Rådet for
Digital Sikkerhed

30. januar 2023

Manglende cyber- og informationssikkerhedskompetencer

Kære uddannelses- og forskningsminister, Christina Egelund, børne- og undervisningsminister, Mattias Tesfaye, og forsvarsminister, Jakob Ellemann-Jensen

Danmark er blandt de mest digitaliserede samfund i verden, og vi er blevet afhængige af, at det digitale fungerer, at det altid er til rådighed, og at den digitale behandling sker korrekt. Danmark står over for et væsentlig skærpet trusselsbillede, og vi skal derfor kunne håndtere trusler som cyberangreb[1]. Det fremgår af en analyse udarbejdet af regeringens sikkerhedspolitiske analysegruppe. Det stiller os med et akut kompetencebehov indenfor sikkerhedsområdet, da Danmark i 2030 vurderes at mangle 15-20.000 fagfolk indenfor cyber- og informationssikkerhed[2]. Med dette brev kommer vi med en række anbefalinger til at understøtte denne udvikling.

Behov for en samlet indsats, der kan sikre Danmark de nødvendige kompetencer.

Vi skal både sikre flere med dybdefaglig teknologisk baggrund og tilføje teknologiske/digitale komponenter til de samfundsvidenskabeligt og humanistisk uddannede. Vi har brug for en bredde af kompetencer. Alt fra teknologifaglige, der arbejder med at styrke sikkerheden, til dem, der udarbejder trussels- og risikovurderinger, undersøger menneskers digitale adfærd, og har indsigt i staters og andre aktørers intentioner og lovgivning om alt fra brugen af logning til GDPR. Der er behov for særligt at sætte fokus på kapacitetsudbygningen på cyber- og informationssikkerhed. Det kan ske gennem etablering af flere uddannelser og øget mulighed for merit/kompetence-anerkendelse mellem alle niveauer i uddannelsessystemet. Anbefalinger til, hvorledes vi opbygger cyberkompetencer (uddybes i bilag):

1. Erhvervserfaring med cyber- og informationssikkerhed bør være meritgivende i uddannelsessystemet
2. Tydeligere karriereveje inden for cyber- og informationssikkerhed
3. Etablering af et offentlig-privat samarbejde om en erhvervspraktik for studerende på alle niveauer
4. Bedre muligheder for omskoling/efter- og videreuddannelse indenfor cyber- og informationssikkerhed
5. Digital teknologiforståelse i grundskolen
6. Klare og synlige veje igennem hele uddannelsessystemet.
7. Flere forskningsmidler skal understøtte forskningsmiljøerne på universiteterne
8. Etablering af en offentligt-privat rådgivende arbejdsgruppe
9. Øget optag på cybersikkerhedsuddannelser
10. Tiltrækning og fastholdelse af internationale talenter
11. Etablering af en taskforce der kan sikre koordinering

Vi ser frem til dialoger med jer om, hvordan udfordringerne kan mødes i den kommende tid.

Med venlig hilsen
DI Digital, Dansk IT, Djøf, Ingeniørforeningen, IT-Branchen, PROSA, Rådet for Digital Sikkerhed

[1] https://www.forsvaret.dk/globalassets/fmn/dokumenter/nyheder/2022/-dansk-sikkerhed-og-forsvar-mod-2035-den-sikkerhedspolitiske-analyserapport-.pdf
[22] Se vedhæftede analyse

Rådet for Digital Sikkerhed
Vester Farimagsgade 37B, 1.th., 1606 København V
Telefon: +45 53 36 02 23 mail: info@digitalsikkerhed.dk web: www.digitalsikkerhed.dk

Bilag: Konkrete forslag til fremme opbygningen af cyber-kompetencer i Danmark.

1. Dokumenteret arbejds- og erhvervserfaring med cyber- og informationssikkerhed bør være meritgivende i uddannelsessystemet.

