Digital sikkerhed i danske SMV'er 2024

Styrelsen for Samfundssikkerhed
December 2024

Indhold

1. Introduktion

Danmark er et digitalt forgangsland, og de danske virksomheder er for eksempel langt fremme, når det kommer til SMV'ernes digitaliseringsgrad, brugen af big data, cloud computing og kunstig intelligens[1]. Desværre findes der også en bagside af medaljen, da den høje digitalisering naturligt medfører et parallelt behov for at styrke virksomhedernes digitale forsvar mod cyberangreb.

Center for Cybersikkerhed vurderer, at truslen for cyberkriminalitet er MEGET HØJ og kan gå ud over både den enkelte borger, myndigheder og virksomheder uanset størrelse og sektor. Det vurderes som meget sandsynligt, at danske myndigheder og virksomheder vil blive ramt af cyberkriminalitet inden for de næste to år[2].

Den kommende NIS 2-lov er rettet mod myndigheder og virksomheder i sektorer, som anses for at være kritiske for samfundet. Lovgivningen vil stille en række krav til, hvad de omfattede myndigheder og virksomhederne skal gøre for at styrke modstandsdygtigheden mod cyberangreb. NIS 2-loven omfatter som udgangspunkt kun mellemstore virksomheder og opefter.

Ca. 300.000 danske virksomheder er dermed ikke omfattet af NIS 2-lovgivningen, fordi de ikke tilhører de kritiske sektorer, som lovgivningen omfatter. Det drejer sig i høj grad om de danske små- og mellemstore **virksomheder** (SMV'er), som dog ikke går fri af cybertruslen. Opportunistiske cyberkriminelle går ofte efter ofre, som de nemt kan kompromittere - og derfor kan de mindre virksomheder udgøre lavthængende frugter for de cyberkriminelle[3].

Styrelsen for Samfundssikkerhed arbejder for at løfte de danske SMV'er's digitale sikkerhed gennem oplysning og konkrete værktøjer. For at kunne målrette denne indsats, viser denne analyse, hvordan de danske SMV'er arbejder med digital sikkerhed. Herunder hvilke sikkerhedsforanstaltninger, som de danske SMV'er anvender, og hvilke udfordringer som de oplever i forbindelse med it-sikkerhedsarbejde. Det er femte gang, at analysen udgives.

[1] Digitaliserings- og Ligestillingsministeriet (2024): Redegørelse om Danmarks Digitale Udvikling
[2] Center for Cybersikkerhed (2024): Cybertruslen mod Danmark
[3] Center for Cybersikkerhed (2024): Cybertruslen mod Danmark

1.1 Analysens hovedresultater

Analyse viser, at der fortsat er et markant behov for at løfte den digitale sikkerhed blandt de danske SMV'er, da hele **40 pct.** af SMV'erne fortsat ikke har et digitalt sikkerhedsniveau, som matcher deres risikoprofil, ligesom **15 pct.** af SMV'erne ikke anvender helt essentielle sikkerhedstiltag (løbende opdatering af styresystemer og backup af data). Analysen viser desuden plads til forbedring, hvad angår SMV'ernes brug af øvrige it-sikkerhedstiltag. For eksempel anvender **40 pct**. af SMV'erne fortsat ikke stærke adgangskoder til autentificering[4], og det vil gøre det nemmere for de it-kriminelle at bryde koden og få adgang til virksomhedens systemer og data.

Samtidig viser analysen, at SMV'er er sårbare over for angreb, der vil lamme deres systemer, da **60 pct.** af dem slet ikke eller kun i lav grad vil kunne udføre virksomhedens kerneopgaver uden adgang til interne centrale it-systemer. Samme andel ses hos store virksomheder med 250+ ansatte. Langt over halvdelen af SMV'erne (**61 pct**.) har systemer, der behandler eller opbevarer forretningskritisk data, såsom forretningshemmeligheder og/eller kundedatabaser, ligesom godt en fjerdel af SMV'erne (**28 pct**.) har systemer, som opbevarer eller behandler persondata med særlig risiko, eksempelvis følsomme persondata, CVR-numre mv. SMV'erne er således også sårbare over for uvedkommende, som forsøger at få adgang til virksomhedens data.

Et cyberangreb kan være meget omkostningstungt for en virksomhed, det kan have store konsekvenser for virksomhedens renommé, og det kan i værste fald koste virksomheden livet. Virksomhedens ledelse bærer derfor ansvaret for virksomhedens digitale sikkerhed. Men besvarelserne i denne analyse viser, at under halvdelen (**40 pct**.) af ledelserne i de danske SMV'er i høj grad tager stilling til virksomhedernes it-sikkerhedsmæssige aktiviteter, mens **17 pct**. slet ikke eller kun i lav grad tager stilling hertil. Der ses også en sammenhæng mellem ledelsesfokus på digital sikkerhed og virksomhedens it-sikkerhedsniveau. Analysen viser nemlig, at i jo højere grad ledelsen tager stilling til virksomhedens it-sikkerhedsmæssige aktiviteter, des højere er virksomhedens it-sikkerhedsniveau.

En anden forklaring på at SMV'erne ikke er i mål med den digitale sikkerhed kan være, at **37 pct**. af SMV'erne oplever udfordringer eller begrænsninger med at øge virksomhedens digitale sikkerhedsniveau. Særligt angives *'usikkerheden om virksomhedens gevinst ved at investere i it-sikkerhed*', som **22 pct.** af SMV'erne angiver som en faktor. Desuden peger

[4] Autentificering er processen, hvor man bekræfter identiteten af en person, system eller enhed, typisk for at give adgang til et beskyttet område, en tjeneste eller information. Det er en vigtig sikkerhedsforanstaltning, da det sikrer, at kun autoriserede brugere får adgang til bestemte ressourcer.

21 pct. af SMV'erne på *'manglende viden og kompetencer til at håndtere it-sikkerhedsløsninger*' samt **15 pct.** på *'manglende økonomiske ressourcer til at investere i it-sikkerhed*' som begrænsninger eller udfordringer i forhold til at øge deres it-sikkerhed.

Af positive resultater kan fremhæves, at hele **94 pct.** af SMV'erne tog backup af deres data i 2023, hvilket er en pæn stigning sammenlignet med **81 pct.** i 2021. Netop backup af data er et helt grundlæggende it-sikkerhedstiltag, som stort set alle virksomheder bør efterleve. Der findes desuden en stigning i andelen af SMV'er, som gennemførte risikoanalyse af virksomheden, fra **54 pct**. i 2021/2022 til **59 pct**. i 2023. Dette er en positiv udvikling, da risikoanalyser er første skridt til at få klarlagt, hvor virksomheden er mest sårbar, så de passende it-sikkerhedstiltag kan prioriteres, og de største risici håndteres og minimeres. Der er dog fortsat **41 pct**. af SMV'erne, som fortsat ikke foretager løbende risikoanalyser af virksomheden, og får dermed ikke kortlagt sandsynligheden for og konsekvenserne ved it-sikkerhedsmæssige hændelser.

1.2 Afgrænsning og datagrundlag

Datagrundlaget i rapporten er beregnet på baggrund af Danmarks Statistiks årlige spørgeskemaundersøgelse "IT-anvendelse i virksomheder" (ITAV). Denne rapport baserer sig på data indsamlet i 2023, der består af besvarelser fra 4.557 virksomheder med 10+ ansatte inden for de private, ikke-finansielle byerhverv. I visse spørgsmål om it-sikkerhed bedes virksomhederne forholde sig til og besvarer ud fra deres situationen i det forgange år, i dette tilfælde 2022. Det gælder fx spørgsmålet om, hvorvidt virksomhederne har oplevet en it-sikkerhedshændelse.

Det er obligatorisk for virksomheder at besvare undersøgelsen, hvilket øger besvarelsernes repræsentativitet. Desuden er data vægtet, således at resultaterne afspejler populationen af danske virksomheder.

Ud over den årlige ITAV-undersøgelse (blandt virksomheder med 10+ ansatte) har Danmarks Statistik også i 2023 gennemført en spørgeskemaundersøgelse blandt de helt små danske virksomheder med 5-9 ansatte (mikrovirksomheder). I undersøgelsen stilles mikrovirksomhederne også udvalgte it-sikkerhedsspørgsmål, hvorfor rapporten indeholder et afsnit om mikrovirksomhedernes arbejde med digital sikkerhed sammenlignet med øvrige danske virksomheder. Dette datasæt består af gennemførte besvarelser fra i alt 1.548 virksomheder i de private, ikke-finansielle byerhverv med 5-9 fultidsansatte.

Eftersom den primære målgruppe for analysen er danske SMV'er, er resultaterne i denne rapport opdelt for mikrovirksomheder, virksomheder med 10-249 ansatte (SMV'erne) og virksomheder med 250+ ansatte (store virksomheder). Rapporten "Digital sikkerhed i

danske SMV'er" er gennemført årligt siden 2020[5]. En række spørgsmål i undersøgelsen "it-anvendelse i virksomheder" går igen fra tidligere års undersøgelser, og resultaterne kan således sammenlignes på tværs af årene- I disse tilfælde vil en eventuel udvikling i SMV'ernes arbejde med digital sikkerhed illustreres og beskrives i rapporten.

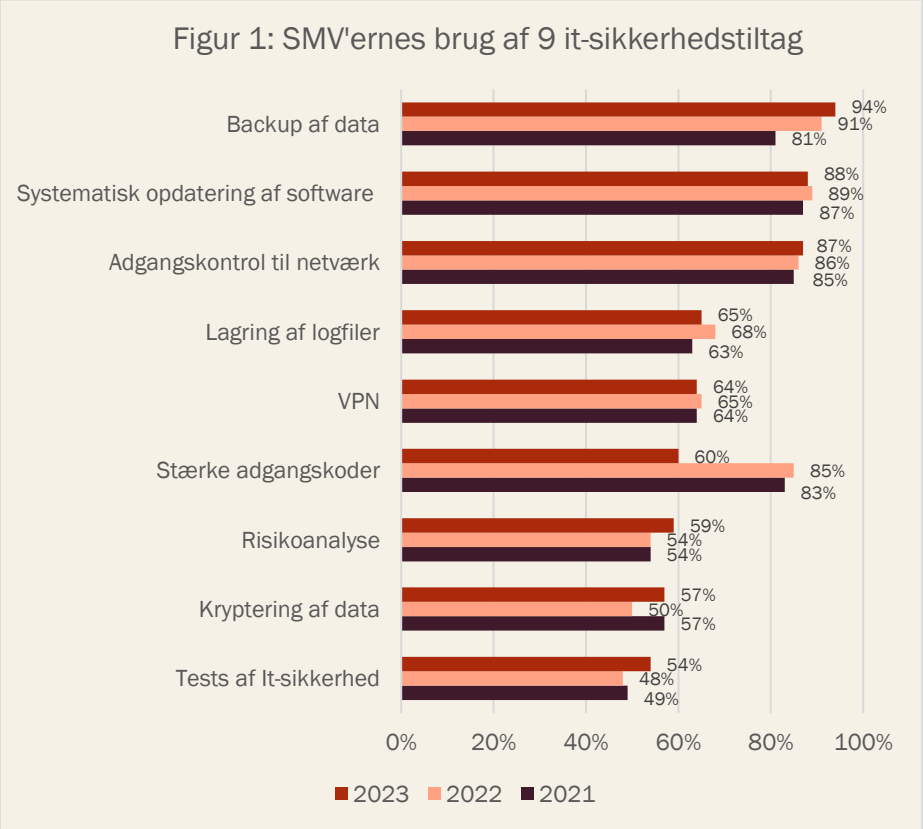
[5] I 2020, 2021 og 2022 er rapporten udarbejdet af Erhvervsstyrelsen. Men som følge af ressortomlægninger er rapporten udgivet af Digitaliseringsstyrelsen i 2023 og af Styrelsen for Samfundssikkerhed i 2024.

2. Virksomheders brug af it-sikkerhedstiltag

Dette kapitel omhandler de danske virksomheders arbejde med it-sikkerhedstiltag. Først vil virksomhedernes brug af tekniske it-sikkerhedstiltag belyses. Dernæst fokuseres på virksomhedernes arbejde med organisatoriske it-sikkerhedstiltag. Kapitlet afsluttes med et afsnit om den digitale sikkerhed blandt mikrovirksomheder med 5-9 ansatte.

2.1 SMV'ernes brug af tekniske it-sikkerhedstiltag

I undersøgelsen 'it-anvendelse i virksomheder' spørges der ind til, hvorvidt virksomhederne anvender ni forskellige tekniske it-sikkerhedstiltag. Figur 1 viser, hvilke sikkerhedstiltag der er tale om, og udviklingen af SMV'ernes brug af disse tiltag fra 2021-2023.



Kilde: Egne beregninger baseret på data indsamlet af Danmarks Statistik 2023 (ITAV)

Som det fremgår af figuren tog hele 94 pct. af SMV'erne backup af deres data i 2023, hvilket er en pæn stigning sammenlignet med 81 pct. i 2021. Som det næste afsnit kommer tilbage til, anses netop backup af data som et helt grundlæggende it-sikkerhedstiltag, som stort set alle virksomheder bør efterleve, og det er derfor positivt, at der især fra 2021-2022 findes en stor fremgang i virksomhedernes brug heraf. På Sikkerdigital kan SMV'er blandt andet få konkrete råd til gode backup-rutiner i virksomheden: Tag backup af data (sikkerdigital.dk).

