte skriver om behovet for at kombinere kompetencer inden for teknik og forretning:

"Vi har en høj grad af outsourcing af vores IT. Vi har brug for kompetente medarbejdere, til at sikre at vores leverandører leverer tilstrækkeligt sikre og de rigtige ydelser."
Simon Thyregod, CISO, Nykredit

"Som rådgiver inden for sikkerhedsbranchen ser jeg både internt og i særdeles eksternt stigende behov for folk som har kompetencer inden for it-sikkerhed. Dette både den mere tekniske del men også generalister inden for it-governance. Manglen på uddannede folk gør desværre at vi ser en del autodidakte it-sikkerhedsfolk som ikke altid helt har forstået hvad de

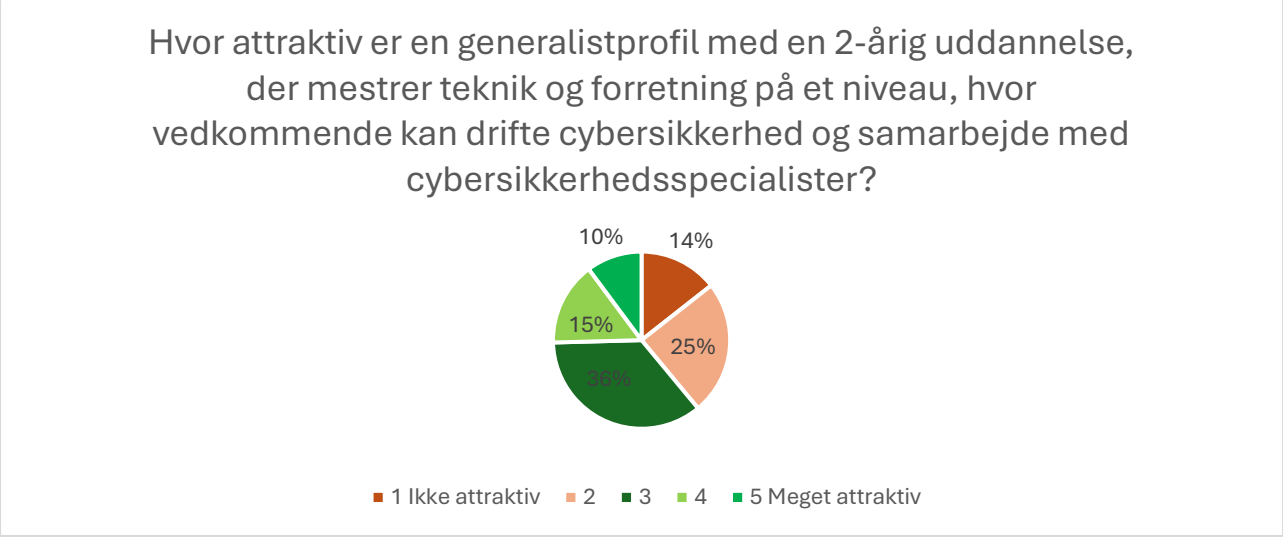
går og laver eller hvordan det de laver skal understøtte forretningsstrategien for den konkrete virksomhed de arbejder for."
Mikkel Jon Larssen, Partner, Chef for Risk Assurance i BDO (It-revisorer og cyberspecialister), BDO Statsautoriseret Revisionsaktieselskab

"[...] For de længere uddannelser er den tekniske og forretningsmæssige forståelse vigtig. Hvis det tekniske fundament er i orden, kan vi som regel godt hæve det tekniske niveau, hvor imod det forretningsmæssige helst skal være på plads når de kommer fra skolen."
Ralph Olsen, Consultant Manager, Conscia Danmark A/S

Da respondenterne giver udtryk for behov inden for et bredt udsnit af emner inden for cybersikkerhed, mener vi, at analysen understøtter professionsbacheloruddannelsens opbygning som en profil med en bred teknisk grundviden og en dybere specialisering enten inden for teknik eller forretning.

For erhvervsakademiuddannelsen er de primære aftagere enten store organisationer, der kan bruge dem til support og gentagne overvågningsopgaver eller små/mellemstore virksomheder, der har behov for en medarbejder til cybersikkerhedsdrift. Af figur 7 fremgår det, at 25% af respondenterne bedømmer en erhvervsakademiuddannelse med en drift- og supportprofil til 4 eller 5 på en skala fra 1-5, hvor 1 er ikke attraktiv og 5 er meget attraktiv.

Figur 7



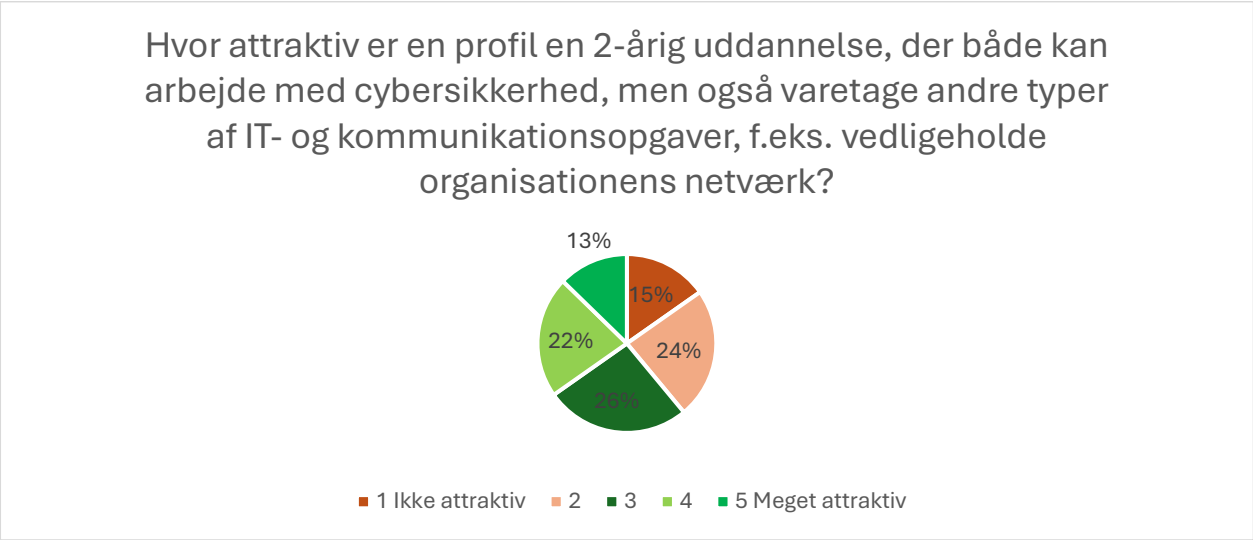
En større virksomhed skriver om behovet for en cybersikkerhedsdrift- og supportprofil:

"[...]Jeg har derimod brug for medarbejdere, der ud fra de strategier og retningslinjer, som udstikkes af specialisterne kan udføre de daglige kontroller (eks. CIS) og sikre at det tekniske landskab drives efter de fastlagte retningsliner. Så teknikere, som kan samarbejde og arbejde i forlængelse af specialisternes retningslinjer."

Jacob Behrend, IT-chef, Lyngby Taarbæk Forsyning

Af figur 8 fremgår det, at 35% af respondenterne bedømmer en erhvervsakademiuddannet med en cybersikkerheds- og IT-driftprofil til 4 eller 5 på en skala fra 1-5, hvor 1 er ikke attraktiv og 5 er meget attraktiv.

Figur 8



To mindre organisationer skriver om deres behov for medarbejdere til cybersikkerhedsdrift:

"En cybersikkerhed-uddannelse, hvor andre typer IT-opgaver kan også blive varetaget, vil klart være at foretrække i forhold til en virksomhed af vores størrelse. Vores virksomhed (og de fleste små virksomheder) vil givevis ikke have budget til en dedikeret medarbejder til KUN cybersikkerhed. Umiddelbart vil der være en del øvrige opgaver som ville give mening - fx systemdrift (hardware og software), support, softwarevedligeholdelse o.lign."
Tomasz Otap, IT-Partner, Move On Career

"I dag er det ofte specialiserede virksomheder, der leverer konsulentydelser indenfor cybersikkerhed. Ydelserne ligger på et prisniveau, der ikke er muligt at være med på for mindre virksomheder. Uddannes der fremadrettet flere, der har kendskab til både den tekniske og forretningsmæssige del af cybersecurity, vil det forhåbentlig medføre, at det bliver mere "tilgængeligt" for mindre virksomheder at ansatte medarbejdere, der kan løfte opgaven."
Ann Christina Rindom Sørensen, Direktør, SafeJournal ApS

3.5 AFRUNDING

Fagområdet cybersikkerhed i dag minder om IT-faget for 30 år siden, hvor der var få, højt uddannede og dyre specialister og mange autodidakte med forskellige uddannelsesbaggrunde. Siden har erhvervsakademierne med succes uddannet mange IT-professionelle med en 2-2 1/2 -årig uddannelse.

