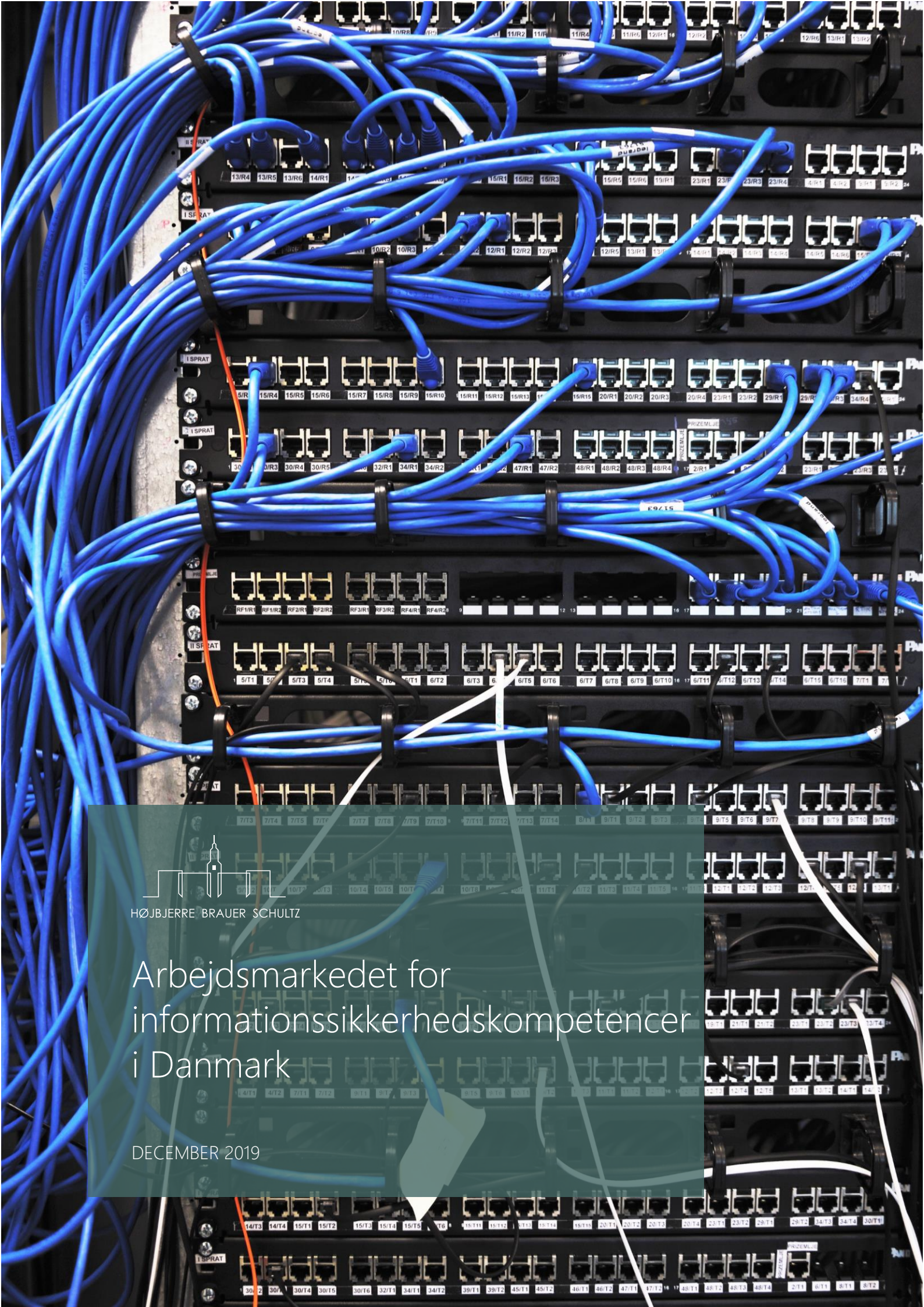


HØJBJERRE BRAUER SCHULTZ

Arbejdsmarkedet for informationssikkerhedskompetencer i Danmark

DECEMBER 2019

Arbejdsmarkedet for informationssikkerhedskompetencer i Danmark

Højbjerre Brauer Schultz
Ny Kongensgade 9B, 1. sal
1472 København K
Tlf. 8181 6262
info@hbseconomics.dk
www.hbseconomics.dk

Indhold

1. Indledning

Det danske samfund bliver i stigende grad digitaliseret. Det gælder på tværs af forretningsområder i virksomheder og i opgaveløsningen hos myndigheder. Med digitalisering følger et behov for informationssikkerhed. For at nå et højt niveau af informationssikkerhed kræver det de rette kompetencer og nok af dem. Behovet for kompetencer er ikke længere begrænset til specialister, men siver ud til en bred vifte af funktioner i virksomhederne og hos myndighederne.

Formålet med denne rapport er at undersøge det danske arbejdsmarked inden for informationssikkerhed. Det sker ved at kortlægge og kvantificere efterspørgsel og udbud efter kompetencer inden for informationssikkerhed. Rapporten sætter fokus på, hvilke konkrete kompetencer, der efterspørges af både myndigheder og virksomheder, og i hvilket omfang udbuddet matcher efterspørgslen. Endeligt undersøges virksomhederne brug af efteruddannelse til opkvalificering af de ansatte, der arbejder med informationssikkerhed.

Som grundlag for rapportens resultater er der etableret et omfattende datagrundlag. De tre væsentligste kilder er (i) efterspørgsel kortlagt og analyseret ud fra 2,4 mio. jobopslag, (ii) en repræsentativ spørgeskemaundersøgelse blandt myndigheder og virksomheder samt (iii) en række interview med relevante myndigheder og virksomheder samt udvalgte uddannelsesinstitutioner.

Anvendte definitioner og forkortelser

Informationssikkerhed (ISK) er en bred betegnelse for de samlede foranstaltninger, der skal sikre information i forhold til fortolighed, integritet (ændring af data) og tilgængelighed. I arbejdet indgår blandt andet organisering af sikkerhedsarbejdet, påvirkning af adfærd, processer for behandling af data, styring af leverandører samt tekniske sikringsforanstaltninger.

Cybersikkerhed omfatter beskyttelse mod de sikkerhedsbrud, der opstår som følge af angreb mod data eller systemer via en ekstern net- eller systemforbindelse. Arbejdet med cybersikkerhed fokuserer således på sårbarheder ved sammenkoblingen af systemer, herunder forbindelser til internettet.

IT-sikkerhed (ITS) er den delmængde af informationssikkerhed, der vedrører IT-systemer. Ved IT-systemer forstås software såvel som hardware – både uafhængig og forbundet i netværk.

I rapporten anvendes informationssikkerhed som en samlende betegnelse for ovenstående begreber.

Rapporten er udarbejdet på opdrag af Erhvervsstyrelsen, Digitaliseringsstyrelsen, Center for Cybersikkerhed samt Uddannelses- og Forskningsministeriet.

Den er udarbejdet af partner Martin Brauer, partner Andreas Højbjerre, seniorkonsulent Christoffer Ramsdal Hansen, konsulent Nicoline Lund Dahl, alle Højbjerre Brauer Schultz, samt Lektor og Head of Cyber Security Section Christian Damsgaard Jensen, Danmark Tekniske Universitet og konsulent Hanne Shapiro, Hanne Shapiro Futures. Ansvar for eventuelle fejl og mangler ligger hos Højbjerre Brauer Schultz.

København, november 2019.

2. Resumé og anbefalinger

Danmark har et højt digitaliseringsniveau, som ikke afspejles i virksomhedernes adfærd vedr. informationssikkerhed. Især blandt SMV'er er der virksomheder, der har et lavt niveau. Behovet for kompetencer inden for informationssikkerhed skal også ses i lyset af den stigende cybertrussel – en udvikling, der forventes at fortsætte.

Udviklingen i IT-kriminalitet og en dybere IT-integration i virksomhedernes processer stiller krav om øget bevågenhed og fokus på et velfungerende arbejdsmarked, som kan sikre virksomhederne den rette forsyning af kompetencer.

Denne rapport har til formål at kortlægge efterspørgsel og udbud af kompetencer inden for informationssikkerhed på arbejdsmarkedet og afdække eventuelle ubalancer herimellem. Rapporten peger derudover på områder, hvor der er behov for at fortsætte arbejdet med at skabe et bedre match mellem myndighedernes og virksomhedernes behov for informationssikkerhedskompetencer og udbuddet heraf.

Rapporten analyserer virksomheders og myndigheders behov for og udbuddet af kompetencer inden for informationssikkerhed. Der er altså tale om en bred vifte af kompetencer fra organisatoriske og juridiske kompetencer til meget IT-tekniske kompetencer.

2.1 Hovedresultater

Rapportens resultater er baseret på et omfattende datagrundlag. Det omfatter bl.a. en registerbaseret analyse af udviklingen i beskæftigelse og uddannelser, en systematisk kortlægning og tekstanalyse af ca. 2,4 mio. relevante jobopslag fra 2008-2018, survey-besvarelser fra ca. 1.300 virksomheder og myndigheder samt 10 kvalitative dybdegående interview. Analyserne har ledt til følgende hovedresultater:

- **Markant stigning i efterspørgslen efter kompetencer vedr. informationssikkerhed.** Arbejdsmarkedet for informationssikkerhed (ISK) udgør knap 2 pct. af den samlede efterspørgsel i Danmark, målt ved jobopslag. Efterspørgslen efter ISK-kompetencer er tredoblet de sidste 10 år, og den er steget mere end for andre personalegrupper. Efterspørgslen er større, end man ser inden for andre digitale jobfunktioner, og funderet bredt i mange brancher.
- **Størst efterspørgsel efter tekniske kompetencer.** Efterspørgslen er steget for alle jobprofiler inden for ISK-området. Efterspørgslen er størst for de mere tekniske jobprofiler, der beskytter virksomheden mod angreb, forebygger IT-nedbrud, udvikler sikre IT-systemer og vedligeholder dem. Fokus på regler om databeskyttelse (GDPR) har dog fra 2016 og frem øget efterspørgslen efter jobprofiler, der arbejder med jura og databeskyttelse.
- **Få egentlige ISK-uddannelser.** Der er kun identificeret syv videregående uddannelser, som tilbyder et højt indhold af informationssikkerhed svarende til mindst 30 ECTS-point. Heraf har kun én uddannelse et højt indhold af informationssikkerhed i de obligatoriske kurser. I alt er der fundet 32 uddannelser, hvor det er muligt at tage et kursus i informationssikkerhed. Mindre end 1 pct. af den samlede arbejdsstyrke har taget en uddannelse relateret til informationssikkerhed, hvoraf 8 ud af 10 er IT-uddannelser. Mange af disse personer vil arbejde inden for andre brancher, da informationssikkerhed kun indgår som en del af deres uddannelse.
- **Mange i ISK-jobs uden en ISK-relateret uddannelse.** Det skønnes, at knap 20.000 personer arbejder i et job med et ISK-indhold. Rapporten skønner, at under 10 pct. af dem, som arbejder i et ISK-job, har en ISK-relateret uddannelse bag sig. Dermed opnår relativt få deres ISK-kompetencer gennem det ordinære uddannelsessystem. Virksomheder og myndigheder bruger

derimod oplæring og specialisering på arbejdspladsen, private kurser eller interne opkvalificeringsforløb. Knap 70 pct. af virksomhederne inden for *Information og kommunikation* anvender intern oplæring, der er det mest anvendte middel til opkvalificering.

- **Store rekrutteringsudfordringer**. Godt 20 pct. af organisationer, der har forsøgt at rekruttere ISK-arbejdskraft, har enten ikke kunnet ansætte eller har måttet ansætte en profil, som ikke havde alle af de ønskede kompetencer. På de tekniske dele af arbejdsmarkedet, herunder brancherne *Information og kommunikation* samt *Finansiering og forsikring*, er udfordringerne større. Her er det 30 pct. af organisationerne, som har forgæves rekrutteringer, når de forsøger at ansætte ISK-arbejdskraft.
- **Forventning om et voksende udbud af ISK-kompetencer.** Frem mod 2030 vil forventede ændringer i sammensætningen af de ordinære, videregående uddannelser øge udbuddet af personer med ISK-relevante uddannelser. Rapporten estimerer, at antallet af personer i arbejdsstyrken med en ISK-relevant uddannelse vil vokse med ca. en tredjedel. Af dem vil knap 9 ud af 10 være inden for Informations- og kommunikationstekniske (IKT) uddannelser, fx dataloger.
- **Forventning om en kraftigt stigende efterspørgsel.** Flere indikatorer peger på, at efterspørgslen efter arbejdskraft med kompetencer inden for informationssikkerhed vil stige. Forsætter de seneste års udvikling i efterspørgslen, skal der frem mod 2030 besættes 13.000 flere ISK-jobs end i dag. Det betyder, at ISK-arbejdsmarkedet vil vokse fra ca. 20.000 til 33.000 beskæftigede.
- **Risiko for intensiverede rekrutteringsudfordringer.** På trods af at udbuddet af ISK-kompetencer forventeligt vil stige i lyset af et øget optag på bl.a. IT-uddannelserne, er det sandsynligt, at rekrutteringsudfordringerne intensiveres frem mod 2030, da mange ISK-relaterede uddannelser også fungerer som fødekanal til andre IT-specialistjobs. Dertil kommer, at efterspørgslen også forventes at stige fremadrettet.

Samlet set peger resultaterne af denne rapport på, at rekrutteringsudfordringer allerede i dag udgør en barriere for virksomheders og myndigheders aktiviteter – og at de sandsynligvis vil blive intensiveret. ISK-arbejdsmarkedet udvikler sig kraftigt i disse år. Dette udfordrer arbejdet fra offentlig side med at *time* og dosere de rette tiltag. Især udfordrer følgende usikkerheder arbejdet med at udforme tiltag og aktiviteter:

- **Stigende efterspørgsel.** Der er fortsat tegn, på at virksomheder og myndigheder ikke fuldt ud har erkendt deres behov for ISK-arbejdskraft, og at deres investeringer i informationssikkerhed ikke er fulgt med i samme omfang som den øvrige digitalisering. Det gælder især SMV'er. En professionalisering af informationssikkerhed i især SMV'er kan øge omfanget og ændre efterspørgslen yderligere, ud over, hvad der er identificeret i denne rapport.
- **Øget specialisering**. ISK-arbejdsmarkedet i Danmark er fortsat ikke lige så specialiseret som i andre lande. Mange virksomheders og myndigheders kompetencebehov dækkes ofte af medarbejdere, som ikke er specialiseret inden for informationssikkerhed, men som typisk har det som en del af deres arbejdsopgaver. Øget bevidsthed på området og en dybere integration af IT i forretningskritiske processer kan øge efterspørgslen efter arbejdskraft, der har mere specialiserede ISK-kompetencer.
- **Relativt nyt ISK-indhold**. Udbuddet af informationssikkerhed er relativt nyt på mange uddannelser.
- **Mange relevante tiltag allerede igangsat**. En række relevante initiativer er for nyligt sat i søen blandt andet i regi af den Nationale Strategi for Cyber- og Informationssikkerhed, Danish Hub for Cyber Security, Teknologipagten, Cyber Security Challenge og Virksomhedsrådet for IT-sikkerhed. De tiltag vil i de kommende år sandsynligvis styrke arbejdet på informationssikkerhedsområdet, men omfanget af konkrete tiltag og effekten af disse er fortsat usikker.

2.2 Resultaterne peger på tre indsatsområder

Med udgangspunkt i ovenstående usikkerhedsmomenter vurderes det relevant, at der fra offentlig side arbejdes videre inden for tre centrale indsatsområder:

INDSATSOMRÅDE 1. AFHJÆLP DE AKTUELLE REKRUTTERINGSUDFORDRINGER

- **Understøt, at rekrutteringsudfordringer mindskes**. Virksomheder og myndigheder oplever rekrutteringsudfordringer i forhold til at besætte ISK-jobs. De rette kompetencer er både en forudsætning for et højt niveau af informationssikkerhed og en forudsætning for at realisere de samfundsøkonomiske gevinster ved digitalisering. Relevante myndigheder bør fortsat understøtte, at rekrutteringsudfordringerne mindskes – med særligt fokus på informationssikkerhedsområdet.
- **Anvend offentlig voksen- og efteruddannelse (VEU) aktivt.** VEU kan være en vej til at øge udbuddet af ISK-kompetencer på den korte bane. Der er allerede igangsat indsatser, som skal styrke det videregående VEU-udbud, herunder Arbejdsgruppen for udvikling af videregående VEU samt analyser igangsat af Uddannelses- og Forskningsministeriet. Det bør sikres, at dette arbejde fokuserer på virksomheders og myndigheders behov for opkvalificering af kompetencer vedr. informationssikkerhed. Der kan med fordel foretages en afdækning af om og hvordan offentlig VEU kan bidrage til bedre ITS-kompetenceudvikling.
- **Offentlig VEU kan ikke alene løse behovet for tekniske kompetencer**. Rapporten viser, at offentlig VEU bruges i mindre grad inden for de tekniske jobfunktioner i ISK-arbejdsmarkedet. Her anvender organisationerne primært specifikke private uddannelsestilbud (certificeringer). Interviewene peger på, at den faglige udvikling inden for informationssikkerhed sker hurtigt og er så kompleks, at det er usikkert, om det offentlige VEU-system kan agere tilstrækkeligt agilt til at løse organisationernes behov på det tekniske område. Her er løbende opkvalificering via private kurser en vigtig forudsætning for, at virksomhederne får adgang til de rette kompetencer. Samtidig giver de offentlige uddannelser giver det større overblik og tillader en samlet forståelse af de specifikke teknologier. Det bør overvejes, hvordan man understøtter, (i) at virksomheder og myndigheder kan finde det rette private udbud, (ii) at der i virksomheder og myndigheder arbejdes systematisk med en opkvalificering, (iii) at samspillet med virksomhederne tænkes ind i de ordinære uddannelser, fx i form af karriereveje ind i jobfunktioner inden for informationssikkerhed, samt (iv) at de videregående uddannelsesinstitutioner spiller en større rolle, da det er her man kan få uvildig og produktuafhængig efteruddannelse.

INDSATSOMRÅDE 2. FØLG OG UNDERSTØT UDVIKLINGEN PÅ ARBEJDSMARKEDET

- **Følg udviklingen på arbejdsmarkedet tæt**. Arbejdsmarkedet for informationssikkerhed er forholdsvist nyt og under hastig forandring. I denne udvikling er der risiko for et voksende mismatch mellem udbud og efterspørgsel – ikke mindst for specialistfunktioner. De ansvarlige myndigheder og andre relevante aktører bør derfor følge udviklingen i efterspørgslen nøje for at kunne understøtte denne bedst muligt.
- **Anvend NICE-framework til opbygning af systematisk overvågningssystem.** Kompetencebehovene på området kan være diffuse for både virksomheder og myndigheder. Internationale analyser peger således på et behov for en formel forståelse af, hvad der udgør informationssikkerhedsjob, og hvad der karakteriserer kompetencekravene til dem. Rapportens bearbejdning af NICE-rammeværket til danske forhold kan danne udgangspunkt for et arbejde med en bedre forståelse af ISK-arbejdsmarkedet. Det kan også strukturere virksomheders og myndigheders tilgang til kortlægning af behovet for ISK-arbejdskraft og -kompetencer. NICE-rammeværket er i andre lande (fx USA, Storbritannien og Canada) omsat til et monitoreringssystem. Dette værktøj giver individer, uddannelsesinstitutioner og policy-aktører mulighed for at følge udviklingen på

ISK-jobmarkedet vha. en analyse af elektroniske jobopslag[1]. Værktøjet kan anvendes til både at styrke og strukturere virksomheders og myndigheders erkendelse af kompetencebehov, men vil også kunne understøtte en dynamisk justering af det eksisterende udbud af både VEU og ordinære uddannelser.

- **Understøt den digitale udvikling.** I offentligt regi understøtter man på forskellige måder virksomhedernes digitale udvikling, fx i Innovationsnetværk Danmark Programmet og i SMV:Digital. Det bør sikres, at ISK fortsat prioriteres højt i dette arbejde, fx ved at der på tværs af netværkene tilbydes ISK-relevante aktiviteter eller at det i højere grad tænkes ind i det offentlige udbud.

INDSATSOMRÅDE 3. TILPASNING AF UDBUDDET AF ISK-KOMPETENCER PÅ LÆNGERE SIGT

- **Undersøg, hvordan informationssikkerhedsuddannelserne modtages på arbejdsmarkedet.** Som nævnt er der en række usikkerhedsmomenter, som vil præge udviklingen i efterspørgslen efter ISK-kompetencer i de kommende år. Både med hensyn til omfang og karakter. Hertil kommer, at ISK-indholdet i mange uddannelser fortsat er nyt, og det er usikkert, hvordan de vil blive modtaget på arbejdsmarkedet. Det bør derfor overvejes, om der er behov for nærmere at følge de dimittender, som har gennemført en videregående uddannelse relateret til informationssikkerhed. Derved kan oplevet relevans afdækkes, både ud fra virksomhedernes og dimittendens perspektiv. Resultaterne herfra kan danne grundlag for eventuelle justeringer og igangsætning af ISK-specifikke tiltag inden for de videregående uddannelser
- **Evaluer igangsatte tiltag, som øger optaget på relevante uddannelser**. Der er allerede igangsat mange tiltag med fokus på at udvide optaget på IT-uddannelser, fx understøttet i Teknologipagten, der bl.a. fremmer udbuddet af STEM-kompetencer. En central opgave bliver at vurdere virkningen heraf, fx om det resulterer i et øget udbud inden for de uddannelser, som er fødekanaler for ISK-arbejdsmarkedet.
- **Monitorér løbende tekniske minimumsstandarder.** På det tekniske område viser rapporten, at virksomhederne og myndigheder ofte efterspørger dygtige IT-uddannede med høj teknisk kunnen, men at virksomhederne selv står for opkvalificering af virksomhedsspecifik ISK-domæneviden. Det stiller krav til det tekniske niveau i de IT-uddannelser generet, som ofte udgør fødekilden til ISK-jobs. En løbende overvågning af, om det tekniske niveau på mere generelle IT-uddannelserne lever op til virksomhedernes behov, kan være en vej til at understøtte, at udbuddet af kompetencer matcher virksomheders og myndigheders efterspørgsel.

Rapporten er struktureret i otte kapitler. Indledning, resume og anbefalinger er i kapitel 1 og 2. I kapitel 3 beskrives den overordnede efterspørgsel i Danmark og branchernes efterspørgsel kortlægges. I kapitel 4 fokuseres på specifikke kompetencer ved at opdele efterspørgslen i syv overordnede kompetenceprofiler, der alle arbejder med informationssikkerhed. I kapitel 5 kortlægges uddannelser relateret til informationssikkerhed. I kapitel 6 undersøger vi rekrutteringssituationen for informationssikkerhedskompetencer samt vurderer, hvad det fremtidige behov er. I kapitel 7 er fokus på virksomheders og myndigheders brug af opkvalificering og efteruddannelse til at dække behovet for kompetencer. Endelige indeholder kapitel 8 en beskrivelse af metoden, der ligger til grund for rapportens resultater.

[1] I Holland har man derimod gennemført et review af flere rammeværk og på den baggrund udviklet et såkaldt metarammeværk kaldet Cyber Cube. Se https://www.tno.nl/en/focus-areas/defence-safety-security/roadmaps/national-security/the-dutch-cyber-cube-method-improving-human-capital-for-socs-and-csirts/

3. Efterspørgslen efter informationssikkerhed

Afsnittets hovedresultater

- Efterspørgslen efter kompetencer inden for informationssikkerhed er tredoblet i det seneste årti.
- Efterspørgslen er steget både i antal og som andel af den samlede efterspørgsel efter arbejdskraft. I 2008 blev der efterspurgt informationssikkerhedskompetencer i godt 1.700 jobopslag, svarende til 0,6 pct. af alle jobopslag, mens der i 2018 blev efterspurgt informationssikkerhedskompetencer i godt 5.000 jobopslag, svarende til 1,8 pct. af alle jobopslag.
- På trods af den stigende efterspørgsel er personer med informationssikkerhedskompetencer en forholdvis lille faggruppe i Danmark. I 2018 udgjorde informationssikkerhedsjobopslag mindre end 2 pct. af den samlede efterspørgsel efter arbejdskraft. Men faggruppen er voksende i forhold til andre faggrupper, fx IT-ansatte generelt.
- Den stigende efterspørgsel efter informationssikkerhedskompetencer er bredt funderet i dansk erhvervsliv. Efterspørgslen er dog højest i IKT-branchen.
- I den offentlige sektor er efterspørgslen efter informationssikkerhedskompetencer klart størst i de statslige institutioner, herefter følger kommunerne og regionerne.
- Virksomheder med mere end 250 ansatte har i højere grad kompetencer inden for informationssikkerhed tilstede på arbejdspladsen end virksomheder med færre end 10 ansatte. Generelt stiger sandsynligheden for at have ISK-kompetencer på arbejdspladsen med virksomhedens størrelse.
- Organisationer i Region Hovedstaden har den højeste efterspørgsel efter informationssikkerhedskompetencer, men den stigende tendens i efterspørgslen er gældende for hele landet.

Efterspørgslen efter informationssikkerhedskompetencer er en indikator for, hvor stort behovet for arbejdskraft med kompetencer inden for informationssikkerhed er. Især udviklingen i efterspørgslen kan frembringe viden om, hvorvidt det er et arbejdsmarked i vækst. Forskelle i efterspørgslen mellem sektorer eller brancher afdækker forskelle i behovet for og fokus på informationssikkerhed. En naturlig måde at opgøre efterspørgslen på er at kigge på, hvilke konkrete kompetencer der efterspørges i jobopslag.

3.1 Det overordnede billede

I dette afsnit sætter vi først fokus på den overordnede udvikling i efterspørgslen efter ISK-kompetencer. Dernæst dykker vi ned i ISK-efterspørgslen for udvalgte faggrupper.

EFTERSPØRGSLEN EFTER ISK-KOMPETENCER ER TREDOBLET

Efterspørgslen efter arbejdskraft med ISK-kompetencer er stigende. I 2018 blev der slået godt 5.000 stillinger op, hvor der blev efterspurgt ISK-kompetencer. Det er næsten en tredobling i forhold til antallet af ISK-jobopslag i 2008, hvor ISK-kompetencer var efterspurgt i godt 1.700 opslag, jf. figur 3.1.