Der ses desuden en stigning i andelen af SMV'er, som gennemførte risikoanalyse[6] af virksomheden, fra 54 pct. i 2021/2022 til 59 pct. i 2023. Dette er en vigtig udvikling, da risikoanalyser er første skridt til at få klarlagt, hvor virksomheden er mest sårbar, så de

[6] Defineres som: *periodevis vurdering af sandsynlighed og konsekvenser for it-sikkerhedsmæssige hændelser.*

passende it-sikkerhedstiltag kan prioriteres, og de største risici håndteres og minimeres. Der er dog fortsat 41 pct. af SMV'erne, som ikke gennemfører løbende risikovurderinger – til dem stiller Sikkerdigital.dk et IT-risikovurderingsværktøj til rådighed, som kan hjælpe virksomheder i gang med en enkel og praktisk brug af risikovurdering.

Det får virksomheden med IT-risikovurderingsværktøjet

IT-risikovurderingsværktøjet er henvendt til små og mellemstore virksomheder og de it-faglige personer med kendskab til virksomhedens it-setup. Det kan være virksomhedens egen it-ansvarlige eller en leverandør.

Med værktøjet får virksomheden en grundlæggende it-risikovurdering i Excel-format samt en vejledning, som kan downloades.

Risikovurderingen indikerer, hvor virksomheden har de største risici, og vejledningen hjælper i forhold til, hvad der kan gøres for at håndtere de forskellige udfordringer og dermed mindske it-risici i virksomheden i fremtiden.

Figur 1 ovenfor viser også et bemærkelsesværdigt stor fald i SMV'ernes brug af stærke adgangskoder fra 85 pct. i 2022 til blot 60 pct. i 2023. En forklaring på dette kan dog skyldes en ændring i spørgsmålsformuleringen i 2023, da anbefalingerne er opdateret fra minimum 8 karakterer i 2022 til minimum 12 karakterer i 2023[7].

Passwords: Længden på adgangskoden er vigtig, når den skal være sværere at bryde for hackere. I takt med den stigende digitale trussel og brug af mere avancerede digitale teknologier, er anbefalingen om antal minimumstegn steget over årene. Den nuværende anbefaling er, at adgangskoder har en minimumslængde på 15 tegn eller flere. Enhver organisation bør dog tage afsæt i sin egen situation og risikoprofil (CFCS "Passwordsikkerhed" 2023).

[7] Definition i 2021: M*inimumslængde på 8 blandede karakterer og periodevis ændring af adgangskode.*
Definition i 2023: *Minimumslængde på 12 blandede karakterer og at koden ikke bruges flere steder.*
OBS. Siden undersøgelsen i 2023 er anbefalingen igen blevet opdateret og virksomheder anbefales nu at anvende 15 tegn eller flere (se evt. sikkerdigital.dk)

På Sikkerdigital kan SMV'erne finde konkrete råd til stærke passwords og læse mere om vigtigheden af to-faktor login: Lav stærke adgangskoder (sikkerdigital.dk).

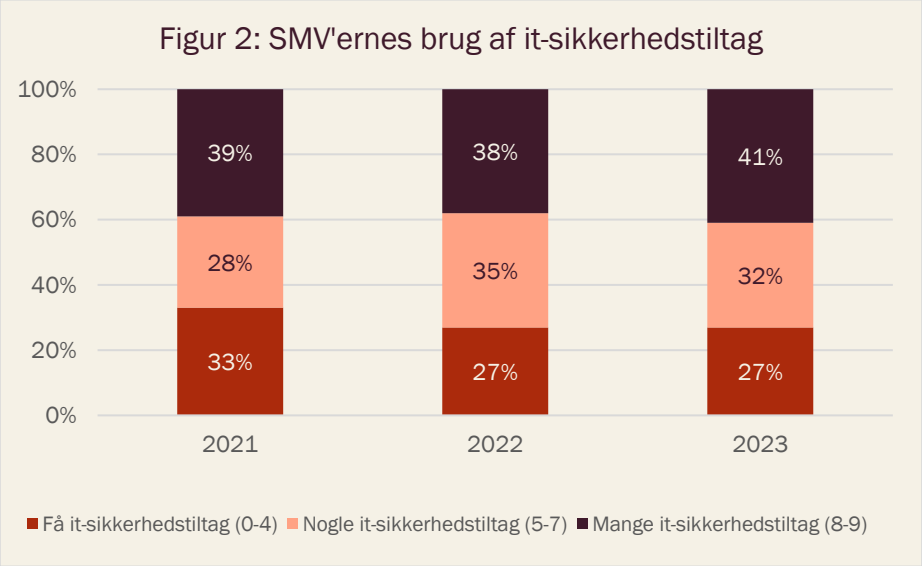
Samtlige ni tekniske it-sikkerhedsforanstaltninger i figur 1 er blevet omdannet til et indeks, der angiver, om en virksomhed anvender hhv. 'få', 'nogle' eller 'mange' tekniske it-sikkerhedsforanstaltninger, som beskrevet i nedenstående tekstboks.

Tabel: Operationalisering af virksomheders brug af it-sikkerhedstiltag

Få it-sikkerhedstiltag	Nogle it-sikkerhedstiltag	Mange it-sikkerhedstiltag
Brug af 0-4 it-sikkerhedstiltag + virksomheder, der ikke har implementeret de to essentielle sikkerhedstiltag	Brug af 5-7 it-sikkerhedstiltag. På nær virksomheder, der ikke har implementeret de to essentielle sikkerhedstiltag	Brug af 8-9 it-sikkerhedstiltag. På nær virksomheder, der ikke har implementeret de to essentielle sikkerhedstiltag

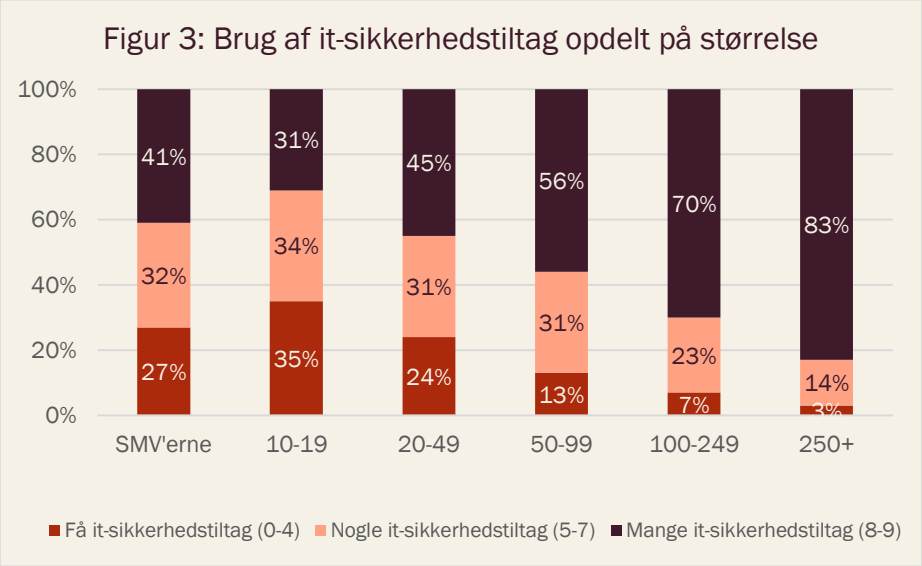
Note: En nærmere forklaring af denne operationalisering fremgår af kapitel 8. Metode

Figur 2 viser SMV'ernes brug af de ni it-sikkerhedstiltag i hhv. 2021, 2022 og 2023. Flere af SMV'erne er i 2023 begyndt at anvende 'mange' (8-9) it-sikkerhedstiltag, nemlig 41 pct., hvilket året før var 38 pct. Sammenligner man SMV'ernes brug af sikkerheds-foranstaltninger i 2022 og 2023, har en mindre andel af virksomhederne flyttet sig fra 'nogle' til 'mange' sikkerhedsforanstaltninger, hvorimod der ikke findes en udvikling blandt de SMV'er, som har 'få' (0-4) it-sikkerhedstiltag. Dette kan være et udtryk for, at cybersikkerhed fylder en smule mere i SMV'ernes bevidsthed.



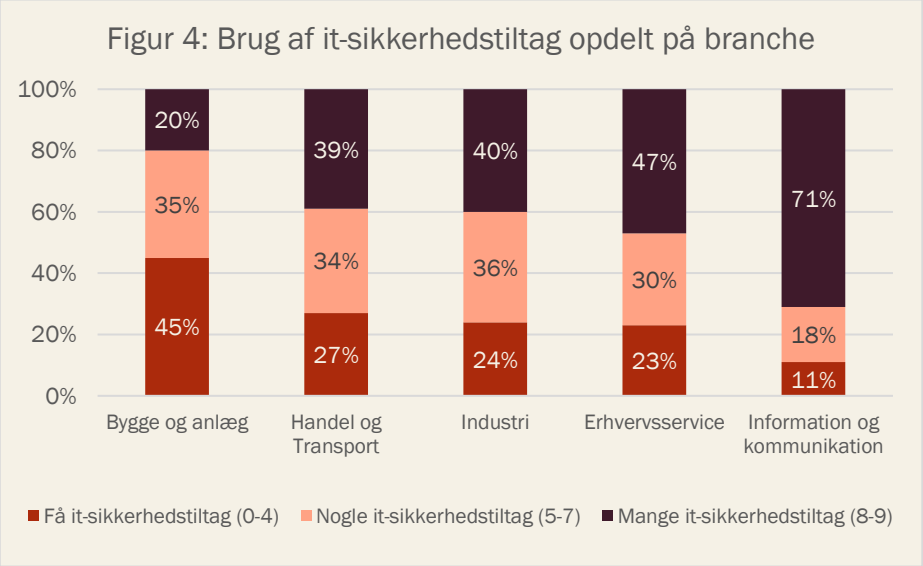
Kilde: Egne beregninger baseret på data indsamlet af Danmarks Statistik 2023 (ITAV)

Figur 3 viser SMV'ernes brug af it-sikkerhedstiltag på tværs af virksomhedsstørrelse. Her ses en klar tendens, nemlig at virksomhedernes størrelse påvirker brugen af sikkerhedstiltag i den forstand, at jo mindre virksomhed, jo mindre gøres der brug af it-sikkerhedstiltag. Disse resultater står i lighed med resultaterne fra tidligere års analyse af 'Digital sikkerhed i danske SMV'er'. Forskellen mellem SMV'erne (det samlede vægtede resultat blandt danske SMV'er) og virksomheder med +250 ansatte tydeliggør dette. Kun 3 pct. af virksomhederne med +250 ansatte bruger "få" it-sikkerhedstiltag, hvilket gælder 27 pct. af SMV'erne – altså en forskel på 24 procentpoint.



Kilde: Egne beregninger baseret på data indsamlet af Danmarks Statistik 2023 (ITAV)

Figur 4 viser SMV'ernes brug af it-sikkerhedsforanstaltninger opdelt på branche. Igen i 2023 er branchen med mindst fokus på digital sikkerhed 'bygge og anlægsbranchen' (hvor hele 45 pct. anvender "få" tiltag). Ligeledes er det igen i år 'information og kommunikationsbranchen', som har størst fokus på digital sikkerhed. Men da virksomhederne i denne branche typisk har flere ansatte, der arbejder digitalt med adgang til kundedata osv., bør der også her være et større fokus på digital sikkerhed. Det vender vi tilbage til i kapitel 3, som ser nærmere på virksomhedernes sikkerhedsniveau set i forhold til deres risikoprofil.



Kilde: Egne beregninger baseret på data indsamlet af Danmarks Statistik 2023 (ITAV)

2.2 SMV'ernes brug af essentielle it-sikkerhedstiltag

To af de ni tekniske it-sikkerhedstiltag anses som værende helt essentielle og nødvendige for en virksomheds digitale sikkerhed, nemlig backup af data og systematisk opdatering af software[8]. Stort set alle virksomheder bør derfor som minimum anvende disse to tiltag, som en del af deres digitale sikkerhed.

[8] Deloitte (2017): It-sikkerhed og datahåndtering i danske SMV'er

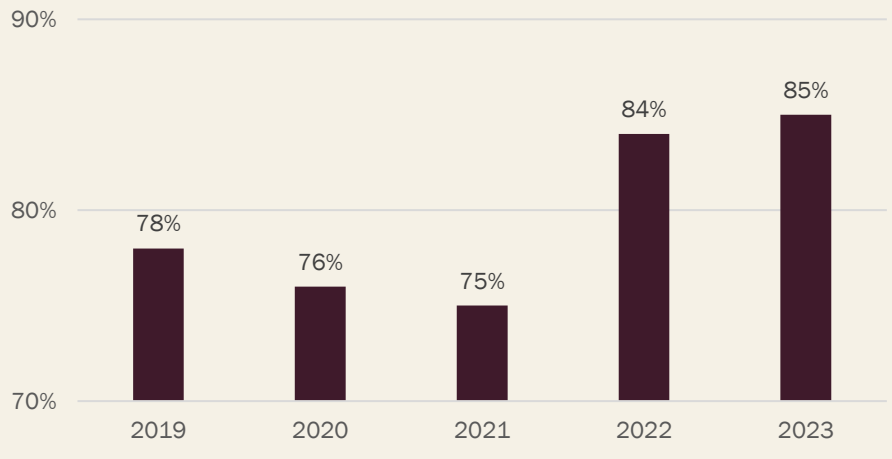
Essentielle it-sikkerstiltag: systematisk opdatering af software og backup af data

Systematisk opdatering af software er essentiel for virksomhedens digitale sikkerhed, da systemer og programmer løbende repareres for fejl og "sikkerhedshuller", og derved reduceres sandsynligheden for digitale angreb. En backup-procedure gør det muligt for virksomheden at få sine systemer relativt hurtigt op at køre igen efter et eventuelt succesfuldt cyberangreb.

