Deloitte.

Analyse af markedet for cyber- og informationssikkerhed

Hovedrapport

Marts 2023

Indhold

1. Om analysen

Cyber- og informationssikkerhed er en strategisk satsning for Aarhus Kommune, der gennem etablering af et Security Tech Space vil udbygge en styrkeposition i Aarhus og Østjylland.

Deloitte har i perioden januar-februar 2023 gennemført en analyse af markedet for cyber- og informationssikkerhed i Aarhus og Østjylland, herunder en vurdering af markedspotentialerne og betydningen af et Security Tech Space, et tæt og systematisk samarbejde mellem offentlige og private aktører samt uddannelses- og forskningsinstitutioner, for realiseringen heraf.

Arbejdshypoteserne er, 1) at cyber- og informationssikkerhed er forbundet med væsentlige erhvervsmæssige potentialer, og 2) at Aarhus og Østjylland har en styrkeposition inden for cyber- og informationssikkerhed og gennem innovation, erhvervsudvikling og samarbejde kan spille en central rolle i indfrielse af de nationale såvel som europæiske målsætninger på området. Et Security Tech Space skal i den forbindelse udgøre et fyrtårn i den samlede indsats.

Denne rapport sammenfatter de centrale resultater, konklusioner og anbefalinger af dataindsamlings- og analyseaktiviteterne, der er gennemført som led i analysen.

1.1. Formål

Formålet med analysen er for det første at dokumentere og beskrive markedspotentialerne samt Aarhus og Østjyllands styrkeposition inden for cyber- og informationssikkerhed. For det andet at beskrive, hvordan etablering af et Security Tech Space kan bidrage til realisering af potentialerne til gavn for erhvervsudvikling og vækst lokalt samt en styrket cyber- og informationssikkerhed nationalt.

Dermed udgør analysen en væsentlig del af det vidensgrundlag, der skal danne udgangspunkt for centrale beslutninger og prioriteringer i Aarhus Kommune vedrørende kommunens strategiske målsætninger inden for cyber- og informationssikkerhed.

1.2. Data og metode

Den samlede analyse kombinerer kvalitative og kvantitative datakilder og analysemetoder. Udgangspunktet er et dokumentstudie af relevant viden fra lovtekster, strategi- og visionspapirer, fagbøger, analyser og artikler. Derudover har vi gennemført en markedsanalyse baseret på beskrivende statistik af registerdata fra Danmarks Statistik om markedet for it-branchen[1]. Et opmærksomhedspunkt er i den forbindelse, at it-branchen beskæftiger sig med andet end cyber- og informationssikkerhed, hvorfor de beskrevne nøgletal også dækker over andre brancheområder med en bredere afgrænsning. Omvendt vil der også være beskæftigelse og omsætning i andre brancher, fx rådgivningsbranchen, som skyldes efterspørgsel efter produkter og ydelser inden for cyber- og informationssikkerhed. Endeligt er der gennemført semi-strukturerede, virtuelle interviews med

[1] Det er virksomheden eStatistik, der har stået for dataindsamling og -behandling, hvorfor Deloitte ikke har været involveret i beslutninger om populationer, variabeludvælgelse, afgrænsning og periodisering.

repræsentanter fra Konsortiet for Cyber- og Informationssikkerhed samt styregruppen i Aarhus Kommune.

1.3. Analysens centrale fund

Med afsæt i disse datakilder og metoder har analysen resulteret i otte centrale fund:

#1 Lovgivning og regulering vil drive en markant efterspørgsel – og dermed udfoldelsen af et markant erhvervspotentiale med store internationale ambitioner

Ny lovgivning og regulering vil få danske virksomheder til at efterspørge ydelser og kompetencer inden for cyber- og informationssikkerhed. I de kommende år vil et stadigt større antal direktiver og forordninger blive forhandlet og vedtaget i EU. Senest i rækken er det netop vedtagne NIS2-direktiv. NIS2-direktivet stiller skærpede krav til sikkerhedsniveauet hos de offentlige og private enheder, der leverer samfundskritiske ydelser, herunder fx forsyningsvirksomheder, den finansielle sektor samt virksomheder på sundheds- og transportområdet.

Ifølge Industriens Fond og Dansk Industris nylige vurdering forventes det at omkring 1.079 virksomheder i Danmark vil være direkte omfattet af NIS2-direktivet hvoraf ca. 230 befinder sig i region Midtjylland. Ifølge EU Kommissionen vil direktivet medføre øgede investeringer i cybersikkerhed hos virksomhederne i målgruppen på mellem 20 og 30 pct. i forhold til det nuværende niveau. Analysevirksomheden IDC skønner, at dette svarer til en samlet investering på ca. 448 mio. kr. i hele landet.

Efterspørgslen fra virksomhederne vil dog forventeligt være større. Først og fremmest er cyber- og informationssikkerhed i stigende grad blevet en prioritet i direktioner og bestyrelser. Det viser blandt andet Deloittes Cyber Survey 2023. Samtidig har krigen i Ukraine, hvor cyberangreb bruges sideløbende med konventionel krigsførelse, aktualiseret behovet for at styrke modstandsdygtigheden hos virksomheder verden over, herunder ikke mindst i den vestlige verden og Europa. Dernæst er det vigtigt at sige, at NIS2-direktivet kun er en del af den lovgivning på området, der vil ramme virksomhederne i de kommende år. Eksempelvis er krav til virksomhedernes it-sikkerhed også en del af regulering inden for Environment, Social Governance (ESG). Effekten af NIS2 i de virksomheder, der er direkte omfattet af direktivets krav, vil desuden have afledte effekter for virksomheder i de omfattede virksomheders værdikæder.

#2 It-branchen i Aarhus er i kraftig vækst og konkurrencedygtig

I perioden 2016-2021 har Aarhus oplevet en større vækst i it-branchen end Aalborg, Odense og København. Fra 2016 til 2021 har Aarhus eksempelvis haft en vækst i beskæftigelsen, der er 57% højere end København. I samme periode er væksten i omsætningen 55% højere i Aarhus end i København. Sammenligningen er alene baseret på virksomheder med hovedsæder i de respektive byer. Dette tyder på, at Aarhus har udviklet sig markant inden for it og teknologiske produkter og tjenester i de seneste år og har stærke kompetencer på området. Forklaringerne på dette skal ifølge flere informanter findes i en mere dynamisk og innovativ it-klynge i Aarhus og byens tætte samarbejde mellem virksomheder, uddannelsesinstitutioner og offentlige institutioner. Institut for Datalogi på Aarhus Universitet er placeret i top tre indenfor kryptologi på verdensplan. Alexandra Instituttet rådgiver virksomheder i hele landet om it-sikkerhed, ligesom Flere virksomheder er sprunget ud af det aarhusianske universitetsmiljø[2].

Markedet for it-ydelser er dog stadig større i København end i Aarhus, der som sådan ikke er markedsledende på området. Men her er det relevant at fremhæve, at den

[2] Herunder blandt andet Crypthomatic, Alexandra Instituttet, Partisia og Sepior

gennemsnitlige ansatte i it-branchen i Aarhus skaber mere værdi end den gennemsnitlige ansatte i København. Således er værditilvæksten pr. årsværk i Aarhus 1 million kroner, mens den i København er 125.000 kr. om året.

Ovenstående bidrager til et samlet billede af konkurrencedygtige aarhusianske og østjyske it-virksomheder, som også er interessante i et investorperspektiv. Kombineret med tilstedeværelsen af Aarhus Universitet og investorernes oplevelse af relativt mindre konkurrence om it-talenterne giver de værdiskabende aarhusianske it-virksomheder byen en komparativ fordel i forhold til København, når der skal rejses kapital.

#3 Aarhus Universitet er et vigtigt aktiv for den østjyske styrkeposition inden for cyber- og informationssikkerhed

Virksomheder på både udbuds- og efterspørgselssiden forventer at skulle investere i ydelser og talentmasse for at følge med udviklingen og den stigende kompleksitet, hvor hackere og cyberkriminelle også bliver mere sofistikerede i deres metoder og fremgangsmåder. I den forbindelse spiller særligt universiteterne en vigtig rolle, som leverandører af talent til virksomhederne. Flere af de virksomheder, som Deloitte har interviewet, og som udbyder produkter og service inden for cyber- og informationssikkerhed, fremhæver således eksplicit Aarhus Universitets positive betydning for deres forretningsmæssige muligheder. Universitetets beliggenhed er således afgørende for, at de har adgang til kvalificeret arbejdskraft.

Samtidig vidner tal fra Computer Science Rankings om, at Aarhus Universitet også har en relativ styrkeposition på området i sammenligningen med andre universiteter. Målt på publikationer er Aarhus Universitet nr. 1 i Danmark med mere end 10 gange så mange publikationspoint (38,4) som nr. 2, DTU (2,7). Aalborg Universitet er ikke med. Aarhus Universitets point betyder også, at institutionen – målt på publikationer og dermed forskning på området – er blandt de højest placerede i verden.

Endeligt er et velrenommeret universitet også et aktiv i forhold til tiltrækning af investeringer til området. Fra investorernes perspektiv understøtter universitetets beliggenhed mulighederne for rekruttering af talent, som i disse år er en af de mest kritiske faktorer for realisering af de markedsmæssige potentialer. Samtidig bidrager universitetet til et innovativt miljø.

#4 Økosystemet til at videreudvikle og innovere den østjyske styrkeposition er på plads

Netop forskning og innovation er afgørende, hvis cyber- og informationssikkerheden skal styrkes og generere vækst og erhvervsudvikling i området. I den forbindelse er et tæt samspil mellem forskningsverdenen samt private og offentlige virksomheder vigtigt. Aarhus Kommune har med nedsættelsen af et Konsortium for Cyber- og Informationssikkerhed taget de første skridt til mere formaliserede rammer for samarbejde om cyber- og informationssikkerhedsagendaen. Konsortiet tæller repræsentanter fra hele økosystemet af private virksomheder, beredskab, interesseorganisationer, væksthuse mv. Kombineret med en partnerskabskultur karakteriseret som samarbejdsvillig og hjælpsom, og hvor lokale aktører kender hinanden, vurderer flere informanter, at konsortiet og et mere forpligtende samarbejde i regi af et Security Tech Space har gode forudsætninger for at blive en succes.

