# Cyber- it- og informations-sikkerhed

## Har Danmark de rigtige kompetencer?

2023

Det bedste valg for dig, der arbejder
med naturvidenskab, it eller som ingeniør.

# Forord

## IDA – i fællesskab vil vi vise vejen for teknologi og mennesker

Den aktuelle verdenspolitiske situation kræver, at Danmark har et solidt niveau af digital sikkerhed. Det gælder både offentlige myndigheder og private virksomheder. Forsvarets Efterretningstjeneste har flere gange siden 2021 hævet trusselsvurderingerne for både cyberkriminalitet, cyberaktivisme mod danske myndigheder og virksomheder, og cyberspionage mod især universiteter og forskningsinstitutioner – ikke mindst aktualiseret af krigshandlingerne i Ukraine.

Danmark er i top, når det gælder digitalisering, men ikke helt det samme sted, når det handler om at opfylde krav til sikkerhed. 40 procent af de små og mellemstore virksomheder har et utilstrækkeligt digitalt sikkerhedsniveau, og i den offentlige sektor er kun 54 procent af de samfundskritiske it-systemer sikkerhedsmæssigt tilstrækkelige.[1]

Vi har med andre ord brug for en opgradering. Det får vi kun, hvis vi sikrer, at vi har de rette kompetencer. Det kræver et godt forskningsmiljø, de rette muligheder for uddannelse og efteruddannelse, flere kvinder med interesse for it og et samarbejde mellem universiteter, uddannelsessteder, erhvervsliv og offentlige organisationer.

Digital sikkerhed består af flere elementer. I denne rapport skelner vi mellem it-sikkerhed, informationssikkerhed og cybersikkerhed. De tre områder kræver forskellige typer af opgraderinger i form af uddannelser og efteruddannelser.

Denne rapport har fokus på det offentlige udbud af uddannelser, som er relevante for at dække dette kompetencebehov. Den giver et overblik over de kompetenceprofiler, der er brug for, og hvilken uddannelsesbaggrund, de kan have.

**Denne rapport er udarbejdet af IDAs ekspertudvalg for cybersikkerhed**
Tak til DigitalLead og Digitaliseringsstyrelsen for sparring

***IDAs ekspertudvalg består af:***

Anders Bjerg Frederiksen, it-netværksspecialist, Jens Myrup Pedersen, professor i cybersikkerhed, Julie Kjeldsen, cybersecurity advisor, Shayma Yassen, cybersecurity manager techresilience, Jørn Guldberg, it-sikkerhedsspecialist, Michael Lind Mortensen, security & compliance manager, Ricky Kofoed-Madsen, cybersecurity specialist, Sofie Freja Christensen, security and compliance manager.

***Fra IDA:*** Uddannelsespolitisk chef Lisbet Møller Nielsen og digitaliseringspolitisk chef Grit Munk

# Indhold

# Samlede anbefalinger

## Her finder du et overblik over rapportens anbefalinger:

**1. Overordnet skal der sikres langt flere uddannede indenfor digital sikkerhed:**

### It-uddannelser skal undtages fra loftet over optag i de store byer

It-uddannelser, som arbejdsmarkedet har stor efterspørgsel på, skal undtages fra den politiske begrænsning i optaget, som følger af aftalen om udflytning af uddannelser.

### Øget optag af internationale studerende

Det nuværende loft over optag af internationale studerende skal fjernes, som minimum for de it-uddannelser, som arbejdsmarkedet har stor efterspørgsel på. Derudover skal et øget optag af internationale studerende på relevante professionsbachelor- og erhvervsakademiuddannelser gøres muligt.

### Flere kvinder med interesse for it

På tværs af uddannelser bør der findes tiltag til at styrke interessen blandt kvinder for at søge optagelse på tekniske it-uddannelser. Her kan bl.a. arbejdes med formuleringer og branding samt med udvikling af uddannelser, som kombinerer de teknisk tunge it-uddannelser med fagområder, som har større søgning fra kvinder.

**2. Der er behov for at uddanne flere fra specialiserede cybersikkerhedsuddannelser:**

### Øget optag på uddannelser inden for cybersikkerhed

Kapaciteten på de specialiserede uddannelser inden for cybersikkerhed skal fortsat øges, bl.a. med konsolidering af eksisterende uddannelser og oprettelse af nye.

### Flere ph.d.-stillinger med fokus på cybersikkerhed

Der er mangel på undervisere, hvilket kræver en målrettet opbygning af forskermiljøet. Uden dette vil et øget optag og flere uddannede ikke kunne opnås.

### Forsøg med virksomhedssamarbejde om eksterne undervisere

Der er behov for flere samarbejdsinitiativer med virksomheder, fx ”top-op-løn” fra virksomheden til eksterne lektorer, som kan undervise i cybersikkerhed.

Bedre realkompetencevurdering (RKV) og alternative veje ind for medarbejdere med erfaring.

Det anbefales, at der udvikles et RKV-værktøj til at screene for cybersikkerhedskompetencer, så medarbejdere, der har praktisk erfaring, men ikke formel uddannelse, kan få adgang til videreuddannelse på rette niveau.

Flere valgfag/kurser i it-sikkerhed på it-uddannelser

Studerende på it-uddannelser skal have bedre mulighed for at vælge valgfag/kurser inden for cybersikkerhed.

**3. Der er behov for flere medarbejdere med kompetencer indenfor informationssikkerhed**

Bedre overblik over kurser til efter- og videreuddannelse

Mange virksomheder ved ikke, hvilke kurser der er mest relevante for dem. Derfor er der brug for et brugervenligt overblik, som kan guide virksomheder og medarbejdere.

Kursuskatalog målrettet studerende

Som studerende kan det være vanskeligt at finde de rigtige it-fag. Der bør derfor udvikles et kursuskatalog, der forklarer, hvilke opgaver man vil kunne løse ved at tage de enkelte kurser.

Specialisering på kandidatniveau til tværfaglig kompetence

Der skal være bedre muligheder for at skabe sig en informationssikkerhedsprofil både på samfundsvidenskab og humaniora. Enten på eget eller på andre universiteter.

Ny specialisering i informationssikkerhed på samfundsvidenskab

Der bør skabes mulighed for en egentlig kandidat-specialisering i informationssikkerhed, som kombinerer juridisk/administrativ viden med teknisk indsigt og færdigheder.

**For at sikre tilstrækkelig opmærksomhed på it-sikkerhed i dagligdagen hos it-udviklere og it-driftsmedarbejdere er der brug for:**

**4. Grundlæggende it-sikkerhed skal være obligatorisk på it-uddannelser**

Optaget skal øges på it-uddannelserne.

Som situationen er i dag, må forskellige it-brancher kannibalisere på hinanden, og det er uholdbart. Det kræver først og fremmest lempelse af eller undtagelse fra de politiske fastsatte lofter.

**Definitioner**
I denne rapport arbejder vi med en tredeling af it-opgaverne i henholdsvis cybersikkerhed, informationssikkerhed og it-sikkerhed. Samlet set bidrager de tre områder til digital sikkerhed.

***Cybersikkerhed*** handler om at forebygge, opdage og handle på egentlige digitale angreb mod organisationen. Det er primært den tekniske håndtering og forebyggelse af fx hackerangreb eller DDoS-angreb (overbelastning af server) fra organiserede kriminelle, fremmede stater, terrororganisationer eller aktivister. Medarbejderne i denne gruppe udfører fx udvikling af sikre systemer, kommunikations- og netværkssikkerhed, hændelseshåndtering og efterforskning af hændelser.

***Informationssikkerhed*** er defineret som opgaven med at beskytte systemerne og de data, der er opbevaret i organisationen, mod uautoriseret brug. Det handler fx om at beskytte personlige oplysninger i et kunderegister eller borgeres, medlemmers og medarbejderes personfølsomme data. Det kan være fra sygejournaler, medlemskab af en fagforening eller andre informationer omfattet af GDPR. Ifølge NIST, det amerikanske National Institute of Standards and Technology, er målet at sikre tilgængelighed, integritet og fortrolighed af informationer, både digitalt og på papir. Medarbejdere i denne gruppe arbejder indenfor GRC-feltet (Governance, Risk & Compliance) og udarbejder risikovurderinger, politikker og systemer til at beskytte informationer. Da det kommende NIS2-direktiv, se faktaboks s. 8, medfører en række krav om fx afrapportering og risikoanalyser, er det ekspertgruppens overbevisning, at denne medarbejdergruppe kommer til at spille en afgørende rolle i de kommende år.

***It-sikkerhed*** ses her som en primært teknisk funktion med drift og vedligehold af organisationens it-systemer, både software og hardware. For medarbejdere i denne gruppe er det ofte en grundforudsætning, at organisationen er digitalt velfungerende, og at systemerne ikke forældes eller slides i stykker og går ned. Men i fremtiden bør denne gruppe også i stigende grad være opmærksom på it-sikkerhed ved indkøb af it-systemer, materiel og it-support. En anden gruppe medarbejdere er udviklerne, der bl.a. står for virksomhedens egen programmering, enten i driftssystemerne eller i de produkter, som virksomheden sælger. Også her stiger behovet for et større fokus på it-sikkerhed.