På Sikkerdigital kan SMV'erne orientere sig i syv råd for IT-sikkerhed, herunder vejledning om bl.a. opdatering af systemer og backup: **Syv råd om it-sikkerhed (sikkerdigital.dk)**

Det er derfor også positivt, at 85 pct. af SMV'erne anvender begge disse essentielle it-sikkerhedstiltag, som en del af deres digitale forsvar i 2023 og derved opretholder det relativt høje niveau fra 2022.

Figur 5: Andel af SMV'er der anvender essentielle it-sikkerhedsiltag 2019-2023



Kilde: Egne beregninger baseret på data indsamlet af Danmarks Statistik 2023 (ITAV)

Som figuren viser, findes særligt en fremgang i SMV'ernes brug af essentielle it-sikkerhedstiltag fra 2021 til 2022. Som også beskrevet i sidste års rapport, kan denne fremgang skyldes flere faktorer. Det kan blandt andet være et udtryk for, at virksomheder

generelt er blevet mere digitale efter COVID-19[9], hvilket også gør dem mere udsatte for digitale angreb, og behovet for at sikre sig herimod. Det kan også skyldes det øgede trusselsbillede, som Europa og resten af verden står over for efter Ruslands invasion af Ukraine i februar 2022[10]. En tredje forklaring kan være et større fokus på digital sikkerhed fra politisk side. Fx ved at lancere den første nationale strategi for cyber- og informationssikkerhed i 2018, hvormed der blev igangsat en række konkrete initiativer med fokus på at styrke den digitale sikkerhed blandt borgere, myndigheder og virksomheder. I 2022 blev en opfølgende strategi for cyber- og informationssikkerhed igangsat[11]. Endelig kan et øget ambitionsniveau fra øvrige aktører, fx brancheorganisationer, og mediernes fokus på området også have medvirket til en større forståelse for vigtigheden i at have den basale digitale sikkerhed på plads.

Mens dette afsnit har fokuseret på it-sikkerhedstiltag af mere teknisk karakter, vil det kommende afsnit se på SMV'ernes brug af organisatoriske it-sikkerhedstiltag.

2.3 SMV'ernes brug af organisatoriske it-sikkerhedstiltag

På lige fod med andre forretningsbeslutninger er det ledelsen, som bærer ansvaret for virksomhedens digitale sikkerhed. Derfor er det interessant at se nærmere på, i hvilket omfang virksomhedens øverste ledelse tager stilling til virksomhedernes it-sikkerhedsmæssige aktiviteter.

Stærk digital sikkerhed starter hos ledelsen

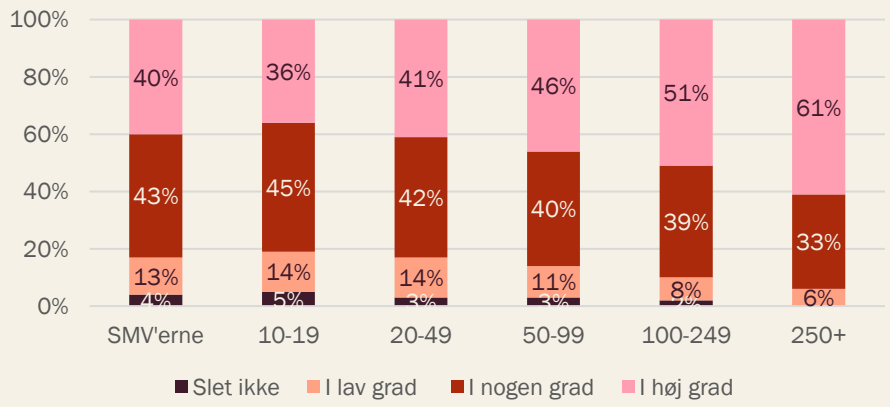
IT-sikkerhed er en kritisk forretningsfunktion, der kræver ledelsens opmærksomhed og engagement. Ledelsen spiller en afgørende rolle i at fremme en sikkerhedskultur, allokere nødvendige ressourcer og sikre, at politikker og procedurer implementeres effektivt. Uden ledelsens støtte kan sikkerhedsinitiativer mangle den nødvendige prioritering og ressourcer, hvilket øger risikoen for cyberangreb og databrud.

[9] Norlys (2021): rapport om digital mindset
[10] Center for cybersikkerhed (2023): Cybertruslen mod Danmark

Figur 6 viser sammenhængen mellem virksomhedsstørrelse, og i hvilket omfang at ledelsen har taget stilling til virksomhedens it-sikkerhedsmæssige aktiviteter. Samlet set svarede 40 pct. af de adspurgte SMV'er, at virksomhedens ledelse i høj grad er involveret heri. Til sammenligning gælder dette 61 pct. blandt de store virksomheder med 250+ ansatte. At ledelsens involvering i digital sikkerhed stiger i takt med antal ansatte i virksomheden kan muligvis forklares med, at store virksomheder ofte også har en højere risikoprofil, hvilket uddybes i kapitel 3.

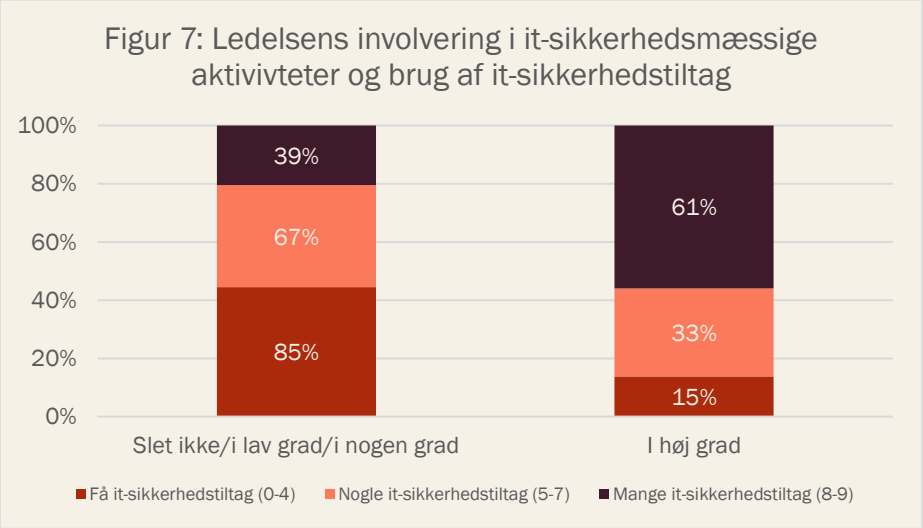
Samlet set er 40 pct. af ledelserne i de danske SMV'er i høj grad involveret i virksomhedens arbejde med digital sikkerhed, hvilket er en lille fremgang siden sidste år på 36 pct. Men der er fortsat hele 17 pct. af ledelserne, som *slet ikke* eller kun *i lav grad* tager stilling til virksomhedernes it-sikkerhedsmæssige aktiviteter.

Figur 6: I hvilket omfang tager virksomhedens topledelse og/eller bestyrelse stilling til it-sikkerhedsmæssige aktiviteter



Kilde: Egne beregninger baseret på data indsamlet af Danmarks Statistik 2023 (ITAV)

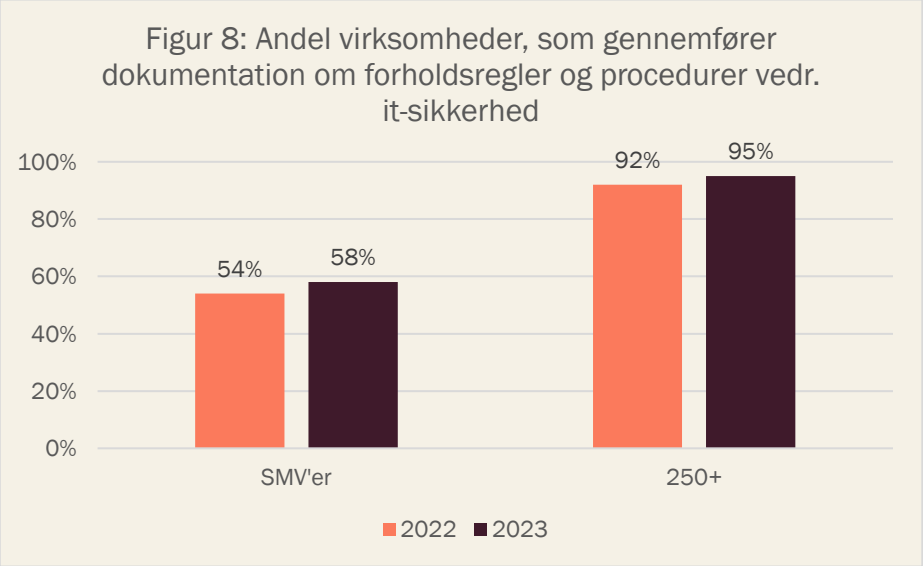
Blandt de 40 pct. af SMV'erne, hvor ledelsen i høj grad er involveret i virksomhedens it-sikkerhedsmæssige aktiviteter, bliver der anvendt betydeligt flere it-sikkerhedstiltag i forhold til de 60 pct. af SMV'erne, som kun i nogen grad, lille grad eller slet ikke er inde over de it-sikkerhedsmæssige aktiviteter, jf. figur 7.



Kilde: Egne beregninger baseret på data indsamlet af Danmarks Statistik 2023 (ITAV)

Dokumentation og dermed delbar viden om it-sikkerhedstiltag og -regler er et væsentlig element i virksomhedernes arbejde med digital sikkerhed. En veludført dokumentation af virksomhedens it-sikkerhedsprocedure- og politikker kan for eksempel bidrage til at sikre klare retningslinjer og handlingsplaner, hvis en sikkerhedshændelse opstår og dermed minimere skader og nedetid. Dokumentation af it-sikkerhedsprocedurer kan også skabe en standardiseret tilgang til it-sikkerhed på tværs af virksomheden, hvor fx klare it-sikkerhedspolitikker kan være et vigtigt værktøj til at øge medarbejdernes bevidsthed om it-sikkerhed. Desuden kan nedskrevet procedurer og politikker være nødvendigt for at dokumentere overholdelse af lovgivning på området.

Som figur 8 viser, havde 58 pct. af SMV'erne i 2023 gennemført dokumentation om forholdsregler, aktiviteter og procedurer vedr. it-sikkerhed. Der var således fortsat 42 pct. af SMV'erne, der ikke havde dokumenteret deres it-sikkerhedstiltag mv., hvilket gjaldt 5 pct. af de store virksomheder. Der findes dog en mindre stigning i andelen af virksomheder, der gennemførte dokumentation fra 2022 til 2023 for begge størrelsesgrupper.



Kilde: Egne beregninger baseret på data indsamlet af Danmarks Statistik 2023 (ITAV)

På Sikkerdigital.dk ligger guides, værktøjer og skabeloner til rådighed, som hjælper danske virksomheder til blandt andet at dokumentere forholdsregler og procedure vedr. digital sikkerhed. Blandt andet findes der hjælp til:

- Risikovurdering, som giver et overblik over, hvor virksomheden er mest sårbar, og hvad der kan gøres for at reducere sårbarheden.
- En beredskabsplan, som beskriver, hvem der gør hvad i hver enkelt situation, og sikrer, at virksomheden reagerer hurtigt, målrettet og tilstrækkeligt, hvis der opstår en it-sikkerhedshændelse.
- It-sikkerhedspolitik, som kan bidrage til at skabe klare retningslinjer om, hvad der forventes af både leder og medarbejder, når det gælder it-sikkerhed.

Kontrolleret for virksomhedsstørrelse og branche gælder, at virksomheder, der arbejder med hhv. ledelsesinvolvering og dokumentation af procedure vedr. it-sikkerhed, også anvender flere tekniske it-sikkerhedsforanstaltninger. Der findes således en sammenhæng mellem virksomhedernes arbejde med tekniske og organisatoriske it-sikkerhedstiltag. Det næste afsnit ser på den digitale sikkerhed blandt de helt små virksomheder med 5-9 ansatte.