#5 Et forpligtende samarbejde med klare mål og kommunal involvering er en forudsætning for succes

Repræsentanter fra Konsortiet for Cyber- og Informationssikkerhed ser et triple helix inspireret samarbejde, der yderligere kan materialisere sig i et Security Tech Space, som et vigtigt fundament for realisering af det forretningsmæssige potentiale for

virksomhederne selv som for den østjyske styrkeposition inden for cyber- og informationssikkerhed samlet set. Årsagen er, ifølge flere informanter, at cyber- og informationssikkerhed kræver tværfaglige kompetencer, der skal kombineres på tværs, og at teori skal kombineres med praksis. Dette kan et formaliseret samarbejde omkring et Security Tech Space understøtte, og som sådan anses et Security Tech Space som et vigtigt initiativ, hvis ambitionerne på cyber- og informationssikkerhedsområdet i Aarhus og Østjylland skal indfries. Et vigtigt initiativ hvor Aarhus Kommune skal stå i spidsen som facilitator og katalysator for et tæt og forpligtende samarbejde på tværs af aktørerne.

Et gennemgående budskab fra informanterne er samtidig, at succesen af både samarbejdet i konsortiet og om et Security Tech Space afhænger af, at der opstilles klare mål og initiativer for samarbejdet, og at dette skal have en forpligtende karakter. Samtidig fremhæver flere informanter Aarhus Kommunes og borgmesterens engagement og investeringsvillighed i samarbejdet som motivation for dem selv til at gå ind i samarbejdet og som en afgørende faktor for målopfyldelsen heraf. Kommunens involvering legitimerer samarbejdet og giver det en forpligtende karakter.

#6 Et selvstændigt Security Tech Space som katalysator for handling

Arbejdet med etablering af et Security Tech Space er allerede begyndt, og Aarhus Kommune har konkrete idéer til projekter, der kan forankres i et Security Tech Space. Nærværende analyse har som supplement hertil taget afsæt i de markedsmæssige potentialer for cyber- og informationssikkerhed i Danmark og afdækket, hvordan et tæt og forpligtende samarbejde mellem forskellige aktører i regi af et Security Tech Space kan bidrage til erhvervsudvikling og vækst samt et generelt øget cyber- og informationssikkerhedsniveau i samfundet. En central konklusion er, at viljen til samarbejde om agendaen er til stede, men at der er behov for en instans, der tager styring og driver udviklingen. Ellers er der en risiko for, at den eksisterende styrkeposition udvandes i konkurrencen om talent og markedets stigende efterspørgsel. Denne instans kan være et Security Tech Space, der med finansiering og et bredt mandat fra hele økosystemet i ryggen kan være katalysator for handling. Dette forudsætter, at et Security Tech Space opererer som en selvstændig enhed. På baggrund af analysen anbefaler vi et murstensløst Security Tech Space med huse i tilknytning til et forsknings- og/eller innovationsmiljø og en direktør og en bestyrelse med repræsentanter fra det brede interessentlandskab i spidsen. Et Security Tech Space kan være fondsfinansieret med midler fra de vigtigste interessenter i økosystemet, herunder kommunen. De juridiske og finansielle rammer forbundet med realiseringen af et Security Tech Space skal dog afdækkes yderligere. Dog vil initiativet kræve finansiering, da de indtægtsgenererende aktiviteter vil være begrænsede.

#7 Et Security Tech Space skal fokusere på tre konkrete behov forbundet med realisering af markedspotentialerne

Analysen afdækker tre overordnede og delvist forbundne indsatsområder for et Security Tech Space. For det første skal et Security Tech Space indeholde et innovationslaboratorium på tværs af aktører i det samlede økosystem med det formål at udvikle bæredygtige løsninger og forretningsmodeller, der modsvarer behov og efterspørgslen i markedet. Heri ligger også initiativ til accelerator-programmer og lignende initiativer, der skal hjælpe blandt andet startups med at få udviklet og markedsført deres produkter og services.

For det andet skal et Security Tech Space understøtte markedsmatching på flere måder og med flere formål. Et formål er at gøre innovationsprocessen fra ide til marked så hurtig og effektiv som mulig. Dette kan ske ved at agere bindeled mellem særligt forskere, startups, mikrovirksomheder, investorer og samarbejdspartnere, der

kan hjælpe med at realisere markedspotentialerne gennem kapital, kommerciel strategi og vækst. Et andet formål er at understøtte, at udbud af og efterspørgsel efter kompetencer inden for cyber- og informationssikkerhed møder hinanden, og at der sker vidensoverførsel mellem særligt universitetsverdenen og erhvervslivet. I dette tilfælde er der tale om markedsmatching mellem studerende og virksomheder.

For det tredje skal et Security Tech Space være et videns- og rådgivningscenter. Særligt i forhold til rådgivning af virksomheder om forhold relateret til cyber- og informationssikkerhed, døgnet rundt – alle ugens dage. Inden for dette indsatsområde ligger også træningsaktiviteter og informationsmøder, ligesom Konsortiet for Cyber- og Informationssikkerhed i regi heraf kan bidrage med fakta og viden i debatten og de politiske beslutningsprocesser på området.

#8 Aarhus og Østjylland skal etablere en kernefortælling med afsæt i regionens komparative styrker inden for cyber- og informationssikkerhed
Skal Aarhus og Østjylland differentiere sig i forhold til andre vækstregioner i Danmark og supplere allerede igangværende initiativer for dermed at realisere visionen og de markedsmæssige potentialer i relation hertil, skal indsatsen fokuserer på de områder, hvor Aarhus og Østjylland har de relativt største markedsfordele og/eller der er et udækket markedsbehov. Særligt tre kerneelementer skal fremhæves. 1) Adgangen til talent. Tilstedeværelsen af udbuddet af arbejdskraft i Aarhus opleves som relativt større og mere tilgængeligt af investorer og virksomheder end eksempelvis i København. 2) De forsknings- og markedsmæssige resultater inden for kryptologi og andre sikkerhedsteknologier som blockchain giver Aarhus en komparativ fordel og solid erfaringsbase at bygge videre på. 3) Manglende viden, kompetencer og ressourcer i det store danske erhvervslandskab af små og mellemstore virksomheder udgør en stor trussel mod den generelle cyber- og informationssikkerhed i samfundet, men også et udækket behov, som Aarhus og Østjylland kan bidrage til at opfylde.

I de følgende kapitler beskriver og begrunder vi de centrale fund.

1.4. Rapportens struktur

Rapporten er struktureret i seks hovedkapitler, inklusive dette indledende kapitel. **Kapitel 2** definerer den konceptuelle ramme for analysen gennem en beskrivelse af, hvordan markedet for cyber- og informationssikkerhed er karakteriseret ved produkter og tjenesteydelser målrettet flere forskellige behov samt mennesker processer og teknologi. I forlængelse heraf beskriver **kapitel 3** NIS2-direktivet med fokus på, hvordan dette direktiv såvel som anden lovgivning påvirker efterspørgslen og dermed markedspotentialerne for produkter og serviceydelser inden for cyber- og informationssikkerhed nu og i fremtiden. **Kapitel 4** indeholder resultaterne af den registerdatabaserede markedsanalyse af virksomheder, ansatte og økonomiske nøgletal i it-branchen. Dernæst præsenterer **kapitel 5** resultaterne af en analyse af det strategiske udgangspunkt for markedet for cyber- og informationssikkerhed i Aarhus og Østjylland. Vi afslutter rapporten i **kapitel 6**, hvor vi beskriver hvordan etablering af et Security Tech Space kan understøtte realiseringen af de markedsmæssige potentialer inden for cyber- og informationssikkerhed med fokus på interessenter, indsatsområder og organisering.

Resultater fra analysen har dannet afsæt for udarbejdelsen af en kernefortælling om den aarhusianske og østjyske styrkeposition inden for cyber- og informationssikkerhed. Denne fortælling er kommunikeret i en særskilt PowerPoint præsentation.

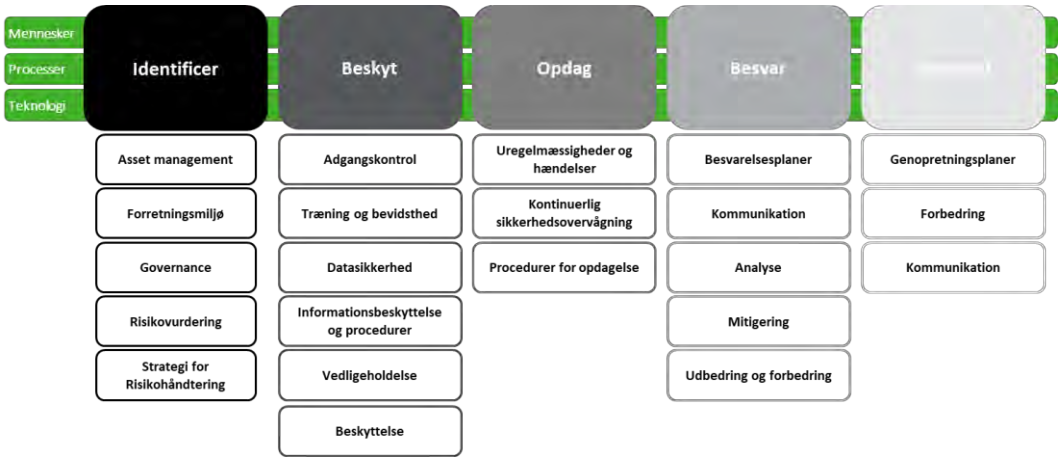
2. Den konceptuelle ramme

Markedet for produkter og ydelser, der skal øge cyber- og informationssikkerheden i samfundet, favner bredt. Det handler om teknologi, men i lige så høj grad om kompetencer, mennesker og processer – og ikke kun processer for at beskytte sig, men også for at reagere, når skaden er sket.

Vores analyse tager afsæt i en grundlæggende forståelsesramme for cyber- og informationssikkerhed, som markedet og potentialerne beskrives i forhold til.

En ofte brugt forståelsesramme er NIST CSF som er delt op i fem fundamentale områder. Dette giver en helhedsorienteret tilgang til cybersikkerhed, der kan hjælpe organisationer med at forstå, hvordan de bedst kan beskytte deres kritiske aktiver mod cybertrusler. I Aarhus og Østjylland findes virksomheder som dækker forskellige dele af disse områder.

De fem områder er visualiseret og beskrevet nedenfor.



Identifikation: Dette område fokuserer på hvordan organisationer identificerer de ressourcer og aktiver der skal beskyttes, samt de specifikke trusler, der kan påvirke dem. Det giver en forståelse af organisationens risikoprofil og muliggør en mere effektiv beskyttelsesplan.

Beskyttelse: Her tager man de nødvendige skridt til at beskytte ressourcer og aktiver mod identificerede trusler. Det inkluderer at etablere passende sikkerhedsforanstaltninger og at sikre, at medarbejdere og brugere har passende adgangs- og sikkerhedsrettigheder.

