Styrelsen for Samfundssikkerhed

ANALYSE AF CYBER- OG INFORMATIONSSIKKERHED I DANMARK

December 2025

Indhold

Baggrund for analysen

Styrelsen for Samfundssikkerhed har udarbejdet en analyse som grundlag for regeringens udspil til en ny strategi for cyber- og informationssikkerhed. Analysen skal danne et overblik over cybersikkerheden på tværs af samfundet og identificere de væsentlige udfordringer på området med henblik på igangsættelse af relevante initiativer. Som grundlag for den nye strategi indgår desuden erfaringer fra tidligere strategier, hændelseserfaring og lovmæssige forpligtelser, herunder NIS 2-direktivet.

Analysen fokuserer på områder, som ikke er direkte omfattet af kravene i NIS 2-loven. Analysen omhandler følgende fire temaer: Borgernes cybersikkerhed, cybersikkerheden i små og mellemstore virksomheder, cybersikkerhed i kritisk infrastruktur og den danske cyberindustri og -forskning. I de følgende afsnit beskrives analysens væsentligste resultater.

Borgernes cybersikkerhed

Selvom borgerne er bevidste om truslerne og generelt har et højt vidensniveau, omsættes det ikke til sikker adfærd

Ifølge analysen *Danskernes Informationssikkerhed 2024* er 72 pct. af danskerne i høj grad eller i meget høj grad opmærksomme på digital svindel. Alligevel viser tal fra samme analyse, at hovedparten af befolkningen bruger det samme password til alle eller flere af deres enheder/tjenester, ligesom mere end hver femte dansker er villig til at dele deres kodeord, og under halvdelen af befolkningen anvender stærke adgangskoder og tager sjældent sikkerhedskopiering af filer og dokumenter. Derudover mangler borgerne forståelse for risici ved manglende sikker digital adfærd.

Tal fra samme analyse viser, at de unge er mere tilbøjelige til at dele deres kodeord til e-mails eller sociale medier, ligesom de er mere tilbøjelige til at genbruge deres kodeord. Tal fra *Danskernes Informationssikkerhed 2022* har omvendt vist, at den ældre befolkning i højere grad synes sårbare over for særligt investeringssvindel og kontaktbedrageri, hvilket blandt andet kan skyldes større formuer.

Ifølge tal fra Det Kriminalpræventive Råd var over halvdelen (54 pct.) af borgerne i 2024 uenige i, at det er tydeligt, hvor de kan søge hjælp, mens kun 17 pct. angav, at de ved, hvor de skal søge hjælp og støtte i tilfælde af, at de udsættes for digital svindel.

Digital svindel er en udbredt trussel mod borgerne, og borgerne har sværere ved at gennemskue svindlen

Digital svindel er en meget udbredt trussel mod borgerne, og svindlen påvirker borgere på tværs af alder, køn og uddannelsesniveau. Tal fra Nationalt Center for It-relateret økonomisk Kriminalitet (NCIK) viser, at der har været en stigning i antal anmeldte sager vedrørende digital svindel i 2024, ligesom tal fra Finans Danmark understøtter, at der generelt er stigende økonomiske konsekvenser heraf.

Cybersikkerheden i små- og mellemstore virksomheder

Stor variation i sikkerhedsniveau på tværs af størrelse og brancher

Flere undersøgelser viser, at mindre virksomheder generelt har implementeret færre sikkerhedstiltag end større virksomheder, og især mikrovirksomheder med fem til ni ansatte har et lavt digitalt sikkerhedsniveau ifølge tal fra 2024 fra Danmarks Statistik. Flere analyser viser ligeledes uafhængigt af hinanden, at der er variation mellem brancher, hvor virksomheder i nogle brancher er længere fremme i arbejdet med it-sikkerhedstiltag end i andre brancher. Informations- og kommunikationsbranchen synes at være længst fremme i arbejdet med digital sikkerhed, mens bygge- og anlægssektoren generelt har mindre fokus på digital sikkerhed end øvrige brancher.

40 pct. har ikke et sikkerhedsniveau, der passer til deres risikoprofil

Tal fra Styrelsen for Samfundssikkerheds analyse *Digital sikkerhed i danske SMV'er* viser, at 40 pct. af SMV'erne i 2024 fortsat ikke har it-sikkerhedstiltag om stærke adgangskoder, hvilket kan gøre det nemmere for it-kriminelle at bryde koder og få adgang til virksomhedens systemer og data. SMV'erne påpeger særligt mangel på tid, ressourcer og kompetencer som forklaring på manglende sikkerhedstiltag. Ligeledes viser analysen, at 40 pct. af SMV'erne har et digitalt sikkerhedsniveau, der ikke stemmer overens med deres risikoprofil.

Undersøgelser viser, at både store virksomheder og SMV'er er sårbare over for angreb. 60 pct. af SMV'erne vil slet ikke eller kun i lav grad kunne udføre deres kerneopgaver uden adgang til centrale it-systemer.

Cybersikkerhed i kritisk infrastruktur

Nye forpligtelser med CER og NIS 2

Med NIS 2- og CER-lovene får en række aktører i cyberøkosystemet nye forpligtelser, og der vil blive stillet nye krav til den nationale CSIRT's (Computer Security Incident Response Team) kapaciteter særligt med fokus på hændelsesindberetning og -håndtering. Den nationale CSIRT har blandt andet til formål at overvåge og analysere cybertrusler på nationalt plan og yde bistand til væsentlige og vigtige enheder, jf. NIS 2-loven.

Komplekst cyberøkosystem med mange aktører

Det danske cyberøkosystem er komplekst, og det er vigtigt, at der faciliteres et effektivt samarbejde mellem aktører på forskellige niveauer, herunder internationalt for at beskytte samfundet mod angreb i cyberdomænet. Der er behov for veldefinerede roller for aktørerne, så alle ved, hvad de skal gøre i tilfælde af en hændelse eller krisesituation. Der er ligeledes behov for fokus på effektivisering af samarbejde, videndeling og øvelser for at styrke den operative kapacitet.

Behov for at træne, øve og teste cyberberedskabet

Det er nødvendigt at træne, øve og teste beredskabet i og på tværs af sektorer og organisationer, så man er bedre stillet, hvis en reel situation skulle opstå. Ved at øge fokus på træning og beredskab, skabes der større klarhed om ansvar og rollefordeling for aktører i forskellige sektorer, herunder hvor der er snitflader.

Den danske cyberindustri og -forskning

En voksende branche med potentiale for øget koordination mellem virksomheder, forskning og myndigheder

Cyberindustrien er voksende med mange forskellige aktører, som udtrykker behov for øget koordination og fælles sigte for branchens udvikling. Der er derfor potentiale for øget koordinering mellem virksomheder, forskning og myndigheder og et fælles strategisk sigte for branchens udvikling.

Stærke forskningsmiljøer inden for blandt andet kryptologi, it-sikkerhed, dataorganisering og algoritmer

Danmark har stærke forskningsmiljøer inden for kryptologi, it-sikkerhed, dataorganisering og algoritmer samt særligt potentiale i teknologier, der både kan anvendes civilt og militært.

Efterspørgsel på kompetencer og kvalificeret arbejdskraft

Udfordringer med at rekruttere kvalificeret arbejdskraft og specialiserede kompetencer opleves som en væsentlig barriere for vækst og udvikling i cybersikkerhedsbranchen. Særligt blandt startups og scaleups opleves der udfordringer med at rekruttere de rette kompetencer.

1 Indledning

Det danske samfund står over for alvorlige cybertrusler. Nedbrud og cyberangreb på den kritiske infrastruktur kan have store samfundsmæssige konsekvenser og påvirke os alle sammen. Det stiller krav til myndigheders og virksomheders operative samarbejde og hændelseshåndtering i tilfælde af hændelser og kriser, ligesom det stiller krav til øget videndeling, en klar rolle- og ansvarsfordeling, monitorering, detektion og øvelsesaktivitet, både nationalt og internationalt.

Med digitaliseringen af samfundet er de kriminelles metoder i stigende grad også blevet digitale, og cyberkriminalitet påvirker i dag dagligt borgere og virksomheder. Særligt er digital svindel en udbredt kriminalitetsform, som rammer mange borgere. Cyberkriminalitet kan have store økonomiske og personlige konsekvenser for ofrene og svække borgernes tillid til de offentlige myndigheder. Samtidigt kan et cyberangreb på små- eller mellemstore virksomheder (SMV'ere) f.eks. resultere i, at mange borgeres private oplysninger lækkes på internettet, og at virksomheder mister deres forretningsgrundlag. Det kan i værste fald betyde, at ramte virksomheder må dreje nøglen om, og det kan, grundet leverandørkæder, have konsekvenser for øvrige virksomheders drift.

Den danske cyberindustri er en voksende branche med potentiale for yderligere udvikling, men det kan være svært for startups i branchen at opnå markedsgennembrud blandt andet på grund af manglen på specialiserede kompetencer. Den danske cyberindustri kan bidrage til at styrke Danmarks konkurrenceevne og øge europæisk modstandsdygtighed over for globale hændelser. Nye teknologier, f.eks. kunstig intelligens, kan medvirke til at øge truslen fra blandt andet cyberkriminalitet samtidigt med, at de også kan skabe nye muligheder for at styrke bolværket mod statslige hackere, it-kriminelle og nedbrud.

Styrelsen for Samfundssikkerhed har udarbejdet en analyse som grundlag for regeringens udspil til en ny strategi for cyber- og informationssikkerhed, der skal understøtte sikkerheden bredt på tværs af samfundet. Analysen skal danne et overblik over cybersikkerheden på tværs af samfundet og identificere de væsentlige udfordringer på området.

Formålet med analysen er, at der med den nye strategi igangsættes initiativer med størst mulig effekt. Som grundlag for den nye strategi indgår desuden erfaringer fra tidligere strategier, hændelseserfaring og lovmæssige forpligtelser, herunder NIS 2-direktivet.

NIS 2-direktivet er en grundsten i arbejdet med cyber- og informationssikkerhed i Danmark. NIS 2-direktivet er implementeret i dansk ret med NIS 2-loven, som trådte i kraft den 1. juli 2025. Et stort antal virksomheder og myndigheder vil som følge af NIS 2-direktivet skulle leve op til en række nye og skærpede krav til deres cyber- og informationssikkerhed, ligesom der vil være en øget tilsyns- og håndhævelsesforpligtigelse. Den nationale strategi har blandt andet til formål at skabe en politisk ramme for øget koordinering mellem de kompetente myndigheder i henhold til NIS 2 og de kompetente myndigheder med henblik på udveksling af oplysninger om risici, cybertrusler og hændelser samt om ikke-cyberrelaterede risici, trusler og hændelser og udøvelse af tilsynsopgaver. Strategien vil bygge videre på kravene i NIS 2-loven, ligesom det også følger af et krav i direktivet, at den nationale strategi skal vedtage politikker til fremme af aktiv cyberbeskyttelse som led i en bredere defensiv strategi.

NIS 2-direktivets artikel 7 stiller ligeledes krav til, at den nationale strategi blandt andet skal højne cyber- og informationssikkerheden for de målgrupper, der ikke er omfattet af NIS 2, navnlig borgere og SMV'er. Analysearbejdet fokuserer derfor på områder, som ikke er direkte omfattet af kravene i NIS 2-loven. Analysen omhandler følgende fire temaer: Borgernes cybersikkerhed, cybersikkerheden i små og mellemstore virksomheder, cybersikkerhed i kritisk infrastruktur og cyberindustri og -forskning.

Analysen er udarbejdet på baggrund af konsolidering af eksisterende viden samt ekspert-inddragelse, som primært er indhentet fra medlemmer af Cybersikkerhedsrådet og Cybersikkerhedspagten. Derudover er relevante input fra branche- og forbrugerorganisationer inddraget løbende i analysearbejdet.

Cybertruslen mod Danmark 2025

- Truslen fra cyberkriminalitet er **MEGET HØJ**. Cyberkriminelle rammer hele tiden ofre i Danmark med forskellige cyberangreb, fra omfattende ransomware-angreb til tyveri af sensitiv viden og svindel af den enkelte borger.

- Truslen fra cyberspionage er **MEGET HØJ**. Særligt Rusland og Kina retter løbende cyberangreb mod danske organisationer i forsøg på at få adgang til viden af blandt andet udenrigs- og sikkerhedspolitisk karakter samt indsigt i informationer med betydning for Danmarks forsvar.

- Truslen fra cyberaktivisme er **HØJ**. Særligt pro-russiske hackere rammer løbende danske mål med DDoS-angreb, og i nogle tilfælde gøres også forsøg på at manipulere med operationel teknologi (OT), som f.eks. da et dansk vandværk blev ramt i slutningen af 2024. Det er sandsynligt, at nogle pro-russiske hackergrupper har forbindelse til den russiske stat.

- Truslen fra destruktive cyberangreb er **MIDDEL**. Det er særligt Ruslands risiko-villighed i forhold til brugen af hybride virkemidler, der kan komme til udtryk i form af wiper-angreb og angreb mod OT med begrænsede effekter.

- Truslen fra cyberterror er **INGEN**. Styrelsen for Samfundssikkerhed vurderer, at ingen militante ekstremister aktører aktuelt har kapacitet til eller intention om at udføre cyberterror mod Danmark.