Spørgeskemaundersøgelsen og interviews med aftagere har gjort det klart, at der er behov for en uddannelse, der uddanner profiler med hybride kompetencer, der kan tænke

cybersikkerhed ind i forretningen samtidig med at de mestrer et bredt felt af tekniske kompetencer. Den iterative udviklingsproces i tæt dialog med aftagere og interessenter har sikret, at uddannelsen vil være opdateret og møder aftagernes behov.

4. UDDANNELSENS INDHOLD

4.1 UDDANNELSENS FORMÅL OG ERHVERVSSIGTE

Formålet med professionsbachelor- og erhvervsakademiuddannelsen 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 og drift af it-systemer i såvel private som offentlige virksomheder.

4.2 UDDANNELSENS OVERORDNEDE MÅL FOR LÆRINGSUDBYTTE

Læringsmål for professionsbacheloruddannelsen i cybersikkerhed

Viden
Den uddannede har:

- udviklingsbaseret viden om erhvervets praksis og anvendt teori og metode inden for forebyggelse, identificering af og reaktion på cybersikkerhedstrusler i en kompleks organisatorisk sammenhæng
- udviklingsbaseret viden om erhvervets praksis og anvendt teori og metode inden for analyse af organisationskulturers påvirkning af cybersikkerhed samt designprincipper for strukturer, der fremmer cybersikkerhed
- forståelse for praksis og anvendt teori og metode inden for nationale og internationale sikkerhedsstandarder og kan reflektere over cybersikkerhedsprincipper

Færdigheder
Den uddannede kan:

- anvende metoder og redskaber inden for forebyggelse, identificering af og reaktion på cybersikkerhedstrusler og mestre analyse af mulige angreb
- anvende metoder og redskaber inden for nationale og internationale standarder til design og udvikling af cybersikkerhedssystemer, herunder mestre implementering af kryptografiske tiltag
- anvende metoder og redskaber inden for udvikling, drift og governance af IT-systemer og strukturer, der fremmer cybersikkerhed i en kompleks organisatorisk sammenhæng, herunder mestre automatisering af cybersikkerhedsopgaver
- vurdere praksisnære og teoretiske problemstillinger inden for cybersikkerhed samt begrunde og vælge relevante løsningsmodeller for cybersikkerhedstiltag i en kompleks organisatorisk sammenhæng
- formidle praksisnære og teoretiske problemstillinger og løsninger inden for cybersikkerhed til samarbejdspartnere, interessenter og brugere

Kompetencer
Den uddannede kan:

- håndtere komplekse og udviklingsorienterede situationer i forhold til udvikling, drift og governance af IT-systemer, der fremmer cybersikkerhed i en organisation, samt udvikling og implementering af foranstaltninger til at sikre kritisk data
- håndtere komplekse og udviklingsorienterede situationer i arbejds- eller studiesammenhænge i forhold til udvikling og implementering af compliance og sikkerhedskultur i en kompleks organisatorisk sammenhæng
- selvstændigt indgå i fagligt og tværfagligt samarbejde og påtage sig ansvar inden for rammerne af en professionel etik i forhold til at rådgive om samt udvikle og drifte cybersikkerhedsforanstaltninger
- identificere egne læringsbehov og udvikle egen viden, færdigheder og kompetencer i relation til cybersikkerhed, herunder nationale og internationale trusselsbilleder og sikkerhedsstandarder

Uddannelsen vil blive tilrettelagt med udgangspunkt i følgende 3 fagområder, som vægtes 1:1:1

1) Cybersikkerhedsledelse, governance og processer

Fagområdet indeholder centrale teorier og metoder til at forhindre, detektere og reagere over for trusler mod fortrolighed, integritet og tilgængelighed af systemer og applikationer. Fagområdet indeholder endvidere tilrettelæggelse af sikkerhedsarbejdet i organisationen samt grundlæggende principper og antagelser i cybersikkerhed herunder etiske, juridiske, politiske og ledelsesmæssige aspekter af cybersikkerhedsarbejdet.

2) Netværkssikkerhed og arkitektur

Fagområdet indeholder netværksarkitekturer, medier og protokoller, samt de enheder og andre foranstaltninger, der anvendes til at forhindre, detektere, og reagere over for trusler mod fortrolighed, integritet og tilgængelighed af netværkskommunikation.

3) Software-, datasikkerhed og automation

Fagområdet indeholder arbejde med sikkerhedsperspektivet i software, blandt andet programkvalitet og betydning af fejl- og datahåndtering for en software-arkitekturs sårbarheder. Der arbejdes med forskellige sikkerhedsdesignprincipper. Desuden indeholder fagområdet tiltag til kryptering og lagring, samt overvejelser i forbindelse med automatisering.

Læringsmål for erhvervsakademiuddannelsen i cybersikkerhed

Viden

Den uddannede har:

- viden om erhvervets praksis og central anvendt teori og metode inden for forebyggelse, identificering af og reaktion på cybersikkerhedstrusler, herunder governance og sikkerhedsprocedurer
- viden om erhvervets praksis og central anvendt teori og metode inden for organisationskultur og kommunikation samt designprincipper for strukturer, der fremmer cybersikkerhed
- forståelse for praksis og central anvendt teori og metode inden for cybersikkerhed samt forståelse for erhvervets anvendelse af teori og metode og de forskellige roller i en cybersikkerhedsorganisation

Færdigheder
Den uddannede kan:

- anvende centrale metoder og redskaber inden for forebyggelse, identificering af og reaktion på cybersikkerhedstrusler samt governance af cybersikkerhedsstrukturer, og anvende de færdigheder, der knytter sig til beskæftigelse inden for cybersikkerhed
- vurdere praksisnære problemstillinger inden for cybersikkerhed samt opstille og vælge løsningsmuligheder
- formidle praksisnære problemstillinger og løsningsmuligheder inden for cybersikkerhed til samarbejdspartnere og brugere

Kompetencer
Den uddannede kan:

- håndtere udviklingsorienterede situationer inden for opsætning og drift af IT-systemer og strukturer, der fremmer cybersikkerhed i en organisation, samt implementering af foranstaltninger til at sikre kritisk data
- deltage i fagligt og tværfagligt samarbejde i forbindelse med udvikling, drift og compliance inden for cybersikkerhed med en professionel tilgang
- i en struktureret sammenhæng tilegne sig ny viden, færdigheder og kompetencer inden for cybersikkerhed

Uddannelsen vil blive tilrettelagt med udgangspunkt i følgende 3 fagområder, som vægtes 1:1:1

1) Forretningsforståelse, governance og kommunikation

Fagområdet indeholder centrale teorier og metoder til at forhindre, detektere og reagere over for trusler mod fortrolighed, integritet og tilgængelighed i en organisation. Fagområdet indeholder endvidere tilrettelæggelse af sikkerhedsarbejdet i organisationen samt grundlæggende principper og antagelser i cybersikkerhed herunder etiske, juridiske, politiske og ledelsesmæssige aspekter af cybersikkerhedsarbejdet, samt metoder til at kommunikere dette på forskellige niveauer.

2) Netværkssikkerhed og arkitektur

Fagområdet indeholder grundlæggende netværksarkitekturer, medier og protokoller, samt faktorer som kan påvirke fortrolighed, integritet og tilgængelighed af netværkskommunikation. Desuden indeholder fagområdet grundlæggende arbejde med de tekniske komponenter som udgør de forskellige IT-systemer.

3) Software-, datasikkerhed og automation

Fagområdet indeholder arbejde med sikkerhedsperspektivet i datahåndtering, blandt andet fejlhåndtering og lagringsstrategier. Fagområdet beskæftiger sig også med basal scripting. Desuden indeholder fagområdet tiltag til kryptering, samt overvejelser i forbindelse med automatisering.

