

Er jeres virksomhed
klar til i morgen?

2025

Executive Summary

I en mørk og usikker tid ser danske virksomheder stadig **lyst på fremtiden**

Det seneste år har været udfordrende for danske virksomheder og vores samfund generelt. Ikke desto mindre understreger dette års undersøgelse foretaget i slutningen af 2024 af det internationale analyseinstitut Ipsos på vegne af TDC Erhverv, at danske virksomheder fortsat har stor tiltro til fremtiden. Men er vi for optimistiske?

Geopolitiske stridigheder i flere dele af verden og et amerikansk valg, der har kastet mange bolde op i luften, har skabt generel usikkerhed, mens stigende omkostninger, mangel på kvalificeret arbejdskraft og et lavere forbrug har medvirket til at udfordre danske virksomheders drift.

For andet år i træk stiller TDC Erhverv skarpt på den digitale udvikling hos de danske virksomheder og undersøger deres parathed inden for områder som digitalisering, fremtidens krav og den trussel, som mangelfuld it-sikkerhed kan medføre.

Den gode nyhed er, at på trods af udfordringerne føler de fleste virksomheder sig rustede til fremtiden – i endnu højere grad end for et år siden, hvor

TDC Erhverv og Ipsos for første gang undersøgte danske virksomheders it-parathed på den korte og den lange bane. Andelen af virksomheder, der føler sig godt klædt på, er steget med 16%, og blandt store virksomheder føler 3 ud af 4 sig i høj eller meget høj grad klar på fremtiden. Det skal bemærkes, at denne rapport er udgivet i marts 2025. Var undersøgelsen foretaget i dag, ville optimismen nok være knap så markant.

Digitale udfordringer

Undersøgelsen peger dog også på en række udfordringer, som i en vis grad modsiger den store optimisme. 8 ud af 10 virksomheder – lige så mange som sidste år – oplever, at det er svært at følge med den digitale udvikling. Kun lidt over halvdelen af de adspurgte virksomheder betegner sig selv som fuldt digitaliserede, og man kæmper bl.a. med at finde tid, penge og de rette kompetencer til at skrue op for digitaliseringen.

Danske virksomheder er ligeledes udfordret på it-sikkerheden. Flere og flere udsættes for cyberkriminalitet, og de økonomiske kon-

sekvenser er enorme. Afhængig af virksomhedens størrelse vurderes et cyberangreb at koste virksomheden mellem 47.000 kr. og 200.000 kr. om dagen.

Alligevel har kun 1 ud af 5 virksomheder en fuldt implementeret plan, hvor alle medarbejdere ved, hvad de skal gøre i tilfælde af angreb. Og selv om der generelt er fokus på it-sikkerhed i virksomhederne, lægger særligt de små og mellemstore for få penge og for lidt handling bag ordene. Det er naturligvis en udfordring set med sikkerhedsbrillerne på. Men de manglende investeringer i it-sikkerhed og digitalisering er kritiske, for det er samtidig investeringer i vækst og nye muligheder for innovation, effektivisering og vækstskabelse i Danmark. Til glæde for jeres virksomhed, samfundet og borgere.

I denne rapport tager vi temperaturen på små, mellemstore og store danske virksomheders syn på it-sikkerhed, digitalisering og kunstig intelligens. I forhold til hvor meget det fylder i dag, og hvad virksomhederne vil prioritere højest i fremtiden.

I forhold til 2023 er andelen af virksomheder, der føler sig godt klædt på til fremtiden, steget med

16%

It-sikkerhed

Når truslen stiger, skal it-sikkerheden følge med

Selvom danske virksomheder i stigende grad udsættes for it-angreb, og relativt få organisationer har en fuldt implementeret plan, føler virksomhederne sig godt sikret mod cyberkriminalitet. Måske lidt for godt?

Siden sidste år er truslen mod det danske samfund og vores virksomheder desværre kun steget. Den sikkerhedspolitiske situation og konkurrencen mellem stater smitter også af på cyberområdet, og danske virksomheder er af flere grunde fortsat attraktive mål for it-kriminelle. TDC Erhverv Sikkerhedsrapporten 2024 viser således, at antallet af blokeringer af ondsindede domæner med Internetfilter steg fra omkring 10 millioner i 2023 til over 27 millioner i 2024.

Den markante stigning peger på, at mobilkunder ikke er undtaget fra de digitale trusler, og det derfor er vigtigt, at vi er på vagt, uanset hvilket device vi benytter, og hvor vi logger på.

Hackerne udvikler hele tiden nye metoder, og cybertruslen er blevet et grundvilkår, som alle

virksomheder, medarbejdere, offentlige institutioner og borgere i Danmark er nødt til at leve med. Det opleves tydeligt i mediebildet, hvor historier om cyberangreb og nedbrud fylder spalterne med hyppigere mellemrum. Det betyder også, at der stilles stigende krav til virksomhedens beskyttelse af systemer, netværk og data mod bl.a. phishing-angreb, malware, ransomware, finansiell svindel, tyveri af data og DDoS-angreb.

Ikke længere et spørgsmål 'om', men 'hvornår?'

Ifølge Ministeriet for Samfundssikkerhed og Beredskab (CFCBS) vurderes truslen fra cyberkriminalitet og it-angreb mod danske virksomheder og organisationer fortsat som værende meget høj. Det anses således som meget sandsynligt, at danske myndigheder og virksomheder vil blive ramt af cyberkriminalitet inden for de næste to år.^[1]

Alle typer organisationer og virksomheder kan blive ramt, uanset branche og størrelse. Små

^[1] Cybertruslen mod Danmark, side 12.



og mellemstore virksomheder er typisk interessante for hackerne, fordi it-sikkerheden her ofte er mere mangelfuld og derfor lettere at bryde, og fordi mindre virksomheder ofte benyttes som indgang til større organisationer. Mens de store virksomheder er på lystavlen hos it-kriminelle, fordi de her har mulighed for at sikre sig et stort udbytte, hvis de først får adgang til it-systemer eller data.

Tusindvis af potentielle angreb hver dag

TDC Erhverv Sikkerhedsrapport 2024 viser, at der i 2024 blev foretaget 27.198.791 blokeringer af besøg på ondsindede domæner med Internetfilter. I gennemsnit over 70.000 blokeringer om dagen.

Den seneste undersøgelse foretaget af Ipsos understreger således også, at en stor del af de adspurgte danske virksomheder har været udsat for cyberkriminalitet i løbet af de seneste fem år. De store virksomheder har været mest udsatte. Her har mere end hver tredje virksomhed været ramt, og halvdelen af disse angreb er sket inden for de seneste år. Hvilket er med til at understrege den stigende risiko.

De små og mellemstore virksomheder har ligeledes været udsatte. 17% af de små har oplevet cyberangreb, mens 23% af de mellemstore organisationer har været ramt af it-kriminalitet – og knap 1/10 af denne gruppe virksomheder har oplevet mere end ét angreb de seneste fem år.

Angrebene kan ske på flere måder. Blandt de hyppigste er ransomware-angreb, hvor it-kriminelle får adgang og herefter krypterer virksomheders data og it-systemer. Herefter kræver hackerne en løsesum for at gøre de krypterede data eller systemer tilgængelig igen. De it-kriminelle kan ligeledes true med at lække eller sælge de stjålne data, hvis organisationen ikke betaler løsesummen.^[2]

Rammer økonomien på flere måder

Cyberangreb kan altså ramme virksomhedernes økonomi på flere fronter. Dels kan hackerne kræve en betragtelig løsesum for at give adgang til eller undlade at frigive data. Men typisk repræsenterer det faktisk den mindste udgift. Tidligere undersøgelser peger således på, at de samlede udgifter ved et ransomware-angreb er mere end syv gange højere end den gennemsnitlige løsesum.^[3]

Det gælder blandt andet udgifter som følge af tabt indtjening og nedetid i produktionen samt udgifter til f.eks. advokatsalærer, eksterne konsulenter og overvågning. Samtidig er der naturligvis også en stor udgift forbundet med at genoprette systemer og drift efter et angreb.