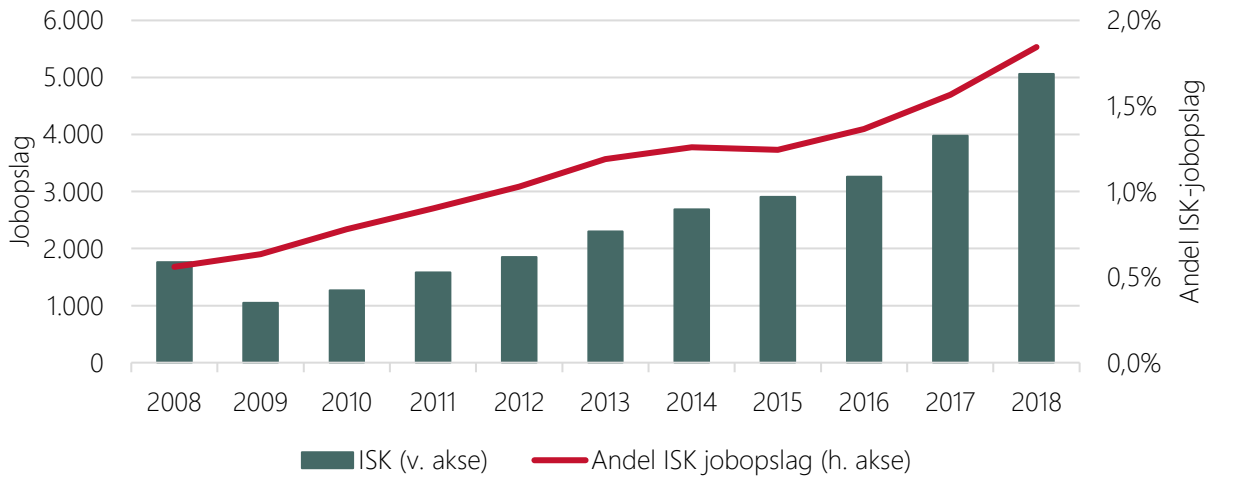
Efterspørgslen efter ISK-kompetencer stiger mere end den samlede efterspørgsel efter arbejdskraft. I 2008 blev der efterspurgt ISK-kompetencer i 0,6 pct. af alle jobopslag, og i 2018 lå den tilsvarende andel på 1,8 pct. Dermed udgør efterspørgslen efter ISK-kompetencer en stigende andel af den samlede efterspørgsel, jf. figur 3.1.

Denne tendens er ikke særskilt for Danmark, men også gældende for andre lande. Ser vi fx på USA, som er toneangivende inden for informationssikkerhed, finder vi også her en stigende efterspørgsel. Konkret er antallet af ISK-jobopslag i USA næsten fordoblet siden 2013, hvilket er samme udvikling, som vi ser i Danmark. Antallet af øvrige IT-jobopslag i USA er vokset med 30 pct. i samme periode[2]. Således udgør efterspørgslen efter informationssikkerhed en stigende andel af den samlede efterspørgsel efter IT-arbejdskraft i USA.

I løbet af det seneste årti er der kommet langt større fokus på informationssikkerhed, hvilket udtrykker sig i den voksende efterspørgsel efter arbejdskraft med ISK-kompetencer. Siden 2008 er antallet af ISK-jobopslag steget kontinuerligt (bortset fra et lille fald i forbindelse med finanskrisen i 2009) og mere end den generelle efterspørgsel i alle år.

Figur 3.1 Efterspørgslen efter ISK-kompetencer er stigende

Udvikling i ISK-jobopslag



Kilde: HBS Jobindex
Anm.: Andelen af ISK-jobopslag er beregnet som andelen af alle jobopslag.

Hvordan har vi identificeret efterspørgslen efter informationssikkerhed?

Efterspørgselsanalysen er foretaget på baggrund af godt 2,4 mio. jobopslag i Danmark i perioden 2008-2018. Alle jobopslag er gennemlæst ved brug af tekstanalyse. Derefter er alle jobopslag, hvor der efterspørges ISK-kompetencer, kategoriseret som et ISK-jobopslag. Se afsnit 8 for uddybende information.

ISK-efterspørgselsintensitet
I afsnittet anvendes begrebet 'ISK-efterspørgselsintensitet' – det er et mål for antallet af ISK-jobopslag relativt til det samlede antal jobopslag i en given jobopslagspopulation.

Efterspørgslen efter ISK-kompetencer er altså steget både absolut og relativt til det samlede antal jobopslag. Det er et udtryk for, at danske arbejdspladser har øget deres fokus på informationssikkerhed og derfor i højere grad har behov for arbejdskraft, der besidder kompetencer inden for ISK. Den stigende efterspørgsel skal ses i lyset af større fokus på IT-sikkerhedstrusler såsom malware og datatyveri[3]. Denne udvikling er sket, til trods for at der er stor variation i organisationers generelle bevidsthed om den forretningskritiske betydning af informationssikkerhed.

Udviklingen i virksomhedernes fokus på informationssikkerhed underbygges af data fra Danmarks Statistik. Ifølge Danmarks Statistik øgede godt hver fjerde virksomhed sine investeringer i informationssikkerhed fra 2014-2015. Analysen viser, at 27 pct. af de danske virksomheder med 10 ansatte eller derover øgede deres investeringer i IT-sikkerhed i 2015, mens 70 pct. af virksomhederne havde uændret niveau fra 2014-2015. I alt havde 82 pct. af de danske virksomheder implementeret IT-sikkerhedsmæssige foranstaltninger i 2015[4].

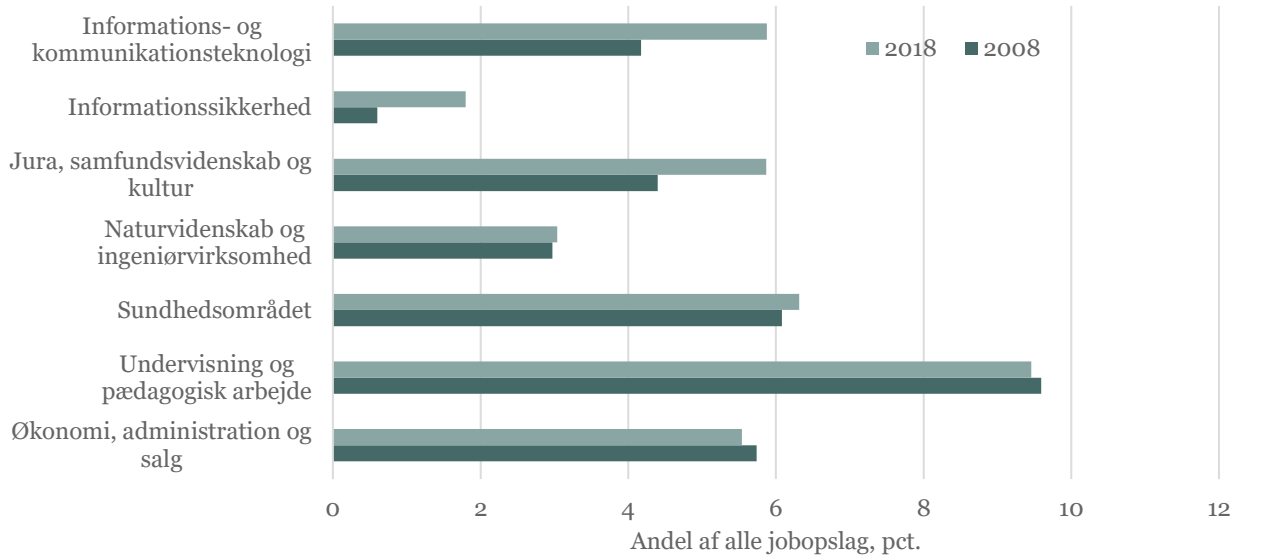
[2] Burning Glass (2019): Recruiting Watchers for the Virtual Walls
[3] Se fx Rambøll (2018): Analyse af data- og cybersikkerhed
[4] Danmarks Statistik (2016): It-anvendelse i virksomheder 2016

STIGENDE EFTERSPØRGSEL – MEN EN FORHOLDSVIS LILLE FAGGRUPPE

På trods af den stigende efterspørgsel er personer med ISK-kompetencer en forholdvis lille faggruppe i Danmark. I 2018 udgjorde ISK-jobopslag mindre end 2 pct. af den samlede efterspørgsel efter arbejdskraft. Til sammenligning udgør efterspørgslen efter personer, der arbejder med viden på højeste niveau inden for fx *Informations- og kommunikationsteknologi* 6 pct. af alle jobopslag. Derudover udgør *Naturvidenskab og ingeniørvirksomhed* 3 pct. af den samlede efterspørgsel, mens *Jura, samfundsvidenskab og kultur* udgør knap 6 pct., jf. figur 3.2.

Figur 3.2 Sammenligning med andre faggrupper på arbejdsmarkedet

Arbejde, der forudsætter viden på højeste niveau inden for pågældende område



Kilde: HBS Jobindex
Anm.: Inddelingen af faggrupper følger den danske fagklassifikation DISCO-08 bortset fra IT-sikkerhed, der følger metoden som beskrevet i dette kapitel, jf. Boks. ISK-jobopslag kan indgå i de nævnte fagklassifikationer fra Danmarks Statistik.

Som beskrevet tidligere er andelen af ISK-jobopslag steget kraftigt i løbet af det seneste årti. Den stigende efterspørgsel er en tendens, der gør sig gældende inden for informations- og kommunikationsteknologi generelt. Således er andelen inden for denne faggrupper steget fra at udgøre ca. 4 pct. af alle jobopslag i 2008 til at udgøre 6 pct. i 2018. Stigningen er imidlertid kraftigst for ISK-faggruppen, hvis andel er tredoblet fra 2008-2018. Til sammenligning har faggruppen *Jura, samfundsvidenskab og kultur* også opleveret en betydelig fremgang i efterspørgslen og er gået fra at udgøre 4,4 til 5,9 pct. af alle jobopslag. For andre faggrupper har efterspørgslen været nogenlunde konstant eller svagt faldende[5].

Ser man på de virksomheder, der helt eller delvist sælger hardware-og softwarebaserede IT-sikkerhedsløsninger og rådgivning om sikkerhed, så er der tale om 263 virksomheder med en omsætning på 6,4 mia. kr. og knap 3.000 fuldtidsbeskæftigende[6]. Således er der tale om et forholdsvist lille erhvev på nuværende tidspunkt i Danmark. Til sammenligning var der i 2018 godt 230.000 fuldtidsbeskæftigede i industrien.

3.2 Branchernes ISK-efterspørgsel

I dette afsnit undersøger vi, hvordan efterspørgslen efter ISK-kompetencer varierer på tværs af brancher, og efterfølgende sætter vi fokus på tre udvalgte dele af samfundet, hvor ISK-kompetencer forventes at spille en særlig rolle: samfundskritiske sektorer, den offentlige sektor og industrien. Tilsammen udgør disse tre dele langt hovedparten af alle myndigheder og virksomheder i Danmark.

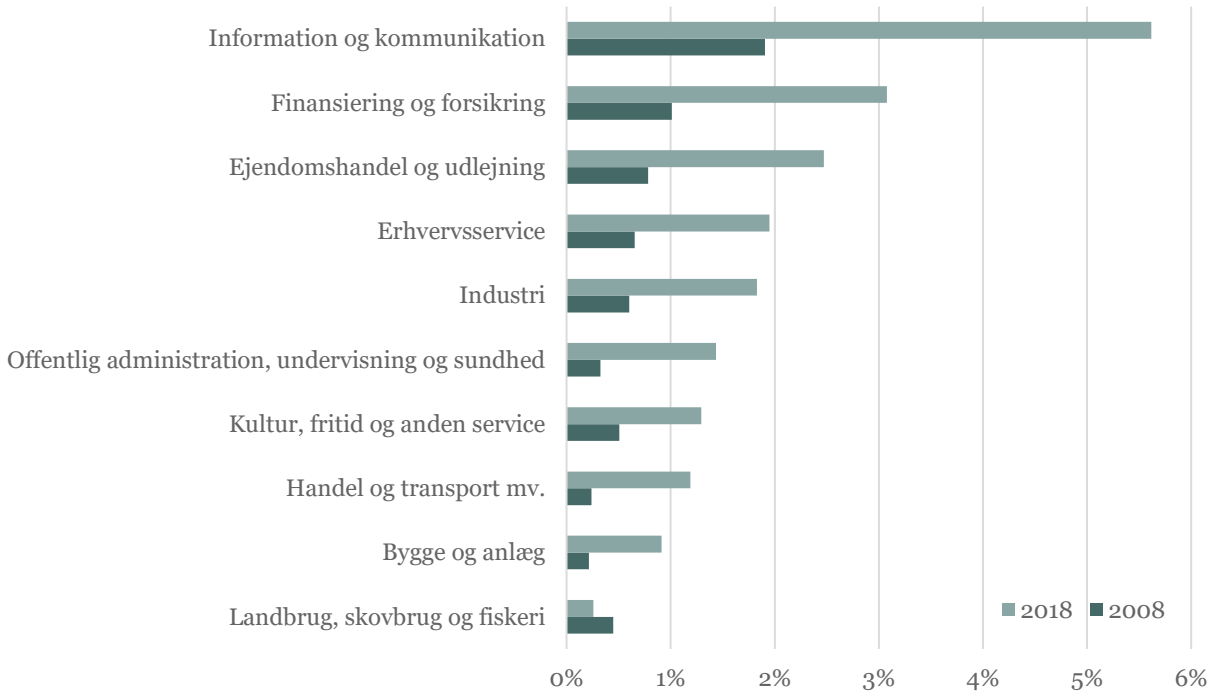
[5] ERST *IT-sikkerhed og databehandling i danske SMV'er* (2018)
[6] DAMVAD Analytics (2018): "Den danske IT-sikkerhedsbranche"

BREDT FUNDERET EFTERSPØRGSEL

Den stigende tendens i efterspørgslen efter informationssikkerhedskompetencer er bredt funderet i dansk erhvervsliv. Men efterspørgslen efter ISK-kompetencer er højest inden for branchen *Information og kommunikation*[7], hvor ISK-jobopslag i 2018 udgjorde knap 6 pct. af alle jobopslag i branchen, jf. figur 3.3. Den relativt høje efterspørgsel efter ISK-kompetencer i branchen *Information og kommunikation* er ikke overraskende, idet branchen omfatter IT-virksomheder generelt, hvor informationssikkerhed i sagens natur er en vigtig funktion. Branchen omfatter også deciderede IT-sikkerhedsvirksomheder, der har gjort IT- og informationssikkerhed til deres forretningsområde.

Finansierings- og forsikringsvirksomheder efterspørger også i høj grad ISK-kompetencer. Det skal ses i lyset af, at bank- og betalingsystemer i dag er digitale, samt den store mængde af følsomme data, som branchen behandler. Godt 3 pct. af alle jobopslag i branchen *Finansiering og forsikring* er ISK-jobopslag, og det er således den branche med den næsthøjeste efterspørgsel efter ISK-kompetencer, jf. figur 3.3.

Figur 3.3 Andel ISK-jobopslag på brancheniveau, 2018



Kilde: HBS Jobindex
Anm.: Jobopslag fra virksomheder med uoplyst branche indgår ikke.

Efterspørgslen efter ISK-kompetencer er i perioden 2008-2018 steget i alle brancher, bortset fra branchen *landbrug, skovbrug og fiskeri*, der i forvejen har en lav efterspørgsel efter ISK-kompetencer. Efterspørgslen efter ISK-kompetencer er steget mest i de brancher, hvor efterspørgslen i forvejen var højest. Det gælder især brancherne *Information og kommunikation*, *Finanasering og forsikring* samt *Offentlig administration, undervisning og sundhed*.

[7] Brancheinddelingen følger Danmarks Statistiks brancheinddeling. Danmarks Statistik anvender Dansk Branchekode DB07, der er en statistisk klassifikation af økonomisk aktivitet.

3.3 Den offentlige sektor

Den offentlige sektor er den første hovedsektor, vi sætter fokus på. Statslige institutioner, regioner og kommuner omfatter offentlige institutioner med betydning for landets sikkerhed og borgernes trivsel og velbefindende. Og store dele af opgaveløsningen og kommunikationen er digitaliseret. Det giver en øget afhængighed af digitale løsninger og dermed en øget sårbarhed overfor cybertruslen. I dette afsnit afdækker vi, i hvilket omfang statslige institutioner, regioner og kommuner efterspørger ISK-kompetencer.

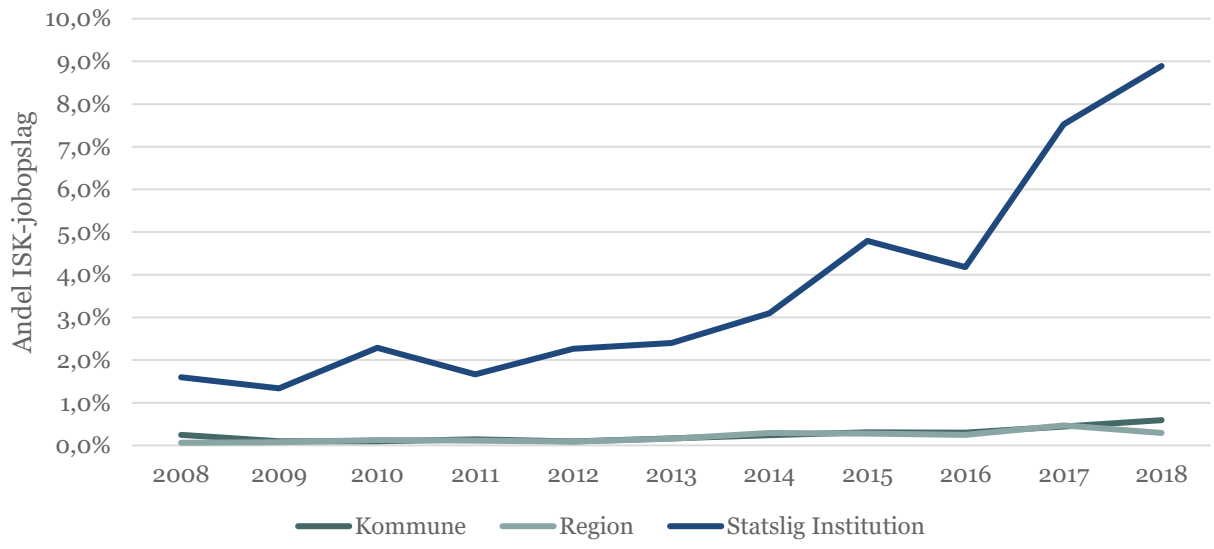
STATSLIGE INSTITUTIONER HAR KLART STØRST EFTERSPØRGSEL EFTER ISK-KOMPETENCER

Knap 9 pct. af alle jobopslag i 2018 fra statslige institutioner kan relateres til informationssikkerhed. Dermed ligger efterspørgslen i staten på et højt niveau. Betydeligt højere end for virksomheder og myndigheder generelt, der som helhed ligger på knap 2 pct. Men også højere end branchen *Information og kommunikation*, der ellers er den branche med den højeste efterspørgsel, jf. afsnit 3.2.

Den høje efterspørgsel er især drevet af en tiltagende efterspørgsel i politiet og forsvaret. Efterspørgslen er også høj i IT-tunge ministerier og styrelser som fx Statens IT, Skatteforvaltningen og Danmarks Statistik. En lange række andre statslige institutioner efterspørger også ISK-kompetencer – om end på et lavere niveau end for de førnævnte myndigheder. Set over de seneste år er andelen af ISK-jobopslag i staten steget med knap 6 pct. point i perioden 2014-2018, jf. figur 3.4.

Figur 3.4 Statslige institutioner efterspørger oftere ISK-kompetencer

ISK-efterspørgselsintensitet for statslige institutioner, kommuner og regioner



Kilde: HBS Jobindex

Den høje og stigende efterspørgsel efter ISK-kompetencer i statslige institutioner skal ses i lyset af et øget fokus på informationssikkerhed. I 2014 blev den første nationale strategi for cyber- og informationssikkerhed lanceret, hvor målet bl.a. var at hæve niveauet for det statslige cyber- og informationssikkerhedsarbejde. I strategien indgik blandt andet krav om implementering af den internationale sikkerhedsstandard iso27001 og krav om et systematisk og professionelt tilsyn med informationssikkerheden i staten.

I strategien for cyber- og informationssikkerhed fra 2018 blev der stillet yderligere krav til de statslige institutioner. Herunder blev alle statslige myndigheder omfattet af minimumskrav for arbejdet med cyber- og informationssikkerhed. Minimumskravene er både tekniske og organisatoriske og skal understøtte en ensartet tilgang til arbejdet samt sikre et tilstrækkeligt højt niveau for beskyttelse mod cyber- og informationssikkerhedshændelser.

I regionerne og kommunerne ligger efterspørgslen efter ISK-kompetencer på et noget lavere niveau sammenlignet med både staten og den generelle efterspørgsel for virksomheder og myndigheder. Således kan 0,3 pct. af jobopslagene i regionerne henføres til kompetencer vedrørende informationssikkerhed, mens det tilsvarende tal for kommunerne er 0,6 pct. Set over det seneste årti har der været en svagt stigende tendens i ISK-efterspørgslen for både kommuner og regioner – men niveauet er fortsat lavt.

Den lave efterspørgsel efter ISK-kompetencer er et udtryk for, at regioner og kommuner i mindre omfang rekrutterer personer med ISK-kompetencer. Det kan afspejle, at mange jobfunktioner i regioner og kommuner kræver andre typer af arbejdskraft som fx pædagoger, lærer og sygeplejersker, der alle er store faggrupper og derfor fylder meget. Samtidig er det faggrupper, hvor udførslen af arbejdet – relativt set – i mindre grad beror på digitale løsninger.

Derudover kan det også være et udtryk for, at regioner og kommuner anvender eksterne underleverandører til håndtering af IT-funktioner, herunder informationssikkerhed. Et eksempel er gymnasier, der indgår i et IT-fællesskab, hvor én værtsinstitution står for IT-infrastrukturen og dermed sikkerheden for fællesskabet. Tilsvarende kan institutioner og myndigheder hyre private virksomheder til at varetage IT-driften og sikkerheden. Endelig kan en lav efterspørgsel også være udtryk for et manglende kendskab til og bevidsthed om behovet for informationssikkerhed.

3.4 Samfundskritiske sektorer

De samfundskritiske sektorer er fokuspunkt i analysen. Den nationale strategi for cyber- og informationssikkerhed[8] identificerer seks samfundskritiske sektorer, der har særlig betydning for cyber- og informationssikkerheden i Danmark. De samfundskritiske sektorer kan bestå af både myndigheder og virksomheder og er givet ved[9]:

- Finanssektoren, dækker bl.a. over pengeinstitutter og forsikringsselskaber (fx Danske Bank, TopDanmark Forsikring og Nets Denmark).
- Telesektoren, dækker over telekommunikation, herunder fastnetbaseret, trådløs og satellitbaseret telekommunikation (fx TDC, Telia og Viasat).
- Transportsektoren, dækker over landtransport, luftfart og kurertjenester (fx DSB, SAS, Banedanmark og PostNord).
- Energisektoren, dækker over produktion, transmission, distribution og handel med elektricitet (fx Ørsted, EnergiNet, SEAS og Modstrøm).
- Søfart, dækker skibsfart (fx Mærsk, DFDS og Scandlines).
- Sundhedssektoren, dækker bl.a. over hospitaler, praktiserende læger, tandlæger, fysioterapeuter, psykologer og kiropraktorer.

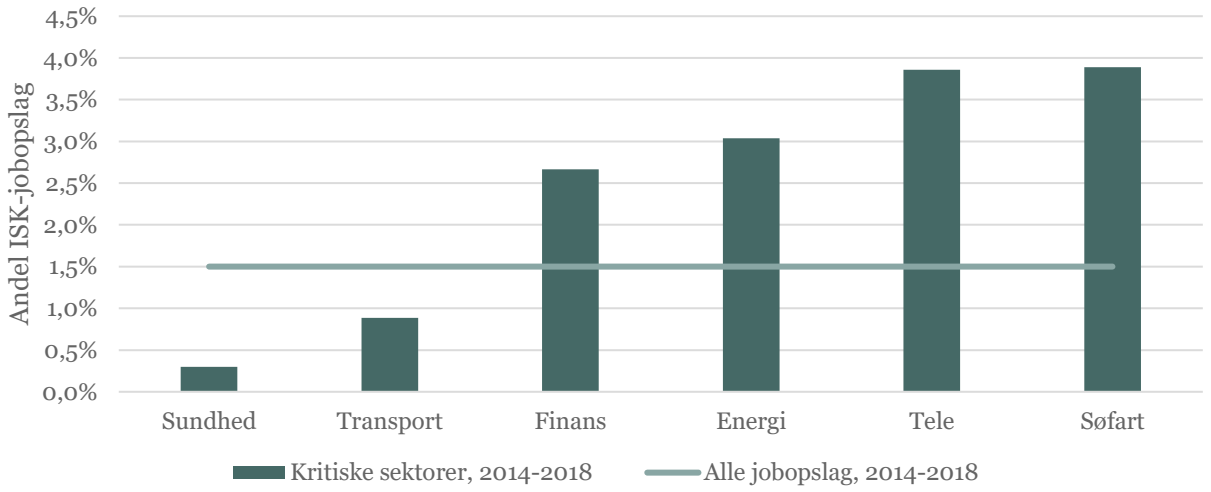
I dette afsnit undersøger vi, i hvilket omfang de seks sektorer efterspørger ISK-kompetencer.

Søfart og telesektoren er de to samfundskritiske sektorer, der i gennemsnit har haft den højeste ISK-efterspørgselsintensitet for perioden 2014-2018. Derudover er ISK-efterspørgslen også høj i henholdsvis finans- og energisektoren, jf. figur 3.5. I ca. 3-4 pct. af jobopslagene for de samfundskritiske sektorer søfart, energi, tele og finans efterspørger arbejdsgiverne ISK-kompetencer, hvilket er et godt stykke højere end gennemsnittet på 1,5 pct. for det samlede arbejdsmarked i samme periode.

[8] Se: https://www.fm.dk/publikationer/2018/national-strategi-for-cyber-og-informationssikkerhed
[9] De samfundskritiske sektorer er afgrænset ved brug af Dansk Branchekode (DB07), jf. metodebeskrivelsen.

Figur 3.5 Sundhed og transport har relativt få ISK-jobopslag

ISK-efterspørgselsintensiteter, gennemsnit for perioden 2014-2018



Kilde: HBS Jobindex

Sundhedssektoren er dén samfundskritiske sektor med den laveste ISK-efterspørgselsintensitet. Kun i 0,3 pct. af jobopslagene i sundhedssektoren efterspørger arbejdsgiverne ISK-kompetencer. Det skal ses i lyset af, at efterspørgslen efter ansatte med ISK-kompetencer i regionerne generelt er relativt lav, jf. afsnit 3.3 om den offentlige sektor. En stor del af opgaveløsningen i sundhedssektoren beror på IT-systemer med personfølsomme oplysninger om borgerne i Danmark. Det gør sundhedssektoren sårbar over for cybertruslen. Det bekræftes af den seneste trusselsvurdering fra Center for Cybersikkerhed fra 2018. Her fremgår, at danske forskningsresultater, patientdata og driften af sygehusene risikerer at blive mål for cyberangreb. Center for Cybersikkerhed vurderer også, at det er meget sandsynligt, at fremmede stater har hensigt og kapacitet til at udføre cyberspionage mod den danske sundhedssektor[10].

Transportsektoren har også en lavere ISK-efterspørgselsintensitet end landsgennemsnittet. Det kan være problematisk, hvis den lave efterspørgselsintensitet i transportsektoren er udtryk for, at sektoren ikke har et tilstrækkeligt fokus på at beskytte sig mod cybertruslen. Informationssikkerhed er også i stigende grad vigtig for transportsektoren. Fly, biler og tog er i stigende grad forbundet med eller styret af IT-systemer – en udvikling, der øger branchens sårbarhed. Ifølge den seneste trusselsvurdering fra Center for Cybersikkerhed fra 2018 er der en væsentlig trussel mod den danske transportsektor. Truslen kommer især fra cyberkriminalitet, hvor trusselsniveauet ifølge CFCS' vurdering er meget højt[11].

Det er vigtigt at bemærke, at det ikke nødvendigvis er et problem med en lav efterspørgsel efter informationssikkerhedskompetencer til trods for en høj trusselsvurdering. Det er således muligt, at sektorerne enten har eksterne leverandører til at varetage sikkerheden, eller at de allerede har de nødvendige kompetencer.

