Juni 2025

MELLEM PIZZA OG POLITIK:

Eksplorativ Undersøgelse af IT-sikkerhed i Små- og Mellemstore Virksomheder samt Viden og Praksisser fra Formelle Uddannelser og Uformelle Samlinger.

Vejleder: Christian Ravn Haslam

Asbjørn Kjærgaard Andersen
Aske Brask Christensen
Freja Vigen Larsen
Laura Nicolaas

IT-Ledelse
Aalborg universitet

10. semester

Titelblad

Projekttitel:

Mellem Pizza og Politik: Eksplorativ Undersøgelse af IT-sikkerhed i Små- og Mellemstore Virksomheder samt Viden og Praksisser fra Formelle Uddannelser og Uformelle Samlinger

Projekt: Specialeafhandling, 10. semester, Cand. it. i IT-ledelse på Aalborg Universitet

Gruppemedlemmer:

Asbjørn Kjærgaard Andersen
Studienummer: 20203545

Aske Brask Christensen
Studienummer: 20184327

Freja Vigen Larsen
Studienummer: 20202934

Laura Nicolaas
Studienummer: 20231630

Vejleder: Christian Ravn Haslam

Antal anslag: 191774

Antal sider: 79,9

Antal bilag: 25

Afleveringsdato: 28. Maj, 2025

Abstract

This exploratory study investigates how informal and formal learning environments contribute to cybersecurity competence development in Danish small and medium-sized enterprises (SMEs). The study draws on qualitative data, including 21 semi-structured interviews. The investigation identifies several barriers that hinder SMEs from developing sufficient cyber resilience. These range from structural limitations such as resource scarcity and recruitment challenges, to cultural and organizational factors including low awareness levels and fragmented practices. However, the study also uncovers underutilized opportunities embedded in informal learning communities, where tacit knowledge and practical experience play a significant role. Multiple key opportunity areas are identified: the formation of industry-specific learning communities, the prioritization of intentional and practice-oriented security training, improved role clarification in collaborations with IT providers, and the inclusion of non-traditional profiles through hands-on, context-based upskilling. Additionally, the need for a coordinated national support function tailored to SMEs is emphasized. Findings suggest that cybersecurity learning is not only a technical challenge but also a social and organizational one. The study argues that bridging informal and formal learning spaces may offer a more sustainable and context-sensitive approach to capability building.

Forord

Specialegruppen vil gerne udstede en stor tak til vores vejleder Christian Ravn Haslam, og de informanter der har delt ud af deres viden. Der skal ligeledes rettes en særlig tak til de personer, som har assisteret med at identificere relevante informanter og etablere kontakt til potentielle respondenter. Deres bidrag har haft afgørende betydning for projektets datagrundlag.

Indholdsfortegnelse

1. Indledning

1.1 Problemfelt

I takt med udviklingen af digitalisering af samfund og kritisk infrastruktur er der også fulgt forskellige negative konsekvenser med. En af disse er IT-kriminalitet, som Det Kriminalpræventive Råd opdeler i tre kategorier: 1) Computer-integritetsforbrydelser (CIF), 2) computer-assisterede forbrydelser og 3) computer-indholdsforbrydelser (Det Kriminalpræventive Råd, 2025). I dette speciale tages der udgangspunkt i den første kategori, computer-integritetsforbrydelser, som har til formål at skade en persons eller en virksomheds IT-system. Interessen for CIF opstår på baggrund af den stigende tendens, der har været inden for denne type kriminalitet det seneste årti. Ifølge IT-virksomheden AAG var der i 2022 over 236.1 millioner ransomware-angreb på verdensplan (Griffiths, 2025). Endvidere beskriver Arctic Wolf, en Software-as-a-Service-leverandør, IT-kriminalitet som en 1.5 milliard dollar-industri. Disse tal understreger, at der er en betydelig økonomisk gevinst ved at udføre IT-kriminalitet, og massive mængder af angreb finder sted dagligt. Prisen for, at en virksomhed bliver ramt af et cyberangreb, kan variere afhængigt af, hvilke kilder man anvender. Ifølge en rapport fra IBM (IBM, 2024) kostede et gennemsnitligt angreb i 2024 en virksomhed 4.88 millioner US dollars (USD), mens Arctic Wolf har en mere nuanceret graf over de økonomiske konsekvenser af et angreb, hvor det, afhængigt af hvilken sektor der bliver angrebet, er median løsesummen på ransomwareangreb 600K. USD (Arctic Wolf, 2025, s. 11).

1.1.1 Danmark vinkel

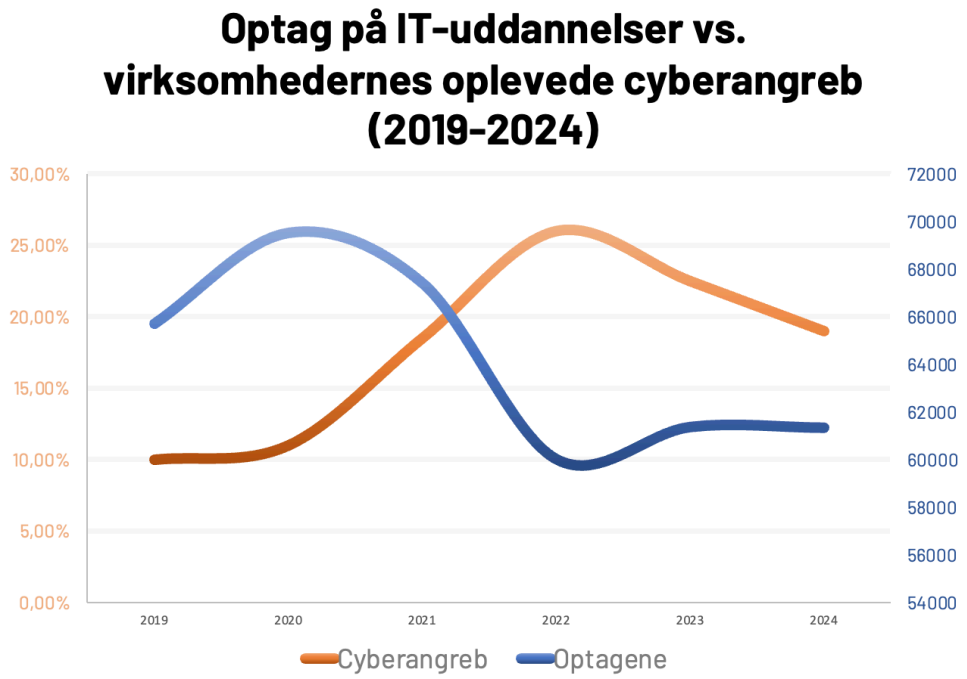
Ifølge EU-kommissionens undersøgelse af den digitale økonomi i 2022, er Danmark en digital frontløber både i Europa og på globalt plan (Europa-Kommissionen, 2022). I takt med dette oplever Danmark en stor IT-sikkerhedstrussel. Ifølge Forsvarets Efterretningstjenestes (FE) rapport, *Udsyn*, hvor trusselsniveauet inddeles i kategorierne: 1) Ingen, 2) lav, 3) middel, 4) høj og 5) meget høj, har truslen fra IT-kriminalitet mod Danmark været vurderet som *meget høj* siden 2022 (Forsvarets Efterretningstjeneste, 2024). Især små og mellemstore virksomheder (SMV'er) er udsatte. SMV'er udgør en betydelig del af den danske økonomi,

og ifølge SMV Danmark var der i 2022 cirka 300.000 SMV'er, som tilsammen beskæftigede 1.031.950 personer (SMVdanmark, u.å.). SMV'er varierer i størrelse, fra små virksomheder med få ansatte, til større organisationer med op mod 250 ansatte og er tit attraktive mål for IT-kriminalitet, da mange af disse virksomheder ikke har tilstrækkelige ressourcer eller ekspertise til at sikre deres IT-infrastruktur effektivt. SMV Danmark fremhæver, at alle virksomheder er potentielle ofre for IT-kriminalitet, men at SMV'er er særligt sårbare, da de ofte prioriterer forretningsudvikling frem for investeringer i IT-sikkerhed. Denne manglende prioritering efterlader mange SMV'er sårbare over for cyberangreb, der kan have alvorlige økonomiske og operationelle konsekvenser (SMVdanmark, u.å.). I en undersøgelse af 30 danske SMV'er (Kocksch & Jensen, 2024) blev der udledt, at SMV'er håndterer IT-sikkerhed forskelligt, ofte med en pragmatisk og improviseret tilgang frem for en systematisk og strategisk sikkerhedsmodel. Mange virksomheder opererer med et minimum af IT-sikkerhedsforanstaltninger og anvender løsninger, der er "gode nok" snarere end optimale. Denne tilgang kan ifølge Kocksch & Jensen skyldes økonomiske hensyn, teknologisk gæld og en lav risikobevidsthed blandt virksomhedsledere. De fandt også, at det ofte er en generalist, såsom en medarbejder i IT-afdelingen eller direktøren selv, der varetager IT-sikkerheden, hvilket kan føre til fragmenterede og utilstrækkelige sikkerhedsstrategier. Denne problematik kan sidestilles med, at 58 % af danske virksomheder angiver at de har ledige stillinger, der er vanskelige at besætte grundet mangel på færdigheder inden for informations- og kommunikationsteknologi (EU-komissionen, 2022, s. 3). Danmark fremlagde derfor 2022 sin nationale digitale strategi, som inkluderer fire initiativer vedrørende digitale færdigheder og uddannelse, blandt andet med fokus på øgede digitale kompetencer af lærerne på grundskoler samt færdighederne på videregående uddannelser.

1.1.2 Stagnering i uddannende specialister

Nedenstående graf viser udviklingen i diskrepansen mellem andelen af virksomheder, der har oplevet brud på IT-sikkerheden, og antallet af optagne på IT-baserede uddannelser. Dataen på mængden af virksomheders angreb er hentet fra Danmarks Statistiks (DST) årlige undersøgelse: *IT-anvendelse i virksomheder*. Data er særligt hentet fra spørgsmål to i spørgeskemaet: *"2. Havde brud på IT-sikkerheden?"* (Danmarks Statistik, 2025). Da der mangler data for årene 2021 og 2023, har vi anvendt lineær interpolation til at estimere de manglende værdier og sikre en visuel kontinuitet i tidsserien.

N i respondenter der besvarede DST indsamlingen var 4.139, ud af en samlet population på 18.379. Disse data er sammenholdt med optagelsestal fra Den Koordinerede Tilmelding (KOT) for årene 2019 til og med 2024 (Uddannelses- og Forskningsministeriet, 2024). Det skal bemærkes, at kvantitative data som disse aldrig udgør et fuldstændigt billede af virkeligheden, men snarere fungerer som indikatorer, der peger på tendenser og udviklinger. Særligt i denne analyse, hvor data for visse år er estimeret ved lineær interpolation, og hvor rapporteringen fra virksomheder er baseret på selvrapporterede brud, kan der forekomme skyggetal og underrapportering. Disse tal sammenlignes, fordi optagelsestal afspejler udbuddet af fremtidige IT-specialister, mens virksomheders oplevede cyberangreb illustrerer den aktuelle efterspørgsel efter IT-sikkerhedskompetencer. Da KOT-registeret indeholder omkring 930 unikke uddannelser og over 5.400 uddannelsesforløb, har gruppen primært baseret kategoriseringen på Undervisningsministeriets (UG) officielle oversigter over uddannelsesindhold og uddannelsestitler med klar relevans for IT-sikkerhed, såsom datalogi og beslægtede fagområder. I tilfælde hvor relevansen var uklar eller tvivlsom, er de tilhørende studieordninger blevet gennemgået for at sikre en korrekt placering. På baggrund af de fem års indsamlede data har det højeste antal optagne været i 2020, bestående af 69.526 personer, hvor det laveste år 2022, bestod af 60.034 optagne, hvorefter antallet har stagneret.



Figur 1: *Optagne på IT-Uddannelser vs. virksomhedernes oplevede cyberangreb (2019-2024)*

På trods af den hastige stigning i cyberkriminalitet har antallet af personer, der vælger at uddanne sig indenfor IT-sikkerhed i Danmark, ikke fulgt med denne udvikling. Mens cyberangrebene er steget med 90 % fra 2019 til 2024, er antallet af optagne på IT-uddannelser faldet med 6,64 % i samme periode. Denne modsatrettede udvikling udgør en væsentlig udfordring for både erhvervslivet og samfundet som helhed og skaber et pres på både virksomheder, der søger at beskytte sig selv, og samfundet som helhed, som skal håndtere de stigende trusler. Der er derfor, og der kommer sandsynligvis til at være, et markant behov for flere veluddannede fagfolk, som kan imødekomme de digitale udfordringer, der følger med den moderne udvikling.

1.1.3 Uformelle organisationer

Udover de formelle uddannelser som beskrevet i ovenstående graf, eksisterer der mange uformelle organisationer i Danmark der, enten gennem interesse i feltet eller med en politisk agenda, samler individer i fællesskaber hvor omdrejningspunktet er videndeling og udvikling af kompetencer inden for IT-sikkerhed. Heriblandt er der De Danske Cybermesterskaber, en konkurrence for 15-25-årige, der inkluderer online træning, en kvalifikationsrunde og en finale på Aalborg Universitet i København (De Danske Cybermesterskaber, u.å.). Her konkurreres der i IT-sikkerhed, men samtidigt er der sat både online og offline træningssessioner op fra Aalborg til København. Disse initiativer kan ses som en strategi til at øge interessen og engagementet omkring konkurrencen. En nærmere undersøgelse af konkurrencens sponsorer afslører samtidig, at der også kan være flere strategiske motiver bag. Blandt sponsorerne findes eksempelvis Forsvarets Efterretningstjeneste, som har en tydelig interesse i at fremme talentudviklingen inden for IT-sikkerhed i Danmark med henblik på at styrke det nationale cyberforsvar. Udover professionelle konkurrencer findes der i Danmark også en række frivillige grupper, såkaldte Capture-the-Flag-grupper (CTF), som spiller en central rolle i udviklingen af IT-sikkerhedstalenter.

1.1.4 Problemformulering:

IT-kriminalitet er en voksende trussel, og selvom der findes formelle uddannelser og uformelle initiativer som cybermesterskaberne, er der stadig en kritisk mangel på specialister. Samtidig er SMV'erne særligt sårbare over for cyberangreb, da de ofte ikke prioriterer

sikkerhed i tilstrækkelig grad og mangler ressourcer. Derfor finder vi det relevant at udforme følgende problemformulering:

"*Hvilken viden og hvilke praksisser fra nuværende formelle og uformelle uddannelser og samlinger kan benyttes af SMV-segmentet i Danmark til at imødekomme det stigende IT-sikkerhedsbehov?*"

1.1.5 Begrebsafklaring

Som set i problemformuleringen, har dette speciale fokus på tre kategorier: SMV'er samt formelle uddannelser og uformelle samlinger. Dette afsnit vil derfor definere dem for at beskrive betydningen af dem, samt tydeliggøre afgrænsningerne af dem.

Små og mellemstore virksomheder

Dette speciales forståelse af begrebet "Små virksomheder" er defineret ud fra årsregnskabsloven som definerer dem som i to regnskabsår ikke at have overskredet to ud af tre kriterier: 50 heltidsbeskæftigede, 89 millioner kr. i omsætning og 44 millioner kr. i balancesum. Mellemstore virksomheder er i årsregnskabsloven defineret som der ikke er små virksomheder, og i to regnskabsår ikke overskrider 2 ud af 3 kriterier: 250 heltidsbeskæftigede, 313 millioner kr. i omsætning og 150 millioner kr. i balancesum (Civilstyrelsen, u.å.). For at tjekke om informanterne til dette speciale tilhører virksomheder indenfor disse afgrænsninger, er deres årsrapporter indeholdende information vedrørende deres omsætning og balancesum samt antal ansatte hentet fra CVR registeret (*CVR - Det Centrale Virksomhedsregister*, u.å.).

Formel uddannelse

Specialet har valgt at referere til rapporten fra UNESCO som definerer det som følgende:

> *Formel uddannelse defineres som uddannelse, der er institutionaliseret, bevidst og planlagt gennem offentlige organisationer og anerkendte private organer, og som samlet udgør et lands formelle uddannelsessystem. Formelle uddannelsesprogrammer anerkendes således som sådanne af de relevante nationale uddannelsesmyndigheder*

> *eller tilsvarende, f.eks. andre institutioner i samarbejde med de nationale eller regionale uddannelsesmyndigheder.* (UNESCO, 2011, s. 8)

I Danmark defineres formelle uddannelsesinstitutioner yderligere som institutioner, der er godkendt af Uddannelses- og Forskningsministeriet og blandt andet kan være registreret i KOT-systemet, samt erhvervsuddannelser.

Uformel uddannelse

Dette speciales forståelse af uformelle samlinger beror på en blanding af ovenstående afsnit 1.1.3, og tilstedeværelsen af uformel uddannelse i disse. Uformel uddannelse er baseret på Europa-Kommissionen (2012)'s definition, der beskriver det som noget der sker på forskellige måder og i forskellige sammenhænge uden for formelle uddannelsesinstitutioner. Her bliver det ydermere delt op i "*ikkeformel læring*" og "*uformel læring*" hvor førstnævnte er en mere struktureret og tilrettelagt undervisning, eksempelvis på arbejdspladsen, og sidstnævnte opstår naturligt som en del af forskellige aktiviteter. Dette kan eksempelvis være i forbindelse med digitale færdigheder, der bliver udviklet gennem fritidsaktiviteter såsom i uformelle samlinger. Uformel læring og validering deraf blev sat på den Europæiske dagsorden siden 2001, og der er siden da indført en række initiativer og retningslinjer, der kan hjælpe uformel uddannelse med at blive valideret. I Danmark blev der eksempelvis indført en lov om anerkendelse af realkompetence på voksen- og efteruddannelsesområdet (Undervisningsministeriet, 2008). Realkompetence er det, man har lært og kan, både fra skole, job, frivilligt arbejde og andre erfaringer i livet, uanset om det er noget, man har lært formelt eller mere tilfældigt undervejs. For at reducere kompleksiteten af begreber forstås ikkeformel læring og uformel læring som det samme i specialet og derfor betegnes som uformel læring fremadrettet.

2 Forskningsmæssig Forståelsesramme

Formålet med dette afsnit er at skabe et opdateret billede af, hvordan nyere forskning forholder sig til en række centrale temaer, som vi vurderer er særligt relevante for specialets problemstilling. Ved at tage afsæt i nyere og anerkendte forskningsartikler, særligt reviewartikler og systematiske oversigter, etableres en forståelsesramme, der forankrer

specialets fokus i det eksisterende vidensfelt. Det gør det muligt at tydeliggøre, hvor specialets undersøgelse kan bidrage med ny indsigt eller praksisnær operationalisering, frem for at gentage allerede etableret viden. Afsnittet er struktureret omkring fire nøgletemaer: Først fokuseres der på generelle trends og udfordringer i IT-sikkerhed samt betydningen af kunstig intelligens (AI). Dernæst belyses danske SMV'ers arbejde med IT-sikkerhed, hvorefter kompetencemangler og træningsmetoder inden for IT-sikkerhed gennemgås. Denne tematiske afgrænsning skal ikke forstås som dækkende for hele forskningsfeltet, men som en strategisk udvælgelse, der understøtter og perspektiverer specialets metodiske og analytiske fokus.

2.1 IT-sikkerhed og emergerende trends

Dette afsnit giver et overblik over centrale tendenser og aktuelle forskningsbidrag indenfor IT-sikkerhed. Der vil blive belyst både klassiske og nyere problemstillinger, såsom fremkomsten af avancerede trusselsaktører, effekten af IT-sikkerhedstræning samt anvendelsen af kunstig intelligens som et potentielt værktøj i fremtidens sikkerhedsstrategier. IT-sikkerhed har udviklet sig markant i takt med den stigende digitalisering af samfundet. Ifølge Perwej, Abbas, Dixit, Akhtar & Jaiswal (2021) har cyberangreb ført til betydelige udfordringer inden for databeskyttelse, hvor metoder såsom phishing, malware og avancerede trusselsaktører kontinuerligt udvikler nye angrebsformer. Dertil beskriver de, hvordan stigende kompleksitet i IT-infrastrukturer, herunder integrationen af Internet of Things (IoT), har medført en øget eksponering over for trusler, hvilket kræver nye og effektive sikkerhedsforanstaltninger. Effektive IT-sikkerheds-træningsprogrammer er essentielle for at mindske risikoen for brud forårsaget af menneskelige fejl. En systematisk gennemgang af Prümmer, van Steen & van den Berg (2024) viser, at de mest anvendte træningsmetoder inkluderer gamification, simuleringer og informationsbaserede træningsmoduler. Selvom de fleste studier rapporterer en positiv effekt af træning, varierer resultaterne afhængigt af designet og konteksten for tiltagene. Problematikken med "shadow security", en adfærd hvor ansatte bevidst går på kompromis med sikkerheden for at opnå primære forretningsmål, fremhæver nødvendigheden af at gøre træningsmetoder mere praksisnære og engagerende (Kirlappos, Parkin & Angela Sasse, 2015). Den seneste udvikling inden for kunstig intelligens (AI), herunder store sprogmodeller (LLM), har åbnet nye muligheder for IT-sikkerhed. Zhang, Bu, Wen, Liu, Fei, Xi, Li, Yang, Zhu & Meng (2025) gennemgik over

300 studier og fandt, at LLM'er kan anvendes til trusselsopsporing, sårbarhedsanalyse og automatiseret IT-sikkerhedstræning. Dog fandt de udfordringer forbundet med skalerbarhed og bias i modellerne, hvilket kræver en mere systematisk tilgang til implementering og validering af LLM-baserede løsninger.

2.2 Digital sikkerhed i danske SMV'er

Dette afsnit undersøger, hvordan danske SMV'er forholder sig til digital sikkerhed, herunder investeringer, implementering af basale sikkerhedstiltag, ledelsesmæssig engagement og afhængighed af eksterne leverandører. Dertil afdækkes både fremskridt og vedvarende udfordringer, der præger det digitale trusselsbillede i danske SMV'er.

Danske SMV'er har øget deres investeringer i IT-sikkerhed markant de seneste år. I 2021 rapporterede 37 % af SMV'erne, at de havde øget deres investeringer i IT-sikkerhed sammenlignet med året før, hvilket er den største stigning siden 2018 (Digitaliseringsstyrelsen, 2023, s. 9). Der ses en positiv udvikling i implementeringen af grundlæggende sikkerhedstiltag blandt SMV'er. Andelen af virksomheder, der ikke anvender basale sikkerhedstiltag såsom softwareopdateringer og backup, faldt fra 24 % i 2021 til 16 % i 2022 (s. 9). Dog er der fortsat udfordringer, især blandt mikrovirksomheder (fem til ni ansatte), hvor 29 % stadig ikke anvender de mest basale sikkerhedsforanstaltninger. Til sammenligning er denne andel kun 16 % blandt SMV'er med 10–249 ansatte (s. 18). Kun 54 % af danske SMV'er har dokumentation for IT-sikkerhedsprocedurer, og blandt disse har kun 36 % opdateret denne dokumentation inden for de seneste 12 måneder. Ledelsens involvering i IT-sikkerhed er ligeledes begrænset, idet blot 36 % af SMV'erne angiver, at deres ledelse i høj grad deltager i beslutninger om digital sikkerhed (s. 15). En væsentlig udfordring for SMV'er er manglen på kvalificerede IT-specialister. I 2021 forsøgte 17 % af SMV'erne at rekruttere IT-specialister, hvoraf 60 % oplevede vanskeligheder med at besætte stillingerne (s. 27). For mange SMV'er betyder dette, at generelle IT-medarbejdere håndterer sikkerhedsopgaver, hvilket kan resultere i lavere sikkerhedsniveauer. En analyse af danske produktions-SMV'er viser, at IT-sikkerhed i stigende grad bliver en prioritet. Dog har 35 % af virksomhederne stadig et for lavt sikkerhedsniveau i forhold til deres risikoprofil, om end dette er en forbedring fra 44 % året før (Stentoft, Mikkelsen, Schmitt, Keating, Theussen, Peressotti, Mayer, Kankam-Boateng & Tumchewics, 2024, s. 9). En væsentlig andel af produktions-SMV'erne anvender eksterne leverandører til deres IT-sikkerhed. I 2022

outsourcede 77 % af virksomhederne deres digitale sikkerhedsopgaver, men 25 % af disse virksomheder stillede ikke krav til leverandørerne om datasikkerhed, dokumentation eller håndtering af IT-sikkerhedsforanstaltninger (s. 27). Der er en tydelig sammenhæng mellem digital sikkerhed og virksomhedernes arbejde med dataetik. Blandt de SMV'er, der aktivt arbejder med dataetik, implementerer 62 % mange tekniske sikkerhedstiltag, mens kun 27 % af de virksomheder, der ikke arbejder med dataetik, gør det samme (Digitaliseringsstyrelsen, 2023, s. 34).

2.3 Kompetencemangler

En væsentlig udfordring indenfor IT-sikkerhed er manglen på velkvalificeret arbejdskraft samt et misforhold mellem efterspørgsel og udbud af relevante færdigheder (Ruoslahti, Coburn, Trent & Tikanmäki, 2021). I et systematisk studie af akademisk litteratur fremhæver de, at behovet for kompetente IT-sikkerhedsmedarbejdere er stigende, og at organisationer ofte savner egnede uddannelsesprogrammer, der hurtigt kan opkvalificere eksisterende personale. Samtidig peger Goupil, Laskov, Pekaric, Felderer, Dürr & Thiesse (2022) på en betydelig "skill gap," hvor både antallet af specialister og deres konkrete faglige kunnen ikke matcher branchens behov.

Desuden fandt de, at udfordringen er todelt. For det første er der en kvantitativ mangel på medarbejdere, hvilket medfører adskillige ubesatte stillinger. For det andet er der en kvalitativ forskel på de kompetencer, der typisk efterspørges i jobopslag, sammenlignet med indholdet i de uddannelser, der udbydes. Den manglende overensstemmelse kommer blandt andet til udtryk i, at studieretningerne ofte fokuserer på klassiske IT-sikkerhedsemner som kryptografi, men i mindre grad inkluderer nyere krav om eksempelvis compliance og risikostyring (Goupil et al., 2022; Ruoslahti et al., 2021).

I forlængelse heraf påpeger Ruoslahti et al. (2021), at et tættere samarbejde mellem uddannelsesinstitutioner og erhvervslivet potentielt kan mindske denne kløft. Dette kunne indebære en systematisk dialog om pensumdesign, hvor særligt praksisnære kompetencer som trusselsanalyse, sårbarhedsvurdering og løbende compliance-opdateringer integreres i uddannelsesforløb. Endelig peger Goupil et al. (2022) på, at udvikling af fleksible træningsformer, eksempelvis e-læring og mikro-certificeringer, kan lette

kompetenceudvikling for nuværende medarbejdere og dermed bidrage til at afhjælpe den eksisterende kompetencemangel.

2.4 Træningsmetodikker

Dette afsnit giver et overblik over de mest anvendte IT-sikkerheds træningsmetoder, herunder simulationer, gamificering og konkurrencebaseret læring samt e-læring og nudging, endvidere diskuterer deres styrker, begrænsninger samt potentiale for at understøtte varig adfærdsændring.

Effektiv IT-sikkerhedstræning er afgørende for at forbedre medarbejders adfærd og organisationers evne til at modstå cybertrusler. Ifølge Prümmer et al. (2024)'s litteraturstudie findes der tre primære træningsmetoder i IT-sikkerhed: simulationer, gamificering og e-læring.