[2] <https://www.europarl.europa.eu/topics/da/article/20220120STO21428/cybersikkerhed-de-vigtigste-og-storste-trusler>

[3] <https://www.version2.dk/artikel/ny-rapport-loesesum-men-udgoer-kun-15-procent-af-udgifter-ved-ransomware-angreb>

Mere end hver tredje store virksomhed har været udsat for cyberkriminalitet i løbet af de seneste fem år

29.903

virksomheder udsat for cyberangreb

17% af små virksomheder i vores undersøgelse har været udsat for cyberangreb. Hvis det er tilfældet med alle Danmarks omkring 175.900^[5] små virksomheder (1-49 ansatte), svarer det til 29.903 angrebne virksomheder*.

Endeligt kan et it-angreb medføre stor skade på virksomhedens troværdighed og omdømme overfor kunder, borgere og samarbejdspartnere, hvis deres data lækkes. Hvilket igen kan medføre en nedgang i ordrer og på den måde ramme virksomhedens økonomi på den længere bane.

Bevidste om store omkostninger

De adspurgte virksomheder i undersøgelsen er generelt bevidste om de økonomiske konsekvenser ved et eventuelt cyberangreb. De store virksomheders estimat er mere end fire gange så højt som de mindste virksomheders estimat. De store virksomheder vurderer således, at hvis deres it-systemer og procedurer lukkede ned som følge af et angreb, ville det koste dem mindst 200.000 kr. pr. dag. Det tal kan endda være underestimeret, da over en tredjedel af de adspurgte store virksomheder forventer en omkostning ved angreb på over 250.000 kr. om dagen.

Med afsæt i at 38% af store virksomheder i undersøgelsen har været udsat for cyberangreb de seneste fem år, og der findes omkring 900 store virksomheder (+250 ansatte) i Danmark, svarer det til 342 angrebne virksomheder. Hvis de 38% altså gælder for alle store virksomheder herhjemme. Antager man noget naivt, at angrebene kun varer en enkelt dag, er det altså en umiddelbar omkostning på over 68 mio. kr. Undersøgelser peger dog på, at nordiske virksomheder i snit bruger over 300 dage på

at håndtere et cyberangreb, og så hedder den samlede udgift svimlende 20,5 mia. kr. – eller 60 mio. kr. per angreb på en stor virksomhed.^[4]

Når det gælder små og mellemstore virksomheder, vurderes de daglige omkostninger ved et cyberangreb til at være henholdsvis 47.000 kr. og 140.000 kr. Der findes omkring 175.900 små virksomheder i Danmark med mellem 1 og 49 ansatte.^[5] Hvis 17% af dem har oplevet cyberangreb inden for de seneste fem år, som det er tilfældet i vores undersøgelse, svarer det til 29.903 virksomheder udsat for. Så best case – hvor intet angreb varer mere end en dag – er det en estimeret omkostning på over 1,4 mia. kr. Eller 1,4 mio. kr. for et enkelt angreb, der varer en måned*.

[4] www.computerworld.dk/art/277667/hackerangreb-koster-i-gennemsnit-de-ramte-virksomheder-16-5-millioner-kroner

[5] www.dst.dk/da/Statistik/emner/erhvervsliv/erhvervslivets-struktur/firmaer-og-koncerner

* Beregningen af det samlede antal angreb forudsætter, at de 17% små virksomheder, der har oplevet angreb, gælder alle danske virksomheder med 1-49 ansatte.

De store virksomheder vurderer således, at hvis deres it-systemer og procedurer lukkede ned som følge af et angreb, ville det koste dem mindst 200.000 kr. pr. dag.



Behov for beredskabsplan

I takt med at risikoen for cyberangreb er stigende, og it-kriminelle hele tiden udvikler nye teknikker og metoder at angribe virksomheder på, er det vigtigt, at virksomheder arbejder proaktivt i forhold til it-sikkerheden og tænker den ind i it-infrastrukturen og den daglige drift.

Jo hurtigere virksomheden kan få angrebet bremsset og dæmmet op for skader, jo bedre. Men det kræver mange overvejelser og beslutninger.

Derfor er det vigtigt med en klar beredskabsplan, så man ikke skal forholde sig til for meget eller tage for mange vigtige beslutninger, når først skaden er sket.

Samme beredskabsniveau

Trods stigende risiko for cyberangreb og det generelt høje trusselsniveau er der i seneste undersøgelse færre virksomheder (77%), der har en plan for, hvad de skal gøre, hvis de bliver udsat for cyberkriminalitet end sidste år, hvor andelen lå på 82%.

Ser man på virksomheder med en fuldt implementeret plan i tilfælde af angreb er dette års tal nogenlunde på niveau med sidste år. Der er fortsat kun knap 1 ud af 5 adspurgte virksomheder, der har en plan, hvor alle medarbejdere ved, hvad de skal gøre, hvis virksomheden angribes. Et meget lavt tal set i lyset af, at de danske virksomheder som tidligere nævnt er opmærksomme på de økonomiske konsekvenser ved et cyberangreb.

Det er også bekymrende i forhold til, at phishing fortsat er blandt hackernes mest udbredte metoder, da det er effektivt og nemt at udføre. Ved phishing forsøger it-kriminelle at narre mailmodtagere til at videregive personlige eller andre kritiske oplysninger eller give uretmæssig adgang til it-systemer. På den måde kan det blive den indledende adgang til et ransomware-angreb. Ifølge TDC Erhvervs sikkerhedsrapport fra 2024 var 15% af angrebene i det år phishing-angreb.

Derfor er det vigtigt, at alle medarbejdere er opmærksomme på risikoen og overholder de foreskrevne sikkerhedsprocedurer for overførsler og betalinger i virksomheden. Det er også nødvendigt i forhold til at leve op til det europæiske NIS2-direktiv om cybersikkerhed og risikostyring, der bl.a. omfatter virksomheder indenfor energi, transport, bank og finans, sundhedssektoren, digital infrastruktur og offentlige myndigheder. NIS2 skærper bl.a. kravene i forhold til, at virksomheder og organisationer skal have en dokumenteret beredskabsplan for at håndtere cybertrusler og -angreb.

Fokus på it-sikkerheden

It-sikkerheden fylder meget hos især de større danske virksomheder. Det kan skyldes, at eventuelle cyberangreb rammer økonomien hårdere, jo større virksomheden er. Omvendt rammes små forretninger tilsvarende hårdt målt i forhold til deres omsætning. Til gengæld er der muligvis et større fokus på it-sikkerhed hos de

98%

af de store virksomheder har allerede investeret i it-sikkerhed – en stigning i forhold til 2023. Men knap halvdelen mener, at der er plads til at forbedre sikkerhedsprocesser

store, fordi digitaliseringen generelt fylder mere. 58% af de store virksomheder har stort fokus på digitalisering mod kun 35% af de små. I forlængelser heraf er det kun naturligt, at it-sikkerhed også fylder mere i bevidstheden.

Hos 70% af de adspurgte virksomheder er it-sikkerhed et fast punkt på dagsordenen hos den øverste ledelse, en stigning på 7% i forhold til undersøgelsen 2023. 45% af de store virksomheder har it-sikkerhed som et fokusområde og 87% har det kontinuerligt på dagsordenen. Som beskrevet tidligere er det sikkerhedsmæssige fokus dog ikke strømmet ned gennem organisationen, for færre end sidste år har en plan i tilfælde af cyberkriminalitet. Set i lyset af, at mange angreb sker via phishing hos medarbejdere, er det et problem, hvis kun ledelsen er opmærksomme på de sikkerhedsmæssige udfordringer.