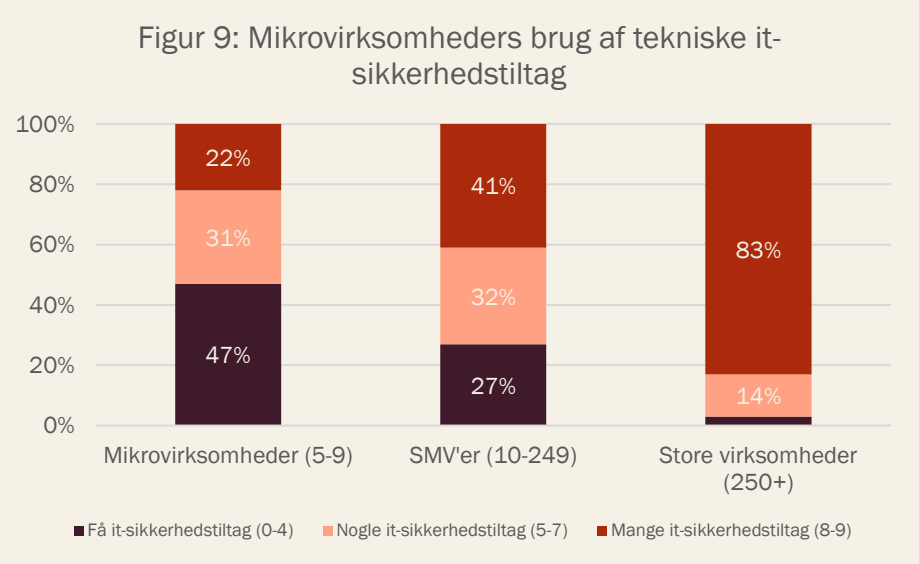
2.4 Digital sikkerhed blandt mikrovirksomheder

Ud over den årlige ITAV-undersøgelse (blandt virksomheder med 10+ ansatte) har Danmarks Statistik gennemført en temaanalyse i 2024 blandt de helt små danske

virksomheder med 5-9 ansatte (mikrovirksomheder). Stikprøven består af gennemførte besvarelser fra i alt 1.548 virksomheder i de private, ikke-finansielle byerhverv med 5-9 fultidsansatte. I undersøgelsen stilles mikrovirksomhederne blandt andet udvalgte it-sikkerhedsspørgsmål, herunder et spørgsmål til deres brug af de ni tekniske it-sikkerhedsforanstaltninger.

Figur 9 viser mikrovirksomhedernes brug af hhv. "få, "nogle" og "mange" it-sikkerhedsforanstaltninger sammenlignet med SMV'erne og de store virksomheders brug heraf.

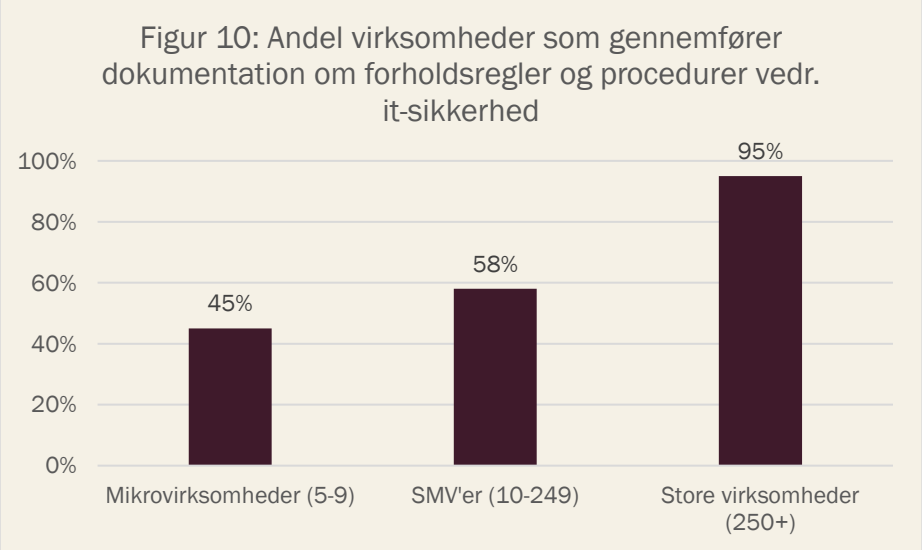
Som det fremgår har mikrovirksomhederne et særligt lavt digitalt sikkerhedsniveau, da næsten halvdelen (47 pct.) af denne virksomhedsgruppe blot anvender "få" it-sikkerhedstiltag. Der findes dog en lille fremgang siden den seneste analyse blandt mikrovirksomheder i 2022, hvor 52 pct. blot anvendte "få" it-sikkerhedstiltag.



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (It-anvendelse i virksomheder 2023 og Aktiviteter i små virksomheder 2024).

Hvad angår de to essentielle sikkerhedstital (backup af data og systematisk opdatering af software) er det 73 pct. af mikrovirksomhederne, som anvender begge disse tiltag. Derved er der 27 pct. af mikrovirksomhederne, som ikke anvender de essentielle sikkerhedstiltag, hvilket til sammenligning var 15 pct. i den samlede SMV'gruppe med 10-249 ansatte. Igen findes dog en lille stigning siden seneste undersøgelse blandt mikrovirksomheder i 2022, hvor 29 pct. ikke anvendte de to helt essentielle sikkerhedstiltag.

Hvad angår mikrovirksomhedernes brug af organisatoriske tiltag gør samme billede sig gældende; nemlig at niveauet er lavere end for de øvrige virksomhedsgrupper. Som figur 10 viser, er det under halvdelen (45 pct.) af mikrovirksomhederne, som gennemfører dokumentation om forholdsregler og procedurer vedr. it-sikkerhed. I Afsnit 2.3 er det kort beskrevet, hvorfor det er en god idé at gennemføre denne dokumentation, samt hvordan man kan finde hjælp hertil på Sikkerdigital.dk.



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (It-anvendelse i virksomheder 2023 og Aktiviteter i små virksomheder 2024).

Dette kapitel har vist en klar sammenhæng mellem virksomhedsstørrelse og branche og virksomhedens digitale sikkerhedsniveau - både hvad angår tekniske og organisatoriske sikkerhedstiltag. Det skal dog understreges, at ikke alle virksomheder bør have det samme digitale sikkerhedsniveau. Derfor omhandler næste kapitel, i hvilken grad SMV'erne har en risikoprofil, som matcher deres it-sikkerhedsniveau.

3. SMV'ernes it-sikkerhedsniveau ift. risikoprofil

Det forgangne kapitel har set på SMV'ernes brug af hhv. tekniske og organisatoriske it-sikkerhedstiltag. I forlængelse heraf vil dette kapitel sammenstille SMV'ernes digitale sikkerhedsniveau med virksomhedernes risikoprofil.

Ikke alle virksomheder bør have det samme digitale sikkerhedsniveau. Derimod bør digital sikkerhed ses i relation til den kontekst, som den enkelte virksomhed opererer i. For eksempel kan virksomheders brug af digitale løsninger og teknologier medvirke til flere digitale sikkerhedsrelaterede risici. Det gælder fx, hvis de digitale løsninger er afhængige af systemer eller består af kritiske informationer, som it-kriminelle ikke må komme i besiddelse af, eller hvis et nedbrud på disse systemer vil påvirke virksomhedens daglige drift. De danske SMV'er bør derfor have et digitalt sikkerhedsniveau, som matcher deres risikoprofil.

Til brug for analysen er der udregnet 1) et indeks over SMV'ernes it-sikkerhedsniveau og 2) et indeks over SMV'ernes risikoprofil. Metoden bygger på et overordnet framework, hvor en række spørgsmål samlet skal udgøre et mål for virksomhedernes it-sikkerhedsniveau og deres risikoprofil, med en mulighed for at sammenholde disse to. En uddybning af metoden fremgår af kapitel 8. Metode (afsnit 8.2 Måling af hhv. it-sikkerhedsniveau og risikoprofil).

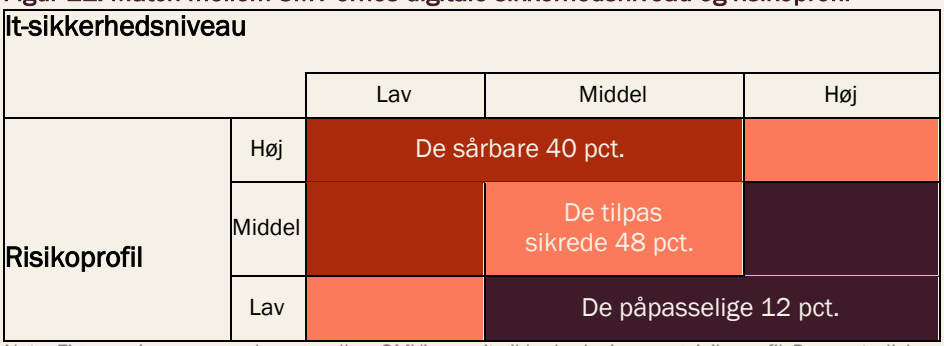
Indekset for SMV'ernes it-sikkerhedsniveau baserer sig på spørgsmål om, hvilke sikkerhedstiltag som SMV'erne har implementeret – fx om virksomhedens ledelse tager stilling til it-sikkerhedsmæssige aktiviteter, virksomhedens brug af tekniske it-sikkerhedstiltag mfl. Indekset for SMV'ernes risikoprofil baserer sig på spørgsmål, der siger noget om konsekvensen ved og sandsynligheden for, at en virksomhed bliver udsat for en

it-sikkerhedshændelse (fx antal ansatte, sektor, tekniske angrebsflader, opbevaring af persondata, afhængighed af it-systemer mm.).

I forhold til at vurdere matchet mellem SMV'ernes sikkerhedsniveau og deres risikoprofil anvendes niveauerne "lav", "middel" og "høj" til at inddele SMV'erne i tre typer. Hvis fx både sikkerhedsniveau og risikoprofil er middel, vurderes virksomheden til at have et tilpas it-sikkerhedsniveau. I rapportens metodeafsnit (kapitel 8) gives en detaljeret redegørelse for den metodiske fremgangsmåde for de to indeks og matchet mellem disse.

Nedenstående figur 11 sammenstiller de danske SMV'ers it-sikkerhedstiltag med virksomhedens risikoprofil. Resultatet er, at 40 pct. af de danske SMV'er ikke har et digitalt niveau, som lever op til deres risikoprofil, og derfor er særlig sårbare overfor et cyberangreb. For disse SMV'er vurderes konsekvensen af en it-sikkerhedshændelse samt sandsynligheden for, at en sådan finder sted, til at overstige det nuværende it-sikkerhedsniveau. Figuren viser desuden, at 48 pct. af SMV'erne har et digitalt sikkerhedsniveau, som matcher deres risikoprofil, mens 12 pct. har et højere digitalt sikkerhedsniveau end deres risikoprofil tilskriver, og de kategoriseres derfor som "påpasselige".

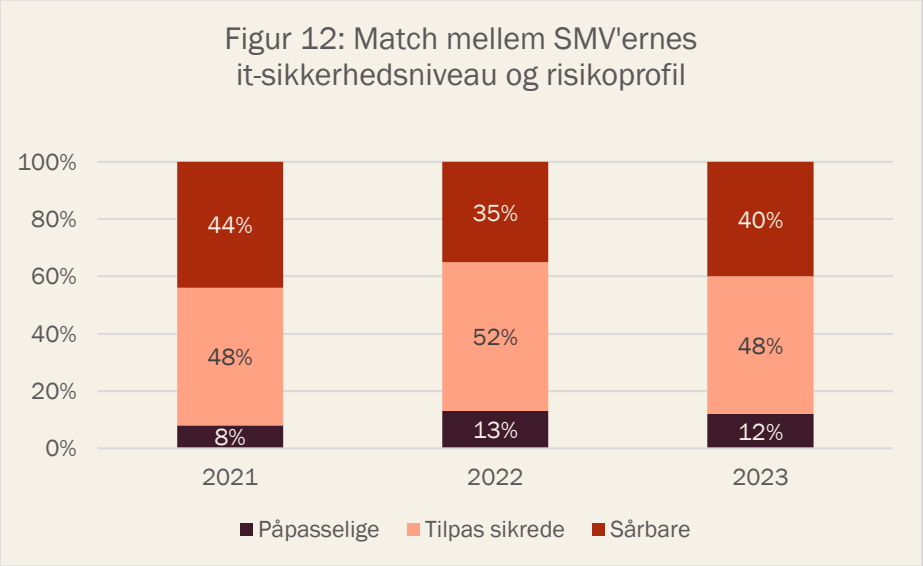
Figur 11: Match mellem SMV'ernes digitale sikkerhedsniveau og risikoprofil



Note: Figuren viser sammenhæng mellem SMV'ernes it-sikkerhedsniveau og risikoprofil. Den metodiske fremgangsmåde for udviklingen af de to indeks samt matchet mellem disse er uddybet i kapital 8.
Kilde: Egne beregninger baseret på tal fra Danmarks statistik (ITAV 2023).

Figur 12 viser andelen af hhv. sårbare, tilpas sikrede og påpasselige SMV'er i perioden fra 2021-2023, hvor de to indeks har været udarbejdet baseret på data fra undersøgelsen "It-anvendelse i virksomheder".

Som det fremgår af figuren, havde 35 pct. af SMV'erne ikke et tilstrækkeligt højt digitalt sikkerhedsniveau i 2022, hvilket er steget til 40 pct. i 2023.



Kilde: Egne beregninger baseret på tal fra Danmarks statistik (ITAV 2023).

En forklaring på, at vi ser en stigning i andelen af SMV'er med et utilstrækkeligt digitalt sikkerhedsniveau er, at flere SMV'erne er blevet mere digitale og i højere grad arbejder med digitale teknologier, hvilket øger deres risikoprofil, uden at et højere digitalt sikkerhedsniveau er fulgt med. Der findes nemlig en større andel af SMV'er, som gået fra at have en "lav" risikoprofil i 2022 til et "middel" risikoprofil i 2023, mens der ikke er en tilsvarende stor andel, som er rykket fra et "lavt" til et "middel" it-sikkerhedsniveau fra 2022 til 2023.