Cybersikkerhed i rammen af EU

EU har etableret en sammenhængende lovgivningsramme på det digitale område, særligt på cybersikkerhedsområdet, som er forklaret nedenfor.

Forordningen om horisontale cybersikkerhedskrav til produkter med digitale elementer (CRA) introducerer krav til cybersikkerhed i software- eller hardwareprodukter, der har en digital komponent. Kravene omfatter f.eks. produktsikkerhed fra design til udfasning, rapportering af sårbarheder og udgivelse af sikkerhedsopdateringer.

Cybersikkerhedsforordningen (CSA) sikrer certificeringsordninger, så man som køber kan identificere sikre produkter, tjenester og processer. Certificeringen kan potentielt bruges til at dokumentere efterlevelse af visse krav i CRA.

NIS 2 stiller krav til informationssikkerhed i en bred vifte af sektorer, herunder transport, sundhed og digital infrastruktur. Formålet er at styrke samfundets cybersikkerhed ved at sikre, at kritiske sektorer arbejder systematisk med risikostyring, hændelseshåndtering og sikkerhedstiltag. NIS 2-omfattede virksomheder og myndigheder skal indberette væsentlige hændelser via Virk.dk. Håndteringen af hændelser efter NIS 2-direktivet er delt ud på de respektive kompetente myndigheder for hver sektor. Dertil er NIS 2 implementeret specifikt for telesektoren i *Loven om sikkerhed og beredskab i telesektoren* og de tilhørende bekendtgørelser, og på samme måde for energiområdet. Finansområdet reguleres tilsvarende af NIS 2, men via særskilt direktiv og lovgivning (DORA).

Hvor NIS 2 relaterer sig til cybersikkerhed, omhandler CER-direktivet (Critical Entities Resilience) den fysiske sikkerhed i de samme sektorer, herunder blandt andet energi-, transport-, fødevare- og sundhedssektoren og pålægger sektorerne at beskytte sig mod en bred vifte af trusler og hændelser. Formålet med loven er at sikre, at samfundsvigtige funktioner kan opretholdes i bedst muligt omfang – også ved alvorlige hændelser som naturkatastrofer, terror eller tekniske sammenbrud. Enheder, der bliver omfattet af CER-loven, udpeges af de kompetente myndigheder, som er fastsat af Ministeriet for Samfundssikkerhed og Beredskab. Udpegningen af enheder skal senest ske den 17. juli 2026. Når de kritiske enheder er blevet gjort bekendt med deres udpegning, har de mindst ni måneder til at opfylde kravene i CER.

Med forordningen om cybersolidaritet (CYSOL) oprettes et europæisk cybersikkerhedsvarslingssystem, bestående af nationale og tværnationale cyberknudepunkter (såkaldte Cyber-hubs). Medlemsstater kan tilslutte sig disse på frivillig basis. Derudover oprettes en cyberreserve, hvorigennem medlemslande og godkendte tredjelande kan modtage assistance til støtte cyberhændelser. Moldova har blandt andet lige fået adgang til reserven.

Nedenstående *figur 1* giver et overblik over den europæiske lovgivningsramme på cyberområdet.

Figur 1: Europæisk lovgivningsramme på cyberområdet

2 Borgernes cybersikkerhed

Det følgende kapitel afdækker det aktuelle situationsbillede vedrørende borgernes cybersikkerhed, herunder cybertruslen mod borgerne, samt beskriver de forskellige tendenser inden for digital svindel. Herefter beskrives forskellene blandt befolkningsgrupper samt borgenes digitale adfærd.

2.1 Cybertruslen mod borgerne

Cybertruslen mod borgere vokser i takt med den digitale udvikling. Ifølge Styrelsen for Samfundssikkerheds årlige trusselsvurdering *Cybertruslen mod Danmark* fra 2025, er truslen fra cyberkriminalitet meget høj, og særligt digital svindel er en udbredt trussel. Ligeledes viser trusselsvurderingen, at cyberkriminalitet typisk er udført af apolitiske og opportunistiske aktører med henblik på at opnå et så stort økonomisk udbytte som muligt. Cyberkriminalitet kan have store personlige konsekvenser for ofrene og svække borgernes tillid til de offentlige myndigheder.

Bekymringen for cyberkriminalitet er udbredt i befolkningen. Styrelsen for Samfundssikkerheds undersøgelse Danskernes Informationssikkerhed fra 2024 viser, at phishing er den mest udbredte digitale trussel mod borgerne, som rammes blandt andet gennem direkte svindel eller ved, at kriminelle tilegner sig personfølsomme oplysninger fra virksomheder og myndigheder, såsom CPR-numre og kreditoplysninger, der senere misbruges. Undersøgelsen viser, at 76 pct. af danskerne i 2024 havde været udsat for forsøg på digital svindel inden for det seneste år, og 22 pct. var blevet svindlet eller franarret informationer.Samtidigt viser tal fra IDA's undersøgelse *Privacy og datasikkerhed* fra marts 2025, at 55 pct. af befolkningen har oplevet forsøg på en eller flere typer af it-kriminalitet de seneste to år.

> **76 PCT**. AF DANSKERNE I 2024 HAR VÆRET UDSAT FOR FORSØG PÅ DIGITAL SVINDEL INDEN FOR DET SENESTE ÅR OG **22 PCT**. ER BLEVET SVINDLET ELLER FRANARRET INFORMATIONER.

Den samme undersøgelse fra IDA fra marts 2025 som nævnt ovenfor viser, at 60 pct. er bekymrede for identitetstyveri. Ifølge *Styrket bekæmpelse af digital svindel,* som er en undersøgelse foretaget af Finans Danmark i 2023, var hver anden dansker bekymret for at blive udsat for
it-relateret økonomisk kriminalitet. Ligeledes viser analysen *Danskernes Informationssikkerhed 2024* en høj og stigende bekymring for digital svindel blandt befolkningen - fra 29 pct. i 2022 til 35 pct. i 2024. I samme analyse fremgår det, at kun 61 pct. af danskerne føler sig godt rustet mod digital kriminalitet, hvilket er et fald fra 67 pct. i 2022.

2.2 Digital svindel

Danske borgere udsættes i stigende grad for it-kriminalitet og forsøg på digital svindel. I 2024 opgjorde National enhed for Særlig Kriminalitet (NSK) i deres årsrapport, at de modtog 39.824 anmeldelser om it-relateret økonomisk kriminalitet – en stigning på 14 pct. siden 2023 og 40 pct. siden 2020. Den primære årsag til stigningen fra 2023 til 2024 er kontaktbedrageri, hvor kriminelle manipulerer ofre til selv at overføre penge eller udlevere følsomme oplysninger.

De samlede økonomiske konsekvenser af digital svindel kan være vanskelige at opgøre præcist. Ifølge Finans Danmarks analyse *Styrket bekæmpelse af digital svindel* viser tal fra Danmarks Nationalbank og Finans Danmark, at det i 2023 lykkedes kriminelle at svindle for 464 mio. kr. relateret til netbank-, investerings-, dating- og betalingskortsvindel. Det er en stigning på knap 108 mio. kr. i forhold til 2022, svarende til en vækst på 30 pct. Denne udvikling understreger, at digital svindel fortsat er et stigende problem.

Når svindlerne franarrer oplysninger fra borgerne: phishing, smishing, vishing

Phishing er en form for svindel, hvor svindlere forsøger at franarre borgere personlige oplysninger som f.eks. betalingsoplysninger, adgangskoder eller MitID-oplysninger. Offeret kan f.eks. blive lokket til at udlevere disse oplysninger ved at klikke på et link, der leder til en falsk login-side, hvor loginoplysningerne kan indsamles. Phishing kan foregå via mail (phishing), sms (smishing) eller telefon (vishing).

Smishing er særligt udbredt. I 2024 omhandlede 30 pct. af alle opkald til cyberhotlinen sms-relateret svindel, mens f.eks. opkald vedrørende misbrug eller spærring af MitID udgjorde syv procent.

Selvom smishing er udbredt, vurderes det dog af Det Kriminalpræventive Råd i undersøgelsen *Ansvars- og rollefordelingen i forebyggelsen af IT-relateret økonomisk kriminalitet* fra 2024 rettet mod voksne borgere, at økonomiske tab kun registreres i omkring halvdelen af de rapporterede smishing-tilfælde, hvilket peger på, at en stor del
af angrebene opfanges eller ignoreres, inden de resulterer i økonomiske tab.

2.2.1 Svindel med betalingssystemer og –midler.

Svindel med betalingssystemer og -midler dækker over en bred vifte af økonomiske forbrydelser, hvor kriminelle udnytter digitale betalingsløsninger, bankkonti og personlige oplysninger
til at gennemføre uautoriserede transaktioner. Det kan ske gennem hacking, phishing eller misbrug af stjålne kort- og kontooplysninger.

Særligt de former for svindel, hvor kriminelle misbruger tjenester som MitID eller opnår uautoriseret adgang til borgeres bankkonti, synes at være faldende. Ifølge Nationalt Center for It-relateret økonomisk Kriminalitets (NCIK) årsrapport fra 2024 er antallet af anmeldelser vedrørende denne type svindel faldet med 40 pct. fra 2023 til 2024.

En lignende tendens ses i Finans Danmarks opgørelser over netbankssvindel. Her fremgår det, at antallet af sager, hvor ofre mistede penge, faldt med over 24 pct. fra 2023 (9.127 sager) til 2024 (6.919 sager). Det dækker både over netbanksvindel med og uden brug af cyberangreb såsom malware samt social engineering, hvor borgere narres til selv at udlevere følsomme oplysninger. Ligeledes faldt det samlede økonomiske tab som følge af denne form for svindel med næsten 22 pct. i samme periode ifølge Finans Danmark.

Nationalbanken peger i undersøgelsen *Svindel og misbrug med digitale betalinger i Danmark* på, at faldet i netbanksvindel i høj grad kan tilskrives, at bankerne har intensiveret deres indsats mod digital svindel blandt andet gennem implementering af tekniske løsninger såsom en daglig beløbsgrænse for straksbetalinger uden forudgående kontakt med banken samt øvrig regulering. Derudover fremhæver NCIK i deres årsrapport fra 2024, at en styrket phishing-sikring af MitID har bidraget til at reducere antallet af denne type svindelsager.

Svindel med betalingskort kan f.eks. skyldes, at kortoplysninger er blevet kompromitteret ved tyveri, aflurede pinkoder eller ved misbrug gennem falske betalingslinks eller netbutikker. Ifølge NCIK's seneste årsrapport faldt antallet af anmeldelser vedrørende misbrug af kortoplysninger med fem pct. fra 2023 til 2024. Imidlertid viser tal fra Nationalbankens undersøgelse *Svindel og misbrug med digitale betalinger i Danmark*, at på trods af et generelt fald i misbruget af danske betalingskort i de seneste år, har der siden 2021 været en stigende tendens inden for svindel i forbindelse med udenlandsk e-handel – særligt uden for EU. I 2023 blev der misbrugt danske betalingskort for 219 mio. kr. alene i udenlandsk e-handel, hvilket svarer til ca. 75 pct. af det samlede kortmisbrug. Denne form for svindel sker ofte via falske hjemmesider, hvor forbrugere lokkes til at handle uden at opdage, at deres kortoplysninger stjæles og misbruges.

Nationalbanken peger på, at denne stigning skyldes, at europæiske sikkerhedskrav, f.eks. indførelsen af to-faktorgodkendelse, kan have skubbet kortmisbrug uden for Europa.

2.2.2 Samhandels- og investeringssvindel

Tal fra Styrelsen for Samfundssikkerheds analyse *Danskernes Informationssikkerhed* fra 2024 viser, at omkring hver tredje dansker har oplevet svindel i forbindelse med online handel på den ene eller anden vis. 19 pct. af danskerne har været udsat for svindel via fupannoncer eller fupbutikker, 17 pct. har oplevet bedrageri ved handel mellem private, og 16 pct. har været udsat for investeringssvindel, hvilket indikerer, at digital svindel rammer bredt på tværs af handels- og investeringsplatforme.

> **19 PCT.** AF DANSKERNE HAR VÆRET UDSAT FOR SVINDEL VIA FUPANNONCER ELLER FUPBUTIKKER, **17 PCT.** HAR OPLEVET BEDRAGERI VED HANDEL MELLEM PRIVATE, OG **16 PCT.** HAR VÆRET UDSAT FOR INVESTERINGSSVINDEL

Ifølge NCIK's årsrapport fra 2024 steg antallet af anmeldelser vedrørende samhandelssvindel med fire pct. fra 2023 til 2024. Denne type svindel omfatter primært sager, hvor borgere bliver snydt i forbindelse med køb af fysiske varer såsom elektronik, tøj og tasker, der aldrig bliver leveret. En anden variant af samhandelssvindel er billetsvindel, hvor forbrugere betaler for koncert- eller sportsbilletter via online markedspladser, men aldrig modtager de købte billetter.

En lignende form for digital svindel, der har været i kraftig vækst, er investeringssvindel, som dog ikke omfattes af NCIK's opgørelser over anmeldelser. Her lokkes borgere til at investere i fupprojekter, der lover højt afkast, men hvor pengene i realiteten går tabt. Ofte involverer investeringssvindel, at ofrene opfordres til at indsætte penge i tilsyneladende legitime

handelsplatforme, der i virkeligheden er kontrolleret af svindlere. Ifølge Finans Danmarks tal for investeringssvindel fra 2024 steg antallet af sager, hvor svindlerne lykkedes med at opnå en økonomisk gevinst, med 33 pct. fra 2023 (836 sager) til 2024 (1.112 sager). Det samlede økonomiske tab for denne type svindel voksede markant fra næsten 48 mio. kr. i 2023 til 95 mio. kr. i 2024.