3.5 Industrien

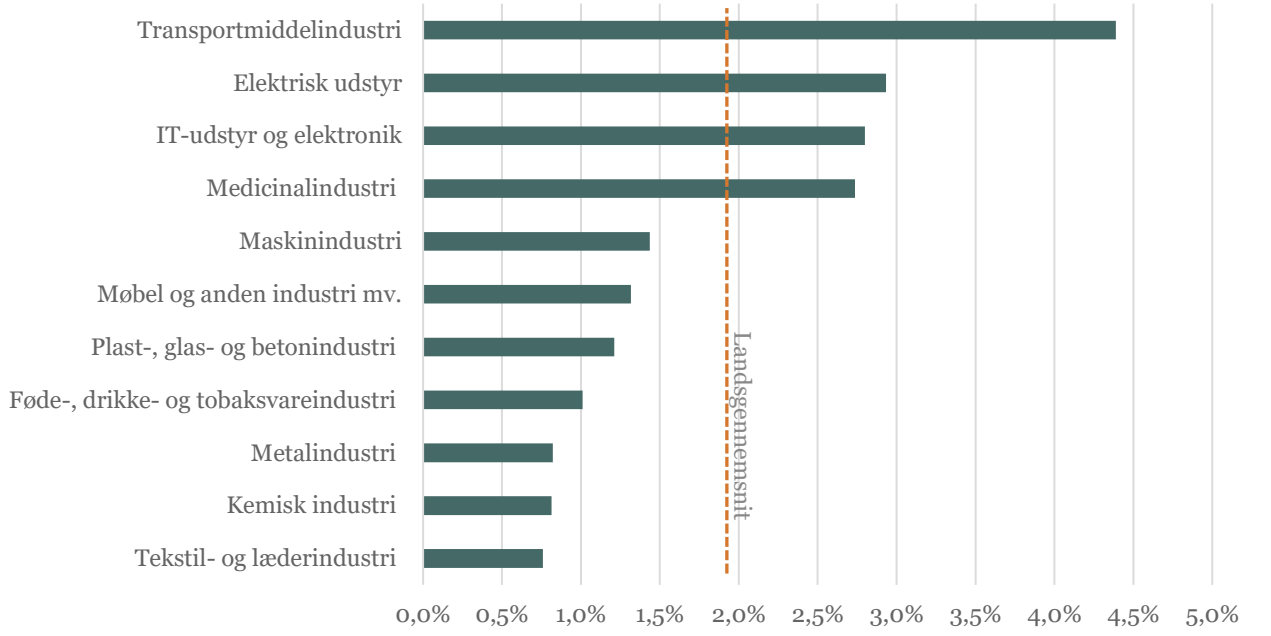
Industrien er den tredje af de tre hovedsektorer, vi sætter fokus på i dette kapitel. Industrien befinder sig midt i en større omstilling, ofte betegnet som Industri 4.0. Udviklingen er kendetegnet ved en stigende integration af den digitale verden og den fysiske produktion. Den tiltagende digitalisering gør virksomhederne sårbare overfor hændelser, der medfører nedbrud af IT-systemer eller brud på datas fortrolighed, tilgængelighed og integritet.

[10] Center for Cybersikkerhed (2018): Cybertruslen mod sundhedssektoren
[11] Center for Cybersikkerhed (2018): Cybertruslen mod land- og lufttransport

I Danmark har fire brancher inden for industrien en efterspørgsel efter ISK-kompetencer, der ligger over landsgennemsnittet. Det er *Transportmiddelindustrien*, *Elektrisk udstyr*, *IT-udstyr og elektronik* samt *Medicinalindustri*. For brancherne *Elektrisk udstyr* samt *IT-udstyr og elektronik* gælder, at deres produkter i høj grad er relateret til IT, hvorfor informationssikkerhed ligger i naturlig forlængelse af deres primære forretningsområde. Den høje ISK-efterspørgselsintensitet i *Medicinalindustri* kan være udtryk for, at det er en forskningsbaseret industri, der lever af patenter. Det er derfor vigtigt, at medicinalindustrien sikrer virksomhederne mod eksterne angreb som fx cyberspionage.

Figur 3.6 Efterspørgsel efter ISK-kompetencer i industrien

ISK-efterspørgselsintensitet i industrien, 2018



Kilde: HBS Jobindex
Anm.: Træ- og papirindustri, trykkerier samt Olieraffinaderier mv. indgår ikke, da figuren kun medtager brancher med minimum 300 jobopslag I 2018.

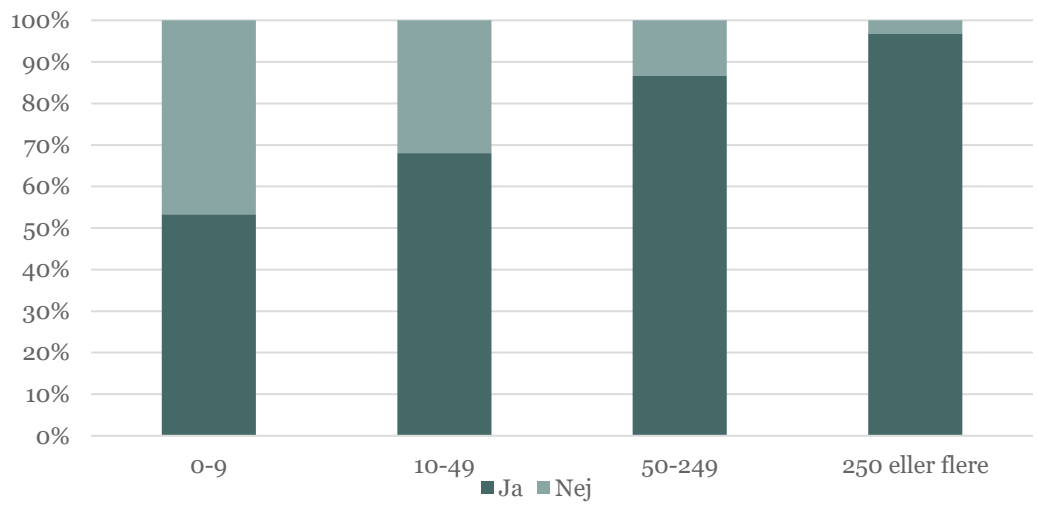
Der er imidlertid syv brancher i industrien, hvor efterspørgslen ligger lavere end landsgennemsnittet. Fx efterspørger *Føde-, drikke og tobaksindustrien* i mindre grad ISK-kompetencer, til trods for at produktionen af fødevarer i stigende grad bliver digital. En vis grad af informationssikkerhed er derfor væsentlig for at sikre en stabil produktion. Samtidig stiller forbrugerne stigende krav til indholdet i og produktionen af fødevarer.

3.6 Store virksomheder har flere med ISK-kompetencer

I de sidste to afsnit i dette kapitel beskriver vi karakteristika for virksomheder med ISK-kompetencer. Vi sætter særlig fokus på størrelse og efterspørgslen på tværs af regioner i Danmark.

Virksomhedens størrelse spiller en afgørende rolle for, om der er ansatte med ISK-kompetencer til stede på arbejdspladsen. Generelt vokser sandsynligheden for, at virksomheden har specifikke ISK-funktioner på arbejdspladsen, med virksomhedens størrelse, jf. figur 3.7. Blandt de adspurgte virksomheder i surveyen med færre end 10 ansatte er det kun 53 pct., der har ISK-kompetencer på arbejdspladsen. For virksomheder med 250 eller flere ansatte er det godt 96 pct. af virksomhederne, som har ISK-kompetencer på arbejdspladsen.

Figur 3.7 Andel af virksomheder med ISK-funktioner fordelt på virksomhedsstørrelse



Kilde: HBS Survey
Anm.: n=1146

Disse resultater afspejler, at store virksomheder i højere grad har kapacitet til varetage ISK-jobfunktioner i virksomheden. Således er store virksomheder mere tilbøjelige til at have ansatte med ISK-kompetencer. Derudover har store virksomheder qua deres størrelse bedre råd til at ansætte arbejdskraft med specialistkompetencer, mens små virksomheder i mindre grad har ansatte med en ISK-jobfunktion. Det betyder dog ikke, at små virksomheder nødvendigvis har et mindre fokus på informationssikkerhed, da det kan afspejle, at de i højere grad hyrer hjælp udefra.

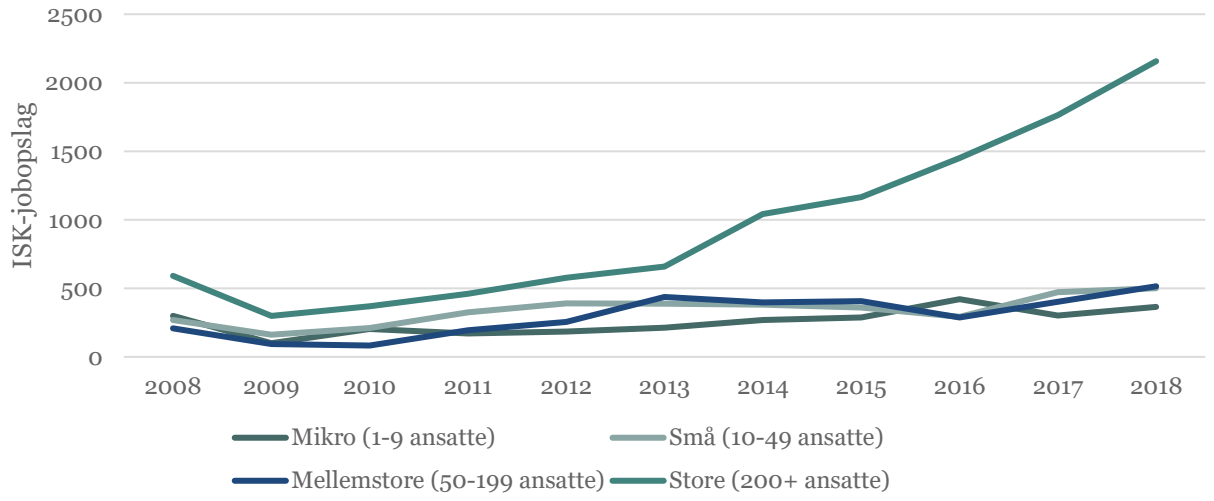
Samtidig er IT oftere en dybt integreret del af store virksomheder sammenlignet med SMV'er, hvilket medfører et øget behov for informationssikkerhed blandt store virksomheder[12]. Således vil virksomhens IT-systemer typisk blive mere omfattende og avancerede, jo større virksomheden er.

Store virksomheder har også en højere efterspørgsel efter arbejdskraft med ISK-kompetencer, og efterspørgslen er steget kraftigt, jf. figur 3.8. Fra 2013 til 2018 er antallet af ISK-jobopslag fra virksomheder med mere end 200 ansatte mere end tredoblet. Til sammenligning er ISK-efterspørgslen for SMV'er kun steget med 30 pct i samme periode. Resultatet skal ses i lyset af, at de store virksomheder alt andet lige har en større efterspørgsel, idet de har mange ansatte.

[12] Oxford, Shapiro Futures *Digitalisering i SMV'er* (2018)

Figur 3.8 Kraftig stigning i ISK-efterspørgslen for store virksomheder

Udvikling i ISK-jobopslag fordelt efter antal ansatte



Kilde: HBS Jobindex
Anm.: Antal ansatte er opgjort på baggrund af data fra CVR-registret.

Resultaterne er i overensstemmelse med, at 66 pct. af danske SMV'er har outsourcet hele eller dele af deres IT[13]. Virksomhederne outsourcer bl.a. deres IT, fordi de ikke har de nødvendige kompetencer på arbejdspladsen eller en decideret IT-afdeling. Når en virksomhed outsourcer IT-funktioner vil den ofte også vælge at outsource den tilhørende IT- og informationssikkerhed. I mange tilfælde er det dog relevant for virksomheden at have en vis kompetence internt fx ved håndtering af databehandleraftale.

Herudover er mange SMV'er ikke så langt fremme med digitaliseringen som store danske virksomheder, fordi de oplever en række barrierer[14]. Danske SMV'er har derfor alt andet lige et mindre behov for IT- og informationssikkerhed end store virksomheder. Det er dog ikke ensbetydende med at danske SMV'er ikke har et behov for informationssikkerhed. En tidligere analyse viser, at 39 pct. af danske SMV'er ikke besidder et tilstrækkeligt niveau for IT-sikkerhed og dermed er sårbare overfor IT-sikkerhedsangreb[15].

Både danske og internationale analyser peger på, at en af udfordringerne for SMV'erne er den manglende ledelsesmæssige erkendelse af betydningen af informationssikkerhed. En mundtlig og uformel kultur for informationssikkerhed i SMV'erne medvirker til, at det er sværere at få udviklet indlejrede rutiner og processer for, hvordan informationssikkerhed håndteres.

3.7 ISK-kompetencer er mest efterspurgt i Hovedstadsregionen

Efterspørgslen efter ISK-kompetencer varierer ikke kun på tværs af brancher og virksomhedsstørrelse, men også på tværs af geografi, som er fokus i dette afsnit. I 2018 var knap 3 pct. af jobopslagene i Region Hovedstaden ISK-jobopslag. Det gør Region Hovedstaden til den region, hvor arbejdsgiverne oftest efterspørger ISK-kompetencer. Tilsvarende var knap 1 pct. af alle jobopslag et ISK-jobopslag i Region Sjælland og Region Nordjylland. Således er efterspørgslen efter ISK-kompetencer lavest i disse to regioner, jf. figur 3.9.

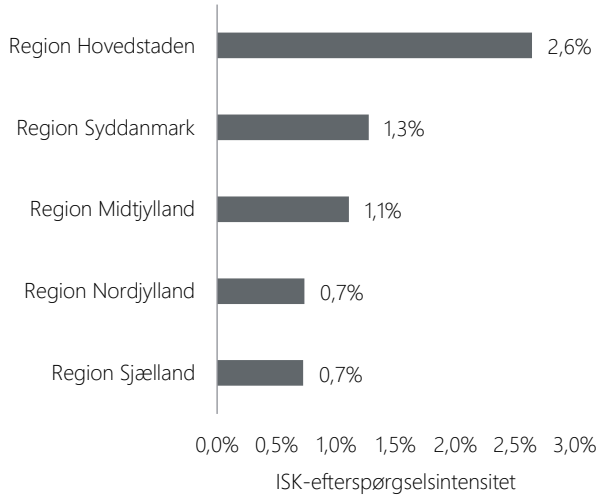
[13] IT-sikkerhed og datahåndtering i danske SMV'er (2018)

[14] Strategi for Danmarks digitale vækst (2018)

[15] IT-sikkerhed og datahåndtering i danske SMV'er (2018)

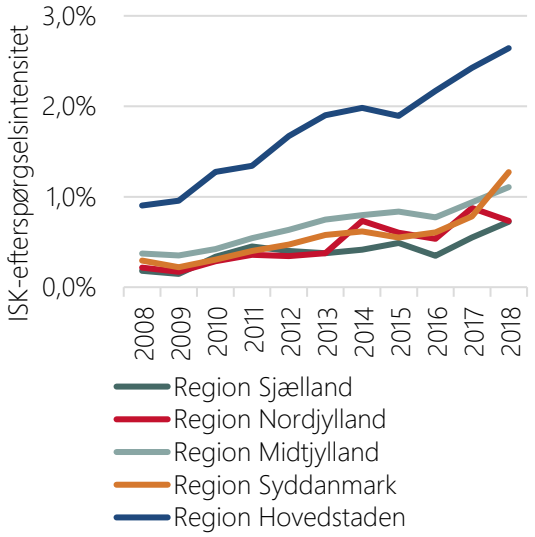
Mange IKT-virksomheder, banker og forsikringsselskaber er placeret i Region Hovedstaden, og det er sandsynligvis forklaringen på, at efterspørgslen efter ISK-kompetencer er størst i Region Hovedstaden. Samtidig er disse brancher kendetegnet ved at have en høj koncentration af ISK-kompetencer, jf. afsnit 3.2.

Figur 3.9 Andel ISK-jobopslag fordelt på regioner, 2018



Kilde: HBS Jobindex

Figur 3.10 Udvikling i ISK-jobopslag fordelt på regioner, 2008-2018



Kilde: HBS Jobindex

Efterspørgslen efter ISK-kompetencer er stigende i hele landet. For alle regioner gælder det, at ISK-efterspørgslen er steget i perioden 2008-2018, jf. figur 3.10. I 2018 var efterspørgslen efter ISK-kompetencer i alle regioner ca. tre gange så stor, som den var i 2008. Den stigende tendens for efterspørgslen efter ISK-kompetencer er altså gældende i hele landet, selvom efterspørgslen er størst i Region Hovedstaden.

4. Efterspørgsel efter specifikke kompetenceprofiler

Afsnittets hovedresultater

- Det danske arbejdsmarked for informationssikkerhed er koncentreret om syv kompetenceprofiler. Kompetenceprofilerne inden for informationssikkerhed er med denne rapport for første gang systematiseret, kategoriseret og kortlagt i Danmark.
- Den stigende efterspørgsel efter kompetencer inden for informationssikkerhed i Danmark favner bredt. Således er efterspørgslen efter alle syv kompetenceprofiler steget betydeligt i det seneste årti.
- Efterspørgslen er størst for de mere tekniske kompetenceprofiler, der beskytter virksomheden mod angreb, forebygger IT-nedbrud, udvikler sikre IT-systemer og vedligeholder dem.
- Efterspørgslen efter specialiserede jobfunktioner, der bl.a. skal monitorere organisationens IT-systemer og efterforske cyberangreb, ligger på et relativt lavt niveau. Det hænger sammen med, at der er tale om specialiserede jobfunktioner inden for cybersikkerhed.
- Efterspørgslen efter arbejdskraft, som skal lede, styre og udvikle organisationens IT-sikkerhed, ligger ligeledes på et lavt niveau sammenlignet med de øvrige profiler.

Informationssikkerhed er et bredt begreb, der dækker mange forskellige typer af arbejdsopgaver. Opgaverne spænder bredt fra beskyttelse af oplysninger om forretning og borgere til sikring af IT-systemer og produktionsanlæg imod cyberkriminalitet og cyberspionage. De nødvendige kompetencer for at løse disse opgaver spænder ligeledes bredt fra netværksbeskyttelse, kryptografi, statistiske evner og softwaredesign til blødere kompetencer inden for ledelse, risikostyring og jura mv.

Den stigende efterspørgsel efter kompetencer inden for informationssikkerhed, som vi fandt i kapitel 3, siger ikke noget om, hvilken type af arbejdskraft inden for informationssikkerhed der er særlig høj efterspørgsel efter. I dette afsnit kortlægger vi efterspørgslen efter specifikke kompetencer ved at opdele efterspørgslen i syv overordnede kompetenceprofiler, der alle arbejder med informationssikkerhed.

4.1 Kompetenceprofiler for informationssikkerhed

For at få en dybere forståelse af behovet for kompetencer inden for informationssikkerhed i virksomheder og hos myndigheder etablerer vi i dette afsnit et rammeværk til systematisering af kompetenceprofiler for informationssikkerhed i Danmark. En kompetenceprofil dækker over et arbejdsområde, hvortil der knytter sig et sæt specifikke kompetencer. Kompetenceprofilerne er ikke nødvendigvis gensidigt udelukkende. For især mindre virksomheder gælder det, at samme person skal varetage opgaver, der dækkes af forskellige kompetenceprofiler.

Hvordan er kompetenceprofiler etableret?
Hvert ITS-jobopslag er kategoriseret på baggrund af, hvilke kompetencer der nævnes i jobopslaget. Et jobopslag kan tilhøre mere end en jobprofil, fordi (1) nogle kompetenceord vil tilhøre mere end en jobprofil, eller (2) der i jobopslaget nævnes flere kompetencer som tilhører forskellige jobprofiler. Se afsnit 8 for en udførlig beskrivelse af metoden bag analysen.

Kompetenceprofilerne er etableret med udgangspunkt i det amerikanske rammeværk for informationssikkerhed *National Initiative for Cybersecurity Education (NICE)*[16]. NICE er udviklet i USA som et nationalt rammeværk til kategorisering og beskrivelse af arbejde inden for informationssikkerhed, uanset hvor eller for hvem arbejdet udføres. Formålet er at skabe dybere forståelse i

[16] https://www.nist.gov/itl/applied-cybersecurity/nice

både den offentlige, private og akademiske sektor for behovet for kompetencer inden for informationssikkerhed.

Der er en række fordele ved at tage udgangspunkt i NICE. For det første er USA på forkant med udviklingen af kompetencer, processer og teknologier relateret til informationssikkerhed. Rammeværket vedligeholdes og opdateres løbende af amerikanske myndigheder i et samarbejde mellem offentlige aktører, erhvervslivet og uddannelsesinstitutioner. Således vil rammeværk i denne rapport løbende kunne opdateres i henhold til udviklingen i USA. Yderligere er rammeværket internationalt anerkendt og ligger til grund for officielle kortlægninger af informationssikkerhedskompetencer i en række lande, fx Storbritannien, Canada og Australien[17].

Det danske arbejdsmarked for informationssikkerhed er koncentreret omkring syv kompetenceprofiler.

Tabel 4.1 Syv kompetenceprofiler for informationssikkerhed i Danmark

Kompetence-profil	Beskrivelse
1. Ledelse og organisation	Har til opgave at lede, styre og udvikle organisationers IT-sikkerhed. Skaber sikkerhedsbevidst adfærd og vaner. Står for risikomanagement og udvikler beredskabsplaner mv. Udgøres af en bred gruppe af personer med forskellige uddannelser, men vil ofte være personer med en akademisk uddannelse (fx samfundsvidenskabelig baggrund, merkantil baggrund eller IT-baggrund). Eksempler på jobtitler er fx CSO/CISO (Chief Information Security Officer), CTO (Chief Technology Officer) og CRO/CRMO (Chief Risk Management Officer).
2. Jura og Databeskyttelse	Har til opgave at udvikle processer til overholdelse af lovgivning, bekendtgørelser og politikker vedrørende databeskyttelse og andre lovkrav. Det kan fx være en DPO (Data Protection Officer), en administrativ medarbejder eller en jurist med speciale i datasikkerhed.
3. Udvikling af sikre systemer	Har til opgave at konceptualisere og implementere sikkerheden i organisationers IT-systemer, IT-infrastruktur og produkter. Designer og implementerer konkrete løsninger og udvikler software til håndtering af IT-sikkerhed. Der er typisk tale om en IT-specialist som fx IT-løsningsarkitekt, Software Architect eller IT-/softwareingeniør.
4. Drift og vedligeholdelse	Har til opgave at drifte og vedligeholde IT-systemer, netværk mv. Opgaver relateret til IT-sikkerhed er styring af adgangsrettigheder, opsætning af firewall og VPN, rettighedsstyring (Identity & Access management) samt backup og kryptering. Der er typisk tale om en IT-teknikker som fx Datamatiker eller IT-teknolog.
5. Beskyttelse og forsvar	Har til opgave at opdage, rådgive om og/eller implementere teknologiske løsninger, der skal beskytte organisationen mod cyberangreb. Typiske arbejdsopgaver er penetrationstest, implementering af anti-phishingværktøjer, e-mail fraud detection, red teaming og firewall audit. Har ofte en akademisk uddannelse med naturvidenskabelig baggrund. Eksempel på jobtitler er Security Consultants eller IT Security Advisor.
6. Analyse og monitorering	Har til opgave løbende at analysere og monitorere IT-systemer i organisationer. Typiske arbejdsopgaver er verifikation (e-mail, faktura etc.), SOC (Security Operation Center) og SAC (Security Analytics Center). Har ofte en akademisk uddannelse med naturvidenskabelig baggrund. Eksempel på jobtitel er IT-analytiker, loganalytiker, netværksanalytiker, IT-/softwareingeniør eller -udvikler.
7. Efterforskning	Har til opgave at efterforske cyberangreb. Arbejdsopgaver er blandt andet incident response, reverse engineering, datagendannelse mv. Har ofte en akademisk uddannelse med naturvidenskabelig baggrund. Eksempeler på jobtiteler er Security Consultants og Incident Response. Consultant.

Kilde: Højbjerre Brauer Schultz baseret på *National Initiative for Cybersecurity Education (NICE)*

[17] Storbritannien (link), Canada (link) og Australien (link)

Kompetenceprofilerne fra NICE er i denne rapport tilpasset en dansk kontekst. Det er sket på baggrund af interview med informationssikkerhedsvirksomheder og via analyse af virksomheders og myndigheders efterspørgsel efter ISK-kompetencer – dels med henblik på at indramme behovet på det danske arbejdsmarked, dels med henblik på at etablere et arbejdsredskab, som fremadrettet kan monitorere udviklingen i behovet for forskellige kompetenceprofiler, koble dem til det formelle uddannelsessystem og derigennem belyse behovet for opkvalificeringen og efteruddannelse.

4.2 Efterspørgsel efter kompetenceprofiler

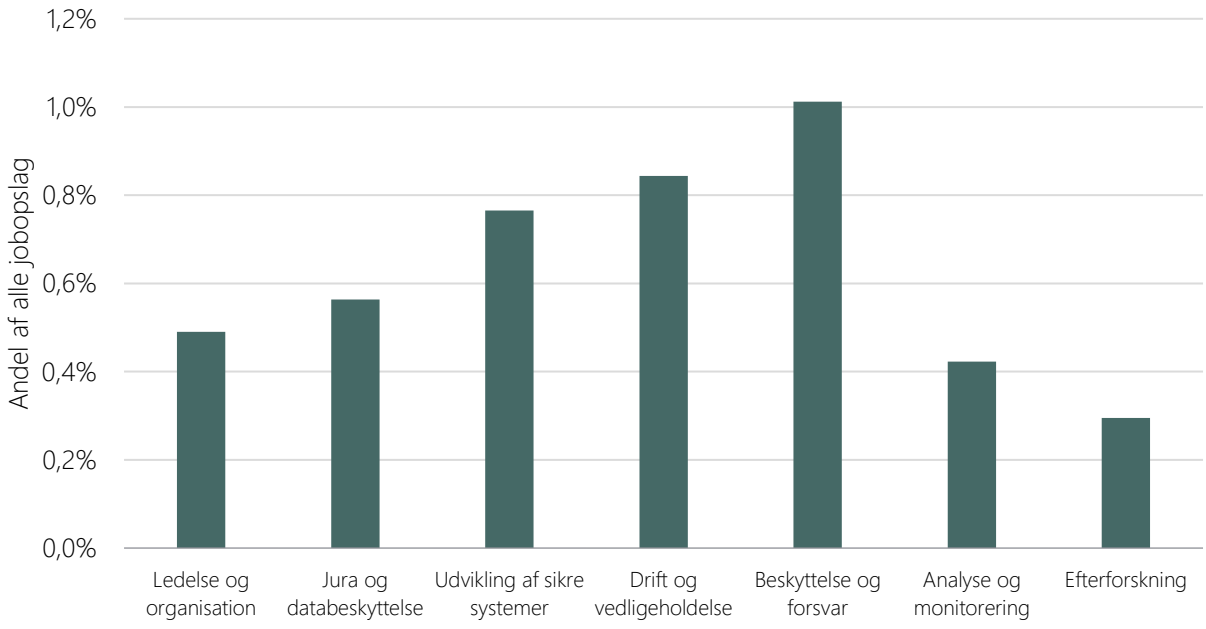
I dette afsnit undersøges, hvilke kompetenceprofiler der er efterspurgt af virksomheder og myndigheder på det danske arbejdsmarked.