**Kompetencesituationen i overblik**
Området for tekniske kompetencer og it, som cybersikkerhed, informationssikkerhed og it-sikkerhed hører ind under, er generelt præget af kompetencemangel. Ifølge Styrelsen for Arbejdsmarked og Rekruttering var 25 procent af alle forsøg på at rekruttere en it-specialist til en ledig stilling forgæves i 2022, hvilket svarer til knap 12.000 forgæves

rekrutteringsforsøg.[2]
It-Branchens it-barometer fra marts 2023 peger ligeledes på en stor efterspørgsel indenfor it generelt og mere specifikt cybersikkerhed. 71 procent af de adspurgte virksomheder peger på mangel på de rette it-kompetencer og 47 procent har indenfor de seneste 12 måneder haft ledige it-stillinger, som man har måtte opgive at besætte. 51 procent af de adspurgte virksomheder efterspørger kompetencer indenfor sikkerhed og compliance.[3]

Efterspørgslen efter kompetencer på it-sikkerhed er ifølge en rapport udarbejdet for Erhvervsstyrelsen i december 2019, tredoblet på 10 år. Samtidig skønner rapporten, at kun 10 procent af dem, der arbejder i et it-sikkerhedsjob, har en it-relateret uddannelse bag sig. Knap 70 procent af virksomhederne indenfor IKT (informations- og kommunikationsteknologi) anvender intern oplæring.[4] Et initiativkatalog fra Rådet for Digital Sikkerhed påpeger, at hver femte virksomhed har svært ved at finde en medarbejder med alle de rette kompetencer – store virksomheder går på kompromis og oplærer selv til dele af kompetencerne. Og endelig er der efterspørgsel efter kompetencer, som ikke udbydes i uddannelsessystemerne.[5]

Manglen på it-sikkerhedskompetencer er danske SMV'ers største udfordring i forhold til at hæve cybersikkerhedsniveauet. 12 procent af SMV'erne svarede i en analyse for Erhvervsstyrelsen[6] i 2020, at de ikke har den nødvendige viden og kompetencer til at øge deres it-sikkerhed. Samtidig har 17 procent af de adspurgte SMV'er oplevet it-sikkerhedshændelser som for eksempel blokeret adgang til services, sletning, ødelæggelse, misbrug eller videregivelse af data eller it-relateret økonomisk svindel. I alt vurderes 44 procent af SMV'erne i denne analyse til at være sårbare overfor cyberangreb.

Der er samtidig en tydelig sammenhæng mellem ansættelse af højtuddannede indenfor cyber- og informationssikkerhed og niveauet af SMV'ernes it-sikkerhedsforanstaltninger. Samlet set har 18 procent af SMV'erne ansat medarbejdere specialiseret indenfor cyber- og informationssikkerhed, mens det samme gælder hele 90 procent af virksomhederne med over 250 medarbejdere.

**NIS2-direktivet**

I efteråret 2024 træder NIS2-direktivet i kraft, hvilket er endnu en grund til, at efterspørgslen på kompetencer inden for cyber- og informationssikkerhed vil stige. DI vurderer[7], at 1.079 virksomheder på tværs af 12 sektorer vil blive direkte omfattet af NIS2-direktivets stigende krav til it-sikkerhed. Derved adskiller NIS2 sig væsentligt fra det nuværende NIS-direktiv, da langt flere virksomheder vil blive anset for at være en del af den kritiske infrastruktur.

**NIS2 stiller 10 minimumskrav til overholdelse af en række sikkerhedstiltag, som kræver forskellige kompetencer:**

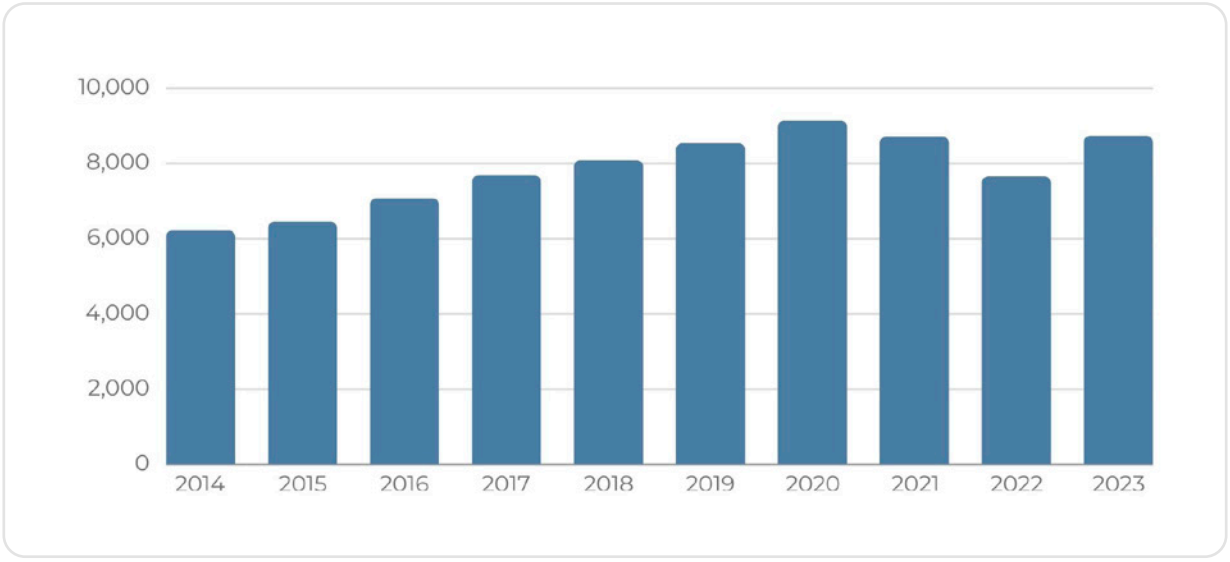
1. Politikker for risikoanalyse og informationssystemsikkerhed
2. Håndtering af hændelser
3. Driftskontinuitet, såsom backup-styring og reetablering efter større sikkerhedsbrud, og krisestyring
4. Forsyningskædesikkerhed, herunder leverandørstyring/-sikkerhed
5. Sikkerhed i forbindelse med indkøb, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder
6. Politikker og procedurer (test og revision) til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici
7. Grundlæggende cyberhygiejnepraksis og cybersikkerhedsuddannelse
8. Politikker og procedurer vedrørende evt. kryptering
9. Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver
10. Brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering mv., "hvor relevant".[8]

En del af disse krav vil virksomhederne formentlig allerede overholde, da flere af tiltagene ikke er nye, men går igen i GDPR. Men vigtigt er, at der indføres sanktioner, der matcher bødeniveauet på brud på GDPR. Det vil sige, at en organisation, der overtræder NIS2, vil kunne få bøder på op til 7-10 millioner Euro[9] eller 2 procent af organisationens årlige, globale omsætning. Derudover kan ledelsen holdes personligt ansvarlig for brud på NIS2.

**Uddannelseslandskabet**

Som det fremgår af gennemgangen ovenfor, er efterspørgslen på cyber- og informationssikkerhedskompetencer – samt på it-specialister mere generelt – allerede stor og må ventes at blive endnu større i de kommende år. En prognose udarbejdet af Iris Group og HBS Economics for IDA og Danske Gymnasier viser, at antallet af it-uddannede langt fra vil følge med efterspørgslen. Således forventes det, at der i 2030 vil være 8.000 flere uddannede på it-området sammenlignet med 2021, men at der alligevel vil mangle 22.000 kvalificerede it-folk, hvoraf de omkring 15.000 vil være it-uddannede med mellemlange og lange videregående uddannelser.[10]

Derfor følger her et kort overblik over, hvordan optaget på de videregående it-uddannelser ser ud og har udviklet sig. De seneste års optag på de videregående it-uddannelser viser en svag stigning i tilgangen, men ikke i et omfang, som matcher arbejdsmarkedets efterspørgsel, jf. nedenstående figur.[11]

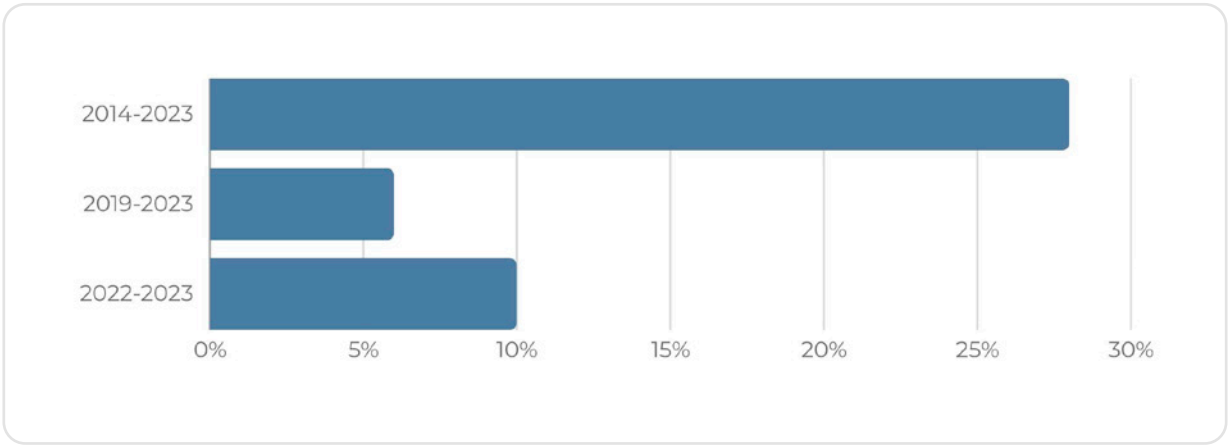



*Kilde: ATV pba. data fra Uddannelses- og Forskningsministeriet (atv.dk)*

Fra 2022 til 2023 er der sket en positiv udvikling, som skal søges fastholdt de kommende år, idet der er optaget 10 procent flere på de videregående it-uddannelser. Bemærk dog, at 2022-optaget også var lavere end i de foregående tre år. Der er også fra 2022 til 2023 sket en stigning i optaget af kvindelige studerende på flere it-uddannelser, fx 12 procent flere kvinder på it-specialistuddannelserne på Aalborg Universitet*[1]*, og på ITU's bacheloruddannelser er 38 procent kvinder.*[2]*