Finans Danmark peger i en nyhed fra marts 2025 på, at de kriminelle i høj grad udnytter annonceplatforme på sociale medier til at nå deres ofre. Dermed er disse platforme afgørende for svindlernes succes, da de her kan opsætte troværdige annoncer, der lokker investorer i fælden.

2.2.3 Kontaktbedrageri

Omfanget af kontaktbedrageri er steget markant og kan have store økonomiske konsekvenser for ofrene. Ifølge NCIK's årsrapport fra 2024 var det rekordhøje antal anmeldelser om økonomisk it-kriminalitet i 2024 primært drevet af en vækst i netop denne type svindel.

Antallet af anmeldte sager om kontaktbedrageri mod private borgere steg fra 2.754 i 2023 til 7.728 i 2024, svarende til en stigning på 181 pct. Ifølge data fra en analyse gennemført af Wilke for Forbrugerrådet Tænk og Trygfonden oplever ofrene ved kontaktbedrageri ofte større økonomiske tab. Samme analyse viser, at det gennemsnitlige tabsbeløb for svindel-webshops, phishing og abonnementsfælder er under henholdsvis 5.000 kr., 9.000 kr. og 3.500 kr., mens det gennemsnitlige tabsbeløb for kontaktbedrageri og malware ligger på omkring 14.000 kr. – beregnet ud fra selvrapporterede tabsbeløb i undersøgelsen.

> ANTALLET AF ANMELDTE SAGER OM KONTAKTBEDRAGERI MOD PRIVATE BORGERE STEG FRA **2.754** I 2023 TIL **7.728** I 2024, SVARENDE TIL EN STIGNING PÅ **181 PCT.**

En særlig variant af kontaktbedrageri, som har været i kraftig vækst, er den såkaldte "bekendt i knibe"-svindel. Her udnytter gerningspersonerne ofrets følelser ved at udgive sig for at være en nær pårørende, typisk et barn, der har akut brug for økonomisk hjælp. Svindlen foregår typisk via sms, hvor offeret modtager en besked med ordlyden "Hej mor/far", efterfulgt af en forklaring om, at afsenderen har mistet sin telefon, er blevet låst ude af MitID eller har fået sit betalingskort spærret. Derefter opfordres offeret til at overføre penge hurtigst muligt. Fra 2023 til 2024 steg antallet af sager med denne svindelform med hele 637 pct., hvilket indikerer en stærk tendens, hvor kriminelle i stadig mere udpræget grad spiller på borgernes følelser, når de skal franarre dem penge.

Udviklingen i kontaktbedrageri synes samlet set at indikere, at svindlere i stigende grad anvender forskellige former for social engineering-strategier til at udnytte deres ofre. Social engineering er en bred betegnelse for teknikker, hvor kriminelle manipulerer eller narrer personer til at afsløre fortrolige oplysninger eller udføre handlinger, der kompromitterer deres sikkerhed, ved at udnytte menneskelig tillid og adfærdspsykologi. Dette understreger behovet for øget opmærksomhed og forebyggende indsats for at beskytte borgere mod denne form for digital kriminalitet. Samtidigt kunne tendensen være et udtryk for, at det er blevet sværere for svindlerne at svindle via netbank og MitID grundet det øgede brug af tekniske foranstaltninger *jf.*

afsnit 2.2.1.
Dette kunne indikere et øget behov for at uddanne borgerne i, hvordan de beskytter sig mod kontaktbedrageri.

Hvad er datingsvindel?

Datingsvindel, også kendt som kærlighedssvindel, er en form for svindel, hvor gerningspersonerne opbygger et tillidsforhold til offeret over længere tid, ofte via datingplatforme eller sociale medier, med det formål at få dem til at sende penge under påskud af en nødsituation eller fælles fremtidsplaner. Modsat kontaktbedrageri som helhed synes niveauet af datingsvindel dog at være relativt stabilt. Ifølge tal fra Finans Danmark fra april 2024 om datingsvindel, har det samlede økonomiske tab ved denne type svindel ligget nogenlunde konstant mellem 17 og 22 mio. kr. i perioden 2019-2023, med undtagelse af 2020, hvor tabet kun var lige over 6 mio. kr. Fra 2023 til 2024 anslår Finans Danmark dog, at der har været en stigning på 13,7 pct. i antallet af sager fra 490 til 557.

Finans Danmark bemærker, at da denne type af svindel ofte er forbundet med stor skam og sårede følelser, vurderes der at være et markant mørketal af sager, som aldrig bliver indberettet eller anmeldt.

2.2.4 Brug af kunstig intelligens i svindelmetoderne

Ifølge Styrelsen for Samfundssikkerheds temaartikel *Hackere misbruger generativ AI* fra april 2024, bliver svindelmetoderne mere avancerede og sværere at gennemskue, da cyberkriminelle nu kan anvende kunstig intelligens (AI) til at målrette deres angreb – eksempelvis via sofistikeret social engineering. Der findes ikke tal på, hvor meget af svindlen, der er AI-drevet, men Europol vurderer i rapporten *The changing DNA of serious and organised crime* fra 2025, at cyberkriminelle netværk udnytter kunstig intelligens til blandt andet automatisering og omgåelse af sikkerhedsforanstaltninger, hvilket gør cyberangreb mere skalerbare og effektive.

2.3 Forskelle i befolkningssegmenter

Styrelsen for Samfundssikkerheds analyse *Danskernes informationssikkerhed* fra 2025 viser, at unge mellem 18 og 29 år i højere grad er mål for phishingforsøg end andre aldersgrupper. 25 pct. af danskere, der angiver at have mødt phishingforsøg, befinder sig i denne aldersgruppe, hvilket kan skyldes deres øgede digitale tilstedeværelse og brug af sociale medier, som forhøjer deres eksponering over for svindlere.

Digital svindel rammer bredt og påvirker borgere på tværs af alder, køn og uddannelsesniveau. Dog viser de nyeste undersøgelser, at visse grupper er mere udsatte end andre – og at især unge mænd ser ud til at være en voksende risikogruppe.

Eksempelvis viser den seneste udgave af *Danskernes Informationssikkerhed*, at unge frem for ældre – og særligt unge mænd – oftere bliver ofre for økonomisk svindel i forbindelse med samhandel. Således har 17 pct. af de unge oplevet svindel i forbindelse med køb og salg på digitale platforme, mens 19 pct. af alle mænd mellem 18 og 29 år har fået franarret deres

informationer. Dette kan skyldes, at unge generelt er mere tilbøjelige til at handle online og via private handelsplatforme, hvilket øger deres eksponering for svindel.

En tidligere udgave af samme analyse fra 2022 viser, at ældre personer var særligt sårbare over for svindel relateret til investeringer, herunder i falske aktier eller kryptovaluta. Blandt borgere over 60 år var det 29 pct., der har været udsat for forsøg på investeringssvindel i 2022. Blandt de 18-29-årige var det 16 pct. En artikel fra 2024 af Faglige Seniorer med titlen *Pas på falske investeringer* viser, at dette muligvis skyldes, at ældre ofte har større økonomiske opsparinger og samtidig kan have mindre erfaring med at identificere digitale svindelmetoder. En anden forklaring kunne være, at svindlerne målretter deres annoncer mod ældre, men dette vides ikke med sikkerhed. Forskningsstudiet *Disseminating fraud awareness and prevention advice to older adults: perspectives on the most effective means of delivery* fra 2024 med data fra Storbritannien og USA viser desuden, at konsekvenserne af svindlen også ofte er alvorligere for de ældre, fordi de dels oplever større økonomiske tab ved svindlen og dels rammes hårdere psykisk.

Ifølge undersøgelsen *Ansvars- og rollefordelingen i forebyggelsen af IT-relateret økonomisk kriminalitet rettet mod voksne borgere* fra Det Kriminalpræventive Råd var over halvdelen (54 pct.) af borgerne i 2024 uenige i, at det er tydeligt, hvor de kan søge hjælp, mens kun 17 pct. angiver, at de ved, hvor de skal søge hjælp og støtte i tilfælde af, at de udsættes for økonomisk svindel på nettet. Ligeledes svarer over 63 pct., at de ønsker, at råd og vejledning om digital svindel synliggøres mere. Manglen på kendskab til hjælpetilbud kan være en medvirkende faktor til, at anmeldelsestallet for it-relateret kriminalitet er relativt lavt. I analysen *Danskernes Informationssikkerhed* fra 2024 vurderer Styrelsen for Samfundssikkerhed på baggrund af tal fra Danmarks Statistisk, at det kun er omkring en femtedel af ofrene, der faktisk anmelder it-kriminalitet til politiet. De reelle tal for økonomisk svindel på nettet må derfor formodes at være væsentligt højere, end de officielle statistikker viser. Den lave anmeldelsesrate kan samtidig betyde, at politiet ikke får adgang til vigtig information, der kunne understøtte efterforskningsarbejdet og forbedre indsatsen mod digital svindel.

> MANGLEN PÅ KENDSKAB TIL **HJÆLPETILBUD** KAN VÆRE EN MEDVIRKENDE FAKTOR TIL, AT ANMELDELSESTALLET FOR **IT-RELATERET** KRIMINALITET ER RELATIVT LAVT.

Det skal tilføjes, at Finans Danmark i en analyse fra december med titlen *500 bankansatte bekæmper digital svindel hver eneste dag* fra 2023 estimerede, at bankerne med hjælp fra it-systemer, overvågning og dedikeret personale formår at stoppe over halvdelen af alle svindelforsøg, før de rammer forbrugerne.

2.4 Borgernes digitale sikkerhedsadfærd

Ifølge Danmarks Statistiks årlige undersøgelse *It-anvendelse i befolkningen* fra 2024 bruger 86 pct. af befolkningen mellem 15-89 år internettet dagligt. Men selvom danskerne er digitale og i høj grad er opmærksomme på digitale trusler, omsættes denne bevidsthed ikke altid til sikre handlinger. Styrelsen for Samfundssikkerhed's analyse *Danskernes Informationssikkerhed* fra 2024 og IDA's *Privacy og datasikkerhed* fra 2025 viser f.eks., at hovedparten af befolkningen

bruger det samme password til alle deres enheder/tjenester eller bruger nogle af deres passwords flere steder, ligesom mere end hver femte dansker er villige til at dele deres kodeord.
Ifølge Danmarks Statistiks årlige undersøgelse *It-anvendelse i befolkningen* fra 2024 anvender under halvdelen af befolkningen stærke adgangskoder (anvender 12 karakterer eller derover i sine kodeord) og tager jævnlig sikkerhedskopiering af filer og dokumenter.

> HOVEDPARTEN AF BEFOLKNINGEN BRUGER DET SAMME PASSWORD TIL ALLE DERES ENHEDER/TJENESTER ELLER BRUGER NOGLE AF DERES PASSWORDS FLERE STEDER, LIGESOM **MERE END HVER FEMTE DANSKER** ER VILLIGE TIL AT DELE DERES KODEORD.

Undersøgelserne *It-anvendelse i befolkningen* af Danmarks Statistik fra 2024 og *Digital svindel i Danmark* fra 2025 af Wilke for Forbrugerrådet Tænk viser, at den yngre del af befolkningen i mindre grad følger forebyggende sikkerhedsanbefalinger sammenlignet med øvrige aldersgrupper. *It-anvendelse i befolkningen* fra 2024 viser eksempelvis, at de unge er mere tilbøjelige til at dele deres kodeord til e-mails eller sociale medier med andre sammenlignet med de ældre generationer, ligesom de unge er mere tilbøjelige til at genbruge deres kodeord til private e-mails m.m. Tal fra IDA's undersøgelse *Privacy og datasikkerhed* bekræfter denne tendens og peger på, at de yngre følger færre sikkerhedsanbefalinger.

Samtidig viser analyserne, *It-anvendelse i befolkningen* og *Danskernes informationssikkerhed*, begge fra 2024, at unge har større tiltro til deres digitale sikkerhedsviden end ældre, ligesom de oplever, at de er bedre klædt på til at genkende digital svindel såsom falske hjemmesider, e-mails og SMS'er. Ifølge *It-anvendelse i befolkningen* angiver 10 pct. af danskerne mellem 15-24 år, at de slet ikke eller i mindre grad kan genkende digital svindel, mens tallet for de 75-84-årige er 30 pct. Derudover viser *Danskernes Informationssikkerhed*, at mænd i højere grad end kvinder tilkendegiver, at de har tilstrækkelig viden om sikkerhed på nettet.

Endvidere viser analysen, at der fra 2022 til 2024 er sket en udvikling i, hvor danskerne søger viden om cyber- og informationssikkerhed. Mens færre henter information fra traditionelle medier, bliver venner, familie og bekendte en stadig vigtigere kilde - og er nu den primære måde, danskerne tilegner sig viden om digital sikkerhed. Samme analyse viser, at relativt flere unge bruger sociale medier til at orientere sig om digital sikkerhed sammenlignet med andre aldersgrupper, mens relativt flere ældre benytter deres omgangskreds til viden på området. Omkring hver fjerde borger modtager information om cyber- og informationssikkerhed gennem deres arbejdsplads eller uddannelsesinstitution. En andel som, baseret på selvrapporterede svar fra borgerne, er faldet fra 2022 til 2024.