Plads til forbedringer

En ting er at være opmærksom på de stigende sikkerhedsudfordringer, noget andet er at gøre noget ved dem. Undersøgelsen understreger, at der kan være et stykke vej fra tanke til handling, og at det stadig halter med at få ført de gode intentioner ud i livet.

Omkring 1 ud af 3 af virksomhederne på tværs ser således større potentiale for at forbedre deres processer, når det gælder datasikkerhed. Og knap halvdelen af de store virksomheder mener, at der er plads til at forbedre virksom-

hedens sikkerhedsprocesser.

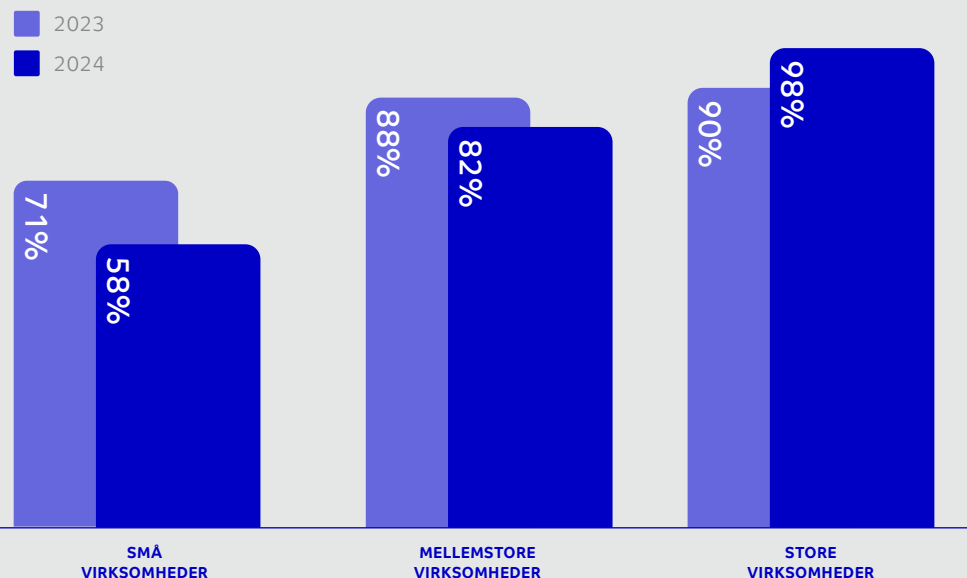
Til trods for det har 98% af de store virksomheder allerede investeret i it-sikkerhed – en stigning i forhold til 2023. Det er også værd at bemærke, at en lige så høj andel forventer at investere endnu mere i fremtiden. De store virksomheder i Danmark er altså bevidste om, at de bliver nødt til at investere i it-sikkerhed, og de er også klar på at bruge penge fremadrettet.

Til gengæld har de mindre virksomheder ikke i samme grad øjnene rettet mod at forbedre sikkerheden. 58% af de små og 82% af de mellemstore virksomheder har investeret i it-sikkerheden f.eks. i form af udstyr til hybridarbejde, VPN-forbindelser og firewalls. Begge disse tal viser et lille fald i forhold til sidste års undersøgelse.

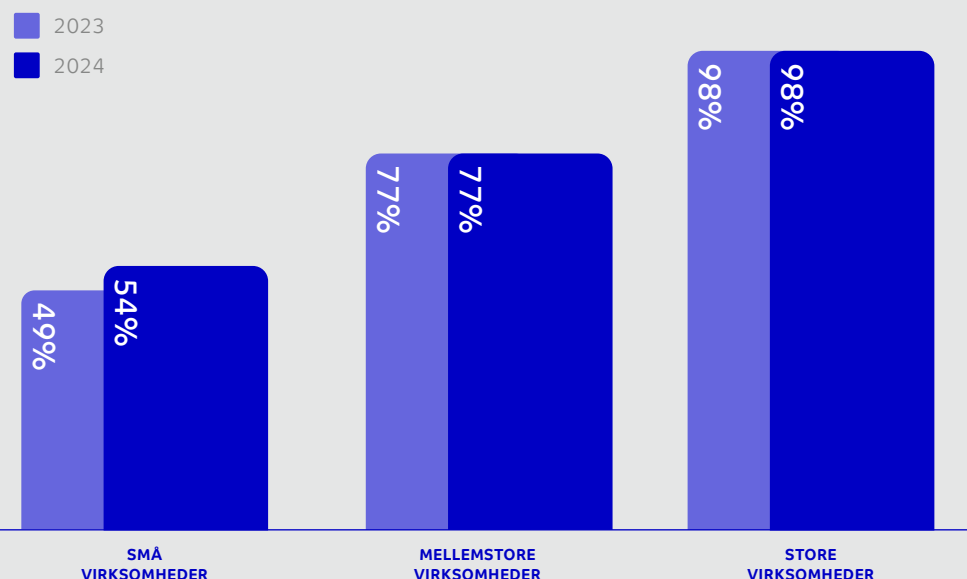
Hos 70% af de adspurgte virksomheder er it-sikkerhed et fast punkt på dagsordenen hos den øverste ledelse

Det samme gør sig gældende, når de små og mellemstore virksomheder kigger fremad. Kun henholdsvis lidt over halvdelen og 3 ud af 4 virksomheder forventer at investere i it-sikkerhed de kommende år – og langt færre forventer at foretage større investeringer.

Har investeret i it-sikkerhed det seneste år



Forventer at investere i it-sikkerhed de kommende år



En interessant kontrast til de små og mellemstore virksomheders bekymringer for at blive udsat for cyberkriminalitet. Henholdsvis 24% og 40% af de adspurgte virksomheder er nervøse for it-angreb.

Vi skal have alle virksomheder med

Det er en stor udfordring, at de små og mellemstore virksomheder halter efter, når det gælder it-sikkerhed. Men det er også forståeligt, at mindre forretninger i højere grad har øjnene rettet mod daglig drift, samarbejdspartnere og overholdelse af lovkrav. Det er ikke desto mindre en udfordring, for cyberkriminalitet rammer generelt bredt, og ingen organisation kan være for lille til at vide sig sikker.

Cyberkriminelle har i stigende grad rettet sig mod mindre virksomheder, som ofte har færre sikkerhedsforanstaltninger og ressourcer til rådighed til at beskytte sig. Men som tidligere tal viser, kan et angreb mod en mindre virksomhed hurtigt koste 1 mio. kr., hvis der strækker sig over 3-4 uger. Og det kan have fatale konsekvenser for den videre drift.

Tal viser imidlertid, at antallet af anmeldte hackerangreb mod små og mellemstore virksomheder steg med 64% fra 2021 til 2022,^[6] og det er ikke noget, der tyder på, at det tal vil falde fremover, tværtimod. Alligevel vurderer Digitaliserings- og Ligestillingsministeriet, at lidt over hver tredje af de små eller mellemstore

virksomheder i Danmark ikke har et tilstrækkeligt sikkerhedsniveau.^[7] Det er ikke blot kritisk for de små virksomheder. Men også en trussel mod de store virksomheder, som de små er leverandører til, og som derfor også risikerer at blive ramt af et angreb.

