

Er jeres virksomhed
klar til i morgen?

2026

Executive Summary

Fokus er ændret, men fortsat stor optimisme hos de danske virksomheder

I det seneste år er danske virksomheder blevet presset på flere områder. Geopolitiske, teknologiske og sikkerhedsmæssige udfordringer stiller flere og nye krav til virksomhederne. Men dette års undersøgelse foretaget af det internationale analyseinstitut Ipsos på vegne af TDC Erhverv viser også, at danske virksomheder står med en række nye muligheder, som de er blevet bedre til at udnytte. Optimismen og troen på fremtiden er derfor stadig stor blandt de danske erhvervsledere og virksomhedsejere.

For tredje år stiller TDC Erhverv skarpt på dansk erhvervsliv og undersøger, hvordan danske virksomheder forholder sig til it-sikkerhed, digitalisering og brugen af nye teknologier som kunstig intelligens. Hvor digitalt modne er virksomhederne i dag, hvordan ser de på fremtiden, og hvad vil virksomhederne prioritere for at imødekomme de stigende udfordringer og muligheder? Det er nogle af de spørgsmål, vi giver svar på i denne rapport.

Undersøgelsen er gennemført på tværs af brancher og virksomhedsstørrelser: Små med 2-50 medarbejdere, mellemstore med 51-249 medarbejdere samt de store med over 250 ansatte. Uanset størrelsen er én ting sikkert – verden er ikke blevet mere forudsigelig og tryk i det forgangne år. Usikkerhed og forandring er blevet et grundvilkår i Danmark og hele Europa. Geopolitiske spændinger med direkte eller indirekte dansk involvering er taget til, og det er med til at udfordre virksomhedernes it-sikkerhed. Resultaterne i undersøgelsen viser således, at de adspurgte virksomheder har oplevet en øget sårbarhed over for cyberangreb det seneste år.

Flere angreb og øgede krav

I alt er knap 11% af virksomhederne i undersøgelsen blevet ramt af cyberkriminalitet i 2025. Det er mere end en fordobling i forhold til året før. Disse tal understreger, at når trusselsbilledet er i konstant forandring, skal sikkerhedsindsatsen hos virksomhederne også følge med.

Det er ikke noget, der kan klares med et enkeltstående indgreb eller investering. Dertil er omkostningerne i forbindelse med et cyberangreb for omfattende. Knap halvdelen af de store virksomheder i undersøgelsen vurderer, at det vil koste over 500.000 kr. om dagen at blive udsat for angreb. Efterfølgende interviews peger endda på daglige udgifter på op til 20-40 mio. kr.

Virksomhederne påvirkes også af et stigende behov for digital suverænitet. Fra politisk side er der en ambition om, at offentlige institutioner, virksomheder og organisationer skal have kontrol over deres data og it-infrastruktur – frem for at være afhængige af udenlandske teknologileverandører og lovgivning. Det handler ikke om at afskære os fra globale samarbejder, men om at få flere valgmuligheder inden for kritiske teknologiområder. Danmark og EU skal ganske enkelt kunne mere selv og have flere kort på hånden.

71%

Samlet set føler 71% af virksomhederne sig i meget høj eller i høj grad klædt på til fremtiden.

Mod henholdsvis 67% i 2024 og 50% i 2023.

På sigt er det en fordel for danske virksomheder, da de får mere kontrol i en usikker verden. Men på den korte bane stiller det krav til bl.a. valg af leverandører og opbevaring af data. Hvilke europæiske alternativer findes der, hvem skal man samarbejde med, og hvilke myndigheder skal have adgang til hvad? Samtidig stilles der øgede krav om dokumentation for datahåndtering og overholdelse af EU-regler, særligt hvis man arbejder med kritisk infrastruktur eller er underleverandør til større koncerner. Rapporten viser, at specielt mellemstore virksomheder oplever, at det er svært at følge med lovkravene.

Kunstig intelligens og ægte optimisme

Årets rapport fremhæver en række områder, hvor der er sket forandringer. Det gælder bl.a. inden for AI og automatisering. Kunstig intelligens er i høj grad blevet et værktøj, som virksomheder i alle størrelser er blevet bedre til at bruge og i langt højere grad prioriterer. AI er ikke længere noget, man kun taler om – det er noget, man benytter. 30% af de store virksomheder bruger

AI i dag, mod kun 8% i 2024. De små og mellemstore virksomheder viser samme udvikling. Men tallene viser også, at der stadig er mange virksomheder, der endnu ikke er kommet i gang.

Til gengæld er ESG og bæredygtighed ikke blandt de højest prioriterede områder i denne undersøgelse. Det afspejler, at der er andre emner, der fylder mere i virksomhedernes bevidsthed i forhold til tidligere år. Det kan også skyldes, at nogle virksomheder føler, at de allerede har opnået en del resultater i arbejdet med ESG og bæredygtighed.

Udfordringer eller ej, så ser de danske virksomheder i rapporten positivt på fremtiden. Størstedelen føler sig godt rustet til de kommende år, og samlet set oplever 4 ud af 5 mellemstore og store virksomheder, at de er godt klædt på. Det er et tal, der er steget gennem alle tre års undersøgelser. Selv om geopolitiske stridigheder, sikkerhedsmæssige trusler og økonomisk usikkerhed fortsat præger dagsordenen.



It-sikkerhed

It-sikkerhed har aldrig spillet en vigtigere rolle

Danske virksomheder oplever en stigende trussel fra cyberkriminalitet, og flere virksomheder har været udsat for konkrete angreb i det seneste år. Fra de små enkeltmandsvirksomheder til de helt store virksomheder. Samtidig er den sikkerhedspolitiske situation omkring Ukraine og Rusland og det internationale spotlys på Danmark kun taget til i styrke. Danske virksomheder er derfor fortsat attraktive mål for it-kriminelle og hackere fra fremmede stater af både økonomiske og politiske årsager.

Dette underbygges af tal fra TDC Erhverv Sikkerhedsrapport. Her angives antallet af forsøg på at tilgå ondsindede domæner, som bliver blokeret af TDC Erhverv Internetfilter. Altså tilfælde af f.eks. phishing og malware, hvor cyberkriminelle forsøger at manipulere brugere – og det antal er kun steget gennem årene. Fra omkring 10 millioner i 2023 til over 27 millioner i 2024. Og ifølge TDC Erhverv Sikkerhedsrapport fortsatte den negative udvikling i 2025.

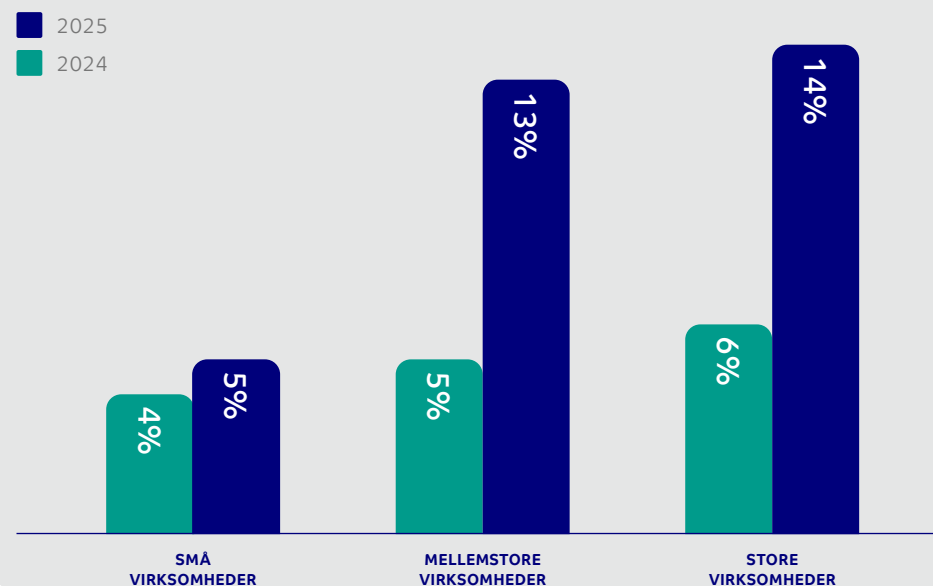
Ser man fremad, kan vi kun forvente, at antallet af cyberangreb vil stige. For i takt med at der udvikles nye teknologier og muligheder inden for bl.a. AI og automatisering, får it-kriminelle også nye værktøjer at arbejde med.

It-kriminaliteten opleves ikke kun som tal i statistikker, men i virksomhedernes hverdag. På tværs af brancher og uanset om det er private virksomheder eller offentlige institutioner. Derfor er det heller ikke overraskende, at danske virksomheder ser et endnu større potentiale for at forbedre deres it-sikkerhed sammenlignet med 2024. Når der sker flere indbrud i et hus, ønsker man naturligt nok at sætte flere og bedre låse på dørene.

Flere cyberangreb end tidligere år

Styrelsen for Samfundssikkerhed vurderer da også truslen fra cyberkriminalitet og it-angreb mod danske virksomheder til fortsat at være meget høj.^[1] Styrelsen fremhæver helt konkret, at det er meget sandsynligt, at danske virksomheder bliver ramt af ransomware-angreb, datatyveri, digital svindel og/eller DDoS-angreb.