STØRST EFTERSPØRGSEL EFTER DE TEKNISKE KOMPETENCER

Den mest efterspurgte kompetenceprofil i Danmark inden for informationssikkerhed er *Beskyttelse og forsvar*, jf. figur 4.1. I 2018 var godt 1 pct. af alle jobopslag, svarende til knap 2.800 jobopslag, målrettet denne jobprofil. Blandt de mest efterspurgte kompetencer, der er kendetegnende for profilen *Beskyttelse og forsvar* er incident management og intrusion detection samt viden om COBIT (Control Objectives for Information and Related Technologies) og cyberforsvar. Certifikater som *Certified Incident Handler (GIAC)* efterspørges i nogen grad.

Figur 4.1 De tekniske jobprofiler er mest efterspurgte

Andel jobopslag, hvor der efterspørges en given kompetenceprofil, 2018



Kilde: Egne beregninger på baggrund af HBS Jobindex
Anm.: Efterspørgselsintensiteten er beregnet som antal jobopslag målrettet en given jobprofil divideret med det samlede antal jobopslag.

Beskyttelse og forsvar har et stort kompetencefællesskab med de andre kompetenceprofiler, der er kendetegnet ved en hovedvægt på tekniske kompetencer. Det gælder især kompetenceprofilerne *Udvikling af sikre systemer, Drift og vedligeholdelse* samt *Analyse og monitorering*. Tekniske kompetencer, der går på tværs af de fire profiler, er specifik viden relateret til navngivne hardwareproducenter eller sikkerhedsmæssige forhold relateret til udstyr og teknologier som firewalls, netværk mv. De tekniske kompetencer er i høj efterspørgsel hos en bred vifte af virksomheder og organisationer og bidrager derfor til at trække efterspørgslen efter de tre kompetenceprofiler op.

Den høje efterspørgsel efter kompetenceprofilen *Beskyttelse og forsvar* vidner om, at danske arbejdsgivere har stort fokus på at identificere trusler mod interne IT-systemer. En dybere integration af IT i virksomheder medfører, at IT-sikkerhedsopgaven bliver større. Det gælder i særdeleshed i de IT-intensive virksomheder, fx inden for finans og IKT. Den høje efterspørgsel er også udtryk for, at virksomhederne generelt i stigende grad har fokus på informationssikkerhed. Herunder tilbyder en række specialiserede virksomheder informationssikkerhed som en service – et område, der er i markant udvikling på det amerikanske arbejdsmarked, jf. Burning Glass (2019). I Finans er reguleringen inden for compliance også med til at drive denne udvikling.

Drift og vedligehold er den anden mest efterspurgte kompetenceprofil i Danmark. I 2018 var godt 0,8 pct. af alle jobopslag, svarende til ca. 2.300 jobopslag, målrettet denne jobprofil. Personer med denne profil er typisk teknikkerer, der drifter og bygger IT-systemer. De har et stort kompetencefællesskab med *Udvikling af sikre systemer* og *Beskyttelse og forsvar*. Således er tekniske kompetencer relateret til udstyr og teknologier som firewalls, netværk mv. også meget efterspurgte for denne profil. Derudover vedrører de mest efterspurgte kompetencer, der er kendetegnende for profilen *Drift og vedligeholdelse,* netværksspecifik viden, sikkerhed vedrørende servere samt viden om backupsystemer. Certifikater som Check Point Certified Security Administrator/Expert (*CCSA/E*) efterspørges i nogen grad.

Udvikling af sikre systemer er den tredje mest efterspurgte kompetenceprofil i Danmark. I 2018 var knap 0,8 pct. af alle jobopslag, svarende til ca. 2.100 jobopslag, målrettet denne jobprofil. En meget efterspurgt kompetence for denne profil er kryptologi, dvs. viden om krypteringsalgoritmer og protokoller. Derudover efterspørges især kompetencer inden for sikkerhedsarkitektur og kontrol af identitet (authentication). Af certifikater er CISSP (Certified Information Systems Security Professional) efterspurgt. Det dækker især kompetencer vedrørende sikkerhedsprincipper som fortrolighed, integritet og tilgængelighed.

Kompetenceprofilerne *Analyse og monitorering* og *Efterforskning* efterspørges i mindre grad. I 2018 var ca. 0,4 pct. af alle jobopslag målrettet kompetenceprofilen *Analyse og monitorering*, og 0,3 pct. var målrette *Efterforskning*. Efterspørgslen efter denne kompetenceprofil adskiller sig ved kompetencer som Certified Ethical Hacker (CEH), security analyse og threat intelligence. Efterspørgslen ligger dog på et lavt niveau. *Efterforskning* adskiller sig fra de andre kompetenceprofiler ved at dække kompetencer vedr. forensics, malware og logging. *Certified Forensics Analyst (GIAC)* efterspørges i et lavt omfang. Arbejdsgiverne efterspørger altså i mindre grad specialiseret arbejdskraft, som kan efterforske hackerangreb og anden cyberkriminalitet.

Den relativt lave efterspørgsel efter kompetenceprofilerne *Analyse og monitorering* samt *Efterforskning* er formentlig et udtryk for, at danske virksomheder i mindre grad har behov for kompetencer til at efterforske cyberkriminalitet eller hackerangreb. Kompetencerne til at løfte denne type opgaver knytter sig til en højtspecialiseret jobfunktion, som de fleste virksomheder sjældent vil have 'in-house'. I stedet vil kompetencer vedr. analyse, monitorering og efterforskning af hackerangreb og anden cyberkriminalitet være koncentreret i få specialiserede konsulentvirksomheder, der rykker ud ved en hændelse, eller i offentlige myndigheder, fx politiet eller forsvarets efterretningstjeneste.

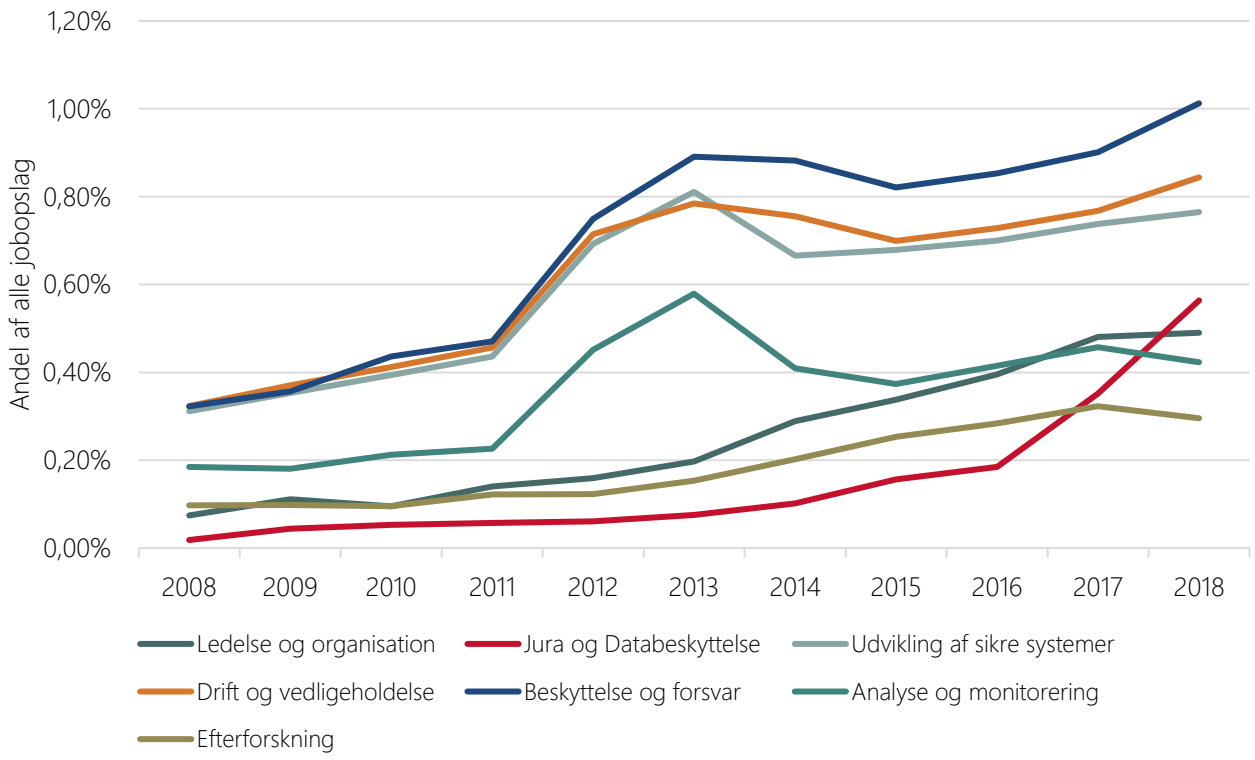
Kompetenceprofilen *Jura og databeskyttelse* ligger i mellemfeltet sammenlignet med de øvrige profiler. I 2018 var 0,54 pct. af alle jobopslag, svarende til ca. 1.300 jobopslag, målrettet denne jobprofil. De mest efterspurgte kompetencer relaterer sig til den nye GDPR-lovning og databeskyttelse. En ofte efterspurgt profil er en *Data Protection Officer (DPO).*

Kompetenceprofilen *Ledelse og organisation* efterspørges relativt lidt sammenlignet med de fleste andre kompetenceprofiler. I 2018 var 0,5 pct. af alle jobopslag, svarende til ca. 1.300 jobopslag, målrettet denne jobprofil. De mest efterspurgte kompetencer for denne profil er ITSM, ISO27001, CISSP og IT-compliance. Et certifikat, som ofte er efterspurgt for denne profil, er Certified Information Security Manager (CISM). Der er tale om viden målrettet informationssikkerhed og styring heraf i en organisation.

EFTERSPØRGSLEN ER STEGET FOR ALLE KOMPETENCEPROFILER

Ser man på udviklingen i efterspørgslen over de seneste ti år, kan man konstatere, at der er sket en kraftig fremgang i efterspørgslen for alle syv kompetenceprofiler, jf. figur 4.2. Samtidig fremgår det, at efterspørgslen efter de tekniske profiler *Beskyttelse og forsvar, Drift og vedligeholdelse* samt *Udvikling af sikre systemer* systematisk har ligget højere end de øvrige profiler, mens især efterspørgslen efter *Ledelse og organisation* samt *Efterforskning* gennem hele perioden har ligget på et relativt lavt niveau.

Figur 4.2 Udvikling i efterspørgselsintensiteter for jobprofiler, 2008-2018



Kilde: Egne beregninger på baggrund af HBS Jobindex

Anm.: Efterspørgselsintensiteten er beregnet som antal jobopslag målrettet en given jobprofil divideret med det samlede antal jobopslag.

For kompetenceprofilerne *Beskyttelse og forsvar, Drift og vedligeholdelse* samt *Udvikling af sikre systemer* sker der en kraftig fremgang i perioden 2011 til 2013, hvorefter udviklingen fortsætter som i perioden før 2011. Udviklingen dækker over en øget efterspørgsel efter kompetencer relateret til fx firewalls, WAN, TCP, SSL og antivirus. Fremgang i perioden fra 2016 og frem drives derimod af kompetencer relateret til kryptering, cyberforsvar, incident response og cloud computing.

For *Jura og databeskyttelse* er der fra 2016 og frem sket en kraftig stigning i efterspørgslen. Udviklingen er udtryk for en stigende efterspørgsel relateret til databeskyttelse. Det skal ses i lyset af GDPR-lovgivningen, der blev vedtaget i 2016 og trådte i kraft i 2018. Indførslen af databeskyttelsesloven øgede efterspørgslen efter jurister og andre medarbejdere med viden om databeskyttelse og databeskyttelseslovgivning.

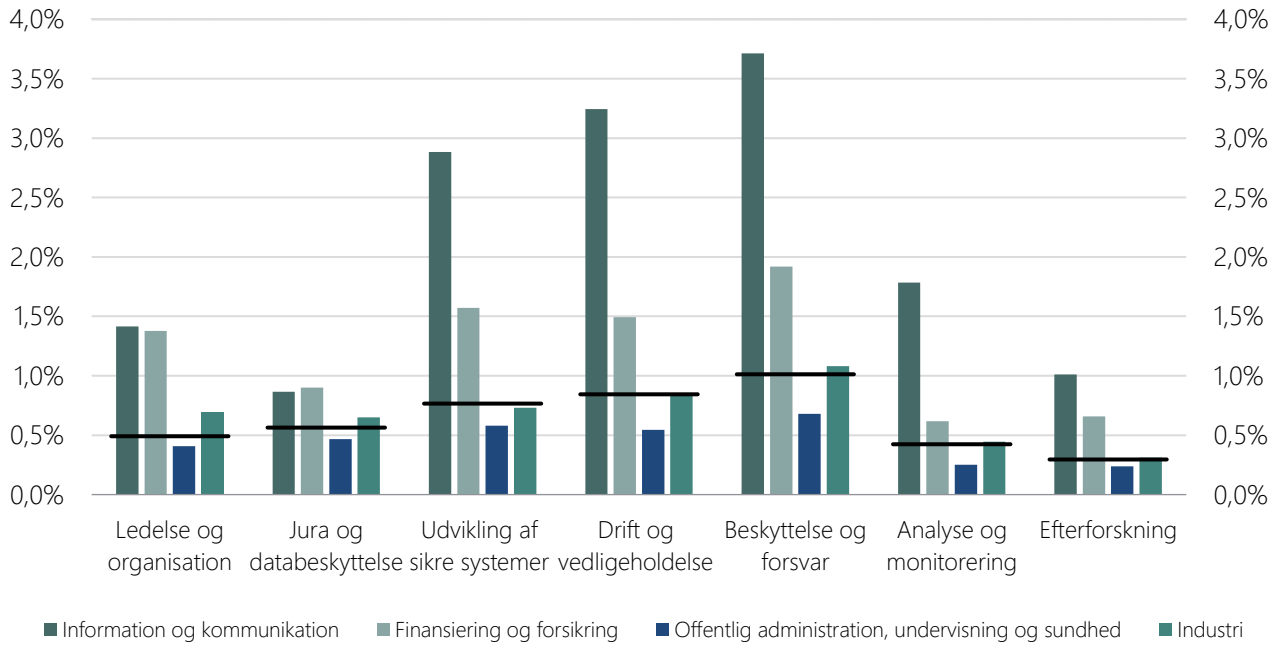
For kompetenceprofilen *Ledelse og organisation* er udviklingen beskeden fra 2008 til 2013. Herefter sker der en mindre acceleration i efterspørgslen, hvilket blandt andet dækker over kompetencer relateret til ISO27001.

4.3 Branchernes efterspørgsel efter kompetenceprofiler

I dette afsnit ser vi på efterspørgslen efter de specifikke kompetenceprofiler i brancherne *Information og kommunikation*, *Finansiering og forsikring* samt *Offentlig administration, undervisning og sundhed* samt industrien. Disse brancher er udvalgt, fordi ISK-jobopslag udgør en relativt stor andel af branchernes samlede efterspørgsel, eller fordi de har en høj absolut efterspørgsel efter ISK-kompetencer, dvs. at branchen slår flest ISK-jobopslag op.

I branchen *Information og kommunikation* er efterspørgslen efter alle seks kompetenceprofiler væsentlig højere end det generelle billede beskrevet i forrige afsnit. Branchen adskiller sig ved en særlig høj efterspørgsel efter de tekniske kompetenceprofiler, dvs. profilerne *Udvikling af sikre systemer*, *Drift og vedligeholdelse* og *Beskyttelse og forsvar*. Der er her tale om virksomheder inden for telekommunikation, softwareudvikling og informationstjenester, der i kraft af deres specialisering inden for IT har en naturlig høj efterspørgsel efter tekniske kompetencer inden for informationssikkerhed. Det er også under denne branche, man finder virksomheder, der er specialiseret inden for cybersikkerhed, hvilket kan forklare den relativt høje efterspørgsel efter kompetencer relateret til *Analyse og monitorering* samt *Efterforskning*.

Figur 4.3 Efterspørgsel efter jobprofiler for udvalgte brancher



Kilde: HBS Jobindex
Anm.: Efterspørgselsintensiteten er antallet af jobopslag for en given jobprofil i en given branche divideret med det samlede antal jobopslag i branchen. Den sorte streg i figuren angiver det gennemsnitlige niveau for alle virksomheder og myndigheder i Danmark (jf. figur 4.1).

Branchen *Finansiering og forsikring* er også kendetegnet ved en høj efterspørgsel på tværs af alle seks kompetenceprofiler sammenlignet med det generelle billede i Danmark. Som beskrevet tidligere hænger det sammen med den omfattende digitalisering af især bankforretning både i forhold til front-end (netbank, mobilbank, mobilepay mv.) samt backend (den bagvedliggende IT-infrastruktur). Branchen adskiller sig også ved at have en særlig høj efterspørgsel efter kompetencer relateret til *Ledelse og Strategi*. Et tilsvarende træk ses for branchen *Information og kommunikation*.

For branchen *Offentlig administration, undervisning og sundhed* ligger efterspørgslen for alle seks kompetenceprofiler på et relativt lavt niveau. Dette billede dækker over to modsatrettede forhold. På den ene side er efterspørgslen i staten generelt meget høj, som beskrevet i kapitel 4. Det gælder for alle syv kompetenceprofi-

ler. På den anden side er efterspørgslen i regionerne og kommunerne for alle syv kompetencekategorier betydelig lavere end landsgennemsnittet. Idet kommuner og regioner udgør ca. 86 pct. af jobmarkedet for den offentlige sektor, trækker det den offentlige sektor som helhed ned under det generelle niveau.

Endelig gælder for industrien, at efterspørgslen efter alle kompetenceprofiler ligger lidt over det generelle niveau bortset fra profilen *Udvikling af sikre systemer*, der ligger lidt under. Som i de fleste andre brancher er efterspørgslen efter de tekniske kompetencer, dvs. profilerne *Udvikling af sikre systemer*, *Drift og vedligeholdelse* og *Beskyttelse og forsvar*, højest. Industrien adskiller sig dog ved en relativt høj efterspørgsel efter kompetencer relateret til *Ledelse og organisation*.

5. Kortlægning af informationssikkerheds-uddannelser

Afsnittets hovedresultater

- Der er 32 videregående uddannelser i Danmark, som har et element af informationssikkerhed.
- Syv af disse uddannelser tilbyder kurser inden for informationssikkerhed, hvor kurserne på hver enkel uddannelse tilsammen giver mere end 30 ECTS-point (dvs. et semester).
- Der er én informationssikkerhedsuddannelse i Danmark, der har et obligatorisk indhold af informationssikkerhed, som fylder mere end 30 ECTS-point.
- De videregående uddannelser med et indhold af informationssikkerhed udbydes langt overvejende på universiteterne – virksomheder svarer også, at det er herfra, de primært ansætter.
- Flest uddannelser matcher med kompetenceprofilen, der arbejder med udvikling af sikre systemer.
- Omkring 17.000 har en uddannelse med et indhold af informationssikkerhed, men få arbejder i jobs, hvor de beskæftiger sig med informationssikkerhed.
- Få af dem, der starter i et informationssikkerhedsjob, har en uddannelse relateret til informationssikkerhed.

Uddannelsessystemet spiller en central rolle ift. antallet af personer, som har kompetencer inden for informationssikkerhed, og ikke mindst hvor mange der har mulighed for at opnå disse kompetencer i fremtiden. I dette kapitel ser vi derfor på, hvor mange uddannelser i det danske uddannelsessystem, der tilbyder kurser relateret til informationssikkerhed. Derefter forsøger vi at estimere størrelsen af arbejdsstyrken, som har kompetencer til at indgå på arbejdsmarkedet for informationssikkerhed.

5.1 Videregående uddannelser med indhold af informationssikkerhed

I dette afsnit kortlægger vi udbuddet af ordinære videregående uddannelser[18] målrettet informationssikkerhed. Først vil vi se på det generelle billede, dernæst dykker vi ned i, hvad der karakteriserer de enkelte niveauer. Herefter ser vi på linket imellem uddannelser og kompetenceprofiler, og endeligt belyser vi, hvilke uddannelser virksomhederne typisk ansætter folk fra.

Hvordan har vi kortlagt uddannelsesudbuddet?
Populationen af informationssikkerhedsuddannelser er dannet ved at gennemgå kursusbeskrivelser for obligatoriske fag og valgfag til relevante uddannelser. Herefter er uddannelserne kategoriseret efter, hvor mange ECTS-point der vedrører informationssikkerhed. I opgørelsen skelnes ikke mellem obligatoriske kurser og valgfag.

Vi inkluderer udelukkende uddannelser, som indeholder 'rene' informationssikkerhedskurser. Uddannelser som tilbyder kurser, hvor informationssikkerhed er et delelement, indgår altså ikke.

[18] Den anden del af det danske uddannelsessystem er systemet for voksen- og efteruddannelse, som ikke indgår i denne kortlægning. Se fx Børne- og Undervisningsministeriets overblik over uddannelsessystemet: https://www.uvm.dk/uddannelsessystemet/overblik-over-det-danske-uddannelsessystem/voksen-og-efteruddannelsessystemet

DER ER 32 VIDEREGÅENDE UDDANNELSER MED ET INDHOLD AF INFORMATIONSSIKKERHED – FÅ TILBYDER ET HØJT INDHOLD AF INFORMATIONSSIKKERHED

Ifølge vores kortlægning af det ordinære danske uddannelsessystem er der i alt 32 videregående uddannelser i Danmark, som i større eller mindre grad tilbyder et indhold, der relaterer sig til informationssikkerhed, jf. tabel 5.1. Der er tale om en simpel optælling baseret på, hvor mange ECTS-point inden for informationssikkerhed, der udbydes på uddannelsen (både valgfrie og obligatoriske).

Der er syv uddannelser, der tilbyder et højt indhold af informationssikkerhed i Danmark. En af disse uddannelser har et obligatorisk indhold vedrørende informationssikkerhed, som overstiger 30 ECTS-point. Det er professionsbacheloruddannelsen i IT-sikkerhed, der kan læses som en overbygning på en erhvervsakademiuddannelse eller som en diplomuddannelse. Uddannelsen udbydes på tre erhvervsakademier.

De resterende seks uddannelser med et højt indhold af informationssikkerhed udbyder et eller flere kurser, der tilsammen giver mindst 30 ECTS-point inden for informationssikkerhed. Det kan både være valgfrie og obligatoriske kurser. Et eksempel er diplomingeniøruddannelsen i IT-elektronik på DTU, hvor der er et obligatorisk kursus om sikkerhed i indlejrede systemer, mens der samtidig er mulighed for valgfrie kurser om informationssikkerhed. Et andet eksempel er kandidatuddannelsen i informationsteknologi, hvor de studerende kan vælge en specialisering inden for computer security. Af de seks uddannelser er to bachelor- og professionsbacheloruddannelser og fire kandidatuddannelser.

Tabel 5.1 Kortlægning af videregående uddannelser

UDDANNELSE	UDDANNELSER MED ET HØJT INDHOLD AF INFORMATIONSSIKKERHED (>=30 ECTS)	UDDANNELSER MED ET DELVIST INDHOLD AF INFORMATIONSSIKKERHED (>=15 ECTS)	UDDANNELSER MED ET LAVT INDHOLD AF INFORMATIONSSIKKERHED (<15 ECTS)
Erhvervsakademiuddannelser	0	1	0
Bachelor- og professionsbacheloruddannelser, herunder diplomingeniør	3	1	11
Kandidatuddannelser	4	5	7
I alt	7	7	18

Kilde: Egen tilvirkning
Anm.: Kategoriseringen er foretaget på baggrund af uddannelsernes kursusbeskrivelser. Både bacheloruddannelser og den tilhørende kandidatuddannelse kan indgå i tabellen. For en uddybende liste over, hvilke uddannelser som ligger til grund for tabellen, se bilag 1.

Derudover er der syv uddannelser som tilbyder minimum 15 ECTS-point (½ semester) inden for informationssikkerhed. Heraf en erhvervsakademiuddannelse (IT-teknolog), en diplomingeniøruddannelse (IT og økonomi på DTU) og fem kandidatuddannelser. Kandidatuddannelserne dækker hovedsageligt over tekniske uddannelser som fx kandidatuddannelsen i Software Engineering på SDU. Kandidatuddannelsen i jura på KU, der fx tilbyder kurser i persondataret, ligger dog også i denne kategori.

Langt størstedelen af uddannelserne (18) har et lille indhold af informationssikkerhed (mindre end 15 ECTS). Heraf en diplomingeniøruddannelse, en professionsbachelor, ni bacheloruddannelser og syv kandidatuddannelser. Gruppen består både af tekniske uddannelser (fx bachelor i netværksteknologi og IT på DTU) og uddannelser, hvis indhold i højere grad er relateret til lovgivning vedr. informationssikkerhed (fx kandidat i jura på AU eller bachelor i sundhed og information på KU).

Overvejelser ved brug af ECTS-point til at inddele uddannelser

ECTS-point giver et objektivt mål for, hvor meget et givent kursus fylder. Mange uddannelser vil ofte indeholde elementer fra forskellige fagområder, og derfor er det mere meningsfyldt at sætte en ECTS-grænse end at kræve, at hele uddannelsen omhandler informationssikkerhed.

Men grænsen for, hvor mange ECTS-point vedrørende informationssikkerhed en uddannelse skal indeholde, har stor betydning for, hvor mange uddannelser der defineres som informationssikkerhedsuddannelser. Jo højere grænsen sættes, jo færre uddannelser vil defineres som informationssikkerhedsuddannelser, og omvendt jo lavere grænsen sættes.

Tabel 5.1 giver også et billede af, at langt de fleste uddannelser med et indhold af informationssikkerhed stammer fra universiteterne (bachelor-, ingeniør- og kandidatuddannelser) eller professionsbacheloruddannelserne. Samtidig er der flest kandidatuddannelser, der har et højt eller delvist indhold af informationssikkerhed.

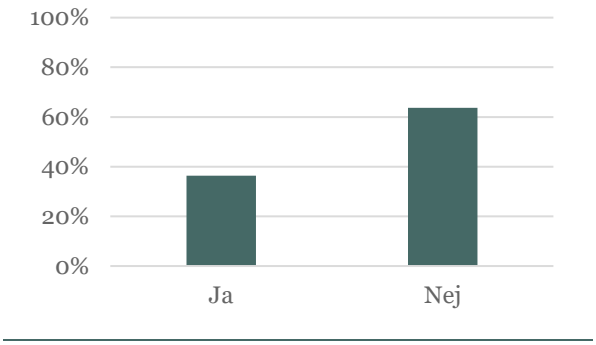
Samlet set viser kortlægningen altså, at der er relativt få videregående uddannelser i det danske uddannelsessystem, som tilbyder kurser inden for informationssikkerhed. Til dette hører også, at mange af de uddannelser og kurser, der vedrører informationssikkerhed, er meget nye. Fx blev professionsbacheloruddannelsen i IT-sikkerhed først oprettet i 2017. Således var de første dimittender færdige i starten af 2019. Ligeledes vil kurser i GDPR selvsagt være helt nye, da databeskyttelsesloven først trådte i kraft i 2018.

DE FLESTE NYANSÆTTELSER HAR EN IT-UDDANNELSE FRA UNIVERSITETET

Resultaterne fra spørgeskemaundersøgelsen viser, at mere end hver tredje virksomhed eller myndighed inden for det seneste år har ansat en medarbejder med en IT-uddannelse til at dække sine behov for kompetencer inden for informationssikkerhed, jf. figur 5.1 og figur 5.2.

Figur 5.1 Mere end hver tredje organisation har for nyligt ansat én med en IT-uddannelse...