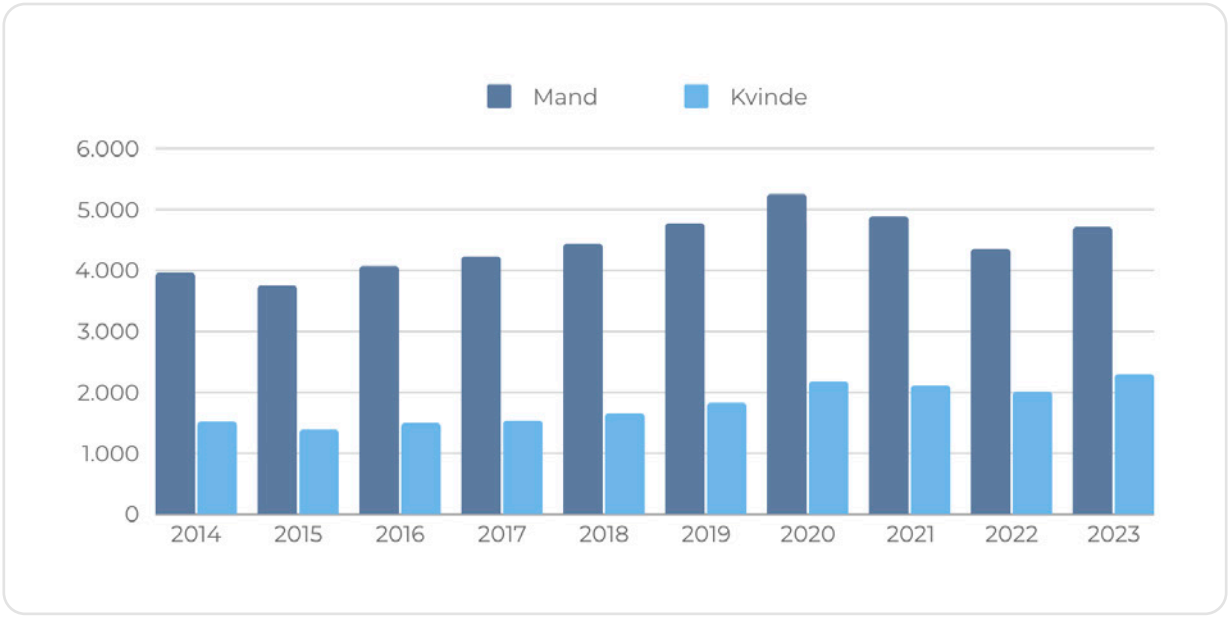
Flere kvindelige studerende på uddannelser og efteruddannelser har betydning både for antallet af medarbejdere med it-kompetencer bredt, men er også afgørende for at undgå blinde vinkler i både udtænkning og implementering af tiltag for at sikre et højere niveau af digital sikkerhed."

**Der er optaget 10 procent flere på it-uddannelserne fra 2022 til 2023**




*Kilde: ATV pba. data fra Uddannelses- og Forskningsministeriet (atv.dk)*

**Antallet af kvinder optaget på it-uddannelser er steget med 282 personer fra 2022 til 2023**




*Kilde: ATV pba. data fra Uddannelses- og Forskningsministeriet (atv.dk)*

Med til billedet hører også, hvordan søgningen til it-uddannelserne har udviklet sig. Altså i hvilken grad de unge er interesserede i at tage de it-uddannelser, som er relevante for at sikre et godt it-sikkerhedsniveau i danske virksomheder og organisationer. Og kigger man over en årrække og ikke kun på de pæne tal for optag i 2023 kan man se, at søgningen til it-uddannelserne samlet set ligger på samme niveau i 2023 som i 2019 (søgningen er 2 procent højere i 2023). Det er langt fra nok til at møde den øgede efterspørgsel på arbejdsmarkedet. Se mere her.

Dermed er der også en del af de it-uddannelser, som er relevante i forhold til informations- og cybersikkerhed, som har ledige pladser i dag.

Universiteterne fastlægger selv, hvordan de fordeler deres pladser på forskellige uddannelser. Men især loftet over optaget i de store byer sætter begrænsning på, hvor mange studerende der samlet set kan optages. I fordelingen af studiepladser arbejder universiteterne aktivt for at flytte pladser fra uddannelser med ledighed til uddannelser, hvor der er stor efterspørgsel på dimittenderne. I den interne prioritering søger man altså at sikre, at alle ansøgere, som opfylder de formelle adgangskrav – eller i hvert fald så mange som muligt – optages på de tekniske it-uddannelser, som arbejdsmarkedet har stor efterspørgsel på. Fx har Aalborg Universitet besluttet, at der skal være 'frit optag' (adgang for alle ansøgere, der opfylder kravene) på bacheloruddannelserne Computerteknologi, Datalogi, Design og anvendelse af kunstig intelligens (diplomingeniør), Elektronik og systemdesign, Software, Elektronik (diplomingeniør) og på kandidatuddannelserne Datalogi, Elektroniske systemer, Robotteknologi og Software. Lignende prioriteringer findes på andre universiteter.

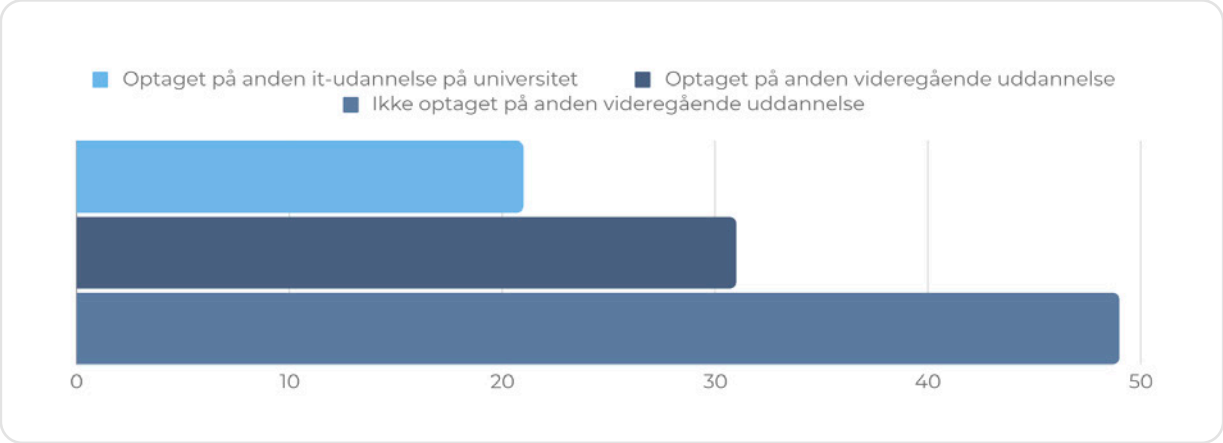
På flere af uddannelserne melder universiteterne, at de ville prioritere uddannelserne yderligere og oprette flere pladser, hvis der var ansøgere nok til det. Det gælder bl.a. Datalogi, Datavidenskab og machinelearning, Cyber- og computerteknologi og Computerteknologi (eksempler fra Aalborg Universitet). Denne mulighed er dog mest oplagt for de store universiteter med flere hovedområder, som har en større kapacitet at prioritere inden for, mens fx IT-Universitetet er begrænset af deres størrelse og p.t. fylder alle deres uddannelser op.

Samtidig ser vi også, at der er uddannelser, som – trods stor efterspørgsel på arbejdsmarkedet – har måttet afvise kvalificerede ansøgere. Det skyldes bl.a., at der politisk er truffet beslutning om at lægge loft over optaget på de videregående uddannelser i de store byer. I aftalen om regionalisering af uddannelser er det politisk besluttet, at universiteterne skal begrænse optaget i de store byer. Det har bl.a. betydet, at DTU i 2023 har reduceret sit optag med 2 procent, selv om de har oplevet en øget søgning.