Investeringer fører til flere investeringer

Vores undersøgelse peger på, at de virksomheder, der vælger at bruge penge på it-sikkerhed, oplever, at de får værdi for pengene. I hvert fald forventer omkring 4 ud af 5 små og mellemstore virksomheder, der allerede har investeret i it-sikkerhed, at investere endnu mere. Mens 75% af de små virksomheder, der endnu ikke har investeret, heller ikke har planer om at gøre det fremadrettet. En høj andel set ud fra den stigende trussel og de økonomiske konsekvenser, som et cyberangreb kan medføre også for små virksomheder. Hvis omkostningen ved et cyberangreb på små virksomheder som tidligere nævnt vurderes til at ligge på 47.000 kr. pr. dag, kan man stille spørgsmålstejn ved, hvor mange og hvor lange angreb, man kan overleve, før pengeskassen er tom.

[6] SMV Danmark Temaanalyse: Antallet af anmeldte hackerangreb slår rekord.

[7] Redegørelse om Danmarks Digitale Udvikling 2024, side 9.

De små virksomheders manglende villighed til at bruge penge på it-sikkerhed er også paradoksalt set i lyset af, at 55% af dem har it-sikkerhed som et fast punkt på dagsordenen hos den øverste ledelse – en markant stigning i forhold til sidste års 37%.

Men når først virksomheder vælger at bruge en del af budgettet på it-sikkerhed, tyder det altså på, at organisationerne får øjnene op for fordelene og ønsker at investere endnu mere i it-sikkerhed. Af den grund er det også vigtigt at få de små og mellemstore virksomheder med på sikkerhedsvognen.

Sikker men også bekymret

Hvordan ser det så ud, hvis man kigger på sikkerhedsfølelsen og hvor godt, virksomheds-ejerne sover om natten? Generelt føler virksomhederne sig sikret mod cyberkriminalitet. 2 ud 3 virksomheder føler sig i høj grad eller i meget høj grad sikret, og det fordeler sig nogenlunde jævnt på tværs af størrelse. Som det i øvrigt også var tilfældet i sidste års undersøgelse.

Ligesom sidste år er virksomhederne dog også relativt bekymrede for it-kriminalitet. De små virksomheder er mindst bekymrede (24%), men de store virksomheder topper. Her er 55% af de adspurgte virksomheder i høj eller meget høj grad bekymret for cyberkriminalitet. Det kan virke paradoksalt, da store virksomheder

investerer klart mest i it-sikkerhed og har størst ledelsesmæssigt fokus på det. Omvendt er det også de store organisationer, der er mest økonomisk udsatte i forbindelse med cyberangreb. I det lys er det naturligt, at de store virksomheder bekymrer sig mest.

Danske virksomheders tillid har brug for et reality check

Konklusionen er, at der er stort fokus på it-sikkerhed i dansk erhvervsliv, og der er generelt en villighed til at investere også i sikkerheden. Men der investeres ikke nok. Særligt de små og mellemstore virksomheder halser efter, og det kan skyldes flere ting.

Dels er vi en nation præget af høj tillid og stor optimisme. Vi stoler på vores kollegaer og hinanden, og vi har stor tillid til de mange digitale løsninger, der er med til at gøre vores hverdag lettere og styrke samarbejdet mellem virksomhederne. Tilliden er altså på mange områder en stor fordel, men i denne sammenhæng kan det også forhindre virksomheder i at tage truslen fra cyberangreb alvorligt nok. Selv om alt peger på, at mindre virksomheder i stigende grad er udsatte, og et angreb kan få store konsekvenser for en organisation, der ikke har tilstrækkeligt med ressourcer eller midler i ryggen til at modstå angreb.



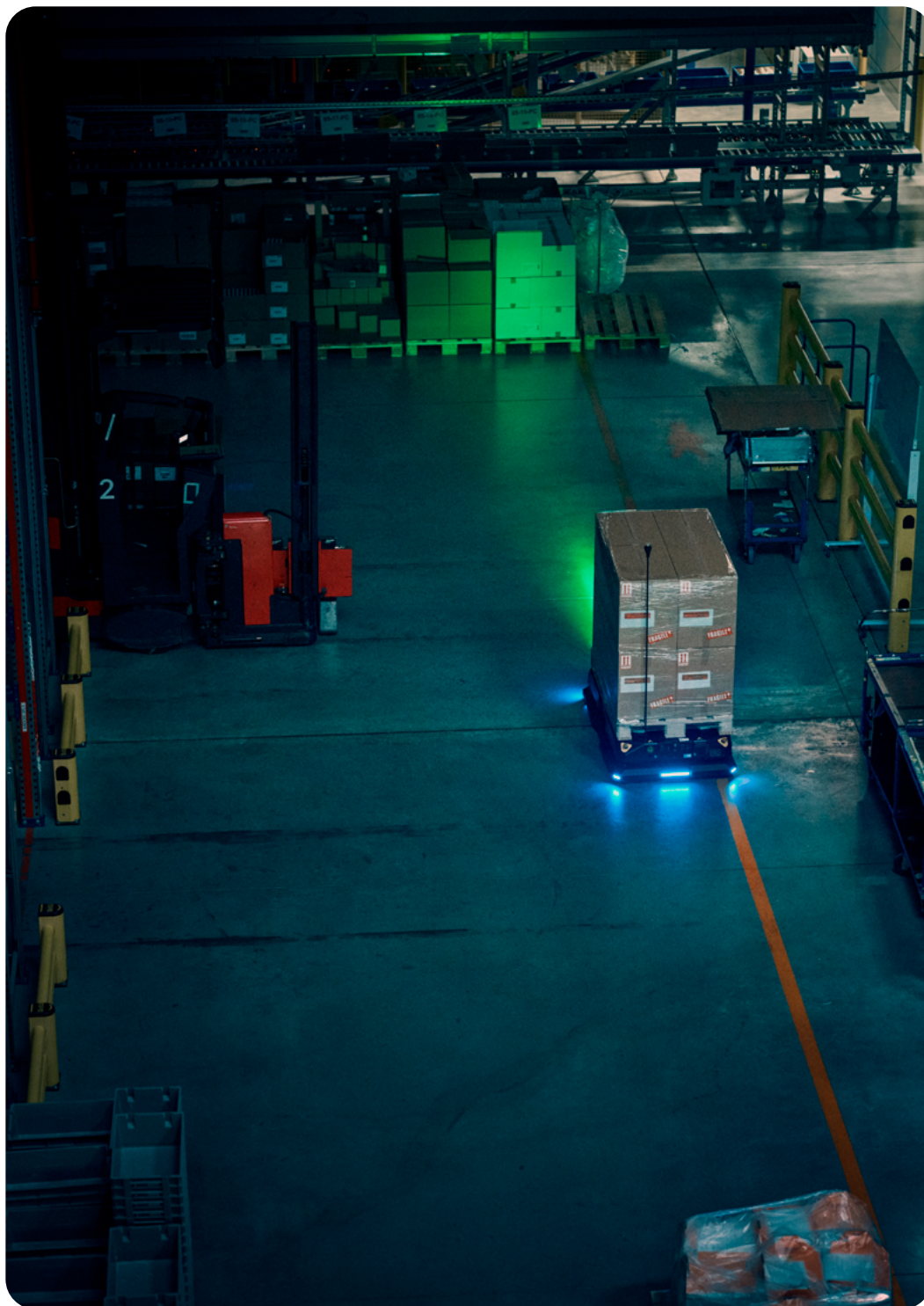
Mindre virksomheders manglende investeringer i it-sikkerhed kan også skyldes andre faktorer. Dels er det forståeligt, at små og mellemstore virksomheder har fokus på den korte bane og driften her og nu. Ingen af de små eller mellemstore virksomheder i undersøgelsen har således it-sikkerhed på top 3 over fokusområder i den nærmeste fremtid.