Der skal dog også gøres opmærksom på, at der fra år til år findes mindre formuleringsmæssige ændringer til flere af de spørgsmål, som indgår i de to indeks, hvilket der må tages forbehold for ved sammenligning af resultaterne over årene. Det kan således også være en del af forklaring på udsvingene mellem årene. I rapportens kapitel 8. Metodeafsnit beskrives de konkrete forskelle på spørgsmålsformuleringerne mellem årene.

Til virksomheder som ønsker hjælp med at undersøge, om deres it-sikkerhedsniveau er godt nok, udbydes Sikkerhedstjekket.

Hvad er Sikkerhedstjekket?

Sikkerhedstjekket er en online test for virksomheder, som virksomheden kan bruge til vurdering og forbedring af sin it-sikkerhed. Værktøjet tager afsæt i den internationale sikkerhedsstandard ISO27001 og favner kategorier som organisation, ledelse og processer.

Med Sikkerhedstjekket får virksomheden:

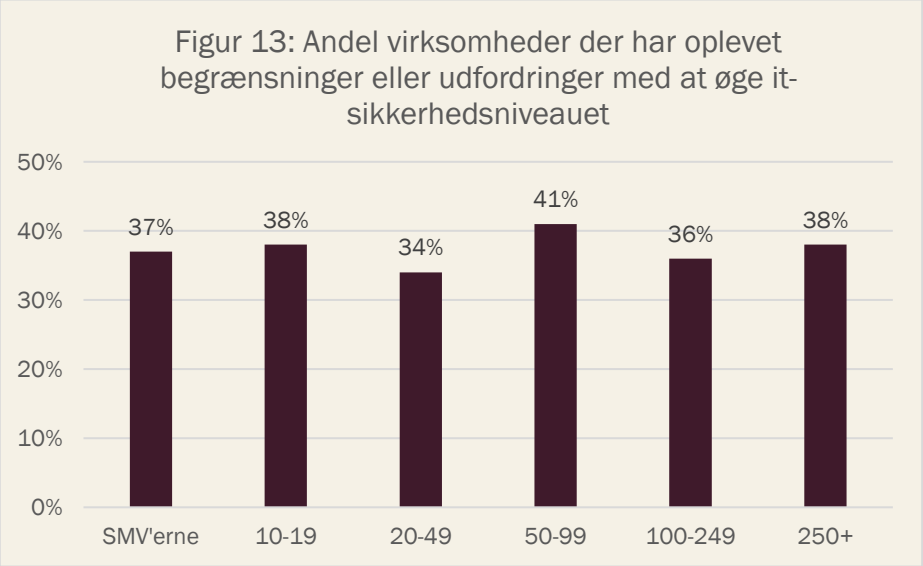
- Overblik over virksomhedens svage punkter
- Konkrete anbefalinger og værktøjer til, hvordan virksomheden kan styrke sin sikkerhed og dermed blive mere attraktiv over for kunder og samarbejdspartnere.

4. Udfordringer med at øge it-sikkerheden blandt virksomheder

Analysen har vist, at 40 pct. af danske SMV'er ikke har den rette balance mellem deres it-sikkerhedsniveau og deres risikoprofil. Dette afsnit vil i forlængelse heraf se på hvilke begrænsninger eller udfordringer, som virksomhederne oplever i forhold til at øge deres digitale sikkerhedsniveau.

Samlet set har 37 pct. af SMV'erne angivet, at de har oplevet begrænsninger eller udfordringer med at øge it-sikkerhedsniveauet i virksomheden, som illustreret i figur 13. Dette gælder for 38 pct. af de store virksomheder med 250+ ansatte. Et interessant resultat fra figur 13 er, at der ikke findes betydelig forskel på virksomhedsstørrelse og andelen af virksomheder, der oplever udfordringer med at øge it-sikkerhedsniveauet.

Der skal gøres opmærksom på, at virksomhederne er blevet spurgt til, om de har oplevet begrænsninger eller udfordringer for at øge it-sikkerhedsniveauet i virksomheden i 2022 (referenceperioden er således det forgange år).



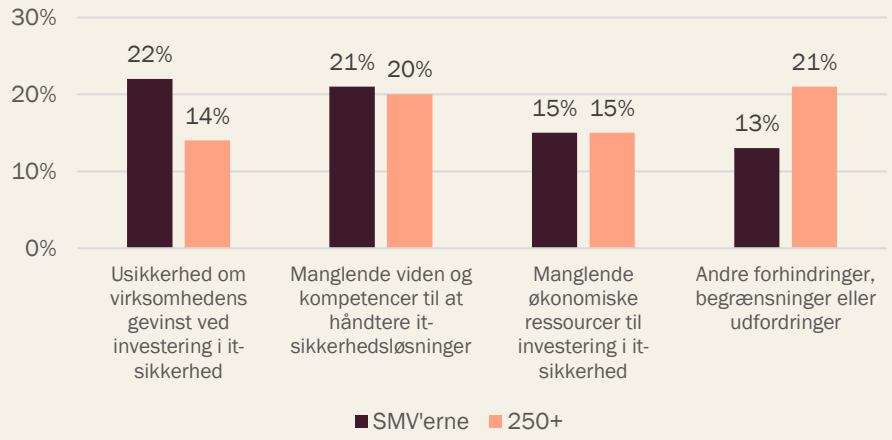
Kilde: Egne beregninger baseret på data indsamlet af Danmarks Statistik 2023 (ITAV)
Anm: Figuren er baseret på spørgsmålet: "Har virksomheden i 2022 oplevet følgende begrænsninger eller udfordringer for at øge it-sikkerhedsniveauet i virksomheden?". Andelen i figuren udgøres af de virksomheder, som har svaret 'ja' til minimum én af de adspurgte udfordringer, som fremgår af figur 14.

Der findes imidlertid forskel på, *hvilke* begrænsninger eller udfordringer som virksomhederne oplever alt efter virksomhedsstørrelse, jf. figur 14 nedenfor. Mens den største begrænsning for SMV'erne er 'usikkerheden om virksomhedens gevinst ved at investere i it-sikkerhed', oplever de store virksomheder især 'andre forhindringer, begrænsninger eller udfordringer´. Det er desværre ikke muligt at angive, hvad denne andet-kategori dækker over, da det ikke har været muligt for virksomhederne at uddybe deres besvarelser. En tidligere analyse af Digital sikkerhed i danske SMV'er viser dog, at de store virksomheder med 250+ ansatte i høj grad oplever 'manglende tilslutning eller opbakning fra medarbejderne' som udfordring for at øge deres it-sikkerhedsniveau[12] (en svarkategori som ikke indgår i dette års spørgeskema).

Figur 14 viser endvidere, at relativt mange SMV'er (21 pct.), såvel som store virksomheder (20 pct.) peger på 'manglende viden og kompetencer til at håndtere it-sikkerhedsløsninger' samt 'manglende økonomiske ressourcer til at investere i it-sikkerhed' (15 pct.) som begrænsninger eller udfordringer i forhold til at øge deres it-sikkerhed.

[12] Digitaliseringsstyrelsen (2022): Digital sikkerhed i danske SMV'er, side 15

Figur 14: Oplevede udfordringer for at øge it-sikkerhedsniveauet



Kilde: Egne beregninger baseret på data indsamlet af Danmarks Statistik 2023 (ITAV)
Anm.: Figuren er baseret på spørgsmålet: "Har virksomheden i 2022 oplevet følgende begrænsninger eller udfordringer for at øge it-sikkerhedsniveauet i virksomheden?". Samlet set har 37 pct. af SMV'erne og 38 pct. af de store virksomheder svaret 'ja' til minimum én udfordring, jf. figur 13 ovenfor.

I sammenligning med tidligere års analyser ser vi en relativ stor stigning i andelen af SMV'er, der oplever begrænsninger eller udfordringer med at øge it-sikkerheden fra 17 pct. i undersøgelsen i 2021 til 37 pct. i undersøgelsen fra 2023. Resultaterne kan dog ikke sammenlignes én til én, da svarkategorierne har ændret sig mellem årene[13].

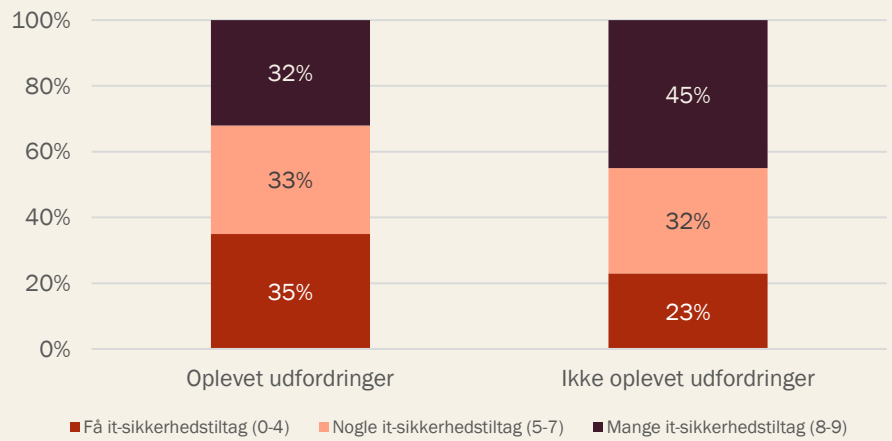
Én svarkategori går dog igen i 2021 og 2023, nemlig udfordringen omkring 'manglende viden og kompetencer til at håndtere it-sikkerhedsløsninger'. Her viser resultaterne en stigning i andelen af SMV'er, der oplever denne udfordring fra 12 pct. i 2021 til 21 pct. i 2023 (mens udfordringen har ligget stabilt på 20 pct. for de store virksomheder i begge år). Én forklaring på denne stigning kan være, at SMV'erne i højere grad er begyndt at arbejde med digital sikkerhed og dermed også oplever et større behov for (og udfordring med) at ansætte medarbejdere med den rette viden og kompetencer inden for it-sikkerhed. Det kan også skyldes, at jo mere virksomhederne arbejder med digital sikkerhed og kompleksiteten heri, desto mere bliver de bekendte med, hvad de ikke ved.

[13] Spørgsmålsformuleringen omkring udfordringer og begrænsninger blev ændret i 2020, og der ikke blev spurgt til oplevede udfordringer i 2022. Det bedste sammenligningsgrundlag er således mellem undersøgelserne indsamlet i 2021 og 2023. Her var svarkategorierne dog forskellige på nær andet-kategorien og mangel på viden og kompetencer-kategorien.

4.1 Virksomheder, der oplever udfordringer med at øge deres it-sikkerhedsniveau, anvender færre it-sikkerhedstiltag

Figur 15 viser, at de virksomheder som har oplevet begrænsninger eller udfordringer med at øge deres it-sikkerhedsniveau – ikke overraskende – også anvender færre it-sikkerhedstiltag sammenlignet med de virksomheder, som ikke har oplevet en eller flere begrænsninger eller udfordringer.

Figur 15: Sammenhæng mellem oplevede udfordringer og brug af it-sikkerhedstiltag



Kilde: Egne beregninger baseret på data indsamlet af Danmarks Statistik 2023 (ITAV)

4.2 Hjælp til at styrke virksomheders digitale sikkerhed

For virksomheder, der efterspørger konkrete råd og værktøjer til at øge deres digitale sikkerhed, er der hjælp at hente på **Sikkerdigital.dk**, som kort uddybet i nedenstående tabel.

Tabel: Overblik over udvalgte tilbud til virksomheder på Sikkerdigital.dk

Syv gode råd	Test og værktøjer	Læs om NIS 2
På Sikkerdigital.dk findes syv gode råd om it-sikkerhed, som er et godt sted at starte for virksomheder, der ønsker at styrke sikkerheden Læs de syv råd her	På Sikkerdigital.dk findes en række gratis online testværktøjer, som eksempelvis hjælper virksomhederne med at få overblik over deres værdifulde systemer og data, og giver anbefalinger til forbedringer af sikkerheden tilpasset risikoprofil mv. Se test og værktøjer her	NIS 2-direktivet har til formål at skabe et højere og mere ensartet cybersikkerhedsniveau på tværs af EU. Med den kommende NIS 2-lov, der implementerer NIS 2-direktivet, stilles der bl.a. krav til, hvad de omfattede myndigheder og virksomhederne skal gøre for at styrke modstandsdygtigheden mod cyberangreb. Læs om lovforslaget og hvad det betyder for de omfattede virksomheder. Læs om NIS 2 her

Til de virksomheder, der foretrækker den personlige kontakt, er det muligt at ringe til Cyberhotline for digital sikkerhed. Cyberhotlinen er oprettet til borgere og virksomheder, som ønsker vejledning om, hvordan de bliver mere digitalt sikre samt håndterer og forebygger digital svindel og cyberangreb. Og så kan virksomheder få hjælp og vejledning, hvis de står i den svære situation at være udsat for et cyberangreb. Cyberhotlinen drives af Styrelsen for Samfundssikkerhed.

Åbningstider og kontakt til cyberhotline:

- Telefonnummer: 33 37 00 37
- Ved spørgsmål og generelle hændelser er der åbent fra 8-20 på hverdage og 10-16 i weekender og på helligdage.
- Uden for åbningstid hjælpes der kun med spærring af MitID, eller hvis virksomheden er under angreb.