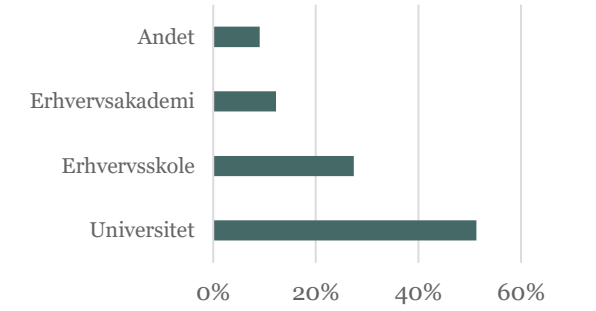
Har din arbejdsplads inden for det seneste år ansat en person med en IT-uddannelse til at dække jeres behov for IT-sikkerhedskompetencer?



Kilde: Spørgeskemaundersøgelse.
Anm.: N=817, fratrukket virksomheder uden en informationssikkerhedsjobfunktion til stede på arbejdspladsen.

Figur 5.2 ... Og det er primært personer med en universitetsbaggrund.

Hvor har de taget uddannelsen?



Kilde: Spørgeskemaundersøgelse.
Anm.: N=297

For mere halvdelen af de adspurgte virksomheder har de nyansatte en IT-uddannelse fra et universitet, mens 27 pct. af de adspurgte virksomheder og myndigheder svarer, at den ansatte har taget en IT-uddannelse på en erhvervsskole.

5.2 Sammenhængen mellem uddannelser og kompetenceprofiler

Et andet aspekt af kortlægningen af informationssikkerhedsuddannelser er sammenhængen med de kompetenceprofiler, som vi beskrev i kapitel 4.

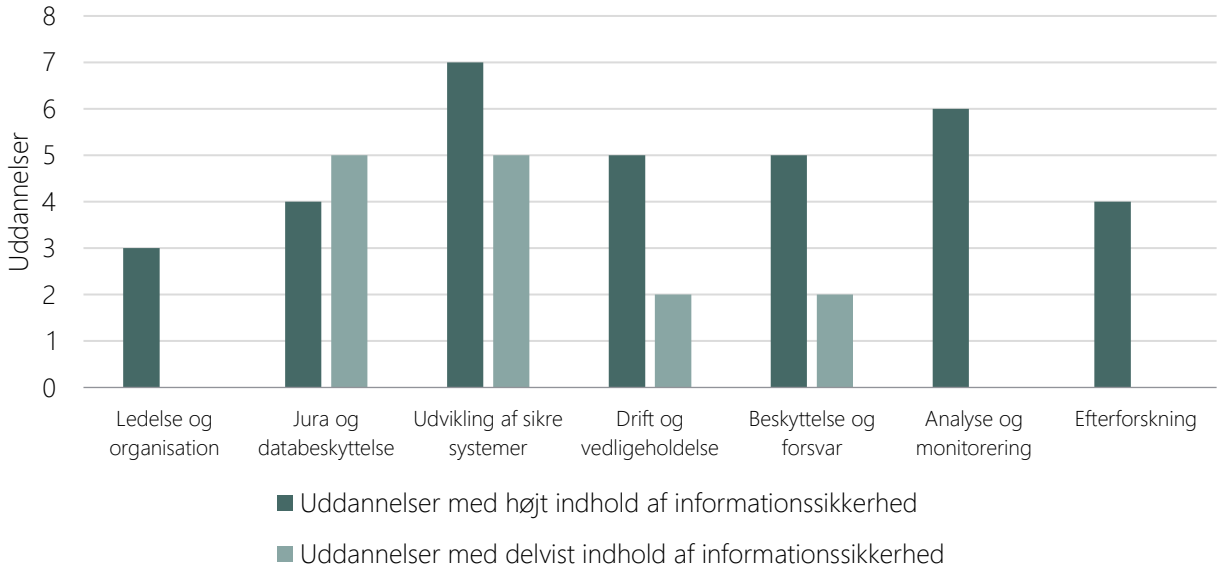
Uddannelserne er matchet med kompetenceprofilerne på baggrund af indholdet i kursusbeskrivelserne. Det vil sige, at vi konkret har set på læringsmål og kursusbeskrivelser i de enkelte uddannelser og sammenlignet med det 'kompetenceindhold', der er i en kompetenceprofil, og identificeret sammenfald. Da en uddannelse eller et kursus vedrørende informationssikkerhed sjældent er målrettet en kompetenceprofil, er de fleste uddannelser matchet med mere end en kompetenceprofil.

Matchet viser, at der er flest informationssikkerhedsuddannelser for kompetenceprofilen *Udvikling af sikre systemer*, det kan fx være en IT-ingeniør, hvis jobfunktion er at udvikle sikre systemer eller netværk. Her er der kortlagt syv uddannelser, som tilbyder mere end 30 ECTS-point inden for informationssikkerhed, jf. figur 5.3. Det fremgår også, at der for kompetenceprofilen *Ledelse og organisation* er færrest uddannelser, hvis kompetencer matches med profilen. Denne kompetenceprofil dækker over medarbejdere, der skal sikre, at organisationen som helhed har en politik for informationssikkerhed. Det er desuden også en af de kompetenceprofiler, som er mindre efterspurgt, jf. afsnit 4.

Af figur 5.3 fremgår det også, at uddannelser med et delvist indhold af informationssikkerhed kun dækker kompetenceprofilerne *Jura og databeskyttelse*, *Udvikling af sikre systemer*, *Drift og vedligeholdelse* samt *Beskyttelse og forsvar*. Det indikerer, at de resterende kompetenceprofiler er mere specialiserede og kun dækkes, hvis uddannelsen har et højt indhold af informationssikkerhed.

Figur 5.3 Flest uddannelser matcher kompetenceprofilen *Udvikling af sikre systemer*

Informationssikkerhedsuddannelser kategoriseret efter kompetenceprofiler



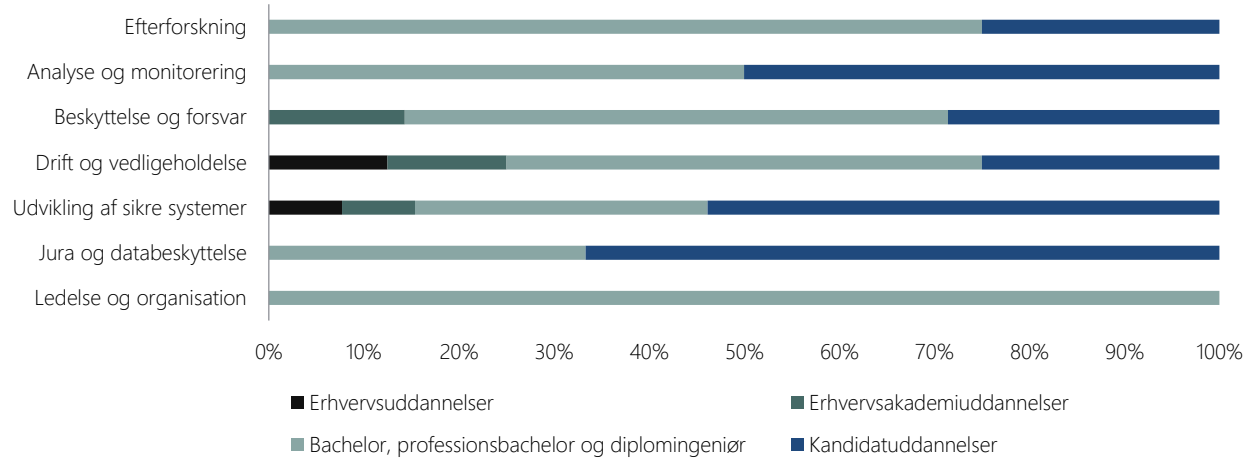
Kilde: HBS' gennemgang af informationssikkerhedsuddannelser.
Anm.: En informationssikkerhedsuddannelse kan matche med flere kompetenceprofiler.

Dykker vi ned i, hvordan mønsteret er for uddannelsesniveauet for de enkelte kompetenceprofiler, så bekræftes det igen, at (professions)bachelor- og kandidatuddannelser fylder mest, jf. figur 5.4. Vi ser også, at det er kompetenceprofilen *Jura og databeskyttelse,* som har den største andel af kandidatuddannelser. Andelen er

her mere end halvdelen (66 pct.), hvor det for kompetenceprofilen Drift og vedligeholdelse også er erhvervsuddannelser og erhvervsakademiuddannelser, der giver kompetencer.

Figur 5.4 De mellemlange og lange videregående uddannelser fylder mest

Fordelingen af uddannelser i kompetenceprofiler opgjort på uddannelsesniveau



Kilde: HBS' gennemgang af informationssikkerhedsuddannelser.
Anm.: En informationssikkerhedsuddannelse kan matche med flere kompetenceprofiler.

For kompetenceprofilerne *Efterforskning, Analyse og monitorering* og *Jura og databeskyttelse* er det uddannelser på (professions)bachelor- og kandidatuddannelsesniveau, der tilbyder de relevante kompetencer.

5.3 Personer i arbejdsstyrken med en uddannelse relateret til ISK

17.000 HAR EN UDDANNELSE, DER GIVER KOMPETENCER TIL AT ARBEJDE MED INFORMATIONSSIKKERHED

Som nævnt er der én formel uddannelse i det danske uddannelsessystem, som er fuldt rettet mod informationssikkerhed. Ligeledes er der få uddannelser, som tilbyder mere end 30 ECTS-point inden for informationssikkerhed. Fødekæden til arbejdsstyrken inden for informationssikkerhed er dog bredere og inkluderer også uddannelser, som tilbyder kurser, hvor den studerende lærer om informationssikkerhed relateret til et specifikt emne (fx Software Engineering). Derfor inkluderer vi også personer, som har gennemført sådanne uddannelser, når vi i det følgende opgør, hvor stor en del af arbejdsstyrken der har en uddannelse relateret til informationssikkerhed og dermed grundlæggende kompetencerne til at træde ind på dette arbejdsmarked.

Hvordan har vi målt ISK-arbejdsstyrken?
For at kvantificere, hvor mange i arbejdsstyrken der har opnået kompetencer relateret til informationssikkerhed (ISK-arbejdsstyrken) gennem uddannelsessystemet, har vi anvendt registerdata.

ISK-arbejdsstyrken består af personer, der:

(i) Har gennemført en **uddannelse med et højt indhold af informationssikkerhed**, dvs. hvor det i dag er muligt at opnå minimum 30 ECTS-point inden for informationssikkerhed.

Eller

(ii) Har gennemført en **uddannelse med et obligatorisk indhold af informationssikkerhed**, dvs. hvor der er obligatoriske kurser der tilsammen giver minimum 15 ECTS-point og informationssikkerhed indgår i læringsmålene (men ikke nødvendigvis udgør hele kurset).

I 2017 var der ca. 17.000 personer i den danske arbejdsstyrke, som havde gennemført en uddannelse relateret til informationssikkerhed[19] (se boks for definition på forrige side). Langt størstedelen af disse (85 pct.) har en videregående uddannelse inden for informations- og kommunikationsteknologi (IKT). Mens de resterende har en videregående uddannelse inden for fagområderne *Teknik, teknologi og industriel produktion* eller *Erhvervsøkonomi, administration og jura*[20].

Samlet set udgør arbejdskraft med en uddannelse relateret informationssikkerhed under 1 pct. af den samlede arbejdsstyrke. Men betragter vi de specifikke fagområder, er der stor variation i, hvor stor en andel der besidder kompetencer inden for informationssikkerhed. Således er det 42 pct. af arbejdsstyrken med en IKT-uddannelsesbaggrund, som besidder kompetencer vedrørende informationssikkerhed, jf. tabel 5.2, mens de tilsvarende andele for arbejdsstyrken med en uddannelsesbaggrund inden for *Teknik, teknologi og industriel produktion* og *Erhvervsøkonomi, administration og jura* er meget lave.

Tabel 5.2 Personer med ISK-kompetencer udgør en lille del af arbejdsstyrken

	Andel af arbejdsstyrken der har kompetencer inden for informationssikkerhed, 2017
Erhvervsøkonomi, administration og jura	0,2%
Teknik, teknologi og industriel produktion	0,6%
Informations- og kommunikationsteknologi (IKT)	42%

Kilde: HBS-beregninger på baggrund af data fra Danmarks Statistiks registre KOTRE og RAS.
Anm.: Arbejdsstyrken er afgrænset til beskæftigede og arbejdsløse i alderen 15-64 år. Inddeling af uddannelser i fagområder er baseret på Danmarks Statistiks uddannelsesklassifikation DISCED-15, Fagområde.

FÅ, DER FINDER ET INFORMATIONSSIKKERHEDSJOB, HAR EN UDDANNELSE RELATERET HERTIL

Meget få personer, der starter i et job, hvor arbejdsgiverne efterspørger informationssikkerhedskompetencer, har gennemført en uddannelse relateret til informationssikkerhed som kortlagt i dette kapitel. Beregningerne er foretaget på baggrund af jobopslagsdata matchet med data for jobskifte, jf. boks.

Resultaterne fra matchet mellem jobopslag og jobskiftedata viser at hver 5. person, der starter i et job, hvor arbejdsgiverne efterspørger informationssikkerhedskompetencer, har en teknisk uddannelsesbaggrund, jf. figur 5.5. Ligeledes har hver femte person en uddannelsesbaggrund inden for fagområdet *Erhvervsøkonomi, administration og jura*.

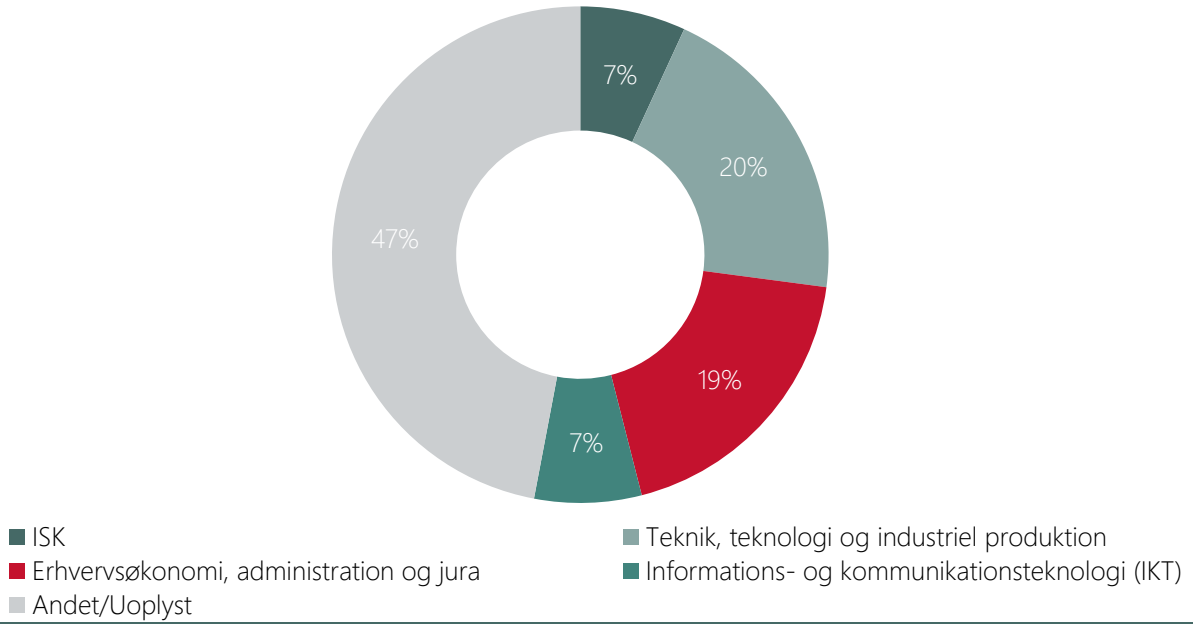
Hvordan kvantificerer vi, hvem der finder et informationssikkkerhedsjob?

Beregningerne for, hvem der bliver ansat i et informationssikkerhedsjob, er foretaget ved at matche jobopslag med personer, der skifter job. Matchet mellem jobopslag og jobskifte er baseret på virksomhedens CVR-nummer og jobopslagets stillingsbetegnelse. Herefter er der tilkoblet data for, om personen har gennemført en ISK-relateret uddannelse.

[19] Beregningen er foretaget på baggrund af data fra Danmarks Statistiks registre KOTRE og RAS.

[20] Inddelingen i fagområder er baseret på Danmarks Statistiks uddannelsesklassifikation DISCED-15, Fagområde.

Figur 5.5 Uddannelsesbaggrund for ansatte i et informationssikkerhedsjob



Kilde: HBS-beregninger på baggrund af HBS Jobindex og Danmarks Statistiks registre AMRUN og KOTRE for 2010-2017.

Mange af dem, der starter i et informationssikkerhedsjob, har altså ikke gennemført en uddannelse relateret til informationssikkerhed. Dette indikerer, at arbejdsmarkedet for ISK-arbejdskraft er kendetegnet ved at de beskæftigede opnår deres kompetencer på anden vis. Dette resultat afspejler sandsynligvis også, at udbuddet af ISK-relaterede uddannelser er relativt nyt. Således vil en stor del af dem, der arbejder inden for informationssikkerhed i dag, have opnået deres kompetencer på anden vis end gennem det formelle uddannelsessystem.

Disse resultater stemmer også overens med andre undersøgelser, der peger på, at IT-branchen er karakteriseret ved, at mange af de beskæftigede er autodidakte[21]. De kvalitative interview bekræfter ligeledes dette. Informanter fra offentlige myndigheder beskriver eksempelvis, hvordan medarbejdere med akademisk baggrund (fx DJØF'eren) i høj grad varetager opgaver i relation til GDPR-reglerne.

[21] Højbjerre Brauer Schultz: Virksomheders behov for digitale kompetencer (2016)

6. Rekruttering og fremtidigt behov for kompetencer

Afsnittets hovedresultater

- Arbejdsmarkedet for informationssikkerhedskompetencer i Danmark er præget af stærk konkurrence
- Danske organisationer er meget digitaliserede, men der et uindfriet potentiale for arbejdsmarkedet for personer med kompetencer inden for informationssikkerhed
- Hver femte organisation har svært ved at rekruttere medarbejdere med de rette kompetencer – udfordringerne er størst for SMV'er
- Særligt medarbejdere med tekniske kompetencer relateret til informationssikkerhed er vanskelige at rekruttere
- Ændring af uddannelsessammensætning frem mod 2030 trækker i retningen af et øget udbud af personer med informationssikkerhedskompetencer

I dette afsnit vil vi se på rekrutteringssituationen for informationssikkerhedskompetencer (ISK-kompetencer) samt vurdere, hvad det fremtidige behov er. Først beskrives, hvordan arbejdsmarkedet ser ud for ISK-kompetencer, da det giver en forståelse for udgangspunktet. Dernæst beskrives rekrutteringssituationen og det fremtidige behov.

6.1 Hvordan er presset på arbejdsmarkedet for Informationssikkerhed?

I dette afsnit beskriver vi konkurrencepresset for kompetencer vedr. informationssikkerhed. Fokus er på ledighed og løn, idet begge er indikatorer for, om der er mangel på arbejdskraft for en given gruppe.

LAV LEDIGHED OG HØJ LØN – ISÆR BLANDT DEM MED TEKNISK KOMPETENCER

Personer med en uddannelse inden for informationssikkerhed har lav ledighed og høj løn. Det er en indikator for, at efterspørgsel efter denne faggrupper er relativt høj. For personer med en kort eller mellemlang uddannelse inden for informationsteknologi lå ledigheden på 3 pct. i 2017, mens ledigheden for dem med en langvideregående uddannelse var helt nede på 1 pct. i samme år. Det er betydeligt højere end andre faggrupper som fx samfundsvidenskab og naturvidenskab, jf. Tabel 6.. Tilsvarende lå den gennemsnitlige løn også højere for personer med en uddannelse inden for informationsteknologi sammenlignet med de andre grupper. Det gjaldt, uagtet om det er på kort, mellemlangt eller videregående niveau.

Tabel 6.1 Ledighed og løn for udvalgte fagområder

Hovedområde	Fagområde	Ledighed	Gennemsnitlig løn
Korte videregående uddannelser, KVU	Samfundsvidenskab	3%	349.419
Korte videregående uddannelser, KVU	Naturvidenskab	2%	402.374
Korte videregående uddannelser, KVU	**Informations- og kommunikationsteknologi (IKT)***	**3%**	**445.370**
Mellemlange videregående uddannelser, MVU	Samfundsvidenskab	4%	372.132
Mellemlange videregående uddannelser, MVU	Naturvidenskab	11%	360.860
Mellemlange videregående uddannelser, MVU	**Informations- og kommunikationsteknologi (IKT)***	**3%**	**421.972**
Lange videregående uddannelser, LVU	Samfundsvidenskab	4%	457.512
Lange videregående uddannelser, LVU	Naturvidenskab	3%	493.058
Lange videregående uddannelser, LVU	**Informations- og kommunikationsteknologi (IKT)***	**1%**	**526.098**

Kilde: Danmarks Statistik, RAS (ledighed) og SMALT_LOENBELOEB (LØN).
Anm.: *Kun ITS-uddannelser indgår. Ledigheden er beregnet pr. 30. november 2017. Kun personer i arbejdsstyrken, som indgik i befolkningen pr. 1. januar 2017, indgår i tabellen. Gennemsnitlig løn er beregnet på baggrund af de beskæftigede og er ekskl. ATP og frynsegoder.

Det er et billede, der bliver bekræftet af de kvalitative interview. Her peger informanterne fra både den offentlige og private sektor på, at medarbejdere med kompetencer inden for informationssikkerhed er stærkt efterspurgt. Det er særligt medarbejdere med, hvad informanterne kalder for 'tekniske kompetencer', der er stærkt efterspurgt, og om hvem konkurrencen er størst. Med tekniske kompetencer menes oftest medarbejdere med ingeniørbaggrund. Konkurrencen kommer ifølge informanterne til udtryk ved, at de har en høj løn og ofte skifter job.

Desuden peger to kommunale informanter på, at de ikke kan konkurrere med det private lønniveau. Derfor må de i højere grad selv oplære medarbejdere for at dække behovet for medarbejdere med ITS-kompetencer. Dette afspejles også i resultaterne om kommunernes brug af opkvalificering, jf. afsnit 8. Her fremgår det, at kommunerne i særlig grad benytter sig af oplæring.

6.2 Rekruttering af kompetencer inden for informationssikkerhed

I dette afsnit undersøger vi, om virksomheder og myndigheder oplever udfordringer ved rekruttering af arbejdskraft med kompetencer inden for informationssikkerhed.

REKRUTTERING ER KONCENTRERET PÅ UDVALGTE BRANCHER

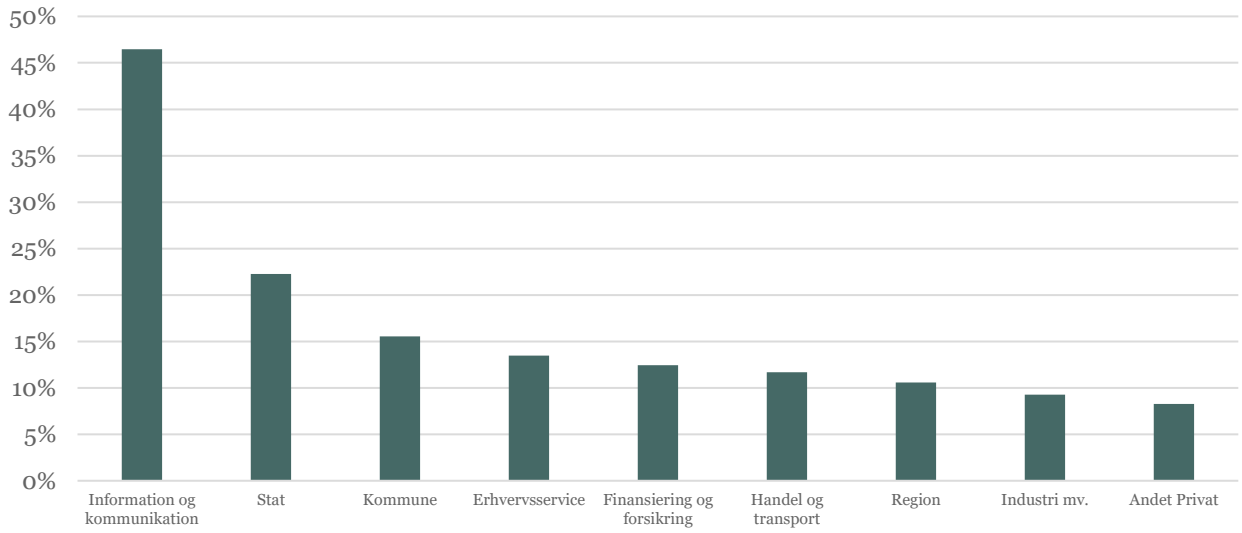
Overordnet set er det et mindretal af de adspurgte organisationer, der har forsøgt at rekruttere kompetencer inden for informationssikkerhed. Vores spørgeskemaundersøgelse viser endvidere, at det i udtalt grad er inden for branchen *Information og kommunikation*, at flest virksomheder har forsøgt at rekruttere inden for det seneste halve år. Det gælder 46 pct. af de adspurgte virksomheder i branchen, jf. Figur 6.1. Det flugter med tidligere analyser, der peger på, at *Information og kommunikation* er den største aftagerbranche af medarbejdere med IT-sikkerhedskompetencer[22]. Derudover er det i staten (22 pct.), kommunerne (16 pct.), i Erhvervsservice (13 pct.) samt Finansiering og forsikring (12 pct.), at rekrutteringsbehovet er størst.

[22] Kilde: Højbjerre Brauer Schultz: Efterspørgslen efter IT-sikkerhedsmedarbejdere i Hovedstadsområdet (2017). Undersøgelsen er ikke 1:1 sammenlignelignelig, da den ser på behovet for IT-sikkerhedsmedarbejdere og ikke benytter den definition, som denne rapport gør, nemlig informationssikkerked.

Dette billede er i overensstemmelse med analysen af efterspørgsel efter ISK-kompetencer i kapitel 3. Således er efterspørgslen efter arbejdskraft med ISK-kompetencer (målt på antal jobopslag) størst i brancherne *Offentlig administration, undervisning og sundhed*, *Information og kommunikation* samt *Erhvervsservice*. Tilsammen står de tre brancher for godt 60 pct. af alle ISK-jobopslag i 2018.

Figur 6.1 Størst rekrutteringsbehov inden for Information og kommunikation

Andel af virksomheder, der inden for det seneste halve år har forsøgt at rekruttere ansatte med ITS-kompetencer inden for en given branche



Kilde: Spørgeskemaundersøgelse.
Anm.: N=817. 'Industri mv.' dækker over brancherne Industri, råstofindvinding og forsyningsvirksomhed.

Det er konklusioner, som også er afspejlet i andre undersøgelser, fx i Europakommissionens analyse af behovet for IT-kompetencer i SMV'er[23].

HVER FEMTE ORGANISATION HAR UDFORDRINGER MED AT REKRUTTERE

Vi har yderligere undersøgt, i hvilket omfang en organisation kan rekruttere medarbejdere med de rette kompetencer inden for informationssikkerhed. Det er gjort ved at spørge organisationer om rekrutteringsforsøg, og om stillingen blev besat med den rette profil. Resultatet rapporteres ved brug af begrebet 'forgæves rekrutteringsrate' (FRR), der er andelen af organisationer, som ikke har fået stillingen besat med den rette profil.