Ramt af cyberangreb det seneste år



[1] Cybertruslen mod Danmark 2025.

Det stemmer godt overens med resultater fra denne undersøgelse. For flere danske virksomheder har været ramt af cyberangreb inden for det seneste år, end vi har set i tidligere års undersøgelser.

Flere virksomheder af alle størrelser har været udsat for cyberangreb i 2025 end i tidligere års undersøgelser.

I 2025 blev 14% af de adspurgte store virksomheder i undersøgelsen ramt af cyberkriminalitet, mens tallet i 2024 kun var 6%. Tager man udgangspunkt i, at der er omkring 900 store virksomheder i Danmark med over 250 medarbejdere, svarer det altså til, at 126 af dem har været udsat for cyberangreb i 2025. Blandt de mellemstore i undersøgelsen er udviklingen den samme, da andelen af virksomheder udsat for angreb i det forgangne år er steget fra 5% i 2024 til 13% i 2025.

Set over en længere periode opleves samme tendens. Totalt set er 18% af de små virksomheder i undersøgelsen blevet ramt af cyberkriminalitet inden for de seneste fem år, mens det er tilfældet for 38% af de mellemstore og 44% af de store virksomheder i samme periode. 24% af de store virksomheder er endda blevet ramt af it-angreb mere end én gang.

Ser man mere detaljeret på, hvornår angrebene har fundet sted i den femårige periode, er der en tydelig koncentration af angreb de senere år. Hele 76% af de mellemstore virksomheder, der har oplevet it-kriminalitet inden for de seneste fem år, er blevet angrebet inden for de seneste to år. I undersøgelsen fra 2024 hed det tal blot 44%. De små virksomheder oplever samme udvikling. Her har i alt 65% af dem, der er blevet ramt, oplevet angreb inden for de seneste to år, mens tallet fra 2024 kun var 33%.

Der er altså flere virksomheder, der har været udsat for cyberkriminalitet i løbet af året 2025 end tidligere år. Mens en stigende del af dem, der er blevet angrebet inden for de seneste fem år, er blevet ramt i løbet af 2024 og 2025.

Teknologien arbejder også for de it-kriminelle

Hvordan sker de typiske it-angreb så? Phishing er fortsat en populær angrebsteknik blandt it-kriminelle, og det vurderes, at hackere fortsat vil anvende phishing mod danske virksomheder og organisationer i de kommende år.² Ved phishing forsøger hackerne ved hjælp af mails, sms'er eller andre kommunikationsformer at narre en medarbejder til at åbne en vedhæftet fil eller klikke på et link og på den måde aktivere malware, der giver hackerne adgang til virksomhedens it-systemer. Herefter kan de f.eks. kryptere virksomhedens data og kræve en løsesum for at gøre disse data eller systemer tilgængelige igen. Det er også kendt som et ransomware-angreb.

[2] Styrelsen for Samfundssikkerhed, Cybertruslen mod Danmark 2025.



500.000 kr.

i daglig omkostning

Knap halvdelen af de store virksomheder forventer en daglig omkostning ved et cyberangreb på over 500.000 kr.
Inden for produktion og retail tales der om daglige tab på op mod 20-40 mio. kr.

Styrelsen for Samfundssikkerhed nævner desuden en tendens, som sandsynligvis vil påvirke truslen fra cyberangreb og phishing de kommende år. Nemlig udviklingen af kunstig intelligens.^[3] Hackere kan bl.a. anvende AI til at forbedre og målrette deres phishing-beskeder, så de bliver endnu sværere at identificere for modtagerne. AI kan også være tidsbesparende for it-kriminelle, der f.eks. kan benytte sprogmodeller til hurtigere at skrive mere overbevisende phishing-beskeder. Det er derfor også muligt, at phishing i fremtiden vil blive mere sofistikeret, mere udbredt og mere effektiv.

I forhold til it-sikkerhed er AI altså både en del af truslen og en del af løsningen. For AI har også et stort potentiale i forhold til at udvikle nye værktøjer og software, der kan øge virksomheders modstandsdygtighed.

Cyberangreb koster milliarder for virksomhederne

Cyberangreb kan have stor betydning for den enkelte virksomheds bundlinje og være forbundet med store udgifter. Hackerne kan kræve en betragtelig sum penge for at give adgang til krypterede data ved ransomware-angreb. Men cyberangreb kan også medføre store omkostninger som følge af tabt indtjening og nedetid i produktionen samt udgifter til at genoprette systemerne og driften.

Mindst lige så vigtigt: Det kan belaste virksomhedens troværdighed og omdømme blandt kunder, borgere og samarbejdspartnere, hvis deres data lækkes. Hvilket bl.a. kan medføre en nedgang i ordrer og produktiviteten og på den måde skade virksomhedens økonomi på den længere bane.

Undersøgelsen understreger, at de danske virksomheder er meget bevidste om udgifterne forbundet med cyberangreb. Knap halvdelen af de adspurgte store virksomheder vurderer, at omkostningerne ved et angreb vil være på over 500.000 kr. om dagen.

Hvor slemt det kan gå, er angrebet på bilfabrikanten Jaguar Land Rover et eksempel på. I september 2025 blev virksomhedens centrale it-struktur angrebet, og det tog seks uger, før Jaguar kunne genoptage fuld produktion. Angrebet er blevet kaldt verdens dyreste cyberangreb. Salget af biler fra Jaguar faldt med 43% i følgende kvartal, og skaden vurderes til at koste omkring 1,9 milliarder pund for den britiske økonomi alene.^[4]

[3] Styrelsen for Samfundssikkerhed, Cybertruslen mod Danmark 2025.

[4] <https://www.theguardian.com/business/2026/jan/06/jaguar-land-rover-sales-us-tariffs-cyber-attack-shares-tata-motors>
<https://www.danskindustri.dk/brancher/di-digital/nyhedsarkiv/nyheder/2025/11/verdens-dyreste-cyberangreb-da-jaguar-land-rover-gik-i-sta/>

Hvis et it-angreb på en stor virksomhed i snit varer otte måneder, ender det med en regning på 120 mio. kr. for én virksomhed og over 15 mia. kr. i alt for de store virksomheder alene.

Interviews med større virksomheder i produktion og retail viser, at daglige tab ved it-angreb kan løbe op i **20-40 mio. kr.** ved fuld nedlukning.

I lyset af en international undersøgelse foretaget i 2025, der peger på, at et it-angreb på en nordisk virksomhed i gennemsnit varer otte måneder eller 240 dage,⁵ svarer det altså til, at et gennemsnitligt angreb på en stor dansk virksomhed lander på en regning på 120 mio. kr. Hvilket igen fører til en samlet omkostning for de store virksomheder på over 15 mia. kr. årligt. Samtidig er angrebene naturligvis også en stor belastning for både samfund og borgere.

At udgifterne ved et cyberangreb i virkeligheden kan være langt højere fremgår af en række dybdeinterviews, vi har foretaget. Vi har talt med beslutningstagere i større virksomheder (+250 ansatte) i produktion og retail for at få et mere nuanceret billede af konsekvenserne bag tallene. Her peges der på, at det daglige tab ved it-angreb kan løbe op i to cifrede millionbeløb og ofte mellem 20-40 mio. kr. ved fuld nedlukning.⁶ Størrelsen på tabet afhænger af, hvor i produktionsprocessen nedlukningen sker. Processtop og spild kan fordoble konsekvensen afhængigt af, hvornår nedlukningen rammer, og om der f.eks. allerede er indkøbt råvarer, der må skrottes.

Som en af beslutningstagerne udtaler: "Hvis det er tidligt i en proces, hvor vi endnu ikke har påført en masse af de dyre råvarer, der bliver brugt i vores produktion, så ligger det i den lave ende. Hvis vi har brugt de råvarer, og vi bliver nødt til at stoppe processen, og uden at vi kan genanvende, så ligger det i den høje ende."

Ser man på de små og mellemstore virksomheder i vores undersøgelse, så estimerer de den daglige udgift ved cyberangreb til at ligge på henholdsvis 70.000 kr. og 190.000 kr. Hvis man er optimistisk og sætter et cyberangreb til at vare blot 30 dage, svarer det altså til en gennemsnitlig udgift på knap 4 mio. kr. Mindre beløb end for store virksomheder, men til gengæld er hele forretningen ofte på spil, når små eller mellemstore virksomheder rammes af cyberangreb, da de kan være økonomisk eller ressourcemæssigt udfordrede i forhold til at genopbygge virksomheden efter et angreb.

Trods de store omkostninger forbundet med et cyberangreb forventer virksomhederne dog ikke, at et angreb vil føre til konkurs. Kun mellem 1% og 4% af de adspurgte virksomheder forventer med 75-100% sandsynlighed, at et angreb vil medføre konkurs inden for 12 måneder. Set i lyset af, at de estimerede udgifter ved et cyberangreb altså ligger på mindst 70.000 kr. om dagen, virker det paradoksalt, at særligt de små virksomheder ikke ser cyberkriminalitet som en større trussel mod deres eksistens.

[5] https://www.fastly.com/resources/industry-report/security/cybersecurity-at-the-crossroads-nordics-2025?utm_source=chatgpt.com

[6] Interviews foretaget i 2026 af analysevirksomheden GetWhy

35%

af de små virksomheder har slet ingen plan i tilfælde af cyberangreb.