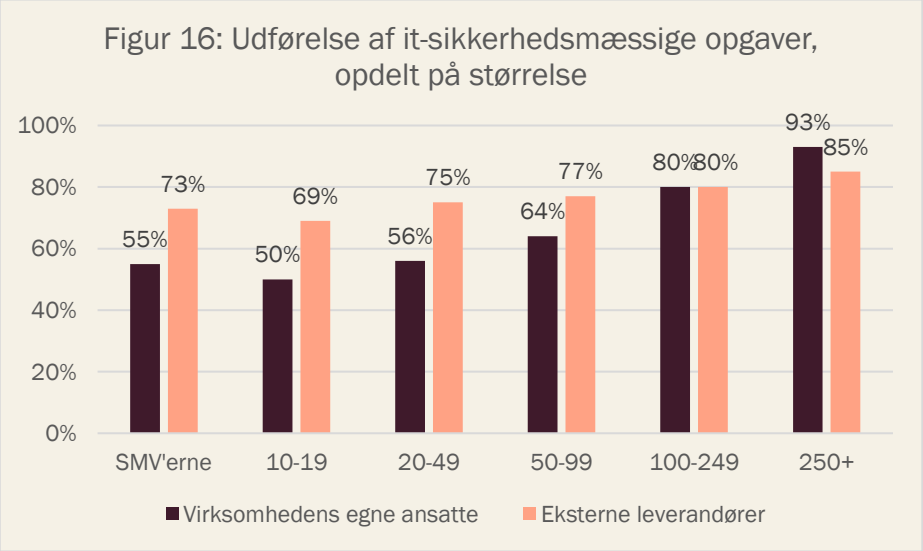
5. Varetagelse af it-sikkerhedsmæssige opgaver

Kapitel 4 har vist, at 'manglende viden og kompetencer til at håndtere it-sikkerhedsløsninger' er en relativ stor og stigende udfordring for SMV'erne. Dette afsnit vil i forlængelse heraf se på, hvem der varetager de it-sikkerhedsmæssige opgaver i virksomhederne.

5.1 Størstedelen af danske virksomheder udliciterer it-sikkerhedsmæssige aktiviteter til eksterne leverandører

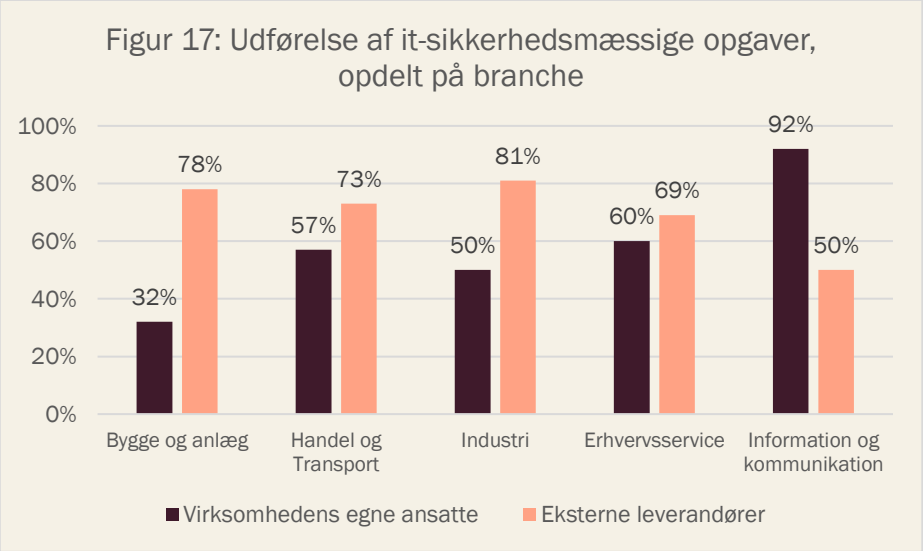
Figur 16 neden for viser, at hele 73 pct. af SMV'erne og 85 pct. af de store virksomheder udliciterer hele eller dele af de it-sikkerhedsmæssige opgaver til eksterne leverandører. Som figuren også illustrerer, er andelen, der udliciterer it-sikkerhedsmæssige opgaver, nogenlunde ens på tværs af virksomhedsstørrelse. Til sammenligning anvender blot 55 pct. af SMV'erne egne medarbejdere til at varetage it-sikkerhedsmæssige opgaver, hvilket gælder hele 93 pct. af de store virksomheder med 250+ ansatte[14]. Dette billede har været ens over årene, og kan skyldes, at de mindre virksomheder ikke har behov for eller ressourcer til at ansætte en decideret it-sikkerhedsansvarlig/it-afdeling.

[14] Dette spørgsmål er bredt formuleret og kan både tælle medarbejdere, der er ansat som it-sikkerhedsspecialister, men også ansatte, som varetager de it-sikkerhedsmæssige opgaver ved siden af andre arbejdsopgaver.



Kilde: Egne beregninger baseret på data indsamlet af Danmarks Statistik 2023 (ITAV)

Ligeledes er der en tendens til, at de mindre digitale brancher såsom 'bygge og anlæg' i højere grad benytter sig af eksterne leverandører end egne ansatte, hvorimod branchen 'information og kommunikation' i høj grad benytter sig af virksomhedens egne ansatte til at løfte de it-sikkerhedsmæssige opgaver. De konkrete resultater opdelt på branche fremgår af figur 17 nedenfor.



Kilde: Egne beregninger baseret på data indsamlet af Danmarks Statistik 2023 (ITAV)

Selvom virksomheden vælger at udlicitere hele eller dele af sin it-sikkerhed, er det fortsat vigtigt, at virksomheden forholder sig til og tager ansvar for den digitale sikkerhed - blandt andet ved at stille krav til sin leverandør. På Sikkerdigital kan virksomheder downloade et dialogværktøj, der indeholder et skema med konkrete forslag til spørgsmål, som virksomheder med fordel kan stille til sin it-leverandør.

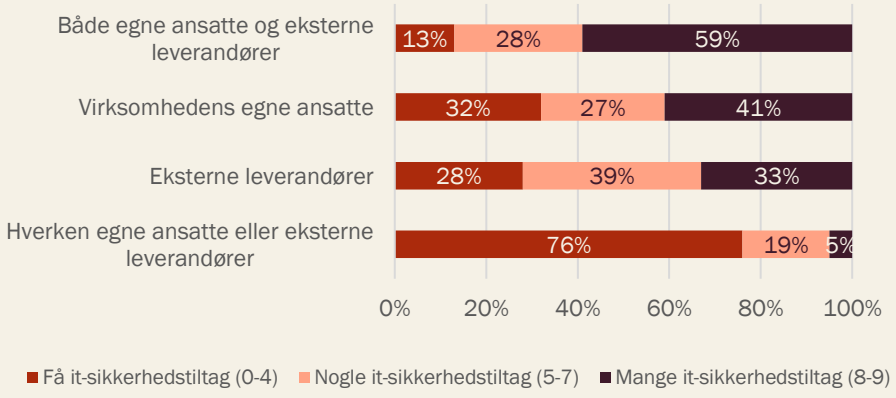
Det følgende afsnit ser på sammenhængen mellem, hvem der varetager it-sikkerheden i virksomheden, og hvor mange it-sikkerhedstiltag som virksomheden har implementeret.

5.2 Høj digital sikkerhed blandt de virksomheder, som *både* har egne ansatte og eksterne leverandører til at varetage it-sikkerheden

Samlet set har 34 pct. af SMV'erne *både* egne ansatte og eksterne leverandører til at varetage it-sikkerhedsaktiviteter, 22 pct. har *kun* eksterne leverandører, og 38 pct. har *kun* egne ansatte til at varetage it-sikkerhedsaktiviteter, mens en lille andel på 5 pct. *hverken* har egne ansatte eller eksterne leverandører ansat til at varetage it-sikkerhedsaktiviteter.

Virksomheder, der *både* benytter sig af eksterne leverandører og egne ansatte til at varetage it-sikkerhedsmæssige opgaver, anvender i gennemsnit flere it-sikkerhedstiltag end alle øvrige virksomheder (denne forskel er signifikant kontrolleret for størrelse og branche). Modsat anvender den mindre gruppe af virksomheder, der *hverken* har egne ansatte eller eksterne leverandører, langt færre sikkerhedsforanstaltninger end øvrige virksomheder, jf. figur 18.

Figur 18: Udførelse af it-sikkerhedsmæssige aktiviteter og brug af it-sikkerhedstiltag



Kilde: Egne beregninger baseret på data indsamlet af Danmarks Statistik 2023 (ITAV)

Interne såvel som eksterne kompetencer er således helt afgørende for, at den digitale sikkerhed kan løftes i virksomhederne. Og netop kompetencer er også ét af de spor, som Cybersikkerhedspagten beskæftiger sig med. Cybersikkerhedspagten er et offentlig-privat samarbejde, som sekretariatsbetjenes af Styrelsen for Samfundssikkerhed. Formålet med Cybersikkerhedspagten er at styrke sikkerhedsniveauet i danske SMV'er, og dermed bidrage til at styrke det samlede danske cyberforsvar.

Cybersikkerhedspagten skal medvirke til at sikre:

- Sammenhæng og synergi mellem eksisterende og nye SMV-rettede indsatser på cybersikkerhedsområdet
- Udveksling af data, viden og erfaringer mhp. at skabe et nationalt billede af sikkerhedssituationen for SMV'erne
- At der skabes nye samarbejder på tværs af den offentlige og private sektor om at styrke SMV'ernes muligheder for at beskytte sig mod cyberangreb

6. It-sikkerhedshændelser i danske virksomheder

Tidligere afsnit har vist, at 40 pct. af danske SMV'er ikke har et tilstrækkeligt digitalt sikkerhedsniveau, og at godt hver tredje SMV har oplevet begrænsninger eller udfordringer med at øge it-sikkerhedsniveauet i virksomheden. Dette afsnit ser nærmere på, hvilke it-sikkerhedshændelser som de danske virksomheder oplever, samt hvilke konsekvenser de kan opleve som følge af hændelserne.

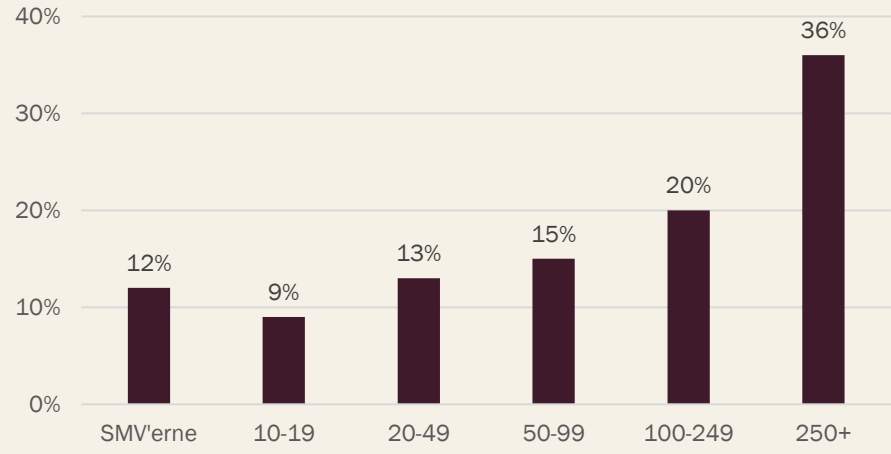
Virksomhederne er blevet spurgt til, om de har oplevet en it-sikkerhedshændelse i 2022 (dvs. at referenceperioden for it-sikkerhedshændelser er det foregående kalenderår). Eftersom både spørgsmål og dertilhørende svarkategorier vedrørende it-sikkerhedshændelser er omformuleret over årene, kan resultaterne i dette afsnit ikke sammenlignes med resultater i tidligere års analyser[15].

Det er desuden værd at bemærke, at resultaterne i dette afsnit må anses som konservative resultater, da it-sikkerhedshændelser ofte er behæftet med væsentlige "mørketal". Det skyldes blandt andet, at virksomheder ikke er forpligtet til at indrapportere alle typer af it-sikkerhedshændelser, og at mange virksomheder ikke ønsker at dele, hvis de bliver ramt af en hændelse. Der kan også være virksomheder, som slet ikke ved, at de har været udsat for en hændelse (fx hvis der er tale om spyware, der ligger gemt i virksomhedens systemer).

Samlet set har 12 pct. af SMV'erne og 36 pct. af de store virksomheder angivet, at de har oplevet en eller flere it-sikkerhedshændelser i løbet af 2022. jf. figur 19.