4.3 UDDANNELSENS INDHOLD OG TILRETTELÆGGELSE

Overordnet tilrettelæggelse

Professionsbacheloruddannelsen i cybersikkerhed
Uddannelsen er normeret til 210 ECTS-point, der omfatter:

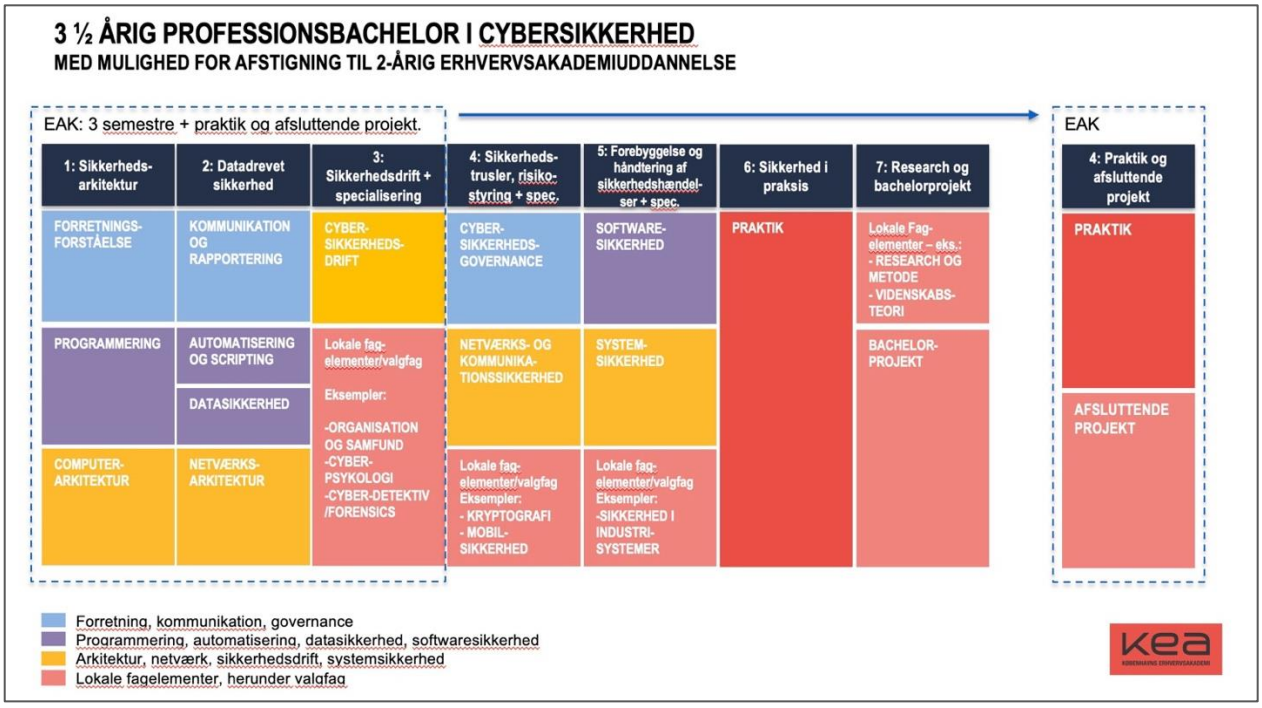
- uddannelseselementer med et samlet omfang på 160 ECTS-point, der udmønter uddannelsens faglige områder
- herunder 50 ECTS lokale uddannelseselementer, inklusive valgfag
- praktik med et samlet omfang på 30 ECTS-points.
- afsluttende bachelorprojekt på 20 ECTS-point.

Erhvervsakademiuddannelsen i cybersikkerhed
Uddannelsen er normeret til 120 ECTS-point, der omfatter:

- Uddannelseselementer med et samlet omfang på 90 ECTS-point, der udmønter uddannelsens faglige områder
- Herunder 20 ECTS lokale uddannelseselementer, inklusive valgfag
- praktik med et samlet omfang på 15 ECTS-points.
- afsluttende hovedopgave på 15 ECTS-point.

Figur 9 viser en oversigt over opbygningen af professionsbacheloruddannelsen med mulighed for afstigning på erhvervsakademiniveau.

Figur 9



Uddannelsens indhold

Uddannelsen indeholder følgende fagelementer på de tre første semestre, som vil være fælles for professionsbacheloruddannelsen og erhvervsakademiuddannelsen. De fælles fagelementer fremgår af tabel 3. Fagelementer der udelukkende ligger på professionsbacheloruddannelsen fremgår af tabel 4.

Tabel 3

Fagelementer 1.-3. semester	ECTS
Forretningsforståelse: Fagelementets formål er at kvalificere den studerende til at kunne forstå sammenhængen mellem forretning, informationsteknologi og cybersikkerhed. Den studerende får kompetencer til at arbejde med strategiske problemstillinger relateret til forskellige interessenters roller og ansvar i forhold til cybersikkerhed i en organisatorisk kontekst.	**10**
Programmering: Formålet med fagelementet er at sætte den studerende i stand til at løse konkrete problemstillinger inden for cybersikkerhed gennem udarbejdelsen af mindre scripts. Den studerende bliver i stand til på egen hånd at arbejde med algoritmer, opskrifter og programmering af computere.	**10**
Computerarkitektur og kommunikation Fagelementets formål er at kvalificere den studerende til at forstå og arbejde med computer- og cloud-arkitektur, inkl. hardware, software, styresystemer og cloud-modeller. Den studerende får kompetencer til at identificere og beskrive, hvor og hvordan sikkerhedssårbarheder kan opstå i denne arkitektur.	**10**
Kommunikation og rapportering Fagelementets formål er at kvalificere den studerende til at løse skriftlig og mundtlige kommunikationsopgaver inden for cybersikkerhed i en organisation. Den studerende får kompetencer til at udtrække, behandle og præsentere data fra sikkerhedsværktøjer til fagfolk og ikke-fagfolk, såvel internt som eksternt.	**10**
Automatisering og scripting Fagelementets formål er at kvalificere den studerende til at automatisere sikkerhedsopgaver ved anvendelse af scriptingsprog. Den studerende får kompetencer til at anvende biblioteker af funktioner og programmer i deres egne programmer med særligt fokus på at parse logs fra organisationens sikkerhedssystemer.	**5**
Datasikkerhed Fagelementets formål er at kvalificere den studerende til at anvende metoder til lokal og skybaseret datalagring samt anvende principper for sikkerhedsdesign. Den studerende får kompetencer til at sikre data gennem adgangskontrol og kryptering.	**5**
Netværksarkitektur Fagelementets formål er at kvalificere den studerende til at forstå netværksdesign og –strukturer i et sikkerhedsperspektiv. Den studerende får kompetencer til at planlægge og implementere effektive netværksløsninger.	**10**
IT-sikkerhedsdrift Fagelementets formål er at kvalificere den studerende til at forstå principper og praksis for IT-drift med fokus på sikkerhed. Den studerende får kompetencer til at implementere og vedligeholde sikkerhedsforanstaltninger, risikostyring, trusselsvurderinger og sikre kontinuerlig drift i en IT-infrastruktur.	**10**
Lokale fagelementer Der vil være et udbud af aktuelle lokale, herunder valgfrie, fagelementer på 20 ECTS. Eksempler på lokale fagelementer: organisation og samfund, cyber-psykologi, cyber-detektiv / forensics.	**20**

For erhvervsakademiuddannelsen i cybersikkerhed

For studerende, der ønsker at afslutte uddannelsen som en erhvervsakademiuddannelse, vil 4. semester indeholde praktik på 15 ECTS og en afsluttende opgave på 15 ECTS.

For professionsbacheloruddannelsen i cybersikkerhed

Professionsbacheloruddannelsen i cybersikkerhed indeholder følgende fagelementer på de resterende 4 semestre.