Ligeledes viser analysen, at to tredjedele af befolkningen oplever fortsat udfordringer med at opretholde en sikker digital adfærd i hverdagen. Blandt dem, der ikke benytter forebyggende sikkerhedstiltag, skyldes det ofte en opfattelse af, at digital sikkerhed er besværligt, unødvendigt eller tidskrævende. Konkret mener 23 pct. af befolkningen, at det er vanskeligt at holde styr på sikkerhedsforanstaltninger, 14 pct. glemmer at følge anbefalingerne,15 pct. oplever, at de er

begrænset af manglende viden og 9 pct. har svært ved at forstå anbefalingerne for en sikker digital adfærd.

Analysen viser desuden, at mange borgere oplever cybersikkerhed som kompleks og uoverskueligt. Der er ofte en manglende forståelse for, hvilke risici der følger med lav digital sikkerhed, f.eks. at deres personlige data kan være attraktive for kriminelle. Hele 16 pct. af befolkningen vurderer ikke, at der er stor risiko for at blive snydt, når de handler eller færdes på nettet og 14 pct. anser det ikke for sandsynligt, at andre kan få adgang til deres data.

> MANGE BORGERE OPLEVER CYBERSIKKERHED SOM **KOMPLEKS OG UOVERSKUELIGT.** DER ER OFTE EN MANGLENDE FORSTÅELSE FOR, HVILKE RISICI DER FØLGER MED LAV DIGITAL SIKKERHED, F.EKS. AT DERES **PERSONLIGE DATA** KAN VÆRE ATTRAKTIVE FOR KRIMINELLE.

2.5 Delkonklusion vedrørende borgernes cybersikkerhed

For borgere er digital kriminalitet blevet en del af hverdagen. Digital svindel er en udbredt trussel mod borgerne, og svindlen påvirker borgere på tværs af alder, køn og uddannelsesniveau. Der har været en stigning i den digitale svindel og de økonomiske konsekvenser heraf. Dette kan skyldes, at svindelmetoderne er blevet mere avancerede f.eks. ved brug af kunstig intelligens, hvilket gør det svært for borgerne at gennemskue svindlen. Der har været et fald i nogle typer af svindel. Eksempelvis er svindel med MitID samt netbanksvindel faldende, hvilket kan skyldes flere tekniske foranstaltninger og regulering i kampen mod digital svindel. På den anden side har særligt kontaktbedrageri været i stigning, hvor svindlerne benytter psykologiske greb og udnytter borgernes tillid. Denne tendens kunne være et udtryk for, at det er blevet sværere for svindlerne at svindle via netbank og MitID, tyr svindlerne til andre metoder. Dette kunne indikere et øget behov for at uddanne borgerne i, hvordan de beskytter sig mod særligt kontaktbedrageri, ligesom der er behov for, at myndighederne følger med i, hvilke metoder svindlerne udvikler, så de kan tilrettelægge målrettede indsatser herefter.

Med hensyn til borgernes sikkerhedsadfærd skiller særligt unge og ældre sig ud. De unge viser en tendens til at bruge færre sikkerhedsforanstaltninger som f.eks. at opdatere antivirusprogrammer samt at bruge stærke og unikke adgangskoder. Dette kan hænge sammen med, at de har en anden risikoforståelse end ældre, og at flere unge end ældre ikke på samme måde har opfattelsen af et eget ansvar for at løfte sikkerheden. På den anden side synes særligt de ældre at være sårbare over for visse svindeltyper, såsom investeringssvindel. Hos borgerne er en af de største barrierer for en sikker digital adfærd en manglende forståelse for behovet for sikker digital adfærd, der opleves som teknisk og tidskrævende, ligesom over halvdelen af befolkningen svarer, at de ønsker, at råd og vejledning om digital svindel synliggøres mere. Dette peger på, at der er behov for at gøre det nemmere for borgerne at agere sikkert. Mange tilkendegiver desuden, at de ikke er tilstrækkeligt informeret om, hvor de kan få hjælp, hvis de bliver ramt, hvilket indikerer, at der er behov for mere tydelig og ensartet kommunikation til borgerne.

3 Cybersikkerheden i små og mellemstore virksomheder

Nedenstående kapitel præsenterer først cybertruslen mod virksomheder i Danmark, herunder cybertruslen mod SMV'erne. Herefter beskrives tilstanden for SMV'ernes brug af tekniske it-sikkerhedsforanstaltninger, medarbejdernes kompetencer samt ledelsesforankringen af arbejdet med cyber- og informationssikkerhed i SMV'erne. Til sidst gennemgås, hvad SMV'erne oplever som barrierer og drivers i arbejdet med digital sikkerhed.

3.1 Truslen mod virksomheder generelt

Styrelsen for Samfundssikkerhed vurderer i *Cybertruslen mod Danmark* fra 2025, at truslen fra cyberkriminalitet er meget høj. Styrelsen for Samfundssikkerhed vurderer blandt andet, at antallet af ransomware-angreb mod virksomheder lige så vel som myndigheder og andre organisationer i Danmark i 2024 var rekordhøjt.

NIS 2 vil i de kommende år sætte retningen for arbejdet med cyber- og informationssikkerhed for NIS 2-omfattede enheder, men de fleste SMV'ere vil ikke blive omfattet af de nye regler.

Samtidig eksisterer der en stigende bekymring for cyberangreb blandt virksomheder, hvilket har ført til øget motivation til at opprioritere investeringer i cybersikkerhed. I PwC's seneste *cybercrime survey* fra 2024 angiver 60 pct. af virksomhederne, at de er mere bekymrede for cybertrusler end året før, og 66 pct. af virksomhederne forventer at hæve deres sikkerhedsbudget inden for de næste år.

Et højt trusselsniveau bekræftes af samme undersøgelse. Blandt virksomheder med mere end 200 ansatte angiver 54 pct., at deres virksomhed har været ramt af mindst én sikkerhedshændelse i løbet af det seneste år, mens det gælder 35 pct. af virksomhederne med færre end 200 ansatte. Analysen viser ligeledes, at phishing-angreb står øverst på listen over de typer af sikkerhedshændelser, som virksomhederne udsættes for.

Data fra Styrelsen for Samfundssikkerheds undersøgelse *Digital sikkerhed i danske SMV'er* fra 2024 viser, at både store virksomheder og SMV'er er sårbare over for angreb. 60 pct. af SMV'erne og 62 pct. af de store virksomheder vil slet ikke eller kun i lav grad kunne udføre deres kerneopgaver uden adgang til centrale it-systemer. Over halvdelen af SMV'erne (61 pct.) og 92 pct. af store virksomheder har systemer, der behandler eller opbevarer forretningskritisk data, såsom forretningshemmeligheder og kundedatabaser. Desuden har 28 pct. af SMV'erne og 43 pct. af de store virksomheder systemer, der opbevarer eller behandler persondata med særlig risiko, herunder følsomme persondata og CVR-numre. Analysen *Er jeres virksomhed klar til i morgen?* fra TDC Erhverv i 2025 viser, at et hackerangreb koster små danske virksomheder 47.000 kr. om dagen, og at det for de store virksomheder er 200.000 kr. om dagen.

3.2 Teknisk it-sikkerhed i SMV'erne

Undersøgelsen *Cyberbarometer* fra 2024 af Analyse & Tal på vegne af Industriens Fond viser, at "tekniske" it-sikkerhedstiltag er de mest udbredte blandt danske virksomheder, efterfulgt af "forankring og styring" og endelig "rutiner og træning". *Cyberbarometer* og *Digital sikkerhed i danske SMV'er* fra 2024 viser, at der blandt de mest anvendte tekniske it-sikkerhedstiltag er løbende opdatering af software, backup af data, adgangskontrol til netværk og foranstaltninger mod malware.

Førnævnte undersøgelse *Digital sikkerhed i danske SMV'er*, gennemført af Styrelsen for Samfundssikkerhed i 2024, viser, at 85 pct. af SMV'erne har implementeret to af de mest grundlæggende it-sikkerhedstiltag: systematisk opdatering af software og backup af data. En positiv udvikling er, at 94 pct. af SMV'erne tog backup af deres data i 2023, hvilket er en stigning på 13 procentpoint siden 2021. Undersøgelsen *Cyberbarometer* fra Analyse & Tal viser også en lille positiv udvikling i antallet af implementerede cybersikkerhedstiltag blandt SMV'er, herunder en fremgang i brug af automatisk backup.

En tydelig tendens på tværs af undersøgelserne *Digital sikkerhed i danske SMV'er* (2024), *Cyberbarometer* (2024), *Øget it-sikkerhed i små og mellemstore virksomheder* (2024) og *Segmenteringsanalyse af små og mellemstore virksomheder* (2021) er, at mindre virksomheder generelt har færre implementerede sikkerhedstiltag end større virksomheder. Ifølge tal fra Danmarks Statistiks undersøgelse *Små virksomheder har mindre fokus på IT-sikkerhed* fra 2024 har især mikrovirksomheder med fem til ni ansatte et lavt digitalt sikkerhedsniveau.

Analysen om *Digital sikkerhed i danske SMV'ere* viser, at 40 pct. af de danske SMV'er ikke har et digitalt sikkerhedsniveau, som matcher deres risikoprofil. Blandt andet anvender 40 pct. af SMV'erne fortsat ikke stærke adgangskoder, hvilket kan gøre det nemmere for it-kriminelle at bryde koden og få adgang til virksomhedens systemer og data.

> **40 PCT.** AF DE DANSKE SMV'ER HAR IKKE ET DIGITALT SIKKERHEDSNIVEAU, SOM MATCHER DERES RISIKOPROFIL. BLANDT ANDET ANVENDER **40 PCT.** AF SMV'ERNE FORTSAT IKKE STÆRKE ADGANGSKODER, HVILKET KAN GØRE DET NEMMERE FOR IT-KRIMINELLE AT BRYDE KODEN OG FÅ ADGANG TIL VIRKSOMHEDENS SYSTEMER OG DATA.

Der er ligeledes variation mellem brancher, hvor virksomheder i nogle brancher er længere fremme i arbejdet med it-sikkerhedstiltag end i andre brancher. Undersøgelserne fra 2024 *Digital sikkerhed i danske SMV'er*, *Cyberbarometer* og *Øget it-sikkerhed i små og mellemstore virksomheder* viser, at information- og kommunikationsbranchen er længst fremme i arbejdet med digital sikkerhed, mens bygge- og anlægssektoren generelt har mindre fokus på digital sikkerhed end øvrige brancher. Undersøgelsen *Cyberbarometer* fra 2024 viser desuden, at der i bygge- og anlægsbranchen ikke findes samme positive fremgang i brugen af it-sikkerhedstiltag som i de øvrige brancher.
Sammenhæng mellem virksomheders størrelse og brancher og deres sikkerhedsniveau kan hænge sammen med, at de store virksomheder ofte er mere udsatte for angreb, da flere

medarbejdere skaber større angrebsflader, ligesom store virksomheder og nogle brancher ofte er mere digitaliserede og derfor har flere systemer og data, som skal sikres, opdateres og patches. Desuden har større virksomheder ofte en bedre økonomi, som kan øge motivationen hos it-kriminelle i forventningen om at kunne få et stort udbytte. Derved har virksomhedsstørrelse og branche betydning for virksomhedens risikoprofil.

3.3 Kompetencer og træning

Opbygningen af stærk digital sikkerhed handler ikke kun om teknologi, men også om medarbejdernes kompetencer. Det gælder både i forhold til rekruttering af medarbejdere med de rette cybersikkerhedsfaglige kompetencer og i forhold til at sikre, at virksomhedens øvrige ansatte har den nødvendige viden om cybersikkerhed.

En væsentlig udfordring for danske virksomheder er manglen på kvalificerede cybersikkerhedsfaglige kompetencer. Ifølge analysen *Arbejdsmarkedet for informationssikkerhedskompetencer i Danmark,* udarbejdet af konsulenthuset Højbjerre Brauer Schultz i 2019, er efterspørgslen efter cyber- og informationssikkerhedskompetencer tredoblet over det seneste årti, og hver femte virksomhed har haft udfordringer med at rekruttere de nødvendige kompetencer. Udfordringen er særlig stor for virksomheder inden for brancherne ”information og kommunikation” samt ”finans”, hvor 28 pct. forgæves har forsøgt at rekruttere medarbejdere med cyber- og informationssikkerhedskompetencer.

It-Branchens *It-barometer* fra marts 2023 bekræfter denne tendens, da 51 pct. af de adspurgte virksomheder efterspørger kompetencer inden for sikkerhed og compliance. Ligeledes viser PwC’s *cybercrime survey* fra 2023, at 49 pct. af virksomhederne, der har forsøgt at rekruttere medarbejdere inden for cybersikkerhed de seneste 12 måneder, har oplevet udfordringer hermed.

Undersøgelsen *Segmenteringsanalyse af små og mellemstore virksomheder* fra 2021, udarbejdet af Epinion på vegne af Styrelsen for Samfundssikkerhed (daværende Erhvervsstyrelsen), viser, at kompetenceudfordringen også gælder for SMV’erne specifikt. Konkret viser analysen, at 25 pct. af SMV’erne ser mangel på cybersikkerhedsfaglige kompetencer som en barriere.

