Behov for viden om cyber - og informationssikkerhed

uddrag af baggrundsrapport

Riis, Marianne; Østergaard, Jørgen Theibel; Hellensberg, Christina Elisabeth; Eychenne, Daniele Edith; Nielsen, Charlotte Barbara; Sterup, Lotte; Elise Wied, Mia

Publication date:
2019

Document Version
Også kaldet Forlagets PDF

KØBENHAVNS PROFESSIONS HØJSKOLE

BEHOV FOR VIDEN OM CYBER- OG INFORMATIONSSIKKERHED

- uddrag af baggrundsrapport

Marianne Riis, Jørgen Theibel Østergaard, Christina Hellensberg, Danièle Eychenne, Charlotte Barbara Nielsen, Lotte Sterup og Mia Elise Wied

Udarbejdet af Københavns Professionshøjskole for Undervisningsministeriet – Styrelsen for It og læring

Institut for Didaktik og Digitalisering
Københavns Professionshøjkole
September 2018, uddrag marts 2019

KØBENHAVNS PROFESSIONS HØJSKOLE

Kolofon

Om rapporten
Rapporten er udarbejdet af Københavns Professionshøjskole for Styrelsen for It og Læring, STIL. Forfattere: Marianne Riis, Jørgen Theibel Østergaard projektleder, Christina Hellensberg projektleder, Danièle Eychenne, Charlotte Barbara Nielsen, Lotte Sterup & Mia Elise Wied.

Institut for Didaktik og Digitalisering,
Københavns Professionshøjskole

Indhold

DEL 1 - Indledning 4
Kort om projektet 4
Undersøgelsesspørgsmål- og tilgang 4
Rapportens opbygning 6
DEL 2 - Om cyber- og informationsikkerhed 7
Cyber- og informationssikkerhed på dagsordenen 8
Behov for kompetenceudvikling om cyber- og informationssikkerhed 8
Undersøgelser af kompetenceudviklingsbehovet ifm. cyber- og informationssikkerhed 9
Udvalgte resultater fra Epinion (2018) 9
Udvalgte resultater fra Digitaliseringsstyrelsen, DKCERT og DeIC (2017) 11
Udvalgte resultater fra /KL.7 (2017) 12
DEL 3 - Tværgående analyse baseret på interessentinterview 14
Interview med interessenter 15
Kort om interviewdelen 15
Overordnede resultater 16
Danskernes videns- og kompetenceniveau er generelt godt, men kunne være bedre 16
Børn og unges viden og kompetencer skal omsættes til handling 16
Voksne mangler – især teknisk - viden og kompetencer ift. at tage ansvaret på sig 17
Behov for organisationsdidaktisk udvikling og målrettede strategier 17
EUD, FGU og VEU er oversete målgrupper 17
Generelt behov for nytænkning af undervisning i cyber- og informationssikkerhed 18
Udfordringer med anvendelse af sociale medier i undervisning 18
Fokus på køns-, alders- og generationsforskelle 18
Flere aktører på banen 19
Specifikke faglige kompetenceudviklingsbehov 19
Emner inden for cyber- og informationssikkerhed, der med fordel kan styrkes 20
Del 4 – Sammenfatning 22
Referencer 25

DEL 1 - Indledning

Denne rapport er en del af den første delleverance i projektet 'Vidensområder på EMU om cyber- og informationssikkerhed'. Et projekt som Københavns Professionshøjskole, Institut for Didaktik og Digitalisering løser på opdrag fra Styrelsen for It og Læring (STIL), Undervisningsministeriet i perioden 2018-2019.

Kort om projektet

Det overordnede formål med projektet er at etablere videnområder på Danmarks læringsportal, EMU'en om cyber- og informationssikkerhed. Baggrunden herfor skal b.la. findes i Regeringens nationale strategi for cyber- og informationssikkerhed (2018-2021), der har til formål at sikre, at befolkningen, virksomheder og myndigheder kender og kan håndtere digitale risici (Finansministeriet, 2018).

Som led i strategiens *initiativ 2.1. Digital dømmekraft og kompetencer via uddannelsessystemet* skal der etableres vidensområder om cyber- og informationssikkerhed på EMU'en bestående forskellige materialeformer, der kan understøtte kompetenceudvikling. Målet er at medvirke til at sikre, at børn, unge og voksne skal kunne færdes sikkert på internettet og udnytte de digitale muligheder på en tryg, forsvarlig og etisk korrekt måde. Det vurderes i denne sammenhæng, at der er behov for kompetenceudvikling, og det kræver bl.a. tilgængelige, relevante materialer.

De, i projektet, udvalgte eksisterende og nyudviklede materialer om cyber- og informationssikkerhed skal kunne bruges i undervisningen i grundskolen, de gymnasiale uddannelser, erhvervsuddannelser, FGU og VEU. Indhold (og efterfølgende udbredelsesaktiviteter) skal være målrettet lærere, pædagoger, undervisere og skoleledelser. Materialer kan i denne sammenhæng både omfatte videoer, film, rapporter, hjemmesider, evalueringer, kampagner og kampagnesites, test, cases, øvelser, baggrundsmateriale og forslag til undervisnings- og læringsaktiviteter, samt ledelseshandlinger.

Undersøgelsesspørgsmål- og tilgang

I forbindelse med opgaveløsningen inden for denne delleverance af projektet, har vi bl.a. arbejdet ud fra et undersøgelsesspørgsmål, der lyder som følger:

> Hvilke *kompetenceudviklingsbehov* ift. cyber- og informationssikkerhed kan identificeres hos målgrupperne i hhv. grundskolen, de gymnasiale uddannelser, erhvervsuddannelser, FGU og VEU, heriblandt også lærere/undervisere og andet pædagogisk personale, samt skoleledelser? Og hvilke *materialeudviklingsbehov* kan på den baggrund anbefales?

Kompetenceudviklingsbehov henviser i denne sammenhæng til de behov for udvikling af viden, færdigheder og kompetencer, som kan udledes dels af eksisterende undersøgelser og dels af interessenternes vurderinger. Der kan være tale om kompetenceudviklingsbehov for alle målgrupper, dvs. både elever, studerende, kursister, lærere, undervisere, andet pædagogisk personale og ledelsesniveauet.

Indledningsvist har vi studeret udvalgte eksisterende undersøgelser om danskernes viden om cyber- og informationssikkerhed. Formålet har været at skabe et foreløbigt overblik over feltet og at kvalificere vores efterfølgende undersøgelser og analyser. I denne forbindelse har vi udvalgt tre undersøgelser, der i varierende omfang kan bidrage med viden dels om, hvilke kompetenceudviklingsbehov, der måtte være i forskellige målgrupper og i mindre omfang også hvilke materialeudviklingsbehov, der kan udledes heraf.

Dernæst har vi interviewet 16 udvalgte interessenter (fremgår af rapportens tredje del), der alle arbejder med og har viden om forskellige emner inden for fagfeltet cyber- og informationssikkerhed. Analysen har haft til formål at afdække interessenternes vurdering af bl.a. status på området ift. indhold og materialer, samt at pege på kompetence- og materialeudviklingsbehov.