Simulationer skaber sikre og realistiske øvelser, som eksempelvis kan styrke medarbejdernes evne til at genkende trusler, det påvises at gentagne phishing-simulationer reducerer klikraten på ondsindede links med op til 60 % (Prümmer et al., 2024). Gruppens litteraturstudie fra 9. semester (Bilag 22) viser tilmed, at cyberranges tilbyder IT-specialister værdifuld hands-on erfaring med angrebshåndtering, hvilket forbedrer reaktionstid og beslutningstagning. Dernæst belyses det at gamification øger engagement og læring gennem spilelementer såsom points og konkurrencer, og samtidig påvises det at den langsigtede adfærdsændring ofte er begrænset, hvis gamificering ikke kombineres med andre metoder (Prümmer et al., 2024). Endvidere identificeres det at CTF-øvelser kan styrke tekniske færdigheder og samarbejde, men deres langtidseffekt kræver organisatorisk opfølgning (Prümmer et al., 2024; Bilag 22). E-læring anvendes ofte som en skalerbar løsning, men dens effektivitet afhænger af implementeringen. Ifølge Prümmer et al. (2024) er effekten af traditionelle e-læringsmoduler begrænset uden interaktive elementer. Bilag 22 understreger ligeledes, at blended learning-tilgange, hvor e-læring kombineres med praktiske øvelser, giver bedre resultater. Adfærdsændrende interventioner, nudging, kan forbedre læringseffekten. Ved at anvende små visuelle påmindelser eller interaktive advarsler i systemer kan virksomheder reducere menneskelige fejl (Prümmer et al., 2024). Mikrolæring, hvor medarbejdere får korte, fokuserede læringsmoduler, kan være en effektiv metode til løbende kompetenceudvikling (Bilag 22).

Disse metoder varierer i effektivitet afhængigt af målgruppen og organisationens behov. Bilag 22, supplerer, at kombinationen af træningsmetoder ofte giver den bedste læringseffekt inden for IT-sikkerhedstræning, da forskellige teknikker appellerer til forskellige læringsstile.

2.5 Opsummering

For at opsummere de vigtigste fund fra den gennemgåede forskning, præsenteres nedenfor en tabel, der opdeler resultaterne i fire centrale temaer: IT-sikkerhed og emergerende trends, digital sikkerhed i danske SMV'er, kompetencemangler og træningsmetodikker.

Tema	Key findings
IT-sikkerhed og emergerende trends	IT-sikkerhed er blevet mere kompleks med digitalisering, IoT og nye angrebsformer som phishing og malware. Der er et behov for effektive træningsprogrammer, herunder gamification og simuleringer. AI, især store sprogmodeller (LLM), har potentiale til at forbedre IT-sikkerhed, men der er udfordringer med skalerbarhed og bias.
Digital sikkerhed i danske SMV'er	Der er en markant stigning i danske SMV'ers investeringer i IT-sikkerhed, især brug af ekstern bistand. Dog er der udfordringer, især blandt mikrovirksomheder, der ikke anvender basale sikkerhedstiltag. Ledelsens involvering i digital sikkerhed er begrænset, og der er mangel på kvalificerede IT-specialister.
Kompetencemangler	Der er stor mangel på kvalificerede IT-sikkerhedsmedarbejdere, og et misforhold mellem de nødvendige færdigheder og de uddannelser, der tilbydes. Der er behov for tættere samarbejde mellem uddannelsesinstitutioner og erhvervslivet samt fleksible træningsformer som e-læring og mikro-certificeringer for at afhjælpe kompetencemanglen.
Trænings metodikker	De mest effektive træningsmetoder er simulationer, gamificering og e-læring. Simulationer, især phishing-simulationer, kan reducere fejlklik markant. Gamificering øger engagementet, men skal kombineres med andre metoder for langsigtet effekt. E-læring skal være interaktiv for at være effektiv, og mikrolæring kan bidrage til løbende kompetenceudvikling.

Tabel 1: Opsummering af litteraturgennemgang

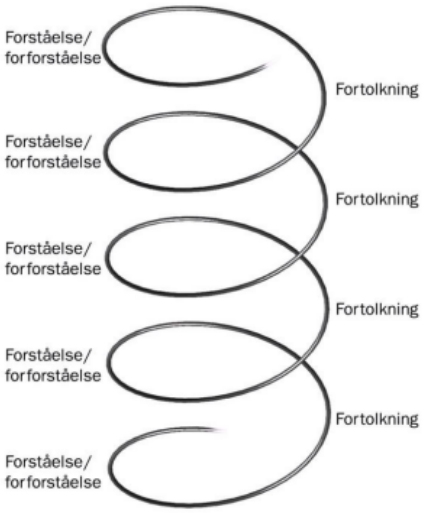
3. Metode

Metodeafsnittet har til formål at beskrive undersøgelsesdesignet af specialet, herunder hvilken videnskabsteori der benyttes, hvordan indsamling af empirien er planlagt og udført samt hvilke etiske overvejelser der er blevet gjort i sammenhæng med sidstnævnte. Sidst vil der redegøres for specialets "Erkendelser" som opstod i krydsfeltet mellem empiriindsamlingen og analysen, hvorefter afsnittet vil afslutte med en gennemgang af specialets analysedesign, under afsnittet 3.7 "Kodning".

3.1 Videnskabsteoretisk tilgang

I dette speciale anlægges der en hermeneutisk tilgang til at opnå en dybere forståelse af hvordan viden og praksisser fra formelle og uformelle uddannelser og samlinger kan benyttes af SMV'er i Danmark til at imødekomme det stigende IT-sikkerhedsbehov. Tilgangen er inspireret af Hans-Georg Gadamer, der betragter forståelse som en dialogisk proces mellem fortolkeren og det, der fortolkes (Egholm, 2014, s. 95). Hermeneutikken har til formål at afdække meningen bag det undersøgte fænomen gennem en iterativ fortolkningsproces, og herved kan det analyseres hvordan SMV'er opfatter og håndterer IT-sikkerhed i praksis. Dertil kan det analyseres, hvordan organisationer underviser i IT-sikkerhed og sikrer, at personalet kan håndtere de ovenstående faktorer. Ontologisk positioneres specialet mellem idealisme og realisme, idet der anerkendes, at IT-sikkerhed både er et teknisk og et organisatorisk fænomen, som opfattes forskelligt af forskellige aktører. Dette afspejler sig i interessen for at udforske de subjektive perspektiver på IT-sikkerhed, herunder hvordan virksomhedsledere og IT-ansvarlige i SMV'er navigerer i et landskab præget af regulering, risikovurdering og teknologisk udvikling. Der søges således ikke en entydig sandhed, men en nuanceret forståelse af de forskellige måder, hvorpå IT-sikkerhed implementeres og prioriteres i SMV'er (Egholm, 2014, s. 91). Epistemologisk er fokusset rettet mod, hvordan viden om IT-sikkerhed opstår i en SMV-kontekst, og hvordan organisationernes kompetencer udvikler sig over tid. For at undersøge dette, anvendes der en kvalitativ metode, hvor interviews og etnografi danner grundlaget for den empiriske analyse. Der trækkes på Gadamers koncept om den hermeneutiske spiral (Se Figur 2), hvor forståelse opnås gennem en kontinuerlig vekselvirkning mellem helhed og dele af et fænomen (Egholm, 2014, s. 91).

Denne iterative tilgang sikrer, at der ikke blot beskrives IT-sikkerhedsudfordringer statisk, men i stedet bliver engageret i en proces, hvor indsigt og forståelse udvikles løbende.



Figur 2: Illustration af den hermeneutiske spiral (Systime 2023).

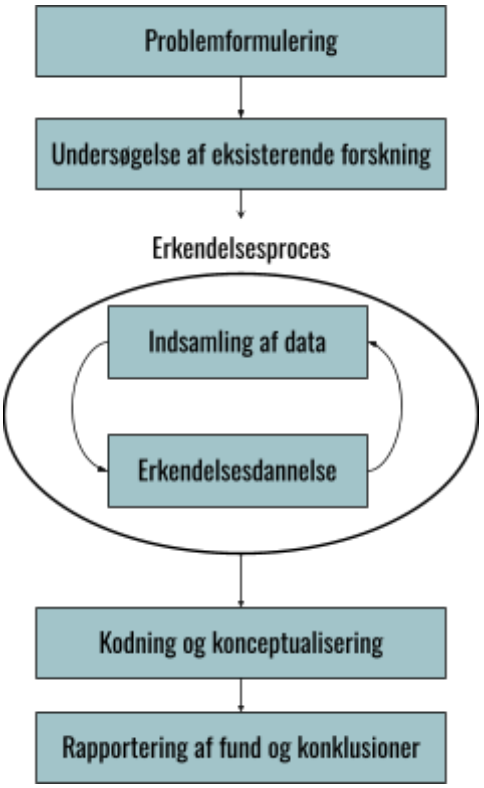
Valget af hermeneutik er begrundet i to centrale faktorer. Først anerkendes betydningen af specialegruppens egne forforståelser som en del af forskningsprocessen. Vores baggrund inden for IT-ledelse og IT-sikkerhed påvirker tilgangen til emnet, og derfor er vi bevidste om, at forståelsen af IT-sikkerhedsudfordringer ikke kan adskilles fra de kontekster, de optræder i. For det andet ønskes der at præsentere en fortolkende analyse, hvor resultaterne ikke alene betragtes isoleret, men som en del af en bredere systemisk sammenhæng. Derfor vil specialet inddrage empiriske eksempler og citater fra vores datamateriale for at illustrere de forskellige perspektiver, der bidrager til en helhedsforståelse af IT-sikkerhed i SMV'er.

3.2 Kvalitativ metode

I dette speciale er den kvalitative metode valgt af flere årsager. Den første og vigtigste årsag er, at tilgængeligheden af data på området er begrænset i en dansk kontekst, og tiden til indsamling er for kort til selv at indsamle en passende mængde data til at skabe en normalfordeling. Den anden årsag er ønsket om at forstå de forskellige interessenters opfattelse af, hvordan IT-sikkerhedskompetencer bedst opnås og anvendes bagefter. Dette kræver en dybdegående dialog for at forstå nuancerne og, endnu vigtigere, for at undgå misforståelser.

3.3 Undersøgelsesdesign

Dette afsnit har til formål at tydeliggøre specialets undersøgelsesdesign samt de begrundelser og overvejelser, der har ført til dets specifikke udformning. Som overordnet tilgang er der valgt en eksplorativ metode, hvilket er begrundet i manglen på tidligere forskning inden for feltet, samt specialegruppens begrænsede forudgående viden på området. Thomas Harboe (2006) beskriver i *"Indføring i samfundsvidenskabelig metode"*, hvordan en eksplorativ tilgang anvendes i samfundsvidenskaben, når forskeren ikke har en særlig forudgående indsigt i undersøgelsesfeltet (Harboe, 2006, s. 32). Det eksplorative design kan blandt andet omfatte feltarbejde, observationer og interviews, men følger ikke en standardiseret metode. Dette skyldes, at undersøgeren ofte har en teoretisk og erfaringsbaseret idé om, hvad der kan forventes i feltet, men ikke på forhånd ved, hvordan undersøgelsen vil forløbe, eller hvilke iagttagelser der vil blive registreret (Harboe, 2006, s. 32). Dette gør sig også gældende for dette speciale, hvor der, som beskrevet i 3.1 "Videnskabsteoretisk tilgang", eksisterer en forforståelse, der løbende udvikler sig.

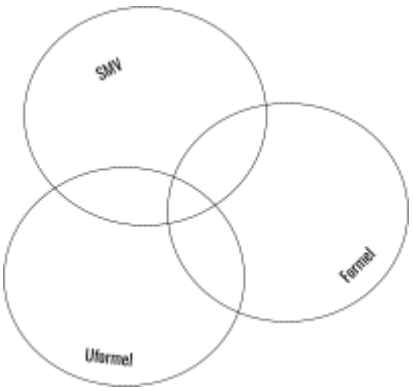


Figur 3: Undersøgelsesdesign

Ovenstående figur illustrerer specialets eksplorative design, hvor erkendelsesprocessen udfolder sig som en iterativ vekselvirkning mellem dataindsamling og datafortolkning. Denne proces afspejler den hermeneutiske spiral, hvor nye erkendelser løbende former både metode og fokusområder. Modellen viser, hvordan arbejdet tager udgangspunkt i problemformuleringen og en indledende undersøgelse af eksisterende forskning, hvorefter den centrale erkendelsesproces, præget af fortolkning og tilpasning, fører frem mod kodning, konceptualisering og til sidst rapportering af fund og konklusioner.

3.4 Empiriindsamling

For at sikre, at specialet opnår en fyldestgørende mængde empiri og i et forsøg på at opnå empirimætning, er der valgt at anvende flere metoder til indsamlingen af empiri. Som beskrevet nedenfor, er der anvendt semi-strukturerede interviews (Se afsnit 3.4.1 Semistruktureret Interviews) samt sekundær empiri, eksempelvis tidligere forskning i SMV Danmark. Empiriindsamlingen er struktureret således, at der opnås indsigt i SMV Danmarks udfordringer i forhold til skill-gappet, som beskrevet i problemfeltet, dog med hovedvægt på at afdække, hvordan IT-sikkerhedskompetencer opnås i Danmark, både formelt og uformelt. Den overordnede empiriindsamling har til formål at afdække tre centrale kategorier: SMV, uformel -og formel læring. Denne afgrænsning blev brugt til at strukturere empirien, hvilket muliggjorde identificeringen af informanter, der kunne afdække de aspekter, som andre informanter ikke kunne belyse. Dette grundet, at der skulle være en lige fordeling af mængden af informanter i hver kategori, således at alle perspektiver blev dækket så grundigt som muligt. For at skabe et helhedsperspektiv, blev der udarbejdet en strategi for at opsøge informanter, der ikke kun bevæger sig inden for ét område, men som opererer i to eller alle tre. Dette er eksemplificeret i nedenstående venn-diagram (Se figur 4), hvor det ses, hvordan områderne overlapper og dermed muliggør både en isoleret forståelse af de enkelte elementer og en holistisk forståelse af det samlede undersøgelsesfelt.

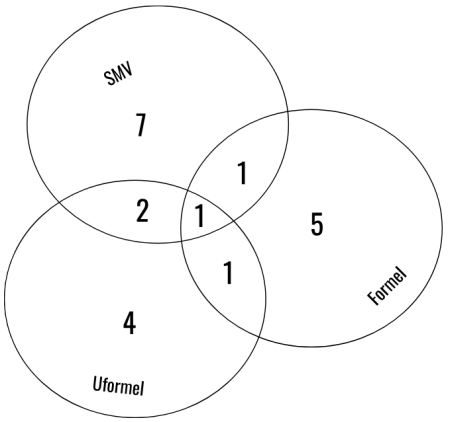


Figur 4: Venn-diagram over informanttyper

Eftersom dette var en kvalitativ undersøgelse, blev der forsøgt at indsamle så meget data som muligt, med en stræben efter mest mulig variation i informanterne. Ved hjælp af en Pipeline, blev der dannet overblik og struktur på tværs af forskningsgruppen på, hvilke informanter der var kontaktet, manglede at blive kontaktet, var opsat et møde med, eller ikke ville deltage samt begrundelsen for dette. Der blev indledningsvist identificeret relevante personer i de formelle og uformelle kategorier, blandt andet gennem Cyberskills og De Danske Cybermesterskaber. Kontakten til informanterne blev initieret gennem flere kanaler og strategier, såsom deltagelse i konferencer, LinkedIn, e-mail, telefonisk kontakt og i stor grad Snowball Sampling (Naderifar, Mahin & Goli, Hamideh & Ghaljaei, Fereshteh, 2017). Snowball Sampling er anvendt i flere studier (Yingling & McClain, 2015; Edmonds, 2019; Bindah, 2019) til at identificere en større gruppe af ukendte og/eller svært tilgængelige informanter, som er relevante for undersøgelsens fokus. Metoden involverer indledningsvist at udvælge individer, som ikke nødvendigvis selv er informanter, men kan identificere dem, og har adgang til dem. Dette var mest relevant for SMV'erne, som er mere under radaren og sjældent har tid til at deltage i interviews. På tværs af hver kategori blev informanterne identificeret og kontaktet som følgende: 1) *SMV-området, 2) den formelle kategori og 3) den uformelle kategori*.

SMV-området blev blandt andet kontaktet gennem en facilitator fra erhvervsservicen Væksthimmerland, som skabte kontakt til SMV'er samt informanter med dybdegående og bred SMV-kendskab, f.eks. konsulenter og rådgivere. Derudover blev der lavet LinkedIn-opslag, som nogle SMV-eksperter reagerede på med interesse for at deltage i interviews, mens andre SMV'er, der allerede var i gruppens LinkedIn-netværk, blev kontaktet direkte. Der blev forsøgt at række ud til flere forskellige virksomheder, hvor flere svarede, at

de enten ikke havde nok viden om emnet IT-sikkerhed, eller/og havde outsourcet denne del. En SMV, der arbejder med lys- og lydinstallationer og en skole deltog dog i interviews. Disse er førstehåndskilder, som fortæller om deres specifikke udfordringer i egen kontekst. Som nævnt, blev konsulentvirksomheder og andre rådgivende virksomheder til SMV'er kontaktet som et resultat af Snowball Sampling. Disse blev brugt som understøttende eksperter, ved at de fortalte om deres adskillige erfaringer med SMV'er, hvilket var mere bredt afdækkende og derfor nærmere fungerede som en generaliserbar viden. Der blev skabt kontakt til informanter i den formelle kategori gennem Cybersecurity, Learning, Education and Research (CLEAR)-netværket, der består af undervisere med speciale i IT-sikkerhed. Disse informanter har dertil henvist til andre eksperter inden for især den formelle kategori, men også de to andre kategorier. Andre formelle informanter reagerede på gruppens LinkedIn-opslag, mens andre blev opsøgt ved hjælp af uddannelsesstedernes egne hjemmesider og derefter kontaktet på mail. Gruppen kontaktede informanter i den uformelle kategori, da der gennem eget netværk allerede var etableret forbindelse til flere uformelle CTF-grupper, som for eksempel Foreningen for Danske Cyber Alumner (FDCA). En professor fra Aalborg Universitet i København har fungeret som facilitator, suppleret af gruppens eget netværk. Denne tilgang har sikret en bred indgangsvinkel til hver kategori. Nedenstående venn-diagram viser den endelige fordeling af informanter i undersøgelsen, og der var i alt 21 informanter.



Figur 5: Afsluttende Venn-diagram

3.4.1 Semistruktureret interview

Med udgangspunkt i Brinkmann & Tanggaard (2020)'s bog om kvalitative metoder, vil dette afsnit redegøre for vores interviewmetode samt den proces, vi har fulgt i forbindelse med

interviewene. Det semistrukturerede interview kombinerer åbne og strukturerede spørgsmål med det formål at opnå en nuanceret og dybdegående forståelse af IT-sikkerhedsudfordringerne, som danske SMV'er, uformelle samlinger og formelle uddannelser står over for. Den semistrukturerede tilgang muliggør tilmed en systematisk ramme for interviewet, samtidig med, at den giver fleksibilitet til at stille supplerende og opklarende spørgsmål. Indledningsvist anvendes primært åbne spørgsmål for at give den interviewede mulighed for at udfolde sin viden og erfaringer. En interviewguide fungerer overordnet som et redskab til at strukturere interviewforløbet. I takt med interviewets progression samt den viden der udvikles løbende, kan intervieweren stille opfølgende og undrende spørgsmål, som ikke indgår i den forberedte interviewguide. Dette sikrer, at de nødvendige indsigter indhentes for at kunne besvare forskningsspørgsmålet.

Specialets interviewguide (Bilag 23, interviewguides) var opdelt i tre fokuserede områder for at belyse forskellige perspektiver på IT-sikkerhedskompetencer. Den første del rettede sig mod formelle uddannelser med henblik på at undersøge både deres viden om og praksis for udvikling af IT-sikkerhedskompetencer. Den anden del fokuserede på uformelle uddannelsesformer og havde til formål at afdække, hvordan disse arbejder med IT-sikkerhedsundervisning, både hvad angår viden og praksis. Endelig blev SMV'er inkluderet for at kortlægge deres eksisterende IT-sikkerhedskompetencer samt deres opfattelse af det aktuelle trusselsbillede inden for IT-sikkerhed. Denne opdeling gjorde det muligt at opnå en nuanceret forståelse af de forskellige aktørers roller og udfordringer på området (Bilag 23, Interviewguides).

Vores interviewdesign er desuden informeret af den eksisterende forskningslitteratur (Se afsnit 2. Forskningsmæssig Forståelsesramme). Et centralt tema fra denne forskning omhandlede IT-sikkerhedens kompleksitet og udvikling i takt med digitalisering, samt de udfordringer og løsninger, der relaterer sig til både teknologiske fremskridt og menneskelige faktorer. På baggrund af disse indsigter har vi eksempelvis formuleret spørgsmål således: "*Hvordan tror du, at et cyberangreb kunne påvirke jeres virksomhed? Samt hvilke konsekvenser kan det have for virksomheden?*". Dette spørgsmål relateres til litteraturens fokus på de teknologiske og menneskelige faktorer, som spiller en væsentlig rolle i forståelsen af IT-sikkerhedsrisici. Ved at stille spørgsmålet søger vi at få indsigt i, hvordan SMV'er opfatter de potentielle konsekvenser af et IT-sikkerhedsbrud og hvilke udfordringer, der knytter sig til at håndtere sådanne hændelser. Vores interviewdesign har gjort det muligt

at indsamle nuancerede data, der belyser forskellige perspektiver på IT-sikkerhedskompetencer inden for både formelle og uformelle uddannelser samt SMV-sektoren. Gennem en systematisk udvikling af vores interviewguides og inddragelse af relevant forskningslitteratur har vi skabt et solidt grundlag for at analysere og fortolke de indsamlede data.

3.4.2 Etiske overvejelser

Etiske overvejelser er en integreret del af enhver forskningsproces. Det er essentielt at være opmærksom på, hvordan data præsenteres, og hvordan dette kan påvirke forskellige interessenters synspunkter. Det er derfor nødvendigt at sikre, at data præsenteres præcist og pålideligt, samtidig med at alle involverede parters rettigheder respekteres. Dette kræver en omhyggelig tilgang før, under og efter dataindsamlingen, hvor etiske dilemmaer håndteres med passende forsigtighed. Nedenstående diskussion vil uddybe, hvordan disse etiske overvejelser manifesterer sig i specialet.

Inden for kvalitativ forskning kan der identificeres fire centrale etiske principper: 1) Informeret samtykke, 2) fortrolighed og anonymitet, 3) konsekvenser og 4) forskerens rolle i dataindsamling og -behandling (Brinkmann & Tanggaard 2020, s. 597-599). Informeret samtykke opnås ved at give en grundig præsentation af interviewets formål forud for selve interviewet. Deltagelse er frivillig, og informanterne har ret til at undlade at besvare spørgsmål eller trække sig tilbage når som helst (s. 597-599). Fortrolighed og anonymitet udgør et særligt etisk dilemma i specialet og repræsenterer det andet princip. Samarbejdet omfatter ikke kun universiteter, men også erhvervseksperter, ansatte og ledere med mere. Derfor er det essentielt at sikre korrekt anonymisering af data for at beskytte informanternes identitet og sikre deres fremtidige beskæftigelsesmuligheder og samarbejdsrelationer. Her er det vigtigt at sikre sikker opbevaring af lyd- og videooptagelser, hvilket i dette speciale foregår på Sharepoint, som fjerner materialet automatisk efter 60 døgn. Fejlagtig anonymisering af informanter kan have negative konsekvenser for deres fremtidige arbejdsforhold og samarbejdsrelationer med IT-sikkerhedsbranchen i værste fald. Derfor anonymiseres navne på de informanter, der har ønsket dette, for at gøre dem så uidentificerbare som muligt (s. 597-599).

Konsekvenser, det tredje princip, omhandler både mikro- og makrokonsekvenser (s. 597-599), og i dette speciales sammenhæng oversættes det til henholdsvis de individuelle informanter og de virksomheder, de er tilknyttede. Specialet adresserer individuelle konsekvenser ved at sikre fortrolighed og anonymitet for informanterne, som nævnt ovenfor. Virksomhedsmæssige konsekvenser anses som betydningsfulde for især dette speciale, da emnet IT-sikkerhed kan være et ømt emne for virksomheder i den sammenhæng, at offentliggørelse af angreb mod dem og sårbarheder i deres virksomheder kan skade deres omdømme, og dermed fremtidige kunderelationer, hvilket i sidste ende kan ramme dem på bundlinjen. Derudover kan deres specifikke sårbarheder være med til at øge cybertruslen for de medvirkende virksomheder, hvis informationer ender i hænderne på personer der har i sinde at bruge det imod dem, eksempelvis gennem cyberangreb. I sidste ende vil disse etiske overvejelser derfor være med til at undgå en potentiel forværring af cybertruslen mod SMV'er.

Det sidste princip vedrører forskerens rolle i interviewet, og hvordan forskerens holdning og fordomme kan påvirke resultaterne. Dette imødegås ved at anvende en åben interviewguide og tilstedeværelsen af to personer under interviewet, hvoraf den ene agerede som interviewer mens den anden suppleant og dermed kunne give feedback for at sikre en mest mulig objektiv proces (Brinkmann & Tanggaard 2020, s. 597-599). Det er også vigtigt at anerkende de magtrelationer, der kan opstå under et interview. Ved at overholde etiske retningslinjer kan disse magtrelationer mindskes, hvilket er afgørende for at sikre specialets validitet. Hvis ikke magtrelationerne tages i betragtning og imødegås tilstrækkeligt, kan det påvirke deltageres udsagn samt undersøgelsesområdet og dermed skade specialets validitet (Brinkmann & Tanggaard 2020, s. 597-599).

Kunstig intelligens

Brugen af kunstig intelligens (AI) til transskribering og analytisk sparring har rejst en række væsentlige metodologiske og etiske overvejelser. Anvendelsen af AI rummer dog både potentiale og begrænsninger, der nødvendiggør en kritisk refleksion over teknologiens rolle i den akademiske forskningsproces.

For det første indebærer brugen af AI til transskribering en potentiel risiko for datasikkerhed og fortrolighedsbrud. Da interviewmaterialet udgør en central del af specialets empiriske

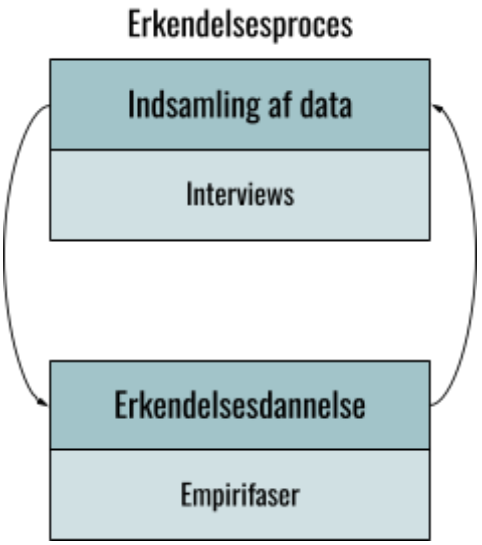
grundlag, er det afgørende at implementere stringente sikkerhedsforanstaltninger. Dette indebærer blandt andet korrekt anonymisering og en bevidsthed om, hvilke platforme der benyttes til transskriberingsprocessen. Aalborg Universitets retningslinjer for beskyttelse af personlige data understreger vigtigheden af, at sådanne oplysninger ikke deles på platforme, hvor forskeren mister kontrol over dataens behandling og opbevaring (Aalborg Universitetsbibliotek, u.å. -a). Derudover rummer AI-transskription en iboende fejlmargin og risiko for bias. Selvom AI kan levere hurtige og relativt præcise transskriptioner, kan algoritmernes forforståelser og begrænsninger medføre fejlfortolkninger, særligt når det gælder komplekse sproglige nuancer, dialekter eller kontekstafhængige betydninger. Derfor har det været nødvendigt at fastholde en kritisk tilgang til AI's output og supplere transskriptionerne med manuel efterbearbejdning for at sikre datakvalitet og validitet.

AI har også spillet en rolle i de erkendelsesfaser, hvor specialet har søgt at identificere mønstre og adskillelser i de tematikker, der er fremkommet gennem den empiriske analyse. Her har ChatGPT været anvendt som et analytisk støtteværktøj til at belyse sammenhænge og potentielle kategoriseringer af data. Det er dog væsentligt at understrege, at AI ikke har fungeret som en autonom fortolkningsinstans, men derimod som en supplerende ressource, der har assisteret den menneskelige analytiske proces. Dette er i tråd med Aalborg Universitets anbefaling om at anvende generativ AI som et tilladt hjælpemiddel, forudsat at brugen er dokumenteret og metodologisk begrundet (Aalborg Universitetsbibliotek, u.å.- b).