Samtidig kan manglende investeringer også skyldes, at mindre virksomheder har sværere ved at forstå, hvordan de skal gribe sikkerhedsspørgsmålet an. Det er vigtigt, at man har en overordnet og sammenhængende tilgang, så investeringerne i it-sikkerhed anvendes effektivt. På den måde undgår virksomheder at bruge penge på sikkerhedsløsninger, der ikke hænger sammen, kan øge kompleksiteten i it-miljøet og føre til højere omkostninger, både hvad angår indkøb og vedligeholdelse af løsninger samt krav til medarbejdertræning.

Fokus eller ej, så understreger undersøgelsen ikke desto mindre, hvor vigtigt det er at have styr på it-sikkerheden. Dels i forhold til at undgå udgifter ved cyberangreb, der vurderes at koste mellem 47.000 kr. og 200.000 kr. om dagen. Men ligeledes for at kunne leve op til aktuelle EU-direktiver som NIS2 og DORA, der har til formål at højne den generelle it-sikkerhed i hele Europa. At kunne efterleve disse EU-krav vil gardere virksomheder bedst muligt mod direkte angreb og stille dem i en fordelagtig position som samarbejdspartner med andre virksomheder.

For at tackle alle disse udfordringer er det essentielt for virksomheder at arbejde tæt sammen med rådgivere og sikkerhedsudbydere, der har en strategisk tilgang til it-sikkerhed. Det indebærer en grundig vurdering af virksomhedens samlede sikkerhedsbehov, udarbejdelse af en sammenhængende strategi for sikkerheden samt implementering af løsninger, der spiller sammen og på den måde beskytter virksomhedens digitale aktiver mod et bredt spektrum af trusler. Både på den korte og den lange bane.

Virksomheder
i undersøgelsen
vurderer, at et
cyberangreb
vil koste dem
mellem 47.000
og 200.000 kr.
om dagen.



Digitalisering

Digitalisering er **vejen** til **vækst** i erhvervslivet

Der er fortsat stort potentiale for øget digitalisering blandt danske virksomheder. Det er vigtigt, for digitaliseringen rummer mange muligheder for at styrke samarbejdet, løfte produktiviteten og præge udviklingen i Europa og resten af verden.

Uanset hvordan man vender og drejer det, så ligger Danmark med helt fremme, når det gælder digitalisering. Vi er kåret til verdensmestre i offentlig digitalisering fire gange i træk, og Danmark bliver bl.a. rost for sit stærke digitale lederskab og nationale digitaliseringsstrategi. Vi er ligeledes et af verdens mest digitaliserede lande, når det gælder digitale færdigheder blandt borgere, nethandel, internetadgang og brug af sociale medier.

Digitalisering åbner døren for både muligheder og usikkerheder

Set fra de danske virksomheders synspunkt befinder de sig i en tid med mange muligheder og lige så mange udfordringer, når det handler om digitalisering. Big data, kunstig intelligens,

hybridarbejde, it-sikkerhed og rekruttering er nogle af de vigtige ting, som virksomhederne skal forholde sig til.

Det er vigtigt, at de danske virksomheder øger digitaliseringen. Det vil give dansk erhvervsliv et stort løft, for digitaliseringen kan i høj grad være med til at effektivisere driften og medføre en lang række fordele på det globale marked. Omvendt vil øget digitalisering potentielt set også åbne døren for it-kriminelle og fremmede stater med onde bagtanker. Derfor er det vigtigt, at danske virksomheder digitaliseres på en rigtig og sikker måde.

En proces med udfordringer

Hvordan ser det så ud med digitaliseringen blandt de danske virksomheder? Overordnet set spiller digitaliseringen en vigtig rolle blandt virksomhederne, og knap halvdelen af organisationerne har stort fokus på digitalisering – med overvægt blandt de store virksomheder.

Andelen af virksomheder, der opfatter sig selv som lidt eller kun i nogen grad digitaliseret, er faldet i 2024 i forhold til året før. Henholdsvis fra 52% til 45% for små virksomheder, fra 41% til 40% for de mellemstore og fra 50% til 40%, når det gælder de store virksomheder. Til gengæld betegner kun mellem 55% og 61% af virksomhederne sig selv som fuldt digitaliseret eller i høj grad digitaliseret. Igen med de store virksomheder som topscorere.

Knap halvdelen af de adspurgte virksomheder erkender da også, at der er potentiale for øget digitalisering. Mens omkring lige så mange anser digitaliseringen som en proces. Virksomheder, der endnu ikke er fuldt digitaliserede, angiver netop den igangværende proces som en årsag sammen med manglende ressourcer. Man er altså i gang, men mangler tid og/eller de rette medarbejdere og kompetencer for at komme videre med digitaliseringen.

Endnu flere data i skyen

Et af de områder, hvor danske virksomheder virkelig har taget digitaliseringen til sig, er, når det gælder brugen af cloudtjenester og lagring af data i skyen. Det er en naturlig konsekvens af, at vi alle arbejder mere hjemmefra og er digitalt forbundet i alle led i virksomheden og på tværs af lokationer.

Omkring 9 ud af 10 virksomheder opbevarer data i skyen, og det er uanset virksomhedernes størrelse. I forhold til sidste års undersøgelse er

det desuden værd at bemærke, at virksomhederne generelt har fået større tillid til cloudtjenesterne. Hvor der sidste år var en tredjedel, der udtrykte bekymringer omkring opbevaring af data i skyen, er det i seneste undersøgelse kun 1 ud 5, der ikke har tillid til skyen.

Som følge af den stigende tillid, er det også kun naturligt, at flere danske virksomheder vælger at opbevare al data i skyen. Hvor 28% gjorde det i sidste års undersøgelse, er der i år mere end 40%, der lægger det hele i clouden. Den stigende tillid og øgede brug af skyen kan skyldes, at virksomhederne oplever at have fået adgang til bedre cloudløsninger eller i højere grad har vænnet sig til at bruge dem.

Cloud Act og dens betydning for danske virksomheder

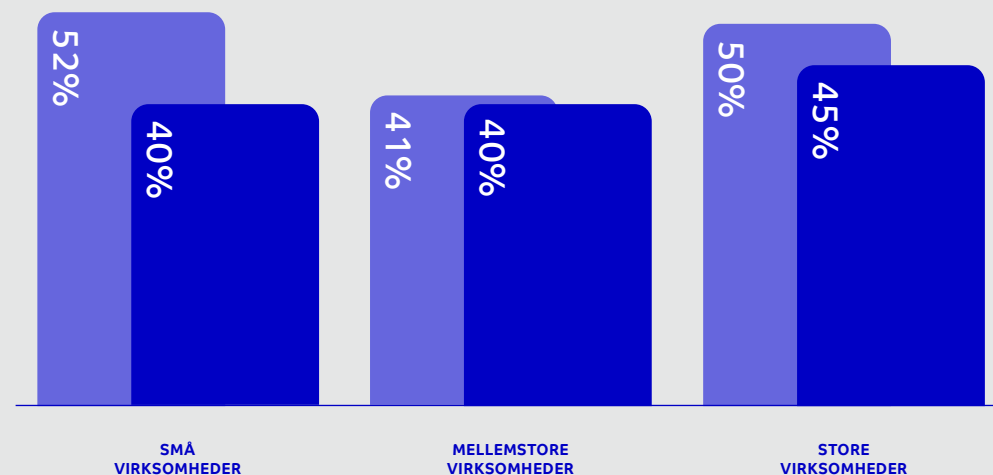
Du kender GDPR, men har du hørt om Cloud Act? I lyset af virksomhedernes forkærlighed for cloudtjenester og den politiske udvikling i USA bør danske virksomheder være opmærksomme på konsekvenserne ved den amerikanske lov, der blev vedtaget i 2018.