Mange i forsvaret, politiet, det offentlige og private arbejdspladser har ikke papir på deres cyber- og informationssikkerheds-kompetencer. Uddannelse indenfor området har nemlig i mange år været præget af "on-the-job" træning og sidemandsoplæring. Kompetencer indenfor cyber- og informationssikkerhed, digital risikostyring og trusler, sårbarheder, kritisk infrastruktur, mest beskyttelsesværdige aktiver samt risikovurderinger og investeringsviden herom, har ikke haft plads i uddannelsessystemet. Selvom der nu er flere uddannelser i gang og på vej, er der et stort behov for, at praktisk erfaring med arbejdet indenfor cyber- og informationssikkerhed kan være meritgivende til flere trin på uddannelsesstigen. Fx kan ingeniøruddannelser alene optage studerende med specielle bacheloruddannelser[3]. Det gør det umuligt for fx studerende med en professionsbachelorgrad at komme ind. Det gælder i høj grad også for ikke-teknisk uddannede, som er beskæftiget med elementer af cybersikkerhed.
På Erhvervsuddannelserne (EUD) og de erhvervsrettede videregående uddannelser (KVU og MVU) findes der lovgivning om Realkompetencevurdering (RKV), men især på de erhvervsrettede videregående uddannelser bliver det stort set ikke brugt, primært pga. institutionelle barrierer. Uddannelses- og forskningsministeriet bør derfor sætte sig for bordenden og, sammen med arbejdsmarkedets parter, tage hånd om de institutionelle barrierer. Sideløbende bør der politisk arbejdes med, hvorledes der også kan etableres RKV aktiviteter i forhold til de universitære uddannelser (LVU) på en måde, som samtidig sikrer, at man ikke går på kompromis med det faglige niveau.

2. Tydeligere karriereveje inden for cyber- og informationssikkerhed

Mange unge finder det svært at gennemskue, hvordan man kommer fra "studievalg" til job indenfor cyber – og informationssikkerhed. Der er behov for at skabe et samlet overblik og strategi for, hvordan en vertikal uddannelsesproces med fokus på cyber- og informationssikkerhed kombineret med behovet for mere horisontal kompetenceudvikling, kan understøtte de behov, der vil være i fremtiden. Der er behov for en samlet kortlægning af, hvilke uddannelser der har fokus på cyber- og informationssikkerhed - lige fra gymnasial uddannelse, erhvervsuddannelse, erhvervsakademiuddannelse, professionsbachelor, kandidat til ph.d. - som kan danne grundlag for en strategisk indsats på området med afsæt i det kompetencebehov, der vil være i de kommende år. Et sådant overblik vil også hjælpe dem, der skal guide de unge i deres uddannelsesvalg. Dernæst bør uddannelsesmulighederne inden for cyber- og informationssikkerhed kommunikeres langt mere tydeligt over for de unge, som skal vælge uddannelse. Dette kunne fx gøres på UG.dk (Uddannelsesguiden) og gennem en målrettet indsats overfor vejlederne i folkeskolen og ungdomsuddannelserne. Derudover er der også behov for at arbejde med at synliggøre karrierevejene indenfor cyber- og informationssikkerhed, fx med udgangspunkt i ENISA's European Cyber Security Skills Framework.

3. Etablering af et offentlig-privat samarbejde om en cyber-lærlinge ordning / erhvervspraktik for studerende på alle niveauer (EUD, KVU, MVU og LVU)

Den praksisnære tilgang til uddannelse indenfor it -området skal fastholdes. På både EUD, KVU og MVU er der som en del af uddannelsen praktik. Her kunne man med et partnerskab sikre, at en del af praktikken også indeholder relevant viden om cyber- og informationssikkerhed for den givne uddannelse. For LVU bør det overvejes, hvor læring emnet giver mening for den givne uddannelse. Der er brug for flere eksperter indenfor cyber- og informationssikkerhed, men også for at der er en stærk grundlæggende viden indenfor

[3]jf. bekendtgørelsen https://www.retsinformation.dk/eli/lta/2021/104 (bilag 2)

relaterede fagområder (som IT, ledelse, risikostyring) f.eks. gennem kurser eller integreret i eksisterende kurser. Desuden anbefaler vi, at Industriens Fond, herunder deres initiativer som Skills og Digital Dogme, inddrages i udmøntningen af dette forslag.

4. Bedre muligheder for omskoling/efter- og videreuddannelse indenfor cyber- og informationssikkerhed

Cyber- og informationssikkerhed er meget mere end bare teknik (ingeniører, datamatikere). Der er også karrieremuligheder indenfor f.eks. jura, etik, governance, risikostyring, kommunikation, formidling, strategi, og politik. Derfor skal området tænkes bredt, og mulighederne for at tilføre kompetencer til professionelle indenfor forskellige faggrupper bør styrkes osv. Det skal understøttes, at generalister inden for fx samfundsvidenskab og humaniora er rustet til at arbejde med området, fx gennem opkvalificering via VEU/VVEU.

5. Digital teknologiforståelse i grundskolen

Viden om og interesse for digitale teknologier og digital sikkerhed skal grundlægges tidligt. Det sker desværre ikke på systematisk vis i skolen i dag. De fleste børn og unge mangler en grundlæggende teknologiforståelse. Derfor bør teknologiforståelse indføres som et selvstændigt og obligatorisk fag i grundskolen. Ligeledes bør teknologiforståelse integreres i skolens øvrige fag med afsæt i erfaringer fra forsøget med teknologiforståelse. Fagområdet skal klæde eleverne på til at anvende, udvikle og forstå digitale teknologier, ligesom de skal blive i stand til at tage kritisk stilling til digitale teknologier og deres betydning for deres eget liv såvel som for vores samfund.