En central etisk problemstilling i brugen af AI til mønstergenkendelse er risikoen for at forstærke eksisterende bias eller skabe nye metodologiske blindvinkler. AI-algoritmer er trænet på store datasæt, der kan afspejle og videreføre strukturelle skævheder, hvilket kan påvirke fortolkningen af det empiriske materiale. Det er derfor nødvendigt med en kontinuerlig refleksion over, hvordan AI anvendes, samt en metodisk transparens omkring, hvilke dele af analysen der er påvirket af teknologien. I denne sammenhæng har vi beskrevet, hvordan AI er blevet anvendt i transskriberingsfasen og den efterfølgende analytiske proces. Dokumentationen af dette har omfattet en tydelig angivelse af, hvordan AI er blevet brugt til mønstergenkendelse og kategorisering af data, samt en vurdering af de potentielle bias og begrænsninger, der følger med denne anvendelse. En sådan dokumentation styrker forskningens troværdighed og sikrer, at AI anvendes i overensstemmelse med god akademisk praksis.

3.5 Erkendelsesprocess

Specialets erkendelsesproces bygger på den hermeneutiske spiral (Se afsnit 3.1 Videnskabsteoretiske Tilgang), da der er opstået flere nye erkendelser og forståelser undervejs i empiriindsamlingen. Nedenstående figur, som bygger videre på den tidligere figur i afsnit 3.3 Undersøgelsesdesign, belyser hvordan indsamling af data samt fortolkning af dette opstod i en iterativ erkendelsesproces. Det betyder, at gruppens empiriindsamling naturligt er påvirket af de observationer og indsigter, som der bliver tilegnet løbende.



Figur 6: Erkendelsesproces

Med inspiration fra Lisl Zachs artikel "Using a Multiple–Case Studies Design to Investigate the Information-Seeking Behavior of Arts Administrators" (2006) blev det besluttet før empiriindsamlingens begyndelse, at resultaterne fra allerede-udførte interviews burde være med til at styre retningen for fremtidig undersøgelse, resulterende i en iterativ tilgang. Dette var med til både at kunne ændre kurs efter behov, samt til at undgå datatab, da empiriindsamlingen foregik på over en måned, og vigtige tematikker kunne være gået tabt hvis analysen foregik til sidst. Dermed begyndte analyseprocessen allerede på uformel vis i første fase, hvor Gioia (2012)'s rammeværktøj (Uddybes senere i afsnit 3.7 Kodning) blev udvalgt som analysemetode og inkorporeret sådan, at 1st-order koncepterne og 2nd-order temaerne blev kodet én fase ad gangen. Processen blev struktureret i ugeblokke fra onsdag til og med tirsdag, i perioden fra uge otte til og med uge 12, kaldt *Empirifaser.* Der var altså i alt

fem faser, og for hver fase udførte specialegruppen en evaluering af ugens empiriindsamling med henblik på at identificere centrale tematikker og relevante pointer fra interviewene.

Temaerne blev præsenteret og diskuteret internt i gruppen for at sikre fælles forståelse og konsensus omkring fortolkninger, resulterende i opsummeringer, kaldet *Erkendelser*. De blev ajourført og samlet i gruppens fælles empirilogbog, som kontinuerligt afspejlede den seneste empiriske indsigt. De nye erkendelser blev derefter anvendt i resten af indsamlingsfaserne, for at undersøgelsen udviklede sig i takt med hvordan forskningsgruppens forståelser har udviklet sig løbende. For hver af de fem faser blev der beskrevet hvilke nye forståelser der opstod, og hvordan de blev anvendt i de næstkommende faser. Dette med det formål at skabe transparens om, hvordan erkendelserne opstod, og som en understøttelse for specialets udvikling.

3.5.1 Erkendelser

I dette afsnit præsenteres de centrale erkendelser fra empiriindsamlingen gennem en kombineret tilgang, der inddrager både en lineær kronologisk fremstilling af dataindsamlingen samt en tematisk redegørelse på tværs af hele forløbet. Denne metode giver et dobbelt overblik: Dels over, hvordan ny viden gradvist er opstået i takt med specialets fem Empirifaser, dels over de gennemgående temaer, der viste sig afgørende for IT-sikkerhed og træning af kompetencer dertil.

I den første dataindsamlingsrunde var de primære kilder formelle undervisere, uformelle organisationer og én SMV. Her identificeres et dobbeltsyn på cybertruslen, tydeliggjort af, blandt andre, en universitetsunderviser og formanden for en uformel forening: Et nationalt perspektiv med fokus på kritisk infrastruktur, og et virksomhedsperspektiv hvor økonomiske konsekvenser er styrende for SMV'en. I de uformelle læringsmiljøer opstod en erkendelse af, at tilgangen til struktur varierer betydeligt. Nogle frivillige organisationer bygger på åbenhed og lave adgangskrav, mens andre arbejder med mere formaliserede rammer og tydelige adgangskrav. Samtidig fremhævede både formelle og uformelle aktører behov for praksisnære læringsmetoder, herunder CTF og simulationsbaserede øvelser, som særligt effektive redskaber.

Disse erkendelser førte til et skærpet fokus på undervisningens indhold og organisering, især i forhold til IT-sikkerhed som modul eller fuld uddannelse i formelle sammenhænge. I de uformelle miljøer blev den tekniske og organisatoriske understøttelse af undervisningen undersøgt, herunder brugen af hardware og samarbejdsformer. Blandt SMV'er blev rekrutteringspraksis og netværk belyst, og det sociale aspekt i uformelle samlinger blev udforsket med fokus på engagement og fastholdelse.

Den anden fase omfattede en bredere gruppe informanter, herunder flere SMV'er, formelle institutioner og uformelle netværk. Gennem disse kilder fremgår det, at onlinefællesskaber, som Discord, ofte vejledte nye medlemmer om karriereveje som pentesting eller DevSecOps. Endvidere blev det tydeligt, at SMV'er generelt prioriterer generalister frem for specialister på grund af begrænsede ressourcer, mens praktisk erfaring og netværk anføres som vigtigere end certificeringer. Outsourcing blev samtidig nævnt som en mulig løsning, men kræver et vist teknisk overblik, så virksomheden kan stille rette krav til eksterne leverandører.

Anden fases erkendelser pegede på IT-sikkerhed som et fælles ansvar, hvor organisatorisk forankring og awareness-indsatser var centrale. Blandt SMV'er blev der fremhævet behov for generalister, begrænsede ressourcer og lav prioritering af sikkerhed. Netværk og faglige fællesskaber blev set som vigtige for videndeling og kompetenceløft. Disse observationer blev videreført i den efterfølgende undersøgelse af videndeling i netværk.

I tredje runde blev der foretaget et interview med en ekspert, en uformel forening og en SMV. Her viste det sig, at flere SMV'er indtager en reaktiv tilgang til IT-sikkerhed og først intensiverer sikkerhedsindsatsen efter et konkret cyberangreb. En af informanterne fremsatte ideen om en "andelsbevægelse for IT-sikkerhed", hvor virksomheder kunne dele ressourcer og knowhow, hvilket potentielt kunne kompensere for en manglende intern IT-specialisering. Samtidig påpegede en uformel netværksgruppe, at deres fokus mest rettede sig mod fællesskab og læring internt, frem for konkret rådgivning til SMV'er. Endelig blev intern IT-kompleksitet nævnt som en betydeligt trussel i virksomhederne, når der ikke foreligger en strategisk sikkerhedsorientering.

Erkendelserne fra denne runde pegede på behovet for kulturelle forandringer, og at tekniske løsninger alene ikke var tilstrækkelige. Disse observationer blev bragt med videre til fjerde

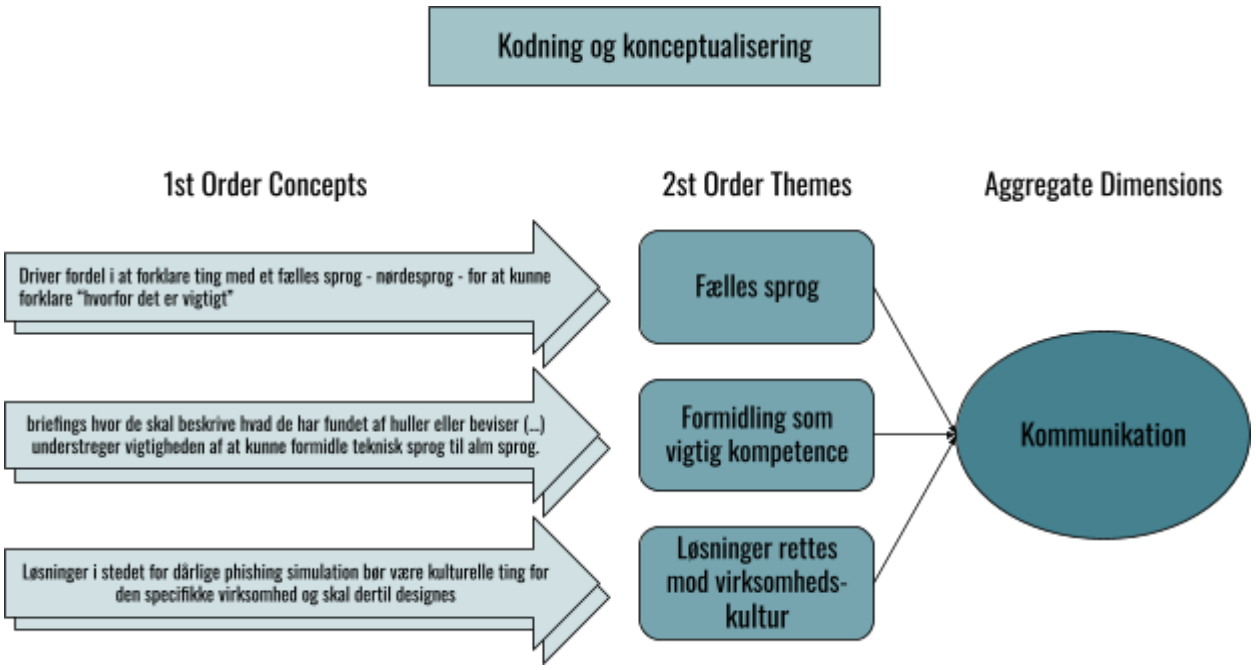
runde, hvor opmærksomheden blev rettet mod praktiske løsninger og organisatoriske strukturer.

Fjerde dataindsamling involverede seks informanter, der talte både SMV- eksperter, aktører fra formelle institutioner samt repræsentanter for uformelle organisationer. De peger samlet på, at mange SMV'er undervurderer cybertruslen, og ofte mangler basale tiltag såsom multifaktor-godkendelse og jævnlige systemopdateringer. Der er endvidere en mangel på specialiseret arbejdskraft samt en tendens til at betragte IT-sikkerhed som et isoleret, teknisk anliggende frem for et ledelsesansvar. Til gengæld blev NIS2 fremhævet som en lovmæssig ramme, der kan motivere SMV'er til at løfte sikkerhedsniveauet. Endeligt pegede erkendelserne fra denne runde på, at IT-sikkerhed ofte opleves som uoverskueligt blandt SMV'er, men at små tiltag kan gøre en stor forskel. Der blev samtidig peget på trusselsbias, manglende IT-kompetencer, urealistiske forventninger samt behovet for ledelsesmæssig opbakning. Forældet IT-infrastruktur blev desuden fremhævet som en væsentlig risiko. Disse indsigter dannede grundlag for den videre undersøgelse af løsninger og ledelsens betydning.

I den femte og sidste runde indgik blandt andet en formel underviser og flere aktører med branche- og politisk indsigt. Fokus var her på uddannelsesmæssige og politiske aspekter. Nogle informanter beskrev lav studenterdeltagelse og et behov for mere praksisnær opkvalificering, mens andre betonede, at et betydeligt antal SMV'er endnu ikke er gået aktivt ind i IT-sikkerhedsområdet. Offentlige-private partnerskaber og regulering, herunder NIS2, blev anskuet som nødvendige redskaber til at fremme et højere sikkerhedsniveau, ligesom rekruttering af flere specialister via politisk prioritering blev fremhævet.

3.7 Kodning

I dette speciale vil Gioia, Corley & Hamilton (2012) blive benyttet som analysemodel, da den er passende til at udføre kvalitative analyser samtidigt med, at den sørger for transparens i analyseprocessen. Denne tilgang er udviklet med henblik på at skabe "qualitative rigor" i induktiv forskning, samtidig med at den understøtter opdagelsen af nye koncepter og teorier. Metoden har vist sig særligt nyttig i studier, der bygger på semistrukturerede interviews, hvor formålet er at forstå og fortolke sociale eller organisatoriske fænomener på et dybdegående niveau.



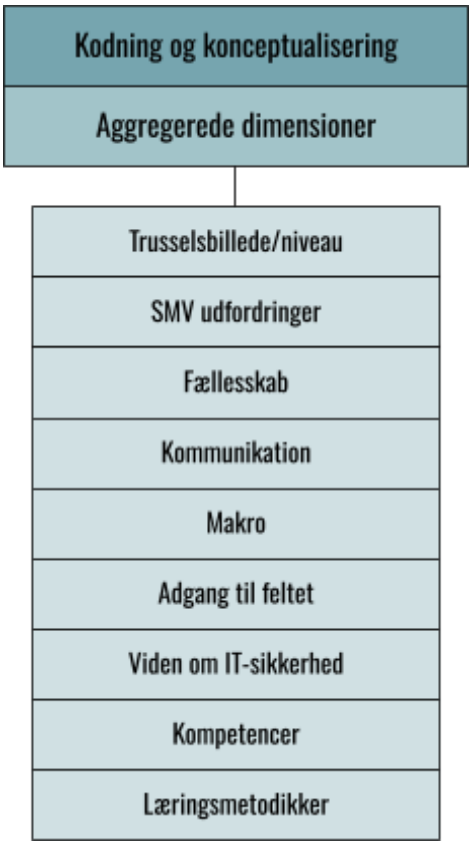
Figur 7: Kodningsprocess

Metoden beskrives ofte som en sekventiel proces, hvor 1st-order-koncepter (informanternes ord og termer), efterfølges af 2nd-order-temaer (forskernes mere teoretiske orienterede begreber). I den aktuelle undersøgelse blev denne rækkefølge dog ikke fulgt stringent, idet denne proces blev udført iterativt. Nedenfor redegøres for fremgangsmåden og begrundelserne herfor.

Kort efter hvert interview blev centrale pointer fra hvert interview noteret og sammenfattet i midlertidige 2nd-order-temaer. De centrale pointer var gruppens opsummering af vigtige nedslagspunkter og blev brugt som 1st-order-koncepter. Denne praksis afveg fra det klassiske Gioia-design på den måde, at der ikke blev fulgt en stringent, sekventiel 1st-order til 2nd-order tilgang, men hvor de begge blev dannet parallelt. Dette var nødvendigt, for at strukturere den store mængde data, og for at sikre, at væsentlige observationer og fortolkninger ikke forsvandt mellem interviewene.

Efterfølgende blev 2nd-order-temaerne gennemgået i en revurdering- og bekræftelsesproces hvor de blev sammenholdt med de fulde transskriptioner i Nvivo. Her blev eksisterende temaer tilpasset, slået sammen, og styrket på baggrund af yderligere tilføjelse af citater fra transskriptionerne fra alle 21 interviews.

Efter gennemførelsen af ovenstående blev 2nd-order-temaer sammensat til en mindre gruppe overordnede dimensioner, kaldet aggregerede dimensioner. Her blev beslægtede temaer samlet, mens mere særprægede temaer blev placeret for sig, hvis de indeholdt unikke perspektiver. Denne fase generede en samlet begrebsramme til at fortolke de væsentligste fund fra undersøgelsen. Gennem denne indsats identificerede gruppen følgende aggregerede dimensioner 1) Trusselsbilledet, 2) Makro, 3) Adgang til feltet, 4) SMV-udfordringer, 5) Lærings Metodikker 6) Fællesskab, 7) Viden om IT-sikkerhed, 8) Kommunikation og 9) Kompetencer.

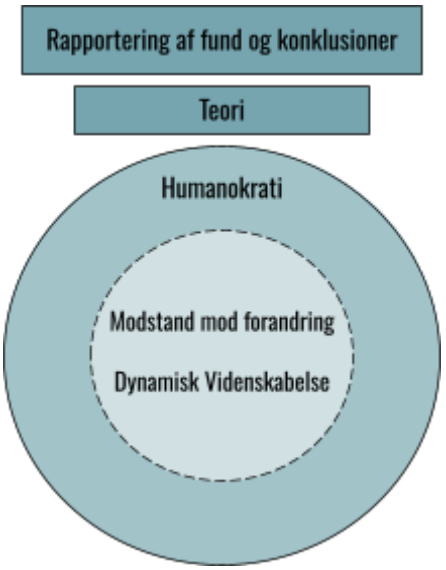


Figur 8: Aggregerede dimensioner

Selvom metoden i praksis adskiller sig lidt fra den klassiske fremstilling af Gioia-metoden, er de bærende principper fortsat opfyldt, direkte afsæt i informanternes eget sprog og en stræben efter gennemsigtighed i datahåndtering. Den iterative proces var et bevidst valg, der havde til formål at udnytte de umiddelbare indtryk fra interviewene optimalt og samtidig skabe plads til en forankring af temaerne i de faktiske transskriptioner. Den praksis har fremmet en åben tilgang, hvor både formelle og uformelle koncepter samt temaer fik lov at opstå og blive revideret flere gange undervejs i analysearbejdet.

4 Teori

Dette afsnit vil redegøre for de tre anvendte teoretiske rammeværktøjer i specialet. De tre teorier, Humanokrati (Hamel & Zanini, 2020), SECI-modellen (Nonaka, 1994) og Modstand mod Forandring (Maurer, 2010) vil blive benyttet til at understøtte analysens fund og bidrager til at løfte forståelsen af problematikken til et højere analytisk niveau både individuelt og i samspil med hinanden. Hvor Nonakas SECI-model og Maurers Modstand mod Forandringsteori anvendes til at identificere konkrete muligheder, løsninger og barrierer i praksis, fungerer Humanokrati i højere grad som et overordnet perspektiv og strategisk mindset. Humanokrati bidrager ikke med operationelle værktøjer på samme måde som de to andre teorier, men løfter blikket og stiller grundlæggende spørgsmål ved de strukturelle og kulturelle rammer, som præger arbejdet med IT-sikkerhed. Denne forskel i anvendelsesniveau og teoretisk funktion er illustreret i *Figur 9*, der viser placeringen af de tre teorier i analysen.



Figur 9: Teoretisk rammeværktøj

Humanokrati-perspektivet inddrages for at belyse, hvordan øget medarbejderinvolvering, fladere strukturer og selvstyring kan styrke organisatorisk læring, tilpasningsevne og engagement i IT-sikkerhedsarbejdet. Det anvendes desuden til at undersøge, hvilke bureaukratiske principper der modvirker en stærk IT-sikkerhedskultur, samt hvordan og hvorvidt Humanokrati-principper kan ændre det eksisterende paradigme og fremme en mere sikkerhedsorienteret organisationskultur.

SECI-modellen og Modstand mod Forandring understøtter en nærmere operationel afdækning af empirien. Nonakas SECI-model for vidensudvikling bruges til at forstå, hvordan viden om IT-sikkerhed skabes, deles og forankres i organisationer og gør det muligt at analysere, hvordan både tavs og eksplicit viden fra uddannelser, samlinger og branchefællesskaber kan omsættes til organisatorisk læring og styrke IT-sikkerhed i SMV'er. Rick Maurers teori om Modstand mod Forandring anvendes til at identificere og analysere de menneskelige og organisatoriske barrierer, der kan opstå, når nye IT-sikkerhedspraksisser skal implementeres i SMV'er. Maurers tre niveauer af modstand: *I don't get it, I don't like it* og *I don't like you,* giver mulighed for at undersøge, hvordan modstand kan opstå i forbindelse med introduktion af ny viden og praksis fra både formelle og uformelle læringsrum vedrørende IT-sikkerhed. I samspil med empirien danner de grundlaget for analysen af, hvordan viden og praksisser fra nuværende formelle og uformelle uddannelser og samlinger kan benyttes af SMV-segmentet i Danmark til at imødekomme det stigende IT-sikkerhedsbehov.

4.1 Humanokrati

Humanokratiet skal forstås som et modsvar til det bureaukrati, der præger mange af nutidens virksomheder. Gennem analogier og konkrete eksempler søger teorien at adressere de udfordringer, som bureaukratiet har skabt, og samtidig tilbyde alternative løsningsmodeller.

Gary Hamel og Michele Zanini argumenterer for et opgør med bureaukratiet i bogen Humanokrati, hvor de opbygger et teoretisk grundlag for, hvordan organisationer kan anvende principperne fra humanokrati til at skabe et rum, hvor energi, kreativitet, innovation og modstandsdygtighed kan trives. De hævder, at bureaukrati er et levn fra fortiden, som endnu ikke er blevet gjort op med, og som derfor hæmmer organisationers evne til at følge med verdens konstante udvikling (s. 25-26).

Dette speciale har valgt at anvende deres syv principper, Meritocracy, Markets, Community, Openness, Experimentation, Paradox og Ownership, til at analysere informanternes udsagn, indsamlet gennem interviews. Hvert princip kan anvendes til at belyse empirien individuelt, men står stærkest i kombination, da de understøtter hinanden. Samlet set understøtter principperne et forslag til, hvordan SMV'er kan modstå den stigende cybertrussel.

De syv principper bygger ikke på at forstå, hvordan andre gør tingene anderledes, men på at forstå, hvordan de tænker anderledes (s. 238). Denne tankegang kan styrke organisationer fundamentalt. Hamel og Zanini sammenligner dette med, hvordan filosoffer i 1800-tallet udfordrede etablerede værdier og gentænkte samfundet. Tilsvarende skal humanokratiske principper gentænke vores tilgang til arbejde og ændre organisatoriske mønstre til noget mere bæredygtigt (s. 239-240). Grundlæggende beskriver de dette som en ændring af organisationens "DNA", ikke blot en ændring af vaner (s. 244). Den følgende tekst vil udfolde de syv principper og illustrere, hvordan de kan anvendes i SMV'ers kontekst. I denne sammenhæng fokuseres der på, hvordan principperne kan forstås og anvendes til at styrke cyberresiliens i SMV'er gennem viden og praksisser fra både formelle og uformelle cybermiljøer i Danmark.

4.1.1 Humanokratiets syv principper

Ownership: Begrebet ownership beskrives som en drivkraft, der understøtter individets evne til at skabe forandring, forudsat at vedkommende får ejerskab over en proces, et projekt eller lignende. Hamel og Zanini henviser til forskning af Dirk Van Dierendonck og Ine Nuijten, der viser, at autonomi og gainsharing, en belønningsmodel, hvor medarbejdere deler gevinster ved forbedret performance eller effektivitet i organisationen, har en positiv korrelation: Medarbejdere, der oplever ansvar og ejerskab i organisationen, motiveres i højere grad af netop autonomi og ansvar (s. 255–257). Princippet giver mulighed for at udforske, hvordan fordelingen af ansvar i ressourcebegrænsede SMV'er påvirker medarbejdernes motivation og holdbarheden af IT-sikkerhedsindsatser. Det åbner samtidig for en diskussion af, om ejerskab placeres individuelt, kollektivt eller forbliver diffust, og hvilke organisatoriske dynamikker dette afføder.

Markets: Begrebet markets forklares med reference til aktiemarkedets funktion. Det er ikke en enkeltpersons opfattelse, der bestemmer en akties værdi, men markedet som helhed, der gennem sin samlede viden og forståelse danner et prissignal (s. 274). Hamel og Zanini bruger dette som en metafor for organisatorisk beslutningstagning, hvor få seniorledere ofte sætter kursen for hele organisationen. Dette skaber risiko for blinde vinkler, da der sjældent gives rum for indsigelser (s. 274-275). Yderligere fremhæver de, hvordan beslutningstagere kan være ramt af confirmation bias og dermed have en tendens til at favorisere deres egne idéer, hvilket igen kan føre til ineffektive beslutninger (s. 278-280). Markets metaforen, kan belyse,

hvorvidt kollektive signaler om risiko, omkostninger og best practice påvirker beslutningsniveauet i SMV'er, eller om lav viden og confirmation bias udvander disse signalers værdi. Dermed kan det undersøges hvordan vidensudveksling i formelle og uformelle netværk former IT-sikkerhedsstrategier.

Meritocracy: Meritocracy beskrives som en idealtilstand, hvor vertikal mobilitet i organisationer baseres på evner og præstationer frem for politisk ageren. Hamel og Zanini henviser til en undersøgelse i Harvard Business Review, hvor 76 % af større virksomheder angiver, at politisk spil har stor indflydelse på, hvem der forfremmes, i modsætning til et meritokratisk system, hvor kompetencer, erfaring og resultater er de bærende faktorer (s. 298–299). De argumenterer desuden for, at mennesker har en tendens til at overvurdere egne evner. Denne fejlvurdering skader organisationens evne til innovation og udvikling, fordi det ofte er beslutningstagere med overvurderet selvtillid, der sætter kursen, uden at mange andre inddrages i processen. Meritocracy gør det muligt at diskutere, om praktisk demonstrerede færdigheder og resultater i realiteten vægtes højere end formelle certifikater og politisk magt i en organisation, og hvordan denne vægtning præger fordelingen af indflydelse og ansvar.

Community: Ifølge Hamel og Zanini er dette princip en grundlæggende del af menneskets natur, hvilket også anerkendes i Maslows behovspyramide, hvor behovet for tilhørsforhold placeres lige over de mest basale behov som mad og sikkerhed (s. 332–333). De illustrerer begrebet gennem eksempler som Alcoholics Anonymous og StrivePartnership, der begge bygger stærke netværk med det formål at løse komplekse problemer. De identificerer fire centrale elementer i denne tilgang: 1) Klarlæg fælles, målbare resultater, som er vigtige for aktørerne i fællesskabet, 2) identificer relevante målgrupper, som skal inddrages, 3) afklar, hvilke kompetencer de forskellige parter har brug for og 4) sammensæt tværfaglige teams og støt dem i løbende, erfaringsbaseret læring (s. 340). Selvom alkoholisme og skoleudvikling er forskellige kontekster, viser begge eksempler, hvordan fællesskaber kan løse komplekse, ikke-rutineprægede problemer. I afsnittet "Getting Started" understreger forfatterne desuden vigtigheden af interpersonelle relationer præget af sårbarhed og ærlighed som en styrke for opbygningen af fællesskab (s. 367). Ydermere synliggør princippet, hvordan uformelle samlinger kan fungere som lærings- og motivationsplatforme, men også hvilke mekanismer der kan hæmme kollektiv vidensdeling og engagement i SMV'er.

Openness: Til at beskrive openness anvender Hamel og Zanini en analogi: En levende by rummer mangfoldighed i, hvordan mennesker tænker, klæder sig, tror, arbejder, elsker og morer sig. Denne diversitet skaber et næsten uendeligt kombinationsrum, hvor idéer, talenter og ressourcer kan bringes i spil på nye måder (s. 369). Dette perspektiv står i kontrast til det, de betegner som closed minds, hvor Thomas Kuhn, amerikansk filosof og historiker, fremhæver, at mennesker ofte er fanget i deres egne paradigmer. Dette underbygger pointer om bias og vores tendens til at tænke inden for snævre rammer (s. 375–376). Openness handler derfor om at være åben overfor nye perspektiver og modvirke ekkokamre, hvilket styrker innovationskraften. Openness belyser betydningen af organisatorisk gennemsigtighed, idet nogle SMV'er deler deres læring fra sikkerhedshændelser åbent, mens andre udviser tilbageholdenhed. Det er dermed interessant at benytte dette princip til at belyse hvordan forskellige grader af åbenhed påvirker læringshastighed, tillidsrelationer og opfattelser af trusselsbilledet.