Tabel 4

Fagelementer 4.-7. semester	ECTS
Cybersikkerhedsgovernance Fagelementets formål er at kvalificere den studerende til at håndtere fundamentale opgaver som sikkerhedsansvarlig. Den studerende får kompetencer til at udføre risikoanalyse og inddrage relevant lovgivning i en organisations sikkerhedspolitikker og –praktikker.	10
Netværks- og kommunikationssikkerhed Fagelementets formål er at kvalificere den studerende til at identificere og håndtere sårbarheder i netværk. Den studerende får kompetencer til at overvåge netværkssikkerhedstrusler samt implementere og konfigurere udstyr til monitorering og mitigering af angreb.	10
Softwaresikkerhed Fagelementets formål er at kvalificere den studerende til at sikkerhedsvurdere software og softwarearkitektur. Den studerende får kompetencer til at opdage trusler mod software og forhindre sårbarheder i programkoder.	10
Systemsikkerhed Fagelementets formål er at kvalificere den studerende til at anvende sikkerhedsprincipper til systemsikkerhed og forensic processer. Den studerende får kompetencer til at udføre, udvælge, anvende og implementere praktiske tiltag til sikring af organisationens udstyr.	10
Resterende fagelementer Der vil være et udbud af aktuelle lokale, herunder valgfrie, fagelementer på 30 ECTS. Eksempler på lokale fagelementer: kryptografi, mobilsikkerhed, sikkerhed i industrisystemer, etisk hacking. 4.-7. semester indeholder et semester med praktik på 30 ECTS og et bachelorprojekt på 20 ECTS.	30

4.4 BESLÆGTEDE UDDANNELSER

I følgende afsnit sammenlignes den faglige profil på den ansøgte uddannelse med beslægtede uddannelser for at tydeliggøre forskellene til de eksisterende uddannelser. I tabel 5 fremgår de uddannelser, der er gennemgået i vores analyse af uddannelsesudbuddet.

Som det fremgår af oversigten, er der ingen af de eksisterende uddannelser, der har samme fagsammensætning og kompetenceprofil, og der er ingen uddannelser, der kan uddanne dimittender til at dække det praksis- og professionsrettede, samtidig med at dimittenderne får de tværfaglige kompetencer, der forener de forretningsmæssige og tekniske dele af cybersikkerhed.

Tabel 5

Uddannelse	Udbudssted	Beskrivelse
Erhvervsakademiuddannelser, 2-2 ½ år		
Datamatiker Erhvervsakademiuddannelse, 2½ år **Adgangskrav:** Matematik B Lokale adgangskrav: Engelsk B eller kundskaber svarende til Engelsk B	KEA, EAAA, Erhvervsakademi SydVest, Erhvervsakademi Dania, Erhvervsakademi MidtVest, Copenhagen Business	<u>Forskelle:</u> • Stort fokus på programmering • Mangler fagelementer inden for netværk ud over det grundlæggende • Har ikke fagelementet kommunikation og rapportering • Har ikke læringsmål i cybersikkerhed • Ingen toning i løbet af uddannelsen i sikkerhed og dimittender får intet mindset inden for cybersikkerhed

Studieplan: https://studieordninger.kea.dk/2024/31/196	Academy, Zealand, UCN, UCL	• Uddannelsen retter sig mod beskæftigelse som IT-udvikler – en meget anderledes profil end en cybersikkerhedmedarbejder
IT-teknolog Erhvervsakademiuddannelse, 2 år **Adgangskrav:** Matematik C Lokale adgangskrav: Engelsk B eller kundskaber svarende til Engelsk B **Studieplan:** https://studieordninger.kea.dk/2024/31/181	KEA, EAAA, Erhvervsakademi Dania, UCL, UCN	Forskelle: • IT-generalistuddannelse uden toning inden for cybersikkerhed • Stort fokus på netværk og hardware, • Mangler programmeringsfag udover det grundlæggende • Uddannelsen har ikke læringsmål i cybersikkerhed • Ingen toning i løbet af uddannelsen i sikkerhed og dimittender får intet mindset inden for cybersikkerhed • Har ikke fagelementet kommunikation og rapportering
Top-up uddannelser, Professionsbachelor 1 ½ år		
IT-sikkerhed Professionsbachelor (top-up), 1½ år **Studieplan:** https://studieordninger.kea.dk/2024/33/183	KEA, EAAA, Zealand, UCN, UCL	Forskelle: • Uddannelsen er en 1 ½-årig top-up, der bygger IT-sikkerhed over på EAK-uddannelser • Meget fokus på teknik og specialisering i IT-sikkerhed • Kort praktik på 10 uger – giver udfordringer med sikkerhedsgodkendelse hos nogle praktiksteder • Ingen fokus på forretningsforståelse
Softwareudvikling Professionsbachelor (top-up), 1½ år **Studieplan:** https://studieordninger.kea.dk/2024/33/192	KEA, Erhvervsakademi Aarhus, Copenhagen Business Academy, Erhvervsakademi Dania, Erhvervsakademi SydVest, UCN, UCL	Forskelle: • Uddannelsen er en 1 ½-årig top-up, der bygger specialisering i softwareudvikling oven på EAK-uddannelser • Fokus er på design og programmering store distribuerede datatunge systemer. • Har ikke læringsmål i cybersikkerhed
Bacheloruddannelser		
Cyberteknologi Bacheloruddannelse (civilingeniør)**Adgangskrav:** Matematik A Dansk A Engelsk B Fysik B / Geovidenskab A Kemi C / Bioteknologi A **Studieplan:** https://www.dtu.dk/uddannelse/bachelor/uddannelsesretninger/cyberteknologi	Danmarks Tekniske Universitet (Lyngby)	Forskelle: • Fokus på tekniske aspekter af cybersikkerhed, herunder netværkssikkerhed, softwareudvikling, og systemarkitektur. • Ingen praktisk og professionsrettet tilgang • Kombinerer ikke cybersikkerhed med forretning • Matematisk baseret • Sigter mod en kandidatuddannelse (Civ. Ing.) • Kræver Matematik A, Dansk A samt to STEM fag på A, B eller C niveau
Cyber- og computerteknologi Bacheloruddannelse (civilingeniør) **Adgangskrav:** Dansk A Engelsk B Matematik A med et gennemsnit på min. 4,0	Aalborg Universitet (København)	Forskelle: • Fokus på tekniske fag inden for netværkssikkerhed, programmering og systemudvikling • Enkelte fag inden for cybersikkerhed • Kombinerer ikke cybersikkerhed med forretning • Matematisk baseret • Sigter mod en kandidatuddannelse i Cybersecurity

Fysik B/ Geovidenskab A **Studieplan:** *https://www.aau.dk/uddannelser/bachelor/cyber-computerteknologi*		• Kræver Matematik A (min. 4,0 i gn.snit) Dansk A samt et STEM fag på A eller B niveau
Kandidatuddannelser		
Cybersecurity Kandidatuddannelse (civilingeniør) **Studieplan:** *https://www.aau.dk/uddannelser/kandidat/cyber-security*	Aalborg Universitet (Aalborg og København)	Forskelle: • Uddannelsen forudsætter en bachelor (ingeniør) • Uddannelse på kandidatniveau • Teoretisk og akademisk uddannelse • Mindre fokus på markedet • Mindre fokus på hands-on praktisk tilgang • Uddanner til specialist- eller ledelsesfunktion på højt niveau inden for cybersikkerhed • Kandidater vil være for specialiserede og omkostningstunge til det operationelle niveau • Rent engelsksproget uddannelse
Computer science and engineering (informationsteknologi) Kandidatuddannelse (civilingeniør) **Studieplan:** *https://www.dtu.dk/english/education/graduate/msc-programmes/computer-science-and-engineering*	Danmarks Tekniske Universitet (Lyngby)	Forskelle • Uddannelse på kandidatniveau som forudsætter en bachelor • Teoretisk og akademisk uddannelse • Ingen praktisk og professionsrettet tilgang • Bred uddannelse inden for datalogi og ingeniørvidenskab med enkelte kurser i cybersikkerhed • Kombinerer ikke cybersikkerhed med forretning • Rent engelsksproget uddannelse
Efter- og videreuddannelse		
IT-sikkerhed (Diplomuddannelse) **Studieplan:** *https://kompetence.kea.dk/uddannelser/it/diplom-i-it-sikkerhed*	KEA, Erhvervsakademi Aarhus, UCL, UCN	Forskelle: • Diplomuddannelse og dermed videreuddannelse • Bygger IT-sikkerhed oven på andre kompetencer • Fokus på teknik og specialisering i IT-sikkerhed • Ingen praktik • Svært at rekruttere til uddannelsen • Ingen fokus på forretningsforståelse • Kræver 2 års relevant erhvervsarbejde inden optagelse
Cybersikkerhed Master **Studieplan:** *Master of Cyber Security - programme specification (dtu.dk)*	Danmarks Tekniske Universitet (Lyngby)	• Masteruddannelse og dermed videreuddannelse • Uddanner til specialist- eller ledelsesfunktion på højt niveau inden for cybersikkerhed • Kræver 2 års relevant erhvervsarbejde og en bacheloruddannelse inden optagelse

Beskæftigelse og dimensionering

I undersøgelse af beskæftigelsesgrundlaget for den nye uddannelse er der fundet ledighedstal på følgende beslægtede uddannelser: erhvervsakademiuddannelserne til datamatiker og IT-teknolog samt professionsbacheloruddannelsen (top-up) i IT-sikkerhed. Data viser, at uddannelserne generelt har en relativ lav ledighed. Det viser samtidig, at ledigheden på KEAs udbud af uddannelserne generelt er lavere end på alle udbud samlet.