Når universiteterne må afvise ansøgere til it-uddannelser, er det langt fra givet, at de afviste ansøgere bliver optaget på en anden tilsvarende uddannelse. DI har lavet analyse af optaget i 2022, som viser, at universiteterne samlet set har givet 300 afslag til unge, som havde søgt en it-bacheloruddannelse som deres første prioriteret – og som alle opfyldte de formelle krav[13]. Samtidig viser DI's analyse, at kun hver femte af de afviste blev optaget på en anden it-uddannelse i stedet. Loftet over optaget resulterer altså i et væsentligt tab af unge, som ellers var parate til at tage en af de efterspurgte it-uddannelser.

**Hver femte afviste ansøger til it-uddannelse på universitetet starter på anden it-uddannelse**

Afviste kvalificerede førsteprioritetsansøgere til it-uddannelser




*Kilde: DI baseret på data fra Danmarks Statistik (danskindustri.dk)*

Når vi på it-uddannelserne ikke uddanner nok til at møde arbejdsmarkedets efterspørgsel, er der altså både (for en del uddannelsers vedkommende) tale om mangel på ansøgere og (for en mindre andel af uddannelsernes vedkommende) tale om, at man ikke kan optage alle, som er kvalificerede. Det sidste skyldes især, at der som led i den politiske aftale om udflytning af studiepladser er lagt loft over optaget i de store byer, men manglende finansiering udgør også i nogen grad et problem.

# Roller og kompetencer i digital sikkerhed

**Kompetenceprofiler inden for cybersikkerhed**
Der er både i Danmark og internationalt udarbejdet forskellige forslag til kompetenceprofiler. Opdelingen i denne rapport er udarbejdet af IDAs ekspertgruppe for cybersikkerhed. Vi har opdelt kompetenceprofilerne i tre hovedgrupper: Medarbejdere indenfor cybersikkerhed, medarbejdere indenfor administration og ledelse, der arbejder med informationssikkerhed, samt it-medarbejdere i bred forstand.

Ifølge et etnografisk studie af cybersikkerhed[14] i danske SMV'er, er alle tre grupper i praksis involveret i at styrke it-sikkerhedsniveauet. Studiet er gennemført af Aalborg Universitet, og i de følgende afsnit vil vi referere hovedpointer fra studiet relateret til hver af de tre kompetencegrupper.

**Cybersikkerhed**
Lille gruppe, dyb cyberfaglighed, cybersikkerhed som primære arbejdsfelt

***Roller:*** Ekspert i cybersikkerhed, konsulent, forsker, på forkant ift. morgendagens udfordringer

**Informationssikkerhed**
Ledelse, sagsbehandling eller administration som primær-faglighed, cybersikkerhed som add-on til at varetage opgaver indenfor informationssikkerhed

***Roller:*** Compliance, strategisk sikkerhed, cybersikkerhed som dimension i ledelsesbeslutninger og virksomhedskultur

**It-medarbejdere (udviklere, it-drift m.v.)**
It som drift, vedligehold og udvikling som primære arbejdsområde

***Roller:*** Ofte de udførende på cybersikkerhedsopgaver, analyse og planlægning af indsats

**Cybersikkerhed**
Cybersikkerhedsspecialister og cybersikkerhedsfaglige er den mindste gruppe. Cybersikkerhed er deres primære arbejdsområde. Ansat som rådgivere/konsulenter i cybersikkerhed, som forskere eller i virksomheder/myndigheder, som har væsentligt behov for at beskytte sig mod cyberangreb.

- Teknisk kandidatuddannelse (fx ingeniør) med specialisering inden for cybersikkerhed
- Professionsbachelor i cybersikkerhed
- Forsvarets uddannelser, cyberværnepligt og FE's cyberakademi

**Informationssikkerhed**
Gruppen omfatter ledere, indkøbere, beslutningstagere og administrativt ansvarlige for virksomhedens/myndighedens informationssikkerhed og compliance. Gruppen har ikke nødvendigvis cyber som deres primære arbejdsområde, men skal sikre, at virksomheden både formelt og i praksis agerer cybersikkert.

- Universitetsuddannelser inden for samfundsfag, jura, humaniora med efteruddannelse inden for cybersikkerhed
- Uddannet indenfor administration eller fx bogholderi

**It-sikkerhed**
Gruppen omfatter dem, som er primært beskæftiget med it, dvs. drift, vedligehold og udvikling af funktionsdygtige it-systemer. De har ikke cybersikkerhed som deres primære arbejdsfelt, men vil i praksis ofte være hovedaktørerne i cybersikkerhedsarbejdet, især hvis ikke der i virksomheden findes eksperter i cybersikkerhed.

- It-uddannelse på universitetsniveau
- Professionsbachelor- og erhvervsakademiuddannelser inden for it
- Erhvervsuddannelse som fx it-supporter eller datatekniker
- Autodidakt/oplært i virksomheden med anden uddannelsesbaggrund

# Cybersikkerheds-specialister & cyber-sikkerhedsfaglige

Cybersikkerhedsspecialister og cybersikkerhedsfaglige er den mindste gruppe. Et fælles kendetegn er, at de har cybersikkerhed som deres primære arbejdsområde. De kan være ansat i virksomheder med et væsentligt behov for at beskytte sig mod cyberangreb, de kan være rådgivere eller konsulenter i cybersikkerhed, eller de kan være forskere.

Uddannelsesmæssigt er gruppen delt i to, som vi her kalder cybersikkerhedsspecialister og cybersikkerhedsfaglige – begge grupper er specialiseret indenfor cybersikkerhed. Der er et begrænset udbud af uddannelser, som leder frem til en egentlig specialist-kompetence i cybersikkerhed, men flere er kommet til de seneste år. Det hænger sammen med, at cybersikkerhed stadig en relativt ny disciplin – i hvert fald som noget, der er et bredere behov for. Dernæst er det en specialiseret kompetence, som mange små virksomheder ikke har behov for at kunne dække med flere årsværk, men fint kan være dækket ind af ekstern rådgivning og efteruddannede it-driftsmedarbejdere.

I det etnografiske studie optræder disse ofte som eksterne rådgivere i de små virksomheder som supplement til de lokale løsninger. Studiet viser, at en relativ hyppig udskiftning af konsulenter kan være en udfordring for at have det rette kendskab til den enkelte virksomheds ofte sammenflettede it-løsninger.

***Cybersikkerhedsspecialisterne*** har typisk en universitetsuddannelse på minimum masterniveau og – i vores definition – en specialisering inden for cybersikkerhed af et omfang på minimum 60 ECTS (= 12 måneders fuldtidsuddannelse). De er typisk ansat som fx it- eller netværksanalytikere, udviklere eller sikkerhedsrådgivere. Det er også denne gruppe, der driver forskningen indenfor den it-tekniske del af cybersikkerhed. Cybersikkerhedsspecialisterne er ansat både i det offentlige og i private virksomheder og arbejder indenfor datalogiske discipliner som udvikling af sikre systemer, kommunikation & netværkssikkerhed, hændelseshåndtering og efterforskning af hændelser.

**Tre eksempler på cybersikkerhedsspecialistens uddannelsesbaggrund**

**Kandidatgrad i Cyber Security, Aalborg Universitet (120 ECTS)**
Kandidatuddannelse målrettet at give kompetencer til at hjælpe virksomheder og offentlige institutioner med at modstå cyberangreb, herunder risikoanalyse, trusselshåndtering, netværkssikkerhed, software og privacy. Forudsætter en bachelorgrad inden for teknisk videnskab.