Opdagelse: Denne funktion hjælper organisationer med at opdage cybertrusler så hurtigt som muligt og reagere på dem på en effektiv måde. Det inkluderer at have passende overvågningssystemer og træne medarbejdere i at genkende og rapportere mistænkelige aktiviteter.

Respons: Dette område fokuserer på at have en plan på plads for at håndtere sikkerhedshændelser, når de opstår. Det inkluderer f.eks. at have klare retningslinjer for, hvordan man skal reagere på forskellige typer sikkerhedshændelser, og at have de nødvendige ressourcer og værktøjer til rådighed for at kunne reagere effektivt.

Genopretning: Det sidste område handler om at gendanne forretnings funktionalitet, IT-systemet og data efter en sikkerhedshændelse. Det inkluderer b.la. at have passende sikkerhedskopier og gendannelsesplaner på plads, så organisationen kan komme hurtigt tilbage til normal drift efter en sikkerhedshændelse.

Sammen dækker de fem områder forskellige aspekter af cybersikkerhed og giver organisationer en helhedsorienteret tilgang til cybersikkerhed, der kan hjælpe med at reducere risikoen ved cyberangreb og minimere de negative konsekvenser af en sikkerhedshændelse.

Inden for de fem områder er der en naturlig understøttende opdeling mellem mennesker, processer og teknologi. Disse tre områder er afgørende for effekten af hvert element i NIST CSF-rammen. Det er vigtigt at bemærke, at teknologi ofte ikke fungerer optimalt uden klare processer, der definerer, hvordan teknologien skal bruges for at skabe værdi for brugerne. Derudover er det vigtigt, at mennesker har de rette kompetencer og forståelse for at udføre deres opgaver korrekt og skabe den nødvendige effekt for at minimere den cyber og informationsmæssige risiko som organisationen står over for.

3. NIS2-direktivet

Regulering er inden for cyber- og informationssikkerhed med til at understøtte en hensigtsmæssig adfærd blandt borgere og virksomheder og vil samtidig drive en efterspørgsel efter produkter og tjenester relateret til sikkerhed. Aktuelt er NIS2-direktivet i fokus hos virksomheder på både udbuds- og efterspørgselssiden.

3.1. Baggrund og formål

Baggrunden for NIS2-direktivet er, at cybertruslen mod kritisk infrastruktur og offentlige tjenester er steget markant i de seneste år. Cyberangreb kan have alvorlige konsekvenser for samfundet og økonomien, og det er derfor afgørende at beskytte disse systemer mod angreb og sikre en hurtig respons i tilfælde af et angreb. NIS2-direktivet stiller strenge krav til, at offentlige og private enheder, der leverer samfundskritiske ydelser skal have et cybersikkerhedsniveau, der modsvarer den risiko, den pågældende enhed er udsat for.

NIS2-direktivet opstiller krav til sikkerhed og beredskab for enheder der leverer kritiske tjenester, herunder digitale tjenester. NIS2 stiller krav til risikostyring, leverandørkontrol, rapportering af sikkerhedsbrud og samarbejde med nationale myndigheder og andre enheder. Direktivet dækker en bred vifte af sektorer, herunder energi, transport, finans, sundhedsvæsen og offentlige myndigheder.

Formålet med direktivet er at sikre en høj fælles standard for cybersikkerhed i hele EU og styrke samarbejdet mellem medlemsstaterne og mellem de omfattede enheder. Direktivet er også en del af EU's strategi for digital sikkerhed, der sigter mod at styrke EU's modstandsdygtighed mod cybertrusler og beskytte EU-borgerne på nettet.

Aktualiteten af det samfundsmæssige behov for en høj cybersikkerhedsmodenhed inden for det samfundskritiske område er tiltaget markant, som følge af krigen i Ukraine, hvor cyberangreb i stort omfang ses anvendt sideløbende med konventionel krigsførelse.

3.2. Omfattede virksomheder af NIS2-direktivet

Ifølge Industriens Fond og Dansk Industris seneste vurdering forventes omkring 1.079 virksomheder i Danmark bliver berørt af NIS2 direktivet hvoraf ca. 230 befinder sig i region Midtjylland. De 230 virksomheder opererer primært indenfor fødevarer, elektricitet, internetudbydere, samt maskiner og udstyr[3].

3.3. Forventede konsekvenser

NIS2-direktivet stiller en række krav til virksomheder og offentlige enheder, der driver eller understøtter samfundskritiske tjenester. De forventede konsekvenser af

[3] Ny analyse: 1079 virksomheder på tværs 12 sektorer ser ud til at blive direkte omfattet af NIS2-direktivet - DI Digital (danskindustri.dk)

direktivet kan variere afhængigt af sektoren og den enkelte enheds eksisterende sikkerhedsforanstaltninger, men nogle generelle konsekvenser kan inkludere:

Større fokus på cybersikkerhed: Direktivet kræver, at de omfattede enheder skal have en klar forståelse af de cybertrusler, de står overfor, og de sikkerhedsforanstaltninger, der skal træffes for at beskytte mod dem. Enhederne vil sandsynligvis skulle investere mere i cybersikkerhed og tilpasse deres eksisterende sikkerhedsforanstaltninger for at overholde de nye krav, herunder at den pågældende enhed kan dokumentere overholdelse af kravene i NIS2.

Øget rapportering: Direktivet kræver, at de omfattede enheder skal rapportere sikkerhedsbrud til nationale myndigheder. Dette kan øge omkostningerne og tidsforbruget i forbindelse med håndtering af sikkerhedsbrud og kan også medføre øget opmærksomhed fra myndighederne.

Samarbejde med andre operatører og myndigheder: Direktivet kræver også, at de omfattede enheder skal samarbejde med andre enheder og nationale myndigheder for at forbedre cybersikkerheden. Dette kan kræve ekstra ressourcer og samarbejde på tværs af sektorer og enheder.

Skrappe sanktioner ved overtrædelse: NIS2 foreskriver, at den øverste ledelse skal kunne holdes ansvarlig for overtrædelser på cybersikkerhedskravene i NIS2. Hertil har NIS2-direktivet høje bødeniveauer. De administrative bødetakster er sat til 1,4 – 2 % af årlig global omsætning, hvilket kan betyde, at virksomhederne kan risikere større økonomiske konsekvenser, hvis de ikke overholder direktivets krav.

Afledte krav i leverandørkæden: Ikke-omfattede virksomheder, der leverer ydelser til omfattede enheder, vil formentlig opleve at blive mødt at kontraktuelle krav om cybersikkerhed, revison og assurance samt bodsbestemmelser og lignende som følge af NIS2. Dette kan medføre, at selv virksomheder, der ikke er omfattet af NIS2 direkte, vil opleve at skulle øge niveauet af cybersikkerhed, for at kunne bevare deres konkurrenceevne.

Overordnet set forventes NIS2-direktivet at øge opmærksomheden på cybersikkerhed i hele EU og styrke beskyttelsen af kritiske infrastrukturer og offentlige tjenester mod cyberangreb. Samtidig kan det også medføre øgede omkostninger og krav til virksomhederne, der skal overholde direktivet – hvilket samtidig medfører et markedspotentiale for virksomheder på udbudssiden.

4. Markedet for cyber- og informationssikkerhed

Aarhus har fundamentet til at drive agendaen på cyber- og informationssikkerhedsområdet med et konkurrencedygtigt landskab af små- og mellemstore it-virksomheder, der skaber vækst og værdi gennem eksport.

Aarhus har oplevet en betydelig vækst i den samlede it-branche med øget omsætning, beskæftigelse og værdiskabelse til følge, hvilket resultaterne i dette kapitel underbygger. I analyserne er tal for Aarhus så vidt som data tillader sammenlignet med hele landet og sammenligningsbyerne København, Odense og Aalborg.

4.1. Beskæftigelse

Aarhus Kommune har haft stor succes med at skabe vækst og nye arbejdspladser i it-sektoren. Beskæftigelsesudviklingen i sektoren er næsten dobbelt så stor som på landsplan, hvor også en højere andel har deres daglige arbejdsgang.

Der har i perioden 2008-2022 været en markant vækst i beskæftigelsen i it-sektoren. Væksten er især drevet af storbyerne Aarhus og København og de omkringliggende områder. Her ses i perioden en vækst på hhv. 57,1% og 78,2%, hvorimod resten af landet faktisk oplever en mindre tilbagegang for samme periode svarende til et fald på 2,9%. Se Figur 1. Udvikling i beskæftigelsen i it-sektoren, 2008K1-2022Disse vækstrater er relativt høje, og understreger potentialet i markedet for Aarhus. Udviklingen i væksten i Aarhus og København adskiller sig på det parameter, at beskæftigelsesvæksten i Aarhus særligt er vokset i den sidste del af perioden, men ligger fortsat en smule bagved København.

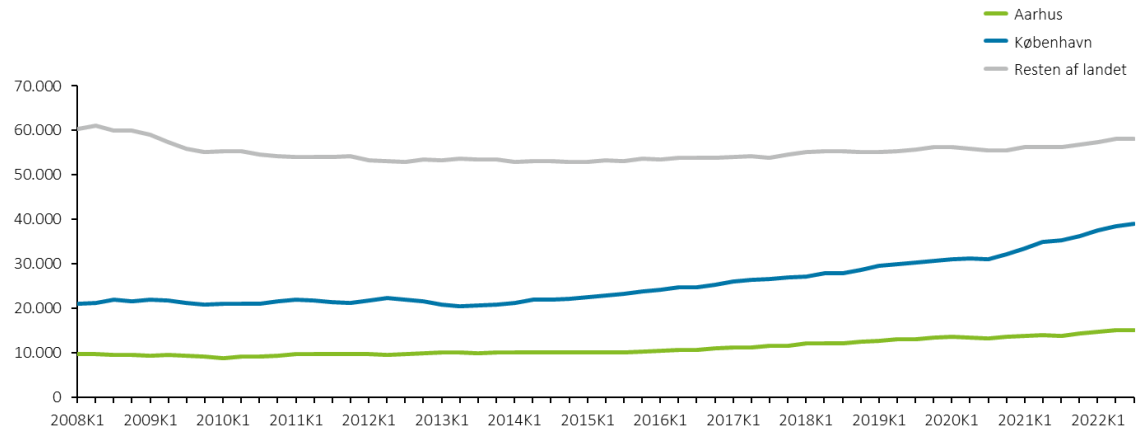
I Aarhus Kommune er it-arbejdsmarkedet øget med 31% fra 2015 til 2021. Det svarer til en stigning på 6.578 beskæftigede. Heraf tegner it-sektoren sig for 4.130 beskæftigede svarende til en vækst på 39% for samme periode. Se Figur 2. It-sektoren udgør altså en stor del af udviklingen på it-arbejdsmarkedet.