Cyber- og informationssikkerhed

I projektet har vi i udgangspunktet arbejdet ud fra de definitioner, der gives for hhv. cyber- og informationssikkerhed i Regeringens føromtalte *National strategi for cyber- og informationssikkerhed*:

Cybersikkerhed	Informationssikkerhed
Cybersikkerhed omfatter beskyttelse imod de sikkerhedsbrud, der opstår som følge af angreb mod data eller systemer via forbindelse til et eksternt net eller system. **Arbejdet med cybersikkerhed fokuserer således på sårbarheder ved sammenkoblingen mellem systemer, herunder forbindelser til internettet.**	Informationssikkerhed er en bred betegnelse for de samlede foranstaltninger til at sikre informationer i forhold til fortrolighed, integritet (ændring af data) og tilgængelighed. I arbejdet indgår blandt andet organisering af sikkerhedsarbejdet, påvirkning af adfærd, processer forbehandling af data, styring af leverandører, samt tekniske sikkerheds-foranstaltninger.

Tabel 1. Definitioner på Cyber- og informationssikkerhed. (Finansministeriet, 2018, s. 7)

Uddannelsesområder

Hele projektet, og således også anbefalingerne i denne rapport, retter sig mod følgende uddannelsesområder:

- Grundskolen
- De gymnasiale uddannelser
- Erhvervsuddannelse (EUD)
- Forberedende grunduddannelse (FGU)
- Voksen- og efteruddannelse (VEU)

Uddannelsesområderne dækker således over både børn, unge, unge voksne og voksne.

Rapportens opbygning

Rapporten består ud over denne indledning af tre dele:

Del 2 omhandler selve det faglige område, cyber- og informationssikkerhed. Baggrunden for at sætte fokus på cyber- og informationssikkerhed foretages med henvisning til den nationale strategi for cyber- og informationssikkerhed (2018-2021). Endvidere præsenteres resultater fra udvalgte undersøgelser på området, der kan have relevans for herværende projekt.

Del 3 omhandler den tværgående interessentanalyse, der er foretaget på baggrund af interviews med interessenter, der alle arbejder med forskellige aspekter af cyber- og informations-sikkerhed.

Del 4 er en kortfattet sammenfatning, som også indeholder anbefalinger ift. kompetence- og materialeudviklingsbehov.

DEL 2 - Om cyber- og informationssikkerhed

I denne del af rapporten beskrives baggrunden for at sætte fokus på cyber- og informationssikkerhed. Dette gøres med henvisning til den nationale strategi for cyber- og informationssikkerhed (2018-2021). Endvidere præsenteres resultater fra udvalgte undersøgelser på området, der kan have relevans for herværende projekt.

Hovedpointerne i denne del er:

- Cyber- og informationssikkerhed er for alvor kommet i fokus i danskernes bevidsthed, og dette har resulteret i en bred anerkendelse af et kompetenceudviklingsbehov inden for området.
- Fra myndighedernes side ønskes dette kompetenceudviklingsbehov klarlagt og adresseret gennem forskellige undersøgelser, strategier og initiativer, herunder dette projekt.
- Tidligere undersøgelser på området bekræfter behovet for kompetenceudvikling, især hvad angår teknisk viden og handlekompetencer.
- Konkrete faglige emner, der med fordel kan styrkes gennem kompetenceudvikling inden for området, kan i en vis udstrækning identificeres ud fra tidligere undersøgelser.
- Generelt ses holdnings- og adfærdsændringer på området som ønskværdige, både blandt børn, unge og voksne.
- Anvendelse af især sociale medier i undervisnings- og læreprocesser ses som en udfordring, men også som et potentiale ift. cyber- og informationssikkerhed, som bør adresseres gennem kompetenceudvikling og udvikling af relevante materialer.
- På baggrund af eksisterende undersøgelser, peges der også på et stort behov for kompetenceudvikling på ledelsesniveauet, og det anbefales at arbejde med deciderede kulturændringer, der kan fremme en mere hensigtsmæssig, etisk adfærd og praksis omkring cyber- og informationssikkerhed i skoler og uddannelsesorganisationer.

Cyber- og informationssikkerhed på dagsordenen

Cyber- og informationssikkerhed er temaer, der for alvor er kommet på dagsordenen i den offentlige debat i Danmark. Senest har opsigtsvækkende sager som Facebook/Cambridge Analytica og Facebook gruppen Offensimentum, på hver deres vis været med til at sætte fokus på cyber- og informationssikkerhed, -adfærd og -etik i den brede befolkning. Sager som disse, har også været med til at skabe opmærksomhed om det kompetenceudviklingsbehov, der er i befolkningen i forhold til at kunne begå sig trygt, sikkert og etisk ansvarligt i et stadig mere digitaliseret og globaliseret samfund.

I foråret 2018, lancerede Regeringen, via Finansministeriet, en ny national strategi for cyber- og informationssikkerhed for perioden 2018-2021 som opfølgning på tidligere strategier. Strategien skal også ses i forlængelse af Forsvarsforliget 2018-2023, der blandt andet har som formål at sikre Danmark mod deciderede cybertrusler.

Strategien indeholder 25 initiativer og seks delstrategier for de mest kritiske sektorers arbejde med cyber- og informationssikkerhed. Initiativ nr. 2 *Bedre kompetencer* har til formål at understøtte udvikling af kompetencer blandt borgere, virksomheder og myndigheder (Finansministeriet, 2018, s. 28-29). Delinitiativ 2.1. handler specifikt om at hæve digital dømmekraft og digitale kompetencer via uddannelsessystemet, i denne sammenhæng forstået som grundskolen, gymnasiet, erhvervsuddannelser (EUD), FGU og VEU. Det er som led i dette specifikke delinitiativ, at dette projekt er igangsat.

Behov for kompetenceudvikling om cyber- og informationssikkerhed

I den nationale strategi for cyber- og informationssikkerhed, konstateres det blandt andet, at:

> Mange børn og unge ved ikke nok om, hvordan de beskytter sig selv og andre på internettet, eller hvilke aktører de skal være opmærksomme på. (Finansministeriet, 2018, s. 28)

Og endvidere at:

> Børn og unge skal have de bedste muligheder for at gribe de digitale muligheder og til at agere kritisk som borgere i et digitaliseret samfund, børn og unge skal have evnerne til at tænke kritisk i forhold til indhold på internettet, så de er opmærksomme på truslen fra falske nyheder, radikalisering, cybermobning, svindel mv. (Finansministeriet, 2018, s. 29)

Arbejdet med at udvikle børn og unges digitale kompetencer er ikke nyt i uddannelsessystemet, men med den aktuelle strategi, er fokus i højere grad end tidligere på de risici og konsekvenser, der kan være forbundet med færden på især internettet. Det er dog værd at bemærke, at der i strategien også tales om, at børn og unge skal kunne udnytte de mange muligheder – bl.a. gennem øget indsigt i tekniske sikkerhedsforanstaltninger. Målet er derfor, at børn og unge skal:

> ... kunne færdes sikkert på internettet og udnytte de digitale muligheder på en tryg og sikker måde, ligesom de skal være bevidste om, hvilke regler og konsekvenser, der følger af at begå sig online. Børn og unge skal gøres digitalt kompetente og opbygge en stærk digital dømmekraft med forståelse af de etiske dilemmaer, der ligger ud over den tekniske forståelse af digitaliseringen. (Finansministeriet, 2018, s. 29)

Således lægges der i strategien op til en kompetenceudvikling, som nok har fokus på den tekniske side af cyber- og informationssikkerhed, men som også i høj grad skal fokusere på udvikling af 'dømmekraft'. I samme delinitiativ lægges der også op til, at voksne skal have øget viden om cyber- og informationssikkerhed, hvorfor projektet her ikke kun retter sig mod grundskolen og ungdomsuddannelserne men en også inkluderer materiale til (unge) voksne, der eksempelvis deltager i FGU eller VEU.