Det kan skyldes, at mange små virksomheder ikke opfatter sig selv som relevante for it-kriminelle, eller at de oplever en form for optimisme-bias, hvor de tænker, at den slags kommer jo ikke til at ske for dem. Der kan også være små virksomheder, der ikke er opmærksomme på, hvor lang tid det reelt tager at komme i fulde omdrejninger igen efter et angreb. Eller på økonomiske følger-virkninger i form af f.eks. tab af kunder og tillid, eventuelle erstatningskrav, nedsat effektivitet samt ekstra omkostninger til genopretning.

Gennemgående følelse af sikkerhed

Den stigende trussel fra cyberkriminalitet og de betragtelige udgifter, der er forbundet med et angreb, medfører dog en øget bekymring hos virksomhederne. Især blandt de store virksomheder, hvor 64% i høj eller meget høj grad er bekymret for cyberkriminalitet. Det er en stigning på knap 10% i forhold til sidste års rapport.

Ikke desto mindre føler virksomhederne sig generelt godt sikret mod cyberkriminalitet. 72% af de mellemstore virksomheder oplever, at de er sikret i høj eller meget høj grad, mens det samme er tilfældet for 64% af de store. De små virksomheder har mindre ro i maven, og kun 46% føler sig i høj eller meget høj grad sikret. Faktisk en mindre tilbagegang i forhold til sidste års tal. Samtidig er der en tendens til, at de virksomheder, der tidligere har været ramt,

i højere grad føler sig sikret. Årsagen kan være, at disse virksomheder allerede har handlet og truffet en række forholdsregler.

Flere har en plan – men er den god nok?

Følelsen af at være sikret blandt de mellemstore og store virksomheder kan skyldes, at flere og flere har en konkret beredskabsplan i tilfælde af cyberkriminalitet, og derfor føler sig godt forberedte. 9 ud af 10 mellemstore og store virksomheder har således en plan. Her er især de mellemstore gået frem i forhold til sidste år, hvor kun 3 ud af 4 havde en strategi i tilfælde af angreb. Dog har kun lige under 1/4 af virksomhederne en fuldt implementeret plan, hvor alle i virksomheden ved præcis, hvad de skal gøre.

De små virksomheder halter dog fortsat efter. 4 ud af 5 af de små har ikke en fuldt implementeret plan, og 35% af disse virksomheder med mellem 2-50 ansatte har slet ingen plan. På trods af at de altså vurderer det gennemsnitlige økonomiske tab til 70.000 kr. om dagen.

Jo hurtigere virksomheden kan få et eventuelt angreb bremsset og dæmmet op for skaderne, jo bedre kan man begrænse den potentielle nedetid og udgifterne. Derfor er det vigtigt, at der ikke skal tages for mange vigtige beslutninger, når først skaden er sket.

I en tid, hvor flere og flere især større virksomheder bliver udsat for cyberangreb, understreger seneste tal altså, at der er plads til betragtelige forbedringer hos virksomhederne. Når et angreb vurderes til at koste op mod 500.000 kr. og i nogle tilfælde langt over, er det ikke nok, at 1 ud af 4 virksomheder samlet set har en detaljeret og gennemført plan.

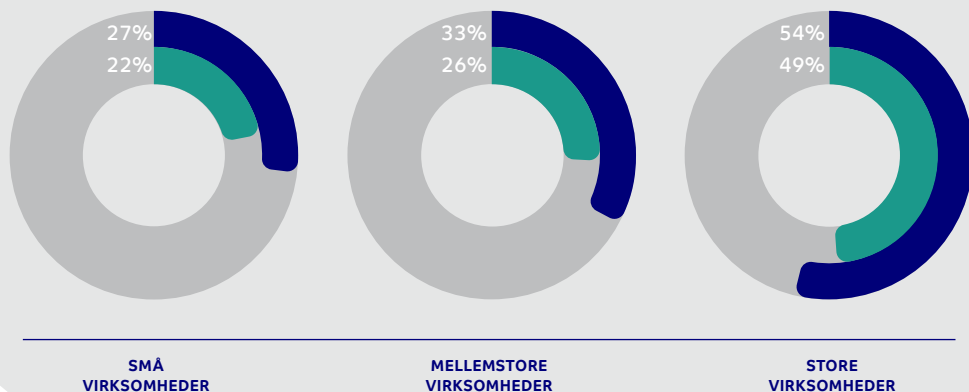
Det er vigtigt, at en beredskabsplan ved angreb er implementeret i hele virksomheden, og at alle er opmærksomme på truslen. Det er der

flere grunde til. Dels sker 25% af alle forsøg på angreb via phishing, hvor it-kriminelle forsøger at narre medarbejdere og vinde deres tillid, så de kan få adgang til it-systemer og vigtige data.⁷ Noget som de it-kriminelle hele tiden bliver bedre og mere overbevisende til at udføre. Men en beredskabsplan er desuden blevet endnu mere relevant efter indførelsen af den danske NIS2-lov, der trådte i kraft den 1. juli 2025.

[7] TDC Erhverv Sikkerhedsrapporten Q2 2025, side 4.

Ser større potentiale for at forbedre processer for datasikkerhed

■ 2025
■ 2024



Beredskab er blevet en nødvendighed

NIS2-loven skærper kravene til it-sikkerhed, ledelsesansvar og beredskab – og den omfatter langt flere virksomheder end tidligere i samfundsvigtige sektorer som f.eks. energi, transport, sundhed, finans, digital infrastruktur og offentlig forvaltning. Også leverandører til disse virksomheder kan blive indirekte ramt gennem krav i kontrakter om dokumentation eller specifikke sikkerhedsforanstaltninger.

Ifølge NIS2-loven skal omfattede virksomheder kunne dokumentere, at de arbejder systematisk med it-sikkerhed, og loven stiller også krav til beredskabsplaner og klare interne processer. På den måde medfører NIS2, at it-sikkerhed går fra at være et teknisk anliggende til at være et strategisk anliggende og et ledelsesansvar. Lever man ikke op til kravene, kan det føre til store bøder, påbud og skærpet tilsyn fra myndighedernes side.

I en tid, hvor omdømme, tillid og stabilitet er altafgørende, er it-sikkerhed og ansvarlig datapraksis altså ikke længere blot en teknisk

nødvendighed, men et konkurrenceparameter.

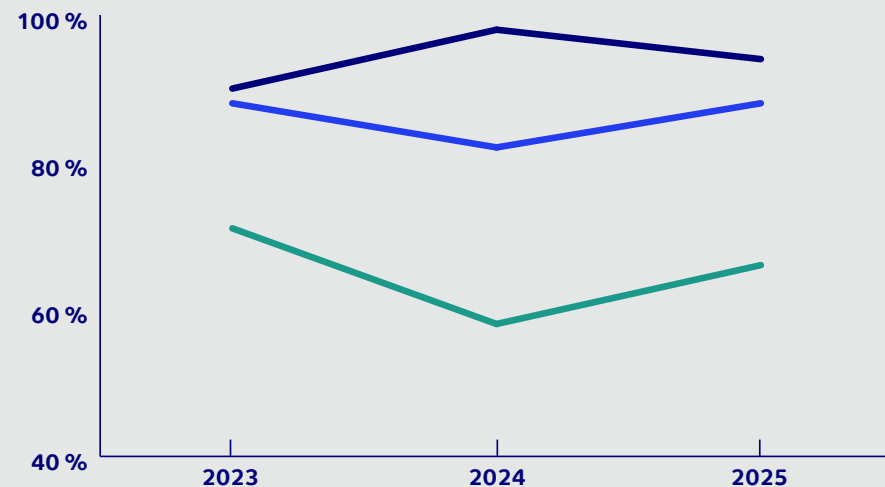
Fremtiden tilhører de virksomheder, der er proaktive og benytter NIS2 som en anledning til at styrke robustheden, tilliden og modenheden – ikke bare som en pligt, men som en investering. Det er den tilgang, som efterspørges af kunder, samarbejdspartnere og myndigheder.

Stort fokus på it-sikkerhed – heldigvis

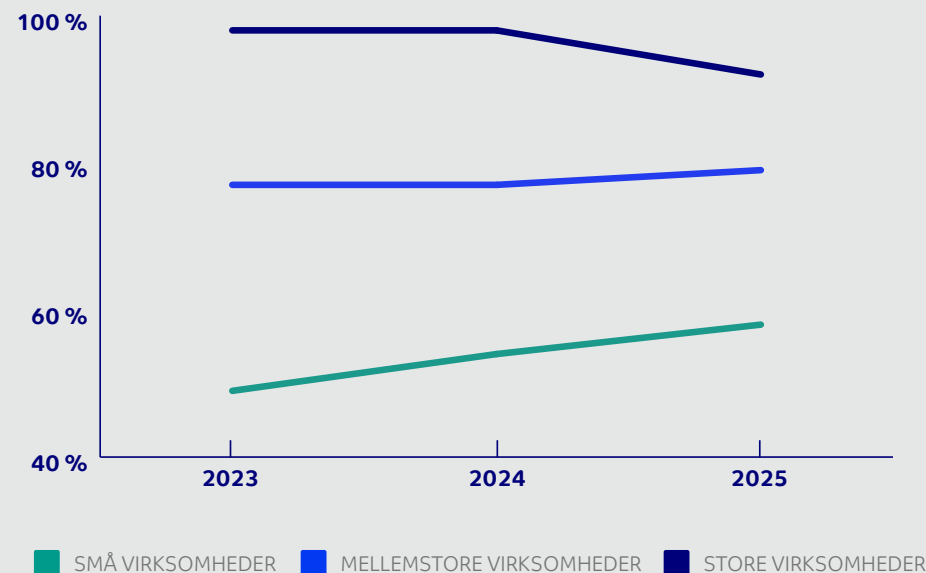
Selv om der stadig er god grund til at optimere beredskabsplanerne, er de danske virksomheder opmærksomme på it-sikkerheden. Rapportens resultater viser, at vedligeholdelse og udbygning af it-sikkerhed fortsat er i top tre over de områder, som de store virksomheder stiller skarpt på nu og i de kommende to år.