Experimentation: Forfatterne fremhæver, at manglen på eksperimentation er en af organisationers største svagheder. Udvikling forudsætter viljen til at eksperimentere, men selv med denne erkendelse er virksomheder ofte tilbageholdende med at understøtte medarbejdere, der ønsker at lære gennem praksis (s. 411). Typisk er eksperimentering begrænset til Research & Development-afdelingen, hvilket udelukker den brede medarbejderstab fra at bidrage med deres viden til løsning af problemer (s. 412). Dette kan skyldes frygt for risiko, hvis afkastet ikke er klart, er ledelsen ofte tilbageholdende med at investere (s. 413). Hamel og Zanini argumenterer derfor for, at alle medarbejdere bør have mulighed for at eksperimentere, og at barrierer, der forhindrer dette, skal fjernes (s. 430). Princippet fremhæver potentialet for små, kontrollerede tests som katalysator for organisatorisk læring, men peger samtidig på risiko, frygt og ressourceknaphed som mulige barrierer. Hermed tilbydes et afsæt for at diskutere, hvorvidt eksperimentel praksis kan integreres uden at eskalere driftsmæssig usikkerhed.

Paradox: Tidsmangel er ofte den største barriere: Skal jeg færdiggøre en opgave, eller skal jeg prioritere noget andet? Hamel og Zanini bruger begrebet paradox til at illustrere denne type dilemma, som vi alle møder i prioriteringen af vores tid (s. 434–435). De henviser til Handelsbanken som eksempel på integrativ tænkning, hvor beslutninger ikke træffes ud fra et enten-eller (trade-offs), men som både-og. Ved at decentralisere beslutningskraften og give afdelingerne indsigt i deres cost-income-ratio blev de bedre rustet til at identificere og

håndtere paradokser (s. 452–460). Afslutningsvis definerer de paradox som balancen mellem frihed og kontrol, og de argumenterer for, at alle i organisationen bør lære at tænke i paradokser for at styrke helhedsforståelsen og beslutningskraften. Paradox begrebet tydeliggør spændingsfeltet mellem forretningskrav om hurtig tilpasning og behovet for robuste sikkerhedsforanstaltninger. Det muliggør en nuancering af, om SMV'er formår at udvikle holistiske strategier, eller om de fanges i monolitiske løsninger.

Samlet set illustrerer Humanokratiets syv principper, at virksomheder bør gentænke deres beslutningsprocesser. En top-down-tilgang risikerer at skabe beslutningsgrundlag, der er for langt fra de konkrete udfordringer og løsninger, som ofte allerede findes blandt medarbejdere. Disse medarbejdere besidder både indsigt i paradokserne og adgang til den samlede viden, der eksisterer i organisationen.

4.2 Dynamisk Videnskabelse

For at forstå, hvordan viden om IT-sikkerhed opstår, deles og omsættes i praksis blandt SMV'er og i uformelle læringsmiljøer, inddrages Nonakas SECI-model (1994). Modellen tydeliggør, hvordan tavs og eksplicit viden cirkulerer i organisationer gennem en spiralformet proces. Nonakas teori giver et perspektiv på vidensdannelse som en dynamisk og kontinuerlig proces, der involverer interaktion mellem to vidensformer: tavs viden, som er implicit, erfaringsbaseret og ofte ubevidst, og eksplicit viden, der er formel artikuleret og dokumenterbar. Denne videnskabelsesproces illustreres i Nonakas teori gennem SECI-modellen, der beskriver fire forskellige måder, hvorpå viden omdannes. Den første af disse er *socialisering*, der er tavs viden, der deles gennem personlige interaktioner og fælles oplevelser mellem individer, typisk via observation, imitation og praktisk deltagelse i opgaver. Denne dimension kræver fysisk nærhed og direkte kontakt. Dernæst kommer *eksternalisering*, der er tavs viden der omsættes til eksplicit viden ved hjælp af kommunikation og dialog, hvor individer artikulerer deres erfaringer og opfattelser. Her er metaforer, analogier og storytelling særligt nyttige redskaber til at synliggøre ellers skjulte aspekter af viden. Den tredje måde er *kombinering* som er overførslen af eksplicit viden til eksplicit viden, og integreres og struktureres gennem formelle processer, såsom dokumentation, databaser, manualer og guidelines. Denne dimension fokuserer på systematisering af viden, der allerede er artikuleret og synliggjort. Den sidste måde er *Internalisering* der er eksplicit viden der integreres i medarbejdernes adfærd og

arbejdspraksis, hvorved den igen bliver tavs viden gennem rutiner, vaner og praksis anvendelse. Denne proces sker gennem praktisk erfaring og gentagelser.

SECI-modellen illustrerer desuden en spiralformet proces, hvor viden konstant skabes, deles og udvikles i organisationen gennem gentagne iterationer af de fire dimensioner. Denne spiraldynamik sikrer, at videnskabelse er en kontinuerlig og progressiv proces, der kan føre til organisatorisk innovation og læring over tid.

I Nonakas teori er det individet, ikke organisationen som helhed, der er den primære skaber af ny viden. Organisationens rolle er at understøtte, forstærke og dele denne viden. Derfor er individets *commitment* essentielt i vidensdannelsesprocessen. *Commitment* opstår gennem tre nøgleelementer: *Intention,* der henviser til det strategiske formål eller den målsætning, organisationen har for videnskabelsen. Intention sikrer tilmed, at vidensprocesser er målrettede og fokuserede på at opnå bestemte organisatoriske resultater. *Autonomi*, som refererer til graden af frihed og råderum, medarbejdere har til at udforske, eksperimentere og tage initiativ i videnskabelsesprocessen. Høj autonomi fremmer også kreativitet, innovation og motivation hos medarbejdere hvor *Miljømæssige fluktuationer* beskriver vigtigheden af dynamiske og fleksible omgivelser, hvor organisationen er modtagelig for forandringer og nye udfordringer. Disse fluktuationer skaber incitamenter til læring og vidensudvikling ved at udfordre eksisterende rutiner og opfordre til innovative løsninger. Det er dog vigtigt at være opmærksom på, at en effektiv videnskabelsesproces fordrer en aktiv dialog mellem tavs og eksplicit viden. Manglende kobling mellem disse kan skabe udfordringer: Ren kombinering af eksplicit viden, risikerer at blive overfladisk og uden tilknytning til den konkrete praksis, hvilket hæmmer dens anvendelighed og videreudvikling i organisationen. Omvendt kan ren socialisering begrænse videns delbarhed, da tavs viden skabt i specifikke sociale kontekster ofte er svær at overføre og anvende uden for disse rammer. Derfor er balancen og samspillet mellem de forskellige vidensformer afgørende for at sikre, at viden ikke blot eksisterer, men også kan deles, anvendes og udvikles i en bredere organisatorisk sammenhæng. Samlet set giver Nonakas teori en omfattende og dybdegående forståelse af, hvordan organisationer kan facilitere og understøtte effektiv videnskabelse gennem strategisk fokus, medarbejderautonomi og en organisatorisk kontekst præget af dynamik og tilpasningsevne.
Dynamisk Videnskabelse anvendes til at belyse, hvordan viden om IT-sikkerhed opstår, deles og forankres i organisatorisk praksis. Modellen er relevant i denne kontekst, da den muliggør en analytisk forståelse af, hvordan både tavs og eksplicit viden bevæger sig mellem individ

og organisation i iterative processer. Dette er centralt i forhold til specialets fokus på uformelle og formelle læringsmiljøers bidrag til SMV'ers vidensdannelse inden for IT-sikkerhed.

4.3 Modstand mod forandring

Følgende afsnit introducerer Rick Maurers teori om modstand mod forandring, og redegør for hans tredeling af modstand samt for hans begreber om synlig og usynlig modstand. Endvidere præsenteres de otte specifikke udtryksformer for modstand, som Maurer identificerer. Teorien vil i analysen blive anvendt som fortolkningsramme til at forstå og kategorisere modstand mod IT-sikkerhedsinitiativer i danske SMV'er, med henblik på at undersøge både årsager og udtryk af modstand.

Rick Maurer (2010) tilbyder en praksisnær og psykologisk forankret forståelse af modstand mod forandring, som er særligt relevant i organisatoriske sammenhænge. Han skelner mellem tre grundlæggende former for modstand: "I don't get it", "I don't like it" og "I don't like you". Disse tre former udgør forskellige indgangsvinkler til at forstå, hvorfor forandringer i organisationer, i dette tilfælde teknologiske og sikkerhedsmæssige tiltag, ofte møder modstand.

Den første form, *I don't get it*, beskriver en kognitiv barriere, hvor modstand opstår, fordi forandringen ikke er forstået. Det kan skyldes uklar kommunikation, utilstrækkelig formidling eller en kompleksitet, der gør det svært at gennemskue nødvendigheden og konsekvenserne af forandringen. Her bliver modstanden et resultat af usikkerhed og misforståelser, som kan føre til passiv tilbageholdenhed snarere end direkte protest fra aktørerne. Den anden form, *I don't like it*, handler om følelsesmæssig modstand. Her er forandringen forstået, men det afføder ubehag, frygt eller bekymring. Forandringen opleves som en trussel mod det velkendte og kan vække modvilje mod at opgive rutiner, rolleforståelser eller oplevelsen af kontrol i arbejdslivet. Den tredje form, *I don't like you*, retter sig ikke mod forandringens indhold, men mod dens afsender. Tidligere dårlige erfaringer, lav tillid til beslutningstagere eller følelsen af at være blevet overset i beslutningsprocessen kan give anledning til en modstand, som i højere grad er relationel end indholdsmæssig (s. 38-41).

Maurer fremhæver, at modstand ikke nødvendigvis skal ses som en forhindring, når den anerkendes og håndteres konstruktivt, kan den blive en værdifuld ressource i forandringsprocessen. I stedet for at se modstand som barrierer, opfordres der til at betragte det som engagement, der viser, at folk aktivt forholder sig til forandringen. I don't get it indikerer et behov for bedre kommunikation, I don't like it peger på vigtige bekymringer, og I don't like you inviterer til at arbejde med relationer og tillid. Ved at tage modstand alvorligt kan man adressere dette på en mere målrettet og meningsfuld måde .

En væsentlig dimension i Maurers tilgang er hans opmærksomhed på forskellen mellem synlig og usynlig modstand. Hvor nogle former for modstand udtrykkes åbent og direkte, kan andre være skjulte og komme til udtryk gennem stiltiende modarbejdelse, lavt engagement eller fravær. Denne mere nuancerede forståelse åbner op for, at ledere og forandringsagenter kan adressere modstand på en mere målrettet og meningsfuld måde. For at understøtte denne pointe beskriver Maurer otte konkrete former for modstand, som spænder fra det åbenlyse til det subtile. Han præsenterer her *confusion*, hvor mangel på forståelse dækker over en modstræben med forandring, samt *immediate criticism,* hvor der afvises nye ideer uden overvejelse, som kan munde i tidligere erfaringer. Endvidere beskrives *denial* samt *deflection* af forandringen som viser sig ved fornægtelse af, om der er behov for forandring mens *malicious compliance* og *sabotage* dækker over handlinger der tilsyneladende støtter forandringen, men i praksis underminerer den ved eksempelvis at være for rigid eller bogstavelig i udførsel eller en medarbejder bevidst undlader at videredele information om vigtige ændringer og skaber forvirring omkring nye arbejdsgange. Yderligere kommer *easy agreement*, hvor man udtrykker støtte uden reel engagement, *silence*, som kan skjule passiv modstand, samt *in-your-face criticism*, der er direkte og konfronterende. Ved at kende og kunne genkende disse former, skaber det bedre forudsætninger for at navigere i og håndtere modstand effektivt og konstruktivt (s. 45-49).

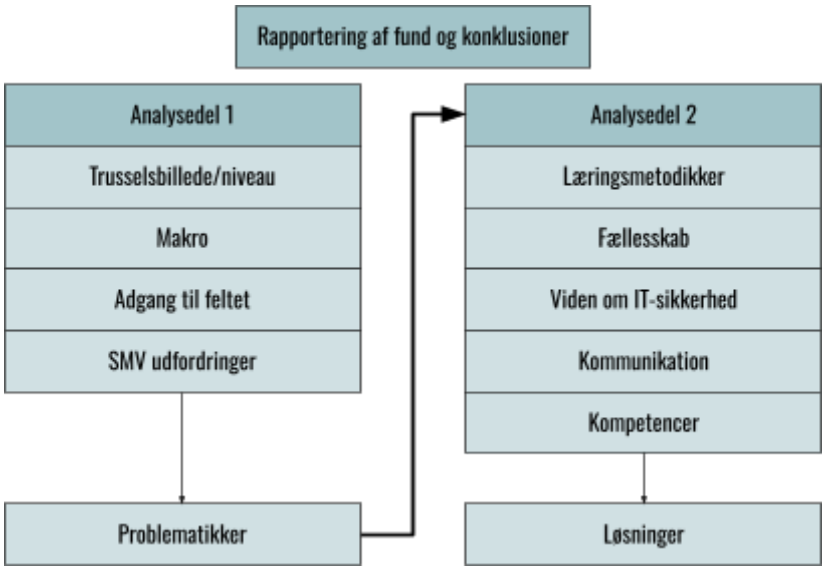
I dette speciale anvendes Maurers teori som analytisk ramme til at undersøge modstand mod IT-sikkerhedsinitiativer i danske SMV'er. Selvom trusselsbilledet skærpes, viser det sig ofte, at virksomheder i dette segment er tilbageholdende med at implementere sikkerhedsforanstaltninger eller investere i IT-sikkerhed. Ved at anvende Maurers begreber som fortolkningsnøgle søger undersøgelsen at afdække, om denne modstand skyldes manglende forståelse for trusler og løsninger, følelsesmæssige reaktioner på potentielle ændringer i arbejdsrutiner og ansvar, eller modvilje mod rådgivere og myndigheder, der

formidler forandringerne. Målet er at skabe indsigt i, hvordan modstand mod IT-sikkerhed i SMV'er kan forstås og imødekommes.

5 Analyse

Følgende afsnit har til formål at besvare specialets problemformulering: *Hvilken viden og hvilke praksisser fra nuværende formelle og uformelle uddannelser og samlinger kan benyttes af SMV-segmentet i Danmark til at imødekomme det stigende IT-sikkerhedsbehov?* Dette gøres ved at opdele analysen i to dele. Den første del har til formål gennem en empirisk analyse at belyse fire af de ni aggregerede dimensioner: 1) Trusselsbilledet, 2) Makro, 3) Adgang til feltet og 4) SMV-udfordringer. Her ønskes det at afdække, og rammesætte, hvilke problematikker der ifølge specialets informanter eksisterer i det danske IT-sikkerhedslandskab, særlig i relation til SMV'er, samt undersøge potentielle barrierer for introduktion af nye fagfolk til feltet.

Anden del af analysen vil bruge de empiriske fund fra del 1 til at gå i dybden med de andre fem aggregerede dimensioner: *Fællesskab, kommunikation, viden om IT-sikkerhed, kompetencer og læringsmetodikker,* gennem en teoretisk analyse. Hvor første del af analysen omhandler generelle problematikker og barrierer, har anden del af analysen fokus på viden og praksisser fra de formelle og uformelle samt SMV'erne og hvordan disse kan anvendes til at understøtte fundene fra første analysedel.



Figur 10: Analyse opdeling

Samlet vil opdelingen af disse to analytiske perspektiver besvare specialets problemstilling ved først at identificere og forstå udfordringerne, og dernæst, med udgangspunkt i empirisk forankring, at undersøge, hvordan eksisterende viden og læringspraksisser kan operationaliseres som løsninger. Dermed sikrer strukturen en logisk og analytisk progression, der samlet set kvalificerer besvarelsen af specialets problemformulering.

5.1 Analysedel 1

5.1.1 Trusselsbilledet

Følgende dimension har til formål at belyse, hvilke trusler og trusselsaktører informanterne beskriver som særligt prævalente for Danmarks kritiske infrastruktur samt for danske SMV'er. Angrebsmønstre fra hackere er blevet mere komplekse og udbredte i takt med den stigende digitalisering af samfundet. En informant nævner eksempelvis teknologisk udvikling, såsom kvantecomputere, som udfordrer den kryptering, vi i dag opfatter som sikker, ved at kunne bryde dekrypteringsnøgler på få sekunder (Bilag 8, l. 216-218). Et svagt digitalt fundament, hvor IT-sikkerhed ikke altid har været tænkt ind fra starten, har gjort kritisk infrastruktur sårbar, som eksemplificeret med Ruslands evne til at ramme den ukrainske energisektor (Bilag 1, l. 423-437). Samtidig er spredningen af falske informationer blevet nemmere, hvilket truer demokratiske værdier og understreger behovet for, at alle borgere besidder en grundlæggende forståelse for IT-sikkerhed, hvilket gør behovet for IT-sikkerheds kompetencer til et samfundsanliggende (Bilag 2, l. 453-457). De konstante angreb har gjort det tydeligt for organisationer, at de har mistet overblikket over deres IT-infrastruktur på grund af en stigende kompleksitet i deres IT-systemer. Dette gør det svært at vide, hvad de skal beskytte sig imod, fordi de ofte ikke er bevidste om deres egne sårbarheder (Bilag 12, l. 154-160;364-366). Et konkret eksempel er private og organisatoriske wifi-access points, som ofte er tændt hele døgnet og dermed giver hackere mulighed for at finde og udnytte sårbarheder uden for normal arbejdstid (Bilag 14, l. 166-175). Især SMV'er er udsatte, da de ofte mangler ressourcer og derfor er sårbare over for ransomware, datalæk og afpresning. Flere SMV'er udtaler sig desuden om frygten for phishing og mener, at det kan have den største konsekvens for deres virksomhed (Bilag 9, l. 71-75). Dette bekræftes af eksempler, hvor skoler har klikket på phishing-mails og derved utilsigtet givet hackere

adgang til virksomhedens systemer (Bilag 10, l. 131-134). En anden SMV fortæller, at de dagligt modtager phishing-mails og har oplevet, at deres hjemmeside blev hacket, heldigvis med mulighed for genetablering (Bilag 13, l. 123-132). Malware leveres ofte netop gennem kompromitterede mailkonti, og derfor er det helt centralt at have styr på den basale cyberhygiejne (Bilag 15, l. 85-90). Hvor SMV'er typisk trues af mere simple aktører, står større organisationer, der håndterer kritisk infrastruktur, over for mere sofistikerede angreb fra såkaldte Advanced Persistent Threats (APT), statsstøttede aktører som Kina, Rusland og Iran, der har både ressourcer og højt specialiserede kompetencer (Bilag 15, l. 94-99). Selvom SMV'er typisk ikke er mål for APT'er, kan de stadig gøre det betydeligt sværere for mindre avancerede trusselsaktører at trænge ind og kan få dem til at vælge lettere mål i stedet, hvis de får en god cyberhygiejne (Bilag 15, l. 183-186). Et fund i sammenligningen mellem SMV'ers opfattelse af det trusselsbillede, de står overfor, som oftest beskrives som phishing, stemmer ikke overens med de formelle og uformelle informanters vurdering af de mest relevante trusler. Informanterne fremhæver i stedet kompleksitet, ransomware, sårbare wifi-access points, kompromitterede konti og manglende cyberhygiejne som centrale angrebsmønstre, hvor phishing blot udgør én blandt mange mulige angrebsformer.

5.1.2 Makro

Denne dimension fremhæver hvilke makrofaktorer, eksempelvis regulative forhold, der kan påvirke danske organisationer både i en positiv og negativ retning mod et styrket IT-sikkerhedsniveau.

Flere mindre virksomheder påvirkes indirekte af NIS2-lovgivningen, fordi det stilles som krav af de brancher eller større kunder, de samarbejder med. Dette medfører mere generelle krav til virksomhedens tilgang til IT-sikkerhed, hvilket samtidig skaber et bedre udgangspunkt for IT-ansvarlige til at argumentere for nødvendige sikkerhedsinitiativer over for ledelsen (Bilag 9, l. 320-324). En informant fremhæver, at selvom arbejdet med NIS2 og tilhørende compliance kan opleves som administrativt tungt, skaber det i sidste ende værdi i form af øget IT-sikkerhed. Derudover argumenteres der for, at det er nødvendigt med politisk regulering for at hæve det generelle IT-sikkerhedsniveau (Bilag 9, l. 384-387;392-394). En anden informant bakker dette op og påpeger, at det ofte er økonomiske argumenter, der spænder ben for investering i sikkerhed, men at virksomhederne i virkeligheden ikke har råd til at lade være (Bilag 12, l. 461-473). En tredje informant tydeliggøre dette ved at italesætte,

at mange SMV'er ikke nødvendigvis er direkte underlagt NIS2, men presses til at leve op til kravene af større kunder, som stiller compliance som betingelse for fortsat samarbejde, alternativet kan være at miste kunden (Bilag 18, l. 469-475). Samtidig fremhæves det, at store virksomheder som Salling Group har påbegyndt en aktiv dialog med deres leverandører og støtter dem i at blive NIS2-compliant, da de har behov for at sikre hele deres værdikæde. Derved går de foran i processen og bidrager til at løfte IT-sikkerhedsniveauet blandt deres samarbejdspartnere (Bilag 20, l. 259-273). Dette kan desuden give en konkurrencefordel i forhold til leverandører, som endnu ikke lever op til kravene (Bilag 20, l. 426-440).

Mens NIS2-lovgivningen udspringer af EU, er der samtidigt nationale politikker og indsatser, eller mangel på samme, som har været med til at danne det digitale fundament vi som samfund har nu. Flere informanter har udtalt sig om en historisk forsømmelse af IT-sikkerhedsområdet, hvor en informant beskriver, hvordan IT-sikkerhed i mange år er blevet ignoreret på politisk niveau. I stedet er det primært Industriens Fond, der har investeret aktivt i området, dog med et snævert fokus på SMV-segmentet (Bilag 1, l. 387-392). Dette har, som tidligere beskrevet, medført et svagt IT-sikkerheds fundament, hvor en anden informant fremhæver, at ligesom basal cyberhygiejne kan afskrække trusselsaktører, kan et stærkt nationalt IT-forsvar virke præventivt mod mere avancerede trusler (Bilag 1, l. 487-488). Særligt den kritiske infrastruktur, herunder telesektoren, energisektoren og fibernet, er ifølge flere informanter særligt udsat, hvilket også fremgår af NIS2's sektorprioritering (Bilag 15, l. 92-99). En informant understreger i forlængelse heraf, at de samfundsmæssige udfordringer, Danmark står overfor, ikke kan løses individuelt, men kræver kollektiv indsats og samarbejde på tværs af sektorer (Bilag 20, l. 91-93). Denne pointe følges op med en appel om, at også staten, og ikke kun private aktører som Industriens Fond, skal bidrage aktivt og økonomisk til opbygningen af et robust digitaliseret samfund (Bilag 20, l. 242-245).

Denne idé om "fællessårbarhed" kan sammenlignes med arbejdsmiljølovgivningen, hvor fagforeninger historisk har spillet en væsentlig rolle i at beskytte arbejdstagere i risikofyldte erhverv. På tilsvarende vis argumenteres der for, at IT-sikkerhed bør integreres i en lignende struktur. Informanten udtrykker dog frustration over, at så snart IT-sikkerhed nævnes i Folketinget, "går klappen ned" (Bilag 18, l. 374-382), hvilket peger på en politisk berøringsangst over for området.

En yderligere kritik af den statslige håndtering af IT-sikkerhed retter sig mod den manglende tovejskommunikation med efterretningstjenesten. En informant påpeger, at virksomheder i dag ikke får noget ud af at dele deres sårbarheder, datalæk eller øvrige informationer, idet deres rolle stopper, så snart data er videregivet, uden at de efterfølgende modtager støtte, viden eller læring retur (Bilag 12, l. 298-302). Denne oplevelse understøttes af en bredere kritik, hvor det fremhæves, at der ikke eksisterer nogen aktør, som reelt hjælper de små og mellemstore virksomheder. Informanten foreslår i forlængelse heraf etableringen af et SMV-CERT, analogt til Sektor-CERT der understøtter energisektoren, som kunne fungere som en strukturel støtteinstans for mindre virksomheder (Bilag 12, l. 332-338).

En anden udfordring, der belyses, er manglen på kvalificerede undervisere inden for IT-sikkerhed. Informanter fremhæver, at det netop er disse undervisere, som skal være med til at uddanne og rekruttere de fagpersoner, der skal løse fremtidens sikkerhedsudfordringer (Bilag 21, l. 315-318). I praksis viser det sig dog, at mange undervisere besidder begrænset erfaring, og at de efter nogle år opbygger kompetencer, som de efterfølgende bringer med sig videre til bedre betalte stillinger i erhvervslivet. Dette efterlader uddannelsesinstitutionerne med en vedvarende mangel på erfarne fagkræfter (Bilag 21, l. 329-339). Afslutningsvis fremhæver en informant, at en af de største udfordringer ikke er mangel på strategier, men mangel på konkret handling. I stedet for at nedsætte endnu en kommission eller udarbejde en ny rapport, som først fører til handling om flere år, bør der handles nu, eftersom truslerne allerede er aktive og aktuelle (Bilag 21, l. 454-459).

To informanter fra formelle uddannelsesinstitutioner påpegede tilmed flere udfordringer i uddannelsessystemet, som kan have påvirkning på de IT-sikkerhedskompetencer der findes i Danmark. Eksempelvis peger de på en strukturel barriere i uddannelsessystemet, som beskrives som firkantet, ufleksibelt og som en jungle. Det er dermed vanskeligt for potentielle fagpersoner at gennemskue, hvordan de skal navigere videre inden for IT-sikkerhedsområdet. Den ene informant fremhæver, at dette fjerner det informative valg af studie og kan føre til mangel på motivation, højt fravær, og fravalg af enkelte kurser (Bilag 16, l. 590-607;497-510). Dertil ses et stort problem i, at IT-sikkerhedfag på flere IT-uddannelser ikke er obligatoriske, men kan tilvælges som top-up, hvilket både komplicerer uddannelsessystemet yderligere og peger på en tydelig mangel på IT-sikkerhedskompetencer i fremtidige fagpersoner (Bilag 1, l. 315-321). Imens efterlyser den anden informant en gentænkning af, hvordan uddannelsesmuligheder inden for IT-sikkerhed formidles og

struktureres, således at potentielle veje og retninger bliver mere tydelige og tilgængelige for både unge og voksne (Bilag 21, l. 107-114).

Udfordringerne i uddannelsessystemets struktur og formidling af uddannelsesveje inden for IT-sikkerhed kan yderligere forstærkes af de forestillinger som potentielle studerende har om fagområdet. En informant fra det formelle påpeger, at en væsentlig udfordring i rekrutteringen og fastholdelsen af deltagere i IT-sikkerhedsuddannelser er den sejlivede stereotyp om, hvad arbejdet indebærer. En underviser beskriver, hvordan det kan være svært at få deltagerne til at forstå, at IT-sikkerhed ikke udelukkende handler om at sidde i hættetrøje og "hacke" sig ind i systemer, men også om mange andre aspekter som risikovurdering, governance og samarbejde (Bilag 1, l. 333-336). Han eksemplificerer denne problematik med en reference til Die Hard 4 eller 5, hvor en karakter, en overvægtig mand i en kælder, fremstilles som "paranoid IT-warlord" med et væld af sikkerhedstiltag. Dette billede er ifølge underviseren repræsentativt for den stereotype opfattelse, som mange kæmper imod, og at IT-sikkerhed typisk er et almindeligt "9-17-job" (Bilag 1, l. 347-359). Denne pointe deles af en anden underviser, som beskriver, hvordan deres uddannelse bevidst forsøger at undgå at tiltrække et ensidigt billede af den "klassiske hættetrøjeprofil", den introverte person i mørke omgivelser, som blot får serveret havregrød og fortsætter arbejdet i tavshed (Bilag 7, l. 187-189). Denne stereotype findes ikke kun i formelle uddannelsesmiljøer, men også i uformelle fællesskaber. En uformel informant for en forening beskriver, hvordan deres medlemmer spænder bredt: fra den klassiske IT-person, der sidder stille i hjørnet med hættetrøje, til den udadvendte, højlydte deltager, hvilket samlet set skaber en mangfoldig og broget gruppe (Bilag 4, l. 275-280). Samtidig peger en anden informant på, at tv-serier og medier ofte forstærker et ensidigt billede af IT-sikkerhed som værende forbeholdt geniale hackere eller personer, der konstant er online og laver incident response, hvilket kan virke afskrækkende (Bilag 17, l. 107-111).