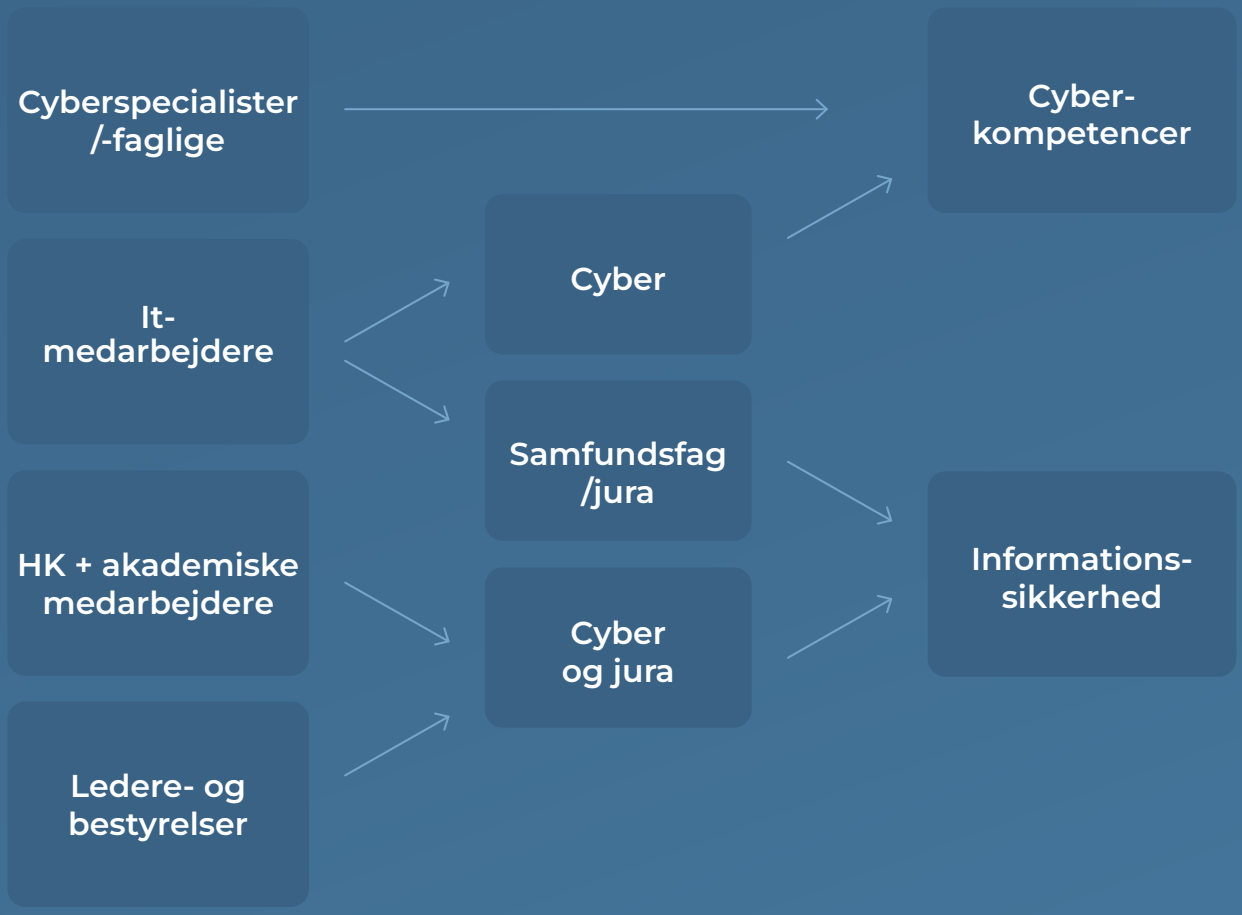
**Master i cybersikkerhed, DTU (60 ECTS)**
En efteruddannelse med deltagergebyr. Målrettet at give kompetencer til at udarbejde risikoanalyser og -styring i forbindelse med cybertrusler mod virksomheder og offentlige institutioner, samt udvikling af sikre it-systemer og udarbejdelse af sikkerhedspolitikker for it-systemer.

**Civilingeniør** eller anden teknisk kandidatgrad med selvvalgt cyberspecialisering (60 ECTS eller mere). En kandidatgrad inden for tekniske videnskaber – fx datalog eller civilingeniør i computerteknologi – kan tones af den studerende, så der opnås en specialistkompetence inden for cybersikkerhed. Det kræver, at der samlet på bachelor- og kandidatuddannelse er plads til mindst 60 ECTS selvvalgte fag inden for cybersikkerhed.

**De relevante kurser kan fx være:**
- Applied Information Security, ITU (7,5 ETCS)
- Cryptographic Computation and Blockchain, ITU (7,5 ETCS)
- Proactive Computer Security, KU (7,5 ETCS)

Sådanne kurser vil ofte også kunne tages som efteruddannelse.

# Hvordan flytter vi de største grupper?



***De cybersikkerhedsfaglige*** er den anden gruppe, som har cybersikkerhed som det primære arbejdsfelt. De har typisk en professionsbachelor i cybersikkerhed, eller de kan være udlært indenfor forsvarets uddannelser for cyberværnepligt og FE's Cyberakademi. Deres uddannelse er lidt mere praksisorienteret, og deres arbejdsfelt vil ofte være tættere på driften, som fx at sikre opdatering af firewall, rettighedsstyring, samt at sikre back up og kryptering.

**Tre eksempler på cybersikkerhedsfagliges uddannelsesbaggrund**

**Professionsbachelor i it-sikkerhed, KEA mfl. (90 ECTS)**
En top-up-uddannelse, som kan bygges oven på erhvervsakademiuddannelserne til datamatiker og it-teknolog. Uddannelsen giver kompetencer inden for god it- og cybersikkerhedsgovernance, herunder om procedurer for at undgå angreb samt opklaring og dokumentation af angreb.

**Diplomuddannelse i it-sikkerhed, Erhvervsakademi Aarhus, (60 ECTS)**
En efteruddannelse med deltagergebyr. Uddannelsen forudsætter en relevant erhvervsakademiuddannelse eller akademiuddannelse (VVU) samt 2 års relevant erhvervserfaring. Der kan også gives adgang gennem en realkompetencevurdering. Uddannelsen giver værktøjer til at analysere, planlægge og vurdere it-sikkerhedsmæssige forhold i forbindelse med drift, kontrol og udvikling af it-systemer i både private og offentlige virksomheder.

**Cyberværnepligt og Forsvarets Efterretningstjenestes Cyberakademi**
Cyberværnepligten, der i maj 2023 blev gjort permanent, er en forlænget værnepligt på 10 måneder, hvor man først gennemfører almindelig værnepligt indenfor et af de tre værn og herefter seks måneders netværksuddannelse med fokus på cybersikkerhed og hackerværktøjer kombineret med en it-supporter-uddannelse[15].

Cyberakademiet er en tre-måneders uddannelse i cybersikkerhed. Efter bestået uddannelse kan eleverne blive ansat i Center for Cybersikkerheds døgnbemandede situationscenter.[16]

**Anbefalinger til cybersikkerhedsspecialister og cybersikkerhedsfaglige**
For denne gruppe er den vigtigste opgave at sikre, at der uddannes flere end i dag, idet ekspertgruppen finder, at der i dag er et væsentligt udækket behov, og at behovet ventes at stige i de kommende år.

**Som illustreret i figuren ovenfor er der to veje til at få volumen op:**
1) at uddanne flere fra specialiserede cybersikkerhedsuddannelser.
2) at "flytte" flere fra de mere generelle it-tekniske uddannelser til cybersikkerhed gennem efteruddannelse eller specialisering på den uddannelse, de har valgt.

**For at uddanne flere fra specialiserede cybersikkerhedsuddannelser er der brug for flere tiltag:**

**Ekspertgruppens vurdering af kompetencesituationen**
Der er et væsentligt udækket behov for specialister i cybersikkerhed. Efterspørgslen på disse kompetencer er steget hurtigt og fortsat er i vækst. Virksomhederne oplever en stor rekrutteringsbyrde: Det tager lang tid at besætte ledige stillinger, og der skal gives en høj løn. Ofte må man opgive at få de specifikke kompetencekrav opfyldt, fordi man ikke kan finde kandidater, som for eksempel både mestrer sikker systemarkitektur og kodning.

Virksomhederne har ofte et behov for medarbejdere, der både kan udvikle nye systemer og produkter, men også har kompetencerne til at tjekke, om sikkerheden er i orden i de samme produkter. Det er ikke en selvfølge, at én person er uddannet til begge opgaver. I stedet vælger virksomheden at hyre eksterne konsulenter til opgaven, eller - hvis man har kapaciteten til det i organisationen - selv bygge kompetencerne op hos medarbejderen efter ansættelse.

Det er positivt, at der i de senere år er kommet flere ordinære uddannelser, som har cybersikkerhed som hovedfokus (jf. eksemplerne ovenfor). Men det er også vurderingen, at der er brug for større volumen for at dække behovet. Derfor er det vigtigt, at de nye uddannelser med fokus på cybersikkerhed får godt fat, og der må gerne komme flere til.

En barriere for at udvide med flere uddannelser og studiepladser er, at forskermiljøet er relativt lille. Det gør det vanskeligt at rekruttere – især dansktalende – undervisere, både til uddannelse og efteruddannelse. Derfor ses der også et behov for at styrke forskningsmiljøet og oprette flere ph.d.-stillinger indenfor feltet cybersikkerhed.

Desuden opleves det som en unødvendig barriere, at erfarne folk, der i årevis har arbejdet med cybersikkerhed eller it, kan opleve at være afskåret fra videre uddannelse i cybersikkerhed på et niveau, der svarer til deres kompetencer. Det skyldes, at de kan have meget forskellige uddannelsesbaggrunde, fordi 'cybersikkerhed' ikke var en uddannelses- eller karrierevej, dengang de først uddannede sig. De opfylder derfor ikke nødvendigvis de formelle adgangskrav i det ordinære uddannelsessystem og er afskåret fra at udvide deres kompetencer med fx en master- eller kandidatuddannelse.

### Øget optag på uddannelser inden for cybersikkerhed

På de uddannelser på universitetsniveau og professionsbachelorniveau, som har cybersikkerhed som hovedfokus, skal optaget fortsat øges, og det kan også være relevant at nye uddannelser kommer til. Det er et fagligt område i udvikling, og det kræver en kapacitetsopbygning.

Som minimum må det sikres, at der ses bort fra disse uddannelser i forhold til de lofter over optaget, som er indført politisk – det gælder både loftet over optag i de store byer (jf. aftalen om regionalisering af uddannelser) og loftet over optag af internationale studerende (som fortsat består, selv om der politisk er lagt op til at lempe det).

### Flere ph.d.-stillinger med fokus på cybersikkerhed

Der er mangel på undervisere, hvilket hænger sammen med, at forskermiljøet i Danmark er lille. Derfor er der brug for en målrettet opbygning af forskemiljøet og dermed et mere solidt grundlag for at sikre, at der er undervisere nok til at uddanne flere studerende. Det vil ikke være muligt at uddanne markant flere på feltet, hvis ikke der sker en kapacitetsopbygning på forsknings- og undervisersiden.