Definition af brancher

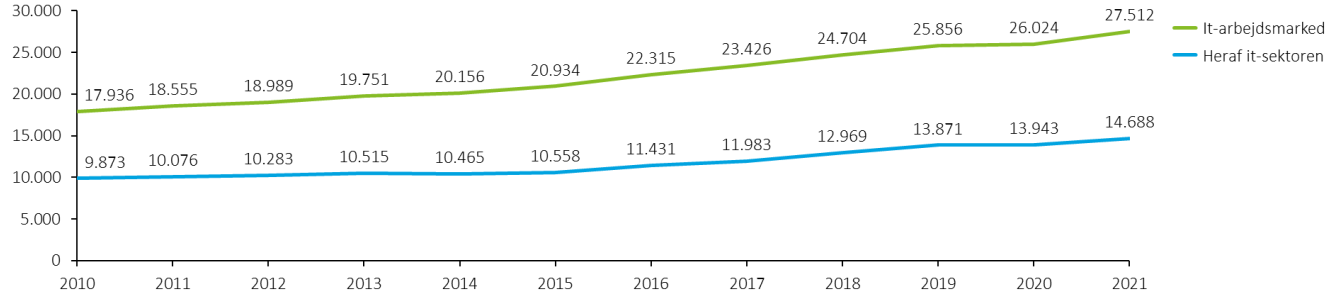
I markedsanalysen opgøres nøgletal på forskellige definitioner af brancher på baggrund af forskelle i datatilgængelighed. Der er gennem årene udarbejdet flere definitioner af it-sektoren. Den nyeste er udført af OECD i 2007 og inkluderer færre undergrupperinger end tidligere for at undgå virksomheder med perifer tilknytning til it-sektoren. Der anvendes endvidere en bredere afgrænsning: IT og kommunikation, men det formål at inkludere videnstunge TECH-virksomheder med hovedsæde i Aarhus. Afslutningsvist defineres it-arbejdsmarkedet som 1) personer med beskæftigede i it-sektoren, 2) personer beskæftigede i it-stillinger udenfor it-sektoren og 3) personer med it-uddannelser. Definitionerne begrænser delvist sammenligningsmulighederne.

Kilde: eStatistik

Figur 1. Udvikling i beskæftigelsen i it-sektoren, 2008K1-2022K1



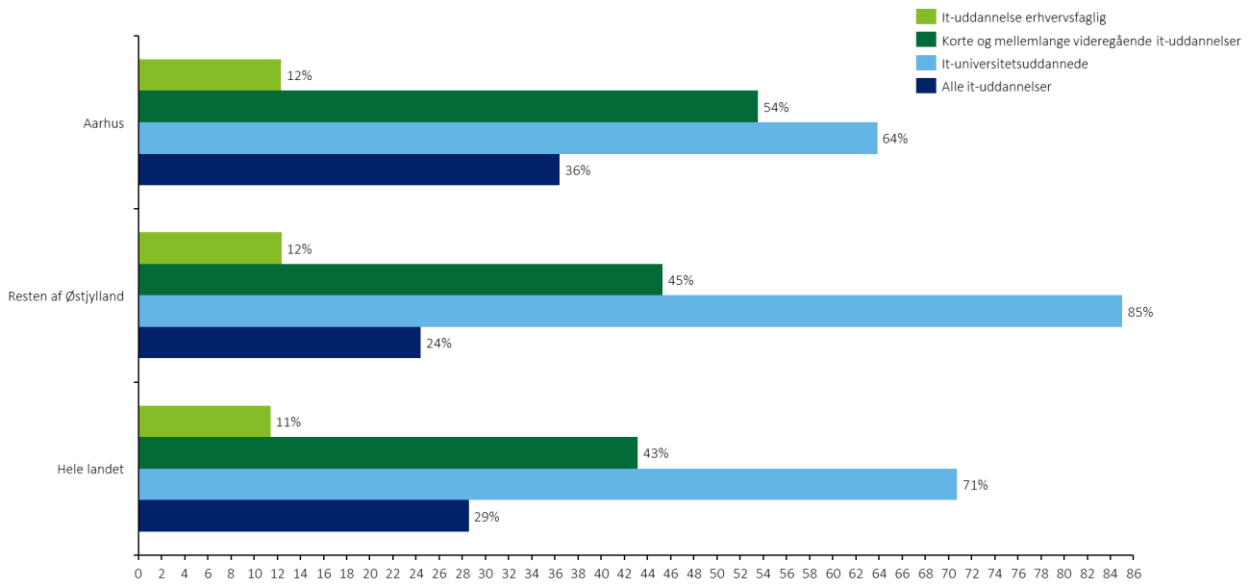
Figur 2. Udvikling i beskæftigelsen på it-arbejdsmarkedet i Aarhus Kommune, 2010-2021



Finanskrisen i 2008 medførte et umiddelbart fald i beskæftigelsen samt en periode med stagnation. På trods af den nuværende trussel om en recession er der en række tendenser, der indikerer at it-sektoren ikke vil opleve samme mønster i den kommende periode. Disse tendenser tæller blandt andet den fremtrædende digitalisering, øgede risiko overfor cyberangreb samt lovgivning og regulering.

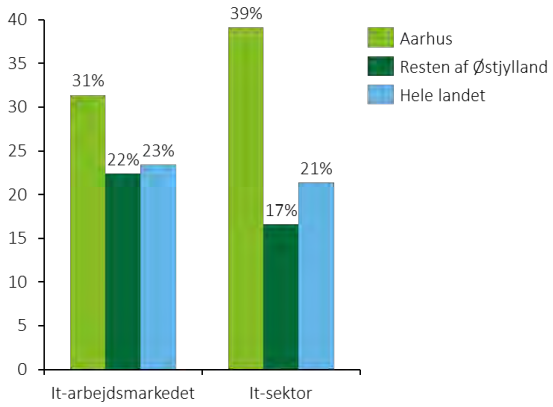
Aarhus har opnået den højeste beskæftigelsesudvikling på 36% baseret på alle it-uddannelser. Se Figur 3. Beskæftigelsesudvikling i it-sektoren fordelt på uddannelsesvalg, 2015-2021It-uddannelserne udgør isoleret set den største gruppe på it-arbejdsmarkedet. Der er særligt sket en udvikling i beskæftigede personer med en it-universitetsuddannelse mellem 2015-2021. Det gælder for både Aarhus, resten af Østjylland og hele landet. Det samme gælder for korte og mellemlange videregående it-uddannelser, hvor Aarhus står i spidsen.

Figur 3. Beskæftigelsesudvikling i it-sektoren fordelt på uddannelsesvalg, 2015-2021



It-arbejdsmarkedet og it-sektoren vokser markant hurtigere i Aarhus kommune end i resten af Østjylland og på landsplan. Mellem 2015-2021 vækstede beskæftigelsen på it-arbejdsmarkedet og i it-sektoren med hhv. 31,4% og 39,1% i Aarhus kommune. Denne vækst lå i samme periode på hhv. 22,4 og 16,6% i resten af Østjylland. Se Figur 4. Der ses altså en særlig markant stigning i beskæftigelsen for de definerede brancher i Aarhus.

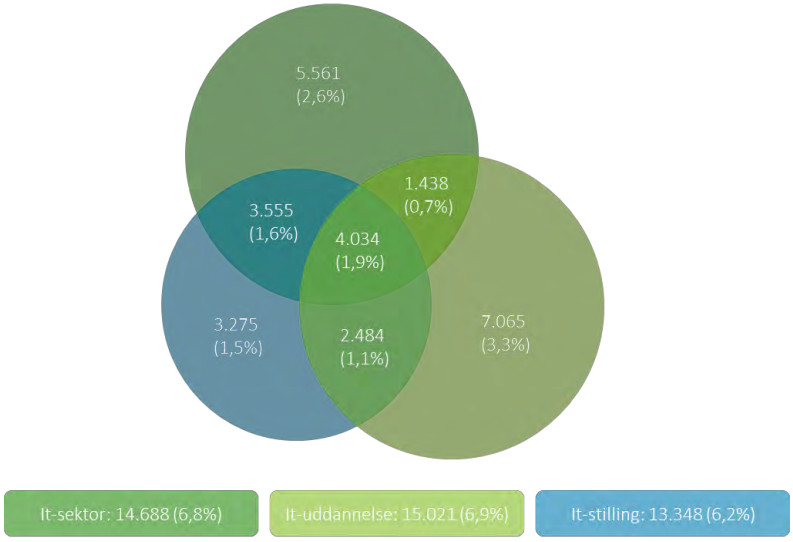
Figur 4. Beskæftigelsesudvikling på branche, 2015-2021



Figur 5 viser fordelingen i beskæftigelse indenfor it-arbejdsmarkedet[4]. På landsplan udgør disse tre grupper tilsammen 8,6% af den samlede beskæftigelse. Kigger vi

[4] Defineret i introduktionen "Definition af brancher"

isoleret på Aarhus kommune, finder man 12,7% af den samlede beskæftigelse i disse tre grupper, mens der i Østjylland fraregnet Aarhus er 5,9% af den samlede beskæftigelse indenfor it-arbejdsmarkedet. Det viser it-arbejdsmarkedets betydning i Aarhus Kommune som it-klynge og at branchen udgør en større andel af beskæftigelsen end den resterende del af Østjylland og på landsplan. Figurerne for Østjylland fraregnet Aarhus og hele landet findes i bilag.Figur 5. Beskæftigelse på it-arbejdsmarkedet i Aarhus Kommune, 2021



"Aarhus har den luksus, at der er viden, talent, vækst og erhvervsliv. De har dermed det fundament der skal til, hvor projekter kan stige i ambition, men samtidig realiseres hurtigt"

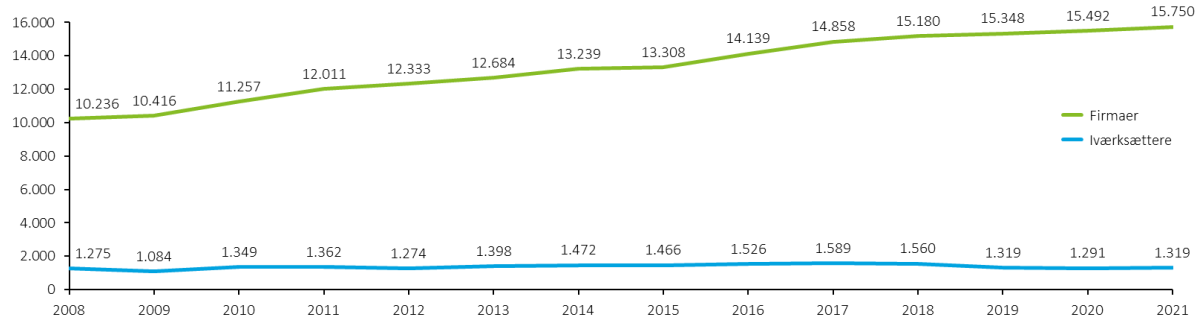
4.2. Virksomheder og ansatte

Antallet af virksomheder inden for it-sektoren i hele landet er steget markant, og Aarhus skiller sig særligt ud med en større vækst end København, Aalborg og Odense i løbet af de seneste fem år. Det gælder både hvad angår antallet af virksomheder og årsværk.