Ledighed på beslægtede uddannelser

Tabel 6

Ledighed 4.-7. kvartal, **IT-sikkerhed**, professionsbachelor (top-up)

IT-sikkerhed	2019		2020		2021	
	Alle	KEA	Alle	KEA	Alle	KEA
Ledighed	7,8 %	5,8 %	10,3 %	6,3 %	6,4 %	3,9 %
Fuldførte	54	27	55	32	59	32

Kilde: Danmarks Statistik

Om data: Gennemsnitlig ledighedsgrad 4.-7. kvartal efter fuldførelse for personer som fortsat har bopæl i Danmark. Fuldførte = fuldførte excl. udvandr.

Tabel 7

Ledighed 4.-7. kvartal, **datamatiker**, erhvervsakademiuddannelse

Datamatiker	2019		2020		2021	
	Alle	KEA	Alle	KEA	Alle	KEA
Ledighed	13,6 %	9,4 %	11,6 %	7,4 %	7,4 %	2,8 %
Fuldførte	509	84	583	102	567	86

Kilde: Danmarks Statistik

Om data: Gennemsnitlig ledighedsgrad 4.-7. kvartal efter fuldførelse for personer som fortsat har bopæl i Danmark. Fuldførte = fuldførte excl. udvandr.

Tabel 8

Ledighed 4.-7. kvartal, **IT-teknolog**, erhvervsakademiuddannelse

IT-teknolog	2019		2020		2021	
	Alle	KEA	Alle	KEA	Alle	KEA
Ledighed	9,5 %	4,1 %	9,0 %	5,3 %	7,4 %	5,4 %
Fuldførte	63	31	103	59	120	65

Kilde: Danmarks Statistik

Om data: Gennemsnitlig ledighedsgrad 4.-7. kvartal efter fuldførelse for personer som fortsat har bopæl i Danmark. Fuldførte = fuldførte excl. udvandr.

Dimensionering

Den nye uddannelse i cybersikkerhed er ift. aftagermarkedet nærmest beslægtet med professionsbacheloruddannelsen (top-up) i IT-sikkerhed. Professionsbacheloruddannelsen (top-up) i IT-sikkerhed er ikke dimensioneret.

De beslægtede uddannelser fra Danmarks Tekniske Universitet og Aalborg Universitet er ikke dimensionerede.

Erhvervsakademiuddannelserne til datamatiker og til IT-teknolog på KEA er dimensionerede til hhv. 280 og 108 pladser.

4.5 VIDEREUDDANNELSESMULIGHEDER

En dimittend fra professionsbacheloruddannelsen eller erhvervsakademiuddannelsen i cybersikkerhed vil kunne træde direkte ud på arbejdsmarkedet og varetage vigtige funktioner inden for cybersikkerhed. Hvis dimittenderne ønsker yderligere uddannelse senere, vil der være forskellige muligheder.

De erhvervsakademiuddannede i cybersikkerhed kan opnå en professionsbachelorgrad ved at tage de sidste to år af PBA-uddannelsen eller tage en diplomuddannelse i IT-sikkerhed eller andre IT-uddannelser på deltid.

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

4.6 REKRUTTERING TIL UDDANNELSEN

Rekrutteringsgrundlaget vil være de gymnasiale uddannelser og relevante erhvervsuddannelser f.eks. data- og kommunikationsuddannelsen.

En stor del af rekrutteringsgrundlaget findes hos de gymnasiale studenter fra Storkøbenhavn og Nordsjælland. I 2023 var der i Region Hovedstaden 14.956 studenter, der fuldførte deres gymnasieuddannelse[1]. Tal fra Børne- og Undervisningsministeriet viser, at der i de kommende år vil blive flere unge i København på trods af generelt faldende ungdomsårgange på landsplan. De fremskriver at antallet af unge på ungdomsuddannelserne i København og i Københavns omegn vil stige med ca. 3300 fra 2018-2030 (BUVM, 2020).

Uddannelsen forventes at differentiere 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 forventer KEA at kunne tiltrække et bredere udsnit af profiler end beslægtede uddannelser.
På IT-teknologuddannelsen (EA) har vi på KEA oplevet en kraftig stigning i søgningen og vi har i år optaget 160 studerende. Ca. 67% af de optagne ønsker at studere videre på PBA i IT-sikkerhed. Vi forventer, at en del af disse studerende fremover vil søge ind på PBA i cybersikkerhed.

5. INTERESSETILKENDEGIVELSER

84 ud af 118 respondenter i KEAs spørgeskemaundersøgelse støtter KEAs ansøgning om den nye professionsbacheloruddannelse i cybersikkerhed med afstigningsmulighed til en erhvervsakademiuddannelse efter 2 år. De resterende respondenter har ikke taget stilling – nogle af dem fordi det er firmapolitik ikke at støtte bestemte udbydere.

5.1 UDPLUK AF STØTTEERKLÆRINGER

”Center for Cybersikkerhed bifalder generelt udbredelsen af uddannelsestilbud, der styrker det samfundsmæssige fokus på og faglige kompetencer inden for cybersikkerhed. Københavns Erhvervsakademis uddannelsesforslag er et væsentligt bidrag hertil.”
Center for Cybersikkerhed

“DI Digital støtter på kraftigeste oprettelsen af en PBA i Cybersikkerhed og afstigningsmuligheden, behovet for cyberkompetencer på alle niveauer stiger voldsomt på grund af den øgede digitalisering og det ændrede trusselbillede.”
Jeppe Engell, Chefkonsulent, DI Digital

”Jeg vil gerne udtrykke min støtte til oprettelsen af Professionsbachelor i Cybersikkerhed. I vores virksomhed, og i branchen generelt, er der et stigende behov for specialister, der kan håndtere komplekse cybersikkerhedsudfordringer. En målrettet uddannelse inden for dette område vil være afgørende for at sikre, at vi har de nødvendige kompetencer til at beskytte vores digitale infrastruktur og data mod trusler. Det vil ikke kun styrke vores virksomhed, men også bidrage til branchens samlede robusthed og innovation.”
Alexandru Gheorghiasa, Senior IT Security Architect, Novo Nordisk

“Koblingen mellem virksomhedsforståelsen, governance og kommunikation er særlig vigtig og ofte noget, som der er mangel på. Vi har et stort behov for dygtige unge mennesker i Danmark indenfor Cyber området. Ikke mindst for at have kompetencerne i DK. Hos ISS f.eks. har vi langt de fleste cyber medarbejdere ansat i udlandet da der ikke er nok i DK og dem der er har enten ikke rette kompetencer eller er økonomisk ikke interessante da man nærmest kun kan finde folk med erfaring (der er alt for få ny-uddannede at tage fra).”
Martin Petersen, Chief Information Security Officer, ISS A/S

”Behovet for medarbejdere med god indsigt i it-sikkerhed stiger markant. Vi har brug for medarbejdere med forskellige kompetencer og uddannelseslængder, vi fleksibelt kan koble sammen på opgaver med interne kollegaer og eksterne specialister.”
Jesper Stæhr Mikkelsen, Kontorchef, Klimadatastyrelsen

”Der er et stigende behov for IT Specialister og i den grad også indenfor IT-Sikkerhed, jeg har oplevet flere gange at det kan være svært at hyre de rigtige medarbejdere. Så jo flere vi uddanner jo bedre, og hvis vi kan få endnu en erhvervs akademi uddannelse indenfor IT er det meget positivt da jeg har den opfattelse af at der er mange som vil kunne gøre sig en god karriere i IT branchen, men som har svært ved at gennemføre de mere boglige IT uddannelser på universiteterne.”
Sebastian Brøndum, Senior Cloud Engineer, Raw Power Games

”Vi forventer at kunne aftage praktikanter og dimittender fra både EAK- og PBA-uddannelsen. I Københavns Kommune støtter vi derfor varmt Københavns Erhvervsakademis uddannelses-forslag til en Professionsbachelor i Cybersikkerhed med mulighed for at stige af efter to år.”
Lisa Hartmann Jensen, Teamkoordinator Sikkerhed, Københavns Kommune