Lige så vigtigt er det, at virksomheder uanset størrelse ser endnu større potentiale for at forbedre deres processer for datasikkerhed, sammenlignet med sidste års rapport. 54% af de store virksomheder mener således, at der er plads til at forbedre virksomhedens processer i forhold til datasikkerhed.

Har investeret i it-sikkerhed det seneste år



Forventer at investere i it-sikkerhed de kommende år



Tilsvarende er it-sikkerhed fortsat et punkt på dagsordenen hos den øverste ledelse hos 82% af de store virksomheder, mens det er tilfældet for 73% af de mellemstore og 49% af de små. På dette område er der generelt ikke sket den store udvikling. Man kan altså konkludere, at mens it-sikkerhed fylder en del på de danske ledelsesgange hos især store virksomheder, så halter det med at få det ført ud i virksomhederne og omsat til nogle detaljerede planer for, hvad alle skal foretage sig, hvis der sker et it-angreb, jf. tidligere omtalte tal omkring beredskabsplaner.

I forhold til at investere i it-sikkerheden forventer virksomhederne på tværs af størrelser fortsat at bruge penge – jo større virksomhed, desto større villighed til at investere. 94% af de store virksomheder har investeret i it-sikkerhed, mens 2 ud af 3 af de små har brugt penge på at sikre sig mod it-kriminalitet. En stigning på 8% i forhold til sidste års rapport. Det er positivt, at danske virksomheder altså er bevidste om, at de bliver nødt til at investere i it-sikkerhed, og at de også gør det. Det gælder også fremadrettet. Forventningerne blandt de mellemstore og store virksomheder ligger nogenlunde stabilt i forhold til tidligere år. 8 ud af 10 mellemstore og 9 ud af 10 store virksomheder regner med at bruge

penge på hardware, software og kompetencer inden for it-sikkerhed i de kommende år.

De små virksomheder vil være med

Blandt små virksomheder i undersøgelsen forventer 3 ud af 5 at foretage yderligere investeringer i it-sikkerhed i de kommende år. En stigning i forhold til 2024 og 2023, hvor tallet hed henholdsvis 54% og 49%. Der er altså et voksende ønske blandt de små virksomheder om at sikre sig mod cyberkriminalitet. Det kan skyldes, at flere og flere hører om cyberangreb hos konkurrenter eller læser om it-kriminalitet i medierne. Men det kan også være fordi, at flere små virksomheder allerede er blevet ramt af cyberangreb inden for de seneste år, og derfor ønsker at skrue op for sikkerheden.

Det er forventeligt, at store virksomheder har større økonomisk fokus på it-sikkerhed end de små. Dels har de flere økonomiske og personale-mæssige ressourcer. Dels er mange mellemstore og store virksomheder nu også underlagt NIS2-loven, som tidligere nævnt. Investeringer i it-sikkerhed er derfor ikke længere noget, man kan udskyde eller begrænse, men er blevet en forretningskritisk investering med direkte konsekvenser, hvis man lader være.



It-sikkerhed er ikke et tilvalg, men et forretningsfundament.

På den anden side er det forståeligt, hvis små virksomheder i højere grad har øjnene rettet mod den daglige drift. Men det er yderst positivt, at de små virksomheder ser ud til at skruer op for investeringerne nu og på den længere bane. En naturlig udvikling, ikke mindst i lyset af en forventet daglig udgift på 70.000 kr. ved et cyberangreb.

Vores undersøgelser viser desuden, at forventningen til at investere i it-sikkerhed er markant højere hos de virksomheder, der allerede har investeret i it-sikkerhed inden for det seneste år, end blandt dem, der ikke har. Således forventer 7 ud af 10 små virksomheder, der allerede har investeret i it-sikkerhed, at gøre det igen, mens tallet kun er det halve for de små, der endnu ikke har brugt penge på sikkerheden.

Det er altså et klart tegn på, at mindre virksomheder, der afsætter midler til it-sikkerhed i budgettet, oplever en fordel og vurderer, at de får

værdi for pengene. Af samme grund er det også vigtigt, at endnu flere af de mindre virksomheder afsætter et budget til it-sikkerhed, så den positive udvikling kan fortsætte.

En overdreven følelse af sikkerhed?

Tal i undersøgelsen viser altså, at danske virksomheder allerede investerer i it-sikkerhed og også agter at gøre det i fremtiden. Særligt de små virksomheder skruer op for ambitionerne på området. Dog halter det stadig i forhold til at få etableret handlingsplaner i tilfælde af angreb og få dem fuldt implementeret i virksomhederne.

Samtidig bliver flere og flere virksomheder angrebet af cyberkriminelle. Derfor er det kun naturligt, at stadigt flere af især de store virksomheder bekymrer sig om risikoen for cyberangreb.

Ikke desto mindre er der en generel følelse af sikkerhed i det danske erhvervsliv, og samlet set

føler virksomhederne sig godt beskyttet mod cyberkriminalitet. 3 ud af 4 af de mellemstore virksomheder oplever, at de er sikret i høj eller meget høj grad, mens det samme er tilfældet for 2 ud af 3 af de store.

Så spørgsmålet er, om virksomhederne tager truslen fra cyberkriminalitet alvorligt nok? Det er positivt, at investeringerne i it-sikkerhed hos små virksomheder stiger, men det gør truslen også. Flere små virksomheder er blevet angrebet, og langt flere inden for de seneste to år.

En del små virksomheder vil være udfordret, når det gælder om at opbygge den nødvendige modstandsdygtighed mod cyberangreb. Derfor er det vigtigt, at sikkerhedsbudgetterne i små virksomheder bruges rigtigt, og at man bliver rådgivet strategisk om løsninger, der møder virksomhedens behov på den korte og den lange bane. Og som lever op til eventuelle lovkrav,

hvis man f.eks. er underleverandør til en virksomhed, der er omfattet af NIS2-loven.

For større virksomheder er udfordringen en anden. Her handler det om at se på it-sikkerhed med nye briller. Det er ikke længere et tilvalg, men et fundament. Både i forhold til den fortsatte drift og nye, omfattende lovkrav som NIS2. Cybersikkerhed er et konkurrenceparameter for fremtidens ambitiøse virksomheder, der ikke blot ønsker at gøre deres forretning mere modstandsdygtig over for cybertrusler. Men som ser det som en investering i virksomhedens image, robusthed og konkurrenceevne.

Selv om flere og flere virksomheder har fået øjnene op for vigtigheden af at investere i it-sikkerhed, er der behov for et markant løft af sikkerhedsniveauet for at kunne matche truslernes alvor og omskiftelighed samt markedets forventninger.



Digitalisering

Digitalisering rummer store muligheder, men stiller også krav

Danmark er et af de mest digitaliserede lande i verden med et højt niveau af digital infrastruktur og digitale tjenester. Vi stoler i høj grad på digitale tjenester fra det offentlige, og mere end 4 ud af 5 danskere bruger tjenester som MitID, e-Boks og Sundhed.dk mindst én gang om ugen.⁸

Ifølge en redegørelse fra Digitaliseringsministeriet fra 2025 er danske virksomheder ligeledes nogle af de mest digitale virksomheder i Europa. 60% af danske virksomheder vurderes til at have et højt digitalt niveau – faktisk kun overgået af finske virksomheder. Det er positivt, da digitaliseringen i dansk erhvervsliv er afgørende for at skabe øget vækst, innovation og produktivitet. Både for den enkelte virksomhed og for Danmark som helhed. Tal fra Danmarks Statistik og Digitaliseringsstyrelsen peger på, at virksomheder med et meget højt digitalt niveau har en gennemsnitlig værditilvækst, der er 19% højere end virksomheder med et meget lavt digitalt niveau.⁹

Der er dog en række områder, som danske virksomheder skal forholde sig til, hvis vi skal bevare den førende position i Europa. Blandt andet når det handler om at komme i gang med kunstig intelligens og nye teknologier, overholdelse af lovkrav, tilstrækkelig it-sikkerhed samt rekruttering af de rette kompetencer. Det er vigtigt, at digitaliseringen hos de danske virksomheder sker på den rigtige måde, så mulighederne ikke overskygges af udfordringer og trusler.