Undersøgelser af kompetenceudviklingsbehovet ifm. cyber- og informationssikkerhed

I det følgende præsenteres udvalgte resultater af tre tidligere undersøgelser, der hver især kan bidrage med viden om, hvilke kompetenceudviklingsbehov, der kan være blandt børn, unge og voksne ifm. cyber- og informationssikkerhed.

Udvalgte resultater fra Epinion (2018)

Kompetenceudviklingsbehovet angående cyber- og informationssikkerhed er for nylig blevet undersøgt i en analyse af børn og unge (12-25 år), lærere og forældres kendskab til it-sikkerhed og god dataadfærd foretaget af konsulent- og analysefirmaet, Epinion på opdrag fra Undervisningsministeriet.

Epinions rapport *Styrkelse af dataetik og it-sikkerhed på undervisningsområdet* (2018) handler ikke kun om cyber- og informationssikkerhed, men afdækker også børn og unges generelle mediebrug i og uden for skolen, samt forældre, lærere og skoleledelsers erfaringer og perspektiver. Som sådan vil resultaterne kunne være relevante for især grundskolen, men også ungdomsuddannelserne og FGU. Det er primært i kapitlerne 7 om *Sikker og kritisk brug af nettet* ift. it-sikkerhed og 8 om *It-sikkerhed, dataetik og datapraksis i skolen* ift. dataetisk praksis, at vi har hentet inspiration.

Epinions undersøgelse dokumenterer først og fremmest, at sociale medier er blevet en integreret del af børn og unges hverdags- og skoleliv. Her er der dog udfordringer både for børn, unge, lærere og skoleledelser ift. at gennemskue it-sikkerhed, især databeskyttelse. Der er også mere interaktionelle og kommunikative udfordringer, idet undersøgelsen også peger på, at kun ca. en sjettedel af børn og unge benytter sociale medier til at deltage i samfundsdebatten gennem deling af indlæg, læsning af nyheder, diskussion af interesser og politik (Epinion, 2018, s. 14-16). I denne sammenhæng, er det også interessant, at 86% af elever og studerende oplever, at ikke-didaktiserede, digitale læremidler er blevet en integreret del af undervisningen.

Hvad angår **it-sikkerhed**, peger Epinions undersøgelse på, at børn og unge i høj grad oplever at have kontrol over de data, som de deler via internetbaserede medier, teknologier, services mv. Denne *høje digitale selvsikkerhed* baseres især på børn og unges erfaringer med at kontrollere,

hvad de selv bidrager med i form af input. Anderledes ser det ud mht. hvad, der efterfølgende sker med deres data, altså på output-siden. Her er der en accept af, at man ikke har kontrol (Epinion, 2018, s.58). Der mangler i denne henseende en mere grundlæggende viden om og forståelse af eksempelvis forretningsmodeller. Epinion konstaterer imidlertid også, at der ikke nødvendigvis er en sammenhæng mellem oplevelse af kontrol og teknisk viden og kunnen.

Kendskab til tekniske sikkerhedsforanstaltninger blandt børn og unge er forholdsvis højt, men der er stor forskel på hvor mange, der faktisk anvender disse. Forskellene ses mellem piger og drenge, hvor sidstnævnte i højere grad benytter sådanne foranstaltninger. Endvidere er der også aldersforskelle, hvor den yngre del af målgruppen (12-14-årige) oplever at have større viden (Epinion, 2018, s. 59). Denne forskel kan dog i en vis udstrækning forklares med, at de lidt ældre i målgruppen er mere bevidste om omfang og kompleksitet og derfor oplever mindre kontrol og overblik på området.

Ift. at anvende (især teknisk) viden om diverse forholdsregler og sikkerhedsforanstaltninger, peger undersøgelsen også på, at der er en generel udfordring mht. især motivationen for at omsætte viden til handling. Der er også en stor gruppe af elever, som er uvidende på dette område, og her peger Epinion på, at mange børn og unge er 'ubevidst inkompetente' (Epinion, 2018, s. 66). Der er også en større del af børn og unge som er indifferente ift. sikkerhedsspørgsmål (ofte grundet afmagt), hvilket tyder på, at der skal arbejdes mere grundlæggende med et holdnings- og adfærdsskifte i målgruppen. På den positive side, ser undervisning i eksempelvis it-sikkerhed ud til at have en gavnlig effekt ift. at skabe mere hensigtsmæssig adfærd i målgruppen (Epinion, 2018, s. 64-65).

Hvad angår **sikker og kritisk brug af internettet**, kan der på denne baggrund peges på følgende kompetenceudviklingsbehov:

- Større viden, færdigheder og øgede handlekompetencer ift. virksomheders brug af data, herunder forretningsmodeller og søgemaskiner blandt alle målgrupper, inkl. lærere/undervisere og ledelser.
- Især pigerne har brug for mere teknisk viden, mens drengenes viden ofte er autodidakt og derfor nok med fordel kan udfordres.
- Der ser også ud til at være et behov for at fokusere på samfundsmæssige og globale sider af it-sikkerhedsspørgsmål (især ang. personlige oplysninger og passwords), idet mange børn og unge primært har fokus på egen adfærd og gerne bryder sikkerheden ift. kammarater og andre, som de har tillid til.
- Hvad angår regler og rettigheder er børn og unges viden og handlekompetencer varierende afhængig af køn og alder. Samlet ser det dog ud til, at børn og unge generelt har mere viden om, hvad de selv må, altså deres rettigheder, end de har med, hvordan de iflg. regler og lovgivning selv er beskyttede. Det peger på, at regler og rettigheder stadig bør være en del af kompetenceudvikling i målgruppen.

Ift. **dataetisk praksis**, peger Epinions undersøgelse på, at der er udfordringer både på organisationsniveau (ledere og lærere/undervisere) og i selve klasserummet (med elever/studerende). Dataetisk praksis (og for den sags skyld it-sikkerhed) opleves som komplekse områder i dagligdagen, og Epinion fremhæver behovet for at gøre op med usikre

vaner for derigennem at skabe en mere overordnet kulturændring på området. I denne henseende spiller it-administratorer og –vejledere også en stor rolle.

Arbejde med elev/-studerendes digitale data er for alvor begyndt at sætte sit præg på mange skoler og institutioner. Her peges der på, at især lærere/undervisere har gavn af efteruddannelse herom ift. at føle sig trygge og kompetente. Det øger også trygheden, hvis der findes ekspertise in-house (Epinion, 2018, s. 81). Der tales i Epinions undersøgelse om, at der foregår en 'dataevolution', som byder på en række dilemmaer for både ledelser, lærer/undervisere og it-fagligt personale, og hvor der mangler grundlæggende viden, ikke kun om tekniske sider, men også mere generelt inden for feltet Learning Analytics og Big Data – både teoretisk og i praksis.

Dataetisk praksis angår også brugen af eksempelvis sociale medier i undervisningen, og her viser undersøgelsen, at der er et dilemma mellem, hvad der kan give god mening at anvende i undervisnings- og læreprocesser og brugernes (elever/studerende) rettigheder ift. data-sikkerhed og privatliv (Epinion, 2018, s. 102). I denne sammenhæng efterlyses også et større fokus på de samfundsmæssige aspekter af dataetisk praksis (Epinion, 2018, s. 107).