6. Klar og synlige veje igennem hele uddannelsessystemet

Der er behov for at se på sammenhængen i uddannelsessystemet. Det bør være således, at uanset hvilket uddannelsestrin man befinder sig på, er der klare veje til næste trin. Der er ligeledes behov for en model i stil med GSK eller RKV, hvor man gennem suppleringskurser kan opnå tilstrækkelig merit til, at man kan springe uddannelseselementer eller -niveauer over, for fx at kunne blive immatrikuleret direkte på en kandidatuddannelse. Det er vigtigt, at de meget dygtige teknikere fra forsvaret (fx de cyberværnepligtige), fra politiet, fra sundhedssektoren, fra den private sektor, som har begrænset eller ingen uddannelse, kan få merit og dermed papir på deres oparbejdede erhvervskvalifikationer i forhold til at videreuddanne sig. Universiteterne bør udbyde fag, som er åbne for alle med relevant erhvervserfaring. Kurserne bør kunne gennemføres på få koncentrerede uger og alligevel give ECTS-point, som kan sammenlægges til en grad. Dette kan evt. laves i samarbejde med folkeuniversitetet. Tiltaget kan kombineres med mønter/medaljer for gennemført kursus, som der har været succes med hos udenlandske kursusudbydere.

7. Flere forskningsmidler skal understøtte forskningsmiljøerne på universiteterne

Det er en stor udfordring, at der mangler forskningsmidler til cybersikkerhed. Der er behov for et stærkere uddannelses- og forskningsmiljø på universiteterne, der kan understøtte en solid forskningsbaseret undervisning indenfor området. Der er fx. behov for flere ph.d.er indenfor området, som kan være med til at skabe en grundstamme for øget undervisning de kommende år. Også her er der brug for en bredde i tilgangen til fagområder, da forskning i cybersikkerhed foregår inden for både tekniske og samfundsvidenskabelige discipliner.

8. Etablering af et offentligt-privat rådgivende arbejdsgruppe

Der bør etableres et rådgivende forum, som kan bistå myndighederne på området og komme med konkrete forslag til, hvorledes man skaber mere fokus på cyber- og informationssikkerhed gennem uddannelsessystemet, og dermed vedvarende får uddannet flere med de rette kompetencer. En sådan

arbejdsgruppe bør sammensættes af eksperter indenfor området, arbejdsmarkedets parter, samt repræsentanter fra uddannelsessystemet og forskningsverdenen. Det skal sikre en solid forståelse af både efterspørgsels- og udbudsside. Der kan evt. ses på eksisterende rådgivende fora, om opgaven meningsfyldt kan indlejres heri. Se vores beskrivelse af Initiativ 1: Nedsættelse af en arbejdsgruppe (Initiativer for "Informationssikkerhed i uddannelsessystemet".

9. Øget optag på cybersikkerhedsuddannelser

For at imødekomme den stigende efterspørgsel efter cybersikkerhedskompetencer bør vi uddanne flere cybersikkerhedsspecialister i Danmark. Derfor er der behov for at øget optagelse på it- og cyberuddannelserne. Det skal ske ved at etablere flere pladser der, hvor efterspørgslen i dag overstiger udbuddet af uddannelsespladser, og hvor kvalificerede ansøgere derfor afvises (fx på AAU i København). Det indebærer øget optag på uddannelser, der er geografisk placeret, hvor de studerende ønsker at bo, og ligeledes hvor koncentrationen af virksomheder og efterspørgslen efter cyberkompetencer sammenfaldende er størst.

10. Tiltrækning og fastholdelse af internationale talenter

For at udvide talentmassen og rekrutteringspotentialet bør Danmark gøre en målrettet indsats for at tiltrække, uddanne og fastholde flere internationale talenter inden for cybersikkerhed. Som en del af indsatsen bør flere it-uddannelser (gen)udbydes på engelsk, og der bør arbejdes særskilt for, at udenlandske studerende på forskellige uddannelsesniveauer kommer i praktik i danske virksomheder, og får en større tilknytning til det danske arbejdsmarked og Danmark.

11. Etablering af en taskforce der kan sikre koordinering

Etablering af en task force, der kan drive initiativerne, så der opnås en samordning og forankring inden for de forskellige ministerområder, der er involveret i dagsordenen og som kan understøtte OPP-arbejdsgruppen (pkt. 8).