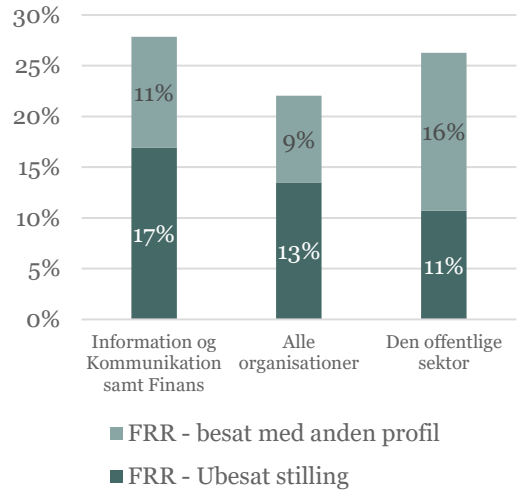
Vores undersøgelse viser samlet set, at mere end hver femte organisation har udfordringer med at rekruttere en medarbejder, som har de efterspurgte kompetencer inden for informationssikkerhed, jf. Figur .

Deler vi resultatet for FRR op, så er det 13 pct. af de adspurgte organisationer, som har ubesatte stillinger, mens 9 pct. af organisationerne ansatte en profil, der ikke havde alle de efterspurgte kompetencer. Det skal bemærkes, at der på dette spørgsmål er en vis usikkerhed, idet det bygger på svar fra 130 organisationer, som havde et rekrutteringsbehov. Dog understøtter de kvalitative interview entydigt dette billede. Informanterne fremhæver særligt, at det er vanskeligt at finde personer, som har alle de kompetencer, organisationer efterspørger, og at man som organisation ofte må gå på kompromis.

[23] Se fx Europakommissionen: Supporting specialised skills development: Big Data, Internet of Things and Cybersecurity for SMEs (2019).

Figur 6.2 Mere end hver femte organisation har svært ved at rekruttere den rette profil inden for informationssikkerhed

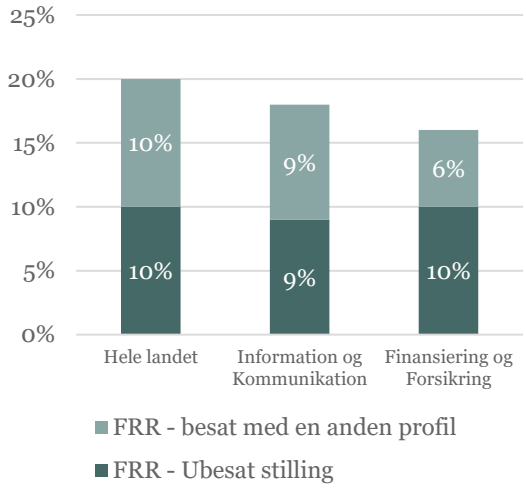
Forgæves rekrutteringsrate (FRR), medarbejdere med kompetencer inden for informationssikkerhed



Kilde: Spørgeskemaundersøgelse.
Anm: n=130. På grund af stor usikkerhed på resultaterne fra øvrige brancher er de ikke inkluderet i denne figur, ligesom nogle brancher er lagt sammen. Kategorien 'den offentlige sektor' består i dette tilfælde af organisationer, som har angivet, at de arbejder i hhv. en region, staten eller en kommune.

Figur 6.3 Lettere at rekruttere, når det ikke kun er kompetencer vedr. informationssikkerhed

Forgæves rekrutteringsrate (FRR), alle typer af medarbejdere



Kilde: Rekrutteringssurvey juni 2019, Styrelsen for Arbejdsmarked og Rekruttering (2019)

Resultaterne viser også, at udfordringerne er størst i brancherne *Information, kommunikation* og *Finans*, hvor 28 pct. af organisationerne ikke fik rekrutteret den rette profil til stillingen. I disse brancher har 17 pct. af de adspurgte organisationer ubesatte stillinger, der kræver kompetencer vedr. informationssikkerhed.

For den offentlige sektor er rekrutteringsudfordringen på niveau med virksomhedernes i brancherne *Information, Kommunikation* og *Finans*. Således fik 28 pct. af arbejdsgiverne i den offentlige sektor ikke rekrutteret den rette profil til stillingen. Men der er en markant forskel i andelen af stillinger, der besættes med en forkert profil. I den offentlige sektor udgøres de forgæves rekrutteringer i højere grad af personer, som ikke har alle de nødvendige kompetencer (16 pct. af de adspurgte myndigheder). Det tyder på, at man i den offentlige sektor i højere grad 'dækker' behovet for kompetencer med personer, der ikke fuldt ud har de rette kompetencer (fænomenet kaldes substitution).

Ifølge de kvalitative interview med informanter fra den kommunale sektor har de generelt vanskeligt ved at rekruttere og fastholde medarbejdere med kompetencer inden for informationssikkerhed, da de ikke kan konkurrere med det private på løn. Det er et velkendt billede, at lønnen for IT-medarbejdere er markant højere i det private end i det offentlige. Fx viser en undersøgelse fra Danmarks Statistik[24], at lønnen for jobfunktionen *Udvikling og analyse af software og applikationer* er det job, hvor forskellen mellem det private og det offentlige er allerstørst (52 kr. i timen).

KOMPETENCER VEDR. INFORMATIONSSIKKERHED ER RELATIVT SVÆRERE AT REKRUTTERE

Så vidt vides eksisterer der ikke andre tal for rekrutteringsudfordringerne for medarbejdere med kompetencer inden for informationssikkerhed. Derfor er der ikke et direkte grundlag at sammenligne med. Styrelsen for Arbejdsmarked og Rekruttering (STAR) udfører løbende undersøgelser af rekrutteringssituationen på det danske arbejdsmarked på en måde, der kan sammenlignes med resultaterne i nærværende analyse. Således

[24] Danmarks Statistik: "Forskellen på lønninger i det offentlige og det private svinger fra job til job", 19. februar 2018.

ser STAR også på ubesatte stillinger og stillinger besat med en 'forkert' profil. Her viser resultaterne[25] på brancheniveau, at den forgæves rekrutteringsrate for *Information, Kommunikation* og *Finans* ligger på hhv. 18 pct. og 16 pct., jf. Figur . Dermed ligger niveauet for forgæves rekrutteringer i disse to brancher betydeligt under, når vi ser på alle kompetencer og ikke isoleret på kompetencer inden for informationssikkerhed. Altså er udfordringerne relativt større i disse brancher, når det gælder medarbejdere med kompetencer inden for informationssikkerhed. Det er ikke muligt i STAR's undersøgelse at isolere den offentlige sektor, hvorfor den ikke er medtaget i figuren.

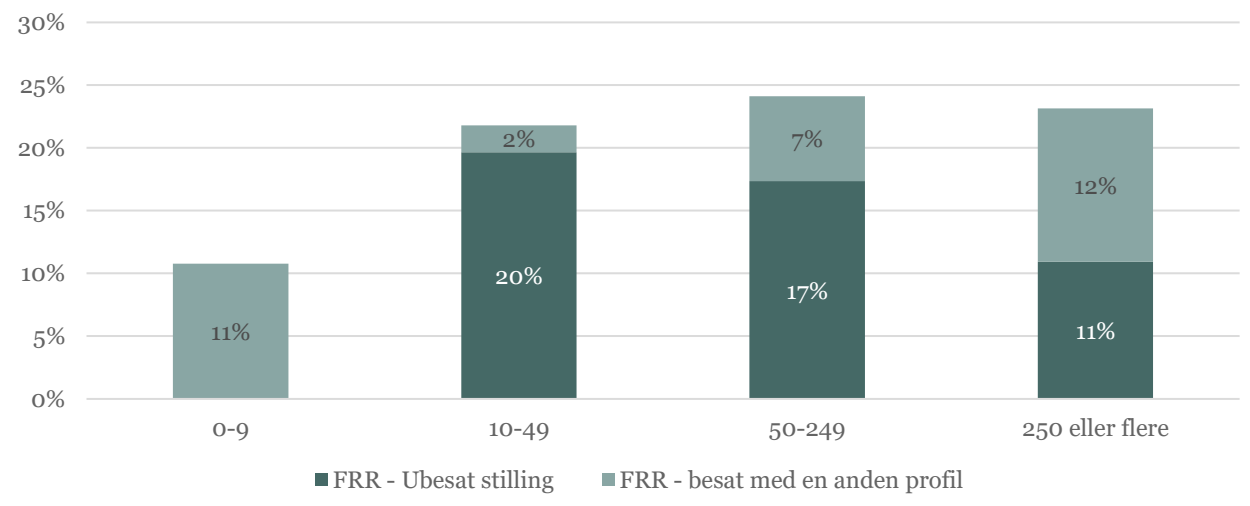
UDFORDRINGERNE ER STØRST I DE MINDRE VIRKSOMHEDER

Vi ved fra tidligere undersøgelser, at organisationsstørrelse har betydning for, hvor veludviklet IT-sikkerhedskulturen er[26]. Derfor vil vi se særskilt på, om vi kan se nogle mønstre i rekrutteringsudfordringerne, når vi tager højde for virksomhedsstørrelse. Her viser vores resultater, at det er virksomheder i størrelsesorden 10-49, som har den højeste andel af ubesatte stillinger, nemlig 20 pct., jf. figur 6.4. Billedet er omtrent det samme for virksomheder med 50-249 ansatte, det vil sige virksomheder i SMV-segmentet.

Resultaterne viser også, at de store virksomheder går mest på kompromis med de kandidater, de ansætter (ansætter profil, der ikke har alle de efterspurgte kompetencer). Således var det 12 pct. af ansættelserne i virksomheder med over 250 ansatte, hvor kandidaten ikke havde alle de ønskede kompetencer. Det kan skyldes, at kompetencebehovet er mere komplekst i store organisationer, eller at store organisationer bedre er i stand til selv at stå for videre- efteruddannelse af de medarbejdere, som arbejder med informationssikkerhed.

Figur 6.4 Mindre virksomheder har sværest ved at rekruttere

Forgæves rekrutteringsrate (FRR), opdelt på organisationsstørrelse.



Kilde: Spørgeskemaundersøgelse.
Anm.: n=130, organisationer, som har haft et rekrutteringsbehov for kompetencer inden for informationssikkerhed.

HVAD ER DET FOR NOGLE KOMPETENCER, DER ER SVÆREST AT REKRUTTERE?

Et andet aspekt af rekrutteringen på arbejdsmarkedet for informationssikkerhedskompetencer er, hvilke konkrete jobprofiler, som er mest vanskelige at rekruttere. Billedet er, at det stort set er lige vanskeligt at rekruttere de enkelte jobprofiler, jf. figur 6.5. Dog viser resultaterne, at organisationerne går mest på kompromis, når de skal rekruttere kompetencer inden for jobprofiler som *Analysere* og *Efterforskning*. Det vil sige, at det er specialiserede kompetencer, som i høj grad kræver tekniske kompetencer, og som bruges til fx at

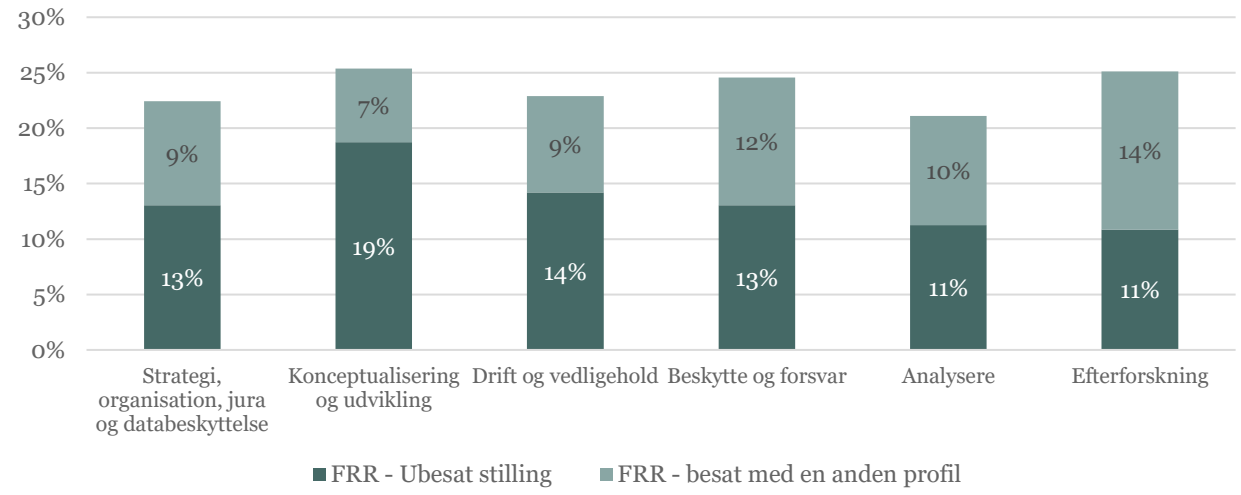
[25] Styrelsen for Arbejdsmarked og Rekruttering: Rekrutteringssurvey juni 2019. Udgivet august 2019.

[26] Deloitte (2018a) It-sikkerhed og datahåndtering i danske SMV'er.

efterforske cyberangreb. Det bemærkes dog, at resultatet for denne konklusion bygger på et relativt lille antal svar, hvorfor resultaterne om forskellene imellem de seks jobprofiler skal tages med forbehold.

Figur 6.5 Kompromis med specialister inden for analyse og efterforskning

Forgæves rekrutteringsrate (FRR), opdelt på jobprofiler.



Kilde: Spørgeskemaundersøgelse.

Anm.: Jobprofilerne Strategi, Organisation samt Jura og databeskyttelse er i denne konkrete figur slået sammen til én, n=19.

Det billede bliver generelt bekræftet på tværs af de kvalitative interview. Det er langt størstedelen af informanterne, som fremhæver, at jo mere tekniske medarbejderne bliver, desto vanskeligere er det at rekruttere. Mønsteret går med andre ord igen fra informanter i både det offentlige og det private, herunder i virksomheder, der specifikt har specialiseret sig i ydelser vedr. informationssikkerhed.

Informanterne fremhæver også, at når de skal rekruttere medarbejdere med de mest tekniske kompetencer, leder de typisk efter medarbejdere, hvis tekniske grundkompetencer er på plads, fx ingeniører. Herefter oplærer de dem i de konkrete kompetencer (*on the job training*). Dette afspejles også i kapitel 7 om opkvalificering og efteruddannelse og kan være et udtryk for, at udbuddet er mindre end efterspørgslen.

6.3 Fremskrivning af udbuddet

I dette afsnit er fokus på det fremadrettede behov for arbejdskraft inden for informationssikkerhed. Det er vanskeligt at forudsige det fremtidige behov for kompetencer inden for informationssikkerhed. Derfor vil vi først beskrive det fremtidige udbud, dernæst den fremtidige efterspørgsel.

ÆNDRINGER I SAMMENSÆTNINGEN AF UDDANNELSER ØGER ISK-UDBUDDET

Udbuddet af ISK-kompetencer i fremtiden afhænger af, hvilke uddannelser arbejdsstyrken vil have. Arbejdskraftudbuddet med en ISK-relateret uddannelse består af:

- Personer, som har gennemført en uddannelse, hvor der som minimum tilbydes 30 ECTS-point inden for informationssikkerhed (uddannelser med et højt indhold af informationssikkerhed)
- Personer, som har gennemført en uddannelse, hvor der som minimum er 15 obligatoriske ECTS-point inden for informationssikkerhed (uddannelser med et obligatorisk indhold af informationssikkerhed).

Til sammen udgør de to det, som i det følgende benævnes ISK-relaterede uddannelser. I kap 5 blev det estimeret, at der er ca. 17.000 i arbejdsstyrken med en ISK-relateret uddannelse.

På trods af, at mange arbejder i ISK-jobs uden en uddannelse, som direkte er relateret til ISK-kompetencer, udgør de ISK-relaterede uddannelser en central fødekilde for organisationerne til at besætte ISK-jobs. For at få et indtryk af, hvordan udbuddet af ISK-kompetencer kan forventes at udvikle sig, er der gennemført en fremskrivning af arbejdskraft med en ISK-relateret uddannelse. Konkret er det en fremskrivning af (i) personer med en uddannelse med et højt indhold af informationssikkerhed og (ii) personer med en uddannelse med et obligatorisk indhold af informationssikkerhed.

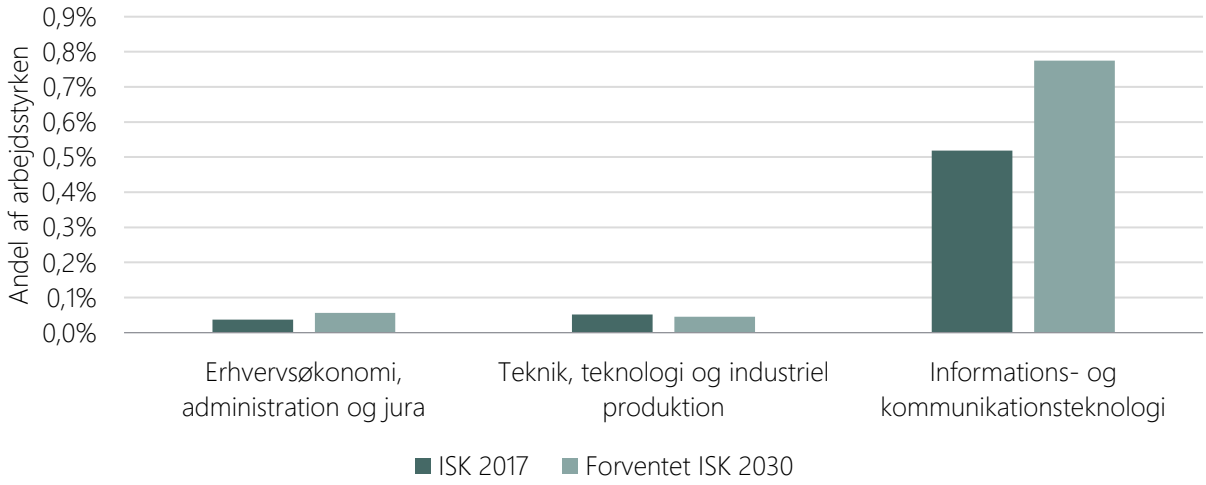
Vi vil fremskrive, hvor stor en del af arbejdsstyrken, som i 2030 forventes at have en ISK-relateret uddannelse. Der er knyttet en vis usikkerhed til disse fremskrivninger, og de vil være alt andet lige-betragtninger, men de giver stadig vigtig viden, der kan bruges til at indikere behovet for ISK-kompetencer. Fremskrivningen bygger videre på Uddannelses- og Forskningsministeriets uddannelsesfremskrivning (se afsnit 8.4 for metode).

Vores fremskrivning viser, at (planlagte) ændringer i sammensætningen af uddannelser vil øge arbejdsstyrken med en ISK-relateret uddannelse frem mod 2030. Fremskrivning af uddannelsesoptaget viser, at antallet af personer i arbejdsstyrken med en ISK-relateret uddannelse vil vokse med ca. 9.000 frem mod 2030. Således forventes der at være 26.000 personer i arbejdsstyrken med en uddannelse relateret til informationssikkerhed. Det svarer til en stigning i andelen af arbejdsstyrken fra 0,6 til 0,8 pct. – eller en tredjedel flere. Fremskrivningen viser altså, at ændringerne i uddannelsessammensætningen i de kommende år vil øge udbuddet af ISK-kompetencer betydeligt.

Hovedparten af den forventede arbejdsstyrke med en uddannelse relateret til informationssikkerhed vil have en uddannelse inden for informations- og kommunikationsteknologi (IKT). Således forventes det, at 8.000 ud af de 9.000 ekstra i arbejdsstyrken med en uddannelse inden for informationssikkerhed vil have en IKT-uddannelse. Det er også for denne faggruppe, at andelen af arbejdsstyrken er størst og forventes at vokse mest – fra 0,5 pct. til 0,8 pct., jf. figur 6.6.

De resterende 1.000, som ISK-arbejdsstyrken forventes at vokse med, vil have en uddannelse, inden for *Erhvervsøkonomi, administration og jura* eller *Teknik, teknologi og industriel produktion*. For begge disse faggrupper gælder det, at andelen af arbejdsstyrken, hvis uddannelse også er relateret til informationssikkerhed, er mindre end 0,1 pct., jf. figur 6.6.

Figur 6.6 Personer med en ISK-relateret uddannelse i dag og i 2030



Kilde. Egne beregninger på baggrund af registerdata og UFM's uddannelsesfremskrivning
Anm.: For 2017 er arbejdsstyrken beregnet som det samlede antal beskæftigede og ledige i alderen 15-64 år. For 2030 er arbejdsstyrken baseret på DREAM's fremskrivning af arbejdsstyrken[27]. Inddeling af uddannelser i fagområder er baseret på Danmarks Statistiks uddannelsesklassifikation DISCED-15, Fagområde.

[27] *DREAM* Fremskrivning af befolkningens arbejdsmarkedstilknytning (2019).

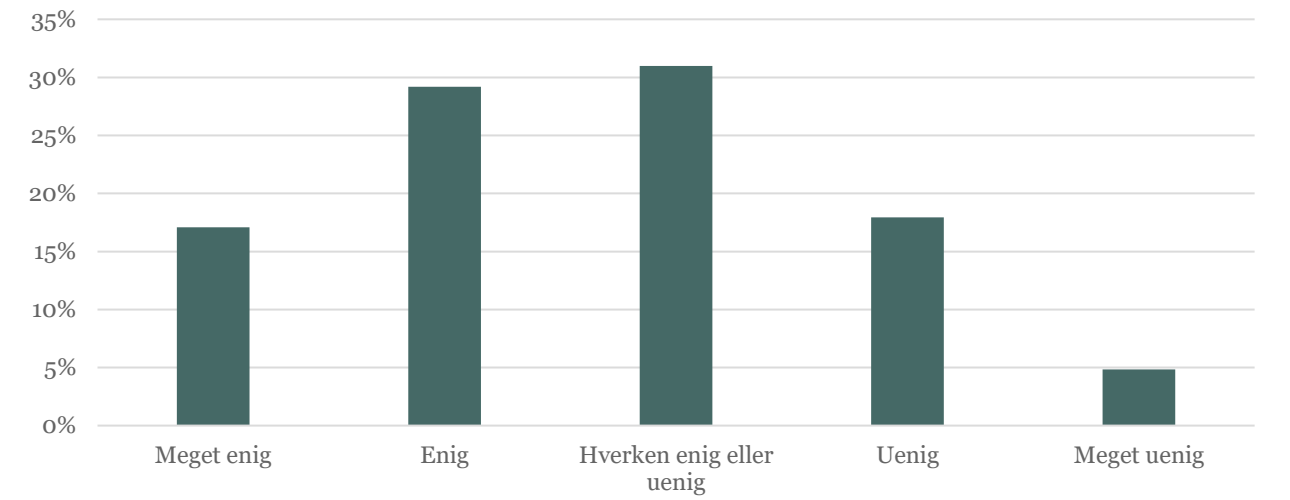
Da der er tale om en fremskrivning af uddannelser, som er relateret til informationssikkerhed, er det ikke nødvendigvis alle uddannede, som opnår ISK-specialistviden. Men alligevel udgør de ofte de personer, som gennem oplæring på virksomhederne og gennem private kurser specialiseres inden for informationssikkerhed. På den baggrund vurderes det at bidrage til at øge udbuddet af ISK-kompetencer. Både ved, at flere opnår ISK-kompetencer gennem deres uddannelse og ved at øge volumen til fødekanalerne for virksomheders og myndigheders egen opkvalificering og specialisering af medarbejderne.

ORGANISATIONERNE FORVENTER, AT BEHOVET VIL VOKSE DE KOMMENDE ÅR

En anden måde at belyse det fremtidige behov på er at spørge organisationerne selv. Organisationernes vurdering er, at behovet for medarbejdere, der arbejder med informationssikkerhed vil stige de kommende 5 år. Således svarer næsten halvdelen (46 pct.), at de er meget enig eller enig i, behovet for medarbejdere, der arbejder helt eller delvist med IT-sikkerhed, vil stige på deres arbejdsplads, jf. figur 6.7. Næsten hver tredje (31 pct.) er hverken enig eller uenig, og de dermed forventer et uændret behov. Næsten hver femte (18 pct.) af de adspurgte organisationer er uenige.

Figur 6.7 Halvdelen af alle organisationer forventer et større behov

Andele, som er enig eller uenig i udsagnet: Om 5 år vil der på min arbejdsplads være behov for flere medarbejdere, der arbejder helt eller delvist med IT-sikkerhed.



Kilde: Spørgeskemaundersøgelse.
Anm.: n=817

Informanterne fra de kvalitative understøtter dette billede entydigt, og de forventer at behovet vil stige markant de kommende år.

FLERE FORHOLD UNDERSTØTTER VURDERINGEN AF ØGET BEHOV

Belyser vi det fremtidige behov yderligere, så peger en række indikatorer og trends peger på, at man kan forvente en stigning i efterspørgslen efter ISK-arbejdskraft i de kommende år. Både de kvantitative indikatorer, som er beskrevet tidligere i denne rapport, fx den markante stigning i efterspørgslen, som har været mere intensiv end den generelle stigning i efterspørgsel efter digitale kompetencer, jf. kapitel 3. Men også en række kvalitative trends, der er baseret på andre analyser, som vi vurderer vil ændre *karakteren* af efterspørgslen. Der er selvfølgelig stor usikkerhed forbundet med konsekvenserne af de kvalitative trends. Med det forbehold vurderer vi, at følgende forhold vil øge og præge efterspørgslen efter kompetencer inden for informationssikkerhed i de kommende år:

- Fortsat digitalisering af samfund og forretningsmodeller
- Høj og stigende cybertrussel

- Professionalisering af informationssikkerhed i SMV'er
- Informationssikkerhed kan blive et konkurrenceparameter for organisationer
- Fokus på informationssikkerhed i den offentlige sektor og offentligt-privat samarbejde
- Den teknologiske udvikling påvirker efterspørgslen
- Efterspørgslen efter efteruddannelse og certificeringer kan stige
- Uindfriet potentiale for efterspørgslen

Nedenfor vil vi beskrive ovenstående forhold yderligere.

Fortsat digitalisering af samfund og forretningsmodeller. En fortsat digitalisering af samfundet og forretningsmodeller vil medføre mere data og et større behov for kompetencer inden for informationssikkerhed. Det dækker blandt andet over, at enheder og systemer er forbundne (fx Internet of Things), og samfundet i stigende grad er afhængigt af digital infrastruktur. Behovet for viden om datasikkerhed, data-samkøring og ansvar, når man fx indgår aftaler med private IT-leverandører, kan udgøre en barriere for den fortsatte digitalisering af det offentlige og ikke mindst til udnyttelsen af AI og datadreven innovation. Det afspejler, at der kan være behov for nye 'hybrid' kompetenceprofiler på et avanceret niveau, der fx kobler jura og informationssikkerhed[28].

Høj og stigende cybertrussel. Der har været et voksende antal tilfælde af IT-kriminalitet, og det forventes, at IT-kriminalitet i de kommende år vil have et større omfang end tyverier i øvrigt. Manglende bevidsthed om arten og omfanget af IT-kriminalitet udgør en barriere for, at virksomheder får udviklet en professionel praksis for informationssikkerhed. Det vil sandsynligvis øge efterspørgslen efter kompetencer inden for informationssikkerhed[29].