Det er veldokumenteret, at der har været en markant beskæftigelsesvækst i it-sektoren. Denne vækst kommer også til udtryk, når vi kigger på udviklingen i antallet af firmaer i it-sektoren. Her har der ligeledes været en massiv vækst. I perioden 2008 til 2021 er antallet af reelle virksomheder vækstet med 54%. Se Figur 6. For den bredere afgrænsning it og kommunikation var der i Aarhus Kommune 1.807 virksomheder i 2016 sammenholdt med 2.130 i 2021. Det svarer til en vækst på 18%. Sammenholdt med landsplan og København lå væksten i samme periode på hhv. 9% og 15% indenfor It og kommunikation. Se Figur 8 og Tabel 1.

Antallet af virksomheder er vokset stabilt over en lang årrække, hvilket også peger på et gunstigt erhvervsklima for branchen sammenholdt med stigende efterspørgsel efter it-ydelser. Hertil har der været en stabil tilførsel af nye virksomheder i it-sektoren. Knap 22% af it-sektorens beskæftigelse findes i virksomheder med en alder på maksimalt ti år. I Aarhus er tallet 20,6% og i København 27,3%. Se Figur 7. Beskæftigelsesandelen er altså primært drevet af de to it-klynger.

Figur 6. Antal reelle virksomheder i it-sektoren i hele landet, 2008-2021

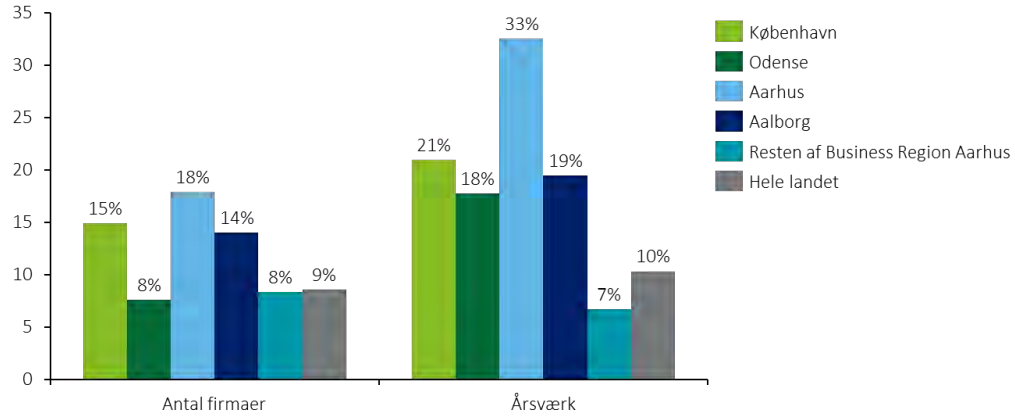


Figur 7. Iværksætteres beskæftigelsesandel i it-sektoren, 2021

I Aarhus var der indenfor it og kommunikation i 2016 11.073 fuldtidsansatte sammenholdt med 14.672 i 2021. Det svarer til en vækst på 33%. Tilsvarende lå væksten i samme periode på 10% på landsplan og på 21% i København. Det fremgår af Figur 8 og Tabel 1.

"I Aarhus er der nogle stærke byggeklodser på plads, som gør det muligt at accelerere et mønstereksempel indenfor cyber"

Figur 8. Procentvise vækst mellem 2016-2021 for antal firmaer og årsværk indenfor it og kommunikation



Tabel 1. Nøgletal for virksomheder i Aarhus Kommune indenfor it og kommunikation, 2016 & 2021

Enhed	2016	2021	Vækst	I pct
Antal firmaer	1.807	2.130	323	18%
Årsværk	11.073	14.672	3.599	33%
Omsætning i mio. kr.	22.453	42.564	10.112	45%
Eksport i mio. kr.	5.897	10.200	4.302	73%
Værditilvækst i mio. kr.	7.964	14.681	6.717	84%

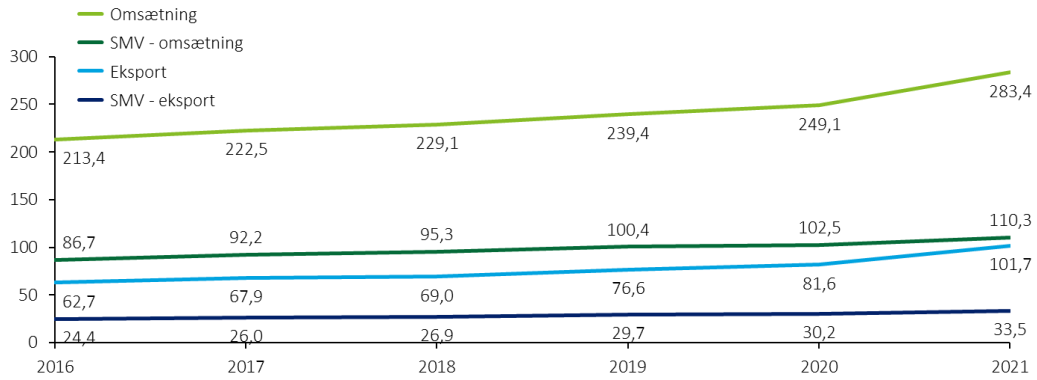
Note: Nøgletallene er for virksomheder med hovedsæde i Aarhus Kommune

4.3. Omsætning, eksport og værditilvækst

De økonomiske nøgletal for it og kommunikation er generelt steget i løbet af de seneste fem år, og det er primært Aarhus, der har stået for den høje vækst. Virksomheder med hovedsæde i Aarhus har øget deres værditilvækst med 84% i samme periode. Som følge af dette har Aarhus opnået en høj produktivitet relativt set sammenlignet med resten af landet og sammenligningsbyerne.

Det er en gunstig periode for it-sektoren, der på alle på måder fylder mere og mere i det danske erhvervsliv. Det illustreres blandt andet ved branchens beskæftigelse, som vi har set ovenfor. Men også omsætningen i it-sektoren vokser år for år. Kigger vi på perioden fra 2016, har der været en vækst i branchens samlede omsætning i alle år, og samlet set er omsætningen vokset fra 213,4 milliarder kroner i 2016 til 283,4 milliarder kroner i 2021. En vækst på 33%. Særligt det seneste år, det vil sige fra 2020 til 2021, er omsætningen skudt voldsomt i vejret. Her er der registreret en vækst i omsætning på 34,3 milliarder kroner (13,8%). Eksporten og SMV-segmentet spiller en væsentlig del af forklaringen på omsætningsvæksten i perioden. Dette er illustreret i Figur 9.

Figur 9. Omsætning og eksport (mia. kr.) i it-sektoren i hele landet, herunder SMV-segmentet, 2016-2021



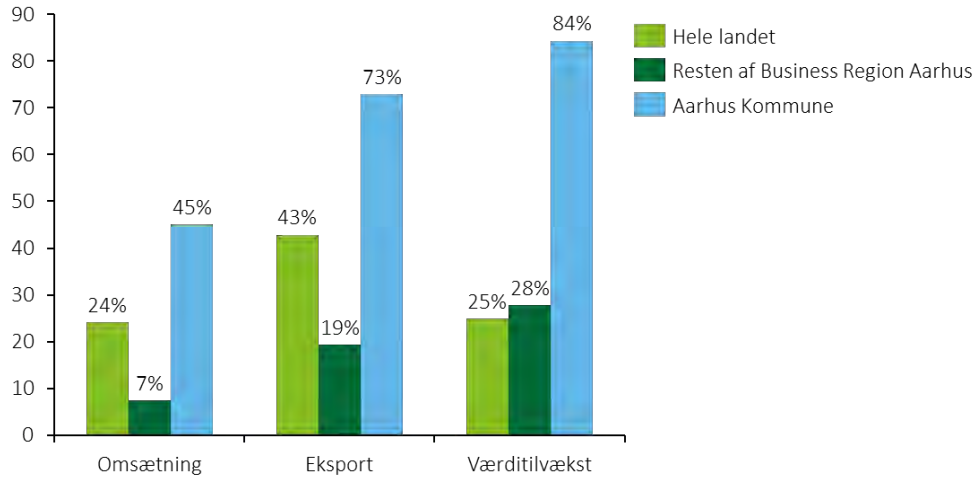
For den bredere afgrænsning it og kommunikation var omsætningen i 2016 22.453 mio. kr. sammenholdt med 32.564 mio. kr. i 2021 i Aarhus. Det svarer til en stigning på 45% på blot 5 år. Eksporten steg fra 5.897 mio. kr. i 2016 til 10.200 mio. kr. i 2021 svarende til en vækst på 73%. Det viser særligt at markedet for it ikke kun vokser nationalt, men særligt også udenfor landets grænser, der trækker på viden og kompetencer centreret i Aarhus. Pointen kommer særligt til udtryk i lyset af den

tilsvarende – om end også høje - vækst i hele landet, der i samme periode lå på hhv. 24% og 43%. Se Figur 10.

Værditilvæksten indenfor it og kommunikation i Aarhus er især steget markant. Væksten er steget fra 7.964 mio. kr. til 14.681 mio. kr. mellem 2016-2021. Det svarer til en udvikling på 84%. Udviklingen vidner om, at de lokalt forankrede virksomheder indenfor den nationale og regionale styrkeposition har formået at skabe høj vækst og værdi gennem de seneste år.

Sammenholdes disse nøgletal med resten af Østjylland og hele landet, så ses det at udviklingen er langt mere iøjefaldende for Aarhus. Se Figur 10. Aarhus Kommune har vækstet mere indenfor de seneste 5 år sammenlignet med hele landet. Det kommer især til udtryk gennem eksport og værditilvækst. Værditilvæksten er mere end tre gange så stor som på landsplan.

Figur 10. Procentvise vækst mellem 2016-2021 for udvalgte nøgletal indenfor it og kommunikation



Note: Nøgletallene er for virksomheder med hovedsæde i Aarhus Kommune.