Stadig plads til digitale forbedringer

Kigger man på de mellemstore og store virksomheder, der har medvirket i vores undersøgelse, er digitalisering fortsat et af de tre største fokusområder i de kommende to år. I forhold til digitaliseringsgraden er andelen af virksomheder, der oplever at være i høj grad eller fuldt digitaliseret, nogenlunde på niveau med sidste

[8] https://www.dst.dk/da/Statistik/temaer/digitalisering?utm_source=chatgpt.com#offdig

[9] Redegørelsen om Danmarks Digitale Udvikling, februar 2025.

års undersøgelse. 64% af de store virksomheder mener, at de er digitaliseret i høj grad eller fuldt, mens det er tilfældet for henholdsvis 56% og 49% af de mellemstore og små virksomheder. I begge disse kategorier er der faktisk sket et lille fald i forhold til sidste år. Der er altså fortsat et stort potentiale i forhold til at øge digitaliseringen i de danske virksomheder uanset deres størrelse.

Blandt årsagerne til den manglende digitalisering peger de store og mellemstore virksomheder på manglende ressourcer samt viden om, hvordan digitalisering kan løfte virksomheden yderligere. Der ligger altså et arbejde i forhold til at gøre virksomheder opmærksomme på værdien af digitalisering og sikre, at de råder over de rette kompetencer. Selv om manglende ressourcer selvfølgelig også kan referere til både tid og økonomiske midler. En undersøgelse fra 2024 viser, at 8% af alle danske virksomheder havde åbne stillinger inden for informations- og kommunikationsteknologi, som de ikke kunne få besat.¹⁰

Manglen på medarbejdere inden for it-udvikling og -drift er en reel udfordring for virksomhederne. For at de kan blive ved med at udvikle og bruge digitale værktøjer, er det vigtigt, at virksomhederne har adgang til arbejdskraft

med it-kompetencer. Selv om der fortsat er en stigning i antallet af ansatte it-specialister, er der stadig mange virksomheder, der forgæves forsøger at rekruttere.

Fortsat mange data i skyen

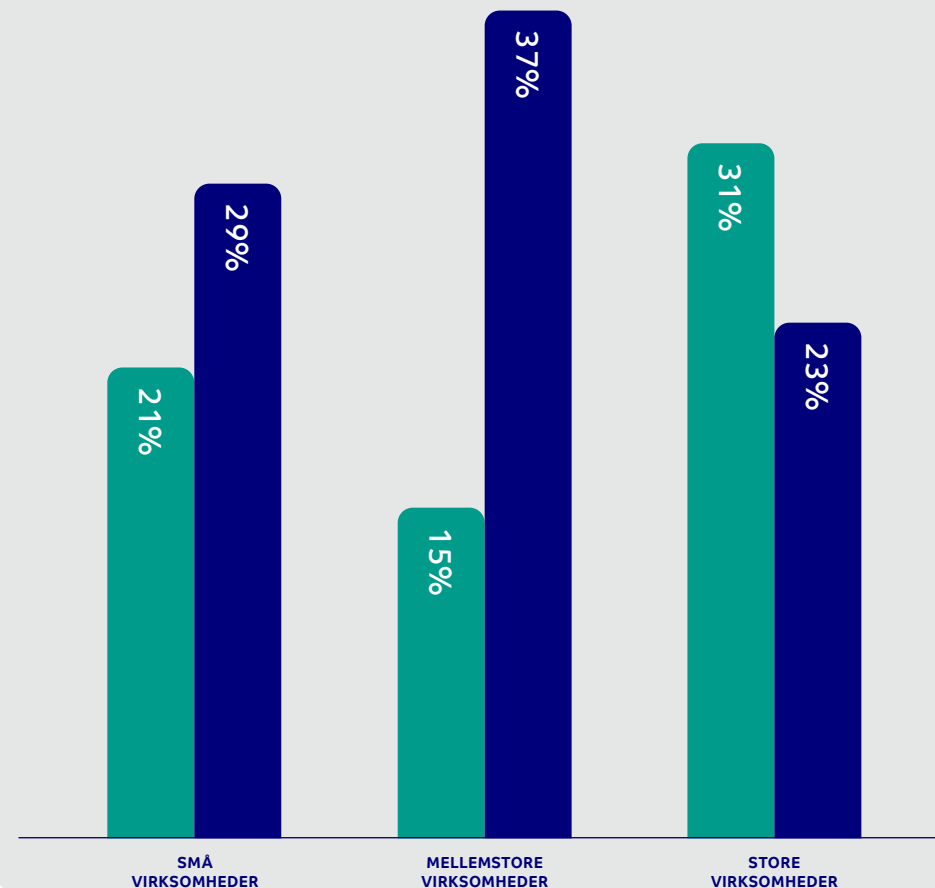
Cloud-løsninger er fortsat populære blandt virksomheder, der ønsker en høj grad af skalérbarhed kombineret med mindre vedligeholdelse og it-drift. Mange adspurgte virksomheder benytter da også fortsat cloud-løsninger til opbevaring af data. 4 ud af 5 virksomheder på tværs af størrelser opbevarer data i skyen – et lille fald i forhold til sidste år, hvor cirka 9 ud af 10 benyttede skyen til dataopbevaring.

Til gengæld er bekymringen for opbevaringen vokset betragteligt hos små og mellemstore virksomheder, der lagrer al deres data i skyen. 29% af de små virksomheder med al data i skyen har bekymringer omkring at opbevare data her. Mod kun 21% i 2024. Mens andelen af bekymrede mellemstore virksomheder er vokset endnu mere – fra 15% i 2024 til 37% i 2025.

Den stigende bekymring blandt virksomhederne kan skyldes de tiltagende geopolitiske stridigheder samt usikkerheden ved at opbevare data hos leverandører uden for EU. På den måde rummer dataopbevaring i skyen flere udfordringer, krav og spørgsmål i dag end tidligere.

Andel af virksomheder, der opbevarer al data i skyen og er bekymrede for det

■ 2025
■ 2024



[10] https://www.dst.dk/en/Statistik/temaer/digitalisering?utm_source=chatgpt.com

Der findes dog også effektive sikkerhedsløsninger udviklet i Danmark, der er designet til at beskytte følsomme og forretningskritiske informationer i cloud-tjenester. Løsningerne sikrer bl.a. virksomheder mod datatyveri og datalæk samt mod udlevering af data til både udbyderen selv og myndigheder i tredjelande som f.eks. USA. Samtidig med at GDPR, NIS2 og andre lovkrav overholdes. Et fravalg af skyen bør derfor ikke ske af sikkerhedsmæssige hensyn.

Fokus på bæredygtighed og ESG er under forandring

Et af de områder inden for digitalisering, hvor der er sket forandringer siden sidste år, er bæredygtighed og ESG. For virksomheder på tværs af størrelser ses det, at ESG ikke længere optræder blandt de øverste fokusområder i de kommende år. Det gælder særligt blandt de små virksomheder, hvor 10% angiver ESG og bæredygtighed som et fokusområde mod 42% sidste år. For de mellemstore virksomheder er andelen faldet fra 52% til 20%, mens 26% af de store virksomheder fortsat har ESG som et nøgleområde mod 40% sidste år.

Udviklingen betyder, at ESG samlet set rangerer lavere blandt de temaer, virksomhederne er blevet bedt om at forholde sig til. Det er dog ikke nødvendigvis et udtryk for, at ESG og bæredygtighed er blevet mindre vigtige områder. En mere nærliggende forklaring kan være, at andre dagsordener er steget i vigtighed, blandt andet som følge af de seneste års geopolitiske, sikkerhedsmæssige og økonomiske udfordringer.

Samtidig har nogle virksomheder givetvis oplevet, at ESG-arbejdet er blevet en integreret del af forretningen. Derfor er fokus i højere grad flyttet fra overordnede, strategiske diskussioner til mere konkrete initiativer og afledte områder. Det gælder eksempelvis energieffektivisering og ansvarlig virksomhedsdrift, som alle kan betragtes som elementer inden for ESG-området.

Grøn it fylder stadig en del

Selv om ESG samlet set rangerer lavere blandt virksomhedernes prioriteringer, er grøn it og den grønne omstilling fortsat vigtige fokusområder for især mellemstore og store virksomheder. Omkring halvdelen af disse virksomheder angiver, at de har et specifikt fokus på grøn omstilling og et bæredygtigt it-setup.



Grøn it og den grønne omstilling
er fortsat vigtige fokusområder for
mellemstore og store virksomheder.

3 ud af 5 mellemstore virksomheder oplever i høj eller meget høj grad, at det er svært at følge med i nye krav og regler.

Grøn it handler om at anvende digitale løsninger og teknologier på en måde, der minimerer klima- og ressourcepåvirkningen, samtidig med at digitalisering bruges aktivt til at understøtte den grønne omstilling. Det handler bl.a. om at implementere en cirkulær tilgang til it-udstyr baseret på genbrug og genanvendelse. På den måde kan både omkostninger og CO2-aftryk reduceres.