”HK Stat bakker fuldt ud op, omkring etableringen af en ny IT-sikkerheds uddannelse, med særligt fokus på cybersikkerhed. Kritisk infrastruktur, demokratiske institutioner og private virksomheder er i stigende grad truet af cyberangreb og senest i juni har CFCS advaret om et øget trusselsniveau mod det danske samfund. Behovet for at få etableret en uddannelse der er målrettet cybersikkerhedsområdet på PBA/KVU-niveau kan derfor ikke undervurderes. Det gælder både inden for Forsvaret, den offentlige forvaltning samt ude i de mange private virksomheder, som skal forebygge og håndtere de mange cyberangreb de oplever. Vi skal kunne rekruttere bredere til feltet og har brug for flere veje ind i faget. Derfor mener vi at denne nye uddannelse understøtter en vigtig samfundsinteresse.”
Heidi Juhl Pedersen, Sektorformand, HK Stat

6. KONKLUSION

Den stigende digitalisering af samfundet stiller større og større krav til virksomheder, organisationer og medarbejderens kompetencer inden for cybersikkerhed. Cybersikkerhed tænkes i stigende grad ind i alle dele af vores samfund, og det er nødvendigt med dygtige medarbejdere for at afværge cyberangreb og udtænke løsninger, som beskytter samfundet. De videregående uddannelser skal løbende tilpasse sig den aktuelle virkelighed, og her er cybersikkerhedsdagsordenen ingen undtagelse. KEA har kompetencerne og viljen til at bidrage til, at den danske sikkerhed og konkurrenceevne styrkes, ved at udbyde en ny professionsbacheloruddannelse indenfor cybersikkerhed.

På baggrund af behovsanalysen har vi dokumenteret behovet for en professionsbachelor i cybersikkerhed, med mulighed for afstigning på en erhvervsakademiuddannelse. 97% af respondenterne i KEAs undersøgelse svarer, at de forventer at det generelle behov for cybersikkerhedsmedarbejdere vil være stigende inden for de næste 5 år. KEAs samarbejdspartnere i erhvervslivet udtrykker et stort ønske og behov for den nye uddannelse i cybersikkerhed, for at imødekomme det voksende behov for cybersikkerhedskompetencer og 74% af aftagerne i KEAs undersøgelse angiver, at de vil være interesserede i at ansætte en eller flere dimittender fra den nye uddannelse.

Behovsanalysen viser, at der er et stort behov for at uddanne dimittender inden for cybersikkerhed. Ved at etablere en ny professionsbacheloruddannelse i cybersikkerhed med afstigningsmulighed på erhvervsakademiniveau får danske virksomheder adgang til medarbejdere med de nødvendige kompetencer, så de kan beskytte, fysisk og digital infrastruktur og afbøde følgerne af angreb, der er en konsekvens af et stigende trusselsniveau.

7. HØRINGSSVAR FRA ANDRE UDDANNELSESINSTITUTIONER

I forbindelse med ansøgningen har KEA foretaget en høring af relevante videregående uddannelsesinstitutioner. Det drejer sig om alle erhvervsakademier samt andre videregående uddannelsesinstitutioner, der er i samme geografiske område og har beslægtede uddannelser. Høringen skal bidrage til at sikre, at den nye uddannelse bidrager til et øget sammenhæng i uddannelsessystemet samt ikke medfører væsentlig forringelse af vilkårene for eksisterende uddannelser og udbud.

7.1 OPSUMMERING AF HØRINGSSVAR

Pointer fra høringssvarene er samlet i tabellen nedenfor. De originale høringssvar er indsat sidst i dokumentet. Følgende institutioner er ikke vendt tilbage på KEAs høringsbrev inden for ansøgningsfristen: Danmarks Tekniske Universitet, Professionshøjskolen UCN, Erhvervsakademi Sydvest, Erhvervsakademi Midtvest.

Institution	**Opsummering af høringssvar**

Aalborg Universitet	- De har søgt om at oprette en diplomingeniøruddannelse i cybersikkerhed i København
	- De to udbud kan sameksistere uden at forringe vilkårene for rekruttering
	  o da der er uudnyttet optagelsespotentiale for studerende inden for området
	  o da de to uddannelser vil have forskellige målgrupper
	- Der er så stor efterspørgsel på dimittender inden for området, at man selv med begge nye uddannelser ikke kan matche efterspørgslen

IT Universitetet	- Emnemæssigt overlap med ITU-uddannelserne: softwareudvikling og Computer Science. - Det vil måske være muligt for dimittender fra PBA at videreuddanne sig på ITUs kandidatuddannelse i Computer Science med specialisering i security. - Generelt er Hovedstadsområdet allerede grundigt dækket af it-uddannelser. Det væsentligste problem er, at de meget søgte it-uddannelser pga. udflytningsreform og kandidatreform ikke må optage flere af de studerende der søger de eksisterende uddannelser.
Zealand	- Støtter ansøgningen - Anerkender mulighed for afstigning til erhvervsakademiuddannelser - Betinger støtte af, at KEA påbegynder udfasning af top-up i IT-sikkerhed - Ønsker at KEA fremtidigt vil orientere dimittender fra datamatiker og IT-teknolog om muligheden for at tage en top-up i IT-sikkerhed på Zealand
IBA Kolding	- Støtter ansøgningen - Er interesseret i at udbyde uddannelsen
Erhvervsakademi Aarhus	- Uddannelsen er udarbejdet i tæt samarbejde med Erhvervsakademi Aarhus, der søger om uddannelsen i samme ansøgningsrunde. På baggrund heraf er der ikke vedlagt høringssvar.
Erhvervsakademi Dania	- Ingen indsigelser til ansøgningen
UCL erhvervsakademi og professionshøjskole	- Støtter ansøgningen - Ser frem til at etablere samarbejde om ansøgningen - Er interesseret i at udbyde uddannelsen [fremgår ikke direkte af svar, men fremgår af høringsbrev]
Cphbusiness	- Ingen indsigelser til ansøgningen

7.2 HØRINGSSVAR VEDLAGT

Aalborg Universitet

AALBORG UNIVERSITET

KEA Digital
Guldbergsgade 29 N
2220 København N

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

Aalborg Universitets høringssvar vedr. prækvalifikation af ny professionsbacheloruddannelse i cybersikkerhed.

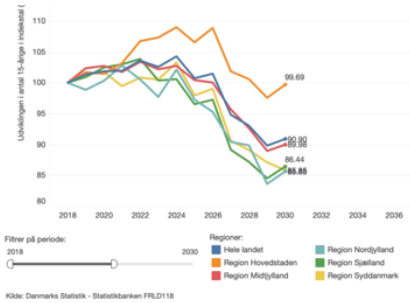
AAU har modtaget orientering om, at Københavns Erhvervsakademi (KEA) ansøger om at udbyde en ny professionsbachelor i cybersikkerhed. AAU er enige med KEA i behovet for flere dimittender indenfor IT – og cybersikkerhed i Danmark, hvorfor AAU ikke har indsigelser mod KEA's ønske om at oprette en professionsbacheloruddannelse i cybersikkerhed.

AAU søger i september 2024 - samtidigt med KEA – om at oprette en diplomingeniøruddannelse i cybersikkerhed. Dette gøres på baggrund af stor efterspørgsel fra branchen samt fra AAU's samarbejdspartnere. AAU lægger i sin ansøgning vægt på sin praksisnærhed, hvor de studerende vil indgå i tæt samarbejde med virksomheder og organisationer indenfor området, og i forlængelse heraf, ønsker AAU at oprette diplomingeniøruddannelsen på AAU's campus i København.

I forbindelse med AAU's afdækning af behovet for en ny diplomingeniøruddannelse i cybersikkerhed er det tydeligt, at der er 1) et uudnyttet og kvalificeret optagelsespotentiale, idet studerende i Københavnsområdet afvises fra deres 1. prioritetsansøgninger og 2) så stor en efterspørgsel på dimittender indenfor cybersikkerhedsområdet, at de eksisterende uddannelser og de to nye uddannelser samlet set ikke kan matche efterspørgslen.

Rekrutterings – og optagelsesgrundlag
AAU har i forbindelse med sin ansøgning om prækvalifikation af diplomingeniøruddannelsen i cybersikkerhed kortlagt rekrutterings – og optagelsespotentialet for at sikre, at AAU's udbud ikke forringer vilkårene for eksisterende uddannelser. På baggrund af data fra KOT for beslægtede uddannelser kan det udledes, at der i 2023 i alt var 264 studerende, som ikke blev optaget på deres 1. prioritet. Specielt på bachelor – og professionsbacheloruddannelserne i Københavnsområdet var der på DTU og ITU i alt 106 afviste 1. prioritetsansøgere. Sammenlignes det tal med antallet af afviste 1. prioritetsansøgere i 2022 (i alt 155, 85 fra universiteter og 70 fra erhvervsakademier), kan der ses en stigning i antallet af afvisninger på 70% på de beslægtede uddannelser.