Brugen af ikke-didaktiserede læremidler, som eksempelvis sociale medier, giver generelt anledning til en række dataetiske udfordringer i praksis, og det skal også bemærkes, at 63% af de adspurgte lærere/undervisere ikke fandt det problematisk eller vidste hvordan, de skulle forholde sig til udfordringer ifm. brugen af sociale medier i undervisning (Epinion, 2018, s. 111).

Hvad angår **dataetisk praksis**, kan der på denne baggrund peges på følgende kompetence-udviklingsbehov:

- Der tegner sig et billede af at skole/institutioner generelt set mangler viden og handle-kompetencer inden for feltet Learning Analytics og Big data, ikke mindst hvad angår dataetik. Dette behov kan identificeres på alle niveauer i organisationerne.
- Der synes også at være et stort behov for at øge lærere/underviseres viden og handle-kompetencer ift. de mere etiske sider af brugen af ikke-didaktiserede digitale teknologier, services mv.
- Ift. at øge viden og handlekompetencer, når det drejer sig om algoritmer, efterlyser lærerne/underviserne kvalificeret materiale og tid til at sætte sig ind i området. Her kan der også med fordel tænkes fagdidaktisk i udviklingen af materialer, da ikke alle lærere/undervisere ser emnet som noget, der naturligt kan integreres i deres undervisning.

Udvalgte resultater fra Digitaliseringsstyrelsen, DKCERT og DeIC (2017)

Kompetenceudviklingsbehovet angående cyber- og informationssikkerhed kan også i en vis udstrækning udledes af en undersøgelse foretaget af Digitaliseringsstyrelsen, DKCERT og DeIC.

Digitaliseringsstyrelsen, DKCERT og DeIC's rapport *Danskernes Informationssikkerhed 2016* afdækker 1) offentligt ansatte, 2) privatansatte og 3) borgeres oplevelser med og kendskab til

informations-sikkerhed, og som sådan kan resultater herfra være relevante for dele af ungdomsuddannelserne, FGU og VEU.

Rapporten viser bl.a. at:

- Alle tre befolkningsgrupper *har oplevet trusler* mod informationssikkerheden (eksempelvis computer vira, tab af data eller at uvedkommende har fået adgang)
- At især borgere *bruger samme password* til flere systemer, andelen er væsentligt lavere hos privatansatte
- At især borgere *anvender offentligt tilgængelige trådløse netværk* uden kryptering

Konsekvenserne af oplevede trusler har medført adfærdsændringer hos alle tre befolkningsgrupper, eksempelvis at undlade at åbne mails fra ukendte afsendere. Rapporten viser også, at alle benytter foranstaltninger i form af sikkerhedssoftware, dog igen lidt færre blandt borgerne end i de to andre grupper. Kun et fåtal falder for svindelforsøg, såsom phishing. Under halvdelen af både offentligt og privatansatte har adgang til single sign-on på deres arbejdsplads, og for alle tre befolkningsgrupper gælder at brugen af password-managers er begrænset. Sikkerheds-kopiering af data er også begrænset, særligt hos gruppen af borgere. Endvidere peges der i rapporten på, at kun halvdelen af medarbejdere har sat sig ind i reglerne om informationssikkerhed på deres arbejdsplads. Endelig bemærkes det, at:

> Seks procent af de offentligt ansatte og ni procent af de privatansatte undlader indimellem at overholde reglerne, fordi de opfattes som en hindring for at udføre arbejdet. (Digitaliseringsstyrelsen, DKCERT & DeIC, 2017, s. 7)

På baggrund af undersøgelsen anbefales det, at ledelsesniveauet igangsætter forskellige indsatser for øget informationssikkerhed og derigennem forsøger at opbygge en egentlig datasikkerhedskultur. Der peges konkret på indsatser mod netbaseret svindel, tab af data, uvedkommendes adgang til data, og der gives konkrete råd, som ledere kan bruge for at øge medarbejdernes informationssikkerhed. I rapporten gives også råd til borgergruppen, men det anerkendes, at borgere ikke nødvendigvis har fået uddannelse i området, og derfor ofte står alene med udfordringerne. Ud fra et kompetenceudviklingsperspektiv er undersøgelsen interessant, idet den bekræfter behov for mere viden og flere handlekompetencer blandt voksne, og endvidere peges der på konkrete udfordringer og emner, der kan genkendes i andre undersøgelser og som vi skal se også hos flere af de interviewede interessenter.

Udvalgte resultater fra /KL.7 (2017)

Kompetenceudviklingsbehovet angående cyber- og informationssikkerhed kan også i en vis udstrækning udledes af en undersøgelse foretaget af /KL.7 på opdrag for Digitaliserings-styrelsen og Erhvervsstyrelsen. /KL.7's rapport *For-analyse af Danskernes informationssikkerhed* afdækker danskernes it-sikkerhed som borgere og medarbejdere, og kan således også være relevant for dele af ungdomsuddannelserne, FGU og VEU. Det er dog i mindre grad selve kompetencebehovet, men derimod *tilgangen til kompetenceudvikling*, som vi har ladet os inspirere af. I denne rapport fokuseres der især på adfærdsmønstre mhp. at komme med konkrete anbefalinger til segmentspecifik budskabskommunikation. Særligt rapportens anbefalinger til kommende kampagneindsatser til forbedring af it-sikkerhed, har vi fundet relevante i denne sammenhæng. Overordnet anbefales det bl.a. at:

- budskaber gøres fysiske eller konkrete, da emnerne ellers kan være for abstrakte og svære at forholde sig til – derved vil forståelsen øges blandt børn unge og voksne
- budskaber skal gøres til anliggender, der vedrører alle, ikke kun udsatte grupper – det vil øge motivationen,
- budskaber bør formidles i konkret hverdagssprog og ekspertsprog bør undgås – det vil øge forståelsen og gøre ønsket adfærd mere overskuelig,
- budskaber bør sættes op i konkrete og handlingsanvisende råd. Hvis disse også giver mulighed for afkrydsning, vil det give en oplevelse af tryghed efter handlingerne.

En væsentlig pointe i rapporten er, at mennesker vil bruge deres *egen* viden og erfaringer til at forstå kommunikation om et givent budskab, i dette tilfælde it-sikkerhed (/KL.7, 2017, s. 23). Set i et kompetenceudviklingsperspektiv er dette væsentligt, da det indikerer, at undervisning, der jo grundlæggende *er* kommunikation, må tage udgangspunkt i målgruppens forudsætninger og erfaringer. Det kan med andre ord være hensigtsmæssigt, at baserede undervisning i og om cyber- og informationssikkerhed på principper om erfaringsinddragelse og dermed også at tilrettelægge undervisningen differentieret. Desuden er /KL.7 rapportens anbefalinger interessante ift. redidaktisering og udvikling af eksisterende og nye materialer.

DEL 3 - Tværgående analyse baseret på interessentinterview

I denne del af rapporten beskrives den tværgående analyse, der er foretaget på baggrund af interviews med interessenter, der alle arbejder med forskellige aspekter af cyber- og informationssikkerhed.