Cloud står i denne forbindelse for Clarifying Lawful Overseas Use of Data. I korte træk giver Cloud Act amerikanske myndigheder mulighed for at kræve adgang til data, som en amerikansk virksomhed har kontrol over, uanset hvor i verden disse data er lagret. Dette kan f.eks. ske i forbindelse med efterforskning af kriminalitet. Det betyder, at de amerikanske myndigheder

Virksomheder, der opfatter sig selv som lidt eller kun i nogen grad digitaliseret.

■ 2023

■ 2024



4 ud af 10 virksomheder har fokus på ESG og bæredygtighed, men under halvdelen af dem har direkte fokus på grøn omstilling og bæredygtighed.

kan bede om at få udleveret kundedata af amerikanske virksomheder, selv om serverne er placeret i Danmark.

Som nævnt har knap 90% af danske virksomheder dataopbevaring i skyen, og selv om din virksomheds data opbevares i skyen i Danmark eller inden for EU's grænser, omfattes disse data typisk også af Cloud Act, hvis du har købt tjenesten af en af de store internationale cloudtjenester. Så er det altså ikke den lokale lov, men den amerikanske Cloud Act, der er gældende. Hvilket igen kan være en udfordring i forhold til det, du lover dine kunder gennem de europæiske GDPR-regler, der stiller strenge krav til beskyttelse af persondata. Det kan ligeledes blive et problem, hvis en dansk virksomhed benytter AI-værktøjer, fordi disse tjenesters "træningsdata" kan inkludere følsomme eller personligt identificerbare data, der lagres eller behandles af det amerikanske selskab, og derfor også omfattes af den amerikanske Cloud Act.

Vil I sikre jeres virksomhed mod juridiske gråzoner i forbindelse med Cloud Act og GDPR? Så findes der heldigvis tekniske løsninger, der kan kryptere din virksomhedens data, så disse vigtige data holdes under lås og slå – også når de ligger i skyen.

Grøn it er stadig sort snak for mange

Et andet område, der er værd at rette blikket mod som virksomhed, er brugen af grøn it. Ligesom sidste år spiller ESG en vigtig rolle

for virksomhederne i undersøgelsen, og det er således et område, som mere end 4 ud af 10 virksomheder har fokus på de kommende år. Interessen for den grønne omstilling og et bæredygtigt it-setup synes at følge med virksomhedens størrelse, men generelt er der et bredt fokus på tværs af organisationer.

Alligevel er det påfaldende, at ESG og bæredygtighed efter mange virksomheders opfattelse ikke kædes sammen med at have 'et bæredygtigt it-setup'. Mellem 40 og 52% angav, at 'ESG og bæredygtighed (herunder grøn it)' var et fokusområde for virksomheden de næste par år. Men under halvdelen af disse virksomheder har direkte fokus på grøn omstilling og bæredygtigt it. Så selv om mange virksomheder tænker i bæredygtighed, er de altså endnu ikke nået til grøn it.

Det skyldes givetvis, at mange virksomheder stadig ikke er klar over, hvad grøn it helt konkret betyder, og hvilken forskel, det kan gøre for forretningen. De grønne intentioner og ambitioner er der, men bæredygtigt it er stadig, nå ja for grønt til, at virksomhederne for alvor har taget det til sig.

Hvad er grøn it?

Der er mange aspekter ved grøn it, men overordnet set handler det om at anvende teknologi på en måde, der er mere bæredygtig og miljøvenlig. Målet er at reducere energiforbruget og CO₂-udledningen fra teknologiske enheder

Grøn it er altså et bredt begreb, der dækker alt fra den hardware og software, som virksomheder bruger, til den måde, de organiserer deres it-infrastruktur på.

92% af de store organisationer mener, at en stærk it-infrastruktur er afgørende for fremtiden.

og systemer, samtidig med at man fremmer løsninger, der støtter op om en grønnere fremtid. Det kan f.eks. ske ved at anvende energieffektive computere, servere og datacentre og optimere software, så det ikke bruger mere energi, end det behøver. Mens forskellige AI- og IoT-løsninger kan hjælpe med at automatisk at slukke lyset og styre forbruget.

Grøn it handler også om cirkularitet af elektroniske produkter og f.eks. sørge for, at gamle enheder bliver genanvendt korrekt eller opgraderet i stedet for at blive smidt ud. Ligesom cloudløsninger er med til at sikre mere effektiv ressourceudnyttelse, da færre fysiske servere er nødvendige, og der derfor spares energi og plads.

Grøn it er altså et bredt begreb, der dækker alt fra den hardware og software, som virksomheder bruger, til den måde, de organiserer deres it-infrastruktur på. Det handler om at tænke på miljøet i alle faser af teknologibrug og -udvikling. Og selv om grøn it stadig er en udefinerbar størrelse for mange, vil det blive en naturlig del af virksomhedernes bæredygtige regnskab fremover. Både når det handler om den energi, som egne systemer og hardware forbruger, de tjenester man benytter sig af og de partnere, virksomhederne samarbejder med. Så den grønne omstilling ikke bliver et bump på vejen, men en hjælp i forhold til at skruer op for digitaliseringen.

Nøglen er en stærk infrastruktur

I forhold til digitaliseringen og de komplekse udfordringer, som de danske virksomheder står overfor, spiller it-infrastrukturen en nøglerolle. Det er mere end 7 ud af 10 virksomheder enige i, og hele 92% af de store organisationer mener, at en stærk it-infrastruktur er afgørende for fremtiden.

Undersøgelsen viser, at virksomhederne typisk samarbejder med mellem to og fem it-partnere, og virksomhedens størrelsen afspejles i antallet af it-partnere, benytter man. Jo større, jo flere partnere. Tallene understreger også, at jo større virksomhederne er, jo mere ser de fordel i at benytte få, stærke partnere, der kan hjælpe dem på tværs af it-sikkerhed, digitalisering og AI.

Man kan argumentere for, at færre it-partnere skaber bedre synergier på tværs af virksomheden. Det må også formodes at gøre det lettere for virksomheden at opretholde et ensartet sikkerhedsniveau på tværs af alle systemer og tjenester. Så der i mindre grad opstår svage led i kæden på grund af varierede sikkerhedsstandarder blandt forskellige partnere.

Samtidig gør færre partnere det lettere at overvåge og sikre, at sikkerhedspolitikker og standarder overholdes. Hvilket igen reducerer kompleksiteten i samarbejdet og mindsker risikoen for misforståelser eller sikkerhedsbrud. Færre adgangspunkter gør det nemmere at beskytte følsomme oplysninger.

50% af virksomhederne erkender, at de har svært ved at finde kompetente netværksarkitekter.

It-eksperter hænger ikke på træerne

En af de største barrierer for digitaliseringen er manglende ressourcer samt manglen på nødvendig ekspertise. I TDC Erhvervs rapport Managed netværksløsninger erkender 50% af virksomhederne, at de har svært ved at finde kompetente netværksarkitekter.*

Den stigende konkurrence om de bedste talenter har gjort det endnu sværere for små og mellemstore virksomheder at tiltrække de nødvendige ressourcer. Men den store efterspørgsel efter dygtige mennesker med digitale kompetencer vil sandsynligvis kun blive større i de kommende år, fordi vi ganske enkelt ikke uddanner nok kandidater inden for områder som ingeniørfagene, it og teknik til at kunne følge med udviklingen.

Kloge hoveder koster, men én ting er lønnen. Især mindre virksomheder vil også fremadrettet have svært ved at tilbyde et fagligt miljø, der er interessant og komplekst nok for at tiltrække og fastholde dygtige netværks- eller sikkerhedsspecialister. Derfor kan adgangen til den rigtige ekspertise nogle gange findes bedre gennem outsourcing, hvor udbyderne har bedre muligheder for at sætte de helt rigtige folk på snævre men komplekse it-udfordringer.