I tillæg til ovenstående viser data fra Danmarks Statistik, at ungdomsårgangene bliver større i Region Hovedstaden modsat udviklingen i resten af Danmark. På nedenstående graf ses det, at antallet af 15-årige stiger flere år i Region Hovedstaden frem imod 2030 og dermed er det samlede antal potentielle studerende stigende.



Det er AAUs forventning, at de to uddannelser vil have forskellige målgrupper. De studerende, der søger om optagelse til AAUs diplomingeniøruddannelse, ønsker at blive ingeniører og har interesse for de ingeniørfaglige discipliner med høje krav til matematik og avancerede tekniske fag, mens de studerende, der søger om optagelse på KEA har interesse i de forretningsmæssige aspekter af cybersikkerhed (jf. KEAs høringsbrev til AAU).

På den baggrund vurderer AAU, at der er et uudnyttet og kvalificeret optagelsespotentiale til begge uddannelser i cybersikkerhed, og at de to udbud kan sameksistere uden at forrige vilkårene for rekrutteringen.

Efterspørgsel på kompetencer indenfor cybersikkerhed
I september 2022 beskrev en rapport fra regeringens sikkerhedspolitiske analysegruppe udfordringerne for dansk sikkerhed og forsvar frem mod 2035. Med udgangspunkt i denne advarede Dansk Industri (DI Digital) om, at Danmark i 2030 vil mangle 15-20.000 fagfolk inden for cyber- og informationssikkerhed.

I afdækningen af arbejdsmarkedets behovet for dimittender med kompetencer indenfor IT – og cybersikkerhed, har AAU desuden fået udarbejdet en behovsundersøgelse af rådgivningsvirksomheden Epinion. En af denne undersøgelses hovedkonklusioner er, at virksomhederne efterspørger både faglige og organisatoriske kompetencer blandt ingeniører inden for cybersikkerhed. 85 pct. af virksomhederne i undersøgelsen angiver, at de i nogen eller høj grad har et behov for ingeniører med kompetencer inden for cybersikkerhed i dag. De forventer desuden, at behovet vokser de kommende år - blandt andet som følge af et øget trusselsbillede og ny lovgivning på området. 69 pct. af virksomhederne forventer, at behovet for denne typer af ingeniører vil være større om tre år.

Selv med udbud af AAU's diplomingeniøruddannelse i cybersikkerhed og KEA's foreslåede uddannelse vil de danske uddannelser inden for området ikke kunne matche behovet for dimittender med kompetencer inden for cybersikkerhed. AAU's behovsundersøgelsen viser, at der i 2022 blev uddannet 183 bachelordimittender med en cybersikkerhedsprofil samt 62 professionsbachelorer (estimeret) med en top-up-uddannelse inden for cybersikkerhed, hvilket i alt giver 245 dimittender. Som beskrevet ovenfor estimerede Dansk Industri (DI Digital), at Danmark i 2030 vil mangle 15-20.000 fagfolk inden for cyber- og informationssikkerhed. AAU har yderligere undersøgt antallet af jobannoncer indenfor området. På Jobindex og Computerworld var der

AALBORG UNIVERSITET

i første halvår af 2023 1395 jobannoncer inden for it- og cybersikkerhed[1]. I tillæg hertil vurderes det i AAUs behovsundersøgelse, at omkring 48% af de deltagende it-virksomheder opgiver at besætte stillinger, idet der ikke er ansøgere til dem.

Behovet for flere dimittender inden for it-området kan kun dækkes ved at udvide det samlede bacheloroptag i Danmark. AAU's diplomingeniøruddannelsen vil være adgangsbegrænset til 30 studerende i 2025.

Det er derfor AAU's vurdering, at arbejdsmarkedets behov for dimittender med kompetencer inden for cybersikkerhed overstiger det forventede antal af dimittender fra hhv. eksisterende uddannelser og AAU's og KEA's nye professionsbacheloruddannelser i cybersikkerhed. Derfor vurderer AAU, at de to uddannelser kan sameksistere uden at forrige vilkårene for dimittenders beskæftigelse efter endt uddannelse.

AAU ser derfor frem til et fortsat godt samarbejde med KEA om uddannelserne indenfor cybersikkerhedsområdet.

Med venlig hilsen

Louise Møller Haase
Prodekan for uddannelse
Det Tekniske Fakultet for IT og Design
AAU

IT Universitetet

Fra: Lene Rehder <lenr@itu.dk>
Sendt: 6. september 2024 13:00
Til: Merete Hess <MHES@kea.dk>
Emne: FW: Høring ifm. KEAs nye uddannelse i cybersikkerhed

> Du får ikke ofte mails fra lenr@itu.dk. Få mere at vide om, hvorfor dette er vigtigt

Kære Merete,
Mange tak for den tilsendte høring vedr. den påtænkte uddannelse.
Vi beklager meget at vi ikke fik svaret på denne indenfor fristen.

ITU har følgende bemærkninger:

- Den påtænkte uddannelse har emnemæssigt noget overlap med IT-Universitetets uddannelser indenfor Softwareudvikling og Computer Science.
- Det vil måske være muligt for dimittender fra den påtænkte uddannelse at videreuddanne sig på ITUs kandidatuddannelse i Computer Science med specialisering i security.
- Generelt er Hovedstadsområdet allerede grundigt dækket af it-uddannelser. Det væsentligste problem er, at de meget søgte it-uddannelser pga. udflytningsreform og kandidatreform ikke må optage flere af de studerende der søger de eksisterende uddannelser.

God dag og god weekend.

Mange hilsner
Lene

Lene Rehder
Studiechef / Head of Student Affairs & Programmes

IT-Universitetet i København / IT UNIVERSITY OF COPENHAGEN
Rued Langgaards Vej 7
DK-2300 Copenhagen S
M: +45 5164 3718
E-mail: lenr@itu.dk
www.itu.dk
IT UNIVERSITY OF COPENHAGEN

IBA Kolding

Fra: Ole Højgaard Scheffmann Pedersen <OHP@iba.dk>
Sendt: 27. august 2024 11:45
Til: Merete Hess <MHES@kea.dk>
Emne: SV: Høring ifm. ny uddannelse i cybersikkerhed

Kære KEA

Mange tak for de tilsendte oplysninger. I lighed KEA ser IBA også et markant behov for kompetencer inden for cybersikkerhed og for at styrke Danmarks digitale sikkerhed. IBA finder det betimeligt, at det etableres en sammenhængende bacheloruddannelse, da området er særdeles vigtigt.

IBA er interesseret i at udbyde uddannelsen. Foruden det nationale behov ser IBA betydelige og specifikke regionale behov, fordi IBAs optageområde er hjemsted for helt centrale samfundskritiske aktiviteter som fx Energinet, Bankdata og cyberværnepligten.

Venlig hilsen
Ole Højgaard Scheffmann Pedersen
Lektor/ Senior Lecturer

Mail: OHP@iba.dk
Telefon: +4572118200
Direkte: +4572118241
Mobil: +4561939541

ERHVERVSAKADEMI KOLDING

Zealand

Høringssvar i forbindelse med prækvalifikation af ny professionsbacheloruddannelse i cybersikkerhed

28. august 2024
Side 1 i 1

Stine Rohde Frederiksen
T: 5076 2781
stfr@zealand.dk

Zealand
Lyngvej 21
4600 Køge

+4550762600
CVR: 31661471

København Erhvervsakademi (KEA) har orienteret Zealand om indsendelse af prækvalifikationsansøgning for ny PBA i cybersikkerhed.

Zealand støtter KEAs ansøgning om oprettelse af den nye uddannelse, og anerkender behovet for en afstigningsmulighed på AK-niveau med samtidig mulighed for at opnå en fuld PBA.

Zealand vil i dog i samme ombæring påpege, at både Zealand og KEA for nuværende udbyder top-up i IT-sikkerhed, der er en overbygning til AK it-teknolog og AK datamatiker. Den nye uddannelse antages at have et lignende indhold, som den eksisterende top-up, og Zealand vil derfor betinge nærværende støtte til oprettelsen mod, at KEA vil påbegynde udfasning af top-up i IT-sikkerhed, ligesom Zealand også håber, at KEA også fremadrettet vil orientere dimittender fra de to AK-uddannelser om muligheden for at tage en top-up i IT-sikkerhed på Zealand.