Professionalisering af informationssikkerhed i SMV'er. Der er en manglende sikkerhedskultur i SMV'erne, fx synes SMV-investeringer i opkvalificering af medarbejderne inden for informationssikkerhed at være sporadisk. Og fx ved vi fra tidligere undersøgelser, at en tredjedel virksomheder investerer i opkvalificering af medarbejdere i informationssikkerhed – 67 pct. svarer nej til, at de træner nogle eller alle medarbejdere i informationssikkerhed. Kulturen er i øvrigt præget af en uformel mundtlig information og kommunikation, som kan udvirke en lav organisatorisk bevidsthed om sikkerhedsproblemstillinger på informationssikkerhedsområdet. Dermed er der også en lav grad af bevidsthed om, hvad man faktisk skal kunne for at håndtere informationssikkerhed professionelt i virksomhedens digitalisering og forretningsmodel[30].

Informationssikkerhed kan blive et konkurrenceparameter. Informationssikkerhed anvendes ikke som konkurrenceparameter af SMV'er, og kun få har implementeret sikkerhedsforanstaltninger af forretningsmæssige årsager. Dette kan betyde, at investeringer i informationssikkerhed, herunder også i opkvalificering og professionalisering af de ansatte, betragtes som en udgift og ikke som et middel til at øge virksomhedens konkurrenceevne[31]. I lyset af ovenstående forhold er det sandsynligt, at informationssikkerhed kan blive et konkurrenceparameter i fremtiden for SMV'erne – man vil som forbruger eller kunde se på, om virksomheden er 'digitalt sikker'. Fx har Folketinget lige besluttet en ny mærkningsordning for IT-sikkerhed og ansvarlig dataanvendelse, hvilket ligeledes vil understøtte denne udvikling[32].

Fokus på informationssikkerhed i den offentlige sektor og offentligt-privat samarbejde. ISO 27001, som er international standard til etablering af et ledelsessystem for informationssikkerhed, skal være implementeret i de statslige myndigheder i 2016. Det skyldes, at standarder kan være drivende for professionaliseringen af informationssikkerhed og påvirke efterspørgslen efter kompetencer. Det kan både være i relation til at lede og planlægge samarbejdet, såvel som for den tekniske og organisatoriske implementering.

[28] Deloitte (2018b) Analyse af barrierer for udbredelse af nye teknologier (for digitaliseringsstyrelsen)
[29] Deloitte (2017). The future market for IT security in Denmark
[30] Deloitte (2018a)
[31] Deloitte (2018a) It sikkerhed- og datahåndtering i danske SMV'er
[32] https://em.dk/nyhedsarkiv/2019/oktober/nyt-maerke-for-it-sikkerhed-og-ansvarlig-dataanvendelse-paa-vej/

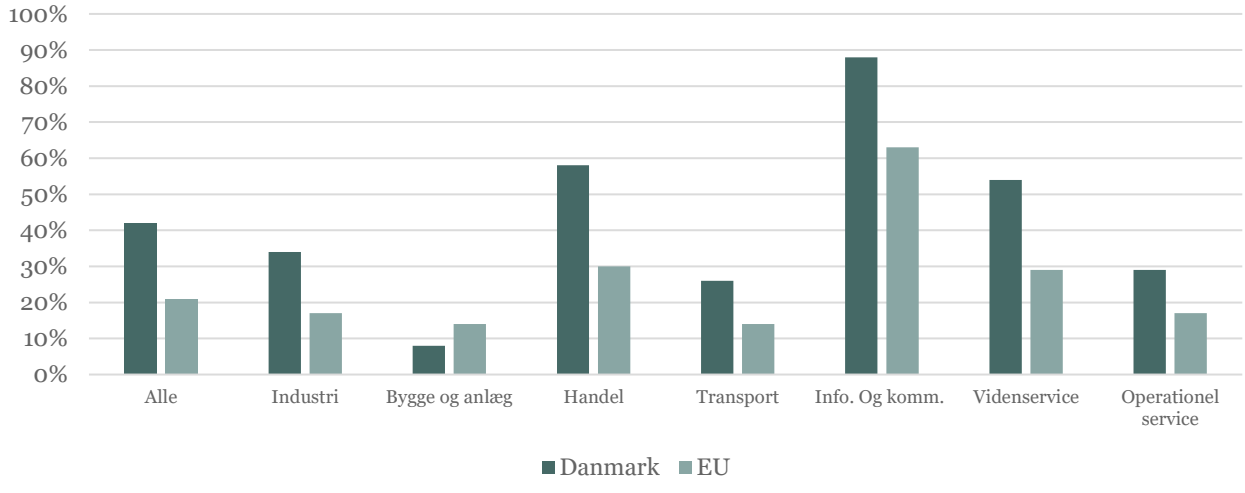
Den teknologiske udvikling påvirker efterspørgslen. Der tegner sig forskellige scenarier for, hvordan den teknologiske udvikling kan påvirke efterspørgslen efter ISK. En faktor, som kan reducere antallet af medarbejdere inden for informationssikkerhed, er automatiseringen af rutineprægede arbejdsfunktioner. Det kan reducere nogle af de mere standardiserede jobfunktioner. Omvendt besidder kunstig intelligens (KI) endnu ikke den kontekstbevidsthed, som mennesker gør. Derfor er vurderingen, at man i langt højere grad vil se, at medarbejdere inden for informationssikkerhed samarbejder med KI-baserede løsninger fremfor et rent automations-scenarie. En anden faktor, som kan påvirke efterspørgslen, er virksomhedernes brug af cloud-løsninger, da cloud-service-leverandører i stigende omfang integrerer sikkerhedsløsninger, som modsvarer en virksomheds digitale stadie og forretningsmodeller (It-security as a service)[33].

Efterspørgslen efter efteruddannelse og certificeringer kan stige. Markedet for videregående voksen- og efteruddannelse (VEU) inden for informationssikkerhed er ikke veludviklet. Det ses både i den begrænsede brug af certificeringer, som er udbudt af private aktører, og i brugen af formel VEU. En begrænset efterspørgsel hæmmer udbydernes incitamenter til at gå i dialog med organisationer om behovet og opkvalificeringsveje. De analyser, der blev gennemført af Ekspertgruppen for voksen-, efter- og videreuddannelse, peger på, at der er en sammenhæng mellem ledelsens prioriteringer af VEU og virksomhedens faktiske VEU-adfærd, herunder også medarbejdermotivation til at deltage i efteruddannelse[34]. Derfor er der et potentiale for, at efterspørgslen herefter kan stige i lyset af de mange tiltag på området, som er sat i gang, samt stigningen i organisationernes generelle efterspørgsel efter kompetencer inden for informationssikkerhed.

Uindfriet potentiale for efterspørgslen. Udgangspunktet i Danmark er, at myndigheder og virksomheder er meget digitaliserede, men at der kan være et uindfriet potentiale. Det vil vi uddybe nærmere, da det ifølge denne rapport er et centralt forhold for fremtidens behov. Tidligere undersøgelser viser, at den danske offentlige sektor er den mest digitale i verden[35]. Danske virksomheder er også blandt de mest digitaliserede i EU, og det er gældende for alle brancher på nær bygge og anlæg, jf. figur 6.8. Det betyder, fx at danske virksomheder i meget høj grad anvender de gængse digitale teknologier, hvilket andre undersøgelser også peger på[36]. Den mere avancerede brug af teknologier – især i form af såkaldt Internet of Things (IoT) og mobile teknologier – øger kravene til virksomhedernes informationssikkerhed[37].

Figur 6.8 Danske virksomheder er blandt de mest digitale i EU

Andelen af virksomheder med høj/meget høj digitaliseringsgrad



Kilde: Redegørelse for Danmarks Digitale Vækst, 2018

Anm.: Operationel service omfatter servicevirksomheder som fx rejsebureauer, vagttjenester, rengøring mv. Inddelingen i erhverv følger Dansk Branchekode DB07 standardgruppe 10. Brancheinddelingen adskiller sig fra andre figurer i denne rapport, da opgørelsen stammer fra Erhvervsministeriet.

[33] Cyber security Workforce study (2018). Cyber security professionals focus on developing new skills as workforce gap widens
[34] Epinon (2017). Analyse af individer og virksomheders brug af voksen- og efteruddannelse
[35] FN's benchmarking af offentlig digitalisering, FN E-Government Index 2018, og EU's DESI Digital Public Services Index 2018
[36] Danmarks Statistik: IT-anvendelse i virksomheder, 2018
[37] Center for Cybersikkerhed: Sikkerhedstruslen i Danmark (2019)

Vi finder dog tegn på, at der er et potentiale for, at den udbredte digitalisering bliver fulgt op af tilsvarende dybdegående informationssikkerhed hos organisationerne. Vi ved allerede fra tidligere undersøgelser, at Danmark halter efter Norge og Sverige, når man måler *Cybersecurity awareness*[38], ligesom vi ved fra Deloittes undersøgelse af IT-sikkerhed i SMV'er fra 2018, at 39 pct. af danske SMV'er har et ikke-tilstrækkeligt IT-sikkerhedsniveau[39].

Det er ikke ligetil at måle potentialet direkte. Men ser man på, hvad der skal være til stede, for at en organisation har et veludviklet niveau for informationssikkerhed, så bekræftes billedet. Man kan således opdele informationssikkerhed i tre elementer, som skal være til stede, for at en organisation er 'veludviklet'. Opdelingen er inspireret af en international kategorisering af organisationers informationssikkerhed[40]. Elementerne er:

1. **Mennesker**, hvor man ser på, i hvilket omfang medarbejdere med ITS-kompetencer er tæt knyttet til ledelsen i organisationen.
2. **Processer**, hvor man ser på, i hvilket omfang der er veldokumenterede og strukturerede processer for informationssikkerhed i organisationen.
3. **Teknologi**, hvor man ser på, hvor dybt sikkerheden er implementeret i organisationens teknologi og enheder (devices).

Ad 1, så ved vi fra en tidligere undersøgelse, at der er en sammenhæng mellem en virksomheds sårbarhed relateret til informationssikkerhed og ledelsens stillingtagen hertil[41]. Undersøgelsen viser, at i næsten hver femte SMV har ledelsen i ringe grad eller slet ikke taget stilling til informationssikkerhed.

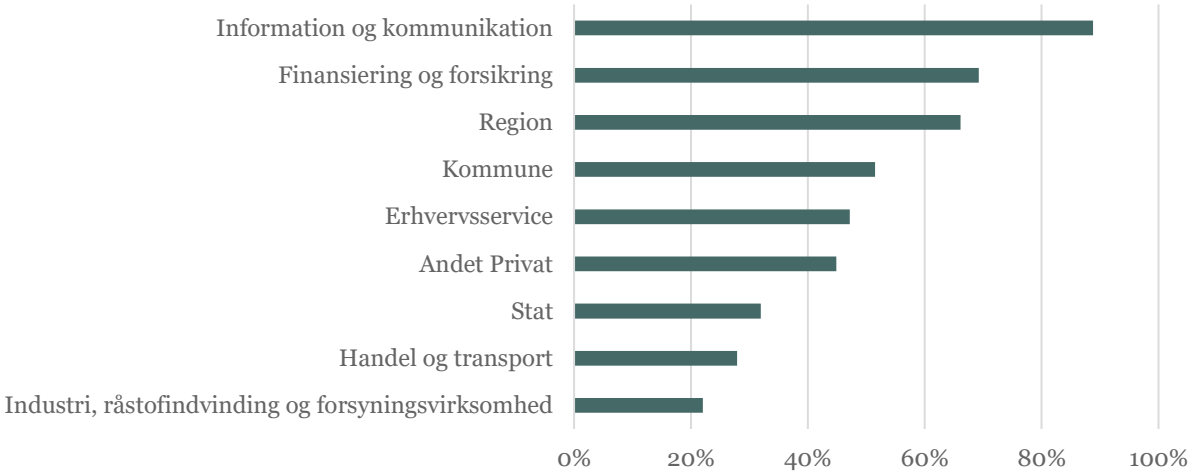
Ad 2, så ved vi også, at SMV'erne i ringe grad har tilrettelagt processer, som sikrer basal informationssikkerhed. Fx har 62 pct. af SMV'erne ikke en dokumenteret politik herom, og 39 pct. har ikke implementeret en fast procedure for håndtering af personfølsomme data. Begge dele må siges at være basal informationssikkerhed.

Ad 3, så har vi i vores undersøgelse set på teknologielementet, idet vi har spurgt organisationerne, i hvilket omfang de tænker informationssikkerhed ind i deres produkter eller ydelser. Det kan være en indikation på, hvor dybt informationssikkerhed er implementeret i organisationen. Her viser vores resultater, at der på tværs af brancher er forskel på, i hvilket omfang dette er tilfældet. Således svarer fx 22 pct. af de adspurgte virksomheder i branchen *Industri, råstofindvinding og forsyningsvirksomhed*, at de i meget høj grad eller høj grad tænker informationssikkerhed ind i deres produkter eller ydelser, jf. figur 6.9. Det er en branche, som bl.a. tæller kritisk infrastruktur. Ligeledes viser svarene fra virksomheder i *Handel og transport*, at 28 pct. af de adspurgte tænker IT-sikkerhed ind i deres ydelser. Det er en branche, der bl.a. tæller e-handelsvirksomheder.

[38] Deloitte: The future market for cybersecurity in Denmark 2018
[39] Deloitte: IT-sikkerhed og datahåndtering i danske SMV'er (2018)
[40] Enterprise Strategy Group Maturity Model (2014). Opdelingen har fire elementer, de tre, som er nævnt i brødteksten, og den fjerde er 'cybersecurity philosophy', som vi i denne undersøgelse har valgt at se bort fra, da den er vanskelig at måle konkret.
[41] Deloitte: IT-sikkerhed og datahåndtering i danske SMV'er (2018)

Figur 6.9 Store forskelle på, om organisationer tænker informationssikkerhed ind i deres produkter eller ydelser

Andel, der svarer, at de "I meget høj grad" eller "høj grad" tænker IT-sikkerhed ind i deres produkter/ydelser



Kilde: Spørgeskemaundersøgelse, N=202

Svarene viser også, at de to brancher, *Information og kommunikation* samt *Finansiering og forsikring*, er der, hvor den største andel af de adspurgte virksomheder tænker informationssikkerhed ind i deres produkter og ydelser. Brancherne er i øvrigt – som nævnt ovenfor i afsnit 2 – der, hvor efterspørgslen efter kompetencer inden for informationssikkerhed er steget mest de senere år.

Samlet set vurderer vi, at der på baggrund af de tre elementer af informationssikkerhed, (1) mennesker, (2) processer og (3) teknologi, er indikationer på, at nogle organisationer har et uindfriet potentiale for at øge deres informationssikkerhed. Indløses dette potentiale, vil det alt andet lige øge behovet. Andre undersøgelser[42] peger som nævnt også herpå.

[42] Deloitte: IT-sikkerhed og datahåndtering i danske SMV'er (2018); Deloitte: The future market for cybersecurity in Denmark (2018)

7. Opkvalificering og efteruddannelse

Afsnittets hovedresultater

- Få virksomheder og myndigheder bruger det etablerede voksen- og efteruddannelsessystem, når det gælder informationssikkerhed.
- Virksomheder og myndigheder bruger i stedet oplæring – typisk vha. sidemandsoplæring kombineret med konferencer, certificeringer eller e-learning.
- Et særtegn inden for informationssikkerhed er, at konferencer er en vigtig kilde til opkvalificering af de ansatte.

En vigtig forudsætning for, at danske virksomheder og myndigheder får dækket sine behov for kompetencer inden for informationssikkerhed er, at medarbejdere løbende opkvalificeres og efteruddannes. Det er en forudsætning, der er gældende for arbejdsmarkedet generelt, men i særlig grad vigtig inden for informationssikkerhed, da udviklingen her sker dynamisk og hastigt. Derfor er det relevant se på, i hvilket omfang og hvordan virksomheder og myndigheder benytter opkvalificering og efteruddannelse til at dække behovet for kompetencer. Det vil vi undersøge i det følgende kapitel.

7.1 Brug af voksen- og efteruddannelsessystemet

Vi har i denne undersøgelse spurgt et repræsentativt udsnit af virksomheder og offentlige myndigheder, hvad de bruger af opkvalificering og efteruddannelse for at dække deres behov for IT-sikkerhedskompetencer. Vi har både set på formel og uformel efteruddannelse og opkvalificering. Formel efteruddannelse og opkvalificering fører til en offentligt godkendt eksamen eller en kvalifikation, mens uformel efteruddannelse eller opkvalificering oftest ikke giver en offentlig godkendt kvalifikation. Formel efteruddannelse vil typisk foregå i det offentlige voksen- og efteruddannelsessystem (VEU-system), mens uformel efteruddannelse kan være certificeringer, kurser, seminarer, sidemandsoplæring mv.

FÅ VIRKSOMHEDER OG MYNDIGHEDER BRUGER DET ETABLEREDE VOKSEN- OG EFTERUDDANNELSESSYSTEM

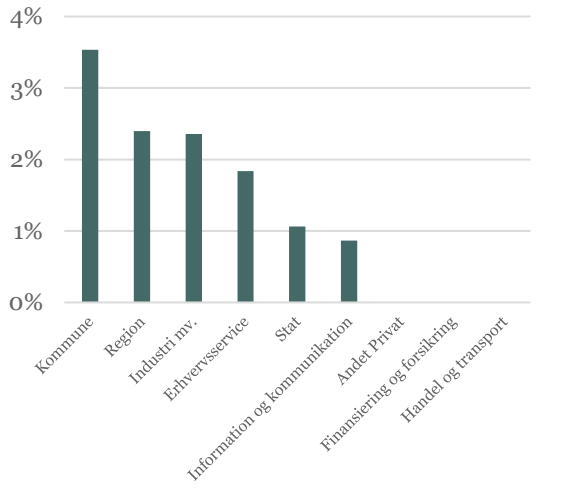
En hovedkonklusion i dette kapitel er, at virksomheder og myndigheder ikke bruger det etablerede voksen- og efteruddannelsessystem til opkvalificering og efteruddannelse, når det gælder informationssikkerhed. Under 4 pct. af de adspurgte virksomheder og myndigheder sender medarbejdere på offentlige efteruddannelseskurser, jf. figur 7.1, og under 6 pct. sender de ansatte på privat udbudte kurser, jf. figur 7.2. Resultatet gælder uagtet branche.

En forklaring kan være, at der er et lille udbud af formelle VEU-kurser om informationssikkerhed[43]. Men det kan også skyldes, at de formelle VEU-kurser ikke i tilstrækkelig grad møder organisationernes behov. Vores kvalitative interview bekræfter dette billede. Her peger informanterne samlet på, at de ikke i særlig grad benytter det formelle system. De bruger i stedet sidemandsoplæring og/eller mere eller mindre formaliseret, interne kurser for at opkvalificere deres medarbejdere. En virksomhed inden for informationssikkerhed har

[43] Højbjerre Brauer Schultz og Teknologisk Institut: Sammenhængen mellem eksisterende videregående voksen-, efter- og videreuddannelse (VVEU) og arbejdsmarkedets kompetenceefterspørgsel (kommende)

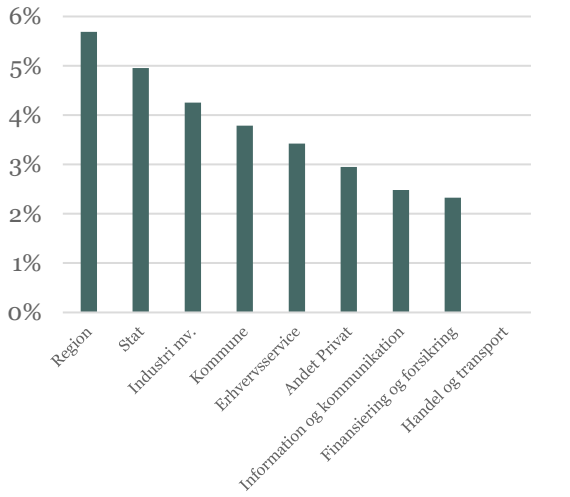
ligefrem oprettet et akademi for at efteruddanne egne og potentielle medarbejdere i de kompetencer, som de har behov for. Informanterne forklarer, at deres prioritering skyldes, at udviklingen inden for informationssikkerhed sker så hastigt og dynamisk, at de har vanskeligt ved at finde formel efteruddannelse, som ikke er forældet. Andre analyser har peget på, at det er et vilkår for IT-branchen[44].

Figur 7.1 Meget få sender medarbejdere på offentlige efteruddannelseskurser…



Kilde: Spørgeskemaundersøgelse, n=817 (virksomheder med ISK til stede)

Figur 7.2 … billedet er det samme for privat udbudte kurser.



Kilde: Spørgeskemaundersøgelse, n=817 (virksomheder med ISK til stede)

Der er – så vidt vides – ikke tidligere lavet undersøgelser i Danmark af, i hvilket omfang virksomheder og myndigheder sender medarbejdere på efteruddannelse i VEU-systemet for at dække virksomhedens behov for kompetencer vedr. informationssikkerhed. Dog har Ekspertgruppen for voksen-, efter- og videreuddannelse, som blev nedsat af den daværende regering i 2016, undersøgt virksomhedernes brug af VEU-systemet generelt. Her flugter billedet med ovenstående hovedkonklusion: at virksomhederne i højere grad benytter uformel efteruddannelse i form af fx sidemandsoplæring fremfor kurser i det etablerede VEU-systemet[45]. Undersøgelsen kan ikke sammenlignes 1:1 med nærværende, men den understøtter det samlede billede.

Ser man på forskelle på tværs af brancher, fremgår det, at offentlige myndigheder i højere grad benytter VEU-systemet end den private sektor. Således er det kommunerne og regionerne, hvor flest anvender offentlige efteruddannelseskurser. For private udbudte kurser er det regioner og stat, hvor flest anvender denne type efteruddannelse, jf. Figur 7.1 og Figur 7.2.

7.2 Brug af uformel efteruddannelse

Vores undersøgelser viser samlet set, at organisationerne i stedet bruger oplæring af medarbejdere, når de skal efteruddanne eller opkvalificere deres medarbejdere med kompetencer inden for informationssikkerhed. For at opnå en præcis forståelse af oplæring, dykker vi ned i oplæring, hvor vi i denne undersøgelse skelner mellem *intern* og *ekstern* oplæring. Intern oplæring er fx sidemandsoplæring og introkurser, der foregår på arbejdspladsen, mens ekstern oplæring som fx certificeringer (se nedenstående faktaboks) finder sted væk fra arbejdspladsen. Som vi beskrev i begyndelsen af kapitlet, så er oplæring – uagtet om det er intern eller ekstern oplæring – uformel efteruddannelse og står dermed i modsætning til formel efteruddannelse, hvor man får et bevis.

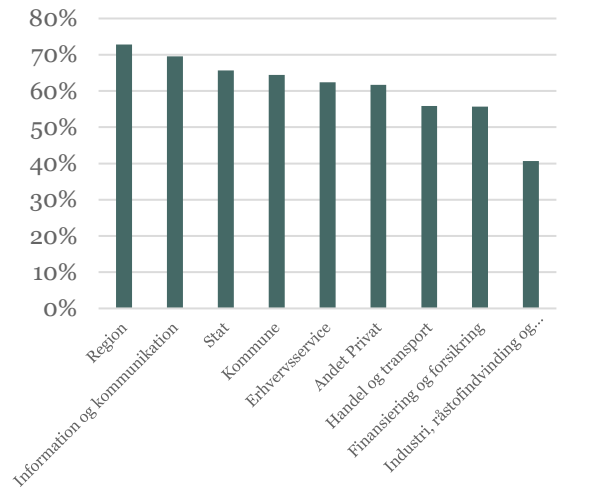
[44] Se fx Højbjerre Brauer Schultz, Kubix og Alexandra Instituttet: Virksomheders behov for digitale kompetencer (2016).
[45] Epinion for Ekspertgruppen for voksen-, efter- og videreuddannelse: Analyse af individers og virksomheders brug af Voksen- og efteruddannelse (2017).

UFORMEL EFTERUDDANNELSE ANVENDES LANGT MERE END FORMEL EFTERUDDANNELSE

Vores undersøgelse viser, at virksomheder og myndigheder i langt højere grad anvender såvel intern som ekstern oplæring end VEU-systemet. Minimum 40 pct., jf. figur 7.3, anvender således intern oplæring, mens minimum 30 pct. anvender ekstern oplæring, jf. figur 7.4. Til sammenligning anvender maksimalt 4-6 pct. af virksomheder og organisationer det etablerede VEU-system, jf. forrige afsnit.

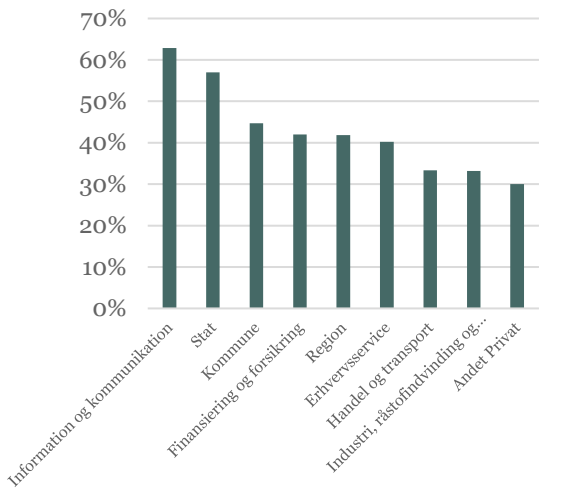
Der er desuden en tendens til, at intern oplæring bliver brugt relativt mere end ekstern oplæring. Således gælder for stort set alle brancher, at en større andel af virksomheder i en given branche anvender intern oplæring sammenlignet med ekstern oplæring. Fx anvender 73 pct. i regionerne intern oplæring, mens 42 pct. anvender ekstern oplæring.

Figur 7.3 Intern oplæring foregår i vid udstrækning i alle brancher…



Kilde: Spørgeskemaundersøgelse, n=817 (virksomheder med ISK til stede)

Figur 7.4 … billedet er stort set det samme for ekstern oplæring.



Kilde: Spørgeskemaundersøgelse, n=817 (virksomheder med ISK til stede)

Ser man på de branchemæssige forskelle, så anvendes intern oplæring relativt mest i regioner, i IKT-branchen samt i staten og kommunerne. Ekstern oplæring anvendes mest i IKT-branchen, staten, kommuner samt i branchen Finansiering og forsikring. Industrien adskiller sig ved at være den branche, hvor færrest svarer, at de bruger oplæring. Billedet er meget klart på tværs af anvendelsen af intern (41 pct.) og ekstern (33 pct.) oplæring. Samtidigt viser resultaterne om benyttelse af VEU-systemet, at industrien – der også tæller virksomheder inden for kritisk infrastruktur såsom råstofudvinding – at, virksomheder her kun i mindre omfang benytter VEU-systemet.