Tilsyneladende er der altså en uoverensstemmelse mellem virksomhedernes lavere prioritering af ESG som samlet begreb og det stigende fokus på bæredygtige initiativer som grøn it. En forklaring kan være, at ESG ofte opfattes som et komplekst og relativt abstrakt begreb, som mange sikkert også forbinder med rapportering og regulering, mens grøn it fremstår mere konkret og forretningsnært. Grønne it-løsninger kan i højere grad kobles direkte til målbare resultater på kortere sigt, eksempelvis i form af reduceret energiforbrug og lavere omkostninger. Samtidig er grøn it ofte forankret i it-afdelingerne frem for på øverste ledelsesniveau, hvilket kan føre til,

at fokus i praksis flyttes fra ESG som overordnet ramme til mere specifikke og operationelle initiativer.

Samlet set peger undersøgelsen altså på, at ESG og bæredygtighed fortsat er relevante temaer for virksomhederne, men at prioriteringen er blevet forskudt i takt med, at andre dagsordener er blevet mere vigtige.

En stærk infrastruktur er fortsat vigtig

Når man taler om digitalisering af virksomheder, er it-infrastrukturen det tekniske fundament, som understøtter og muliggør drift, skalering og udvikling af digitale løsninger. Det er den usynlige motor under alle digitale processer og omfatter både hardware, software, netværk og platforme.

Samtidig sætter it-infrastrukturen grænsen for, hvad en virksomhed overhovedet kan digitalisere – og hvor hurtigt det kan gå. En moderne infrastruktur gør det f.eks. muligt at integrere

systemer, automatisere processer og arbejde datadrevet. En forældet eller fragmenteret infrastruktur kan derimod medføre, at systemer ikke kan tale sammen, eller at nye digitale løsninger bliver umulige at implementere.

Seneste undersøgelse understreger da også, at it-infrastrukturen stadig vurderes til at spille en vigtig rolle for de danske virksomheder. 4 ud af 5 store virksomheder mener, at en stærk it-infrastruktur er afgørende for fremtiden, mens 3 ud af 4 mellemstore virksomheder er enige i det udsagn. For de små virksomheder gælder det omkring halvdelen af de adspurgte. Høje tal, der nogenlunde er på niveau med sidste års undersøgelse.

Valget af it-partner er kritisk for, om virksomhedens it-infrastruktur bliver en løftestang for digitalisering eller en spændetrøje. Det er vigtigt at finde en partner, der forstår både forretningen og teknologien, og derfor kan rådgive strategisk og sammenhængende og på den måde være med til at forme virksomhedens

digitale fundament, hvor it-sikkerheden er tænkt ind fra start.

Stigende krav udfordrer virksomhederne

Samlet set står danske virksomheder over for en lang række vigtige udfordringer og flere afgørende valg. Det gælder f.eks. inden for områder som it-sikkerhed, integrering af AI, GDPR-regler og ikke mindst digital suverænitet. Bevægelsen mod digital suverænitet handler bl.a. om, at virksomheder skal mindske afhængigheden af tredjelandes lovgivning og teknologileverandører, så man opnår fuld kontrol over egne data og infrastruktur. På den måde bestemmer virksomhederne i højere grad, hvor data opbevares, hvem der har juridisk og teknisk adgang, samt hvilke regler man er underlagt.

Det er ikke fordi, danske virksomheder skal isolere sig fra internationale samarbejder, tværtimod. Men det er vigtigt at gøre sig nogle overvejelser i forhold til, om virksomheden har styr på opbevaringen og adgangen til kritiske data.

Samt at evaluere de nuværende it-leverandører og være klar til at sadle om, hvis det bliver nødvendigt.

Ved at få mere kontrol og opnå flere valgmuligheder inden for kritiske teknologiområder såsom AI, cloud og cybersikkerhed kan danske virksomheder ikke blot sikre sig mod uforudsete hændelser. Men også styrke deres forretning og konkurrenceevnen fremadrettet.

Set i det lys og de andre områder, som danske virksomheder skal forholde sig til, er det ikke overraskende, at virksomhederne oplever, at det er svært at følge med. Især de mellemstore virksomheder føler sig i stigende grad udfordrede. 3 ud af 5 mellemstore oplever i høj eller meget høj grad, at det er svært at følge med. Inkluderer man virksomheder, der føler sig udfordrede i nogen grad, kommer tallet helt op på 90%. Både de små og de store virksomheder føler sig lidt bedre klædt på. Kun 50% inden for disse kategorier føler sig presset i høj eller meget høj grad. Generelt er der ikke de store udsving i tallene i forhold til sidste års undersøgelse.

Det samme gør sig gældende, når man ser på virksomhedernes fokusområder de kommende to år. De mellemstore virksomheder har primært fokus rettet mod overholdelse og tilpasning i forhold til lovgivning og krav fra myndigheder. 43% af de mellemstore virksomheder har det som førsteprioritet. Mens de store virksomheders opmærksomhed primært er rettet mod implementeringen af AI.

En mulig forklaring på forskellen på graden af udfordring kan være, at store virksomheder føler

sig mindre udfordret, fordi de allerede har styr på en del lovkrav og til en vis grad er tvunget til det på grund af tiltag som NIS2.

Et af de emner, der til gengæld ikke bekymrer de adspurgte virksomheder på nuværende tidspunkt, er spredningen af misinformation. Det vil sige usande eller vildledende oplysninger, der spredes uden nødvendigvis at have en ond hensigt, men som folk tror er sande og deler videre. Kun omkring 30% af de mellemstore og store virksomheder er i høj eller meget høj grad bekymrede for at møde eller sprede misinformation. For de små virksomheders vedkommende er tallet helt nede på 18%.

Selv om misinformation endnu ikke optager de adspurgte virksomheder i særlig høj grad, kan spredning af falske informationer få store konsekvenser. Fordrejede historier på sociale medier kan f.eks. mindske kundernes tillid og være med til at skade en virksomheds image. I værste fald kan falske informationer også medføre direkte økonomiske tab ved at skade markedsværdien, eller misinformation kan udgøre en del af et hybridangreb, hvor større virksomheder angribes fra flere fronter.

Det er rimeligt at formode, at den øgede digitalisering og brug af AI kun vil føre til flere krav og udfordringer, som virksomhederne skal forholde sig til. Derfor er det vigtigere end nogensinde før, at virksomhederne træffer de rigtige valg i forhold til digitaliseringen og samarbejder med en tæt og betroet it-partner, der kan levere fleksible og fremtidssikre løsninger.



Danske virksomheder har taget AI til sig

Det område, hvor der er sket størst udvikling på tværs af virksomhedsstørrelse siden sidste års undersøgelse, er kunstig intelligens og anvendelsen af AI-løsninger.

Fra at være en teknologi, som alle snakkede om, men mange havde et abstrakt forhold til, er AI for alvor rykket ind på de danske arbejdspladser. Kunstig intelligens spiller således en markant større rolle nu, og forventningerne til AI fremadrettet er ligeledes vokset.

Ifølge Digitaliseringsministeriet er Danmark faktisk det land i Europa, hvor flest virksomheder benytter kunstig intelligens.^[11] Vores undersøgelse peger også på, at virksomhedernes brug af AI er steget fra 7-8% sidste år til op mod 30% i år. Jo større virksomhed, jo større tendens til at benytte AI.

Kigger man på forventninger til AI fremadrettet, er der til gengæld sket størst ændring blandt de små og mellemstore virksomheder. Knap

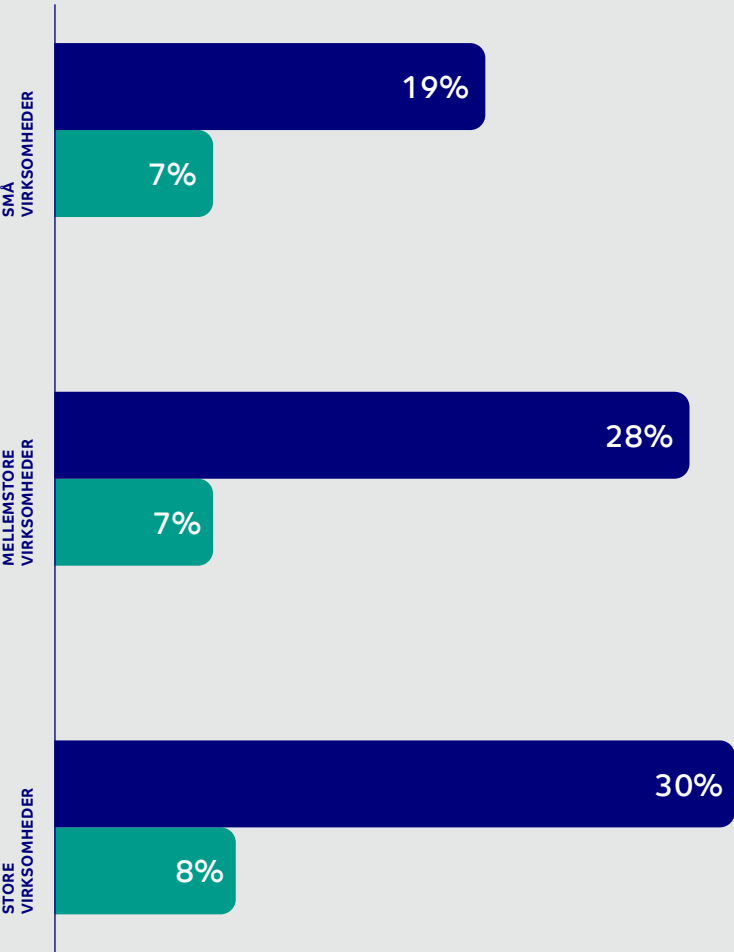
halvdelen af de små forventer, at AI vil spille en stor eller afgørende rolle i løbet af de kommende to år. Det er en stigning fra 32% siden sidste år. For de mellemstore er forventningerne steget fra 44% til 61%.