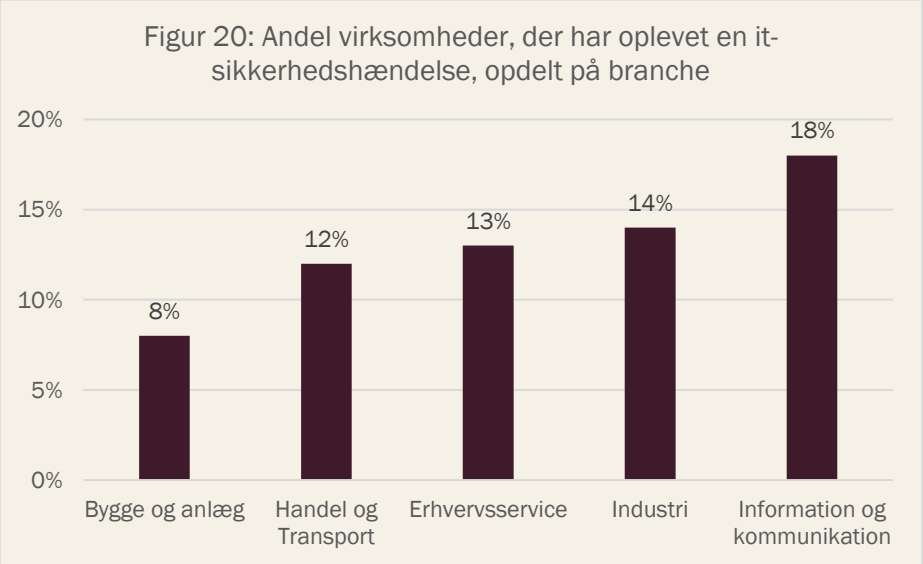
[15] I 2022-undersøgelsen var svarkategorierne fx omformuleret således at også utilsigtede it-sikkerhedshændelser indgik, herunder 'utilgængelighed af it-tjenester på grund af hardware- eller softwarefejl'.

Figur 19: Andel virksomheder, der har oplevet en it-sikkerhedshændelse, opdelt på størrelse



Kilde: Egne beregninger baseret på data indsamlet af Danmarks Statistik 2023 (ITAV)
Anm. Figur 19 er baseret på spørgsmålet: "Har virksomheden haft følgende it-sikkerhedshændelser i 2022?" Andelen udgør de virksomheder, som har svaret 'ja' til én af de listede udfordringer i figur 21.

Især branchen 'information og kommunikation' er udsat, da 18 pct. af virksomhederne i denne branche har angivet, at de var ramt af en hændelse i 2022, hvilket fx kun gælder 8 pct. procent af virksomhederne inden for branchen 'bygge og anlæg', jf. figur 20.

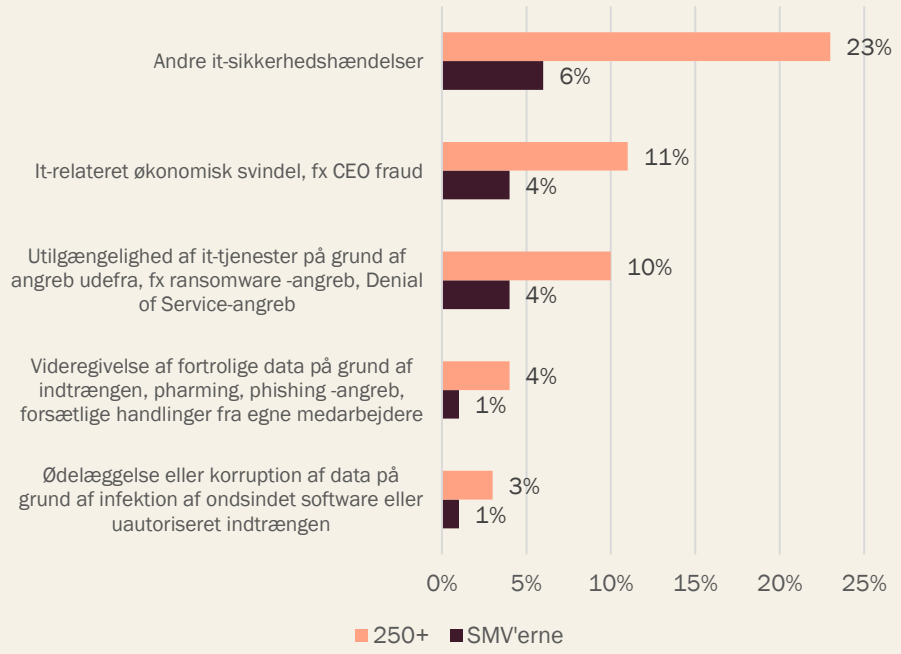


Kilde: Egne beregninger baseret på data indsamlet af Danmarks Statistik 2023 (ITAV)
Anm. Figur 20 er baseret på spørgsmålet: "Har virksomheden haft følgende it-sikkerhedshændelser i 2022?" Andelen udgør de virksomheder, som har svaret 'ja' til én af de listede udfordringer i figur 21.

Figur 21 viser, hvilke it-sikkerhedshændelser som virksomhederne har været udsat for. Som det fremgår, er det især 'andre' it-sikkerhedsoplevelser, som virksomhederne har angivet. Eftersom det ikke har været muligt for virksomhederne at uddybe deres svar, er det ikke muligt at se, hvilke 'andre' it-sikkerhedshændelser, som kategorien dækker over. Det vidner dog om, at de øvrige svarkategorier ikke er udtømmende.

Ud over 'andre' it-sikkerhedshændelser peger virksomhederne især på, at de har været udsat for it-relateret økonomisk svindel samt utilgængelighed af it-tjenester på grund af angreb udefra, fx ransomware–angreb og Denial of Service-angreb.

Figur 21: Typer af it-sikkerhedshændelser



Kilde: Egne beregninger baseret på data indsamlet af Danmarks Statistik 2023 (ITAV)
Anm. Figur 21 er baseret på spørgsmålet: "Har virksomheden haft følgende it-sikkerhedshændelser i 2022?". Virksomhederne har haft mulighed for at angive flere svarmuligheder (multible choice).

På Sikkerdigital.dk findes en række artikler om forskelige digitale trusler.

Hvad truer din virksomhed?

På Sikkerdigital.dk, kan man læse om følgende digitale trusler, samt hvordan virksomheder kan forebygge at blive ramt heraf:

- Ransomware (online afpresning)
- Phishing
- CEO-fraud (direktørsvindel)
- Faktura bedrageri
- DDoS-angreb
- Bevidste insider
- Cyberspionage

Til de virksomheder, som ønsker at få varsler om digitale sårbarheder direkte i indbakken, er det muligt at tilmelde sig **varslingstjenesten** for virksomheder. Ved at være på forkant og lukke sårbarhederne, som anbefalet i varslerne, kan virksomheder mindske risikoen for cyberangreb.

Hvad får virksomheden ud af varslingstjenesten?

Varslerne oplyser om de mest gængse sårbarheder i fx softwaresystemer, som it-kriminelle kan udnytte i forbindelse med angreb på virksomhedernes systemer.

Varslerne sendes typisk samlet i en ugentlig e-mail til de tilmeldte virksomheder. Varslerne kan fås i to versioner:

- En uddybet, mere teknisk version, målrettet virksomheder, der selv arbejder aktivt med egen it-sikkerhed.
- En forenklet version, målrettet mindre virksomheder og virksomheder, der har outsourcet deres it-sikkerhed.

I forhold til resultaterne i dette afsnit, skal der afslutningsvist gøres opmærksom på, at forskellige undersøgelser har vist et bredt spænd i andelen af danske virksomheder, som har oplevet en it-sikkerhedshændelser i 2022 fra 12 pct. til 51 pct.[16], hvilket blandt andet kan skyldes forskellige spørgsmålsformuleringer, målgrupper og rekrutteringsmetoder i de forskellige undersøgelser. Det er ikke kun forekomsten af it-sikkerhedshændelser, som er forbundet med stor usikkerhed. De omkostninger, som er forbundet med en it-sikkerhedshændelse er ligeledes svære at estimere. Det følgende afsnit gives et lille udpluk af de analyser, som har forsøgt herpå.

6.1 Store omkostninger forbundet med et cyberangreb

Cyberangreb kan have stor betydning for de enkelte virksomheders bundlinje, såvel som for samfundsøkonomien som helhed.

[16] Fx viser PXCs årlige cybercrime survey fra 2022, at 51 pct. af de danske virksomheder var udsat for mindst én sikkerhedshændelse inden for det seneste år. Et andet eksempel er en analyse fra Alm. Brand i 2023 som viser, at 25 pct. af de små virksomheder med 0-20 ansatte har haft et brud på it-sikkerheden inden for det seneste år.

SMV:Danmark er blandt andet kommet frem til, at et ransomware-angreb vil koste 376.350 kr. alene i tabt omsætning fra e-handel for en lille virksomhed med 10-49 ansatte[17]. På baggrund af en undersøgelse blandt deres medlemsvirksomheder er Dansk Erhverv kommet frem til, at cyberangreb i gennemsnit koster danske virksomheder 160.000 kr., og at de samlede årlige omkostninger for it-relateret kriminalitet mod danske virksomheder er minimum 4 mia. kr. om året[18].

Eksempler på omkostninger som følge af cyberangreb

Omkostninger som følge af et angreb kan eksempelvis forårsages af:

- Forretningsforstyrrelser og omsætningstab
- Tyveri af kundedata og forretningshemmeligheder
- Skade på omdømme (omkostninger ved at miste kunder)
- Omkostninger til inddragelse af eksterne it-sikkerheds eksperter
- Omkostninger til genoprettelsen af driften
- Omkostninger til håndtering af bruddet, fx krise kommunikation
- Omkostninger ved vellykket digital afpresning eller CEO-fraud
- Juridiske omkostninger

6.2 Afhængighed af centrale it-systemer og opbevaring af data i danske virksomheder

Konsekvenserne ved en it-sikkerhedshændelse kan således være mange, fx at virksomhedens it-systemer skades eller gøres utilgængelige i kortere eller længere tid.

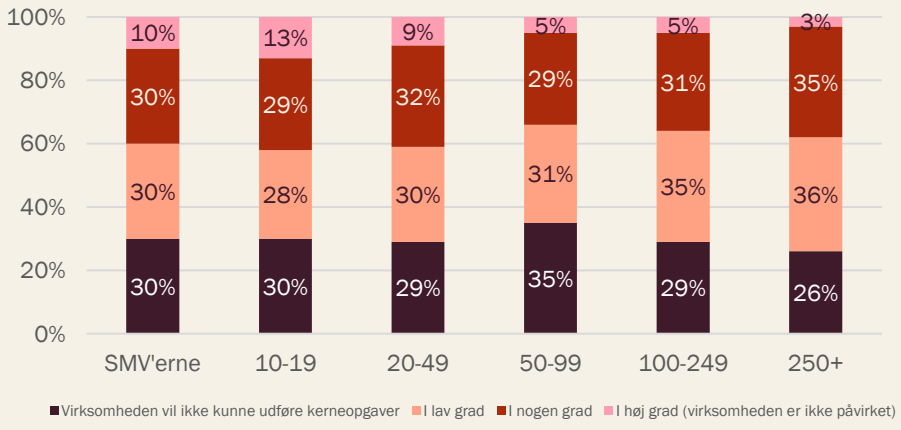
[17] SMV:Danmark (2021): Cyberangreb kan blive en dyr omgang for SMV'erne
[18] Dansk Erhverv (2019): Tryghed i en verden fuld af data

Eksempler på IT-systemer i virksomheder

Nogle af de mest almindelige it-systemer, som virksomheder er afhængige af i deres daglige drift er fx ordresystem, lagersystem, økonomisystem, kommunikationsmidler, kundedatabaser, intranet osv.

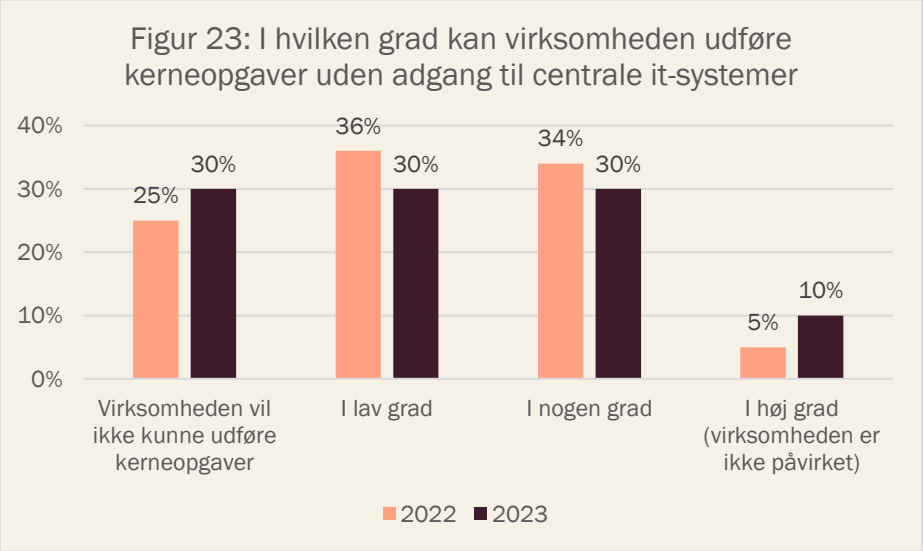
Figur 22 viser, at 60 pct. af SMV'erne og 62 pct. af de store virksomheder *slet ikke* eller kun *i lav grad* vil kunne udføre virksomhedens kerneopgave uden adgang til interne centrale it-systemer. Her er det interessant at bemærke, at der ikke findes en forskel på virksomhedsstørrelse. Alle virksomheder – store som små – er i høj grad afhængige af virksomhedens interne it-systemer og vil dermed opleve store konsekvenser for kerneopgaverne ved utilgængelighed af centrale it-systemer.