### Forsøg med virksomhedssamarbejde om eksterne undervisere

Som led i at sikre imødekomme den store mangel på undervisere foreslår ekspertgruppen som forsøg et samarbejdsinitiativ med virksomheder, der har cybersikkerhedsspecialister ansat. Ideen er, at de fra deres virksomhed kan få top-op-løn, hvis de har virke som eksterne lektorer i cybersikkerhed – i erkendelse af, at uddannelsesinstitutionerne ikke kan matche den løn, de får i virksomheden.

### Bedre realkompetencevurdering og alternative veje ind for medarbejdere med erfaring

Der findes allerede et RKV-værktøj (realkompetence-vurderingsværktøj) til dele af it-området, som kan vurdere en medarbejders it-kompetencer og udarbejde et vandmærket papir, der kan give adgang til det rette videreuddannelsesniveau. Det anbefales, at der udvikles en tilsvarende udgave til at screene for cybersikkerhedskompetencer, så medarbejdere, der har praktisk erfaring, men ikke formel uddannelse, kan blive indplaceret på rette niveau og gives adgang til videreuddannelse, som de i dag er afskåret fra. Dette kan både være tids- og budgetbesparende, men vil også virke motiverende, fordi de pågældende ikke skal opleve at skulle "starte forfra".

Lovgivningen bør også mere generelt ses efter, så det i højere grad bliver muligt at få adgang til videregående uddannelser på rette kompetenceniveau, selv om man har haft en utraditionel vej gennem uddannelsessystemet og måske ikke formelt har papir på det, man kan. Dette skal modvirke situationer, hvor en erfaren medarbejder ikke kan optages på rette niveau, når eneste hindring er mangel på formel uddannelse.

**For øge tilgangen til cybersikkerhedsfeltet fra andre tekniske it-uddannelser bør følgende initiativer sættes i værk:**

### Flere valgfag/kurser i it-sikkerhed på it-uddannelser

Studerende på it-uddannelser skal i langt højere grad møde cybersikkerhed i deres uddannelse og kunne tone deres uddannelse i den retning. Derfor skal der være flere valgfag/kurser inden for cybersikkerhed på tekniske it-uddannelser på universitetet, fx software engineering og datalogi.

Samtidig er der brug for et større samarbejde om sådanne kurser og bedre oplysning om dem til studerende på tværs af uddannelsesinstitutioner og fakulteter. Dels skal flere studerende få kendskab til muligheden for at tage kurser med cybersikkerhedsindhold som led i deres uddannelse, dels skal de studerende i højere grad samles, så det undgås, at fag ikke bliver oprettet, fx fordi der er for få, der søger ind på det.

# Administration og ledelse med ansvar for informationssikkerhed

I denne gruppe finder vi medarbejdere og ledere, der på det administrative niveau og/eller som en del af ledelsen varetager virksomhedens eller myndighedens informationssikkerhed, herunder compliance. Lederne i denne gruppe har det overordnede ansvar for it-sikkerheden.

***Administrationsmedarbejderne,*** som varetager GRC (governance, risk & compliance), kan have en baggrund fra en HK-stilling eller være uddannet indenfor fx samfundsfag eller humaniora. De arbejder primært med opgaver indenfor informationssikkerhed.

Det etnografiske studie viser, at fx medarbejdere i bogholderiet har relevant viden i form af kendskab til både de enkelte medarbejdere og til vigtige it-systemer, herunder løn, regnskab og HR. Denne gruppe har en fin baggrund for at kunne udarbejde fx risikoanalyser og politikker til at beskytte informationer.

Den databeskyttelsesansvarliges primære rolle er at sikre, at hendes organisation behandler personoplysninger om sine medarbejdere, kunder, udbydere eller andre personer (også kaldet registrerede) i overensstemmelse med de gældende databeskyttelsesregler. Den databeskyttelsesansvarliges primære rolle er at sikre, at hendes organisation behandler personoplysninger om sine medarbejdere, kunder, udbydere eller andre personer (også kaldet registrerede) i overensstemmelse med de gældende databeskyttelsesregler. DPO'en (Data Protection Officer) har som primære rolle at sikre, at organisationen behandler personoplysninger om sine medarbejdere, kunder, udbydere eller andre personer i overensstemmelse med de gældende databeskyttelsesregler. Denne gruppe består oftest af jurister, men kan have gavn af teknisk indsigt  for at kunne udstikke retningslinjer, der er lette og præcise at implementere teknisk.

En særlig gruppe omfatter tekniske specialister, der fra det tekniske felt har arbejdet sig ind i en mere administrativ funktion. Disse kan fx supplere en specialistuddannelse indenfor it med en overbygning i samfundsfag, jura eller historie.

Indenfor ledelse er der tale om både administrative ledere i offentlig forvaltning og i virksomheder samt bestyrelsesmedlemmer. Lederne kan have titler som fx CSO (Chief Security Officer) eller CISO (Chief Information Security Officer), som kan dække over fx en akademisk uddannelse med en mere eller mindre tung efteruddannelse indenfor it-sikkerhed. I jobopslag vil der ofte blive efterspurgt målrettet viden om og styring af informationssikkerhed, fx ISO 2700X eller Certified Information Security Manager (CISM) eller lign.[17], altså certificeringer målrettet it-sikkerhedsledelse. Findes der ikke en leder med it-sikkerhed som hovedområde, så bør der som minimum på direktionsniveau være én eller flere, som kan vurdere, om man fx har de rette kompetencer i virksomheden, eller om der er behov for opgradering eller ekstern konsulentbistand.

For bestyrelsesmedlemmer anbefales det, at minimum én person i bestyrelsen har konkret erfaring med digital sikkerhed og kompetencer til at sætte sig ind i en mere grundlæggende teknisk viden om virksomhedens sikkerhedsorganisation.[18]

Man bør have forståelse for risikostyring, det vil sige, at man har et overblik over virksomhedens sårbarheder og det omkringliggende trusselsbillede samt en forståelse for, hvordan virksomhedens it-sikkerhedsorganisation er bygget op.

Uddannelsesmæssigt kræver opgavevaretagelsen på det administrative felt en stor portion tværfaglighed, idet der skal bruges kompetencer fra både det tekniske/it-faglige felt og fra fx samfundsvidenskab, humaniora eller administration. For de fleste vil disse kompetencer opnås ved efteruddannelse, og en forhøjelse af kompetencerne på dette felt kræver gode og let tilgængelige efteruddannelsestilbud.

**Tre eksempler på uddannelsesbaggrund for administrative medarbejdere og ledere med ansvar for informationssikkerhed:**

**Samfundsvidenskabelig akademiker med efteruddannelse fra IT-Vest**
IT-Vest er et samarbejde mellem Aarhus Universitet, Syddansk Universitet og Aalborg Universitet. IT-Vest udbyder bl.a. efteruddannelse, fx en master i it (60 ECTS), hvoraf man også kan vælge blot at tage enkelte moduler eller 'fagpakker'. Blandt fagpakkerne på 15 ECTS findes fx:

- Risikoanalyse, styring og privacy
- Teknisk it-sikkerhed for generalister
- Netværkssikkerhed

**Militær- eller politiuddannede med master i Intelligence and Cyber Studies fra SDU**
Efteruddannelse med deltagerbetaling udbudt af SDU i samarbejde med Forsvarsakademiet, der kan give it-specialister med ledelsesansvar for cybersikkerhed en bredere forståelse af feltet. Målgruppen er personer med en uddannelse på bachelor-, professionsbachelor- eller kandidatniveau inden for det it/tekniske område. Der forudsættes mindst to års erhvervserfaring. Uddannelsen sigter mod at sætte deltagerne i stand til at analysere og reagere på de mange cyber- og intelligence-spørgsmål, der præger de daglige drifts- og beslutningsprocesser.

**Ledere med efteruddannelse i cybersikkerhed fra DTU eller ITU**
Afhængigt af, hvor i organisationen lederne er placeret, og hvilken type organisation, der er tale om, kan den nødvendige indsigt og redskaber i relation til cybersikkerhed fx opnås gennem kurser som disse:

- Cyberdefence og ledelsesansvar, 5 ECTS (DTU)
- Netværksforsvar og angrebshåndtering, 5 ECTS (DTU)
- Netværkssikkerhed, 10 ECTS (DTU)
- Sikker: Cyber, gratis onlinekursus til virksomheder (ITU)

**Ekspertgruppens vurdering af kompetencesituationen**
Denne gruppe vurderes at komme til at spille en afgørende rolle i forhold til at opfylde de kommende reguleringskrav fra f.eks. NIS2. Den store mangel indenfor denne gruppe er den tværfaglige kompetence, hvor teknisk viden og jura/administration forenes.