I perioden 2016-2021 har Aarhus oplevet en større vækst end samtlige af Danmarks storbyer, hvilket tyder på, at byen har udviklet sig markant inden for sektoren og har stærke kompetencer i it-klyngen. Det er overraskende at se, at København i flere tilfælde er den by, der har haft mindst vækst.

Den mest iøjnefaldende forskel er imidlertid mellem værditilvæksten i de to definerede it-klynger, Aarhus og København, hvor forskellen er på hele 460%. Se Figur 11. Dette understreger Aarhus' stærke position inden for IT-området og bekræfter byens evne til at tiltrække og fastholde it-talenter og virksomheder, til trods for at flere respondenter påpeger manglen på kvalificeret arbejdskraft.

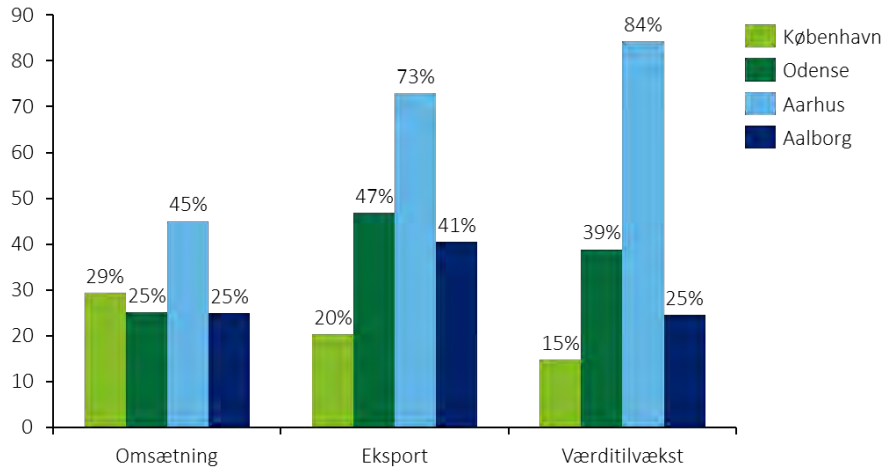
Det er interessant at bemærke, at selvom København har en større befolkning og en mere etableret it-sektor end Aarhus, har Aarhus vist sig at have en større vækst og større potentiale inden for it-området i de seneste år. Dette kan skyldes en række faktorer, herunder en mere dynamisk og innovativ it-klynge i Aarhus og byens tætte

"Aarhus er ikke bare et miljø med startups. Der er en lang historie, der går tilbage til 90'erne, både kommercielt og forskningsmæssigt. Det er helt tydeligt at niveauet er der og det er ikke blevet mindre de seneste år. Det ligger i kølvandet af AU og Alexandra Instituttet"

samarbejde mellem virksomheder, uddannelsesinstitutioner, offentlige institutioner og interesseorganisationer – quardruple helix.

Samlet set bekræfter denne vækst i Aarhus' it-sektor byens position som en af Danmarks mest dynamiske og innovative byer og et attraktivt sted at arbejde og investere i it-industrien.

Figur 11. Procentvise vækst mellem 2016-2021 for udvalgte nøgletal indenfor it og kommunikation fordelt på storbyerne i Danmark



Note: Nøgletallene er for virksomheder med hovedsæde i de respektive byer.

4.4. Nationale markedstendenser

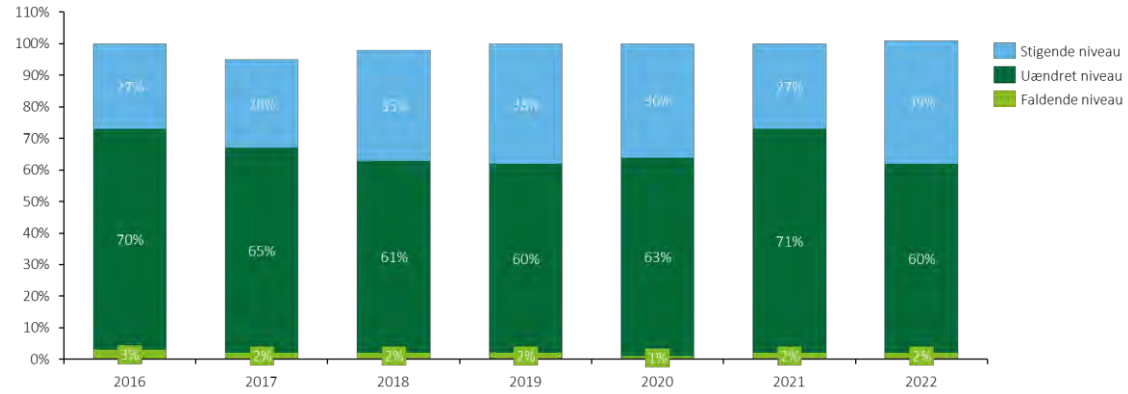
4.4.1. Investeringer i it-sikkerhed

Andelen af virksomheder med et stigende investeringsniveau har på landsplan været voksende siden 2016. Der er en tydelig sammenhæng mellem størrelsen på virksomheder og investeringer i it-sikkerhed. Des større virksomheden, des mere fylder investeringer i it-sikkerhed.

Langt størstedelen af virksomheder med mindst 10 ansatte rapporterer et enten stigende eller uændret niveau for investeringer i it-sikkerhed. Andelen af virksomheder med et stigende investeringsniveau har været voksende siden 2016. Andelen af virksomheder, der investerer mindre i it-sikkerhed, er forsvindende lille - nærmest ikke tilstedeværende. Se Figur 12. Der er altså over en bred kam enighed om i det danske erhvervsliv, at it-sikkerhed er en helt essentiel del af dét at drive virksomhed i dag.

Statistikken opgøres også på virksomhedsstørrelser, og her ses det tydeligt, at des større virksomhederne bliver, des mere fylder investeringer i it-sikkerhed. For virksomheder med 250 eller flere ansatte er det 76% af de adspurgte, der forventer et øget investeringsniveau i 2022, mens 23% forventer et uændret niveau. I takt med den øgede digitalisering og internationalisering, bliver virksomhederne mere og mere afhængige af en stabil og sikker it-infrastruktur, hvorfor behovet for et værn mod nedbrud blot bliver endnu større fremfor. For i takt med, at erhvervslivet er mere og mere afhængigt af it, bliver det selvsagt også mere og mere sårbart overfor forstyrrelser, og derved også for angreb fra it-kriminelle.

Figur 12. Niveau for investeringer i it-sikkerheder, virksomheder med mindst 10 ansatte i hele landet, 2016-2022

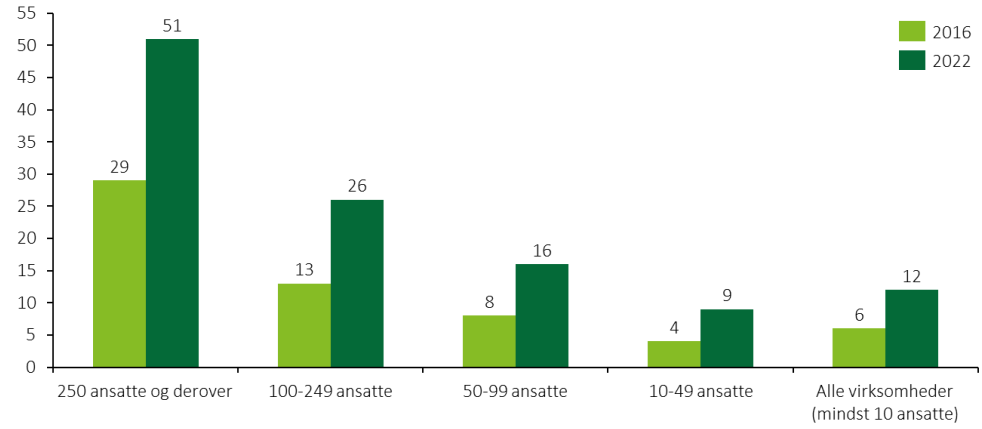


4.4.2. Rekruttering

Som følge af høj beskæftigelse og vækst indenfor it-sektoren oplever virksomheder også i stigende grad vanskeligheder med at rekruttere talenter og kvalificeret arbejdskraft. Det er vigtigt at have for øje, da arbejdskraft potentielt kan være en vigtig faktor for at fremme Aarhus' styrkeposition indenfor cybersikkerhed.

Det øgede fokus på digitalisering og it-sikkerhed kan også aflæses af virksomhedernes omsætning, som påpeget ovenfor. Væksten bør ses i lyset af, at virksomheder oplever betragtelige udfordringer ved at rekruttere, og disse vanskeligheder er kun blevet større de seneste år. I 2016 var det 6% af virksomheder med 10 eller flere ansatte, der oplevede vanskeligheder med at rekruttere kvalificeret it-arbejdskraft. I 2022 er denne andel fordoblet til 12%. Se Figur 13. Kigger man på virksomhedsstørrelser, stiger hyppigheden af rekrutteringsudfordringer i takt med antallet af ansatte. Værst ser det ud for de største virksomheder med 250 eller flere ansatte. Her er det over halvdelen af virksomheder i 2022, der har oplevet vanskeligheder med at få kvalificeret it-arbejdskraft. I 2016 var denne andel på 29%.

Figur 13. Andelen af virksomheder med 10+ ansatte som oplever vanskeligheder med at rekruttere it-specialister i hele landet, 2016 & 2022



5. Aarhus' og Østjyllands relative styrkepositioner

Analyserne dokumenterer et markedspotentiale for cyber- og informationssikkerhed i Aarhus og Østjylland og et solidt fundament for realiseringen heraf via et veletableret økosystem med Aarhus Universitet som aktiv, en forsknings- og forretningsmæssig førertrøje i kryptologi og en partnerskabsorienteret erhvervskultur.

5.1. Styrkepositioner

Aarhus har et stærkt økosystem af konkurrencedygtige it-virksomheder og en forsknings- og markedsmæssig førertrøje i kryptologi

Dette fundament har potentiale til at gavne både samfundet som helhed og den lokale økonomi ved at skabe vækst og arbejdspladser, der styrker Aarhus som en attraktiv by at bo, arbejde og studere i. En række veletablerede virksomheder, der udspringer fra Datalogi på Aarhus Universitet, herunder Cryptomathic, Partisia og Sepior er væsentlige spillere i dette økosystem.