De store virksomheder har stadig de største forventninger til kunstig intelligens. 74% regner med, at AI kommer til at spille en stor eller afgørende rolle. Men det tal er stort set det samme som sidste år. En forklaring kan være, at de store virksomheder allerede er godt i gang med integrationen af AI. Mens de mellemstore og små endnu ikke er kommet så meget med på AI-vognen, og derfor har en naturlig grund til at forvente mere.

[11] Ifølge Redegørelsen om Danmarks Digitale Udvikling, februar 2025.

Virksomheder, der bruger AI i dag

■ 2025
■ 2024



Forskelligt syn på AI i forskellige brancher

Dykker man længere ned, træder nogle interessante forskelle frem. I TDC Erhvervs rapport om fremtidens arbejdsplads undersøges brugen af AI på tværs af brancher.¹² Generelt viser rapporten, at 40% af de adspurgte virksomheder bruger AI. Altså lidt højere tal end i den undersøgelse, som denne rapport er baseret på.

Man er længst fremme inden for finans og forsikring med 54%, mens retail følger efter med 39%, når det gælder brugen af AI og automatisering. Inden for retail kan AI bl.a. benyttes til at analysere kundedata, skabe personaliserede kundeoplevelser og optimere styringen af lageret. På den måde kan AI være med til at løfte konkurrenceevnen betragteligt.

Til gengæld halter logistik og transport efter med kun 9%, mens hele 14% af virksomheder, der arbejder med produktion, slet ikke kunne finde på at benytte AI. Til trods for at AI bl.a. kan løfte produktionen ved at kunne forudsige nedbrud, sikre en ensartet kvalitet samt omsætte data til bedre beslutninger.

Også inden for det offentlige er der et stort uforløst potentiale, når det gælder AI. Både på kontorgangene og ude blandt borgerne. Kun 13% af de offentlige institutioner prioriterer AI og automatisering som en del af deres digitalisering, mens 26% af de adspurgte offentlige institutioner benytter AI i nogen grad. Der er altså store muligheder for at optimere i denne sektor.

I det offentlige kan AI f.eks. spille en vigtig rolle i forbindelse med automatiseret sagsbehandling, chatbot-baseret borgerbetjening og analyse af store datamængder til proaktiv risikovurdering.

AI kan desuden føre til mere effektiv behandling og ressourcebrug, når det gælder sundhed og pleje. Kunstig intelligens kan eksempelvis benyttes i forbindelse med billedgenkendelse i diagnostik, til beregning af indlæggelsesrisici og yde digital hjælp til hjemmeplejepersonale i form af stemmestyring, beslutningsstøtte og realtidsdata om borgernes tilstand.

Stor fremgang – men endnu større potentiale

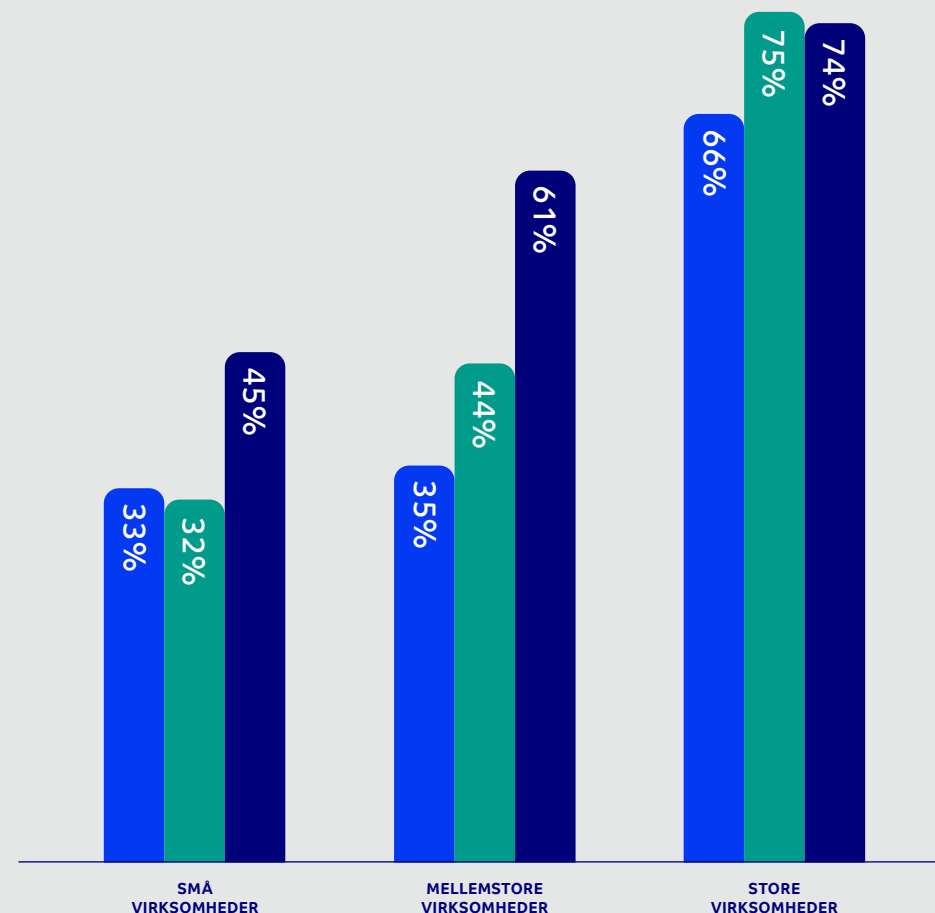
Samlet set er der sket en markant fremgang i brugen af AI-løsninger i danske virksomheder. Flere benytter allerede AI, og forventningerne til teknologiens indflydelse i de kommende år er steget pænt i de små og mellemstore virksomheder. Der er generelt også gode erfaringer med brugen af AI. Ifølge Danmarks Statistik har 70% af de virksomheder, der anvender kunstig intelligens, oplevet en positiv indvirkning gennem effektivisering af arbejdsgange. Omkring halvdelen oplever en forbedring af virksomhedens produkter, tjenester eller ydelser.¹³

[12] Har virksomheder i Danmark fremtidssikret arbejdspladsen?, TDC Erhverv 2025.

[13] <https://www.dst.dk/da/Statistik/udgivelser/NytHtml?cid=55352>

Virksomheder der forventer, at AI vil spille en stor eller afgørende rolle

■ 2025
■ 2024
■ 2023



Selv blandt store virksomheder, hvor brugen af AI er mest udtalt, er 7 ud af 10 ikke kommet ordentligt i gang med AI eller bruger det ikke meget.

Men der er også mange, der ikke har fået kunstig intelligens til at arbejde for virksomheden endnu. Selv blandt store virksomheder, hvor brugen af AI er mest udtalt, er 7 ud af 10 ikke kommet ordentligt i gang med AI eller bruger det ikke meget. Og blandt de små virksomheder er AI ikke blandt de tre områder, der er mest fokus på de næste to år. Det kan skyldes flere ting. Mange virksomheder savner stadig viden om AI og en klar kobling til, hvad det helt konkret kan gøre for deres forretning. Man læser og hører en masse om AI. Men hvordan skal man gribe det an, og hvordan kommer man i gang?

Få AI ind de rigtige steder i virksomheden

For små virksomheder kan det være en god idé at gå praktisk til værks og ikke tænke teknologi, men problemløsning. Hvad bruges der unødigt meget tid på? Hvad end det drejer sig om manuel administration, tilbudsskrivning eller kundeservice, kan færdige AI-værktøjer hjælpe relativt hurtigt. Uden at man skal bruge store summer eller være uddannet it-udvikler. Små virksomheder bør se AI som et produktivitetsværktøj, ikke et it-projekt. Noget man prøver sig frem med og ikke planlægger i årevis. I takt med at man lærer mere og ser tydelige fordele, kan virksomheden gradvist gabe over mere.

I større virksomheder kan det være en udfordring, at diskussionen om AI ikke forankres i ledelsen, men foregår blandt medarbejdere med teknologisk viden og interesse. Det betyder, at AI

ikke kobles på reelle og afgørende forretningsproblemer og heller ikke rulles bredt ud. Kunstig intelligens benyttes muligvis til lavthængende frugter i marketingteamet eller bliver et pilotprojekt i it-afdelingen. Men bliver ikke strategisk forankret og tænkt ind som en afgørende værdiskaber for forretningen.

Samtidig skal både private virksomheder og offentlige institutioner tage hensyn til skærpede krav omkring compliance, dokumentation og ansvarlig brug af data. For eksempel træner eller anvender AI-tjenester ofte data i skyen. Hvis persondata eller følsomme oplysninger bliver delt med disse AI-tjenester uden kontrol, kan der opstå et compliance-problem. Cloud-udbyderen kan blive pålagt at udlevere persondata til koncernhjemlandets myndigheder, hvilket strider mod både europæisk og dansk datalovgivning.