Grundet den generelt store efterspørgsel på arbejdsmarkedet på de tekniske it-kompetencer, findes potentialet for at få flere med disse tværfaglige kompetencer især hos samfundsfagligt uddannede eller medarbejdere med administrativ uddannelse og erfaring, der kan suppleres dette med teknisk viden. Det kan dog også være den anden vej, hvor en medarbejder indenfor cybersikkerhedsområdet videreuddanner sig til f.eks. juridiske kompetencer. Denne gruppe må dog forventes at være markant mindre.

Det er ekspertgruppens erfaring, at det i mange større virksomheder er medarbejdere med en uddannelsesbaggrund inden for samfundsfag eller humaniora, som varetager de løbende opgaver med informationssikkerhed. Dette hænger i vidt omfang sammen med, at det er svært at få medarbejdere, der både forstår organisation og jura, og som samtidig har den tekniske baggrundsforståelse. Typisk har medarbejdere med sådanne uddannelser bygget informationssikkerhedskompetencer på efter endt uddannelse eller som led i deres studiejob.

Det er udbredt, at f.eks.  studentermedhjælpere med en baggrund indenfor humaniora eller samfundsfag varetager en stor del af de løbende opgaver indenfor informationssikkerhed under supervision af den ansvarlige for informationssikkerhed i organisationen. Det kan lade sig gøre på arbejdspladser, hvor der er klare processer for informationssikkerhedsarbejdet.

De samfundsvidenskabeligt og humanistisk uddannede medarbejdere har ofte gode kompetencer inden for skriftlig formidling og systematik i forhold til overholdelse af proceskrav, men mangler i udgangspunktet ofte teknisk forståelse. De fleste virksomheder ville formentlig foretrække en blanding af medarbejdere med teknisk baggrund (fx softwareuddannede) og samfundsfaglig baggrund.

Det er ekspertgruppens opfattelse, at det er en klar fordel at have et godt kendskab til virksomheden, produktionens behov og arbejdspladsens kultur, når informationssikkerhedsopgaver skal løftes. Det er derfor en fordel at opkvalificere og videreuddanne medarbejdere, som allerede har administrative ansvarsområder i virksomheden i stedet for at basere sig udelukkende på eksterne konsulenter. Det gælder især i mindre virksomheder, som ikke naturligt vil have en særskilt afdeling til at varetage informationssikkerhed.

Relevante efteruddannelsestilbud er navnlig kurser og certificeringer i privat regi, men det er ekspertgruppens vurdering, at mindre virksomheder kan være udfordret i at vælge de rette kurser. Derudover vurderer ekspertgruppen, at fremtiden vil byde på endnu mere regulering med bl.a. implementering af NIS2 og regulering af kunstig intelligens. Der er derfor god grund

til at få informationssikkerhed integreret i de ordinære uddannelser, f.eks. med fag indenfor jura, statskundskab eller administration, der specifikt omhandler informationssikkerhed og bygger bro mellem det tekniske og det samfundsfaglige felt.

**Anbefalinger vedr. medarbejdere med ansvar for informationssikkerhed**

I forhold til denne gruppe er den vigtigste opgave at sikre, at der fremover er flere på arbejdsmarkedet, som har kompetencer til at kunne varetage informationssikkerheden i organisationen, også når opgaven bliver mere kompleks.

### Bedre overblik over certificeringer og kurser til efter- og videreuddannelse

Selv om der i dag findes en række relevante efter- og videreuddannelsestilbud, som kan opkvalificere medarbejdere inden for informationssikkerhed, så ved mange virksomheder ikke, hvilke kurser der er mest relevante for dem. Derfor er der brug for et brugervenligt overblik, som kan guide virksomhederne.

### Kursuskatalog målrettet studerende fra andre studieretninger

Som studerende kan det være vanskeligt at finde de rigtige fag eller få øjnene op for mulighederne inden for it- og informationssikkerhed, især hvis man ikke har et dybt kendskab til feltet. Ofte er de klassiske it-begreber og titler uden mening for studerende fra andre studieretninger. Det kan derfor være gavnligt med at kursuskatalog, der i højere grad forklarer, hvilke opgaver man bringes i stand til at løse ved at tage de enkelte kurser.

### Kurser/specialisering på kandidatniveau til tværfaglig kompetence

Informationssikkerhed er en disciplin, som går på tværs af fagligheder, og der er brug for bedre muligheder for, at studerende på deres kandidatuddannelse kan skabe sig en informationssikkerhedsprofil. Det omfatter både muligheden for, at studerende på samfundsvidenskab eller humaniora kan tage kurser, som giver basale færdigheder og forståelse inden for computerteknologi, og muligheden for at studerende på it-uddannelser kan tage kurser i regulering og governance i relation til informationssikkerhed. Sådanne muligheder er kendt indenfor sundhedsteknologi, hvor nogle kandidatfag er målrettet både læger og ingeniører. Ligeledes bør det gøres let at tage enkeltfag på andre universiteter, hvis det tilsvarende fag på ens eget institut bliver aflyst på grund af for få deltagere.

### Informationssikkerhed som kandidatspecialisering på samfundsvidenskab

Når det er forventningen, at informationssikkerhed fremadrettet vil fylde langt mere, og der kontinuerligt vil komme ny/opdateret regulering til, betyder det også, at det kan være relevant med en egentlig kandidat-specialisering i informationssikkerhed, som kombinerer juridisk/administrativ viden på feltet for regulering og governance med teknisk indsigt og færdigheder. En sådan kandidatspecialisering kunne f.eks. ligge på jurastudiet eller på uddannelser inden for offentlig administration og i et samarbejde med tekniske it-uddannelser.

# It-medarbejdere og it-sikkerhed

Gruppen omfatter dem, som er primært beskæftiget med it. De arbejder med udvikling af produkter eller sørger for drift, vedligehold og udvikling af funktionsdygtige it-systemer. Gruppen omfatter både it-udviklere og it-supportere. Udviklerne kan enten være en central del af organisationens forretning med produktudvikling, mens it-driftsmedarbejderne og it-udviklere i stabsfunktioner har ansvaret for at sikre, at organisationen har velfungerende it-systemer. De to gruppers arbejdsfelt har stor betydning for niveauet af cybersikkerhed, da det er her, der er risiko for sikkerhedsbrister. Skal man f.eks. sætte en mailfunktion op, kan man sagtens skabe et system, der virker fint, men som ikke overholder de relevante sikkerhedskrav.

Især i mindre virksomheder vil denne gruppe ofte være helt central for arbejdet med cybersikkerhed, fordi der ikke er kapacitet i virksomheden til at have cybersikkerhedsspecialister ansat.

Det etnografiske studie beskriver denne gruppe (i studiet kaldet it-managers) som den reelt centrale aktør i mange små virksomheders it-sikkerhed. Det bunder i et grundigt kendskab til organisationens forskelligartede it-systemer, hvor medarbejderne i nogle tilfælde selv koder forbedringer ind i systemerne. Det kan derfor også være relativt let at opgradere med den rette efteruddannelse. Det er ekspertgruppens erfaring, at det er nødvendigt med fastansatte medarbejdere med de nødvendige kompetencer. Udfordringerne kan ikke løses ved udelukkende at købe sig til eksterne ydelser, da det er centralt med løbende vedligeholdelse af systemerne, og at nogen "holder øje".

Gruppen omfatter både universitetsuddannede, f.eks. softwareingeniører, og uddannede fra erhvervsakademierne med en it-uddannelse på professionsbachelor- eller erhvervsakademiuddannelse inden for it.  De kan også have en erhvervsuddannelse som f.eks. it-supporter eller datatekniker, eller de kan være autodidakte, altså oplært i virksomheden, men med en anden uddannelsesbaggrund.

**Tre eksempler på uddannelsesbaggrund for it-medarbejdere**

**It-udviklere med it-uddannelse på kandidatniveau**
Der kan være tale om en række forskellige kandidatuddannelser med hovedvægt på det tekniske, f.eks. datalogi, computer science og softwareudvikling.

**Diplomingeniør i elektroteknologi, DTU (ECTS)**
Diplomingeniører i elektroteknologi sigter primært mod den elektrotekniske branche eller offentlige virksomheder, der beskæftiger sig med bl.a. it og kommunikationsinfrastruktur. Målet med uddannelsen er at designe, udvikle, implementere og vedligeholde elektriske og elektroniske produkter og systemer.

**Diplomingeniør – softwareteknologi, Via University College (ECTS)**
Uddannelsen sigter på at understøtte, udvikle og teste it-systemer og softwareløsninger. Som færdiguddannet arbejder man med udvikling af eller rådgivning om it-systemer i samarbejde med programmører og dataloger.

**Datatekniker fra TEC (3 til 6 år, evt. kombineret med EUX).**
Uddannelsen omfatter it-supporter, datatekniker med speciale i infrastruktur og datatekniker med speciale i programmering. Denne gruppe arbejder som it-supporter til kunder eller ansatte, som it-konsulent eller softwareudvikler i offentlige eller private virksomheder.