21 pct. af SMV’erne angiver, i Danmarks Statistiks årlige undersøgelse *It-anvendelse i virksomheder* fra 2023, at mangel på viden og kompetencer til at håndtere it-sikkerhedsløsninger er en konkret udfordring i forhold til at øge it-sikkerhedsniveauet i virksomheden. Der har desuden været en stigning i andelen af SMV’er, der har oplevet denne kompetenceudfordring fra 12 pct. i 2021 til 21 pct. i 2023.

> **21 PCT.** AF SMV’ERNE ANGIVER, AT MANGEL PÅ VIDEN OG KOMPETENCER TIL AT HÅNDTERE IT-SIKKERHEDSLØSNINGER ER EN KONKRET UDFORDRING I FORHOLD TIL AT **ØGE IT-SIKKERHEDSNIVEAUET** I VIRKSOMHEDEN.

Mange SMV’er ansætter ikke dedikerede it-sikkerhedsspecialister, men placerer de it-sikkerhedsmæssige opgaver hos eksisterende medarbejdere. Studiet *"Good" Organizational Reasons for "Bad" Cybersecurity: Ethnographic Study of 30 Danish SMEs* fra Aalborg

Universitet, foretaget blandt 30 SMV'er, viser, at de 30 SMV'er typisk placerer ansvaret for virksomhedens it-sikkerhed hos it-specialister, bogholdere eller kommunikationsspecialister.

Eksperter fra Cybersikkerhedspagten fremhæver, at mange af dem, der arbejder med cybersikkerhed uden en formel uddannelse, kan have svært ved at få anerkendelse for deres tilegnede kompetencer – samt fortsat at kunne videreudvikle sine kompetencer i de tilfælde, hvor formel uddannelse er en forudsætning for adgang til relevant efteruddannelse.

Cybersikkerhedspagten er et offentligt-privat samarbejde med repræsenterer fra blandt andet centrale brancheorganisationer på erhvervsområdet. Samarbejdet skal bidrage til at styrke cybersikkerheden i SMV'er. En række af Cybersikkerhedspagtens medlemmer er i indeværende afsnit anvendt som ekspertkilde.

Foruden it-sikkerhedsansatte spiller virksomhedens øvrige ansatte en vigtig rolle i forhold til virksomhedernes digitale sikkerhed. Mange sikkerhedsbrud skyldes menneskelige fejl, eksempelvis når medarbejdere klikker på phishing-links eller deler adgangskoder. Awareness-træning er derfor en højt prioriteret investering for mange virksomheder, og PwC's *Cybercrime Survey* 2024 viser, at 49 pct. af virksomhederne planlægger at øge investeringerne i awareness-træning. Analysen *Digital sikkerhed i danske SMV'er* fra 2024 viser, at 70 pct. af SMV'erne har informeret deres medarbejdere om deres rolle og ansvar i forhold til digital sikkerhed gennem frivillig eller obligatorisk træning eller via skriftlige kontrakter. Dog gennemfører kun 37 pct. af SMV'erne obligatorisk awareness-træning, sammenlignet med 88 pct. af de store virksomheder.

Dette understøttes af undersøgelsen *A Mixed-method Study on Security and Privacy Practices in Danish Companies*, udgivet af ITU og SDU i 2021, som afdækker sikkerheds- og privatlivspraksisser i danske virksomheder. Undersøgelsen viser, at virksomheder ikke tilbyder tilstrækkelig træning i cybersikkerhed, især ikke for softwareudviklere, og selvom nogle virksomheder tilbyder træning, mener mange ansatte, at den ikke er relevant eller tilstrækkelig praktisk anvendelig.

3.4 Ledelsesforankring af cyber- og informationssikkerhed

På lige fod med andre forretningsbeslutninger har ledelsen ansvaret for virksomhedens digitale sikkerhed. *Digital sikkerhed i danske SMV'er* fra 2024 viser også en direkte sammenhæng mellem ledelsens engagement i cybersikkerhed og virksomhedens sikkerhedsniveau.

Blot 40 pct. af ledelserne i de danske SMV'er er i høj grad involveret i virksomhedens arbejde med digital sikkerhed, mens 17 pct. af ledelserne slet ikke eller kun i lav grad er involveret i dette arbejde. For store virksomheder med 250+ ansatte gælder, at 61 pct. af ledelserne i høj grad er involveret i virksomhedens arbejde med digital sikkerhed.

Ud over ledelsens involvering spiller risikovurdering, beredskabsplanlægning og dokumentation af it-sikkerhed en væsentlig rolle i virksomheders organisatoriske arbejde med digital sikkerhed.

Styrelsen for Samfundssikkerheds analyse *Digital sikkerhed i danske SMV'er* viser, at 41 pct. af SMV'erne ikke foretager løbende risikovurderinger, hvilket betyder, at de ikke får taget systematisk stilling til, hvilke risici der er forbundet med deres organisering og brug af data og teknologier, og de får dermed ikke identificeret og håndteret potentielle trusler.

I 2023 havde 58 pct. af SMV'erne gennemført dokumentation og dermed delbar viden om forholdsregler, aktiviteter og procedurer vedrørende it-sikkerhed. Der var således fortsat 42 pct. af SMV'erne, der ikke havde dokumenteret deres it-sikkerhedstiltag mv., hvilket gjaldt 5 pct. af de store virksomheder. Der findes dog en mindre stigning i andelen af virksomheder, der gennemførte dokumentation fra 2022 til 2023.

For hurtigt at kunne stoppe et eventuelt angreb og begrænse skaderne, bør man have en tydelig beredskabsplan. Data fra TDC Erhvervs undersøgelse *Er jeres virksomhed klar til i morgen?* fra 2025 viser, at knap 1 ud af 5 adspurgte virksomheder har en plan, hvor alle medarbejdere ved, hvad de skal gøre i tilfælde af et angreb.

3.5 Barrierer og drivers i arbejdet med digital sikkerhed

På tværs af analyser fra Styrelsen for Samfundssikkerhed og TDC Erhverv er der afdækket en række fælles udfordringer, der hæmmer virksomheder i arbejdet med digital sikkerhed. De primære barrierer inkluderer mangel på tid, ressourcer og kompetencer.

Ifølge analysen *Digital sikkerhed i Danske SMV'er* fra 2024, baseret på data fra Danmarks Statistik, oplever 37 pct. af SMV'erne udfordringer med at hæve it-sikkerhedsniveauet i virksomheden. Dette gælder for 38 pct. af de store virksomheder med 250+ ansatte, hvilket indikerer, at it-sikkerhedsarbejdet kan være udfordrende for store såvel som små virksomheder.

> **37 PCT.** AF SMV'ERNE OPLEVER UDFORDRINGER MED AT **HÆVE IT-SIKKERHEDSNIVEAUET** I VIRKSOMHEDEN.

Blandt SMV'erne er den største barriere "usikkerheden om virksomhedens gevinst ved at investere i it-sikkerhed" (22 pct.), efterfulgt af "manglende viden og kompetencer til at håndtere it-sikkerhedsløsninger" (21 pct.) samt "manglende økonomiske ressourcer til at investere i it-sikkerhed" (15 pct.).

Disse udfordringer bakkes op af *Segmenteringsanalyse af små og mellemstore virksomheder* fra 2021 blandt danske SMV'er, hvor 49 pct. finder det vanskeligt at prioritere tid til it-sikkerhed, mens 25 pct. oplever udfordringer med at rekruttere medarbejdere med de rette kompetencer, og hele 40 pct. af SMV'erne ser det som en udfordring at oplære deres eksisterende medarbejdere i at være opmærksomme på digitale trusler.

At det er svært at få medarbejderne gjort opmærksomme på digitale trusler, stemmer overens med resultater fra virksomhedsinterviews gennemført af Analyse & Tal i forbindelse med udarbejdelsen af *Cyberbarometer* fra 2024, hvor virksomhedsledere peger på, at en af de største barrierer for at styrke cybersikkerheden er at få det integreret i organisationens daglige rutiner og virksomhedskultur.

En central pointe fra rapporten A *Mixed-method Study on Security and Privacy Practices in Danish Companies*, udgivet af ITU og SDU i 2021, er også, at der ofte er en skævvridning mellem ledelsens og tekniske medarbejderes opfattelse af cybersikkerhed. Rapporten viser, at ledere ofte antager, at it-afdelingen eller softwareudviklere har styr på sikkerheden, mens disse medarbejdere rapporterer om mangel på støtte, ressourcer og tid til at implementere nødvendige sikkerhedsforanstaltninger.

Trods disse udfordringer peger analyser på flere faktorer, der kan øge virksomhedernes fokus på cybersikkerhed. Blandt andet viser analysen *Segmenteringsanalyse af små og mellemstore virksomheder*, at 79 pct. af virksomhederne efterspørger konkrete, letforståelige råd om sikkerhed. 75 pct. ønsker løbende varsler om aktuelle trusler rettet mod deres virksomhedstype, mens 66 pct. efterspørger et overblik over gratis værktøjer til forbedring af it-sikkerheden.

Interviews i forbindelse med *Cyberbarometer* fra 2024 med virksomhedsledere, foretaget af Analyse & Tal for Industriens Fond, viser, at motivationen for at styrke cybersikkerheden i virksomheden ofte udspringer af konkrete sikkerhedshændelser, behovet for digitalisering samt hensynet til kundernes sikkerhed. I mange tilfælde er de første skridt tekniske sikkerhedstiltag, hvorefter sikkerhedstiltag inden for styring, forankring og medarbejdertræning bygges på.

> **79 PCT**. AF VIRKSOMHEDERNE EFTERSPØRGER KONKRETE, LETFORSTÅELIGE RÅD OM SIKKERHED. **75 PCT.** ØNSKER LØBENDE VARSLER OM AKTUELLE TRUSLER RETTET MOD DERES VIRKSOMHEDSTYPE, MENS **66 PCT.** EFTERSPØRGER ET OVERBLIK OVER GRATIS VÆRKTØJER TIL FORBEDRING AF IT-SIKKERHEDEN.

3.6 Delkonklusion vedrørende cybersikkerhed i SMV'er

Cybertruslen mod danske virksomheder er meget høj, og især SMV'er er sårbare. Phishing er den mest udbredte angrebsform, og over halvdelen af virksomhederne forventer at øge deres sikkerhedsbudget. Trods udbredelsen af basale sikkerhedstiltag som backup og opdatering, har 40 pct. af SMV'erne et sikkerhedsniveau, der ikke matcher deres risikoprofil. SMV'er er ofte afhængige af centrale it-systemer og håndterer forretningskritiske og følsomme data, men mangler både tekniske og organisatoriske sikkerhedskapaciteter. Kompetencemangel og lav ledelsesinvolvering er udbredt, og kun en mindre andel gennemfører obligatorisk awareness-træning. Desuden mangler mange risikovurderinger og beredskabsplaner, hvilket svækker evnen til at håndtere angreb effektivt. Virksomhedsstørrelse og branche spiller en tydelig rolle, og store virksomheder har flere ressourcer og formelle sikkerhedstiltag, mens de mindste virksomheder ofte mangler både viden og økonomi.

Samtidig efterspørger mange SMV'er konkrete råd, trusselsvarsler og gratis værktøjer, hvilket tyder på, at der er øget opmærksomhed på cybersikkerhed i SMV'erne, samt at de har behov for mere målrettet støtte.


Information

4 Cybersikkerhed i kritisk infrastruktur

I kapitlet om cybersikkerhed i kritisk infrastruktur redegøres der for truslen mod den kritiske infrastruktur baseret på eksisterende trusselsvurderinger og afhængigheder i kritisk it-infrastruktur. Da der i henhold til både CER- og NIS 2-direktiverne skal være fokus på øget koordinering mellem de kompetente myndigheder samt videndeling om hændelser i den kritiske infrastruktur, ligesom der skal være klarhed over roller og ansvarsområder på nationalt plan, beskrives herefter de relevante cyberaktører i Danmark. Endvidere redegøres kort for, hvordan beredskabsøvelser og internationalt samarbejde er centrale værktøjer til at øge cybersikkerheden.

4.1 Truslen mod kritisk infrastruktur

Nedbrud i den kritiske infrastruktur kan have store konsekvenser på tværs af samfundet, og truslen er høj. Styrelsen for Samfundssikkerhed vurderer, at det er sandsynligt, at statslige russiske hackere udfører cyberspionage mod dansk kritisk infrastruktur, blandt andet for at forberede sig på at kunne udføre destruktive cyberangreb i fremtiden. Truslen fra destruktive cyberangreb mod Danmark blev i juni 2024 hævet fra lav til middel. Destruktive cyberangreb er ét blandt flere hybride virkemidler, som hackere kan bruge til at opnå strategiske fordele. Derudover er truslen fra cyberaktivisme mod danske virksomheder og myndigheder høj, og hvis cyberaktivister angriber organisationer, der forvalter kritisk infrastruktur, kan det få betydelige konsekvenser og påvirke mange borgere i Danmark.

4.2 Tværgående digitale afhængigheder i digital infrastruktur

Et overblik over tværgående digitale afhængigheder kan bidrage til at identificere, hvilke andre sektorer, myndigheder eller virksomheder der potentielt vil blive påvirket, og dermed hvor man skal sætte ind for at opretholde eller genoprette kritiske funktioner, samt prioritere indsatserne.