Hovedpointerne i denne del er:

- Den overordnede vurdering er, at selv om danskernes videns- og kompetenceniveau inden for cyber- og informationssikkerhed generelt vurderes som værende godt, også sammenlignet med andre lande, så er der stadig brug for kompetenceudvikling blandt både børn, unge og voksne.
- Der efterlyses, blandt interessenterne, et generelt holdnings- og adfærdsskifte i retning af at tage cyber- og informationssikkerhed langt mere alvorlig – også inden for uddannelsessystemet.
- Interessenterne peger på en række udfordringer, som bl.a. inkluderer, at børn, unge og voksnes viden ikke i tilstrækkelig grad omstættes til handlinger, at voksne mangler teknisk viden og endelig, at der er behov for organisationsdidaktisk udvikling og målrettede strategier på skoler og i uddannelsesinstitutioner.
- Interessenterne peger på særlige udfordringer, der kan skyldes forskelle mellem køn, aldersgrupper og generationer.
- Helt konkret ser interessenterne store udfordringer mht. anvendelse af især sociale medier i undervisning, og der efterlyses bedre rammesætning og nytænkning af undervisning inden for området.
- Interessenterne peger på, at der mangler viden og materialer, der retter sig specifikt mod EUD, FGU og VEU, der vurderes som værende overset områder.
- Interessenterne taler også for at cyber- og informationssikkerhed gøres til et anliggende for alle, og at der i denne sammenhæng med fordel kan bringes flere aktører på banen, således at området kommer til at omfatte mere end skole- og uddannelsessfæren.
- Endelig peger interessenterne på specifikke kompetenceudviklingsbehov, særlig også blandt lærere/undervisere, og der gives konkrete eksempler på faglige emner, der med fordel kan styrkes i undervisning om og med cyber- og informationssikkerhed.

Interview med interessenter

Vi har foretaget 16 kvalitative interviews med interessenter, der alle arbejder med forskellige aspekter af cyber- og informationssikkerhed. Interessenterne er udvalgt i samarbejde med STIL, og målet har været dels at dække vidensområdet om cyber- og informationssikkerhed så bredt som muligt og dels at dække de forskellige målgrupper og uddannelsesområder, som projektet retter sig imod.

Vi har interviewet repræsentanter fra følgende organisationer, virksomheder, styrelser mv.:

- Center for Digital Dannelse
- Center for Digital Pædagogik
- Dataethics Consulting
- Danmarks it-vejlederforening
- Dansk Center for Undervisningsmiljø
- Det Kriminalpræventive Råd
- Digitaliseringsstyrelsen
- DRskole
- Forbrugerrådet Tænk
- Medierådet for Børn og Unge
- Nationalt Center for Forebyggelse af Ekstremisme
- Nationalt Cyber Crime Center
- Nationalt Forebyggelsescenter
- Nets Danmark
- RedBarnet
- Sex & Samfund

Kort om interviewdelen

Interviewene blev gennemført i august-september 2018 og foregik for de flestes vedkommende ansigt-til-ansigt. Formålet med disse interviews var at få et overblik over, hvilke kompetenceudviklingsbehov interessenterne kunne pege på inden for deres respektive fagområder og målgrupper. Vi bad i den forbindelse også interessenterne om at pege på materialer, som de finder anvendelige (enten selvproducerede og/eller produceret af eller i samarbejde med andre), og disse materialer er løbende blevet taget med i vores materialeoversigt og sidenhen blevet vurderet. Endvidere bad vi interessenterne om at pege på eventuelle mangler ift. eksisterende materialer, hvilket også indgår som en del af vores samlede anbefalinger.

Interviewguiden bestod af ni overordnede spørgsmål og blev anvendt på en semistruktureret måde, således at interessenternes forskellige baggrunde, erfaringer og ekspertiser var med til at forme interviewene. Vi bad interessenterne om at udtale sig som repræsentanter for deres respektive organisationer og lovede dem i øvrigt personlig anonymitet.

Der var forskel på, i hvilket omfang interessenterne har kunne svare på de forskellige spørgsmål. Eksempelvis har de færreste interessenter haft en holdning til hvilke fag på de forskellige uddannelsesområder, der kunne være relevante for undervisning i cyber- og informationssikkerhed.

Overordnede resultater

I det følgende opsummeres de pointer, som interessenterne bredt set har peget på.

Danskernes videns- og kompetenceniveau er generelt godt, men kunne være bedre

Der er blandt alle interessenter en klar oplevelse af, at feltet omkring cyber- og informationssikkerhed er i rivende udvikling, ikke mindst pga. digitaliseringens allestedsnærværende og hastige udvikling. Derfor vurderer alle interessenter, at området vil få større og større indflydelse på samfundslivet bredt set, hvilket igen peger mod et kompetencebehov i befolkningen, som må siges at være dynamisk. På tværs af interessenternes målgrupper ses det som et fælles mål at sikre danskernes trygge oplevelse af og hensigtsmæssige adfærd på især internettet.

Der er blandt interessenterne en anerkendelse af, at danskernes videns- og kompetenceniveau inden for området generelt er godt, når der sammenlignes med andre lande. Dette vurderes positivt, men der peges samtidig på, at der kan være en diskrepans mellem borgernes egne oplevelser af tilstrækkelige kompetencer og det kompetenceniveau, der reelt er behov for. Enkelte interessenter peger således på en form for falsk tryghed, der skyldes borgernes 'ubevidste inkompetence' (jf. også Epinion, 2018). Et eksempel herpå kunne være borgernes manglende forståelse af store it-virksomheders forretningsmodeller, der efter flere interessenters vurdering resulterer i uhensigtsmæssig adfærd (eksempelvis accept af terms-of-service uden læsning og kritisk stillingtagen). På et helt overordnet og generelt niveau er interessenternes vurdering altså, at der stadig er behov for kompetenceudvikling, og at især konsekvenser af uhensigtsmæssig dataadfærd endnu ikke opfattes helt så seriøst, som det burde. Der er i høj grad tale om et ønskeligt holdnings- og adfærdsskifte generelt i befolkningen, ud fra interessenternes vurdering at dømme.

Børn og unges viden og kompetencer skal omsættes til handling

Blandt interessenterne ses børn, unge (og ældre) som særligt sårbare målgrupper, hvor det er nødvendigt at sætte ind med mere viden og kompetenceudvikling. Enkelte interessenter nævner også mennesker med kognitive handicaps som værende en særligt udsat målgruppe, der også bør fokuseres på, ikke mindst af inklusionshensyn. Flertallet af interessenterne fremhæver også demokratisk deltagelse i det stadig mere digitaliserede og globaliserede samfund som et væsentligt pejlemærke i deres arbejde med cyber- og informationssikkerhed.

Ift. børn og unge peger flere interessenter på, at vidensniveauet generelt er udmærket, men at der ofte er forskel på viden og handling. Det nævnes også i denne sammenhæng, at børn og unge ofte har brugsviden, men mangler forståelse for de bagvedliggende, især tekniske mekanismer. Det anbefales derfor, at fremadrettet kompetenceudvikling fokuserer på at understøtte børn og unges konkrete handlingsstrategier, og det understreges, at for at komme dertil, skal der ikke kun arbejdes med at øge vidensniveauet, men også med at bearbejde børn og unges grundlæggende opfattelser af området. Flere interessenter, der arbejder med børn og unge, italesætter en manglende forståelse og anerkendelse af præcis hvor vigtigt det er at beskytte børn og unge, når de færdes online. Det er indtrykket blandt disse interessenter, at der mangler forståelse og anerkendelse heraf både blandt børn og unge selv, men også blandt

de voksne (lærere/undervisere, pædagoger, forældre og skoleledelser), der har ansvar og indflydelse på området.