Stereotypiseringen bærer også ofte præg af et manderettet ideal, hvilket kan virke ekskluderende for kvinder og andre køn. En informant problematiserer dette med følgende citat: *"At det ikke bare et lille felt for mænd, der bor i kælderen i sorte t-shirts og drikker cola og spiser pizza? Men at der faktisk er et meget bredere felt for teknologi og IT-sikkerhed og sådan"* (Bilag 18, l. 735-746). Selvom mange informanter afviser denne stereotyp som generaliserende, peger en informant på, at man stadig i erhvervslivet kan støde på IT-medarbejdere, der passer til billedet: iført heavy metal-t-shirts eller merchandise fra

tidligere Google-konferencer, omgivet af pizzabakker og sodavandsflasker, hvilket fortsat forstærker denne opfattelse (Bilag 18, l. 761-767).

5.1.3 Adgang til feltet

Dette afsnit har til formål at belyse, hvilke barrierer der kan være for at potentielle fremtidige fagfolk kan indtræde i en arbejdsposition i feltet. En underviser på et klassisk universitet fortæller for eksempel, hvordan han integrerer hands-on øvelser i undervisningen, så de studerende får praktisk erfaring med de principper, de senere skal anvende (Bilag 1, l. 185-191). Dette illustreres eksempelvis ved, at man gennemgår en specifik type angreb i teorien og derefter afprøver det i praksis (Bilag 1, l. 197-205). Denne tilgang anvendes også i efteruddannelsesforløb, hvor deltagerne kan koble øvelserne til konkrete erfaringer fra deres egen virksomhed og reflektere over dem i undervisningen (Bilag 1, l. 215-222). På trods af sådanne praksisnære og kompetenceopbyggende tilgange oplever flere informanter, at det kan være vanskeligt at opnå fodfæste i IT-sikkerhedsbranchen uden formelle uddannelsespapirer. En uformel informant fremhæver eksempelvis, hvordan certificeringer ikke anerkendes i offentlige overenskomster, hvor personer uden bachelorgrad automatisk placeres på løntrin 2, uanset kompetenceniveau (Bilag 4, l. 460-464). Samtidig peger flere informanter på, at nogle af de dygtigste IT-sikkerhedsfagfolk de har mødt netop ikke kommer fra traditionelle uddannelsesforløb, men eksempelvis fra fag som slagter eller smed (Bilag 7, l. 253-256). En SMV-informant beskriver tilsvarende, hvordan en medarbejder uden formel IT-sikkerheds baggrund men med interesse for IT-sikkerhed kunne kombinere sin tidligere erfaring med virksomhedens behov og dermed skabe værdi (Bilag 13, l. 517-527). Alligevel beskrives det af flere, hvordan fraværet af formelle papirer kan være en barriere, eksempelvis for tidligere cyberværnepligtige, der på trods af dokumenterede færdigheder og beståede tests, ikke kunne omsætte deres erfaring til anerkendte kompetencer i det offentlige system (Bilag 4, l. 181-184;456-464). En anden informant fortæller, hvordan deltagelsen i De Danske Cybermesterskaber gav adgang til et professionelt netværk, som førte til en studentermedhjælperstilling, og da han senere droppede ud af universitetet, kunne det omdannes til en fuldtidsstilling i IT-sikkerhed (Bilag 3, l. 55-59). Flere SMV'er fremhæver, at de i mangel af formelle beviser vil vurdere kandidater ud fra flere parametre og nogle gange modstridende, som eksempelvis praktisk erfaring og personligt engagement. En informant forklarer: "*Vi vil jo kigge på, hvad de så rent faktisk har arbejdet med, og hvis det var en*

nyansættelse, så ville jeg tage en reference på vedkommende" (Bilag 10, l. 303-306), mens en anden uddyber: "*Jeg spørger ikke ind til, hvor meget de kan (. . .) Jeg vil vide, hvem de er, og hvad de brænder for*" (Bilag 14, l. 473-483). Det understreger, at adgangen til feltet kan være udfordrende, hvis man hverken har formel uddannelse eller dokumenteret erfaring. En anden informant fremhæver dog, at der findes alternative veje til kompetenceopbygning i form af certificeringer, som kan udgøre et supplement eller alternativ til det etablerede uddannelsessystem (Bilag 21, l. 116-121).

De uformelle sammenslutninger af personer med interesse for IT-sikkerhed har hver deres tilgang til, hvordan man får adgang til deres fællesskaber. Én gruppering er mere lukket og stiller krav om, at man tidligere har været cyberværnepligtig for at blive fuldgyldigt medlem. Dog eksisterer der en mulighed for at blive støttemedlem, såfremt man deler gruppens værdier, og et eksisterende medlem kan sige god for én. Dette begrundes med ønsket om at leve op til gruppens formål: at styrke cyberresiliensen i Danmark, og hvis nogen kan bidrage til dette, er der villighed til at inkludere dem (Bilag 4, l. 283-290). En anden uformel samling har et mere legende og inkluderende fokus og tilstræber at fremme IT-sikkerhed gennem sjove aktiviteter. Her er tilgangen, at det skal være så nemt og tilgængeligt som muligt at deltage, hvilket også afspejles i deres optagelseskriterier: "*Du skal bare dukke op, være med og have det sjovt – så længe det er muligt, vi har ressourcerne, og vi kan finde et sted*" (Bilag 19, l. 91-95). Den tredje samling opfatter sig selv som et community og anvender platformen Discord til at organisere sig. Adgang til deres fællesskab sker via åbne invitationer, f.eks. links online, og der er nogle få grundlæggende regler, såsom at man kommunikerer på dansk. Når en person har deltaget i et par CTF-konkurrencer med dem, foretager adminteamet typisk en vurdering af, om personen er klar til at blive en del af fællesskabet (Bilag 11, l. 179-182). Selvom adgangen til disse grupper varierer, har de det til fælles, at de bygger på fællesskab og engagement i IT-sikkerhed, hvad enten det handler om at styrke samfundets cyberresiliens, at konkurrere i CTF'er, eller blot at dele glæden over en fælles passion.

I forlængelse af ovenstående er der en tydelig mangel på repræsentation blandt visse målgrupper inden for IT-sikkerhed, særligt kvinder. Flere informanter fremhæver, at diversiteten generelt er lav i faget (Bilag 5, l. 47-48), og at der derfor er igangsat konkrete indsatser for at fremme en større mangfoldighed (Bilag 8, l. 368-376). Et centralt problem består i, at kvinder har vanskeligt ved at spejle sig i de nuværende aktører i branchen, da der mangler kvindelige rollemodeller. Dette udfordrer rekruttering og fastholdelse af kvinder i

feltet. En af de uformelle samlinger forsøger at imødegå denne udfordring gennem forskellige initiativer, der understøtter synliggørelsen af kvinder i IT-sikkerhed og skaber plads til nye rollemodeller (Bilag 17, l. 119-126;466-469).

Endnu et vigtigt aspekt vedrørende rollemodeller og idealer der dominerer i miljøet handler om når elitære præstationer får størstedelen af opmærksomheden, hvilket risikerer at skabe en snæver forestilling om, hvad det kræver at "høre til" i feltet. Det følgende eksempel illustrerer, hvordan denne form for eksponering kan have en utilsigtet ekskluderende effekt, og særligt for nybegyndere og dem, der ikke identificerer sig med elitemiljøet. Et eksempel er Kalmarunionen, der i dag regnes som et af de bedste CTF-hold i verden. Denne eksponering og succes kan dog også medføre en ny problematik, som en informant formulerer således: "*men det bliver ret hurtigt et superligahold, (. . .) Kalmarunionen er blevet blandt verdens bedste (. . .) vi skal passe på med at (. . .) der lige pludselig kun er superligahold omkring os*" (Bilag 7, l. 380-390). Hermed påpeges risikoen for, at idealet bliver at være blandt verdenseliten, hvilket kan skabe en barriere for deltagelse for dem, der befinder sig på et mere begynderniveau. Informanten understreger, at der findes adskillige "*serie 2 og 3*"-hold i Danmark, som også bidrager positivt til fællesskabet og læringsmiljøet, men som desværre ikke får samme opmærksomhed.

Ved at arbejde med IT-sikkerhed opnås der ofte kompetencer der kan misbruges til egen vinding, hvor den udførende kan komme på kant med loven. En af de uformelle samlinger beskriver deres bidrag til den samlede danske IT-sikkerhed således:

> *Det er, at Jutlandia skaber et rum, hvori vi både, selvfølgelig giver mulighed for, at folk kan lære at hacke – etisk hacke – og udnytte sårbarheder, men egentlig også et rum for, at hvis folk så lærer det, at man gør de rigtige ting, at man ikke selv udnytter [sårbarhederne].* (Bilag 3, l. 248-252).

Dermed etablerer de et læringsrum, hvor individer kan tilegne sig tekniske færdigheder til at identificere og tilgå sårbare systemer, samtidig med at der lægges vægt på at udvikle et moralsk kompas. I stedet for at udnytte de opdagede sårbarheder, opfordres deltagerne til at melde dem til den relevante systemejer, som herefter har mulighed for at udbedre problemet og dermed lukke sikkerhedshullet (Bilag 3, l. 232-238). Denne etiske tilgang bliver også understreget af informanten som vigtigheden af ansvarlighed i arbejdet med tekniske

systemer ved at referere til det velkendte citat fra *Spiderman*: "*With great power comes great responsibility*". Pointen er, at selvom det kan være spændende at opdage sårbarheder i software, er det afgørende, at sådanne fund ikke udnyttes, men i stedet rapporteres til de relevante aktører. På den måde kan fejlene udbedres, og utilsigtede konsekvenser for andre undgås (Bilag 3, l. 257–262).

5.1.4 SMV-udfordringer

Den sidste dimension, i denne analysedel, har til formål at belyse hvilke udfordringer SMV'er står overfor i forhold til at skabe essentiel cyberhygiejne. Her beskriver en informant, hvordan det er svært at indgå kontraktuel tillid mellem organisationer. Men det er omvendt muligt at indgå relationer mellem medarbejdere i hver sin organisation, hvilket gør at de kan stole på hinanden og derved indgå i en tillidsfuld relation (Bilag 4, l. 675-682). Ydermere er det svært for organisationer at åbent diskutere IT-sikkerhed. Mange af virksomhederne vil ikke udstille deres usikkerhed overfor andre og vælger derfor at tie stille (Bilag 20, l. 659-660;684-694). Specielt dette med udstille sig som dum, beskriver en SMV informant som følgende:

> *Så de skal have et sted hvor de kan snakke om det her, hvor direktørerne kan blive enige om jamen hvad har i.. tør godt snakke med nabodirektøren, 'jamen ved du hvad jeg skal i gang med det, jeg ved sgu ikke lige helt hvad jeg skal gøre, jeg vil faktisk hellere lade være med at lave noget så for jeg vil ikke stå og udstille mig selv som dum'.* (Bilag 20, l. 617-621)

Som beskrevet i afsnittet om trusselsbilledet, mangler mange virksomheder en basal cyberhygiejne. En informant beskriver, hvordan deres medarbejdere løbende bliver mere opmærksomme på sikker adfærd, såsom brug af VPN, når de ikke befinder sig på virksomhedens lokationer (Bilag 10, l. 82-86). En SMV-informant uddyber dog, hvordan de ofte oplever, at andre SMV'er har legacy-hardware stående i drift, hvilket udgør en væsentlig sikkerhedsrisiko (Bilag 14, l. 104-110). Samme informant beskriver, hvordan mange virksomheder får leveret et IT-setup, som derefter ikke bliver opdateret eller vedligeholdt i op til fire år (Bilag 14, l. 138-141).

En anden ekspert fremhæver, at virksomhederne ofte mangler både viden og støtte til at opnå en grundlæggende cyberhygiejne. Det gælder beskyttelse af helt basale elementer som endpoints, identiteter, netværk og åbne porte. Derudover mangler de ofte et overblik over deres IT-setup, hvilket er nødvendigt for at kunne forstå og håndtere den underliggende kompleksitet (Bilag 15, l. 159-165).

Tillæg til denne problematik med manglende cyberhygiejne er, at SMV'er ofte står over for økonomiske barrierer. En informant beskriver, hvordan mange SMV'er er fanget i en situation, hvor de fleste IT-sikkerhedsprodukter er målrettet større virksomheder og derfor er meget dyre. Der findes i dag ikke tilstrækkeligt med produkter, der er skræddersyet til mindre virksomheder, hvilket medfører, at SMV'erne ofte tvinges til at investere i løsninger, der overstiger deres behov og økonomiske formåen, blot for at opnå et acceptabelt sikkerhedsniveau (Bilag 20, l. 179-184). En informant uddyber dette med følgende udsagn:

> *Man skal ligesom have hentet eksperter ind til de egentlige områder. Det er ligesom svært, når der også er rigtig mange sælgere derude. Så jeg følte i hvert fald der vi var før, der synes jeg de skød lidt gråspurve med kanoner i forhold til prissætningen og i forhold til vores behov og risikoprofil.* (Bilag 13, l. 239-242).

Udsagnet peger samtidig på den usikkerhed, som mange SMV'er oplever i mødet med et komplekst og kommercielt præget marked. Det tydeliggør behovet for vejledning og tillidsfulde aktører, der kan hjælpe virksomhederne med at træffe informerede beslutninger om IT-sikkerhed.

I tillæg til de ovenstående udfordringer peger flere informanter på, at SMV'er ofte prioriterer indtjening og omkostningsminimering over IT-sikkerhed. En informant refererer til en tidligere studerende, som oplevede at blive bedt om at udvikle software uden fokus på sikkerhed. Da den studerende påpegede de sikkerhedsmæssige mangler, var chefens svar, at kunden ikke havde efterspurgt sikkerhed og at det derfor kunne blive et mersalg, hvis kunden senere identificerede behovet (Bilag 1, l. 299-306). Dette illustrerer en grundlæggende udfordring i branchen, hvor sikkerhed ofte kun betragtes som en kommerciel tillægsydelse. Yderligere understreger samme informant, hvordan sikkerhed ikke altid prioriteres i en hektisk hverdag, hvor opgaver uden for arbejdstiden, såsom afhentning af børn, ofte overskygger IT-sikkerhed, når klokken runder 16 (Bilag 1, l. 262-265). En anden informant

underbygger denne prioriteringsproblematik ved at fremhæve, hvordan fokus i mange virksomheder primært er på at øge salget, og at tiltag som ikke understøtter dette, ofte bliver nedprioriteret (Bilag 7, l. 192-196). Dette illustreres yderligere i en fortælling fra en tidligere direktør, som fortæller om sine tidligere holdning til IT-sikkerhed:

> *Jeg gider simpelthen ikke det der med at skifte mit password (. . .) Der stod i personalehåndbogen, at alle medarbejdere skulle skifte password hver 3. måned, men direktøren han skulle ikke. Det sagde han ja til. Og så ville han godt have mig som kunde stadigvæk, og det synes jeg er skide fedt, ikke?* (Bilag 20, l. 366-377)

Udsagnet vidner om, hvordan selv grundlæggende sikkerhedsforanstaltninger kan tilsidesættes, hvis de opleves som hæmmende for drift eller komfort, selv i ledelsen, og hvordan forretningsrelationer til tider vægtes højere end sikkerhedsprincipper. Samtidig udtrykker flere SMV-informanter bekymring for konkrete trusler som ransomware, hvor angribere enten forsøger at afpresse penge eller true med offentliggørelse af data (Bilag 10, l. 136-141). Ifølge en informant fører netop hændelser i andre lignende virksomheder til en midlertidig øget opmærksomhed på IT-sikkerhed, men denne interesse forsvinder ofte igen, når trusselsbilledet ikke længere føles nært (Bilag 10, l. 332-337). Den økonomiske virkelighed spiller også en væsentlig rolle. En SMV-ekspert forklarer, hvordan mange virksomheder ganske enkelt ikke har ressourcer til at betale for ekstern hjælp til IT-sikkerhed. Informanten stiller derfor det kritiske spørgsmål, om virksomhederne reelt har råd til at lade være, da næsten halvdelen af alle virksomheder, der rammes af alvorlige cyberangreb, aldrig kommer på fode igen (Bilag 12, l. 16-20). Dette økonomiske pres forstærkes yderligere af nødvendigheden af at digitalisere for at forblive konkurrencedygtige. Nogle SMV'er har valgt at imødegå denne udfordring ved at outsource hele deres IT-funktion. En informant beskriver, hvordan denne løsning, selvom den er ressourcekrævende, bliver nødvendig i takt med virksomhedens vækst (Bilag 12, l. 176-184). En anden informant advarer dog om, at outsourcing i nogle tilfælde kan føre til blinde vinkler, hvor virksomhederne fejlagtigt antager, at sikkerheden er fuldt dækket af leverandøren og derfor ikke selv engagerer sig i området og afdække hvad leverandøren har ansvaret for og hvad virksomheden har ansvar for i deres IT-aftale (Bilag 18, l. 174-178).

Som det fremgår af ovenstående, er SMV'er ofte ikke bevidste om deres manglende IT-sikkerhed. En del af forklaringen kan være, at de har outsourcet deres IT-funktion til

eksterne leverandører, hvilket kan skabe en falsk tryghed omkring, at sikkerheden er dækket. En anden forklaring, som en informant fremhæver, er, at mange ledere i SMV'er tilhører en generation, hvor digitalisering ikke var en naturlig del af deres uddannelse eller arbejdsliv, og derfor mangler de ofte en grundlæggende forståelse for IT-sikkerhed (Bilag 21, l. 137-139). Denne uvidenhed er imidlertid ikke begrænset til virksomheder. Den gør sig også gældende i uddannelsessystemet, hvor IT-sikkerhed i mange tilfælde ikke er en obligatorisk del af pensum. En informant fortæller, hvordan vedkommende kender personer med en datalogiuddannelse, som mangler basal forståelse for IT-sikkerhed (Bilag 4, l. 101-105). En anden informant, som arbejder med at træne virksomheder i IT-sikkerhed, understreger, at det ikke handler om, at alle skal være eksperter. I stedet bør alle, på linje med GDPR, have en generel forståelse for IT-sikkerhed, så de kan beskytte sig selv og deres organisation (Bilag 5, l. 394-402).

For at imødegå denne uvidenhed foreslår en informant en metaforisk tilgang: at "*åbne motorhjelmen*", identificere problemerne og gradvist udskifte de manglende komponenter, så "maskinen" fungerer efter moderne krav, eksempelvis dem, der følger med NIS2-direktivet (Bilag 13, l. 617-620). Det er dog vigtigt, at virksomhederne ansætter de rette kompetencer i forhold til deres aktuelle sikkerhedsniveau. Som en informant pointerer, giver det ikke mening at ansætte en Governance, Risk & Compliance (GRC)-specialist, hvis man endnu ikke har styr på de basale sikkerhedsforanstaltninger, men at det blot vil være spild af penge (Bilag 15, l. 244-248).

Til at kunne åbne denne motorhjelm har virksomhederne ofte brug for hjælp eller opkvalificering af deres egne medarbejdere, hvor en formel informant rejser problematikken omkring, at hans studerende i høj grad bliver rekrutteret af store konsulentvirksomheder umiddelbart efter endt uddannelse. Han så dog gerne, at flere af dem i stedet rettede deres kompetencer mod SMV-segmentet i Danmark (Bilag 7, l. 149-157). Denne tendens skal ses i lyset af den stagnering, der er beskrevet i problemfeltet, hvor virksomheder står overfor en stigende trusselsituation og en række nye bureaukratiske krav, som stilles til deres IT-sikkerhed. I dette spændingsfelt bliver prisen en afgørende faktor, og de store konsulenthuse fremstår som attraktive løsninger, både for arbejdsgivere og specialister (Bilag 18, l. 697-708).

Samtidig udgør dette en udfordring for uddannelsesinstitutionerne. Når undervisere opnår et

tilstrækkeligt højt fagligt niveau, vælger de ofte selv at skifte til bedre betalte og mere udfordrende stillinger i erhvervslivet (Bilag 21, l. 328-338). Dermed opstår en risiko for kompetencetab i undervisningssektoren, hvilket igen kan begrænse kvaliteten af den kommende arbejdsstyrke. Et modtræk til denne udvikling er virksomheder, der vælger at efteruddanne deres eksisterende medarbejdere. En formel informant beskriver eksempelvis, hvordan han underviser i et videreuddannelsesprogram med fokus på GRC (Bilag 1, l. 211-222). Derudover tilbyder initiativer som Industriens Fond muligheder for opkvalificering inden for IT-sikkerhed (Bilag 1, l. 386-394), ligesom fagforeninger som Prosa og forskellige brancheorganisationer investerer i uddannelsestilbud til deres medlemmer (Bilag 4, l. 841-846). Det er dog væsentligt at understrege, at en række informanter pointerer nødvendigheden af at løfte hele feltet og ikke blot eksperterne (Bilag 21, l. 274-280).

5.1.5 Delkonklusion

Trusselsbilledet inden for IT-sikkerhed tegner sig som stadig mere komplekst og alvorligt i takt med samfundets stigende digitalisering. Flere informanter peger på en udvikling, hvor angrebsmønstre bliver mere avancerede, hvilket både skyldes den teknologiske fremdrift og et svagt digitalt fundament i mange organisationer. Eksempler som truslen fra kvantecomputere og statsstøttede aktører, såsom APT'er, illustrerer alvoren i den sikkerhedsmæssige situation, særligt for kritisk infrastruktur. Især SMV'er er sårbare over for trusler som phishing, malware og ransomware, som ofte udnytter kompromitterede mailkonti og åbne wifi-access points. Dette forværres af en manglende basal cyberhygiejne og manglende overblik over IT-infrastrukturen, hvilket gør det vanskeligt at identificere og afhjælpe sårbarheder. Der opstår desuden et misforhold mellem SMV'ernes egne opfattelser af trusler, værende primært phishing, og eksperternes vurderinger, som i højere grad peger på systemisk kompleksitet, sårbare systemer og avancerede trusselsaktører.

Adgang til feltet præges af betydelige barrierer og uensartede optagelseskriterier. Selvom flere undervisere og virksomheder anerkender værdien af praktiske og uformelle kompetencer, eksempelvis gennem CTF-deltagelse eller praktisk erfaring, er det stadig vanskeligt at opnå fodfæste i branchen uden formelle uddannelsespapirer. Dette udgør en strukturel udfordring, især for kandidater med alternative baggrunde. Forskelle i adgangskrav iblandt uformelle samlinger forstærker kompleksiteten, hvor nogle netværk er inkluderende og legende, mens andre er eksklusive og kræver tidligere cyberværnepligt. Dertil kommer en

tydelig kønsubalance i feltet, hvor kvinder har vanskeligt ved at identificere rollemodeller og føle sig inkluderet. Stereotype forestillinger om IT-sikkerhedsprofessionelle, som eksempelvis nørdede mænd i hættetrøjer, præger både formelle uddannelsesinstitutioner, populærkulturen og hæmmer diversiteten i feltet.

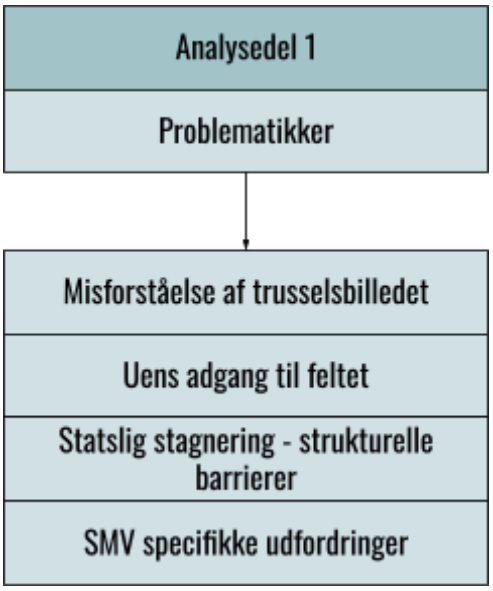
SMV'er står over for en række særegne udfordringer i arbejdet med IT-sikkerhed. En gennemgående bekymring er frygten for at skade virksomhedens omdømme, hvilket ofte fører til tavshed og manglende videndeling om hændelser og sårbarheder. IT-sikkerhed prioriteres ofte lavt, især når den opfattes som en ikke-kommerciel ydelse, hvortil SMV'er ser det som en omkostning snarere end en investering. Dette hænger sammen med, at mange IT-leverandører oplever, at investering i sikkerhed ikke er en del af kundens efterspørgsel. Derudover mangler SMV'erne adgang til IT-sikkerhedsprodukter, der matcher deres behov og økonomiske formåen, hvilket skaber et mismatch mellem udbud og efterspørgsel i markedet.

Denne ubalance forstærkes yderligere af en generel uvidenhed blandt ledere og medarbejdere, som, kombineret med outsourcing og manglende uddannelsesmæssig ballast, ofte medfører en falsk tryghed, hvor sikkerhedsansvaret fejlagtigt antages at være dækket af leverandører. Dette underbygges af informanter, der beskriver, hvordan ledere fra ældre generationer mangler digital forståelse, og hvordan nyuddannede fagfolk primært rekrutteres til store konsulenthuse, hvilket efterlader SMV'er uden adgang til kompetencer. Uddannelsesinstitutioner forsøger at imødegå dette ved at tilbyde efteruddannelse, men udfordres af, at undervisere med erfaring ofte rekrutteres væk til det private erhvervsliv.

På makroniveau identificeres flere strukturelle forhold, som påvirker IT-sikkerhed i Danmark. NIS2-direktivet fungerer som en væsentlig drivkraft, særligt ved at presse SMV'er indirekte gennem større samarbejdspartnere, der stiller krav om compliance. Dette skaber både incitamenter og muligheder for at hæve IT-sikkerhedsniveauet, men opleves samtidig som administrativt tungt. Politisk peger informanter på en historisk forsømmelse af området, hvor staten i mange år har været tilbageholdende med at investere og engagere sig. En yderligere makrostrukturel udfordring er manglen på kvalificerede undervisere og det "firkantede" uddannelsessystem, som gør det vanskeligt for potentielle fagpersoner at finde vej ind i feltet. Den manglende tovejskommunikation mellem erhvervsliv og efterretningstjenester fremhæves også som en barriere, ligesom fraværet af et SMV-tilpasset støtteorgan, som en

SektorCERT gør for energisektoren, gør det vanskeligt for mindre virksomheder at håndtere trusler effektivt.

På tværs af de fire dimensioner fremtræder en række tværgående fund. Først og fremmest udgør manglen på basal cyberhygiejne et centralt og gennemgående problem. Både som trusselsbillede og som SMV-udfordring ses fraværet af grundlæggende beskyttelse af netværk, identiteter og systemer som en væsentlig risikofaktor. Derudover identificeres uvidenhed og manglende forståelse for IT-sikkerhed som et fælles træk i både SMV-udfordringer, adgangsdimensionen og makroperspektivet. Ligeledes går spørgsmålet om anerkendelse af uformelle kompetencer igen, på tværs af dimensionerne "Adgang til feltet" og "SMV udfordringer", hvor fraværet af fleksible kompetencevurderinger hæmmer talentudviklingen. Endelig skaber strukturelle og økonomiske barrierer, fra politisk underprioritering til markedets manglende tilpasning til SMV'ers behov, en fælles udfordringsramme, der kalder på både koordinering, investering og inklusion for at hæve IT-sikkerhedsniveauet i hele samfundet.



Figur 11: Problematikker i analysedel 1

5.2 Analysedel 2

På baggrund af de empiriske indsigter fra analysedel 1 vil denne del af analysen benytte teori til at analysere de resterende fem aggregerede dimensioner: Fællesskab, kommunikation, viden om IT-sikkerhed, kompetencer og læringsmetodikker. Dette med fokus på hvordan

viden og praksisser, både fra formelle og uformelle sammenhænge samt fra SMV'ernes egne erfaringer, kan inddrages analytisk for at nuancere de tidligere fund. Da specialet har en eksplorativ karakter, er analysens struktur tematisk funderet i de centrale empiriske indsigter, hvilket også afspejles i opbygningen og navngivningen af afsnittene. Afslutningsvis samles de vigtigste pointer fra hvert afsnit i en delkonklusion, hvor der også peges på overlap og sammenhænge på tværs af analysens dimensioner.