En konsekvensanalyse udarbejdet af Styrelsen for Samfundssikkerhed og Digitaliseringstyrelsen i 2024 viser i forlængelse heraf, at et nedbrud eller driftsforstyrrelser på MitID, MitID Erhverv og NemLog-In vil have konsekvenser for myndigheders evne til at varetage deres samfundsvigtige funktioner.

Et eksempel på driftsforstyrrelse er Crowdstrike's globale nedbrud i 2024. Nedbruddet skyldtes en fejlslagen softwareopdatering, som blandt andet betød, at 8,5 millioner Windows-enheder var ude af drift i flere timer. Det havde store konsekvenser globalt, og betød i Danmark blandt andet, at Hovedstadens Beredskab ikke kunne modtage automatiske brandalarmer.

I regi af den nationale strategi for cyber- og informationssikkerhed 2022-2024 blev der igangsat et arbejde for at udarbejde en analysemodel til at kortlægge afhængigheder mellem kritisk it-infrastruktur. Formålet var at analysere og prioritere kritisk it-infrastruktur med henblik på at kunne gennemføre en central koordination af den hurtige og effektive imødegåelse af cyberhændelser, som potentielt kunne have effekt på andre sektorer og dermed have

kaskadeeffekter ud i samfundet. Der blev fastlagt en taksonomi og metodebeskrivelse for identifikation af kritisk it-infrastruktur, og der er udviklet metoder til indsamling af relevant data til brug for kortlægning og analyse af kritisk it-infrastruktur.

4.3 Roller, ansvar og videndeling i det danske cyberøkosystem og operativt samarbejde

Lørdag den 19. juli 2025 oplevede Nets et landsdækkende nedbrud på grund af en komponentfejl i leverandørstyret infrastruktur, hvilket medførte at kortbetalinger, hævninger og nethandel i flere timer ikke kunne gennemføres som normalt. Nets offentliggjorde en incident-rapport, mens Finanstilsynet og Erhvervsministeriet har fulgt op med krav om redegørelser og senere påbud om utilstrækkelig kommunikation under hændelsen.

IRIS Groups analyse *Styrket effektivitet i offentlig-privat videndeling på cyberområdet* fra 2024 viser, at et velfungerende økosystem for videndeling om cybertrusler, konkrete hændelser og mitigerende tiltag er vigtigt for at beskytte vigtige samfundsfunktioner mod angreb fra cyberkriminelle. Med den nationale strategi for cyber- og informationssikkerhed 2022-2024 blev der indført flere tiltag for at styrke det offentlige-private samarbejde i Danmark. Evnen til effektivt at dele viden om cybertrusler og hændelser er vigtig for at have et højt cybersikkerhedsniveau og for hurtigt og effektivt at kunne imødegå trusler og konkrete angreb. Førnævnte analyse fra IRIS Group viser desuden, at både private aktører og offentlige myndigheder de senere år har taget en række væsentlige initiativer til at styrke videndeling og erfaringsudveksling mellem offentlige og private aktører. Det har resulteret i, at både private og offentlige aktører på forskellig vis samarbejder om at indsamle og dele viden om trusler, sårbarheder, konkrete angreb og mitigerende tiltag.

4.3.1 Styrelsen for Samfundssikkerhed

Styrelsen for Samfundssikkerhed er national it-sikkerhedsmyndighed, ligesom styrelsen generelt rådgiver og vejleder danske myndigheder, virksomheder og borgere i at styrke cybersikkerheden, så risikoen for cyberangreb mindskes og – såfremt angreb lykkedes – imødegås på den mest hensigtsmæssige måde. I forlængelse heraf har Styrelsen for Samfundssikkerhed dialog med blandt andet statslige myndigheder, brancheorganisationer og større virksomheder inden for de sektorer, der beskæftiger sig med samfundsvigtige funktioner.

Styrelsen er derudover koordinerende myndighed i forhold til implementering af NIS 2 samt sektoransvarlig for statslige myndigheder og kommuner.

4.3.2 National CSIRT

CSIRT står for ”Computer Security and Incident Response Team” og håndterer it-sikkerhedshændelser og varetager de opgaver, der relaterer sig hertil. Kravet om en CSIRT-funktion er en udløber af NIS-direktivet og blev udvidet med NIS 2-direktivet.

CSIRT har en central rolle i modtagelse og håndtering af indberetninger fra myndigheder og virksomheder og skal i visse tilfælde yde teknisk bistand. Derudover skal CSIRT overvåge og

analysere cybertrusler, identificere sårbarheder og reagere på hændelser. En vigtig funktion er at udsende tidlige varsler og alarmer om cybertrusler i tæt på realtid samt, på anmodning, at bistå væsentlige og vigtige enheder med overvågning af deres netværk og informationssystemer. CSIRT skal endvidere indsamle og analysere kriminaltekniske data, udarbejde analyser og skabe situationsbevidsthed om cybersikkerhed. Dette omfatter både et overordnet situationsbillede af cybersikkerhedstilstanden og aktuelle situationsbilleder, som myndigheder kan anvende til krisestyring, og som enheder kan bruge til at træffe operative beslutninger under større hændelser.

En væsentlig opgave for CSIRT er desuden at koordinere krisestyringen ved tværsektorielle cyberhændelser, uanset om de skyldes eksterne trusler som ransomware-angreb eller interne driftsforstyrrelser med sektoroverskridende konsekvenser. CSIRT skal understøtte enheder i at håndtere sådanne hændelser og sikre en effektiv og koordineret respons på tværs af berørte aktører.

4.3.3 Kompetente myndigheder

Cybersikkerhed i Danmark er baseret på sektoransvarsprincippet. Det betyder, at den sektoransvarlige myndighed har ansvaret for at sikre et forsvarligt beredskab og løbende vurdere risikobilledet inden for eget ressort. Det er også den sektoransvarlige myndigheds ansvar at håndtere en hændelse og dens følger.

4.3.4 Computer Emergency Response Teams

Inden for nogle sektorer findes også Computer Emergency Response Teams (CERT'er). Det er operative enheder, som typisk monitorerer kritisk infrastruktur og kan yde teknisk assistance døgnet rundt til systemansvarlige i forhold til at håndtere cybersikkerhedshændelser og -sårbarheder. Nogle CERT'er er private tredjepartsleverandører (f.eks. Improsec), andre er enheder forankret i den kompetente myndighed (f.eks. Sundhedsdatastyrelsen) eller etableret som en forening ejet i samarbejde mellem virksomheder og/eller brancheorganisationer (f.eks. SektorCERT og KommuneCERT). Endvidere har flere større virksomheder egne interne CERT-funktioner.

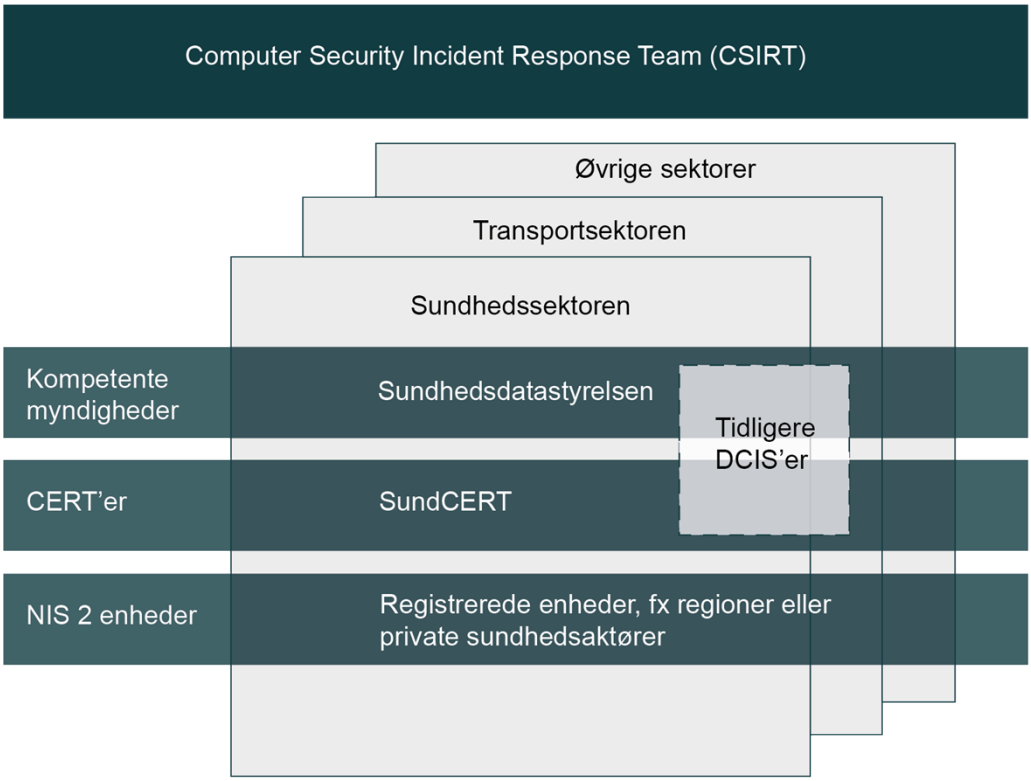
4.3.5 DCIS-enheder

Som led i den nationale strategi for cybersikkerhed 2018-21 og parallelt med implementeringen af NIS-direktivet fra 2016 blev det besluttet, at der inden for de seks samfundskritiske sektorer (energi, sundhed, transport, tele, finans og søfart) skulle nedsættes decentrale cyber- og informationssikkerhedsenheder (DCIS-enheder) og udarbejdes sektorstrategier. Med den efterfølgende nationale strategi for cyber- og informationssikkerhed 2022-2024 blev ministerområder med ansvar for samfundsvigtige funktioner, som i væsentlig grad er it-understøttet, også forpligtet til at oprette DCIS-enheder samt udarbejde delstrategier, der skulle adressere en række krav.

DCIS-enhederne varierer i størrelse og arbejdsopgaver, da det ikke er alle ministerområder, der har ansvar for en sektor. De fleste DCIS-enheder er forankret i relevante styrelser under de pågældende ministerområder. Deres arbejdsporteføljе varierer grundet de forskellige delstrategier, men fælles for DCIS-enhederne er, at de skal fungere som kontaktpunkt for centrale enheder og virksomheder i sektoren.
Det indebærer, at DCIS-enhederne har ansvar for at dele information om blandt andet

sårbarheder til virksomheder og etablere erfaringsudveksling og videndeling mellem enheder inden for sektoren selv og på tværs af sektorer. Kravene til DCIS-enhederne om udarbejdelse af delstrategier bortfaldt ved udgangen af den nationale strategi for cyber- og informationssikkerhed 2022-2024.

Nedenstående *figur 2* opsummerer og illustrerer samspillet mellem aktører i cyberøkosystemet.



Figur 2: Overblik over aktører i cyberøkosystemet

4.4 Bedre videndeling og øvelser mellem aktører

Der er store forskelle i modenhedsniveau blandt de forskellige aktører, og det er en kompleks opgave at etablere effektive økosystemer for videndeling om cybersikkerhed. IRIS Group har i deres undersøgelse *Styrket effektivitet i offentlig-privat videndeling på cyberområdet*, udarbejdet for Cybersikkerhedsrådet i 2024, udført en spørgeskemaundersøgelse, hvor virksomheder er blevet bedt om at svare på, om de er enige i en række udsagn om deres kendskab til aktører i økosystemet og deres praksis omkring deling af viden om cybersikkerhed. Svarene i spørgeskemaundersøgelsen er opgjort i henholdsvis erfarne og mindre erfarne sektorer.

Cybersikkerhedsrådet rådgiver regeringen om, hvordan den digitale sikkerhed styrkes og bidrager til videndeling mellem myndigheder, erhvervsliv og forskningsverden. Cybersikkerhedsrådet er sammensat af medlemmer fra erhvervslivet, myndigheder og forskningsverdenen.

Her ses det, at en væsentlig udfordring er, at virksomhederne har manglende indsigt i økosystemet, hvor kun halvdelen af virksomhederne i de modne sektorer kender til

rollefordelingen mellem det tidligere Center for Cybersikkerhed (nu Styrelsen for Samfundssikkerhed), sektormyndigheden og kompetente myndigheder inden for deres sektor, mens det for virksomheder i de umodne sektorer kun er lidt over hver tredje.

IRIS Groups undersøgelse viser, at der er en række barrierer for at dele viden, herunder uklarheder om, hvad der er relevant at dele og med hvem, manglede tekniske forudsætninger for at identificere og dele relevante hændelser samt usikkerhed om anonymitet og hvem der får adgang til den delte information. Ligeledes fremgår det, at man med fordel kan minimere sådanne barrierer for at fordre bedre videndeling mellem aktørerne.

> DER ER EN RÆKKE BARRIERER FOR AT DELE VIDEN, HERUNDER UKLARHEDER OM, HVAD DER ER **RELEVANT AT DELE** OG MED HVEM, MANGLEDE TEKNISKE FORUDSÆTNINGER FOR AT IDENTIFICERE OG DELE RELEVANTE HÆNDELSER SAMT USIKKERHED OM ANONYMITET OG **HVEM DER FÅR ADGANG** TIL DEN DELTE INFORMATION.

Med implementeringen af NIS 2-direktivet pålægges omfattede enheder inden for samfundskritiske sektorer et krav om at indberette større cyberhændelser inden for 24 timer.