Voksne mangler – især teknisk - viden og kompetencer ift. at tage ansvaret på sig
I forhold til voksne, har interessenterne primært haft fokus på de voksne, der er ansvarlige for uddannelse og kompetenceudvikling, særligt lærere/undervisere, men også forældre og deres roller og ansvar har været nævnt af enkelte interessenter. Blandt de interessenter som har erfaring med skole- og uddannelsesområdet fremhæves et stort kompetenceudviklingsbehov, idet det er vurderingen, at mange lærere/undervisere ikke har tilstrækkelig, især teknisk, viden og tilhørende kompetencer. Hvad angår de mere interaktionelle, kommunikative og adfærdsmæssige sider, vurderes lærere/undervisere til at have gode generelle kompetencer. Det efterlyses dog blandt flere interessenter, at lærerne, underviserne og andet pædagogisk personale i højere grad agerer gode rollemodeller og tænker cyber- og informationssikkerhed ind som et naturligt aspekt af undervisning og andre pædagogiske aktiviteter, når der eksempelvis arbejdes med digitale medier eller internettet.

Behov for organisationsdidaktisk udvikling og målrettede strategier
Blandt flere interessenter, er der en oplevelse af, at kompetencer inden for området ofte er ujævnt fordelt i forskellige lærerkollegier/organiseringer. Den ujævne fordeling af kompetencer gør det også vanskeligt for mange af interessenterne at komme med direkte anbefalinger til i hvilke fag fokus på cyber- og informationssikkerhed bedst kan indgå. Et er hvad, der fagligt ville give mening, noget andet er hvad, der, igen med henvisning til lærernes/undervisernes kompetencer, kan lade sig gøre i praksis. Flere interessenter peger også på, at der ligger en stor organisationsdidaktisk udviklingsopgave ift. området, som også bør omfatte ledere. Hertil kommer bestyrelser og i sidste ende kommunerne, hvor der efterlyses klare strategier og handlingsplaner på området.

EUD, FGU og VEU er oversete målgrupper
Kun et fåtal af interessenterne har haft øje for EUD som målgruppe for deres aktiviteter. Adspurgt herom, forklares dette fravalg som et prioriteringsspørgsmål, og det bemærkes, at EUD er et komplekst uddannelsesområde. Her henvises bl.a. til de 100+ uddannelser, der retter sig mod specifikke erhverv, og som derfor kan tænkes at have helt specifikke behov og tilgange til cyber- og informationssikkerhed. Fokus på området kræver også indsigt i erhvervspædagogik, hvor de fleste interessenter er vant til at arbejde inden for det almene-, gymnasie- eller voksenpædagogiske område.

Flere interessenter har udviklet materialer og igangsat initiativer rettet mod voksne og især ældre (50+), men unge voksne på FGU[1] og voksne på VEU har ikke været i særligt fokus blandt interessenterne. En enkelt interessent nævnte dog den store gruppe af ufaglærte, som mangler grundlæggende it-kompetencer (se eksempelvis EVA, 2017), hvortil viden om cyber- og informationssikkerhed ses som et væsentligt opmærksomhedspunkt, idet manglende viden og kompetencer øger sårbarheden for både individet og virksomheden.

[1] FGU er jo også en ny uddannelseskonstruktion, men adspurgt til eksempelvis produktionsskoleelver som målgruppe for materialer og indsatser, er det ikke en målgruppe som har været i fokus.

Generelt behov for nytænkning af undervisning i cyber- og informationssikkerhed
På baggrund af interviewene tegner der sig et billede af, at manglende viden om området ikke er den største udfordring (dog med visse væsentlige undtagelser, som beskrives neden for), men derimod det at kunne omsætte denne viden til reelle handlekompetencer. I denne forbindelse peger flere interessenter på, at der er behov for at frame eller rammesætte området på nye måder, der vil kunne øge børn, unge og voksnes grundlæggende interesse for og forståelser og anderkendelser af, hvorfor og hvordan det er nødvendigt at beskæftige sig med området.

Det foreslås derfor, at undervisning i, om og med fokus på cyber- og informationssikkerhed gøres (personligt) relevant, målgruppespecifik, erfaringsbaseret og handlingsorienteret. Flere interessenter fremhæver også muligheden for at inddrage målgrupperne i selve udviklingen af nye materialer for netop at øge interesse, motivation og relevans.

Udfordringer med anvendelse af sociale medier i undervisning
Der er blandt mange af interessenterne en bekymring over den stigende anvendelse af sociale medier i undervisning. Der udtrykkes ikke ønsker om forbud, men derimod mere kritisk, reflekteret anvendelse. Mange interessenter erkender vanskeligheden i at gennemskue, hvad eksempelvis store it-virksomheder som Google og Facebook indsamler og anvender af data, men det problematiseres, at nogle lærere/undervisere og ledelser tilsyneladende ikke tager deres ansvar alvorligt i denne sammenhæng. Det bemærkes også, at netop anvendelse af sociale medier med fordel kunne benyttes som anledning til at fokusere på forskellige relevante emner inden for cyber- og informationssikkerhed.

Fokus på køns-, alders- og generationsforskelle
Flere interessenter beskriver nogle af de konkrete udfordringer, der kan være i cyber- og informationssikkerhedsarbejdet, som skyldes forskelle i køn, alder og mellem generationer. Flere undersøgelser (bl.a. Epinion, 2018) bekræfter, at der er forskel på piger og drenges viden og kompetencer. Her peger flere interessenter på behovet for at fastholde målrettede initiativer (som eksempelvis DigiPipi[2] og Coding Pirates[3]), men også at sådanne med fordel kan tænkes endnu mere ind i de formelle skole- og uddannelsessammenhænge og dermed også beskæftige sig med målrettede aspekter af cyber- og informationssikkerhed.

Interessenterne fremhæver også de aldersforskelle, der kan være og vigtigheden af at tilrettelægge undervisning inden for cyber- og informationssikkerhed, som tager højde for deltagerforudsætninger og baseres på en passende pædagogik (eksempelvis gymnasie-, erhvervs- eller voksenpædagogik) ift. målgruppen.

Der tales blandt interessenterne også om den udfordring, der kan være i, at voksen-generationen ikke nødvendigvis forstår og anerkender børn og unges medie- og internetbrug. Der efterlyses muligheder for, at flere materialer kan være med til at 'bygge bro' mellem forskellige opfattelser, erfaringer og generationer.

[2] DigiPipi: https://digipippi.dk/2.0/
[3] Coding Pirates: https://codingpirates.dk/

Flere aktører på banen
Der er blandt interessenterne en forståelse af at cyber- og informationssikkerhed er nødt til at være en sag, der angår alle og i alle livets facetter. Det betyder også, at der fra flere sider peges på, at andre aktører end lige skoler og uddannelsesinstitutioner må på banen. Forældre er allerede nævnt, men interessenterne peger også på SSP-samarbejde, bibliotekarer og evt. aktører fra kultur- og fritidslivet, der med fordel kan tænkes ind i arbejdet med at øge især børn og unges videns- og kompetenceniveau. Enkelte interessenter nævner også, at nogle skoler har haft held med at udpege 'ambassadører' blandt elever, der så får ansvar for at udbrede viden om eksempelvis god adfærd på nettet.