INTERN OPLÆRING: SIDEMANDSOPLÆRING FYLDER MEST

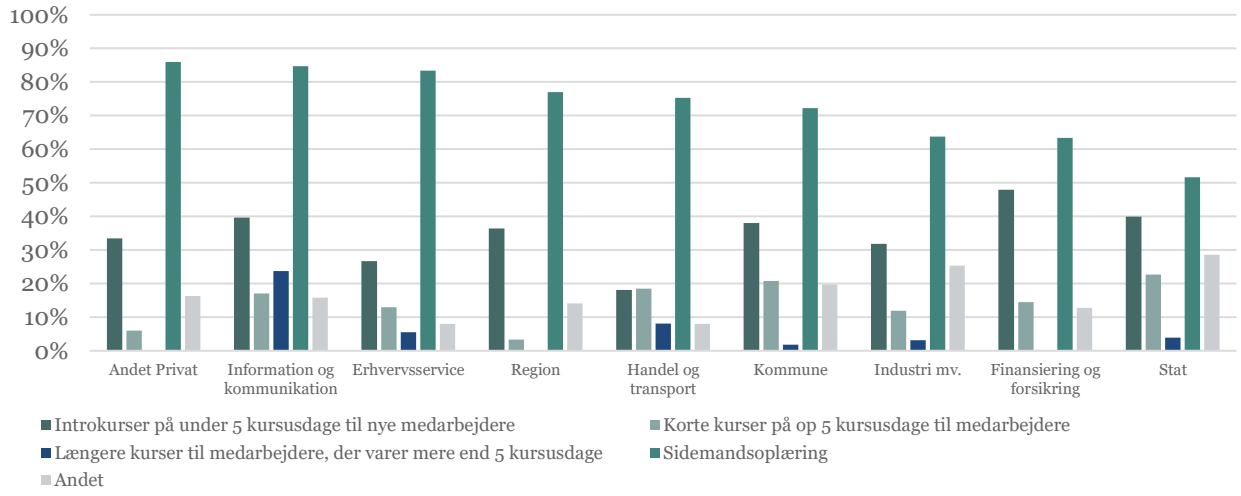
Ser vi nærmere på, hvilken form for *intern* oplæring virksomheder og myndigheder benytter sig af, så viser vores undersøgelse meget tydeligt, at sidemandsoplæring er den mest benyttede form på tværs af brancher, jf.
Figur. Sidemandsoplæring står i vist omfang alene, når organisationerne skal oplære 'in house' – i IKT-organisationer og staten er det mere formaliseret. Det tyder på, at virksomhederne ikke har formaliseret en intern opkvalificeringsproces i form af faste interne kurser. Således svarer virksomheder og myndigheder fra de fleste brancher, at de benytter sig af sidemandsoplæring som et led i at dække deres behov for kompetencer vedr. informationssikkerhed, jf.
Figur.

Det fremgår også, at det er organisationer i branchen *Information og kommunikation*, der i videst omfang oplærer medarbejderne. Således fylder ikke bare sidemandsoplæring meget i denne branche (85 pct.), men

også længere kurser med en varighed på over 5 kursusdage (24 pct.). Faktisk er det den branche, hvor længere kurser fylder klart mest.

Men resultaterne viser også, at i staten fylder kortere introkurser, der typisk dækker over e-learning-kurser eller interne awareness-kampagner om informationssikkerhed, relativt mest. Det kan tyde på, at der i staten er en ret formaliseret struktur for oplæring, fx i form af e-learning-kurser på den statslige læringsløsning Campus.

Figur 7.5 Intern oplæring: sidemandsoplæring fylder mest



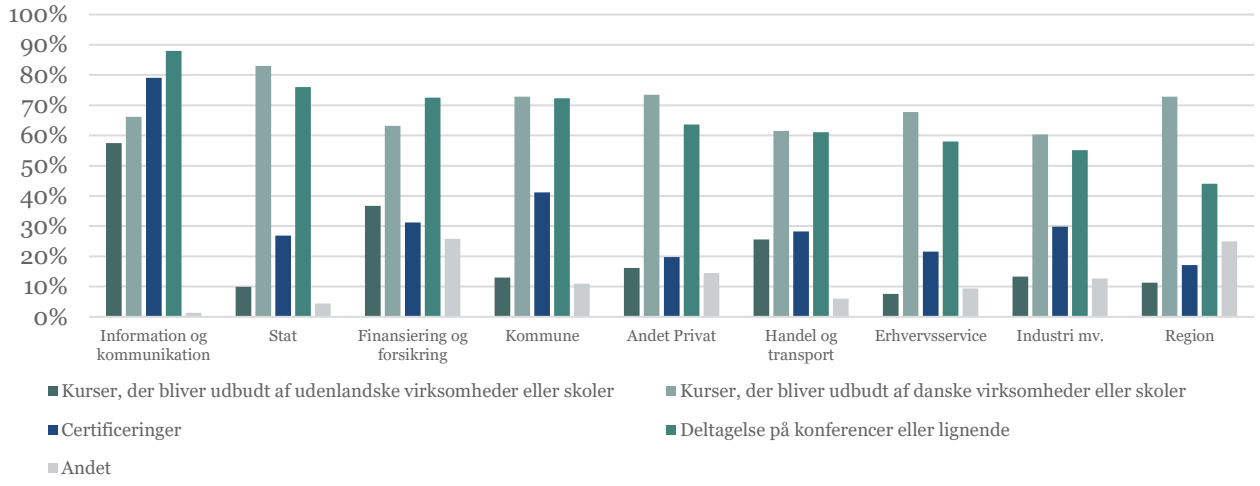
Kilde: Spørgeskemaundersøgelse, n=488 (virksomheder med ISK-kompetencer til stede, som har anvendt intern oplæring)

EKSTERN OPLÆRING: DANSKE KURSER OG KONFERENCER ER MEST UDBREDT

Denne undersøgelse viser, at ekstern oplæring er en vigtig kilde for organisationerne til at efteruddanne eller opkvalificere sine medarbejdere inden for informationssikkerhed – om end intern oplæring blev brugt relativt mere (jf. Figur 7.3 og Figur 7.4). Men det er alligevel interessant for forståelse af, hvordan organisationerne håndterer det konstante behov for efteruddannelse at se på, hvad der karakteriserer den *eksterne* oplæring. Ekstern oplæring er kurser eller lignende, som tages væk fra arbejdspladsen, men som ikke giver formelle kvalifikationer.

Dykker vi ned i brugen af ekstern oplæring, så ser billedet overordnet anderledes, end når vi sammenligner med brugen af intern oplæring. Således fremgår det af svarene fra organisationerne på tværs af brancher, at arbejdspladserne bruger en bredere pallette af forskellige former for ekstern oplæring, jf. figur 8.6. Det vil sige, at svarene ikke viser det samme entydige mønster, som vi så ved intern oplæring, hvor én form for oplæring – sidemandsoplæring – var den mest anvendte form. Det viser, hvordan oplæringen af kompetencer vedr. informationssikkerhed kræver mange forskellige typer af oplæring, og at organisationerne ikke bruger én måde at imødekomme dette behov på.

Figur 7.6 Danske kurser og konferencer er mest udbredt – certificeringer fylder en del



Kilde: Spørgeskemaundersøgelse, n=334 (virksomheder med ISK-kompetencer til stede, som har anvendt ekstern oplæring)

Ser vi på forskellene imellem brancher, så er det tydeligt, at det er de adspurgte organisationer fra branchen *Information og kommunikation*, der flittigst anvender alle former for ekstern oplæring. Det understøtter de tidligere resultater om behovet for rekruttering, hvor det i denne branche var dér, hvor behovet er størst. Der er med andre ord flere resultater, der indikerer, at behovet for informationssikkerhedskompetencer er størst i *Information og kommunikation*. Det er måske ikke overraskende givet branchens profil.

Men når vi ser på resultaterne for brugen af de enkelte former, så er der nogle forskelle. Svarene fra organisationerne viser således, at kurser, der udbydes af danske virksomheder eller skoler er dominerende: fra 63 pct. i Finansiering og forsikring til 83 pct. i Staten. Det er måske en smule overraskende, at det er danske kurser, der fylder mest. Man kunne fx forvente, at udenlandske kurser ville fylde mere, idet informationssikkerhed og de dertilhørende programmer, hardware og litteratur i høj grad er udenlandsk og særligt amerikansk domæne. Omvendt er det mindre omkostningstungt for organisationerne at sende medarbejdere på efteruddannelse i Danmark.

KONFERENCER ER EN VIGTIG KILDE TIL OPLÆRING

En anden interessant pointe er, at deltagelse på konference eller lignende anvendes flittigt – fra 44 pct. i Regioner og 88 pct. i *Information og kommunikation*. Det tyder altså på, at konferencer er en vigtig kilde til at oplære medarbejdere på tværs af brancher. Fx viser en optælling fra Cybersecurity Conference Directory (CCD), som er et netværk bestående danske og udenlandske virksomheder, der har specialiseret sig i informationssikkerhed, at der i 2019 er 12 konferencer i Danmark, som alene omhandler *Cyber Security*[46]. Bemærk, at CCD's definition af cybersikkerhed ikke nødvendigvis følger denne rapports ditto. Derfor kan en optællingen efter denne rapports definition af cybersikkerhed vise et andet resultat. Så vidt vi ved har tidligere undersøgelser ikke haft fokus på, at konferencer udgør en så markant kilde til oplæring af medarbejdere om informationssikkerhed. De kvalitative interview med virksomheder, der har specialiseret sig i informationssikkerhed, bekræfter, at en stor del af oplæringen sker via konferencer eller såkaldte hackathons.

En anden måde at oplære medarbejdere på er såkaldte certificeringer (se nedenstående faktaboks). Vores undersøgelse dokumenterer, at det er udbredt både at efteruddanne og opkvalificere medarbejderes kompetencer inden for informationssikkerhed, jf. Figur . Vores undersøgelse giver ikke et entydigt billede af, hvilke certificeringer de adspurgte virksomheder og myndigheder tager. Der er altså ikke noget mønster heri. Men det fremgår af vores undersøgelse, at certificeringer bliver anvendt i alle brancher. Informanterne fra de kvalitative interview fremhæver, at det er en vigtig kilde til efteruddannelse inden for informationssikkerhed, og

[46] https://infosec-conferences.com/country/denmark/, optalt den 4. september 2019.

det er noget, som medarbejderne stærkt efterspørger. Det skyldes, at informationssikkerhed i udpræget grad er et internationalt/amerikansk domæne, og da viden på området udvikler sig hurtigt og er på engelsk, så er det certificeringer, som medarbejderne efterspørger.

Det er ikke overraskende, at det er for *Information og kommunikation*, at certificeringer fylder mest – knapt 8 ud 10 af de adspurgte virksomheder svarer, at certificeringer er en kilde til efteruddannelse.
Ser vi på forskellene i den offentlige sektor, så er certificeringer mest anvendt i kommunerne (41 pct.), mens det er mindst anvendt i regionerne (17 pct.).

Hvad er certificeringer?
Inden for IT-sikkerhedsområdet er det meget udbredt, at medarbejdere tager en såkaldt certificering i IT-sikkerhed eller informationssikkerhed.

En certificering er et slags kursus, der, når det er gennemført, bekræfter bestemte kompetencer, som en person eller organisation har tilegnet sig. I de fleste tilfælde leveres denne bekræftelse i form af en ekstern gennemgang, vurdering eller revision. Kan udbydes både af private og offentlige organisationer. Typisk kan man opdele certificeringer i leverandørspecifikke såsom Cisco eller leverandøruafhængige som CompTIA.

I USA, som driver markedet for certificeringer, er de mest populære certificeringer (målt på person, som har certificeringen):
1. CompTIA Security+
2. Certified Information Systems Security Professional (CISSP)
3. Global Information Assurance Certification (GIAC)
4. Certified Information System Auditor (CISA)
5. Certified Information Security Manager (CISM)
6. Certified Information Privacy Professional (CIPP)

Kilde: CyberSeek, National Initiative for Cybersecurity Education (NICE), et program under the National Institute of Standards and Technology in the U.S. Department of Commerce

8. Metode

8.1 Efterspørgsel og Jobopslagsanalyse

Efterspørgslen efter informationssikkerhedskompetencer er identificeret ved at gennemgå 2,4 mio. jobopslag fra perioden 2008-2018. Hvert jobopslag er gennemlæst ved brug af tekstanalyse.

Konkret har vi søgt efter godt 350 ord, der relaterer sig til informationssikkerhed. Hvis jobopslaget indeholder et af disse ord, klassificeres jobopslaget som et jobopslag, hvor der efterspørges informationssikkerhedskompetencer. Alle ord er kvalitetstjekket ved manuelt at tjekke de jobopslag, hvor ordet indgår. Fx nævnes det i slutningen af flere jobopslag, at persondata vil blive behandlet fortroligt i overensstemmelse med GDPR. For ikke at klassificere en lang række forkerte jobopslag som værende informationssikkerheds-jobopslag har vi valgt, at ordet "GDPR" skal indgå, samtidig med at et ord relateret til sikkerhed indgår i jobopslaget. Tilsvarende er gældende for andre informationssikkerhedsord, der kan indgå i andre sammenhænge end informationssikkerhed.

Udover listen med ord relateret til IT-sikkerhed er nogle jobopslag klassificeret som et informationssikkerheds-jobopslag ud fra den jobtitel, som anvendes i jobopslaget. Hvis en arbejdsplads fx søger efter en cybersecurity-specialist, klassificeres jobopslaget som et informationssikkerheds-jobopslag.

KOMPETENCEKATEGORIER

Efter identificeringen af jobopslag, hvor der efterspørges kompetencer inden for informationssikkerhed, er alle jobopslag kategoriseret i en eller flere af de syv kompetencekategorier. Kategoriseringen er foretaget ud fra, hvilke informationssikkerheds-ord jobopslaget indeholder. Hvert informationssikkerheds-ord er med hjælp fra Christian Damsgaard Jensen (lektor ved Institut for Matematik og Computer Science på DTU) kategoriseret i en eller flere af de syv kompetencekategorier. Således kan et jobopslag kategoriseres i mere end en kompetencekategori, fordi (1) et informationssikkerheds-ord tilhører mere end en kompetencekategori, eller (2) jobopslaget indeholder flere informationssikkerheds-ord, som tilhører forskellige kompetencekategorier.

FORDELE OG ULEMPER VED AT ANVENDE JOBOPSLAGSDATA

Jobopslagsdatabasen er en unik database, der tillader en lang række analyser af efterspørgslen efter arbejdskraft på det danske arbejdsmarked, som ikke tidligere har været mulige. Ved brug af tekstanalyse kan vi målrettet undersøge, hvilke specifikke kompetencer arbejdsgiverne efterspørger. Dermed kan jobopslagsdatabasen ikke kun bruges til at undersøge efterspørgslen efter informationssikkerhedskompetencer, men også til at undersøge, hvilke specifikke kompetencer arbejdsgiverne efterspørger, fx om de har behov for en jurist til at håndterer GDPR-relaterede arbejdsopgaver eller en teknisk dygtig IT-specialist til at sikre virksomheden mod eksterne hackerangreb.

Brugen af jobopslag til at analysere efterspørgslen efter informationssikkerhedskompetencer har også sine begrænsninger. Først og fremmest kan vi kun måle den formelle efterspørgsel efter informationssikkerhedskompetence. Nogle brancher er mere tilbøjelige til at offentliggøre jobåbninger end andre, fx skal stat, region og kommuner som udgangspunkt slå stillinger op offentligt. Dette tager vi højde for ved at måle efterspørgslen efter informationssikkerhedskompetencer relativt til den samlede efterspørgsel efter arbejdskraft i en given branche. En sidste begrænsning ved analysen er, at den er begrænset til de specifikke kompetencer, der nævnes i jobopslag. Vi kan altså kun identificere en efterspørgsel efter informationssikkerhedskompetencer, hvis det eksplicit er nævnt i jobopslaget.

8.2 Samfundskritiske sektorer

De samfundskritiske sektorer er afgrænset ud fra Dansk Branchekode (DB07) og kan bestå af både myndigheder og virksomheder. Den specifikke afgrænsning ved brug af DB07-koder fremgår nedenfor:

- **Finanssektoren**: 641100-663300
- **Telesektoren**: 611000-619000
- **Transportsektoren**: 491000-495000 og 511010-532000
- **Energisektoren**: 351100-351400
- **Søfart**: 501000-504000
- **Sundhedssektoren**: 861000-869090

8.3 Analyse af udbud

Udbuddet af informationssikkerhedskompetencer er analyseret ved at gennemgå kursusbeskrivelser for valgfag og obligatoriske fag for videregående uddannelser, som vi har vurderet værende relevante ift. informationssikkerhed. For erhvervsuddannelser har vi gennemgået den tilhørende bekendtgørelse.

Det er for hvert kursus vurderet, om kursets læringsmål er relateret til informationssikkerhed. Vurderingen er foretaget på baggrund af, om der indgår et ord relateret til informationssikkerhed. Herefter har vi identificeret, hvor mange ECTS-point relateret til informationssikkerhed der tilbydes på hver uddannelse. Vi har valgt udelukkende at fokusere på 'rene' kurser om informationssikkerhed. Således vil et studie, hvor der tilbydes et 15 ECTS-kursus om GDPR tælle med, mens et studie hvor der tilbydes et 15 ECTS-kursus om netværksteknologi, hvor de studerende også lærer om netværkssikkerhed, ikke vil indgå. Årsagen til dette er, at der ikke findes et objektivt mål for, hvor stor en andel af kurset, der omhandler informationssikkerhed, når det kun er et delelement af kurset.

KLASIFICERING AF INFORMATIONSSIKKERHEDSUDDANNELSER

Vi skelner mellem uddannelser med et højt indhold af informationssikkerhed, uddannelser med et delvist indhold af informationssikkerhed og uddannelser med et lille indhold af informationssikkerhed.

Uddannelser med et højt indhold af informationssikkerhed defineres som uddannelser, der tilbyder minimum 30 ECTS-point inden for informationssikkerhed. Grænsen for et højt indhold er lagt ved 30 ECTS-point, fordi det svarer til det minimum antal ECTS-point, en studerende med en kandidatgrad i informationsteknologi med en *computer-security*-specialisering skal have inden for informationssikkerhed.

Uddannelser med et delvist indhold af informationssikkerhed defineres som uddannelser, der tilbyder minimum 15 ECTS-point inden for informationssikkerhed. 15 ECTS-point svarer til ½ semester, og grænsen er valgt, så vi kan skelne mellem uddannelser med et delvist indhold af informationssikkerhed og uddannelser med et lille indhold.

Uddannelser med et lille indhold af informationssikkerhed defineres som uddannelser med mindre end 15 ECTS-point inden for informationssikkerhed.

OPTÆLLING AF INFORMATIONSSIKKERHEDSUDDANNELSER

For erhvervsakademiuddannelser er der en fælles studieordning på tværs af uddannelsesinstitutioner. Derfor indgår erhvervsakademiuddannelsen i datamatik kun en gang i opgørelsen, til trods for at den udbydes på ni forskellige uddannelsesinstitutioner. Omvendt har universiteterne forskellige studieordninger, og derfor kan

en kandidat i datalogi indgå mere end en gang i opgørelsen, såfremt flere universiteter tilbyder kurser vedrørende informationssikkerhed. Dette øger alt andet lige antallet af videregående uddannelser på kandidat- og bachelorniveau relativt til antallet af korte videregående uddannelser i opgørelsen.

Vi har vurderet, at der findes én erhvervsuddannelse, som giver kompetencer inden for informationssikkerhed (data- og kommunikationsuddannelsen). Men det er ikke muligt at kvantificere omfanget af informationssikkerhed ved brug af ECTS for ungdomsuddannelser, og derfor ses der bort fra denne uddannelse, når uddannelserne klassificeres efter, hvor meget informationssikkerhed de indeholder.

FORDELE OG ULEMPER VED AT ANVENDE KURSUSBESKRIVELSER

Kursusbeskrivelserne fungerer som en førstehåndskilde til indholdet på uddannelserne. Det er derfor en effektiv og konsistent metode til at danne sig et overblik over indholdet i uddannelserne. Dog er analysen begrænset til de læringsmål, som er nævnt i kursusbeskrivelserne. Nogle uddannelsesinstitutioner har mere omfattende kursusbeskrivelser end andre, og dette kan påvirke, hvilke uddannelser der klassificeres som informationssikkerhedsuddannelser. Derudover eksisterer der ikke et objektivt mål for, hvor stor en andel af kurset, som er relateret til informationssikkerhed, og derfor inkluderer vi ikke uddannelser, som kun tilbyder kurser, der ikke er fuldt relateret til informationssikkerhed.

8.4 Fremskrivning

Fremskrivningen af det formelle udbud af personer med informationssikkerhedskompetencer er baseret på to datakilder:

(1) Danmarks Statistiks registre KOTRE og RAS
(2) UFM's uddannelsesfremskrivning

Danmarks Statistiks registre er brugt til at kortlægge arbejdsstyrken med en informationssikkerhedsuddannelse i 2017. Det er sket ved at anvende KOTRE til at identificere alle personer, der har gennemført en uddannelse med et obligatorisk indhold af informationssikkerhed. RAS er anvendt til at afgrænse arbejdsstyrken til alle personer i den arbejdsdygtige alder (15-64 år), som var beskæftigede eller arbejdsløse og indgik i befolkningen pr. 1. januar 2017. ISK-arbejdsstyrken er herefter inddelt efter faggruppe (fx IKT) og uddannelseslængde (fx mellemlang videregående uddannelse). Denne inddeling er foretaget ved brug af Danmarks Statistiks uddannelsesklassifikation DISCED-15.

UFM's uddannelsesfremskrivning er en fremskrivning af beskæftigede personer med en given faggruppe og uddannelseslængde (fx IT, MVU). Vi har grupperet uddannelsesfremskrivningen i samme grupper som ISK-arbejdsstyrken, så vi for hver kombination af faggruppe og uddannelseslængde har et tal for beskæftigede i 2017 og en forventet beskæftigelse i 2030.

FREMSKRIVNING

For hver kombination af faggruppe og uddannelseslængde har vi på baggrund af uddannelsesfremskrivningen beregnet en vækstrate for 2017-2030. For at få et tal for ISK-arbejdsstyrken i 2030 har vi multipliceret ISK-arbejdsstyrken i 2017 med vækstraten for den respektive faggruppe og uddannelseslængde. Den forventede ISK-arbejdsstyrke i 2030 er altså beregnet som:

$$IS_{2030} = \sum_{i,j} IS_{2017,i,j} \cdot r_{2017-2030,i,j}$$

Hvor,

- IS_{2030} er den forventede ISK-arbejdsstyrke i 2030
- i er faggruppen (fx IKT)
- j er uddannelseslængden (fx mellemlang videregående uddannelse)

- $IS_{2017,i,j}$ er den faktiske ISK-arbejdsstyrke i 2017
- $r_{2017-2030,i,j}$ er den forventede vækstrate i beskæftigelsen for en given kombination af faggruppe og uddannelseslængde

Antagelser og usikkerheder
UFM's uddannelsesfremskrivning er baseret på flere uddannelser og ikke kun ISK-uddannelser. Derfor er vi nødt til at anvende ISK-arbejdsstyrken i 2017 for at korrigere UFM's uddannelsesfremskrivning. Dermed antager vi implicit, at vækstraten for ISK-uddannelser i en given kombination af faggruppe og uddannelseslængde er den samme som for alle andre uddannelser i den givne kombination af faggruppe og uddannelseslængde. Hvis man forventer at vækstraten for ISK-uddannelsesgruppen vil være større end for de resterende uddannelser, bl.a. som følge af at der er et stigende fokus på informationssikkerhed, så vil vores fremskrivning undervurdere størrelsen af den fremtidige ISK-arbejdsstyrke. Omvendt vil fremskrivningen overvurdere den fremtidige ISK-arbejdsstyrke, hvis informationssikkerhedsuddannelserne viser sig at vokse langsommere end de resterende uddannelser.

Da UFM's uddannelsesfremskrivning er en fremskrivning af beskæftigede, og vi forsøger at fremskrive arbejdsstyrken, ligger der også en implicit antagelse om at arbejdsstyrken vil opleve samme vækstrate som de beskæftigede i en given uddannelsesgruppe.

Der vil altid være usikkerheder forbundet med en fremskrivning. Men fordi der sker meget på området for informationssikkerhed, og der bl.a. er blevet oprettet en helt ny uddannelse i 2017 (uddannelsen i IT-sikkerhed), er det ekstra svært at fremskrive udbuddet af ISK-arbejdskraft.

8.5 Spørgeskemaundersøgelse til organisationer

Vi har udført en spørgeskemaundersøgelse blandt et repræsentativt udsnit af danske virksomheder og myndigheder. Vi har i juli-august 2019 indsamlet i alt 1338 online survey-svar fra danske virksomheder og organisationer. Svarene er indsamlet elektronisk, og virksomheder og myndigheder er inviteret til undersøgelsen via en e-mailinvitation.

STIKPRØVE OG VÆGTNING

For at sikre, at vi har indsamlet svar fra de mest relevante personer, det vil sige personer, som kan udtale sig om informationssikkerhed og kompetencebehov, har vi hovedsageligt indsamlet svar fra ledelsen af organisationen eller IT-chefen/IT-sikkerhedschefen.

Virksomheder og organisationer er valgt ud fra deres baggrundsoplysninger i Det Centrale Virksomhedsregister (CVR), hvor vi har sorteret holdingselskaber og inaktive virksomheder fra, ligesom virksomheden kun optræder under deres hovedaktivitet (primær branche).

Vi har udviklet en stikprøve, der indsamler svar fra et repræsentativt udsnit af danske virksomheder og myndigheder. Vi har dog indsamlet relativt flere svar fra virksomheder, som ifølge Erhvervsstyrelsens oplysninger er deciderede informationssikkerhedsvirksomheder. Det er sket for at få tilstrækkeligt med repræsentation fra denne gruppe.

Svarene er efterfølgende vægtet, så de afspejler fordelingen i populationen, så de er repræsentative på geografisk spredning (region) og branche – både type af brancher (fx industri, statslig arbejdsplads eller kommunal arbejdsplads etc.) og branchernes størrelse, hvilket er målt på antal beskæftigede i branchen fremfor antal organisationer. Det sidste er ikke retvisende, når man indsamler svar fra store offentlige arbejdspladser, såsom sygehuse, idet de udgør én organisation, men fylder meget i branchen i form af mange ansatte. Data for populationen stammer fra registre i Danmarks Statistik.

8.6 Kvalitative interview

Vi har udført dybdegående interview med 10 informanter (se anonymiseret liste nedenfor) fra danske virksomheder, organisationer og en enkelt interesseorganisation. Interviewene er gennemført i to runder fra juni til september 2019. 1. runde af interview var med virksomheder, som har specialiseret sig i ydelser inden for informationssikkerhed og har været af mere eksplorativ/undersøgende karakter. Den anden runde blev gennemført som interview af mere hypotesetestende karakter og er med både virksomheder og myndigheder. Alle interview er udført som såkaldt semistrukturerede interview, det vil sige, at intervieweren følger en på forhånd udformet interviewguide, men at der er rum til at forfølge pointer eller tema, hvis behovet måtte opstå. Informanterne blev rekrutteret bl.a. på anbefaling fra undersøgelsens projektgruppe. Fordeling af informanter:

- 3 informanter fra en informationssikkerhedsvirksomhed
- 1 informant fra en interesseorganisation
- 1 informant fra en region
- 1 informant fra en statslig arbejdsplads
- 1 informant fra den finansielle sektor
- 2 informanter fra en kommune
- 1 informant fra en mellemstor fremstillingsvirksomhed

HØJBJERRE BRAUER SCHULTZ

> Vi har skabt Højbjerre Brauer Schultz for at levere viden, der kan udvikle og fremtidssikre velfærdssamfundet

HØJBJERRE BRAUER SCHULTZ

er et af Nordens førende samfundsøkonomiske konsulenthuse. Vi rådgiver offentlige myndigheder, interesseorganisationer, private virksomheder og internationale organisationer. Ved at bygge bro mellem faglig viden, empiriske resultater og den politiske virkelighed leverer vi anvendelsesorienterede analyser, som er veldokumenterede og klart formidlet.

NY KONGENSGADE 9B, 1. SAL
1472 KØBENHAVN K
WWW.HBSECONOMICS.DK
INFO@HBSECONOMICS.DK