4.5 Beredskabsøvelser, cybertest mv.

Det er nødvendigt at træne, øve og teste beredskabet i og på tværs af sektorer og organisationer, så man er bedre stillet, hvis en reel situation skulle opstå. En analyse blandt Dansk Industris medlemmer fra 2025 viser, at kun hver tredje virksomhed har øvet sig på, hvad de skal gøre, hvis angrebet rammer.

I 2025 blev der afholdt en national cyberberedskabsøvelse ”Hele Danmark Øver”, hvor både myndigheder, brancheorganisationer og virksomheder deltog. Danmark deltager også i øvelser på EU-niveau, f.eks. Cyber Europe, der blandt andet skal bidrage til at danne overblik over roller og ansvar i forbindelse med hændelser, der går på tværs af medlemslande.

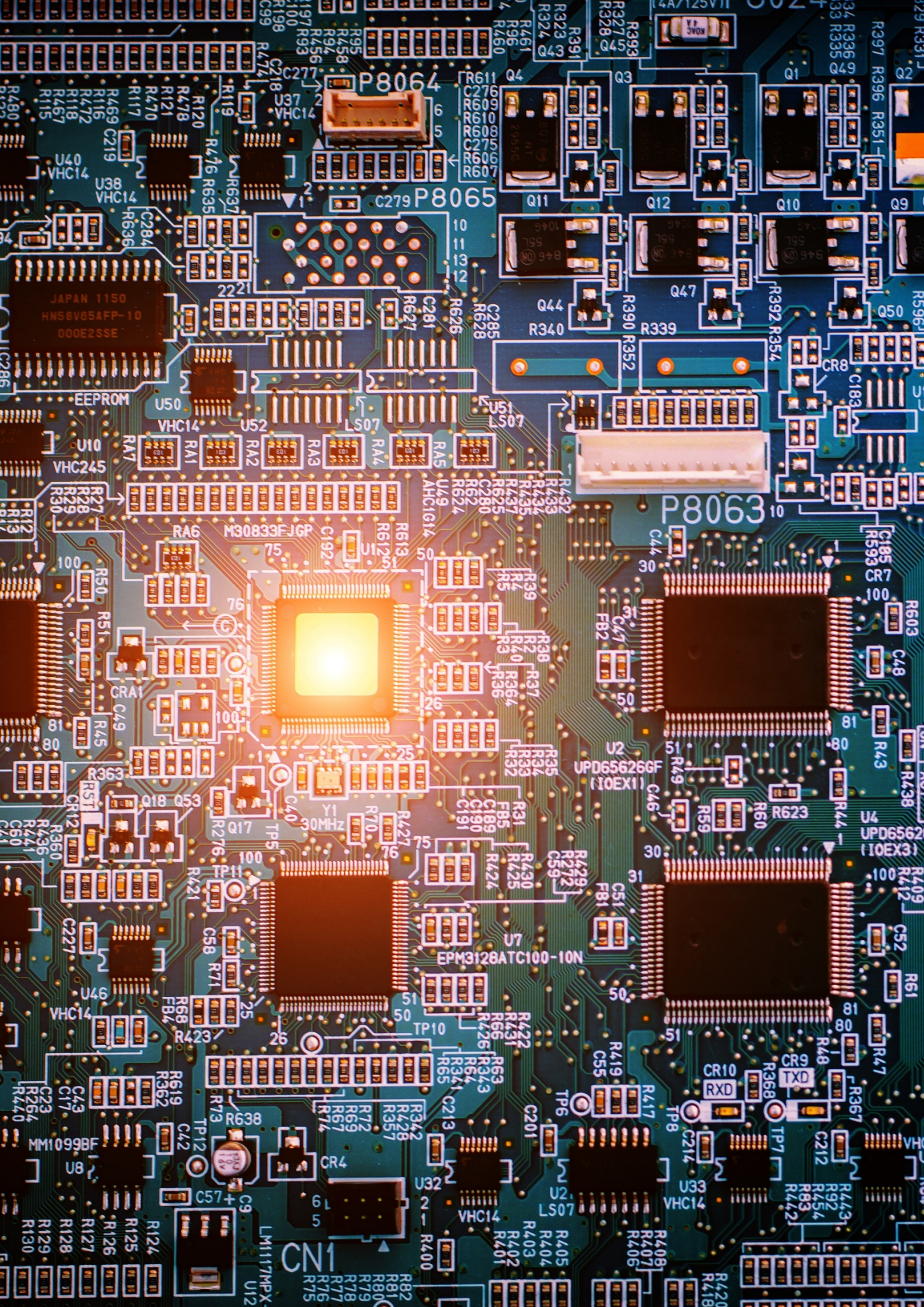
IRIS Groups analyse viser, at der ved at øge fokus på træning og beredskab kan skabes større klarhed om ansvar og rollefordeling for aktørerne i forskellige sektorer, herunder særligt snitflader mellem kompetent myndighed, DCIS-enhederne og it-sikkerhedsmyndigheden. Desuden kan der skabes rammer for, at sektorer, som er omfattet af NIS 2, kan bygge på erfaringerne fra sektorerne, der allerede er omfattet af NIS.

4.6 Delkonklusion vedrørende cybersikkerhed i kritisk infrastruktur

Europæisk lovgivning sætter rammen for arbejdet med cybersikkerhed i samfundskritiske sektorer i Danmark og resten af EU. Med NIS 2 har man øget robustheden af de enkelte myndigheder, virksomheder og sektorer, og der er fokus på de afhængigheder, der er mellem forskellige

organisationer på tværs af sektorer, ligesom der lægges vægt på vigtigheden af at kende til roller og ansvar i forbindelse med krisesituationer.

Med implementeringen af NIS 2 vil aktørerne på området få nye forpligtelser til blandt andet hændelseshåndtering, og der vil blive stillet nye krav til den nationale CSIRT's kapaciteter. Det danske cyberøkosystem er komplekst, og det er vigtigt, at der faciliteres et effektivt samarbejde mellem national CSIRT, CERT'er og øvrige aktører. Der bør derfor være veldefinerede roller for alle aktørerne, og roller og ansvar bør trænes gennem øvelser og tests. Det kræver værktøjer, som kan understøtte vidensdeling og effektiv hændelseshåndtering med henblik på at øge robustheden på tværs af samfundet, så offentlige og private aktører er beredte, når en hændelse indtræffer.


P8064
P8065
P8063
JAPAN 1150
HN58V65AFP-10
000E2SSE
EEPROM
U50
VHC14
U52
LS07
U51
LS07
U10
VHC245
M30833FJGP
U12
U49
AHC1G14
U2
UPD65626GF
(IOEX1)
U4
UPD65626
(IOEX3)
U7
EPM3128ATC100-10N
Y1
30MHz
MM1099BF
U8
U46
VHC14
U37
VHC14
U40
VHC14
U38
VHC14
U32
VHC14
U33
VHC14
U2
LS07
CN1
LM1117MPX-
CR4
CR7
CR8
CR9
TXD
CR10
RXD
CRA1
RST
TP1
TP5
TP6
TP7
TP8
TP10
TP12
Q11
Q12
Q10
Q44
Q47
Q50
Q18
Q53
Q17
Q4
Q3
Q2
Q1
Q43
Q45
Q49
RA1
RA2
RA3
RA4
RA5
RA6
RA7

5 Den danske cyberindustri og -forskning

Det følgende kapitel afdækker den danske cyberindustri, herunder barrierer for vækst i den danske cybersikkerhedsbranche. Herefter beskrives cyberindustriens EU-initiativer omhandlende blandt andet udviklingen og koordineringen af cybersikkerhedsindsatser.

I det følgende afsnit bliver der brugt begreberne cyberindustri og cybersikkerhedsbranche. Med cyberindustri menes en bred betegnelse af alle virksomheder, der beskæftiger sig med produktion eller levering af ydelser inden for cybersikkerhed. Med cybersikkerhedsbranche menes en afgrænset del af industrien, der fokuserer på udvikling, salg og implementering af specifikke cybersikkerhedsløsninger.

5.1 Den danske cybersikkerhedsbranche

Ifølge Deloittes analyse *Potentialet ved et styrket dansk økosystem for cybersikkerhed og -forsvar* fra *2024,* udarbejdet for Security Tech Space og Nationalt Forsvarsteknologisk Center, omsatte den danske cybersikkerhedsbranche i 2023 for ca. 6,4 mia. kr. Det svarer til cirka 2 pct. af omsætningen i den samlede it- og cybersikkerhedsbranche samme år. Det er vanskeligt præcist at opgøre, hvor stor en del af branchen, der udelukkende arbejder med cybersikkerhed, da mange it-virksomheder tilbyder cybersikkerhed sammen med andre produkter og services. Branchen omfatter anslået 300 virksomheder, hvor cybersikkerhed indgår som en del af forretningen.

Deloittes analyse estimerer, at ca. 10.700 fuldtidsansatte er beskæftiget med cybersikkerhed i den danske it- og cybersikkerhedsbranche. Dertil kommer 5.000 - 6.000 fuldtidsansatte, som arbejder med cybersikkerhed i andre brancher. Det bemærkes, at man i Deloitte analysen ikke har kunnet udskille cybersikkerhedsbranchen fra it-branchen.

Endvidere peger analysen på, at ny regulering, herunder NIS 2, sammen med en stigende modenhed blandt virksomhedsledelser og bestyrelser samt et øget politisk fokus på forsvar, samfundssikkerhed og beredskab, vil medføre en markant stigning i efterspørgslen efter kompetencer inden for cybersikkerhed og -forsvar i de kommende år. Samme analyse anslår også, at der vil ske en yderligere vækst i indsatsen med at beskytte det danske samfund og den digitale infrastruktur, hvilket samlet set forventes at kunne fordoble både omsætningen og antallet af fuldtidsansatte i branchen inden for de næste 5-10 år.

5.1.1 Kendetegn for branchen

Det nationale koordinationscenter for cybersikkerhed (NCC) blev oprettet i 2023 og har som formål at understøtte cybersikkerhedsindustrien gennem etableringen af et netværk som fremmer koordinering, videndeling og samarbejde og gennem tilskudspuljer, som skal finansiere cybersikkerhedsprojekter. NCC's netværk udgør knap 170 medlemmer, og af disse er ca. 75 pct. SMV'ere, som beskæftiger sig med cybersikkerhed. I indeværende kapitel er NCC anvendt som ekspertkilde.

Deloittes analyse viser ligeledes, at den danske cybersikkerhedsbranche er kendetegnet ved relativt mange nye SMV'er, der primært er centreret i små klynger i og omkring Aarhus og København. Væksten har ifølge Deloitte især været markant i Aarhus og København, men også Aalborg og Odense har oplevet en fremgang. Som eksempel er flere virksomheder sprunget ud af det århusianske universitetsmiljø, hvor der i Deloittes analyse særligt fremhæves Institut for Datalogi på Aarhus Universitet som vigtig drivkraft, da AU i 1990 etablerede en forskergruppe i kryptografi og cybersikkerhed.

Analysen fra Deloitte viser også, at en væsentlig andel af virksomhederne i cybersikkerhedsindustrien er start-ups med få ansatte. Heraf er hovedparten startet af erfarne konsulenter fra it-virksomheder, tidligere forsvarsansatte eller udspringer af universitetsmiljøerne. Som resultat heraf er cybersikkerhedsbranchen kendetegnet ved en bred diversitet i kompetenceområder, hvilket afspejles i virksomhedernes arbejde med varierende løsninger, der retter sig mod forskellige målgrupper og adresserer et bredt spektrum af it-sårbarheder.

Det er NCC's erfaring, at samarbejdet for at styrke cybersikkerhed går på tværs af virksomheder, myndigheder, forskningsinstitutioner og organisationer. Samarbejdet beskrives af analysen fra Deloitte og af NCC som primært rettet mod beskyttelse af virksomheder og kritisk infrastruktur, og med mindre fokus på at fremme kommercialisering af forskning og at skabe vækst blandt cybersikkerhedsvirksomheder.

5.2 Barrierer for vækst

5.2.1 Manglende koordinering og samarbejde

Analysen fra Deloitte viser, at interessenter og aktører oplever en manglende koordinering af igangværende indsatser på tværs af sektorer, myndigheder og organisationer, hvilket blandt andet fører til overlap af initiativer. Samtidig beskrives det, hvordan cybersikkerhed ofte falder mellem forskellige stole i erhvervsfremmesystemet, hvilket gør det vanskeligt at engagere systemet om fælles projekter, blandt andet på grund af konkurrence.

Det er NCC's erfaring, at der i cybersikkerhedsbranchen er et stort kendskab aktørerne i mellem, og at der i et vist omfang etableres samarbejder. Der er dog stadig et uudnyttet potentiale i forhold til etableringen af samarbejder, som til dels skyldes manglende koordinering samt fraværet af erfarne aktører, som ønsker at lede samarbejder og dermed fremme optag af nye teknologier.

NCC vurderer, at samarbejdet mellem branchen og forskningsinstitutioner af aktører kan være tidskrævende og udfordrende. Virksomheder er bundlinjedrevne, mens universiteter fokuserer på grundforskning med validerede og reproducerbare resultater, hvilket tager tid. Derudover har begge parter ofte faste opfattelser af roller og ansvar, hvilket skaber en gensidig forventning om modstridende interesser – eksempelvis kommerciel værdiskabelse versus ikke-kommerciel videnproduktion.