Flere af interessenterne peger i denne forbindelse på, at de ofte bliver kontaktet med henblik på at komme ud på skoler og uddannelsesinstitutioner som eksperter inden for området. Dette betragtes som værende positivt, da der kan være pædagogiske fordele i at få folk udefra til at vække interesse og motivation. Det ses også som en legitim erkendelse af, at lærere/undervisere og ledere ikke nødvendigvis kan eller skal følge med i især den teknologiske udvikling eller kan forventes at have deciderende specialistkompetencer (eksempelvis inden for det tekniske eller juridiske område).

Specifikke faglige kompetenceudviklingsbehov
Den mere tekniske side af cyber- og informationssikkerhed vurderes blandt flertallet af interessenter som værende meget abstrakt og vanskelig tilgængelig. Af denne årsag foreslås det, at undervisning heri formidles gennem hverdagssprog og -begreber, og at disse finder deres udgangspunkt i målgruppernes 'levede liv', dvs. deres hverdagserfaringer, hvad enten disse foregår i privatsfæren eller i de mere institutionaliserede skole- og uddannelsessammenhænge.

Der peges også på de mere interaktionelle og kommunikative sider af cyber- og informations-sikkerhed, hvor især etiske overvejelser og hensigtsmæssig, 'god' adfærd vurderes som værende områder, der med fordel kan styrkes gennem undervisning og kompetenceudvikling. Her nævner flere interessenter det paradoks, at mange – især unge - har viden om, hvordan man bør (også ift. regler og lovgivning) gebærde sig, men at de ofte alligevel handler mod bedrevidende. Endvidere nævner flere interessenter, at børn og unge ofte opfatter regler og lovgivning i et meget personligt perspektiv, dvs. de er gode til at tage ansvar for egne handlinger og adfærd, mens det ofte kniber med at se tingene i et interaktionelt (fælles) og ikke mindst samfundsmæssigt og globalt perspektiv.

Blandt de interessenter der har ekspertise ift. børn og unge, peges der på radikalisering og ekstremisme som områder af cyber- og informationssikkerhed, der bør have større fokus fremover. Her henviser interessenterne også til lignende tendenser på europæisk og globalt plan. I den forbindelse nævnes også grooming, der nok har haft en vis opmærksomhed ift. seksuelle krænkelser (børneporno mv.), men hvor der ses en tendens til, at sådanne it-kriminelle nu også retter blikket mod en mere økonomisk side af sagen i form af pengeafpresning. Der er således stadig behov for viden og udvikling af kompetencer, hvad angår de mere menneskelige sider af datasikkerhed og tekniske foranstaltninger, der kan afhjælpe sådanne risici.

Om end det generelle videns- og kompetenceniveau, som allerede nævnt, vurderes som værende relativt højt, ser alle interessenter et fortsat behov for at styrke børn, unge og voksnes kritiske sans, stillingtagen og ikke mindst handlinger ifm. færden på især internettet. Der efterlyses i denne forbindelse en lagt bedre forståelse af forskellige risici og konsekvenser af egen og andres adfærd.

Emner inden for cyber- og informationssikkerhed, der med fordel kan styrkes
Opsummeret peger interessenterne på følgende forskellige faglige emner, der med fordel kan styrkes i undervisning og kompetenceudviklingsøjemed:

- **Tekniske sikkerhedsforanstaltninger** – herunder viden om opklaring[4], når skaden er sket og ikke kun forebyggelse
- **Forretningsmodeller** – herunder algoritmisk viden og viden om rettigheder (GDPR)
- **Etik** – herunder det fælles samfundsmæssige (og globale) ansvar
- **Radikalisering og ekstremisme** – herunder viden om 'ekkokamre' og at dette ikke kun handler om terror og religiøs rekruttering
- **Grooming** – ikke kun ift. seksuelle krænkelser, men også ift. økonomisk kriminalitet (afpresning)
- **Kritisk stillingtagen** – refleksion omsat til handlestrategier både for individet og fællesskabet

I forhold til ovennævnte, er det en selvstændig og væsentlig pointe, at viden herom ikke er tilstrækkelig. Derimod skal der opnås reelle handlekompetencer inden for alle emner.
Et specifikt emne, som vi ikke har taget videre i vores materialeanalyse, er Internet-of-Things (IoT), der nævnes af enkelte interessenter. Emnet kan omfatte alt fra kunstig intelligens, algoritmer, logning og dataindsamling og kan som sådan inkluderes i andre delemner. Pointen fra interessenterne gik dog i lige så høj grad på udvikling af en grundlæggende forståelse af netværkssammenhænge og ikke mindst såkaldte 'smarte teknologier'. Armbåndsure med indbygget motionsmonitorering nævnes som et aktuelt opmærksomhedspunkt, idet der hermed ikke kun fokuseres på kommunikative og adfærdsmæssige data, men som noget nyt også på individets fysiske/helbredsmæssige data. Her ses igen et underliggende ønske om at koble viden og kompetenceudvikling til målgruppernes hverdagsliv, og de valg og forholdsregler, der skal tages i forbindelse med anvendelse af digitale teknologier, services mv.

Hvad angår det organisatoriske niveau på skoler og uddannelsesinstitutioner, har vi heller ikke medtaget Learning Analytics og Big Data, der ellers præger mange skole- og uddannelses-debatter i øjeblikket, og som nævnes af et par af interessenterne. Sådanne temaer kunne tages med, men det er vores vurdering, at disse emner med fordel kan tåle at blive behandlet selvstændigt og ikke blot som delemner inden for cyber- og informationssikkerhed. Brugen af ikke-didaktiserede materialer, som eksempelvis sociale medier, i undervisningen kan dog med fordel inkluderes.

Det er vigtigt at være opmærksom på, at selv om ovennævnte emner fremhæves, vurderer interessenterne samtidig, at der stadig er behov for fokus på andre emner (eksempelvis digitale

[4] Her inspireret af det engelske begreb *cyber forencis,* der er stærkt i fokus i amerikansk undervisning om cyber- og informations-sikkerhed (Newhouse, Keith, Scibner & Witte, 2017). I denne forbindelse er færdigheder i teknisk undersøgelse, analyse og vurdering essentielle.

fodspor, regler og adfærd for billeddeling og generel kildekritik), der tidligere har været rimelig godt dækket. Megen af den viden, der skabes og skal formidles inden for området er dynamisk, og derfor er kompetencebehovet ikke blot et spørgsmål om 'at komme i mål', men snarere om 'at have fokus og være i konstant udvikling'.

Del 4 – Sammenfatning

I denne del sammenfatter vi de vigtigste pointer fra undersøgelsen ift. kompetenceudviklings- og materialeudviklingsbehov, som dette er kommet frem gennem læsning af udvalgte undersøgelser på området og interview med udvalgte interessenter. På denne baggrund gives en række anbefalinger.

Medier og digitale teknologier i uddannelsessystemet set fra et cyber- og informationssikkerhedsmæssigt perspektiv

Overordnet set, er det en hovedpointe i vores interessentundersøgelse, at børn, unge og voksne er gået fra at lære *om* medier og digitale teknologier, herunder de cyber- og informations-sikkerhedsmæssige problemstillinger, til også at lære *med* medier og digitale teknologier. Målgrupperne lærer nu også ved at anvende disse teknologier. I kraft af undersøgelsen er det imidlertid blevet tydeligt, at der er behov for begge tilgange i undervisnings- og læreprocesser. Viden om og forståelse af de grundlæggende udfordringer forbundet med cyber- og informationssikkerhed kræver også undervisning i konkrete digitale teknologier.