Venlig hilsen

Rasmus Frimodt
Rektor

Erhvervsakademi Dania

Kære Merete

Erhvervsakademi Dania takker for at have fået jeres prækvalifikation af en ny professionsbacheloruddannelse i cybersikkerhed i høring.

Vi har ingen indsigelser til jeres ansøgning om prækvalifikation.

Venlig hilsen / Kind regards

Suzanne Anthony

Kvalitetschef
Director of Quality

ERHVERVSAKADEMI

Minervavej 63, DK-8960 Randers SØ
Tel. +45 72291006 / +45 24445829
Mail: sua@eadania.dk - eaDania.dk

UCL

Erhvervsakademi og Professionshøjskole

KEA DIGITAL
Guldbergsgade 29 N
2200 København N

Att. Uddannelseschef Merete Hess

Høringssvar vedr. prækvalifikation af professionsbacheloruddannelse i cybersikkerhed

Dato
29. august 2024

Reference
JMP

UCL Erhvervsakademi og Professionshøjskole takker for muligheden for at blive hørt i forbindelse med KEA DIGTALs prækvalifikation af en professionsbacheloruddannelse i cybersikkerhed.

UCL Erhvervsakademi og Professionshøjskole ser et nødvendigt skærpet fokus på samfundssikkerhed, en stigende efterspørgsel for kompetencer indenfor cybersikkerhed i erhvervslivet, og derfor også en stor relevans af en professionsbacheloruddannelse i cybersikkerhed. UCL Erhvervsakademi og Professionshøjskole er derfor positiv overfor ansøgningen af den nye uddannelse.

UCL Erhvervsakademi og Professionshøjskole ønsker KEA DIGITAL held og lykke med ansøgningen af professionsbacheloruddannelsen i cybersikkerhed og ser frem til også at etablere et stærkt samarbejde omkring den nye uddannelse.

Venlig hilsen

Jens Mejer Pedersen
Rektor

jmp@ucl.dk
3062 12 40

Cphbusiness

Kære Merete

Mange tak for høringsbrev om ny uddannelse i cybersikkerhed.

Vi har ingen indsigelser.

Med venlig hilsen

Dorte Schmidt
Kvalitets- og analysechef

Cphbusiness

Cphbusiness Søerne

Nansensgade 19
DK-1366 København K
www.cphbusiness.dk
Tlf.: +45 3615 4500
Dir.: +45 3615 4645
E-mail: dsc@cphbusiness.dk

Uddannelses- og Forskningsministeriet

Kære Steen Enemark Kildesgaard

3. december 2024

Uddannelses- og Forskningsministeriet

Bredgade 40-42
1260 København K

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

CVR-nr. 1680 5408

Ref.-nr.
2024 - 52814

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

Godkendelse af ny professionsbacheloruddannelse i cybersikkerhed (København)

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

Da Københavns Erhvervsakademi er positivt institutionsakkrediteret, gives godkendelsen til umiddelbar oprettelse af uddannelsen.

Uddannelsen vil blive indarbejdet i den relevante bekendtgørelse.

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

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

Med venlig hilsen

Christina Egelund

Bilag: 1 – RUVU's vurdering af ansøgningen

2 – Følgebrev fra Uddannelses- og Forskningsstyrelsen med uddannelsens grundoplysninger

Bilag 1 – RUVU's vurdering af ansøgningen

Nr. A13– ny uddannelse (Efterår 2024)			**Status på ansøgningen:** Godkendt	
Ansøger og udbudssted:	Københavns Erhvervsakademi (København)			
Uddannelsestype:	Professionsbacheloruddannelse			
Uddannelsens navn (fagbetegnelse) på hhv. dansk/engelsk:	Professionsbacheloruddannelse: - Cybersikkerhed - Cyber Security Erhvervsakademiuddannelse: - Operationel cybersikkerhed AK - Operational Cyber Security AP			
Titel, som uddannelsen giver ret til at anvende:	Professionsbacheloruddannelse: - Professionsbachelor i cybersikkerhed - Bachelor of Cyber Security Erhvervsakademiuddannelse (afstigningsmulighed): - Operationel cybersikkerhed AK - Operational Cyber Security AP			
Hovedområde:	Tekniske område		**Genansøgning:**	Nej
Sprog:	Dansk	**Antal ECTS:**	210 ECTS / 120 ECTS	
Link til ansøgning på pkf.ufm.dk:	https://pkf.ufm.dk/flows/aadb35d3332d543ee03886588160c2ed			
RUVU's vurdering på møde d. 1. november 2024	RUVU vurderer, at ansøgningen opfylder kriterierne som fastsat i bilag 4 i bekendtgørelse om akkreditering af videregående uddannelsesinstitutioner og godkendelse af videregående uddannelser (nr. 1558 af 2. juli 2021 med senere ændringer). RUVU lægger vægt på, at ansøgningen dokumenterer, at udbud af såvel erhvervsakademi- som professionsbacheloruddannelsen, både lokalt og nationalt, vil imødekomme behovet for flere dimittender inden for cybersikkerhed. Herunder vil ansøgningerne om uddannelserne i Storkøbenhavn bidrage til antallet af personer med såvel tekniske som forretningsmæssige kompetencer inden for cybersikkerhed i Østdanmark. RUVU finder det desuden positivt, at uddannelsens opbygning indebærer en afstigningsmulighed, der gør det muligt for den studerende at afslutte uddannelsen efter 2 år og opnå en			

	erhvervsakademiuddannelse i operationel cybersikkerhed. RUVU har desuden noteret sig, at institutionen påtænker at lukke en beslægtet uddannelse.

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

Professionsbachelor i cybersikkerhed
Bachelor of Cyber Security

Hovedområde:
Tekniske område

Titel:
Professionsbacheloruddannelse:
Efter reglerne i § 7, stk. 2, i bekendtgørelse nr. 495 af 22. maj 2024 om tekniske og merkantile erhvervsakademiuddannelser og professionsbacheloruddannelser med senere ændring (teknisk LEP-bekendtgørelse), giver uddannelsen ret til at anvende titlen:

- **Dansk:** Professionsbachelor i cybersikkerhed
- **Engelsk:** Bachelor of Cyber Security

Erhvervsakademiuddannelse (afstigningsmulighed):
Efter reglerne i § 7, stk. 1 i lovbekendtgørelse nr. 396 af 12. april 2024 om erhvervsakademiuddannelser og professionsbacheloruddannelser, kan professionsbacheloruddannelsen tilrettelægges således, at uddannelsens første til andet år sammen med et særligt tilrettelagt afsluttende forløb udgør en selvstændigt afrundet erhvervsakademiuddannelse, jf. § 4.

Efter reglerne i § 7, stk. 1, i bekendtgørelse nr. 495 af 22. maj 2024 om tekniske og merkantile erhvervsakademiuddannelser og professionsbacheloruddannelser med senere ændring (teknisk LEP-bekendtgørelse), giver uddannelsen ret til at anvende titlen:

- **Dansk:** Operationel cybersikkerhed AK
- **Engelsk:** Operational Cyber Security AP

Udbudssted:
København.

Sprog:
Dansk

Normeret studietid:
Professionsbachelor:
Efter reglerne i den tekniske LEP-bekendtgørelses § 15, stk. 1, fastlægges uddannelsens normering til 210 ECTS-point.

Erhvervsakademiuddannelse:
Efter reglerne i den tekniske LEP-bekendtgørelses § 14, stk. 1, fastlægges uddannelsens normering til 120 ECTS-point.

Takstindplacering:
Uddannelsen indplaceres til: Takstgruppe 7

Professionsbachelor:
Aktivitetsgruppekode: 4050

Erhvervsakademiuddannelse:
Aktivitetsgruppekode: 4054

Koder Danmarks Statistik:
Professionsbachelor:
UDD: 5896
AUDD: 5896

Erhvervsakademiuddannelse:
AUDD: 5910

Censorkorps
Ministeriet har noteret sig, at uddannelsen tilknyttes Censorkorpset for IT- og softwareudvikling.

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

Adgang via gymnasial eksamen
Specifikke adgangskrav: Matematik B og engelsk B

Adgang via 3-årig erhvervsuddannelse
Specifikke adgangskrav: Matematik B og engelsk B

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