5.2.1 Læringsmetodikker

Som problematiseret i første del af analysen er der bred enighed blandt undervisere om, at praktiske kompetencer er essentielle for IT-sikkerhedsspecialister. Ikke desto mindre viser det sig fortsat vanskeligt at opnå fodfæste i feltet uden formelle kvalifikationer. Dette afsnit uddyber, hvordan sådanne kompetencer opnås gennem både formelle og uformelle læringsveje samt hvilke barrierer og muligheder, der knytter sig hertil.

Der er en bred enighed og benyttelse hos informanterne af praksisbaserede læringsmetoder, det omtales som værende en nødvendighed i træning og undervisning af IT-sikkerhed. Klassisk teoribaseret undervisning erkendes som værende ikke hensigtsmæssig i undervisningen af IT-sikkerhed:

> *Vi er meget praksisnære, meget hands on, fordi det man ofte ser og det vi alle sammen er blevet kvalt i det er forelæsninger og teori. Og inden for det her felt der duer det simpelthen ikke fordi det bliver højtflyvende, og det bliver langt fra virkeligheden. Hvis vi snakker om teoretisk sikkerhed, fordi det kan vi alle sammen snakke om, teoretisk sikkerhed og hvordan man skal opføre sig og hvordan systemet skal være sat op. I praksis fungerer det bare ikke. Så det vi sørger for, er at der er et minimum af teori, maksimum er hands on.* (Bilag 4, l. 329-331)

Dette peger på en generel erkendelse af, at læring i IT-sikkerhed må tage udgangspunkt i konkrete scenarier, hændelser og hands-on erfaring for at være effektiv. Denne erkendelse korresponderer med SECI-modellen, hvor viden opstår i en dynamisk spiral mellem tavs og eksplicit viden. Det praksisnære og fælles arbejde i eksempelvis Capture the Flag-events og workshops svarer til *socialiseringsfasen*, hvor deltagerne gennem observation, samarbejde og eksperimenter tilegner sig tavs viden. Den efterfølgende *eksternalisering* sker, når deltagerne

fortæller om, forklarer eller faciliterer opgaver for hinanden, og derved artikulerer erfaringer til andre. Dette er afgørende i IT-sikkerhed, hvor meget viden er kontekstbundet og situationsafhængig. En deltager forklarer, hvordan *"vi gennemgår de opgaver, vi har klaret (. . .) og prøver at få folk med op på samme niveau"* (Bilag 3, l. 129-132), hvilket viser en bevidsthed om viden som noget, der skal kommunikeres og deles for at kunne anvendes bredt. Et andet tydeligt mønster i dimensionen er den værdi, der tillægges muligheden for at eksperimentere. Flere informanter fremhæver fordelene ved læringsmiljøer hvor der er plads til at lave fejl:

> *Det duer ikke at folk de sidder på deres arbejdscomputer og downloader schooling til at lave cyberangreb. Det skal gerne være sådan nogenlunde self containt, så vi har ligesom et laboratorium hvor at det er hele, det ligesom er lukket inde. Så man kan komme til at ødelægge det hele, og så kan man trykke genstart.* (Bilag 5, l. 128-135)

Eksempelvis gennem sandbox-løsninger, det skaber et trygt rum, fordi man kan teste idéer, begå fejl og lære af dem. Dette afspejler Humanokratiets princip om *experimentation*, hvor det betragtes som afgørende, at medarbejdere har mulighed for at eksperimentere i praksis, uden at konsekvenserne ved fejl hæmmer deres lyst til at deltage eller lære. For SMV'er er dette særligt vigtigt, da eksperimentering ofte bremses af frygt for at gøre noget forkert, mangel på tid og ressourcer, eller en kultur, hvor læring forstås som noget, der først må ske rigtigt. Når der skabes mulighed for at eksperimentere i sikre og kontrollerede omgivelser, bidrager det ikke blot til motivation og kreativitet, men også til reel organisatorisk læring. Her er der en tydelig parallel til SECI-modellens *internalisering*, hvor eksplicit viden, eksempelvis gennem værktøjer, teknikker eller trusselsbilleder, bliver indlejret i deltagernes praksis gennem gentagelse og refleksion. For SMV'er kan eksperimenteringens venlige læringsmiljøer derfor fungere som en træningsbane, hvor IT-sikkerheds viden ikke blot tilegnes, men bliver en aktiv del af medarbejdernes arbejdsmæssige vaner.

Endvidere fremhæves segmentering af undervisningsmaterialet til modtagerne blandt informanterne som en forudsætning for effektiv læring, en repræsentant fra en uformel organisation påpeger, at:

> *Det er simpelthen at kende sin målgruppe, vide hvem fanden det er vi skal undervise (. . .) Hvis vi begynder at snakke avancerede threat hunting med teknikker (. . .) med*

nogle der lige har fundet ud af hvordan man bruger OutLook, så tror jeg vi får et problem. (Bilag 4, l. 765-767)

Her synliggøres behovet for et opgør med den ensrettede og standardiserede tilgang, som ofte præger læringsmiljøer, og netop i denne forbindelse bliver SECI-modellens begreb om *intention* relevant. Såfremt man underviser uden at kende sin målgruppe, risikerer man at mangle en klar intention, i praksis skabes der viden, der ikke er anvendelig for dem, der skal bruge den. For SMV'er kan det derfor være afgørende at sikre, at kompetenceudvikling ikke blot er planlagt, men også målrettet de medarbejdere, der faktisk skal omsætte viden til handling i praksis.

Ydermere viser empirien, at struktur og ustrukturerede tilgange eksisterer side om side i mange af de uformelle læringsfællesskaber. En respondent beskriver, hvordan *"Det skifter meget, om det er struktureret (. . .) ellers er det bare fri leg"* (Bilag 3, l. 129-145). I et humanokratisk perspektiv kan dette ses som et udtryk for princippet *Paradox,* hvor organisationer skal lære at balancere frihed og struktur. Når der gives plads til udforskende læring og samtidig etableres rammer for fælles progression, opstår der en paradoksal veksling, hvor kreativitet og systematik kan eksistere samlet. Dette kan i et SMV perspektiv være en effektiv model, da ressourcerne ofte er knappe og de derfor har et større behov for fleksibilitet men stadig har et behov for en fælles retning i læring.

Endeligt udtrykker en informant en skepsis overfor traditionelle og skalerbare awareness initiativer, da de er for overfladiske og ikke tilrettelagt efter virksomhedskulturen og kategoriseres derfor som ineffektive, "*Det er faktisk meget lav effektivitet man får ud af det*" (Bilag 12, l. 56-57). Det understreges, at awarenessinitiativer ofte bliver reduceret til kampagner og plakater, som ifølge respondenterne ikke formår at skabe reel læring eller adfærdsændring. Awareness bliver dermed et ritual snarere end en meningsfuld praksis, hvilket risikerer at afføde modstand i form af eksempelvis *deflection* eller *easy agreement*. Hvilket kan være begrundet i en manglende viden om IT-sikkerhed hos ledelsen som belyst i del 1 af analysen. Dette afspejler Maurers modstandsbegreb *I don't get it*, hvor modtagerne ikke forstår pointen med tiltaget, enten fordi det er for generisk, for hurtigt glemt eller ikke relaterer sig til deres hverdag. En informant understøtter denne pointe og forklarer: "*Den type undervisning har normalt ikke super høj rating, hvis man kigger på, hvor meget husker folk bagefter (. . .) man skal bruge noget, hvor man har hænderne nede i det*" (Bilag 5, l.

166-172). Dette viser, at uden meningsfuld kontekst og praksisnærhed risikerer awareness-indsatser at skabe modstand frem for læring, særligt i organisationer, hvor ressourcer og tid er begrænsede. Samtidig viser materialet, at mange SMV'er alligevel vælger netop denne type skalerbar træning, eksempelvis i form af videomoduler, månedlige lektioner eller phishingtests leveret af eksterne leverandører som Cyberpilot (Bilag 9, l. 145-147; Bilag 10, l. 57-62). Det kan skyldes, at disse løsninger er nemme at implementere og kræver færre ressourcer. Men hvis målet er adfærdsændring, peger en informanter på, at det ikke er tilstrækkeligt: "*Vi laver en awarenesskampagne og alle intentionerne er sikkert super gode, men (. . .) det er jo bare umuligt at følge med i et felt, der bevæger sig så hurtigt*" (Bilag 12, l. 58-60), og "*principielt imod det synes det er en rigtig dårlig måde at gøre det på, hvor man udstiller folk*" (Bilag 12, l. 63-66). I denne sammenhæng bliver det relevant at inddrage Nonakas SECI-model, hvor begrebet *intention* netop beskriver det strategiske formål med videnskabelse, at læring og viden skal være rettet mod konkrete organisatoriske mål. I forlængelse heraf er det også relevant at inddrage det humanokratiske princip om *community*, hvor "no fingerpointing" (Hamel & Zanini, 2021, s. 67) understreger nødvendigheden af at skabe læringsrum uden skam og straf. Når awareness bygger på udstilling af fejl eller fejlklik, undermineres netop det fælles læringsklima, der skal få folk til at engagere sig i stedet for at frygte konsekvenser. For især SMV'er, hvor ressourcerne er begrænsede og det menneskelige engagement er centralt, er det derfor afgørende at designe læring og awareness som noget, der styrker fællesskab, fremmer deltagelse og legitimerer fejl som del af en fælles læringsrejse. Når awareness ikke tager afsæt i en tydelig intention, heraf en forståelse for målgruppens behov, kultur og praksis, bliver det en løsrevet aktivitet uden reel effekt. For SMV'er betyder det, at awareness-løsninger ikke blot skal vælges ud fra, hvad der er nemt at skalere, men ud fra hvad der er relevant og forankringsdygtigt. Et effektivt awarenessprogram må tage afsæt i virksomhedens konkrete risikobillede, sprogbrug og daglige rutiner. Det kræver ikke nødvendigvis store investeringer, men det kræver, at formålet er tydeligt, og at læringen kobles til modtagerens virkelighed og ikke blot leveres som generisk information. Når awareness bliver en praksis, man deltager i, frem for en kommunikation man passivt modtager, skabes der mulighed for reel adfærdsændring.

5.2.2 Fællesskab

En gennemgående problematik, der blev belyst i første del af analysen, er den udbredte uvidenhed og manglende forståelse for IT-sikkerhed i SMV-segmentet, samt de begrænsede ressourcer, både i form af tid og økonomi, som mange mindre virksomheder har til rådighed. Dertil beskrev foregående afsnit, hvordan hands-on undervisning, segmenteret formidling og trygge læringsrum ikke blot fremmer individuel tilegnelse af viden, men også fælles refleksion og erfaringsdeling. Dette afsnit har derfor til formål at undersøge, hvordan dimensionen Fællesskab kan bidrage med nye perspektiver på problematikken om manglende viden og ressourcer, samt hvordan praksisser i det uformelle IT-sikkerhedsmiljø kan inspirere til udvikling af mere inkluderende, bæredygtige og kapacitetsopbyggende tilgange i SMV'er.

Dimensionen "Fællesskab" er noget der gik igen på tværs af informantkategorier og informanter. For det første, er videndeling ifølge virksomhederne en vigtig del af at holde sig ajourført omkring blandt andet IT-sikkerhed, og bliver endda brugt som en forsvarsmekanisme mod angreb. En SMV-informant nævner, at videndeling foregår internt blandt medarbejderne, fordi de umiddelbart efter at have opdaget en trussel, som eksempelvis florerende phishing-mails i virksomheden, beretter om det (Bilag 13, l. 68-71). Dette er et eksempel på SECI-modellens kombinationsproces, hvor medarbejderne deler deres eksplicitte viden, sandsynligvis ved at formidle det som eksplicit viden endnu engang, ved at informere deres medarbejdere og få truslen om phishing mails kommunikeret ud til deres ansatte. I virksomheder som denne, der efter sigende er "begunstigede" (l. 449) med medarbejdere, som både har denne viden til at kunne opdage trusler og derefter formidler dem videre, fungerer denne tilgang som en effektiv beskyttelse mod udefrakommende trusler. Men eksemplet indeholder to begrænsninger, hvor den første vedrører den initielle manglen på viden. Dette tydeliggør den skrøbelighed, der ligger i en tilgang, hvor sikkerheden afhænger af, at en tilfældig medarbejder både har den nødvendige indsigt og af egen drift deler den med andre. Den anden begrænsning handler om faciliteringen af viden gennem kombinering, altså overførslen af eksplicit viden til eksplicit viden. På trods af, at informationen blev videreformidlet, faldt nogle medarbejdere alligevel i fælden, hvilket peger på, at den eksplicitte viden ikke blev internaliseret. Det er af Nonaka (1994, s. 20) en anerkendt svaghed ved kombinationsprocessen, at den kan føre til en overfladisk tilegnelse af information, hvor modtagerne i dette eksempel måske godt har hørt advarslen, men ikke

nødvendigvis forstået eller indarbejdet den i deres praksis. Det kan derfor argumenteres, at virksomheden mangler at bygge en dialog mellem eksternalisering og internalisering, eksempelvis gennem internalisering og socialisering. Dette afsnit vil dog kun fokusere på socialisering, da det snakker ind i dimensionen, fællesskab. Denne proces, hvor det handler om at man via interaktioner med hinanden kan dele fælles erfaringer og holdninger gennem interaktion, gør det muligt at dele erfaringsbaseret og kropsliggjort viden, som ikke umiddelbart kan skrives ned eller formidles verbalt, som for eksempel intuition, fornemmelser, rutiner eller handlemønstre. For at sådan en proces kan foregå i praksis, kræver det ikke bare viden om IT-sikkerhed, men også tillid fra de ansattes side til at indgå i disse processer, og at de ikke bliver udstillet. Dermed skal der findes en organisationskultur, der inkluderer Humanokratiets fjerde princip, Community. Især informanter fra den uformelle kategori nævner fællesskab som den primære styrke og vigtigste del af at kunne udvikle deres IT-sikkerhedskompetencer og viden:

> *Det man snakker om med organisationer og man siger 'Vi skal have tillid, og vi skal gerne dele viden om trusler' (. . .) Jamen det er svært at indgå kontraktuel tillid, det er noget der sker mellem medarbejdere i organisationer. (. . .) Det der med at sige, at den her organisation har tillid til den her organisation (. . .) det er meget en meget svær øvelse, fordi det handler om personlige relationer langt hen ad vejen, så skal man fandme være god til at lave de der aftaler, hvis man kan dele, og ikke nødvendigvis stole på hinanden. Det er det vi kan med at give hinanden en øl engang imellem.* (Bilag 4, l. 675–682)

Som informanten nævner, kan det være let at opbygge intern tillid kontraktuelt, og ifølge Humanokratiet (s. 166) burde det i teorien også være lettere at opnå i SMV'er, hvor hierarkier og bureaukratier typisk er mindre prævalente, jo mindre virksomhederne er. Men selv her ses det sjældent. De uformelle fællesskaber trives netop, fordi deltagerne engagerer sig frivilligt og ud fra en lyst- og interessebaseret motivation. Her handler det ikke om bundlinjen, men om nysgerrighed, passion og ønsket om at bidrage til et større fælles formål. Det gør det muligt for medlemmerne at dele erfaringer, lære af hinanden og tilbyde hjælp, som blandt andet ses i, at de deler fælles platforme til undervisning, får gratis hjælp af dygtige eksperter som "*tjener på den anden side af 100.000 kr. i måneden*" (Bilag 4, l. 222), og konstant holder sig opdaterede omkring IT-sikkerhed- og trusler. Udsagn fra informanter fra den formelle kategori tyder også på, at fællesskabet kan give værdi ud over de uformelle organisationers

fire vægge, da undervisere er afhængige af både deres kompetencer og platforme. For det første ved, at de kan hyre eksperter ind gratis (Bilag 6, l. 265-268) og for det andet ved at benytte Haaukins-platformen, hvilket frigiver ressourcer i et område, hvor der er stor ressourcemangel. Det er dog vigtigt at påpege, at de nuværende muligheder, eksempelvis brugen af Haaukins platformen, primært er mulige takket være private initiativer som Industriens Fond. Som det fremgår af del 1 af analysen, vil en bæredygtig og langsigtet indsats dog kræve en mere aktiv statslig involvering og støtte. I tråd med dette står SMV'er typisk i samme situation ressourcemæssigt, hvor deres syn på IT-sikkerhed er, at det ikke skal prioriteres, fordi det er dyrt, og samtidigt ikke har en økonomisk gevinst. Her er det relevant at inddrage Humanokratiets paradoks-princip: I stedet for at vælge mellem økonomisk overlevelse og IT-sikkerhed, bør SMV'er finde løsninger, hvor begge integreres, da de som førnævnt ikke har råd til at negligere sikkerhed. Ved at anerkende og navigere dette paradoks, og lade sig inspirere af den samarbejds- og delingskultur, der kendetegner de uformelle IT-sikkerhedsfællesskaber, kan de styrke deres organisatoriske modstandsdygtighed og langsigtede overlevelse. Den centrale udfordring er dog at forene sociale og forretningsmæssige interesser, især *på tværs af* virksomheder, da de har forskellige konstellationer, størrelser og modenhedsniveauer, der er afgørende for hvordan de skal styrke deres IT-sikkerhed:

> *Der er sådan en masse SMV-puljer at det kunne være, at man skulle prøve at se en af dem til at ligesom få belyst det her. For jeg synes faktisk at der desværre i det, de er jo specielle, naboen er speciel.* (Bilag 13, l. 236-240)

I den sammenhæng blev det udforsket, hvorvidt SMV'er kunne være interesseret i at være en del af branchefællesskaber, som går ud på at virksomheder i samme branche går sammen om at dele erfaringer, viden og løse problemer. En idriftsætter af en fællesskabsrettet løsning, nævner et behov for større virksomheder at gå forrest i et fællesskab, som de kalder "lokale clusters", med det argument, at SMV'er lytter til de store virksomheder (Bilag 20, l. 245-248). Et afgørende skridt i at udfordre idéen om trade-offs er tilmed at synliggøre de skjulte omkostninger ved ikke at investere i IT-sikkerhed, herunder nedetid, tab af data og forretningskritisk viden, omdømmeskader og regulatoriske sanktioner. "*Don't assume no data means no downside*" (Hamel & Zanini, 2020, s. 231) kan sidesættes med virksomhedernes reaktive respons på cyberangreb. Når virksomheder mangler konkret indsigt i de trusler, de står overfor, og deres potentielle konsekvenser, risikerer de at undervurdere behovet for

forebyggende investeringer. Denne uvidenhed fører til passivitet, fordi truslen er usynliggjort. Bedre data og dokumentation kan dermed være en nøgle til at ændre både bias og praksis.

5.2.3 Viden om IT-sikkerhed

I analysedel 1 blev det påpeget, at der er mangel på kvalificerede undervisere og specialister inden for IT-sikkerhed, samt at outsourcing af IT-sikkerheden i SMV'er ofte skaber blinde vinkler. Virksomhederne antager fejlagtigt, at leverandøren har det fulde ansvar, hvilket hæmmer deres eget engagement og forståelse af ansvarsfordelingen i IT-aftalerne. Dette skaber et vidensvakuum omkring IT-sikkerhed, både i de formelle uddannelsesinstitutioner og blandt SMV'er, hvor outsourcing kombineret med allerede utilstrækkelig cyberhygiejne forstærker manglen på viden indenfor feltet. Dette afsnit har derfor til formål at analysere, hvordan viden om IT-sikkerhed produceres, deles og vedligeholdes, og hvilke barrierer der hindrer, at denne viden bliver tilgængelig og brugbar i praksis.

Undervisere på alle niveauer oplever, at deres fagstof skal revideres næsten hvert år. En universitetslektor siger at de løbende skal indarbejde nye værktøjer, teknologier og opdaterede metoder i undervisningen (Bilag 2, l. 357-368) for at kunne følge udviklingen. Ligeledes opleves dette på gymnasierne, hvor undervisere konstant skal holde sig opdaterede omkring den nyeste cybertrussel (Bilag 6, l. 252-256). Denne konstante opdatering af undervisningsstoffet afspejler behovet for kombinering, hvor undervisere og praktikere deler erfaringer og indsigt for at kunne eksternalisere, og dermed internalisere viden enkeltvis som undervisere, på et nationalt plan. Da videndeling indtil videre ofte sker løbende og ustruktureret, er det en udfordring at sikre, at relevant og opdateret viden hurtigt når ud til alle relevante parter. Udfordringen med hurtigt forældet materiale viser yderligere et tydeligt behov for en kontinuerlig og struktureret opdatering i materialet, såfremt undervisere og specialister skulle kunne facilitere en dynamisk videnskabelse, og deling heraf, over IT-sikkerhedsfeltet. En uformel underviser som bruger faktiske scenarier fra kritisk infrastruktur, for at gøre alvoren tydelig, fortæller at læring bedre forankres, når studerende kan koble øvelser til konkrete hændelser: "*Vi putter det i real-world-kontekst (. . .) konsekvensen kan være, at en million borgere mister strøm*" (Bilag 4, l. 337-347), mens en formel informant fremhæver, at materiale fra et halvt år i fortiden er irrelevant i dag (Bilag 6, l. 341-346). Dog beskriver informanten også hvordan kobling til virkelighedsnære cases kan

være udfordrende på baggrund af begrænset tid og få samarbejdspartnere, især på et gymnasialt b-niveau-fag der kun rummer få lektioner (bilag 6, l. 323-325).

Der ses ligeledes udfordringer hos SMV'erne hvor en IT-chef beskriver, at man som leder altid vil føle sig på bagkant (Bilag 10, l. 196-200). Dette fund i empirien er i overensstemmelse med analysedel 1, hvor SMV-ledere beskrev en konstant ubalance mellem trusselsbilledet og deres egen viden og kapacitet. Dette afspejler, hvordan viden i mange tilfælde ikke bliver fuldt *internaliseret* eller *eksternaliseret*. Den erfaringsbaserede, tavse viden forbliver lokalt forankret og mangler dokumentation, hvilket afskærer den fra at blive transformeret til delbart læringsmateriale.

Ovenstående fund peger på, at det er kritisk at styrke *kombinationen* af viden gennem samarbejde med industrien og opbygning af databaser med opdateret viden. Dette kan dog komme i farezonen for Maurers modstandsprincip, I don't like it, da den arbejdsbyrde, der ligger i at koordinere og ajourføre disse arkiver, kan overvælde de ansvarlige. Så selvom disse personer vil være fuldt opmærksomme på nødvendigheden af at ændre materiale, vil de vise modstand, da opgaven kan blive for stor.

Ydermere er der en tydelig ubalance mellem udbud og efterspørgsel på IT-sikkerhedskompetencer. SMV'er "*har ikke råd til at have IT-sikkerhedsspecialister*," og en fuldtidsrolle koster typisk "*en halv million om året*" (Bilag 4, l. 626-629). Dette understreges ligeledes i analysedel 1, hvor mangel på kvalificerede fagpersoner og høje omkostninger blev fremhævet som centrale barrierer for SMV'er. Samtidig bekræfter konsulenter, at "*alle taler om IT-sikkerhed, men ikke ret mange ved noget om det*", og understreger, at der er akut mangel på kvalificerede profiler: "*altså kunne du skaffe mig 3 navne der kan noget med med IT-sikkerhed (. . .) så er de ansat næste måned*" (Bilag 14, l. 51-56). Denne mangel er systemisk; selv uddannelsesinstitutioner mangler undervisere og må i flere tilfælde ansætte profiler med en generel IT baggrund, der lærer sikkerhed undervejs (Bilag 21, l. 328-332). Denne todelte problematik, SMV'ernes økonomiske begrænsninger og konsulenthusenes rekrutteringsudfordringer samt manglende adgang til specialiseret arbejdskraft, som også er belyst i analysedel 1, gør det vanskeligt at arbejde med *dynamisk videnskabelse* af IT-sikkerhedsviden. Når konsulenterne samtidig selv mangler medarbejdere med tilstrækkelig teknisk og kommunikativ indsigt, svækkes mulighederne for at gennemføre den *socialisering* og *eksternalisering*, som netop skulle sikre, at grundlæggende sikkerhedsforståelse bliver

kollektivt delt og praktisk anvendt. Dette understreges af de systemiske udfordringer beskrevet i analysedel 1, hvor både uddannelsessystemet og erhvervslivet oplever ressourceknaphed og manglende koordinering. Dermed bliver videnspiralen, særligt de tidlige faser, vanskelig at realisere i praksis for mange SMV'er, og IT-sikkerhed forbliver noget, der "outsources", snarere end integreres som fælles organisatorisk praksis. Tilmed kan det argumenteres at virksomheder som vælger at outsource deres IT-sikkerhed aldrig træder ind i vidensspiralen og dermed forbliver uvidende, især når de bliver mødt med sælgere som ikke sætter sig ind i virksomhedens specifikke behov, eller bare forsøger at sælge en alt-i-en løsning. En SMV ekspert peger eksempelvis på en udfordring i at vurdere konsulenters faktiske kompetencer:

> *Fordi at alle kan sige de kan lave noget sikkerhed og hvis som SMV du sad med en som ikke rigtig ved noget om det jamen så kan du heller ikke rigtig vurdere om det de siger faktisk er rigtigt.* (Bilag 15, l. 451-454)

Når modtagerne ikke besidder den nødvendige faglige dømmekraft til at vurdere, om rådgivning er sagligt funderet eller primært salgsdrevet, opstår der en relationel skepsis, der kan forstås som en form for modstand i tråd med Maurers I don't like you, hvor modstanden ikke retter sig mod indholdet, men mod afsenderens integritet og intentioner. Dette tydeliggør, at når der mangler faglig indsigt og gennemsigtighed, bliver det vanskeligt at etablere tillid. Selv hvis konsulenten er fagligt kompetent, vil SMV'ernes usikkerhed og manglende mulighed for at vurdere ekspertisen kunne føre til modstand. Det handler dermed ikke nødvendigvis om realiteter, men om perception. Denne pointe må dog afvejes mod et modsat problem identificeret i analysens del 1, hvor en overdreven eller blind tillid til leverandører kan skabe en falsk form for tryghed. I sådanne tilfælde risikerer SMV'er at stå uden tilstrækkelig sikkerhedsmæssig dækning, netop fordi de mangler den nødvendige forståelse for de ydelser, leverandøren tilbyder. Dette understreger vigtigheden af, at SMV'er opbygger en grundlæggende intern viden om IT-sikkerhed, ikke blot for at kunne kvalificere og vurdere potentielle leverandører og derved opbygge et tillidsfuldt samarbejde, men også for at undgå, at tilliden bliver en sårbarhed i sig selv. Denne balancegang mellem for meget- og for lidt tillid taler ind i Humanokratiets paradox-princip, hvor organisationer må navigere mellem at udvise tilstrækkelig tillid til eksterne aktører og samtidig bevare den nødvendige kompetence til at sikre robuste og effektive sikkerhedsløsninger. Tillid er en forudsætning for videndeling og organisatorisk læring, men netop den manglende fælles faglige forståelse og

gennemsigtighed underminerer tilliden, der skulle gøre læring mulig. Derfor skal sådan en ændring tilgås med hensigt om at bruge kræfter på at bygge relationer og tillid på begge sider. Dette kan opnås ved at opbygge langvarige samarbejde og sikre, at de aktører, der introducerer forandringerne, har tillid og respekt fra de berørte parter, som tidligere nævnt i afsnit 5.2.2, "Fællesskab".

5.2.4 Kommunikation

En af de problematikker, der blev belyst i del 1 af analysen, er manglen på digital viden blandt den ældre generation, som i dag udgør ledelsen eller ejerkredsen i mange SMV'er. Dette skaber en kommunikationsudfordring, idet disse ledere ofte mangler de nødvendige forudsætninger for at forstå kompleksiteten i deres digitale infrastruktur og dermed også de sikkerhedsmæssige risici, de står overfor. Dette afsnit forsøger derfor at udforske den kommunikative udfordring, og tilmed løsninger, der består i at etablere et fælles sprog og kommunikative broer mellem tekniske eksperter og ikke-tekniske beslutningstagere.