Ved at gå outsourcing-vejen kan virksomheden også tilpasse og skalere aftalen i takt med, at virksomheden vokser. Plus man er sikret en løsning, der følger med tiden og den teknologiske udvikling.

Svært at følge med

Generelt står virksomhederne overfor en lang række krav og udfordringer, hvor valget af it-partnere spiller en vigtig rolle. Det gælder f.eks. truslen fra cyberkriminalitet, integrering af AI og kontinuerlig opfølgning på nye regulativer og muligheder. Og virksomhederne oplever, at det er udfordrende at følge med. Der er flere og flere muligheder for at drage fordel af og udvikle forretningen gennem digitalisering, men mulighederne følges af ligeså mange reguleringer og usikkerheder.

Knap 8 ud af 10 virksomheder oplever, at det er svært at følge med i nye krav og muligheder, og især de mellemstore føler sig udfordret. Her oplever 84%, at det i nogen, høj eller meget høj grad er svært at følge med den digitale udvikling.

Disse tal understreger vigtigheden af at kunne tiltrække dygtige medarbejdere inden for it og vælge partnere, der kan hjælpe jeres virksomhed med at få overblik, prioritere indsatser og skræddersy en fremtidssikret løsning, der matcher netop jeres behov. På den korte og den lange bane.

For digitalisering er ikke et klart defineret projekt med en start- og en slutdato. Det er en proces i evig forandring og uden endeligt slutpunkt, og derfor bør det være et fast punkt på virksomhedens dagsorden.

* Rapporten er lavet af TDC Erhverv i samarbejde med Cisco. Den er baseret på en undersøgelse blandt beslutningstagere indenfor netværk og IT i store danske virksomheder (+250 ansatte) med fokus på bekymringer, økonomi, talent, sikkerhed og bæredygtighed i forhold til netværk.

AI

Kunstig intelligens er blevet en del af arbejdsdagen

Det giver ikke længere mening at diskutere, om man vil benytte AI i virksomheden, men i højere grad hvordan man gør bedst muligt.

I året, der er gået siden vores sidste undersøgelse, er der sket en enorm udvikling inden for kunstig intelligens. Endnu flere og bedre løsninger er blevet lanceret, flere og flere bruger dem på arbejdspladsen og derhjemme, og kunstig intelligens fylder langt mere i den offentlige debat. For mulighederne er nærmest uendelige. Inden for sundhedsvæsenet bruges AI bl.a. til at diagnosticere patienter og vurdere behandlingsformer. På sigt kan kunstig intelligens hjælpe læger med at opdage kræft langt tidligere i forløbet. Mens private virksomheder kan bruge AI til alt fra produktudvikling til markeds- og risikoanalyser, rekruttering og driftsoptimering. En motor for vækst.

Samtidig er det tydeligt, at AI begynder at bryde ud af sin egen boble og ikke længere skal ses som et teknologisk tilvalg, men en vigtig og integreret del af den digitale udvikling. Kunstig

intelligens spiller allerede en voksende rolle i forhold til f.eks. it-sikkerhed, og på sigt giver det ikke mening at tale om digitalisering og AI som separate områder.

Vores undersøgelse viser da også en stigning i virksomheder, der forventer, at AI kommer til at spille en stor eller afgørende rolle fremadrettet. Fra knap 45% i sidste års rapport til over 50% på tværs af virksomheder. Med en klar tendens til, at store virksomheder har størst forventninger til AI. Her forventer 3 ud af 4 virksomheder, at AI får en betydende rolle.

Alle taler om AI – under 10% af virksomhederne bruger det fast

Til gengæld halter det en del med at føre de store forventninger ud i livet. Kun cirka 1 ud af 4 virksomheder siger, at de bruger AI i nogen grad. Og kun 7-8% bruger kunstig intelligens i høj eller meget høj grad. De store virksomheder fører an i brugen af AI, men alt i alt er det overraskende lave tal i forhold til, hvor mange forskellige AI-værktøjer, der efterhånden er

7-8%

Kun 7-8% bruger kunstig intelligens i høj eller meget høj grad.



lanceret, og ikke mindst den værdi, vækst og effektivisering, som brugen af AI kan skabe for virksomheder. Tilbageholdenheden kan skyldes en kombination af manglende overblik over mulighederne i forhold til virksomhedens virkelighed og branche samt manglende ressourcer og kompetencer. Nogle af de udfordringer, som virksomhederne også fremhæver i forhold til digitaliseringen generelt.

En hjælpende hånd, der gør (arbejds)livet lettere

De overordnede økonomiske gevinster gennem effektivisering og automatisering er naturligvis et vigtigt aspekt ved AI. Men kunstig intelligens har også stort potentiale i forhold til at gøre hverdagen lettere for den enkelte medarbejder og skruer op for arbejdsglæden i virksomheden.

Først og fremmest kan kunstig intelligens håndtere en lang række krævende rutineopgaver og på den måde frigøre tid og ressourcer til mere komplekse og kreative opgaver, som kan bidrage til at øge produktiviteten og kvaliteten af arbejdet. Ved at optimere arbejdsprocesser, reducere fejl og øge effektiviteten kan AI ganske enkelt være med til at give medarbejdere en mere effektiv og tilfredsstillende arbejdsdag. Se det som en kollega, der kan klare mange af de faste opgaver i organisationen, der kræver meget tid og fylder meget i arbejdsdagen.

Måden virksomhederne benytter AI på varierer meget. I virksomheder med store kundeserviceafdelinger kan features som chatbots være med

til at optimere responstiden og arbejdsflowet, så tiden i stedet kan bruges på at yde hurtigere, personaliseret og proaktiv kundeservice, der gør kunderne glade. Mange kreative virksomheder inden for design og kommunikation udnytter derimod AI som både idéværktøj, inspirationskilde og kreativ sparringspartner, der f.eks. kan visualisere koncepter og ideer. Mens firmaer i byggebranchen benytter kunstig intelligens til at forbedre planlægning, effektivisere arbejdsstyrken og forudsige vedligeholdelsesbehov, hvilket igen øger produktiviteten og reducerer omkostningerne. AI-løsninger kan f.eks. også bruges til at give virksomheder i detailhandlen en hidtil uset indsigt i kunders præferencer og behov og på den baggrund skræddersy deres oplevelse.

Uanset hvilken branche jeres virksomhed arbejder i, er der helt sikkert også mulighed for at forbedre produktiviteten, opfindsomheden og arbejdsglæden ved hjælp af kunstig intelligens.

AI og grøn omstilling

I forhold til bæredygtighed og grøn omstilling kan AI også få en vigtig rolle. Som nævnt tidligere i denne rapport er brugen af AI-løsninger i dag forbundet med et relativt stort energiforbrug. På den anden side kan kunstig intelligens vise sig at være en gevinst for den grønne omstilling, fordi AI kan hjælpe med at optimere eksisterende, energikrævende systemer, og fordi det kan bidrage til forskning og udvikling i nye, grønne teknologier.

AI kan også bruges til at analysere og anvende store mængder data til at træffe beslutninger og forbedre energieffektiviteten, bl.a. gennem analyser af energimærkningsdata. Der er tale om enorme mængder data, der indsamles fra forskellige kilder som f.eks. satellitter, sensorer og internet of things (IoT)-enheder. En sådan omfattende brug af data gør det muligt at identificere mønstre og tilgange, der ellers ville være skjult for mennesker.

Men kunstig intelligens kan også revolutionere landbrug og fødevareproduktion og komme med kvalificerede forudsigelser om jordens knappe ressourcer. Desuden forventes det, at AI vil kunne muliggøre og accelerere anvendelsen af mange grønne teknologier, der endnu er under udvikling. Som f.eks. brintfremstilling via Power-to-X, superbatterier og grønt brændstof til fly. AI kan hjælpe os med at innovere og forberede os på fremtidige hændelser, og derfor vil den fortsatte udvikling af AI blive afgørende for vores mission om en mere bæredygtig fremtid for alle.