Som omtalt tidligere i rapporten findes der danskudviklede sikkerhedsløsninger, der kan afhjælpe dette problem. Den tekniske foranstaltning beskytter følsomme og forretningskritiske data ved at kryptere dem, før de sendes til cloud-tjenester i et tredjeland. Det betyder, at data kun er læsbare for autoriserede brugere og ikke for cloud-udbyderen eller uvedkommende. Det gør, at virksomheder og institutioner frit kan bruge de AI-tjenester og cloud-løsninger, de ønsker, og altså ikke behøver at fravælge førende softwareleverandører uanset deres nationalitet.

Ud over de teknologiske spørgsmål og dilemmaer kan kulturen i en virksomhed også være en udfordring i forbindelse med AI. Indførelsen af AI-tjenester kan være forbundet med frygt for at miste jobs – og ses som en konkurrent snarere end en hjælpende hånd. Der kan ligeledes være et element af ”sådan plejer vi at gøre”, der skaber skepsis omkring automatisering og AI.

Men det er vigtigt, at danske virksomheder i endnu højere grad byder AI indenfor. Dem, der endnu ikke har prøvet kræfter med AI, skal i gang, og dem, der er startet, skal blive endnu bedre til det. For AI kan hjælpe virksomheder med at innovere smartere, optimere bedre og producere hurtigere. Det kan afhjælpe

problemer med manglende arbejdskraft og bidrage til at skabe nye forretningsmuligheder. Til glæde for virksomhedernes bundlinje og for hele det danske samfund.

Desuden kan AI også spille en helt central rolle i forhold til it-sikkerhed – både som skjold og som tidlig varsling. AI kan analysere enorme mængder netværks- og systemdata og opdage afvigelser fra normal adfærd. Det betyder i praksis, at AI-løsninger bl.a. kan opdage malware, identificere usædvanlig login-adfærd og spotte angreb tidligere. Set med de briller er det derfor også indlysende at få kunstig intelligens til at spille sammen med virksomhedens eksisterende teknologier og systemer.



Konklusion

Virksomhedernes udfordringer overdøves af optimisme

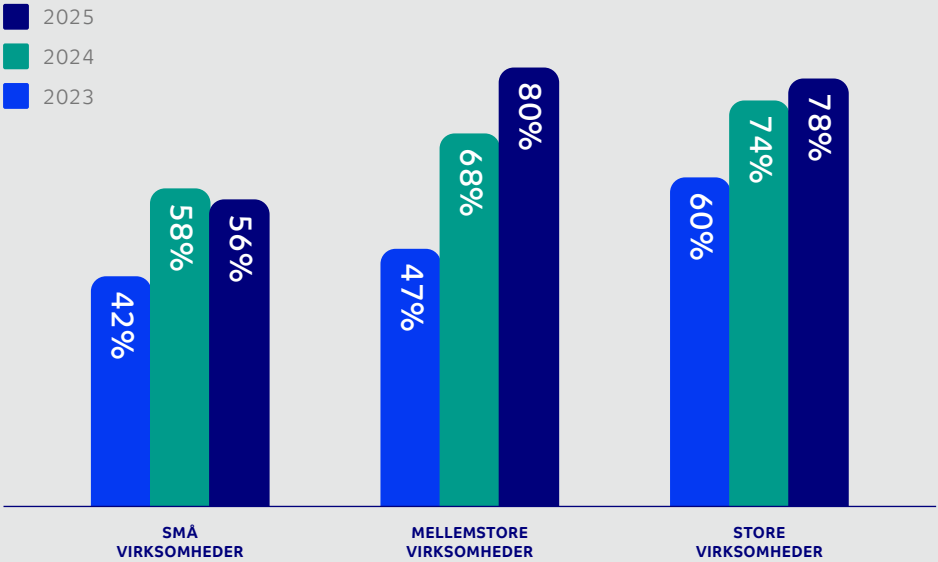
Danske virksomheder har meget at forholde sig til. De skal sikre sig mod cyberkriminalitet, udnytte digitalisering bedst muligt og sørge for, at de råder over de rette it-kompetencer og partnerskaber. De skal også fortsat tage hensyn til ESG og bæredygtighed, selv om det i hvert fald for en stund ikke prioriteres så højt som tidligere. Samtidig skal virksomhederne forholde sig til, hvordan de integrerer AI og udnytter andre nye teknologier bedst muligt.

Vores seneste undersøgelse viser imidlertid, at danske virksomheder generelt føler sig godt rustet til fremtiden – og i højere grad end sidste gang, vi spurgte dem. Især de store og mellemstore virksomheder mener, at de står et godt sted. 78% af de store virksomheder oplever, at de i høj grad eller meget høj grad er godt klædt på til de næste to år. Mod henholdsvis 74% i 2024 og 60% i 2023.

80% af de mellemstore føler sig godt rustet til de næste to år, mens det kun var 68% i 2025 og 47% i 2024. De små virksomheder er knap så optimistiske, men 56% er stadig positive, når de ser fremad. Det var tilfældet for 58% af de små i 2025 og 42% i 2024.

Undersøgelsen understreger paradoksalt nok også, at virksomhederne i stigende grad oplever, at det er svært at følge med. Under hver fjerde danske virksomhed har en fuldt implementeret plan i tilfælde af cyberangreb, og der er en øget bekymring for at blive ramt. Særligt blandt store virksomheder, hvor 2 ud af 3 i høj eller meget høj grad er bekymrede for cyberkriminalitet. Man er altså opmærksom på truslerne og udfordringerne, men det kan ikke dæmpe den voksende tro på fremtiden.

Føler sig i høj eller meget høj grad rustet til fremtiden



Det lyse fremtidssyn kan skyldes, at danskerne generelt har en positiv tilgang til verden. Vi stoler på hinanden og har stor tillid til samarbejdspartnere og it-leverandører, for vi går ud fra, at de har styr på det. Så selv om der sker flere og flere cyberangreb, der medfører høje omkostninger, er der givetvis også en følelse af, at ”det går jo nok”. Det gør det jo også – altså indtil det ikke gør. Og den danske optimisme kan betyde, at truslen fra it-kriminalitet ikke tages alvorligt nok.

Gør optimismen til virkelighed

Optimisme uden grobund er dog ikke en god strategi i forhold til de udfordringer, som virksomhederne står over for i dag, og de vil sandsynligvis kun blive mere udtalte i takt med, at digitaliseringen tager til, og AI for alvor implementeres. Af både virksomheder, offentlige institutioner og it-kriminelle. Det vil stille nye krav til it-sikkerheden, og samtidig vil et område som misinformation også spille en større rolle.

Undersøgelsen viser, at det endnu ikke er noget, der får stor opmærksomhed i erhvervslivet. Kun omkring 30% af de mellemstore og store virksomheder er bekymrede for at møde eller sprede misinformation. For de små virksomheders vedkommende er tallet helt nede på 18%.

Misinformation anses muligvis som et overordnet samfundsproblem og ikke noget, som virksomheder skal forholde sig til. Men med tiden vil vi givetvis se flere eksempler på, at misinformation indgår som et element i hybridtrusler. F.eks. kombineret med cyberangreb, der skaber usikkerhed om driften eller skader tilliden til virksomheden.

Den udfordrende og mere komplekse virkelighed, som danske virksomheder står over for, kræver, at der tænkes endnu mere strategisk og sammenhængende i forhold til it-sikkerhed, digitalisering og AI.

I takt med at jeres udfordringer som virksomhed flyder sammen, skal løsningerne også gøre det. De skal tage udgangspunkt i den øverste ledelse, så den digitale udvikling forankres rigtigt og med de rette it-partnere. På den måde kan jeres virksomhed investere klogest og mest effektivt. Så I får en løsning, der giver jer optimale kort på hånden i forhold til at skabe vækst i forretningen – samtidig med, at I sikres bedst muligt mod it-kriminalitet. Så jeres virkelighed kan efterleve den store optimisme, der opleves blandt danske virksomheder.

Under hver fjerde danske virksomhed har en fuldt implementeret plan i tilfælde af cyberangreb, men 2 ud af 3 store virksomheder er bekymrede for cyberkriminalitet.

Om undersøgelsen

300 C-level medarbejdere (CEO, CFO, CIO) på tværs af brancher og virksomhedsstørrelser i Danmark har deltaget i markedsundersøgelsen foretaget af Ipsos på vegne af TDC Erhverv. Undersøgelsen er gennemført i november 2025 via telefoninterviews på tværs af brancher og virksomhedsstørrelser (små med 2-50 medarbejdere, mellemstore med 51-249 og store med 250+ ansatte). Respondenterne har delt deres syn på deres parathed i forhold til den digitale fremtid og den trussel, som et mangelfuldt it-sikkerhedssystem kan medføre.

Om TDC Erhverv

At være rustet til fremtiden kræver viden og teknologi. TDC Erhverv tilbyder en bred vifte af rådgivning, services og løsninger inden for digitalisering og it-sikkerhed. Uanset størrelse, branche og kompleksitet kan vi hjælpe jeres virksomhed med at udnytte de mange digitale muligheder. Så I kan arbejde smartere og med ro i maven. Og når jeres ambitioner og behov vokser, kan vores løsninger vokse med jer, så jeres virksomhed altid er klar til i morgen.

www.tdc.dk