5.2.2 Mangel på kompetencer og kvalificeret arbejdskraft

Mangel på kvalificeret arbejdskraft og specialiserede kompetencer udgør ifølge Deloitte en væsentlig barriere for vækst og udvikling i cybersikkerhedsbranchen. Det gælder både profiler med tekniske og digitale kompetencer, herunder kryptologi, men også profiler, der kombinerer den tekniske og forretningsmæssige forståelse.

> MANGEL PÅ KVALIFICERET ARBEJDSKRAFT OG SPECIALISEREDE KOMPETENCER UDGØR EN VÆSENTLIG BARRIERE FOR VÆKST OG UDVIKLING I CYBERSIKKERHEDSBRANCHEN.

Det er NCC's erfaring, at hos de cybersikkerhedsstartups og scaleups, hvor man har de tekniske kapaciteter, mangler man at kombinere dem med forretningskompetencer, herunder kommercialisering og markedsføring samt indsigt i finansieringslandskabet, der kan understøtte langsigtet og bæredygtig vækst.

5.2.3 Markedsadgang er en udfordring

Det er NCC's erfaring, at mange nystartede virksomheder oplever høje adgangsbarrierer på aftagermarkedet, da etablerede aktører med stærk troværdighed ofte foretrækkes som leverandører inden for cybersikkerhed. Dette betyder, at mange danske nystartede virksomheder har svært ved at få fodfæste på markedet. Dette bidrager til udfordringen med manglen på kapital til at udvikle og vækste virksomheden. Hertil kommer, at mange startups har svært ved at komme ind på markedet alene fordi, de har svært ved at formidle, hvorfor deres specifikke teknologi er værd at investere i. Det kan være en udfordring at forklare og tydeliggøre teknologiens konkrete fordele for potentielle kunder. Ifølge flere start-ups forværres udfordringen med at forklare teknologiens kompleksitet ofte af, at potentielle kunder mangler den grundlæggende forståelse for cyberteknologi, som er nødvendig for at forstå både produktet og teknologien samt fordelene ved den ene teknologi frem for den anden.

Ligeledes kan efterlevelse af specifikke standarder og/eller certificeringer være en markedsbarriere. Det kan være en udfordring for de virksomheder, f.eks. SMV'er, som ikke har de nødvendige ressourcer til at blive certificeret. Denne udfordring gør sig særligt gældende i relation til forsvarsindustrien, hvor der ofte kan være særlige certificeringskrav, hvilket fremhæves i Erhvervsstyrelsens analyse af *Danmarks forsvarsindustrielle økosystem* fra 2024.

5.2.4 Finansieringslandskabet

En gennemgående problematik, der fremhæves i rapporten *European Cybersecurity Investment Platform fra European Investment Bank* i 2022 er, at de offentlige finansieringsordninger beskrives som fragmenterede. De findes på både nationalt, regionalt og EU-niveau, hvilket gør det svært for virksomheder at navigere i dem og få adgang til kapital. Derudover er der enighed blandt europæiske virksomheder om, at det er for omfattende og bureaukratisk at deltage i EU-programmerne, og at processerne for afrapportering beskrives som afskrækkende for deltagelse. Blandt andet som resultat heraf ansøger danske virksomheder ifølge NCC generelt i lavere grad om EU-finansiering end deres europæiske modparter.

NCC fremhæver, at det ofte er de større virksomheder, der lykkes med at engagere sig i europæiske finansieringsmuligheder. Dette relativt lave niveau af europæiske engagement vurderes også at kunne tilskrives manglende modenhed som manglende erfaring med at udvikle internationalt samarbejde. Hertil kommer også kompleksiteten i reguleringer, lovgivning og krav mellem EU-landene. Samlet set betyder dette manglende dansk hjemtag af EU-finansiering afsat til cybersikkerhed.

5.2.5 Styrkepositioner

NIS 2-direktivet har til formål at ensarte cyber- og informationssikkerheden på tværs af EU-medlemsstaterne. Ifølge EU-Kommissionen vil NIS 2-direktivet forventeligt øge investeringerne i cybersikkerhed med mellem 20 og 30 pct. i forhold til det nuværende niveau. Dette udgør et markedspotentiale for danske virksomheder, der vil kunne befordre vækst og samtidigt understøtte en forbedret cybersikkerhed i Danmark.

5.2.6 Danske forskningsstyrker

Danmark har en række specifikke forskningsstyrker inden for kryptologi, it-sikkerhed, dataorganisering og algoritmer, og hvor der samtidig findes et velfungerende erhvervssamspil inden for forsknings- og innovationssamarbejder samt såkaldte spin-outs.

En spin-out er en virksomhed, der er etableret på baggrund af aftaler med en eksisterende organisation, f.eks. en forskningsinstitution, ved at overføre teknologi eller intellektuelle rettigheder til den nye virksomhed.

Ifølge analysen *Danske styrker inden for forskning, teknologi og uddannelse – og deres betydning for vækst og erhvervsudvikling* fra 2019, udarbejdet af IRIS Group på vegne af Erhvervsstyrelsen, er DTU særligt fremtrædende inden for cybersikkerhed med fokus på emner som privacy by design, letvægtskryptografi, software-verifikation og -protokoller samt governance i forhold til de organisatoriske strukturer, som virksomheder og organisationer har for at forbedre og vedligeholde deres sikkerhedsfunktioner. DTU foretager også vigtig forskning inden for ansvarlig datahåndtering.

Det fremgår af *Analyse af markedet for cyber- og informationssikkerhed* fra 2023, udarbejdet af Deloitte for Security Tech Space, at Aarhus Universitet udmærker sig med en stærk forskningsposition inden for kryptologi, hvor Institut for Datalogi ligger i top tre i verden inden for området, og har skabt spin-outs, der arbejder med avancerede kryptografiske løsninger.

5.2.7 Stærke spin-in teknologier i forsvarsindustrien

Den nuværende geopolitiske ustabilitet og krigen i Ukraine har medvirket til, at cyberteknologi fremhæves af Deloitte i analysen *Potentialet ved et styrket dansk økosystem for cybersikkerhed og -forsvar* fra 2024 og i Erhvervsstyrelsens rapport *Danmarks Forsvarsindustrielle Økosystem* fra 2024 som et område med stort potentiale for integration i forsvarsindustrien.
Det fremgår af Deloittes analyse, at i Danmark består cybersikkerhedsbranchen af specialiserede, men relativt små virksomheder, der er stærke inden for områder, der er afgørende i forsvars- og sikkerhedskritiske sammenhænge, herunder kvantekommunikation og kryptologi. På disse områder har Danmark både konkurrencedygtige virksomheder og stærke faglige universitetsmiljøer.

Det danske spin-in segment, som udvikler produkter og tjenesteydelser til både militær og civil brug, beskrives i flere analyser, som havende et stort potentiale i forsvarsindustrien. Ifølge Erhvervsstyrelsens analyse *Danmarks Forsvarsindustrielle Økosystem* er segmentet kendetegnet ved at være særligt videnstungt og med et samarbejde med universiteter og andre vidensinstitutioner. Det beskæftiger en høj andel højtuddannede medarbejdere herunder personer med militær baggrund eller erfaring fra forsvarsvirksomheder og relevante myndigheder.

Spin-in refererer i denne sammenhæng til teknologi, der oprindeligt er udviklet til et civilt formål, og som bliver integreret og anvendt i forsvarsindustrien.

5.3 Delkonklusion vedrørende den danske cyberindustri og forskning

Den danske cyberindustri spiller en stor rolle for både Danmarks digitale sikkerhed og rummer stærke faglige miljøer inden for kvantekommunikation og kryptologi. Industrien favner bredt fra teknologivirksomheder til konsulenthuse og uddannelsesinstitutioner, men præges af begrænset strategisk koordinering mellem myndigheder, forskning og erhvervsliv. Øget regulering, politisk opmærksomhed og en stigende modenhed i virksomhedernes ledelseslag gør, at der er stor efterspørgsel på cybersikkerhedskompetencer. Samtidig er branchen udfordret af strukturelle udfordringer som mangel på kvalificeret arbejdskraft samt vanskeligheder for start-ups med at opnå markedsgennembrud og kapital.

Med en styrket strategisk koordinering og optimerede rammevilkår er der et betydeligt potentiale for at fremme innovation, styrke modstandsdygtigheden og sikre en mere sammenhængende udvikling af den danske cybersikkerhedsindustri.

stigende grad er blevet bevidste om nødvendigheden af cybersikkerhed, er det en gennemgående udfordring at få omsat denne bevidsthed til konkret handling.

For borgere er digital svindel blevet en del af hverdagen. Langt størstedelen af befolkningen har været udsat for forsøg på phishing eller anden svindel, og mange er reelt blevet snydt, hvilket har store konsekvenser for borgerne og kan svække tilliden til offentlige myndigheder. Svindelmetoderne bliver mere avancerede og benytter i stigende grad psykologiske greb, hvilket gør det svært for borgerne at gennemskue svindel. Flere undersøgelser viser, at faktorer som alder og køn har betydning for, hvor sårbare borgerne er overfor digital svindel. Særligt unge og ældre skiller sig ud. De unge viser en tendens til at bruge færre sikkerhedsforanstaltninger som f.eks. at opdatere antivirusprogrammer samt at bruge stærke og unikke adgangskoder. Dette kan hænge sammen med, at de har en anden risikoforståelse end ældre, og at flere unge end ældre ikke på samme måde har opfattelsen af et eget ansvar for at løfte sikkerheden. De ældre er særligt sårbare overfor visse svindeltyper, såsom investeringssvindel, hvilket kan skyldes større økonomiske opsparinger blandt de ældre generationer. Hos borgerne er en af de største barrierer for en sikker digital adfærd en manglende forståelse for behovet for sikker digital adfærd, der opleves som teknisk og tidskrævende. Mange tilkendegiver desuden, at de ikke er tilstrækkeligt informeret om, hvor de kan få hjælp, hvis de bliver ramt. Der er således behov for en styrket indsats for at øge borgernes kompetencer gennem oplysning, uddannelse og træning samt at designe løsninger, der understøtter sikker digital adfærd i praksis.

Mens opmærksomheden på betydningen af cybersikkerhed vokser, har mange virksomheder stadig udfordringer med at implementere de nødvendige tekniske og organisatoriske sikkerhedstiltag, der vil svare til deres risikoprofil. Det gælder særligt små og mellemstore virksomheder (SMV'er), som kan have svært ved at prioritere cybersikkerhed i en travl hverdag med få ressourcer og kompetencer til at håndtere de stigende trusler. Samtidig ses betydelige forskelle mellem SMV'erne og de store virksomheder i forhold til ledelsesinvolvering og beredskabsplanlægning. En forklaring kan være, at især SMV'erne oplever usikkerhed om afkastet ved investering i it-sikkerhed, hvilket gør det vanskeligt for dem at prioritere området. I flere analyser findes desuden forskel på virksomheders digitale sikkerhedsniveau på tværs af brancher, hvilket skaber uensartet beskyttelse i det samlede erhvervslandskab. Et bredt erkendt problem er også manglen på kvalificerede cybersikkerhedskompetencer – især profiler, der kan bygge bro mellem tekniske løsninger og forretningsmæssige forståelse. For at hæve sikkerhedsniveauet er der behov for øget opmærksomhed i ledelsen, opkvalificering af medarbejdere og en styrket risikobaseret tilgang – særligt hos de virksomheder, hvor sikkerhedsniveauet ikke svarer til deres risikoprofil.

Med implementeringen af NIS 2 vil aktørerne i cyberøkosystemet få nye forpligtelser til blandt andet hændelseshåndtering, og der vil blive stillet nye krav til den nationale CSIRTs kapaciteter. Det danske cyberøkosystem er komplekst, og det er vigtigt, at der faciliteres et effektivt samarbejde mellem den nationale CSIRT, CERT'er og øvrige aktører. Der bør derfor være veldefinerede roller for alle aktørerne, og roller og ansvar bør trænes gennem øvelser og tests. Det kræver værktøjer, som kan understøtte vidensdeling og effektiv hændelseshåndtering med henblik på at øge robustheden på tværs af samfundet, så offentlige og private aktører er beredte, når en hændelse indtræffer.

Den danske cyberindustri har betydning for både Danmarks digitale sikkerhed og den økonomiske vækst. Cybersikkerhedsbranchen spænder bredt fra højt specialiserede teknologivirksomheder til konsulenthuse, uddannelsesinstitutioner og start-up-miljøer. Danmark har stærke faglige miljøer inden for kvantekommunikation og kryptografi. Men flere aktører peger på, at industrien i dag opererer i et fragmenteret landskab, hvor koordinering mellem virksomheder, forskning og myndigheder kan styrkes – blandt andet ved at skabe et fælles strategisk sigte for branchens udvikling. Samtidig efterspørger mange SMV'er konkrete råd, trusselsvarsler og gratis værktøjer, hvilket tyder på, at der er øget opmærksomhed på cybersikkerhed i SMV'erne. Cyberindustrien er en branche i udvikling med mange aktører – virksomheder, forskningsinstitutioner og stærke faglige miljøer.

Styrelsen for
Samfundssikkerhed

Datavej 20
3460 Birkerød
Telefon: + 45 4516 1666
E-mail: samsik@samsik.dk

Forsidefoto: Unsplash, Denmark af Rolands Varsbergs