Institut for Datalogi på Aarhus Universitet er i top tre blandt universiteter, der forsker i kryptologi på verdensplan, og uddanner mange kandidater og Ph.d.er med efterspurgte kompetencer på sikkerhedsområdet. Det stærke faglige miljø med højteknologisk viden i it-byen på Katrinebjerg centrerer sig omkring kryptologi og andre sikkerhedsteknologier som blockchain og MPC[5]. Miljøet giver mulighed for at udnytte vækstmuligheder inden for cyber- og informationssikkerhed i både erhvervslivet og uddannelsesinstitutioner.

Digitalisering stiller høje krav til niveauet inden for cyber- og informationssikkerhed og skaber et uudnyttet potentiale.

Danmark er relativt set godt med inden for sikkerhed, men historisk set har sikkerhed været bagefter i forhold til niveauet af digitalisering. Afhængigheden af digitalisering stiller imidlertid højere krav til niveauet af modenhed inden for sikkerhed, og Danmark skal derfor være dygtige inden for sikkerhed for at kunne følge med. Mange virksomheder har imidlertid ikke forstået risikoen og manglen på reel viden om cybersikkerhed, der kræves for at følge med digitaliseringens hastighed. Virksomheder har derfor tendens til at vælge de lette løsninger inden for sikkerhed, men dette kan føre til, at virksomheder halter bagud på sikkerhedsagendaen. Det er til trods for, at det er påvist, at cybersikkerhedstiltag medfører en bred vifte af konkurrencefordele[6].

Udviklingen i digitaliseringen, reguleringen og øget bevågenhed i medierne har ført til, at cybersikkerhed er blevet en større prioritet for CxO'er og bestyrelser på både udbuds- og efterspørgselssiden. Kombineret med det lave modenhedsniveau inden

[5] Multiparty Computing
[6] Cyberbarometer.dk

for cybersikkerhed udgør dette et stort kommercielt potentiale for de aarhusianske virksomheder, der tilbyder produkter og services inden for cybersikkerhed.

Den aarhusianske partnerskabskultur og infrastruktur har fundamentet på plads til at udvide styrkepositionen.
Aarhus er en by med en kultur karakteriseret ved naturlig velvilje, samarbejde og hjælpsomhed. Dette ses blandt andet tydeligt i relationen mellem byens virksomheder og uddannelsesinstitutioner, hvor flere initiativer er blevet etableret gennem årene som eksempelvis samarbejdet mellem Concordium og Datalogi benævnt COBRA[7].

For at fremme vækst og udvikling indenfor cyber- og informationssikkerhed i Aarhus og Danmark som helhed, er det afgørende fortsat at etablere tætte samarbejder mellem relevante interessenter. Dette kan føre til eksempelvis udvikling af manglende uddannelser og øget fokus på de erhvervsakademiske uddannelser, der kan uddanne praktisk orienterede "cyberhåndværkere". Et sådant samarbejde kan også hjælpe med at omsætte forskning til startups og virkelige problemstillinger til forskningsgenstande, der i forvejen har været kendetegnet i det aarhusianske miljø.

Derudover kan Aarhus opbygge et miljø, hvor it-sikkerhed ses som en konkurrencemæssig fordel og forretningsmæssig risiko, der kan realiseres og mitigeres – og ikke som en forhindring. Aarhus har mulighed for at fungere som forsøgskanin for nye projekter og derefter skalere nationalt på baggrund af byens infrastruktur og størrelse. Der eksisterer en stor vidensbase, talent, vækst og erhvervsliv, hvor Aarhus kan operere som et spændende testcenter. Det er muligt på baggrund af det aarhusianske fundament og infrastruktur, hvor projekter kan stige i ambition, men realiseres hurtigt.

5.2. Udfordringer

I takt med stigende krav fra lovgivning, regulering og cybertrusler inden for datasikkerhed vil en markant efterspørgsel med stor sandsynlighed følge med.
Der er generelt entydig konsensus blandt respondenterne om at mangel på kvalificeret arbejdskraft udgør en signifikant trussel for vækstmulighederne. Det gælder både regionalt og nationalt. Denne trussel forstærkes af at de studerende er mobile, hvilket medfører en risiko for at de fravælger Aarhus og virksomhederne i byen efter endt uddannelse, hvis ikke der er et attraktivt miljø og jobmuligheder.

Da cyber- og informationssikkerhed er en kompleks branche, er det vigtigt, at et initiativ som STS konkretiseres til en håndgribelig størrelse. Der bør være en klar ansvars- og rollefordeling og tilstrækkelig finansiering til etablering og vedligeholdelse af initiativet samt investering i og fra aarhusianske cyber- og informationssikkerhedsvirksomheder.

Endelig er det vigtigt at påpege, at cybertruslen mod Danmark er reel og vil forblive en kontinuerlig trussel på baggrund af Danmarks høje grad a digitalisering[8]. Det skyldes pro-russiske cyberaktivisters høje aktivitetsniveau mod NATO-lande. I takt med stigende krav fra lovgivning, regulering og cybertrusler inden for datasikkerhed vil en markant efterspørgsel med stor sandsynlighed følge med. Det vil skabe endnu større vækstpotentiale og muligheder for at styrke Aarhus' position indenfor cyber- og informationssikkerhed. Som led i et STS, vil Aarhus Universitet og it-byen Katrinebjerg spille en vigtig rolle. Aarhus har som fundament et stærkt økosystem til at videreudvikle og innovere den østjyske styrkeposition.

[7] COBRA
[8] Cybertruslen mod Danmark

6. Et Security Tech Space

Et Security Tech Space skal tage udgangspunkt i tre indsatsområder for at realisere både visionen om øget cybersikkerhed samt de relaterede markedspotentialer. 1) Innovationslaboratorium, 2) markedsmatching og 3) videns- og rådgivningscenter.

Aarhus har et solidt fundament for at agere og accelerere et mønstereksempel inden for cyber- og informationssikkerhed. Aarhus har viden, talent, vækst og et stærkt erhvervsliv. Kombineret med byens størrelse er der gode forudsætninger for at digitaliseringsprojekter nemmere kan realiseres med høje ambitioner samtidig med, at Aarhus kan fungere som incubator og skalere projekter og viden nationalt.

6.1. Interessenter

Der er en stor interesse for og opbakning til et Security Tech Space i Aarhus blandt konsortiemedlemmerne. Resultaterne fra den aarhusianske styrkeposition understreger vigtigheden af et stærkt samarbejde, økosystem og miljø på tværs af kommunen, uddannelsesinstitutionerne og erhvervslivet.

6.2. Organisering

Repræsentanterne der er inddraget i denne analyse, fremhæver behovet for, at der en instans, der tager styring og driver udviklingen for at mindske risikoen for, at den eksisterende styrkeposition udvandes. Denne instans kan udgøres af et Security Tech Space. Denne instans er særligt afhængig af to elementer; 1) at der er tilstrækkelig med finansiering, og at 2) der er bred støtte fra økosystemet.

En oplagt organisering er et murstensløst Security Tech Space med huse i en af konsortiepartnernes bygninger, gerne et forsknings- og innovationsmiljø, eksempelvis INCUBA i it-byen Katrinebjerg, med en direktør, en sekretariatschef og en bestyrelse med repræsentanter fra det brede interessentlandskab i spidsen. At det brede interessentlandskab er repræsenteret, er særligt vigtigt, da cyber- og informationssikkerhed kræver tværfaglige kompetencer, samt at forskning skal kombineres med virksomhedspraksis. Derfor kunne man forestille sig et quadruple inspireret samarbejde, jf. Figur 14 nedenfor:

"Det handler om mennesker. Grunden til de aarhusianske virksomheder gør det godt er, at de har de rigtige mennesker, hvor tilliden er høj. Der er mange andre ting man kan påpege af mere politisk og strategisk karakter, men hvis man skal skære det indtil benet, så handler det om mennesker"

Figur 14. Quadruple helix

Informanterne fremhæver herudover, at det er en væsentlig forudsætning for et Security Tech Space, at der er et forpligtende samarbejde på tværs af aktørerne. Særligt fremhæves det, at det er vigtigt at der er fastsat klare mål og at kommunal involvering er en forudsætning for succes. Flere af informanterne fremhæver Aarhus Kommunes og borgmesterens engagement og investeringsvillighed i samarbejdet som motivation for dem selv til at gå ind i samarbejdet og som en afgørende faktor for målopfyldelsen heraf. Deres involvering legitimerer samarbejdet og giver det en forpligtende karakter. Security Tech Space skal identificere og konkretisere områder, hvor Aarhus ønsker at gøre sig interessant. I fællesskab skal aktørerne gruppere vigtige områder evt. i forbindelse med udarbejdelsen af en cybervision, hvor trusselsbilledet og efterspørgslen bliver fastlagt i dag og i morgen.

Finansieringen af et Security Tech Space kan fondsfinansieres med midler fra de vigtigste interessenter i økosystemet. Dette bidrager tilså desuden at samarbejdet bliver af forpligtende karakter. Initiativet vil fortsætte med at kræve finansiering, da de indtægtsgenererende aktiviteter vil være begrænsede.

Missionen er klar: Et Security Tech Space skal være katalysator for samspil og samskabelse på tværs af det samlede økosystem af både offentlige og private aktører ved at agere bindeled mellem udbud og efterspørgsel, samt forskning og erhverv.

6.3. Indsatsområder

Indsatsen i en Security Tech Space har som fællesnævner, at det er afgørende for bæredygtig vækst, at initiativet fungerer som støtteorgan. Dette er især vigtigt for at udvikle og styrke det allerede solide økosystem og sikre, at erhvervslivet, studerende og offentlige instanser bliver koblet sammen, så vidensdeling kan finde sted og vækst realiseres.

Grundlaget for et Security Tech Space afhænger af indsatsen i Aarhus og Østjylland. Derfor skal der fokuseres på de områder, hvor regionen har relativt store markedsfordele og/eller hvor der er et uopfyldt markedspotentiale, hvis de ønsker at differentiere sig fra andre vækstregioner i Danmark og samtidig supplere allerede igangværende initiativer. Analysen har identificeret tre kerneelementer med stort potentiale for Aarhus og Østjyllands styrkeposition:

1) Innovation, især inden for kryptologi og andre sikkerhedsteknologier som blockchain og MPC
2) Adgang til talent
3) Cyber- og informations-sikkerhed, især i små og mellemstore danske virksomheder.

Baseret på disse potentialer kan der udledes tre essentielle og konkrete indsatsområder. Disse er:


Innovationslaboratorium


Markedsmatching


Videns- og rådgivningscenter

6.3.1. Innovationslaboratorium

For at fremme innovation, samt udvikling af sikkerheds- og forretningsmæssige løsninger inden for kryptering og cybersikkerhed er det vigtigt at skabe en fælles platform for samarbejde mellem forskellige aktører i økosystemet. Et Security Tech Space kan spille en vigtig rolle i denne sammenhæng ved at tilbyde faciliteter og ressourcer til at fremme samarbejde og vidensdeling mellem universiteter, etablerede virksomheder, startups, scaleups, investorer og offentlige institutioner.