Til kamp med AI mod cyberangreb

Ligesom AI spiller en vigtig rolle i forhold til bæredygtighed og grøn omstilling, giver det også mening at tænke den ind i it-sikkerheden. Her er AI i virkeligheden et tveægget sværd. It-kriminelle kan bruge AI-værktøjer til at optimere deres angreb og blive bedre til at skabe mere overbevisende, men falsk kommunikation. Men lige så vigtigt kan AI også bruges til at optimere it-sikkerheden. AI kan f.eks. scanne software og

netværk for sårbarheder, simulere angreb til træning af medarbejdere, analysere e-mails og blokere skadelig trafik.

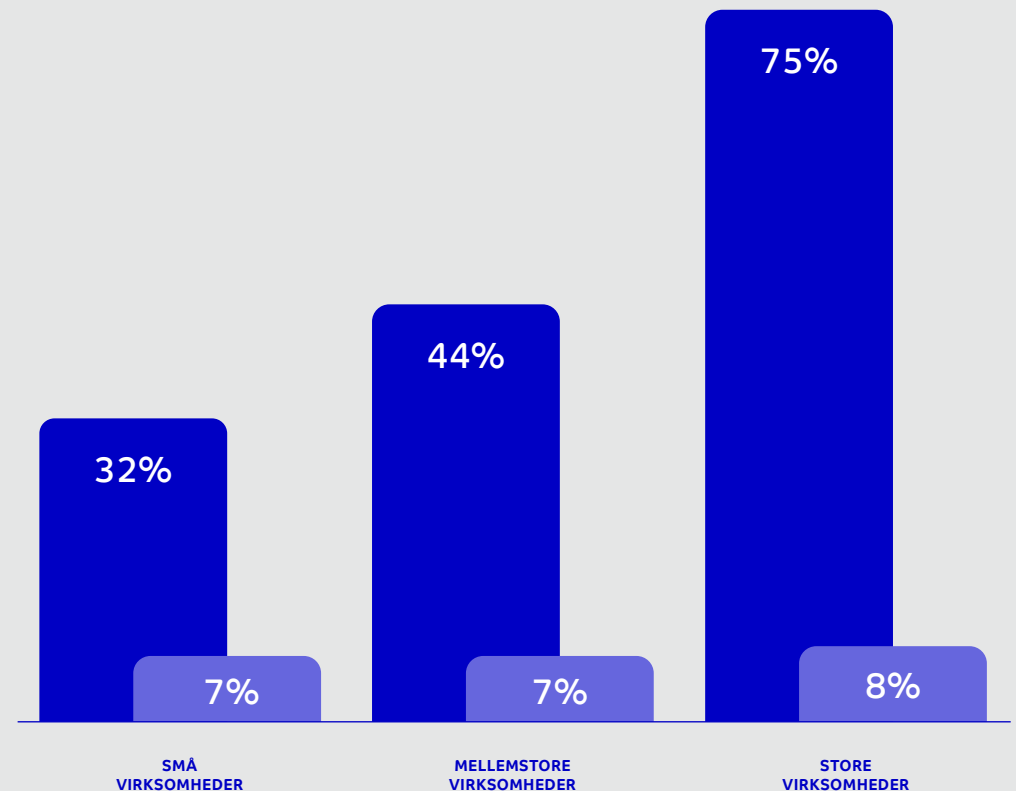
Dette er med til at understrege vigtigheden af at have en overordnet tilgang og se AI, digitalisering og it-sikkerhed som ét sammenhængende område.

Derfor er det vigtigt, at endnu flere danske virksomheder tager hul på brugen af AI og tænker det ind i digitaliseringen. Tag stilling til hvilket område, det giver bedst mening at starte med, og tal med jeres it-partner, hvis I er i tvivl. Især er det vigtigt, at de mindre virksomheder kommer i gang med AI. Både fordi undersøgelsen viser, at der er dem, der halser efter i dag. Men også fordi meget peger på, at det er de små og mellemstore virksomheder, der står til at få det største løft gennem AI. På den måde kan kunstig intelligens være med til at skabe en vis demokratisering i erhvervslivet.

Lige så vigtigt er det, at danske virksomheder ikke kun ser AI som en mulighed for at effektivisere, blive klar til fremtiden og udnytte de muligheder, der allerede eksisterer og forsat vil komme. Men i stedet tænker i digital omskoling og udnytter de ekstra menneskelige ressourcer til at blive endnu dygtigere til alle de opgaver, der kræver kompleks og kreativ tænkning. På den måde kan kunstig intelligens og AI-værktøjer hjælpe os mennesker med at blive bedre til at arbejde og tænke som mennesker.

AI vil blive afgørende for vores fremtid

- Bruger AI i høj eller meget høj grad i dag.
- Forventer at AI vil spille en stor eller afgørende rolle i fremtiden.



Konklusion/afslutning

Føler vi os mere klar, end vi reelt er?

I dag er digitalisering ikke et tilvalg, men en præmis for virksomheders fortsatte eksistens og udvikling inden for stort set alle brancher. Danske virksomheder ser generelt lyst på fremtiden. Men undersøgelsen understreger også, at vi måske er mere optimistiske, end der er grund til at være.

Vores undersøgelse taler sit tydelige sprog. Danske virksomheder går fremtiden i møde med stor selvtillid og optimisme. Trods udfordringer føler størstedelen af de adspurgte virksomheder, at de i nogen eller høj grad er godt rustet til fremtiden – og endnu mere end da vi spurgte dem for et år siden. 94% virksomheder ser sig selv som godt klædt på til fremtiden, og det er en markant stigning i forhold til 2024. Jo større virksomhed, jo større optimisme.

Det er enormt positivt, at danske virksomheder i den grad ser lyst på fremtiden. For virksomhederne føler sig generelt også udfordret i forhold til at følge med udviklingen i forhold til bl.a. AI, GDPR, compliance, it-sikkerhed og cyberkriminalitet. En stor del af virksomhederne erkender, at it-sikkerheden godt kunne få et løft. Og selv om alle tal viser, at hackere og it-kriminelle arbejder endnu hårdere end tidligere, så investerer især mindre virksomheder ganske

enkelt ikke nok i it-sikkerheden og relativt få har en gennemført plan i tilfælde af angreb. Det vil føre til endnu større økonomiske tab og flere virksomheder, der må dreje nøglen om som følge af it-kriminalitet.

Hvis virkeligheden skal afspejle virksomhedernes optimisme, er der derfor behov for at bruge flere ressourcer og kroner på digitaliseringen, og der er brug for at tænke bredt ud fra en overordnet strategi. Hele 92% af de store organisationer mener, at en stærk it-infrastruktur er afgørende for fremtiden. Og den digitale udvikling betyder, at teknologier og indsatsområder i stigende grad flyder sammen. It-sikkerhed er en nødvendig og indgroet del af digitaliseringen, og AI er efterhånden ikke et isoleret tilvalg, men en teknologisk tilgang, der på sigt vil påvirke store dele af jeres virksomheds drift og udvikling.

Den rette strategi og it-partner kan hjælpe jer med at prioritere jeres investeringer effektivt og få forskellige løsninger til at spille sammen med jeres behov nu og på den lange bane. Det kan være med til at sikre, at optimismen ikke bliver en sovepude, og at I står stærkt i forhold til fremtidens udfordringer.

Knap 8 ud af 10 virksomheder oplever, at det er svært at følge med i nye krav og muligheder. Alligevel føler 94% sig godt klædt på til fremtiden.

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 december 2024 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 indenfor 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