Undervisning og læring i cyber- og informationssikkerhed bør ifølge interessenterne kobles til målgruppernes hverdag og sociale omgang med hinanden i - og uden for skolen/ uddannelsesinstitutionen.

Øget grundlæggende forståelse, teknisk forståelse og handlekompetencer

Det påpeges af interessenterne, i baggrundsrapporterne og vores egen analyse af eksisterende materialer viser, at der kan være behov for et fokus i undervisningen og ved udvikling af materialer, som understøtter at lærere/undervisere, børn, unge og voksne får større grundlæggende teknisk forståelse for de medier og digitale systemer, de anvender. Dette er nødvendigt for at målgrupperne kan gennemskue de muligheder, faldgruber og sikkerhedsmæssige problemstillinger, som knytter sig til den daglige brug.

Det anbefales:

- *At formidling af materialetyperne til undervisningen fokuserer på, at børn og unge får grundlæggende teknisk forståelse for de medier og digitale teknologier, de anvender.*
- *At materialetyperne peger i retning af, at målgrupperne får mulighed for at fokusere på handlekompetencer.*

Kompetenceudvikling i uddannelsessystemet kræver, at materialet skal være praksisnært og anvendeligt for lærere/undervisere, samt personligt relevant for eleverne/deltagerne

Flere interessenter har påpeget, at en afgørende faktor for, at både børn, unge og voksne bedst kan lære om og med medier og digitale teknologier er, at undervisningen og det dertil hørende materiale er praksisnært og anvendeligt, samt at både undervisning og materialer gøres personligt relevante.

Samlet set peges der på vigtigheden af, at undervisningen og formidling omkring medier, digitale teknologier, samt cyber- og informationssikkerhed skal knytte an til målgruppernes hverdagsliv, daglige brug og hverdagssprog.

Det anbefales:

- *At materialet til undervisningen med fokus på cyber- og informationssikkerhed gøres relevant, målspecifik, erfaringsbaseret og handlingsorienteret.*

Kompetenceudviklingsbehovet af (unge) voksne på FGU, EUD og VEU

Generelt viser interessentundersøgelsen samt øvrige rapporter og undersøgelser, at der eksisterer et betydeligt kompetenceudviklingsbehov på EUD, FGU- og VEU-området. Samtidig har vores materialeanalyse vist, at mange af de eksisterende materialer kan bruges inden for disse uddannelsesområder. Det vil dog være forbundet med en omfattende redidaktisering målrettet disse uddannelsesområder. Overordnet set udvikles der meget få undervisningsmaterialer til disse områder bl.a. pga. kompleksitet og prioritering blandt materiale-producenterne.

Det anbefales:

- *At kompetence- og materialeudvikling til FGU, EUD og VEU prioriteres højere end tilfældet har været hidtil.*

Materiale- og kompetenceudvikling med fokus på brobygning mellem ungdomskultur og voksenkultur

Bland interessenter og praktikere er der enighed om, at lærere/undervisere som voksengeneration ofte har et væsentligt anderledes medie- og digitalt forbrug, end de børn og unge, som de underviser. Reelt set vurderes det, at voksengenerationen ikke nødvendigvis forstår og anerkender børn og unges brug af medier og digitale teknologier.

Det anbefales:

- *At materiale- og kompetenceudvikling kan bidrage til at bygge bro mellem børn- og voksengenerationens kultur på området.*
- *At materialetyper og kompetenceudvikling bidrager til en videndelende og samskabende tilgang til området cyber- og informationssikkerhed.*

Ekspertviden kan være nødvendig at inddrage i undervisningsmiljøet

Undersøgelserne peger på, at en del faglig viden om cyber- og informationssikkerhed kan være så specialiseret viden, at det kan være nødvendigt og relevant at inviterer eksperter ind i undervisningsmiljøerne, samt ved udvikling og formidling af materialer som baggrundsstof. Eksempelvis nævnes at uddannelsesforløb som 'Hacker for en dag' vil kræve denne specialviden.

Det anbefales:

- *At der fra skoleledelsers og –bestyrelsers side er opmærksomhed på at anerkende ovenstående udgangspunkt og fortsat inddrage eksperter i forhold til det aktuelle vidensbehov og den aktuelle situation.*

Kompetenceudvikling er mere end et mellemværende mellem lærere/undervisere og elever/deltagere.

Af denne undersøgelse fremgår det, at udvikling af kompetencer inden for cyber- og informationssikkerhed ikke blot kan være et anliggende mellem lærere/undervisere og elever/deltagere. Det kræver organisationsdidaktisk udvikling, målrettede strategier og inddragelse af andre aktører, hvilket bør medtænkes i udvikling af nye materialer og forløb.

Det anbefales:

- *At aktører så som skolebestyrelser, skoleledere, forældre og kommuner medtænkes.*
- *At skoler og uddannelsesinstitutioner også arbejder med en mere generel kulturændring, som kræver et organisationsdidaktisk fokus og målrettede strategier.*

Udvikling af holdninger og adfærd – at gøre ansvarlige voksne i stand til at tage ansvaret på sig.

Interessenternes udsagn, sammenholdt med tidligere undersøgelser inden for feltet, kan sammafattende siges at pege på behovet for et holdnings- og adfærdsskift mht. uhensigtsmæssig dataadfærd hos både børn, unge og voksne.

Flere interessenter påpeger vigtigheden af, at voksne (både lærere/undervisere, pædagogiske personale, ledere og forældre) skal være i stand til at tage ansvaret på sig. De skal opnå viden og handlekompetencer, så de reelt kan hjælpe med at gøre børn og unge i stand til at beskytte sig selv og andre, når de beskæftiger sig med medier og digitale teknologier.

Det anbefales:

- *At kompetence- og materialeudvikling inden for cyber- og informationssikkerhed også fokuserer på de voksne, der formodes at skulle kunne tage ansvar for arbejdet med medier og digitale teknologier.*

Referencer

Danmarks Evalueringsinstitut, EVA (2017). *It-færdigheder på et digitaliseret arbejdsmarked*. https://www.eva.dk/voksen-efteruddannelse/it-faerdigheder-paa-digitaliseret-arbejdsmarked [Lokaliseret 06.08.2018]

Digitaliseringsstyrelsen, DKCERT & DeIC (2017). *Danskernes informationssikkerhed 2016*. https://digst.dk/media/13800/danskernes-informationssikkerhed-2016.pdf [Lokaliseret 25.08.2018]

Epinion (2018). *Styrkelse af dataetik og it-sikkerhed på undervisningsområdet*. På opdrag fra Undervisningsministeriet. https://uvm.dk/publikationer/2018/180822-styrkelse-af-dataetik-og-it-sikkerhed-paa-undervisningsomraadet [Lokaliseret 05.09.2018]

Finansministeriet (2018). *National Strategi for cyber- og informationssikkerhed 2018-2021*. På opdrag fra Regeringen. https://digst.dk/strategier/cyber-og-informationssikkerhed/ [Lokaliseret 06.08.2018]

/KL.7 (2017). *Foranalyse af Danskernes informationssikkerhed*. På opdrag fra Digitaliserings-styrelsen og Erhvervsstyrelsen. https://digst.dk/media/13804/foranalyse-af-danskernes-informationssikkerhed.pdf [Lokaliseret 14.09.2018]

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*. NIST.