Cyber- og informationssikkerhed skal være en integreret del af innovation og virksomheders DNA. Et Security Tech Space kan være med til at fremme denne kultur ved at tilbyde træning og uddannelse i sikkerhedsstandarder og -protokoller samt ved at facilitere dialog og samarbejde mellem forskellige aktører om sikkerhedsudfordringer og -løsninger. Det kunne foregå gennem udviklings- og testfaciliteter for studerende, forskere, virksomheder og andre med kvalificerede forretningsideer med interesse for området. Et acceleratormiljø, som på samme måde som INCUBA kan facilitere en Aarhus-baseret forskerpark, hvor relevante aktører kan sparre med hinanden og fastlægge trusselsbilledet og efterspørgslen for produkter og tjenester inden for sikkerhed.

Alt i alt vil et Security Tech Space kunne spille en vigtig rolle i udviklingen af innovative og bæredygtige løsninger inden for kryptering og cybersikkerhed. Ved at tilbyde en fælles platform for samarbejde og vidensdeling og ved at fremme en kultur for sikkerhed kan et Security Tech Space bidrage til at fastholde et fertilt miljø for innovation inden for området og dermed styrke Aarhus' position som et førende center for kryptering og cybersikkerhed.

”Man skal være helt klar på sine succeskriterier. Hvad er det egentlig vi gerne vil opnå?”

6.3.2. Markedsmatching

En af de centrale opgaver, som et Security Tech Space skal løfte, er at assistere aktørerne i deres behov for markedsmatching. Markedsmatching omfatter en række forskellige aktiviteter med forskellige formål. Ét af formålene er at accelerere innovationsprocessen fra ide til marked ved at facilitere samarbejde mellem forskere, startups, mikrovirksomheder, investorer og samarbejdspartnere. Et Security Tech Space kan fungere som en central hub for dette formål ved at etablere et netværk, der fremmer kapital, kommerciel strategi og vækst.

Et andet formål med kerneopgaven markedsmatching er at sikre, at udbud og efterspørgsel efter kompetencer inden for cyber- og informationssikkerhed mødes. Det vil sige at støtte og afdække behovet for talent og kvalificeret arbejdskraft inden for området. Dette kan opnås ved at facilitere et samarbejde mellem studerende, virksomheder og uddannelsesinstitutioner. Studerende og unge kan modtage værdifuld rådgivning, erfaring og vidensoverførsel fra virksomheder og uddannelsesinstitutioner. Omvendt kan virksomheder bruge relationerne som en rekrutteringskanal for at skabe kvalificerede kompetencer, vækst og attraktive arbejdspladser. Dette kan visualiseres som gensidig kompetenceopbygning, hvor både virksomheder og studerende udnytter hinandens potentiale for at opnå vækst

og succes gennem et udviklingssamarbejde mellem forskning og erhverv. Her kan aktørerne samarbejde og sparre med hinanden i et forum med en fælles agenda.

Markedsmatching er en vigtig opgave for et Security Tech Space, da det kan bidrage til at accelerere markedspotentialet og sikre, at udbud og efterspørgsel efter kompetencer inden for cyber- og informationssikkerhed mødes på effektiv vis.

Der findes flere forskellige eksisterende koncepter og initiativer, som kan anvendes som inspiration og/eller videreudvikles, som eksempelvis listet nedenfor:

- Junior Consult – konsulentvirksomhed, der udelukkende drives af studerende
- Coding pirates – fritidstilbud til børn og unge, der promoverer IT-kreativitet
- Teknologiskolen – frivillig forening, der tilbyder teknologisk orienterede fritidsaktiviteter for børn og unge
- Education Esbjerg – sekretariat, der har til formål at fremme Esbjerg som uddannelses by blandt andet gennem samarbejde mellem uddannelse og erhverv
- Det fælleskommunale databehandlersekretariat (DBS) – har til formål at gøre tilsyn med medlemskommunernes databehandleraftaler

Markedsmatching bør være med til at sikre at der skabes og fastholdes en kritisk masse af talenter og virksomheder på lang sigt gennem etableringen af et innovationssamarbejde mellem repræsentanter fra det samlede økosystem.

6.3.3. Videns- og rådgivningscenter

En vigtig kerneopgave for et Security Tech Space er at fungere som videns- og rådgivningscenter, hvor forskellige aktiviteter kan iværksættes. Det er særligt vigtigt at kunne yde rådgivning til SMV'er om forhold, der vedrører cyber- og informationssikkerhed eksempelvis gennem et døgnbemandet ressourcecenter. Med et Security Tech Space suppleres initiativer ved at målrette indsatsen til det civile samfund, og herunder særligt livsnerven i dansk økonomi; de mange små og mellemstore virksomheder, for hvem manglende viden, kompetencer og ressourcer kan være en barriere for handling. Cyber- og informationssikkerhed skal anskues som en forretningskatalysator, der medfører en række konkurrencemæssige fordele. Aktiviteter kan desuden omfatte træningsaktiviteter og informationsmøder, der kan bidrage til samfundsdebatten og de politiske beslutningsprocesser.

Ud over ovenstående tre kerneopgaver er det vigtigt for Aarhus og Østjylland at etablere en klar fortælling om markedspotentialet og regionens styrker. Dette vil hjælpe med at tiltrække investorer og samarbejdspartnere samt styrke regionens position inden for cyber- og informationssikkerhed.

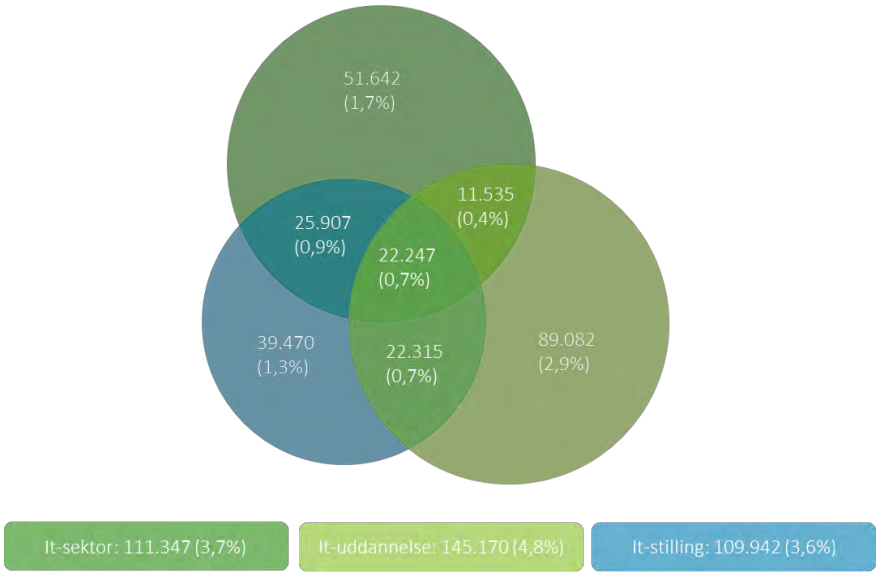
7. Bilag

7.1. Interviewdeltagere

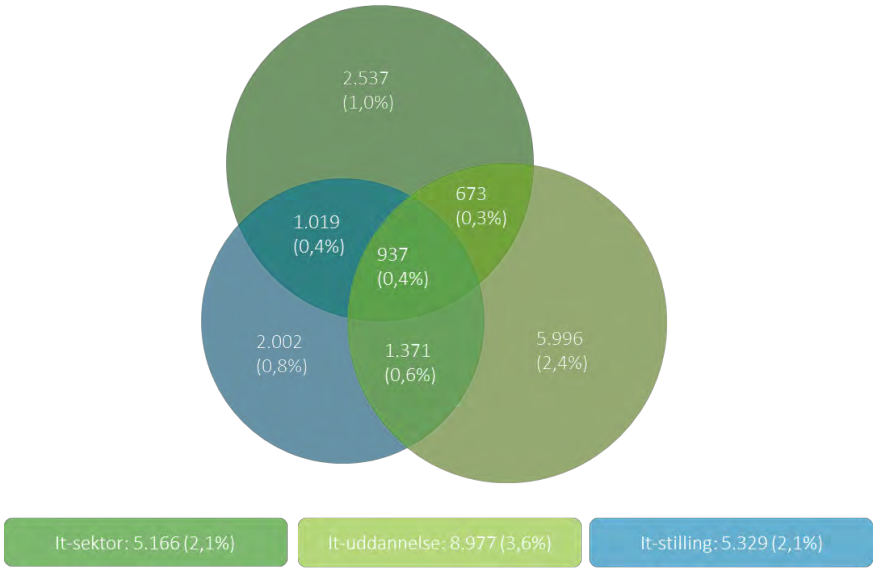
Deltager	Organisation
Kaj Grønbæk	Institut for Datalogi, Aarhus Universitet
Ivan Bjerre Damgård	Institut for Datalogi, Aarhus Universitet
Mikael Bergholz Knudsen	Institut for Elektro- og Computerteknologi, Aarhus Universitet
Jesper Bøhnke	TERMA
Charlotte Møller Andersen	Cryptomathic
Henrik Skovfoged	Trifork
Claudio Orlandi	DIREC
Jakob Pagter	SEPIOR
Kurt Nielsen	Partisia
Birgit Nøhr	DigitalLead
Mai Louise Agerskov	INCUBA
Niels Frimodt Sørensen	Signaturgruppen
Kåre Kjelstrøm	Concordium
Steffen Hofbrandt	TDC Erhverv
Claus Westergaard Jensen	Bankdata
Henrik Christensen Lei	Bankdata
Daniel Milo Farkner	Bankdata
Henrik Skou Pedersen	Erhvervshus Midtjylland
Kasper Sønderdahl	Østjyllands Brandvæsen
Ask Risom Bøge	Erhvervsakademiet Aarhus
Marlene Stidsen	Industriens Fond
Ulrik Ledertoug	Orange Cyberdefense
Lone Juric Sørensen	Aarhus Kommune
Henning Mols	Aarhus Kommune
Marianne Gjerløv	Aarhus Kommune
Christian Brandt Heinel	Cisco

7.2. Figurer

Figur 15. Beskæftigelse på it-arbejdsmarkedet i hele landet, 2021



Figur 16. Beskæftigelse på it-arbejdsmarkedet i Østjylland (fraregnet Aarhus Kommune), 2021



Deloitte.