Etablering af fælles sprog i IT-sikkerheds- undervisning og rådgivning fremstår i empirien som en grundlæggende forudsætning for ideel kommunikation på tværs af organisatoriske og faglige lag. En repræsentant fra en uformel organisation nævner eksempelvis at klassisk teori ikke kan fungere til formidling af IT-sikkerhed, *"det bliver højtflyvende, og det bliver langt fra virkeligheden"* (Bilag 4, l. 330-331), når formidlingen bliver for teoretisk og løsrevet fra praksis, mangler den nødvendige *intention*, der skal sikre, at viden bliver relevant, handlingsorienteret og i sidste ende internaliseret af medarbejderne. Et andet væsentligt aspekt er målgruppekendskab. En respondent fra en uformel organisation beskriver udfordringen ved at anvende avancerede tekniske begreber overfor en person, der netop har lært at bruge Outlook (Bilag 4, l. 762-767). Dette viser en kløft i forståelsen og en erkendelse af, at manglende tilpasning af sprog og niveau underminerer formidlingen og dermed IT-sikkerhedsindsatsen. Flere udtalelser understøtter også, at tillid og relationer spiller en vigtig rolle. Når man taler "i øjenhøjde", fremmes både forståelse og engagement. Disse udtalelser kan være et tydeligt tegn på, at rådgiverne forsøger at mitigere modstandsformen *I don't like you*. At skabe nærhed og gensidig respekt gennem inkluderende kommunikation kan derfor være en strategisk måde at reducere modstand og øge modtageligheden for IT-sikkerheds tiltag. Det fremhæves, at folk lytter mere, hvis de føler sig mødt på deres præmisser, og at charme og ydmyghed kan være mere effektivt end teknisk ekspertise (Bilag

20, l. 751-760). Det viser, at sproget ikke kun er teknisk, men også relationelt. Denne betragtning af formidling af et komplekst vidensfelt, udviser vigtigheden af at kunne kontekstualisere sin formidling hvilket harmonerer med SECI-modellen, da det tydeliggør at viden først bliver brugbar, når den *eksternaliseres* og kobles til konkrete erfaringer, samt kombineres og kontekstualiseres i relation til modtagerens forståelseshorisont.

IT-sikkerhedens kompleksitet og tekniske karakter skaber i sig selv en barriere, dog forstærkes denne når fagpersoner ikke oversætter deres viden til modtagerens virkelighed. En ekspert indenfor SMV feltet underbygger denne barriere ude i praksis, hvor der lægges stærkt vægt på at tale i øjenhøjde med SMV'er frem for at tale ned til dem. Informanten omtaler et arrangement som der afholdes for SMV'er, IT-sikkerhed i øjenhøjde, *"simpelthen for at tale et andet sprog end teknikersproget, fordi så står de af hurtigt."* (Bilag 20, l. 730-731), denne udtalelse afspejler Maurers begreb *I don't get it*, idet modtagerne undlader at engagere sig i informationen, når den formidles på en måde, de ikke forstår. Den manglende forståelse kan føre til en form for defensiv respons, *deflection*, hvilket skyldes en følelsesmæssig trussel, der opstår i mødet med komplekst eller teknisk tungt indhold. Som følge heraf fravælger modtagerne aktivt at tilegne sig informationen og risikerer i stedet at glemme eller ignorere den. Dette fænomen kan yderligere forstås gennem Humanokratiets princip *Openness*, hvor en åben kultur omkring IT-sikkerhed, og særligt erkendelsen af manglende indsigt eller viden, kan skabe et trygt rum for dialog. Her bliver det muligt at adressere misforståelser eller usikkerheder, som ellers ville blive undertrykt i mere lukkede eller præstationsorienterede miljøer.

Endvidere fremhæves en udfordring med, at IT-sikkerhedsprofessionelle og studerende ofte mangler de nødvendige kommunikative kompetencer til at formidle komplekse tekniske problemstillinger i et sprog, der er tilgængeligt for ikke-tekniske målgrupper såsom ledere, beslutningstagere eller kunder. En repræsentant fra en uformel organisation samt en formel organisation omtaler formidlingskompetencer hos IT-specialister som følgende:"*Det er jo ekstremt nørdede mennesker, som formentlig har meget svært ved at kommunikere med den base, vi taler om her, SMV'erne.*" (Bilag 12, l. 360-362). Her bliver det understreget, at IT-specialister, ofte med en meget teknisk og specialiseret viden, kan have svært ved at kommunikere med dem uden en tilsvarende teknisk baggrund, som er tilfældet for mange i SMV'er. Dette viser, at der er en kommunikationskløft, der kan forhindre effektiv vidensdeling og samarbejde. Hvis specialisterne ikke er i stand til at kommunikere deres

tekniske viden på en måde som SMV'erne og eller højere ledelseslag i en organisation forstår, risikerer de, at vigtige beslutninger og løsninger ikke bliver tilgængelige for dem, der behøver dem, da videndelingen ikke formår at blive *eksternaliseret* hos dem. Den anden repræsentant fra en uformel organisation taler om at træne IT-specialisters kommunikative skills og soft skills: "*Så får vi også trænet de her kære nørders kommunikative skills og giver dem nogle af de her soft skills (. . .) Det er svært ofte det, at få kommunikationen fra det tekniske lag og op igennem organisationen"* (Bilag 4, l. 375-377). Dette peger på, at kommunikation ikke blot handler om at udveksle information, men også om at kunne formidle den tekniske viden på en måde, som både beslutningstagere og ikke-tekniske kollegaer kan forstå og handle på. Når de tekniske lag ikke effektivt kan kommunikere op i organisationen, risikerer de, at deres løsninger og anbefalinger ikke bliver forstået og implementeret korrekt, hvilket afspejler den type modstand, Maurer's I don't get it. Dermed bliver træning i formidling ikke blot et spørgsmål om faglig udvikling, men en strategisk nødvendighed for at sikre, at IT-sikkerhed får gennemslag i hele organisationen. Her er det væsentligt at bemærke, at humanokratiets idealer om tillid, fællesskab og flade strukturer ikke i sig selv adresserer den teknisk-kommunikative kløft. Dette skaber et dilemma, hvor de teknisk stærkeste ikke nødvendigvis er de bedste til at skabe forandring, hvis de ikke kan formidle deres viden. Det bliver dermed tydeligt, at formidling ikke blot er en soft skill, men en nødvendig forudsætning for, at sikkerhedsarbejdet kan tages seriøst og implementeres effektivt. Hvilket kan imødegå problematikken fra del 1 af analysen, hvor inklusion i feltet er en mangel.

Denne nødvendighed for klar og målrettet kommunikation hænger tæt sammen med virksomhedens kultur. Når IT-sikkerhed reduceres til standardløsninger og hurtige tekniske fix, som eksempelvis "*bare købe et eller andet hos cyberpilot*" uden at engagere organisationen, har det "*nærmest ingen effekt*" (Bilag 12, l. 67-68). Effektiv sikkerhed starter med mennesker, ikke systemer, og fordrer en kultur, hvor medarbejdere forstår deres rolle i det fælles ansvar: "*Det starter med de mennesker, der bruger systemerne*" (Bilag 18, l. 185-186). Det kræver en inkluderende kommunikationsform, hvor formidling ikke skaber afstand, men inddragelse og hvor man, som det påpeges, ikke "står og peger fingre", men hjælper andre med at forstå og handle på truslerne (Bilag 20, l. 596-599). Som førnævnt bliver *eksternalisering* central, idet eksperters tavse viden skal oversættes til sprog og begreber, som resten af organisationen kan forstå og anvende. Det er i denne proces, at

teknisk indsigt bliver til organisatorisk læring og hvor IT-sikkerhed forankres som en fælles praksis frem for et isoleret ekspertområde. Dermed bliver kommunikationen ikke blot et redskab, men en bærer af den kultur, der gør IT-sikkerhed muligt i praksis. Som Maurer fremhæver, kan sikkerhed ikke påtvinges organisationen udefra. Den skal vokse indefra gennem dialog og samarbejde. For at minimere graden af modstand på sikkerhedsimplementeringer, kræver det, at kommunikation er åben, tillidsfuld og inkluderende, ikke for at få folk til at adlyde, men for at gøre dem til aktive medskabere af en IT-sikkerhedskultur. Hvilket Humanokratiet understøtter i deres principper *Openness*, *Ownership* samt *Community*, hvor at inddrage organisationen med autonomi, tilhørsforhold og brud med nuværende paradigmer, kan fjerne mulig modstand mod en forandring.

5.2.5 Kompetencer

I analysedel 1 blev det nævnt, at beslutningstagningen vedrørende IT-sikkerhed i mange SMV'er varetages af individer, som ikke besidder de nødvendige tekniske kompetencer, hvilket understreges i at mange SMV'er opfatter phishing som den største trussel mod deres virksomhed, modsat eksperter som peger på andre trusler som de mest relevante. Dette kan medføre en strukturel uoverensstemmelse mellem det formelle beslutningsniveau og de medarbejdere, der i praksis har indsigt i virksomhedens risici og sikkerhedsbehov. Som det fremgik i afsnittet 5.2.2 "Fællesskab", vælger flere SMV'er uhensigtsmæssigt at nedprioritere IT-sikkerhed til fordel for kortsigtede økonomiske mål. Når den faglige ekspertise ikke inddrages i beslutningsprocesserne, øges risikoen for fejlagtige prioriteringer og en systematisk undervurdering af det aktuelle trusselsbillede, ifølge princippet om meritokrati bør beslutningskraft placeres hos dem med størst faglig indsigt, ikke nødvendigvis hos dem med formel autoritet. I forlængelse af markets-princippet understreges det tilmed, hvordan beslutninger i SMV'er ofte domineres af få ledere, hvilket kan skabe blinde vinkler og confirmation bias. Dette kan begrænse inddragelsen af relevant faglig viden og svække organisationens evne til at håndtere komplekse IT-sikkerhedstrusler effektivt.

Informanterne i empirien var bredt enige om hvilke kompetencer de mente, som var vigtige i forbindelse med at have viden om IT-sikkerhed. Selvom flere informanter også fremhævede betydningen af et et grundlæggende, teknisk fundament for særligt IT-professionelle, var der tre kompetencer, som der var bred enighed om, var særligt vigtige: 1) Indlejret sikkerhedstænkning: "*Jeg synes ikke der er en enkelt færdighed, som er, eller få færdigheder,*

som er vigtige, fordi det der er det vigtige, det er, at man tænker sikkerhed ind i alt, hvad man gør" (Bilag 1, l. 247). 2) Nysgerrighed: Det er afgørende, at man har en nysgerrig tilgang. Eksempelvis udtrykker en informant at; *"Hvis man forstår, hvis man har den her tankegang, den her nysgerrighed for eksempel* (. . .) *Du behøver ikke at være teknisk savvy, du kan bare sidde og se på en side og tænke okay lege lidt med det"* (Bilag 8, l. 433–435). Nysgerrighed er tilmed vigtigt i IT-professionelle, da cybertruslen og dermed kompetencebehovet ændrer sig konstant, og det kan være med til at holde dem opdaterede. Det går hånd i hånd med 3) kreativitet, ligeledes blev fremhævet som en central egenskab, særligt i læringssammenhænge, hvor det handler om at kunne eksperimentere og samarbejde og kunne tænke som en hacker (Bilag 5, l. 271–283). En informant fra et konsulenthus, der rådgiver SMV'er i IT-sikkerhed, understøtter nødvendigheden af disse kompetencer ved at understrege vigtigheden af at være opmærksom på sårbarheder omkring sig. Eksempelvis kan nødvendigheden for en indlejret sikkerhedstænkning ses gennem en PC, der står i hjørnet på kontoret og er tændt, eller WIFI-routeren der står tændt om natten, og bliver sammenlignet metaforisk med at lade sin hoveddør stå åben og ulåst for indbrudstyven (Bilag 14, l. 166-170). Sådanne situationer som denne kan mitigeres gennem en systematisk indsats for videnskabelse i organisationen. På organisatorisk niveau indebærer dette en eksternalisering af tavs viden, hvor erfaringer og praksis omsættes til eksplicitte vidensressourcer såsom dokumentation og vejledninger. På individniveau forudsættes en internalisering af denne viden, hvilket sker gennem tilegnelse og anvendelse af det udviklede materiale. Denne proces danner en kontinuerlig vidensspiral, hvor eksisterende eksplicit viden, både intern og ekstern, løbende *kombineres* og opdateres for at skabe nye læringsmaterialer.

Disse kompetencer er ikke alene vigtige hver for sig, men deres værdi forstærkes i høj grad gennem samspillet mellem dem. Netop dette samspil, og det forhold, at kompetencer som indlejret sikkerhedstænkning, nysgerrighed og kreativitet ikke blot kan indlæres mekanisk, men forudsætter en dybere forståelse og engagement, blev yderligere fremhævet af informanterne. Disse tre kompetencer blev tilmed præsenteret som tæt forbundne og gensidigt forstærkende. Især blev det fremhævet, at det ikke er tilstrækkeligt at lære regler og teknikker udenad, men at det kræver selvstændig, kritisk tænkning og en lyst til at forstå og lege med systemer. Dette fremhæver denne indlejrede sikkerhedstænkning, hvor det ikke handler om at lære IT-sikkerhed som en færdighed, men at det om et grundlæggende mindset. Informanterne skelnede her mellem den generelle medarbejder og IT-professionelle, hvor

sidstnævnte blev mødt med højere forventninger til teknisk kunnen. Denne forskel i forventinger rejser et centralt spørgsmål om, hvorvidt det er generalister eller specialisters kompetencer, der er behov for i SMV'er. Her peger flere informanter på, at specialiseret viden ikke altid er relevant eller realistisk i en SMV-kontekst. Som denne SMV-informant eksempelvis sagde: "*Og så er det jo klart, jo større vi bliver og jo dybere man kan grave ned i materien, jamen så får du også mere og mere brug for specialisterne, men det er vi slet ikke store nok til*" (Bilag 9, l. 335-336). Det peger på, at mange SMV'er er afhængige af bredt funderede medarbejdere, der kan håndtere flere funktioner på én gang, da virksomheden ikke er store nok eller langt nok i deres implementering af IT-sikkerhed til at det ressourcemæssigt giver mening at ansætte snævre specialister, som oftere rekrutteres af større organisationer med flere ressourcer. Denne erkendelse fører videre til en bredere pointe blandt informanterne, nemlig at IT-sikkerhed ikke skulle reduceres til et isoleret ansvar hos IT-afdelingen- eller eksperten, men at det var op til hele virksomheden at løfte opgaven:

> *Vi er på vej ind i et forskningsprojekt med en række andre universiteter i Norden omkring os, og sige jamen IT er ikke IT-sikkerhedsafdelingens eller IT-afdelingens problem, bare det er alles problem. Det er alles opgave at løfte det her, så det at kende sin faglighed, at være fagfaglig dygtig, men også vide, at jeg besidder ikke alle svarene selv så der er nødt til at foregå i en konstellation af flere entiteter, og det kan være svært, når man i små og mellemstore virksomheder ikke engang har råd til en person.* (Bilag 7, l. 228-236).

Ovenstående citat taler stærkt ind i flere af humanokratiets principper, heriblandt *Openness* og *Community.* I takt med at få alle til at løfte opgaven, kan man, frem for at kigge mere de mere operationelle teorier fra Nonaka og Maurer, fokusere på et mere holistisk mindset, der bør implementeres for at fordre denne slags adfærd. Openness peger på, at frie rammer og åbenhed skaber en ånd af innovation og nytænkning. Ved at føre kulturen i virksomheder hen imod dette princip, kan man håbe at nytænkning og innovation fra alle, vil give et stærkere forhold til opgaven. Som følge af dette ville man ved at skabe en kultur båret af Community, hvor man sigter efter at alle medarbejdere oplever et stort tilhørsforhold til både organisationen og problemstillingen, således at de vil mærke motivation ved at løfte i flok. Sidst taler dette ind i princippet om Ownership*,* hvor autonomi og ejerskab over disse problemstillinger kan øge motivationen og viljen til at løfte opgaven og dermed minimere modstand. En SMV konsulent inden for IT-sikkerhed, og tidligere kemiingeniør, kom for

eksempel med en opfordring til at individer proaktivt tænker sikkerhed ind i arbejdet ligesom han havde gjort i sin tidligere branche, hvor man er vant til at følge procedurer samt kigge på personsikkerhed:

> *Så det er sådan, hvad jeg kalder almindelig sikkerhed. Og lige så snart man sætter ordet cyber foran, så går klappen ned på Folketinget. Man ved ikke hvad man skal gøre. I virkeligheden så er det præcis de samme ting man skal gøre.* (Bilag 18, l. 366-387).

Hvis ansatte har en grundlæggende sikkerhedsforståelse, kan det være med til at styrke SMV'ers IT-sikkerhed, fordi ansvaret og viden er tildelt alle i virksomheden og dermed ikke er isoleret til enkelte medarbejdere og eksperter i virksomheden. Som Kocksch og Jensen (2024) formidlede, var det typisk tilfældet at en sådan kollektiv forankring af sikkerhedskompetencer kan modvirke de fragmenterede og improviserede tilgange, der ofte ses i SMV'er, og understøtter behovet for bredere rolleforståelse og vidensdeling.

Dette kan yderligere forklares ved hjælp af SECI-modellens *commitment*-begreb, som nævner, *autonomi*, fremmer kreativitet og motivation, og at det sammen med *intention*, og *miljømæssige fluktuationer* menes at være en faktor, der understøtter evnen til at tilegne sig viden. Et konkret eksempel på brugen af intention i praksis kommer fra en underviser, der aktivt udfordrer sine studerende til at være opmærksomme og tænke selv:

> *Jeg har lige drillet mine studerende i dag med, at på tavlen stod der noget og så kommer de ind og sætter sig ned, og så slukker jeg tavlen og så siger 'hvad for en IP-adresse stod deroppe på tavlen?'.* (Bilag 7, l. 261-263)

Her ses for det første at underviseren forsøger at skabe en bevidsthed rettet mod digitale sårbarheder, i dette tilfælde en IP-adresse. Her understøttes særligt udviklingen af kompetencer som nysgerrighed og evnen til at tænke i sikkerhed, hvor eleverne rettes mod dette specifikke problem eller objekt, hvorved nysgerrighed vækkes. *Intention* handler dog ikke kun om at rette fokus mod et bestemt emne, men også om at forme, hvordan vi forstår og vurderer information, i lyset af vores underliggende værdier og mål. Hvad vi opfatter som vigtigt, værdifuldt eller rigtigt, afhænger af vores overbevisninger, kulturelle baggrund og strategiske retning. Øvelsen går netop ud på at forme elevernes opfattelse af, hvad der værdifuldt:

> *Der er ikke nogen der lige ligesom… det er så sidste gang i kommer ind i et rum og der står en seddel ikke scanner og observere, så i skal hele tiden være observante på at der er noget her der giver anledning til en sårbarhed (. . .) meget af det er sådan noget man skal træne og være bevidst om ikke, og være observant i sine omgivelser.* (Bilag 7, l. 264-267).

Dette viser netop at underviseren forsøger at tilskrive en værdi til IP-adressen, nemlig at det er en potentiel sårbarhed. Han forsøger hermed at lære eleverne at være opmærksomme og have en intentionel opmærksomhed på sårbarheder, som IP-adresser, og dermed give dem en kognitiv ramme af, at IP-adresser er vigtig og værdifuld information. Denne tilgang kan overføres til arbejdet med IT-sikkerhed i en organisation. Ved at skabe en bevidsthed om sårbarheder blandt medarbejderne og tilskrive værdi til potentielle risici, kan organisationer opbygge en kultur, hvor sikkerhed ikke kun er et teknisk ansvar, men en kollektiv indsats. På den måde kan man styrke organisationens evne til at opdage, forstå og håndtere sårbarheder på tværs af alle niveauer.

5.2.6 Delkonklusion

Anden del af analysen har haft til formål at undersøge, hvordan fem centrale dimensioner, læringsmetodikker, fællesskab, viden om IT-sikkerhed, kommunikation og kompetencer, hver især og i samspil kan bidrage til at styrke IT-sikkerheden i SMV'er. Analysen viser, at læring i IT-sikkerhed er mest effektiv, når den er praksisbaseret, kontekstnær og målrettet den konkrete målgruppe. Hands-on undervisning, scenariebaseret læring og mulighed for eksperimentering i trygge rammer skaber betingelser for både individuel og organisatorisk læring. Det teoretiske fundament i SECI-modellen viser her sin styrke, idet viden skal kunne bevæge sig mellem tavs og eksplicit form for at blive forankret i praksis.

Fællesskab fremstår som en bærende organisatorisk og læringsmæssig ramme, der kan modvirke ressourcemangel og faglig isolation i SMV'er. De uformelle samlinger demonstrerer, hvordan frivilligt engagement, tillid og deling af viden kan danne grundlag for både faglig udvikling og praktisk problemløsning. Det er dog en væsentlig pointe, at mange af de nuværende fællesskabsbaserede læringstilbud, såsom Haaukins-platformen, eksisterer på baggrund af private midler, og derfor ikke er sikret bæredygtighed uden statslig støtte. For at SMV'er kan drage nytte af fællesskabsmodellen, kræver det, at der skabes strukturelle og

kulturelle betingelser for åbenhed, samarbejde og læring på tværs af virksomheder og sektorer.

I forlængelse heraf peger analysen af viden om IT-sikkerhed på, at opdateret og relevant viden ofte ikke når ud til dem, der har mest brug for den. Udfordringen skyldes dels mangel på struktureret videndeling og dels, at mange SMV'er outsourcer IT-sikkerheden og dermed afskæres fra den viden, som kunne opbygge intern kapacitet. Dette forstærkes yderligere af manglen på eksperter og de høje omkostninger ved at tiltrække og fastholde kvalificerede medarbejdere. Hvis ikke viden dokumenteres, deles og kontekstualiseres, risikerer den at forblive tavs, lokalt forankret og utilgængelig for det organisatoriske læringsfællesskab.

Kommunikationsdimensionen viser, at formidlingen af IT-sikkerhed er lige så vigtig som det tekniske indhold. Udfordringen i mange SMV'er består i, at ledelsen ofte mangler grundlæggende digital forståelse, hvilket vanskeliggør både strategisk prioritering og daglig praksis. Derfor bliver det afgørende, at formidlingen af IT-sikkerhed sker i øjenhøjde, og at tekniske eksperter udvikler evner til at oversætte komplekse problemstillinger til relevante og meningsfulde budskaber for ikke-tekniske målgrupper. Manglende målgruppeforståelse eller teknisk kommunikation risikerer at fremkalde modstand snarere end læring, hvilket understreger betydningen af relationel og kontekstualiseret formidling.

Endelig viser analysen af kompetencer, at det ikke alene handler om teknisk kunnen, men om et bredere spektrum af evner, der omfatter nysgerrighed, kreativitet og en indlejret sikkerhedstænkning. Særligt i en SMV-kontekst, hvor ressourcerne er begrænsede, er der behov for medarbejdere, der kan agere bredt og omsætte viden til handling i praksis. Kompetencer skal ikke kun tilegnes individuelt, men også forankres kollektivt gennem fælles ansvar, åbenhed og ejerskab, som foreslået i Humanokratiets principper. Det kræver et brud med forståelsen af IT-sikkerhed som et isoleret ekspertområde og en bevægelse mod en mere helhedsorienteret og inkluderende sikkerhedskultur.

6. Diskussion

Dette afsnit har til formål at perspektivere og kritisk reflektere over specialets metodiske valg, analytiske fund og samspillet mellem empiri og teori. Afsnittet diskuterer både styrker

og begrænsninger ved undersøgelsen samt de dilemmaer og muligheder, der opstår, når man arbejder med IT-sikkerhed og kompetenceudvikling i danske SMV'er.

6.1 Metodisk diskussion

I specialet er der bevidst valgt at afdække et bredt udsnit af informanter både geografisk og i forhold til alder, køn og organisatorisk stilling. Dette valg er truffet ud fra et ønske om at belyse både formelle og uformelle aktører inden for feltet, herunder deres viden og praksisser.

Samlet vurderes materialet at give en vis bred dækning af undersøgelsesfeltet. Det skal dog anerkendes, at der fortsat eksisterer mulighed for at identificere yderligere uformelle fællesskaber og formelle aktører samt for at opnå en dybere indsigt i SMV'ernes interne praksis. Det kan diskuteres, om interviewenes længde har været tilstrækkelig. I gennemsnit varede interviewene cirka 30 minutter, hvor enkelte var væsentligt længere og andre en smule kortere. Det kan ikke udelukkes, at længere og mere dybdegående interviews kunne have afdækket yderligere dimensioner i feltet, som ikke er fremkommet i dette speciale. Der skal dog her tages højde for informanternes begrænsede tid og tilgængelighed.

Et muligt alternativ kunne have været at gennemføre et længerevarende kvalitativt casestudie af enten én enkelt uformel samling, SMV eller formel organisation for at opnå en dybere forståelse af deres interne dynamikker, organisering og vidensdannelse. Det kunne have givet mere dybdegående indsigt i de viden og praksisser, der kunne have været med til at præsentere mere konkrete værktøjer for at SMV'er kunne styrke deres cyberresiliens. Med den indsigt der er opstået i dette speciale af SMV segmentets diverse udfordringer med at opnå en basal cyberhygiejne på baggrund af eksempelvis ressourcebegrænsninger, adgang til viden og forståelse af truslen, vil et dybdegående casestudie risikere at blive for snævert og kun brugbart for meget få virksomheder.

En anden metodisk overvejelse, som opstod undervejs i specialets tilrettelæggelse, vedrører begrebet SMV. Indledningsvis blev en SMV defineret med udgangspunkt i årsregnskabsloven (Se uddybet i afsnit Begrebsafklaring 1.1.6). I løbet af specialet blev det dog tydeligt, at denne tekniske definition ikke er tilstrækkelig i en analytisk sammenhæng. Der er markante forskelle mellem virksomheder inden for SMV-segmentet, både hvad angår branche, krav til IT-sikkerhed, digitalt modenhedsniveau, og hvem der leder og arbejder i dem. Forskellen

mellem en virksomhed med 10 ansatte og en virksomhed med 250 ansatte er så betydelig, at det kan være analytisk vanskeligt at betragte dem som én samlet kategori. Dette lægger op til en retrospektiv rettelse til interviewguiden, der kunne have inkluderet spørgsmål til informanternes definition på SMV'er, for at finde ud af, hvilken del af segmentet deres udsagn dækkede over. Dette ville sandsynligvis have givet mulighed for en mere dybdegående forståelse af kontekstspecifikke problemstillinger og praksisser.

Det vurderes dog, at den valgte tilgang fortsat er hensigtsmæssig i en første eksplorativ undersøgelse, netop fordi den bredere tilgang har muliggjort identifikation af tværgående udfordringer og mønstre i SMV-segmentet som helhed. Et eksempel på dette er en informant, som beskrev, hvordan det i Hirtshals Havn typisk er de større virksomheder, der går forrest i forhold til forandring, og hvordan de kan fungere som løftestang for de mindre virksomheder i området. Dette fund kunne potentielt danne udgangspunkt for en mere afgrænset fremtidig undersøgelse, men det kræver adgang til feltet og viden om dynamikkerne, som først blev muliggjort gennem den åbne og eksplorative tilgang, der er anvendt i dette speciale.