**Autodidakt**
En stor andel af især ældre it-konsulenter er autodidakte som følge af manglende uddannelsesmuligheder indtil 1990'erne. Denne gruppes kompetencer afhænger af erhvervserfaring og kan dække stort set alle områder indenfor it. De autodidakte findes også blandt de øvrige grupper (cybersikkerhedsspecialister, -faglige og medarbejdere med ansvar for informationssikkerhed)

Denne gruppe er relevant som kilde til at få uddannet flere cybersikkerhedsspecialister/-faglige. Med den tekniske uddannelsesbaggrund har de en kortere vej end de fleste til at 'bygge på' med cybersikkerhedskompetencer – enten som en specialisering i deres ordinære uddannelse (via valgmoduler) eller som efteruddannelse. Derfor er der også en tæt sammenhæng mellem den generelle mangel på it-specialister og den specifikke mangel på cybersikkerhedskompetencer. Hvis vi kan uddanne flere med et højt kompetenceniveau inden for it, er der også en større kilde til at få flere cybersikkerhedsspecialister/-faglige. Tilsvarende bliver det sværere at få flere cybersikkerhedsspecialister/-faglige, når der generelt ikke uddannes nok fra de videregående it-uddannelser.

**Vurdering af kompetencesituationen**
Det primære behov i forhold til at forbedre denne gruppes kompetencer indenfor it-sikkerhed er at sikre, at de har en grundlæggende it-sikkerhedsforståelse og en løbende opmærksomhed på it-sikkerhed. Det er ekspertgruppens vurdering, at denne forståelse og opmærksomhed ofte ikke er til stede i de daglige kerneopgaver. Mange organisationer har ikke en 'sikkerhedsmæssig best practice' tydeligt implementeret og er ikke opmærksomme på denne mangel til hverdag.

Behovet hos de store/it-tunge virksomheder vil ofte være at sætte god sikkerhedspraksis i system og udvikle eget set-up for det, mens de små/ikke-it-tunge virksomheder i højere grad kan læne sig op ad den indbyggede sikkerhed i de it-systemer, de bruger, kombineret med opmærksomhed og gode guidelines for it-sikkerhed. Men også hos de små organisationer er det dog stadig en forudsætning, at man i organisationen har en basal viden om it-sikkerhed, og hvordan man sikrer en adfærd, der mindsker risikoen for sikkerhedsbrud.

**Anbefalinger vedrørende it-medarbejdere (udviklere, driftsmedarbejdere mv.)**
Der er to perspektiver på, hvad der er brug for at gøre i forhold til denne store gruppe, som rummer de bredere tekniske it-uddannelser. For det første er det vigtigt, at denne gruppe har en grundlæggende god sikkerhedsforståelse, som de bruger i deres daglige arbejde, også når disse ikke har et sikkerhedsfokus. For det andet er der brug for, at gruppen helt generelt vokser, da der et væsentligt overlap mellem denne gruppe og dem, der er brug for til de mere specifikke felter for cybersikkerhed og informationssikkerhed. Flere it-uddannede skal finde vej over i disse felter gennem toning af deres uddannelse (jf. ovenfor) eller efteruddannelse, og det vanskeliggøres i dag af, at der generelt er så stor efterspørgsel på it-kompetencer, især af den tekniske slags.

**Når begge perspektiver tages i betragtning, giver det grundlag for følgende anbefalinger:**
For at sikre tilstrækkelig opmærksomhed på it-sikkerhed i dagligdagen hos it-udviklere og it-driftsmedarbejdere er der brug for:

### Digital sikkerhed skal gøres opbligatorisk på it-udannelser

Grundlæggende elementer af digital sikkerhed skal gøres obligatorisk på alle it-uddannelser. Det gælder alle de tekniske it-uddannelser på universitets- og professionsbachelorniveau. Dette bliver ikke mindst vigtigt, når der med NIS2 bliver krav til, at der på ledelsesniveau i virksomheder skal være kompetencer i cybersikkerhed

For at sikre et bedre rekrutteringsgrundlag til it-sikkerhedsfeltet er der helt generelt brug for, at der uddannes langt flere it-specialister. Derfor skal optaget øges på it-uddannelserne. Som situationen er i dag, må forskellige it-brancher kannibalisere på hinanden, og det er uholdbart. Derfor er der brug for følgende:

### Undtag it-uddannelser fra uddannelsespolitiske lofter

Dette er også foreslået ovenfor under cybersikkerhedsspecialister, men problemet er det samme her. It-uddannelser, som arbejdsmarkedet har stor efterspørgsel på, skal undtages fra loftet over optaget i de store byer (udflytningsloftet) og loftet over internationale studerende. Disse lofter er en hindring for, at uddannelserne kan optage alle kvalificerede ansøgere på uddannelser, som arbejdsmarkedet har stor efterspørgsel på.

### Tværgående satsning for flere kvindelige ansøgere

På tværs af uddannelser bør der findes tiltag til at styrke interessen blandt kvinder for at søge optagelse på tekniske it-uddannelser. Her kan bl.a. arbejdes med formuleringen og brandingen af uddannelses- og kursusbeskrivelser for at få et bredere ansøgerfelt. Derudover kan der arbejdes med at udvikle nye uddannelser, som kombinerer fagområder, der traditionelt har flere kvindelige ansøgere med de it-områder, som traditionelt har få kvindelige ansøgere – forudsat at der er relevant, naturligvis.

Et succesfuldt eksempel er den nye uddannelse i Kognitions- og datavidenskab, som Københavns Universitet har oprettet i et samarbejde mellem Institut for Psykologi og Datalogisk Institut – uddannelsen giver retskrav til kandidatuddannelsen i datalogi. Ved det første optag på i uddannelsen i 2023 var der rigtig mange ansøgere, hvilket resulterede i en adgangskvotient på 10 og 70 procent kvinder blandt de optagne.

# Kildehenvisninger

[1] Regeringens national strategi for cyber- og informationssikkerhed 2022-2024 19, inkl. Digital sikkerhed i danske SMV'er 2021 og Landsdækkende Center for It-relateret Kriminalitet

[2] DEAs årsdagsrapport 2023: "Til kamp for kompetencerne" s. 28, deas-arsdagsanalyse-2023-til-kamp-for-kompetencerne.pdf (*datocms-assets.com*)

[3] https://itb.dk/tema/branchen-i-tal/it-branchens-krisebarometer/

[4] erhvervsstyrelsen.dk/sites/default/files/2020-03/Arbejdsmarkedet%20for%2 informationssikkerhedskompetencer%20i%20Danmark%20-%20Rapport.pdf

[5] assets.kpmg.com/content/dam/kpmg/dk/pdf/dk-2020/12/Initiativkatalog.pdf

[6] Digital Sikkerhed i danske SMV'er, september 2022, Erhvervsstyrelsen

[7] danskindustri.dk/brancher/di-digital/nyhedsarkiv/nyheder/2023/2/ny-analyse-1079-virksomheder-pa-tvars-12-sektorer-ser-ud-til-at-blive-direkte-omfattet-af-nis2-direktivet/

[8] d-maerket.dk/events-og-artikler/brug-d-maerket-og-bliv-klar-nar-eu-strammer-reglerne-for-cybersikkerhed-med-nyt-nis2-direktiv/

[9] Væsentlige enheder kan straffes med administrative bøder maksimalt på op til 10 000 000 EUR – 2 % af den samlede globale årsomsætning, mens vigtige enheder kan straffes med administrative bøder med et maksimum på op til 7 000 000 EUR eller 1,4 % af den samlede globale årsomsætning. Kilde: NIS2-direktivet, artikel 34.

[10] mismatch-paa-arbejdsmarkedet-for-it-uddannede-i-2030-udgivet-juni-2021.pdf (*ida.dk*)

[11] Figuren nedenfor og de efterfølgende om optag og søgning på de videregående it-uddannelser er alle hentet fra ATV's faktaark om it-uddannelserne: Fakta: Flere ansøgere til alle IT-uddannelser i Danmark | ATV og Faktaark for søgning og optag på IT-uddannelserne 2022 | ATV

**Fra side 9**

*[1]* www.aau.dk *[2]* www.itu.dk

[12] itu.dk/Om-ITU/Presse/Nyheder/2023/Kvinderne-stempler-i-stor-stil

[13] DI, juni 2023: Universiteter afviser kvalificerede ansøgere til IT- og STEM-uddannelser – DI (*danskindustri.dk*)

[14] "Good" organizational reasons for "bad" cybersecurity",
Laura Kocksch og Torben Eigaard Jensen, AAU

[15] forsvaret.dk/da/nyheder/2023/rekordmange-cybervarnepligtige-bliver-ved-forsvaret/

[16] cfcs.dk/da/nyheder/2023/center-for-cybersikkerhed-soger-talenter-til-nyt-cyberakademi/

[17] HBS rapport 2019 https://digst.dk/media/28840/arbejdsmarkedet-for-informationssikkerhedskompetencer-i-danmark-rapport.pdf

[18] CYBERSIKKERHED FOR BESTYRELSER, Marts 2021,
Anbefalinger til Styrkelse af Cyberkompetencer

# Hvem er IDA?

IDA samler alle, der arbejder på højt niveau med teknologi, naturvidenskab og it. Blandt vores medlemmer er der både specialister, generalister, medarbejdere, ledere og selvstændige. Vi understøtter medlemmerne gennem hele livet fra studiet til og med pensionen.

IDA arbejder med at understøtte FNs verdensmål og en bæredygtig fremtid.

Det bedste valg for dig, der arbejder med naturvidenskab, it eller som ingeniør.