6.2 Analytisk diskussion

IT-sikkerhed er i stigende grad blevet en nødvendighed frem for en valgfrihed, også for SMV'er, som stadig tror, at de ikke er mål for angreb. Et centralt dilemma er derfor hvordan de bedst muligt kan udnytte deres allerede begrænsede ressourcer. Nogle SMV'er vælger at outsource deres IT-sikkerhed, da ansættelse af en person med ansvar for IT-sikkerhed ikke er en løsning, indtil de er blevet større. Men ifølge specialets anvendte teori om vidensdannelse, der peger på, at viden er mest effektiv, når den er tæt koblet til praksis samt skabes indefra, betyder denne outsourcing potentielt, at selve viden om IT-sikkerhed forbliver ude af virksomheden. Denne langsigtede ulempe ved outsourcing rejser spørgsmålet om, hvorvidt de alligevel burde investere i ansættelse af generalister, specialister, eller en helt tredje løsning på manglen på viden i virksomhederne. Generalisten kan være en attraktiv løsning, da én persons viden kan dække bredt og kan løse flere opgaver. Dog kan de have svært ved at matche specialisternes tekniske ekspertise. Begge profiler har dog samme ulempe i, at der kan opstå blinde vinkler i deres cyberresiliens, når beslutninger bliver taget på baggrund af et enkelt individs viden. Her kan man rejse spørgsmålet om, hvorvidt en strategisk investering i opkvalificering af allerede eksisterende medarbejdere er mere passende. Her vil det ikke blot være én persons ansvar, men et kollektivt projekt, hvilket stemmer overens med analysens

fund om, at IT-sikkerhed ikke burde isoleres til en enkelt person eller afdeling.
Ideelt burde alle medarbejdere i en SMV have en grundlæggende forståelse for IT-sikkerhed, så de kan beskytte sig selv og bidrage til virksomhedens samlede sikkerhedsniveau. Dog kan der opstå en risiko for udvanding af netop dette ansvar. Når alle formelt set deler ansvaret, bliver det uklart, hvem der faktisk står med det reelle ansvar, og dermed risikerer det at glide mellem hænderne på alle.

Dette aktualiserer spørgsmålet om, hvem der i praksis skal tage initiativ til at starte og drive kommunikation om IT-sikkerhed, særligt i de tilfælde hvor ansvaret er outsourcet. Dertil, hvordan og hvorfra skal de opsøge den nødvendige viden, og hvem skal bære ansvaret for at igangsætte denne proces?

Det er desuden værd at diskutere, hvor realistisk det egentlig er, at tekniske detaljer fuldt ud kan, eller bør, oversættes til en bred organisatorisk forståelse, hvordan skal det kommunikeres, samt skal alle i organisationen have samme niveau af indsigt? Såfremt det er dem i organisationen som er teknisk dygtige, såsom specialisterne, der skal varetage dette ansvar i organisationen, kan dette potentielt have negative konsekvenser for motivationen. Ydermere kan der opstå modstand fra teknisk personale, såfremt de forventes at stå for kommunikation, hvilket ikke matcher deres kernekompetence, og i nogle tilfælde kan være deres svageste kompetence. Opgaven med formidling kan fjerne fokus fra deres tekniske arbejde, hvilket i mange tilfælde er deres primære drivkraft. Hvis virksomheden prioriterer formidling frem for drift, risikerer man at mindske engagement. Omvendt, hvis formidling nedprioriteres, risikerer man, at vigtig viden forbliver tavs og aldrig spredes i organisationen, hvilket kan føre til, at information går tabt og beslutninger træffes på et mangelfuldt grundlag.

Dette peger på et mere grundlæggende spørgsmål: Hvis det ikke er de teknisk dygtige medarbejdere, der skal formidle deres viden, hvem skal så? Kunne det give større udbytte, hvis formidlingsopgaven i højere grad varetages af professionelle med kommunikation som deres kernekompetence, der er vant til at oversætte komplekse emner til forskellige målgrupper? Dette rejser en vigtig overvejelse om balancen mellem teknisk dybde og kommunikativ rækkevidde i arbejdet med IT-sikkerhed.

Udover at kommunikere om IT-sikkerhed skal det også implementeres i SMV'erne hvor der kan opstå en praktisk udfordring i at lære hele virksomheden om grundlæggende forståelse af IT-sikkerhed. Ligesom virksomheders teknologiske modenhed varierer, gør det samme sig gældende internt blandt medarbejderne. Den store forskel i teknologiske forudsætninger og erfaringer kan gøre det vanskeligt at undervise hele organisationen i selv grundlæggende IT-sikkerhed. Det betyder dog ikke, at det er umuligt. Flere uformelle organisationer har vist, at læring med fordel kan segmenteres efter målgrupper og kompetenceniveau. Eksempelvis anvendes hands-on læringsaktiviteter som CTF'er, hvor opgaver og læringsmål tilpasses forskellige niveauer, hvilket muliggør en mere inkluderende og effektiv læringsproces på tværs af forskellige faglige udgangspunkter. Et godt eksempel herpå er Haaukins, som ifølge informanter både bliver brugt i det uformelle og det formelle som læringsplatform.

Samtidig tilføjer uformelle samlinger et sekundært socialt medium som fungerer som fællesskabsstyrkende. Dette skaber ikke blot socialt engagement, men også dybde i læringen gennem socialisering og erfaringsudveksling. Dog er indgangen til læring i sådanne sammenhænge ofte individbaseret og drevet af egen motivation. Det fungerer godt i frivillige læringsfællesskaber, men i virksomheder, især SMV'er, hvor medarbejdernes kompetencemæssige forudsætninger og motivation for at lære varierer betydeligt, og i nogle tilfælde kan være præget af tvang eller pålæg, kan fællesskabet blive udfordret. Her kan der i højere grad risikere at opstå en naturlig segmentering, som risikerer at underminere den fælles læring særligt hvis læringen bliver individualiseret og konkurrencepræget eksempelvis gennem målinger, quizzer eller synliggørelse af "fejl" i awarenesskampagner. Hvor uformelle læringsmiljøer bruger fællesskabet som en læringsmotor, risikerer virksomhedernes interne initiativer at svække fællesskabet, hvis ikke de designes med blik for de sociale dynamikker og interne relationer.

Men selv hvis fællesskabet lykkes at blive etableret, løser det ikke nødvendigvis hele problemet. En anden, og mindst lige så central, udfordring opstår, hvis læringsaktiviteterne mangler en klar intention. Med andre ord: Selv hands-on læring, der ellers betragtes som en effektiv metode til at koble teori og praksis, kan mislykkes, hvis ikke der er tænkt over, hvorfor læringen finder sted, og hvordan den skal anvendes i hverdagen. Dette betyder, at implementationen og planlægningen af selv de mest roste læringsmetodikker, inden for hands-on læring, burde overvejes nøje. Dette aktualiserer behovet for, at virksomheder gør sig bevidste om, hvorfor og hvordan de investerer i træning og læring, særligt mindre

virksomheder der typisk har sparsomme ressourcer. I analysen gives der flere eksempler på, hvordan awarenessprogrammer er blevet et standardprodukt, ofte valgt på et fejlagtigt grundlag, hvor phishing antages at være den primære trussel. Det er dermed ikke blot manglen på intention, men tilmed en mangel på viden og ressourcer, der kan føre til valg af generiske løsninger, som ikke nødvendigvis matcher virksomhedens reelle behov eller modenhedsniveau. Med andre ord opstår der en problematik i, at virksomhederne først skal have nok viden om IT-sikkerhed til at vurdere, hvilke løsninger passer til deres behov, men på samme tid skal denne løsning være med til at give dem denne viden om IT-sikkerhed. Dermed burde viden allerede eksistere forud for investering af eksempelvis awarenessprogrammer

Et generelt fund i dette speciale er fraværet af strukturerede og praksisnære læringsfællesskaber i SMV-segmentet, som ellers ses i formelle og uformelle uddannelsesmiljøer, der deles om for at løfte ressourcen samlet. Her benyttes fællesskaber aktivt til at udvikle og dele læringsmaterialer og skabe trygge rammer for eksperimentering og faglig udvikling. Denne form for socialiseret læring er med til at styrke deltagernes evne til at omsætte viden til praksis. I modsætning hertil står mange SMV'er alene med ansvaret for at opbygge viden om IT-sikkerhed, en opgave, der for mange opleves som både kompleks, overvældende og ressourcekrævende.

Et alternativ til denne tilgang kunne være at anskue IT-sikkerhed som en kollektiv opgave, der varetages i fællesskab. Flere informanter foreslår her etablering af branchefællesskaber eller lokale netværk, hvor SMV'er i fællesskab kan finansiere adgang til specialiseret rådgivning og opdaterede læringsressourcer. Det kunne eksempelvis være gennem fælles sikkerhedskoordinatorer, delte konsulentydelser eller adgang til læringsværktøjer, som stilles til rådighed for alle deltagere. På den måde bidrager hver virksomhed med et mindre beløb, men får adgang til en samlet løsning, der ellers ville være uopnåelig for den enkelte, samt kan sparre med hinanden om oplevelsen, succeser og udfordringer. Dog for at accelerere processen kan et konkret forslag være, at staten i højere grad understøtter denne udvikling, ikke ved at stille nye krav, som det kendes fra reguleringer som NIS2, men ved at bidrage med midler og agere facilitator af at etablere og drive regionale eller kommunale netværk og fællesskaber. På den måde kan fællesskabet blive en løftestang for et segment, der halter efter i feltet.

Det kan dog diskuteres, hvordan sådanne fællesskaber skal organiseres for at sikre, at viden ikke blot deles, men også forankres og omsættes i praksis. Virksomheder kan være tilbageholdende med at deltage i åbne netværk, fordi de frygter at udstille egne mangler. Det betyder, at der skal være fokus på at skabe trygge læringsrum, hvor det er legitimt at stille spørgsmål, begå fejl og dele erfaringer på tværs. Derudover må der også tages højde for de konkurrencemæssige spændinger, der kan opstå i branchefællesskaber. Det kan derfor diskuteres om det er mere hensigtsmæssigt at segmentere fællesskaberne ud fra modenhedsniveau, virksomhedsstørrelse eller geografisk placering, snarere end branchetilhørsforhold.

På baggrund af fundene i (afsnit 5.2 Analysedel 2) kan det argumenteres, at fællesskabsbaserede løsninger har potentiale til at skabe mere robuste og langsigtede kompetenceløft i SMV-segmentet, sammenlignet med individuelle og eksternt forankrede løsninger. Men det kræver, at disse organiseres med blik for både tillid, fleksibilitet og balance mellem bidrag og udbytte. Heri ligger en væsentlig diskussion i specialet, nemlig hvorvidt det er nok, at virksomheder køber sig adgang til ekspertise, eller om det er nødvendigt, at viden og ansvar også forankres i virksomheden selv. I så fald skal fællesskaber ikke blot være adgangsgivere, men også katalysatorer for reel læring og internalisering, ellers risikerer løsningen blot at være en kollektiv variant af den klassiske outsourcingmodel.

6.3 Specialets placering i eksisterende forskning

Dette afsnit har til formål at fremhæve de fund i specialet, som nuancerer eller udfordrer de eksisterende forskningsresultater, som blev præsenteret i afsnit 2. Gennemgangen følger derfor ikke en kronologisk struktur, men fokuserer udelukkende på de områder, hvor specialet bidrager med nye perspektiver eller stiller spørgsmålstegn ved eksisterende forskningsresultater.

Tidligere forskning har peget på, at fleksible træningsformer såsom e-læring og mikrocertificeringer kan understøtte kompetenceudvikling hos nuværende medarbejdere, og dermed være med til at imødekomme det stigende IT-sikkerhedsbehov hos SMV'er. Fundene i dette speciale understøtter denne konklusion i brede træk, men går ind og tilføjer en vigtig dimension, før at disse træningsformer kan have størst effekt, nemlig intentionen i udvælgelsen af træningen. På trods af disse træningsformers fleksible format, der gør, at

forskellige medarbejdere med varierende kompetencemæssige forudsætninger kan lære om IT-sikkerhed på flere niveauer, burde SMV'er sikre, at der er en strategisk tanke og retning bag implementeringen af træning. Alternativt kan de risikere at investere i generiske løsninger, som forhindrer egentlig vidensdannelse og praktisk forankring i hverdagen.

Dernæst har eksisterende forskning identificeret, at outsourcing i stigende grad bliver anvendt som løsning til deres IT-sikkerhedsbehov, samt at nogle ikke stiller krav til leverandøren heromkring. Dog har fundene i dette speciale tilføjet yderligere til denne pointe: Det understreges, at når SMV'er overlader ansvaret for deres IT-sikkerhed til eksterne leverandører, uden at stille kvalificerede krav eller følge op på løsningerne, fralægger de sig samtidig det ansvar og den læring, der kunne styrke deres interne cyberresiliens. Dette kan i praksis føre til en manglende integration af IT-sikkerhed i organisationen, ikke alene fordi trusselsbilledet overlades til tredjeparter, men også fordi intern viden og kompetenceudvikling udebliver. Det opnås således ikke den vidensdannelse, som er nødvendig for at kunne stille krav til eksterne leverandører, evaluere på IT-sikkerhed initiativer eller handle proaktivt. Disse resultater indikerer et behov for en mere kritisk tilgang til outsourcing, hvor SMV'er forud for investering, i løsninger fra eksterne leverandører, opbygger intern viden i organisationen samt behovsafklaring heraf. Fraværet af dette kan føre til suboptimale løsninger og en svækket sikkerhedskultur.

Endvidere præsenteres det i eksisterende forskning, at der er et behov for tættere samarbejde mellem erhvervslivet og uddannelsesinstitutioner for at kunne tilrettelægge pensumdesignet med henblik på at rette det mod erhvervslivets efterspørgsel på kompetencer. Fundene i dette speciale opstiller dog en væsentlig barriere for, at SMV'er kan indgå i dette samarbejde. Blandt andet har SMV'er en antagelse om, at de ikke er interessante nok til at blive angrebet, at deres syn på det reelle trusselsbillede er fejltaget, samt har de ikke en grundlæggende viden om IT-sikkerhed. Dette betyder at, hvis de skal indgå i disse samarbejder, skal de først opbygge denne grundlæggende forståelse, for at kunne præcisere hvilke kompetencer de har behov for, og dermed også engagere sig i uddannelsesinitiativer, der kunne være relevante. Dette skaber en selvforstærkende udfordring, hvor manglende viden hæmmer både efterspørgslen på kompetencer og udviklingen af samarbejder, der kan afhjælpe netop denne mangel.

7. Konklusion

På baggrund af 21 interviews af informanter der enten besidder ekspertviden om, eller indgår i uformelle samlinger, formelle uddannelser og SMV'er, har dette speciale dannet et detaljeret billede af de udfordringer og muligheder, der viser sig for SMV-segmentet. Dette er udført med det formål at besvare problemformuleringen:

"*Hvilken viden og hvilke praksisser fra nuværende formelle og uformelle uddannelser og samlinger kan benyttes af SMV-segmentet i Danmark til at imødekomme det stigende IT-sikkerhedsbehov?*"

Analysen viste først, at basal cyberhygiejne ofte er fraværende, respondenter beskrev forældede systemer og økonomisk motiverede kompromiser, der gør selv simple angrebsvektorer som phishing og ransomware effektive, og gør SMV'er til et nemt mål for trusselsaktører. Disse tekniske mangler forstærkes af en strukturel mangel på kompetencer, forstærket af stramme lønrammer og rekrutteringsudfordringer der gør det vanskeligt for SMV'er at ansætte specialister, mens uddannelsesinstitutioner selv har svært ved at holde på erfarne undervisere. Hertil kommer en tavshedskultur, hvor frygten for at udstille sig som uvidende hæmmer åben videndeling både internt og mellem virksomheder. Endeligt mangler mange virksomheder mekanismer til at omsætte viden, erhvervet gennem medarbejders egne tavse kompetencer, til daglig praksis.

For at forstå disse dynamikker blev fundene diskuteret i lyset af tre teoretiske perspektiver. Nonakas SECI-model tydeliggjorde, at viden først får organisatorisk værdi, når tavse erfaringer socialiseres, eksternaliseres, kombineres og igen internaliseres som rutiner. Rick Maurers modstandsbegreb fremhævede, at modstand mod sikkerhedsinitiativer ofte bunder i uforståelse, frem for modvilje heraf, hvilket understreger behovet for oversættelse fra teknisk til forretningsmæssigt sprog. Endeligt viste Humanokratiet, at flade strukturer, ejerskab og eksperimenterende læringsmiljøer er afgørende for, at ny viden forankres bredt i organisationen.

På baggrund af disse analyser og teoretiske refleksioner står det klart, at der ikke findes frem til én samlet løsning, der kan anvendes på tværs af SMV segmentet. Specialet viser, at de udfordringer, som virksomheden står overfor, både er grundlæggende og samtidig komplekse,

fordi virksomhederne adskiller sig betydeligt fra hinanden. I stedet peger resultaterne på, at arbejdet med IT-sikkerhed må gribes an gennem flere forskellige tiltag, der hver især kan bidrage til at styrke SMV'ernes modstandskraft.

Det første tiltag, der kan styrke IT sikkerheden i SMV segmentet, er etablering og understøttelse af faglige fællesskaber. Analysen viser, at både formelle og uformelle miljøer trækker på fællesskabsbaseret læring og videndeling som centrale mekanismer for kompetenceudvikling. Dog er det tydeligt, at fællesskaber alene ikke er tilstrækkelige i SMV-konteksten. Der bør i stedet etableres branchefællesskaber, som kan målrette indsatser og læringsforløb til de specifikke udfordringer, behov og risici, som kendetegner forskellige brancher. Dette øger både relevansen og anvendeligheden af læringen og skaber mulighed for at koble praksisnær viden med branchekontekstuel forståelse.

Det andet tiltag er et styrket fokus på intention i valget og anvendelsen af læringsressourcer. Som analysen har vist, fører mangel på viden om trusselsbilledet og læringsmetoder ofte til, at SMV'er vælger generiske løsninger, som ikke adresserer deres reelle behov. Eksempelvis reduceres awareness kampagner i mange tilfælde til generiske phishingtests, som ikke skaber varig læring eller organisatorisk forankring. Der er derfor behov for, at SMV'er bliver i stand til at træffe mere kvalificerede beslutninger om deres investeringer i IT-sikkerhed. Her peger analysen på værdien af kombineret og målrettet hands-on læring, hvor hele organisationen involveres, og læring kobles direkte til virksomhedens risikobillede og konkrete praksis. Læring skal ikke blot være informerende, men også have intention.

Det tredje tiltag er forbedret kommunikation og klarere rolleafklaring i relationen mellem SMV'er og deres IT-leverandører. I mange tilfælde hersker der usikkerhed om, hvem der har ansvaret for IT-sikkerhed, både ved outsourcing og ved køb af standardiserede løsninger. Analysen viser, at denne uklarhed kan føre til en falsk tryghed og til, at kritiske sikkerhedsopgaver falder mellem to stole. Det er derfor afgørende, at der skabes transparens i aftaler om ansvar, roller og sikkerhedsniveauer. Samtidig bør leverandørrelationen betragtes som en potentiel læringsressource, hvor erfaringer og viden fra leverandøren bringes i spil hos virksomheden. Dette forudsætter dog, at SMV'en har tilstrækkelig indsigt til at stille de rette spørgsmål og efterspørge den nødvendige dokumentation. Her er det vigtigt at være opmærksom på den digitale kompleksitet, der præger mange SMV'ers systemlandskab.

Manglende overblik over systemer, adgange og integrationer kan skabe blinde vinkler i sikkerheden og gør det vanskeligt at vurdere egne sårbarheder.

Et fjerde tiltag på baggrund af fund i analysen er, at løsningen på manglen på IT-sikkerhedskompetencer ikke nødvendigvis skal findes blandt allerede eksisterende IT-fagpersoner, men i højere grad blandt nye profiler, som kan opbygge relevante kompetencer gennem praksisnær læring. Der argumenteres for at inddrage personer uden traditionel IT baggrund, som gennem hands-on learning, fællesskabsbaseret vidensopbygning og kontekstforståelse kan udvikle sig til brugbare ressourcepersoner inden for IT-sikkerhed, særligt i SMV-segmentet. Det er et afgørende bidrag til kompetenceløsningen, da man undgår at dræne andre kritiske områder for arbejdskraft og i stedet udvider feltets kapacitet. Her er det relevant at tænke i fleksible og modulære efteruddannelsesforløb samt anerkendelse af uformelle kompetencer, eksempelvis gennem CTF-deltagelse, mentorordninger eller communityprojekter.

Femte tiltag på baggrund af et gennemgående tema i analysen er fraværet af en koordineret og tilgængelig støttefunktion målrettet SMV'ers konkrete behov. I dag findes der ingen instans, der samler og formidler relevante værktøjer, trusselsinformation og læringstilbud på en måde, der er tilpasset SMV'er. Et statsligt understøttet SMV-CERT kunne fungere som et lavpraktisk og tillidsvækkende kontaktpunkt, hvor virksomheder kan få vejledning uden salgspres. Dette ville kunne reducere afhængigheden af tilfældige leverandørkontakter og øge chancen for, at SMV'er får adgang til opdateret og relevant viden. Samtidig kunne centret fungere som bindeled til de uformelle fællesskaber og understøtte både national koordinering og lokal forankring.

Litteraturliste

Aalborg Universitetsbibliotek. (u.å. -a). *Protect yourself, others and content*. Hentet fra https://www.en.aub.aau.dk/students/generative-ai/protect-yourself-others-and-the-content

Aalborg Universitetsbibliotek. (u.å. -b). *Good academic practice when using generative AI*. Hentet fra https://www.en.aub.aau.dk/students/generative-ai/good-academic-practice

Arctic Wolf (2025, 26. februar). *2025 Arctic Wolf Threat Report*. https://arcticwolf.com/resource/aw/arctic-wolf-threat-report-2025

Bindah, E. V., (2019). Adoption of snowball sampling technique in an exploratory study of disabled entrepreneurship. In Sage Research Methods Cases Part 2. SAGE Publications, Ltd., https://doi.org/10.4135/9781526487438

Danmarks Statistik. (2025). *Virksomhedernes anvendelse af it efter virksomhedens størrelse og branche (ITAV15)*. Hentet 25. maj 2025 fra https://www.statistikbanken.dk/ITAV15

Danmarks Statistik. (2024). *KOT Hovedtal 2024: 26. juli*. https://www.statistikbanken.dk/ITAV15

De Danske Cybermesterskaber. (u.å.). *Cybermesterskaberne | Mesterskaberne i cyber security*. Hentet 19. maj 2025 fra https://www.cybermesterskaberne.dk/

Det Kriminalpræventive Råd. (2025, 29. april). *It-kriminalitet i tal*. https://dkr.dk/it/it-kriminalitet-i-tal

Digitaliseringsstyrelsen. (2023). *Digital sikkerhed i danske SMV'er 2023*. https://digst.dk/media/45589/digital-sikkerhed-i-danske-smver-2023_endelig0310-a.pdf

Edmonds, W. M., (2019). Snowballing … #prayforme: A qualitative study using snowball sampling. In Sage Research Methods Cases Part 2. SAGE Publications, Ltd., https://doi.org/10.4135/9781526491039

Egholm, L. (2014). *Videnskabsteori: En grundbog*. Hans Reitzels Forlag.

Europa-Kommissionen. (2012). *Forslag til Europa-Parlamentets og Rådets forordning om det indre marked for elektronisk kommunikation* [KOM(2012) 485 endelig]. https://www.eu.dk/samling/20121/kommissionsforslag/kom(2012)0485/forslag/1192200/1451417.pdf

Europa-Kommissionen. (2022). *DESI 2022 – Danmark: Indeks for den digitale økonomi og det digitale samfund*. DESI_2022__Denmark__dk_BApwkRVCXt8yQS86txUoQ54SY_88744.pdf

Forsvarets Efterretningstjeneste. (2024). *Udsyn 2024: En efterretningsbaseret vurdering af de ydre vilkår for Danmarks sikkerhed og varetagelsen af danske interesser*. https://www.fe-ddis.dk/da/produkter/Risikovurdering/risikovurdering/udsyn-2024/

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2012). Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. *Organizational Research Methods*, *16*(1), 15–31. https://doi.org/10.1177/1094428112452151

Goupil, F., Laskov, P., Pekaric, I., Felderer, M., Dürr, A., & Thiesse, F. (2022). Towards understanding the skill gap in cybersecurity. I *Proceedings of the 27th ACM Conference on Innovation and Technology in Computer Science Education – Vol. 1* (s. 477–483). Association for Computing Machinery. https://doi.org/10.1145/3502718.3524807

Griffiths, C. (2025, 1. april). *The latest cyber crime statistics*. AAG IT Support. https://aag-it.com/the-latest-cyber-crime-statistics/

Hamel, G., & Zanini, M. (2020). *Humanocracy: Creating organizations as amazing as the people inside them*. Harvard Business Press.

Harboe, T. (2006). Indføring i samfundsvidenskabelig metode (4. udg., 4. oplag 2009). Samfundslitteratur.

Iacovos Kirlappos, Simon Parkin, and M. Angela Sasse. 2015. "Shadow security" as a tool for the learning organization. SIGCAS Comput. Soc. 45, 1 (February 2015), 29–37. https://doi-org.zorac.aub.aau.dk/10.1145/2738210.2738216

IBM. (2024). *Cost of a data breach report 2024*. https://www.ibm.com/reports/data-breach

Kocksch, L., & Jensen, T. E. (2024). *The mundane art of cybersecurity: Living with insecure IT in Danish small- and medium-sized enterprises*. *Proceedings of the ACM on Human-Computer Interaction, 8*(CSCW2), Article 354, 1–17. https://doi.org/10.1145/3686893

Maurer, R. (2010). Beyond the wall of resistance (2 udg.). Bard Press.

Naderifar, M., Goli, H., & Ghaljaei, F. (2017). Snowball sampling: A purposeful method of sampling in qualitative research. *Strides in Development of Medical Education*, *14*(3), e67670. https://doi.org/10.5812/sdme.67670

Nonaka, I. (1994). *A dynamic theory of organizational knowledge creation*. *Organization Science, 5*(1), 14–37. https://doi.org/10.1287/orsc.5.1.14

Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). *A systematic literature review on the cyber security*. International Journal of Scientific Research and Management, 9(12), EC-2021-669–710. https://doi.org/10.18535/ijsrm/v9i12.ec04

Prümmer, J., van Steen, T., & van den Berg, B. (2024). *A systematic review of current cybersecurity training methods*. Computers & Security, 136, 103585. https://doi.org/10.1016/j.cose.2023.103585

Ruoslahti, H., Coburn, J., Trent, A., & Tikanmäki, I. (2021). Cyber skills gaps – A systematic review of the academic literature. *Connections: The Quarterly Journal*, *20*(2), 33–45. https://doi.org/10.11610/Connections.20.2.04

SMVdanmark. (u.å.). *Fakta om SMV'erne*. Hentet 19. maj 2025 fra https://smvdanmark.dk/analyser/fakta-om-smverne

Stentoft, J., Mikkelsen, O. S., Schmitt, O., Keating, V. C., Theussen, A., Peressotti, M., Mayer, P., Kankam-Boateng, J., & Tumchewics, L. A. (2024). Cybersikkerhed i små og mellemstore danske produktionsvirksomheder.

Tanggaard, L., & Brinkmann, S. (2020). Interviewet: Samtalen som forskningsmetode. I S. Brinkmann, & L. Tanggaard (red.), *Kvalitative metoder: En grundbog* (3. udg., s. 33-64). Hans Reitzels Forlag.

Uddannelses- og Forskningsministeriet. (2024). *KOT Hovedtal*. https://ufm.dk/uddannelse/statistik-og-analyser/sogning-og-optag-pa-videregaende-uddannelser/grundtal-om-sogning-og-optag/kot-hovedtal

Undervisningsministeriet. (2008). *Realkompetencevurdering inden for voksen- og efteruddannelse* (1. udg.). Ministeriet for Børn og Undervisning. https://www.uvm.dk/-/media/filer/uvm/publikationer/uddannelse-og-undervisnin

UNESCO. (2011). *Revision of the International Standard Classification of Education (ISCED 2011)* (36 C/19). United Nations Educational, Scientific and Cultural Organization. https://unesdoc.unesco.org/ark:/48223/pf0000215619

Yingling, J., & McClain, M. (2015). Snowball sampling, grounded theory, and theoretical sampling: Roles in methamphetamine markets. I *SAGE Research Methods*. https://doi.org/10.4135/978144627305014555098

Zach, L. (2006). Using a multiple–case studies design to investigate the information-seeking behavior of arts administrators. *Library Trends, 55*(1), 4–21. https://doi.org/10.1353/lib.2006.0055

Zhang, J., Bu, H., Wen, H., Liu, Y., Fei, H., Xi, R., Li, L., Yang, Y., Zhu, H. & Meng, D. (2025). *When LLMs meet cybersecurity: A systematic literature review*. *Cybersecurity, 8*(55). https://doi.org/10.1186/s42400-025-00361-w