Figur 22: I hvilken grad kan virksomheden udføre kerneopgaver uden adgang til centrale it-systemer



Kilde: Egne beregninger baseret på data indsamlet af Danmarks Statistik 2023 (ITAV)

Resultaterne i figur 23 nedenfor viser, at andelen af virksomheder, der *slet ikke* ville kunne udføre kerneopgaver uden adgang til deres it-systemer, er steget fra 25 pct. i 2022 til 30 pct. i 2023. Omvendt findes der også en stigning i andelen af virksomheder, som angiver, at de ikke vil være påvirket uden adgang til deres it-systemer.



Kilde: Egne beregninger baseret på data indsamlet af Danmarks Statistik 2023 (ITAV)

En anden konsekvens ved It-sikkerhedshændelser kan være, at virksomhedens data skades, gøres utilgængelige eller udsættes for uautoriseret adgang.

Eksempler på centrale virksomhedsdata

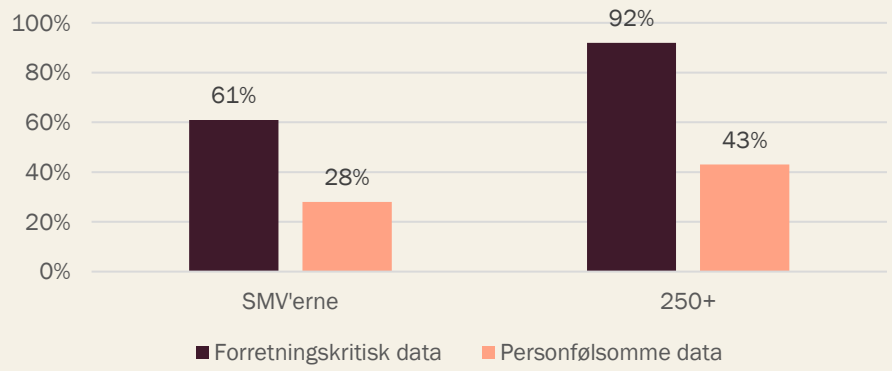
Virksomhedens systemer kan lægge inde med **forretningskritisk data** som eksempelvis forretningshemmeligheder eller kundedatabaser eller **persondata med særlig risiko,** dvs. følsomme persondata, CPR-numre osv.

Figur 24 viser andelen af virksomheder, der angiver, at de har systemer, som behandler eller opbevarer data, som er forretningskritiske (fx forretningshemmeligheder og kundedatabaser), og/eller som har følsomme persondata med særlig risiko (fx CPR-numre mv.), som ikke omhandler virksomhedens egne ansatte.

Selvom resultaterne viser, at de store virksomheder i højere grad end SMV'erne behandler de respektive datatyper, viser resultaterne også, at langt over halvdelen af SMV'erne (61 pct.) har systemer, som behandler eller opbevarer forretningskritisk data, ligesom godt en fjerdel af SMV'erne (28 pct.) har systemer, som opbevarer eller behandler følsomme persondata. SMV'erne er således også i høj grad sårbare over for angreb, hvor

uvedkommende aktører kan få adgang til virksomhedens forretningskritiske- eller personfølsomme data.

Figur 24: Andel virksomheder som opbevarer og/eller behandler forretningskritisk eller personfølsomme data



Kilde: Egne beregninger baseret på data indsamlet af Danmarks Statistik 2023 (ITAV)

Med det nye værktøj Systemoverblikket (på Sikkerdigital.dk) får virksomheder et overblik over deres systemer og data og bliver guidet til, hvordan de kan prioritere og øge cybersikkerheden i centrale it-systemer i netop deres virksomhed.

Hvad får virksomheder ud af systemoverblikket?

Med Systemoverblikket vil virksomheden på ca. 10 minutter blive bedt om atforholde sig til en række spørgsmål, som omhandler:

- Kortlægning af virksomhedens systemer og data
- Vurdering af virksomhedens systemer og data
- Samt spørgsmål om virksomhedens IT-drift og sikkerhed

Ud fra besvarelserne får virksomheden et skræddersyet overblik med konkrete og målrettede anbefalinger til de systemer og data, som er angivet.

7. Digital ansvarlighed: Dataetik og digital sikkerhed

Dette kapitel handler om sammenhæng mellem virksomheders arbejde med dataetik og digital sikkerhed under den fælles betegnelse "digital ansvarlighed".

Digital ansvarlighed handler ikke kun om at skabe digitalt sikre produkter, men også om ansvarlig brug og indsamling af data. Dermed dækker digital ansvarlighed både over digital sikkerhed og dataetik. Flere steder ses initiativer, hvor dataetik og digital sikkerhed tænkes sammen. Et eksempel er D-mærket, som er en dansk mærkningsorden for it-sikkerhed og ansvarlig dataanvendelse, der bidrager til at tydeliggøre, hvilke virksomheder der udviser digital ansvarlighed[19].

Dette afsnit handler derfor om sammenhæng mellem virksomheder, der arbejder med dataetik, og digital sikkerhed. Først introduceres begrebet dataetik.

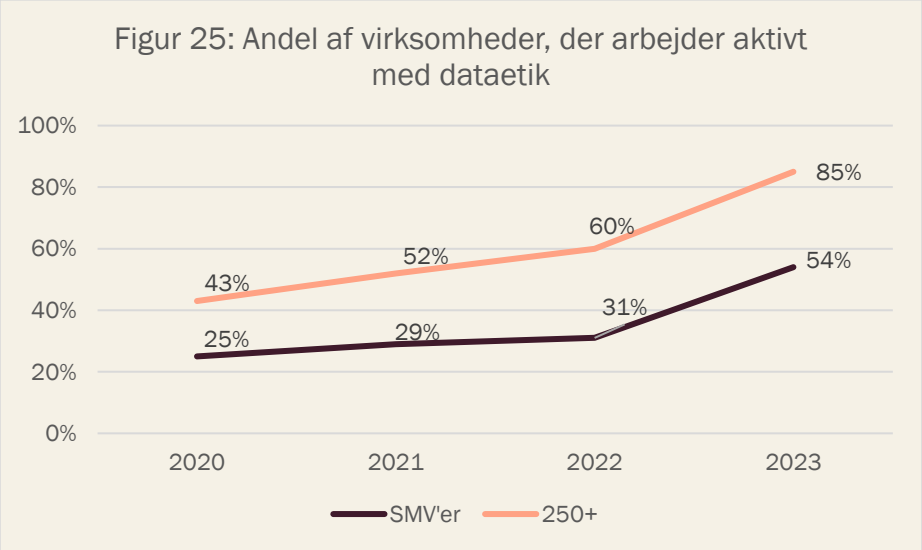
Hvad er dataetik?
Dataetik indebærer, at virksomheden aktivt sikrer en ansvarlig balance mellem på den ene side teknologi og brug af data, og på den anden side, borgernes grundlæggende rettigheder, retssikkerhed og grundlæggende samfundsmæssige værdier.

Det betyder, at dataetik for den enkelte virksomhed ikke blot handler om overholde lovgivning, men at afveje forskellige hensyn, som taler for eller imod en konkret databehandling.

[19] For at opnå D-mærket skal virksomhederne både leve op til en række kriterier inden for it-sikkerhed og ansvarlig dataanvendelse, der passer til deres risikoprofil.

Figur 25 viser andelen af virksomheder, der har svaret, at de arbejder med dataetik. På samme måde som med digital sikkerhed, har virksomhedens størrelse betydning for virksomhedernes arbejde med dataetik. Som figuren illustrerer, er der markant flere store virksomheder end SMV'er, der arbejder aktivt med dataetik.

Figuren viser desuden en positiv udvikling i virksomhedernes arbejde med dataetik fra 2020 til 2023 for begge typer af virksomheder. Det bemærkes, at udviklingen i andelen af virksomheder, der arbejder med dataetik fra 2022 til 2023, blandt andet kan skyldes en ændring i spørgsmålsopsætningen mellem de to år, jf. anmærkning til figuren.



Kilde: Egne beregninger baseret på data indsamlet af Danmarks Statistik 2020-2023 (ITAV)
Anm: I 2023 blev alle virksomheder bedt om at angive "Arbejder virksomheden aktivt med dataetik på følgende måder?" med svarmulighederne: 1) virksomheden har udarbejdet en politik på området, 2) virksomheden skaber awareness ved at oplyse medarbejdere om dataetikmedarbejde, 3) andre områder (ja/nej). Til og med 2022 blev virksomhederne først spurgt til, om de arbejder med dataetik (ja/nej), hvorefter kun dem, som havde svaret "ja", blev bedt om at angive på hvilke måder.

7.1 Sammenhæng mellem SMV'ers arbejde med dataetik og digital sikkerhed

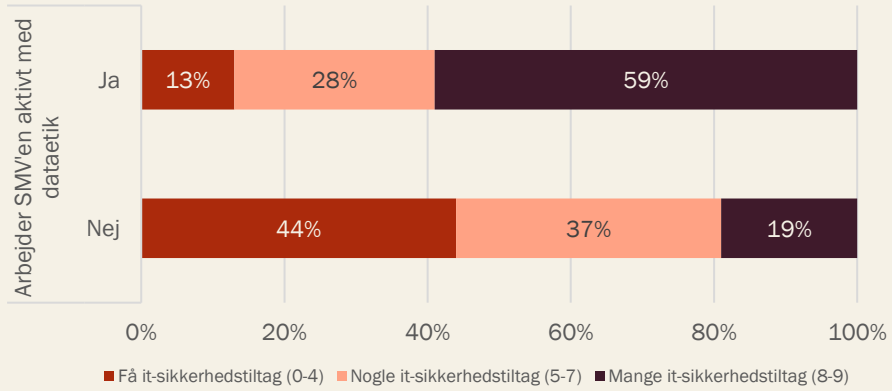
Nedenfor illustreres i figur 26, hvordan SMV'ers svar på, hvorvidt de arbejder aktivt med dataetik, hænger sammen med, hvor mange tekniske it-sikkerhedstiltag de anvender. Her ses en tydelig tendens til, at SMV'ers fokus på digital sikkerhed hænger sammen med et øget fokus på dataetik - og vice versa.

Blandt de SMV'er, som har svaret, at de arbejder aktivt med dataetik, har 13 pct. svaret at de anvender få (0-4) it-sikkerhedstiltag, mens 59 pct. svarer, at de anvender mange (8-9) it-sikkerhedstiltag.

Blandt de SMV'er, der har svaret, at de *ikke* arbejder aktivt med dataetik, har hele 44 pct. angivet, at de har anvendt få (0-4) it-sikkerhedstiltag, og 19 pct. svarer, at de anvender mange (8-9) it-sikkerhedstiltag.

Sammenhængen mellem SMV'er, der arbejde med dataetik og digital sikkerhed, er statistisk signifikant ved kontrol for virksomhedsstørrelse og branche.

Figur 26: Sammenhæng mellem dataetik og digital sikkerhed



Kilde: Egne beregninger baseret på data indsamlet af Danmarks Statistik 2023 (ITAV)

.

8. Metode

Resultaterne i denne analyse er udregnet baseret på undersøgelsen 'IT-anvendelse i virksomhederne' (ITAV), som er en årlig stikprøvebaseret spørgeskemaundersøgelse gennemført af Danmarks Statistik. Data indsamles via digital indberetning. Datavalidering sker i form konsistenskontroller i det digitale skema, samt ved efterfølgende fejlsøgning og eventuel genkontakt til indberetter.

Denne analysen er gennemført på grundlag af den nyeste tilgængelige ITAV-undersøgelse på forskerserveren, som blev indsamlet i 2023. I 2023 indgik 4.557 virksomhedsbesvarelser i undersøgelsen ud af en samlet population på 18.213 virksomheder. Virksomhederne i undersøgelsen har minimum 10 årsværk og tilhører de private, ikke-finansielle byerhverv.

I analysen benyttes vægtet data således, at stikprøven afspejler den fulde population af virksomheder med minimum 10 årsværk inden for de private, ikke-finansielle byerhverv. Det er muligt at læse mere om indsamlingsmetoden samt præcision og pålidelighed på Danmarks Statistiks hjemmeside.

Ved læsning af analysens resultater skal der tages forbehold for, at cybertrusler og digital sikkerhed er områder i hastig udvikling, hvorfor der kan være sket en del på området siden dataindsamlingen i foråret 2023. Særligt i lyset af, at der ved flere spørgsmål – fx hvad angår it-sikkerhedshændelser – spørges til situationen i 2022.

Det skal herudover bemærkes, at undersøgelsens data er baseret på selvrapporterede besvarelser fra virksomhederne. Selvevaluering siger noget om udfylderens egen opfattelse af fx deres digitale sikkerhed, hvilket kan variere fra deres reelle niveau. Dette er dog en metodisk udfordring i samtlige analyser, der baserer sig på selvrapporterede svar. I denne undersøgelse mindskes denne udfordring ved, at besvarelserne er anonyme, således at virksomhedens svar, og dermed sikkerhedsniveau, ikke er tilgængelige for kunder, leverandører, samarbejdspartnere osv. Herudover er spørgsmålene formuleret meget konkrete, så der er mindst muligt overladt til svarpersonens egen fortolkning. Fx bliver der spurgt til implementeringen af konkrete tekniske it-sikkerhedstiltag (fx om virksomheden gennemfører backup af data), frem for om virksomheden har et 'tilstrækkeligt' digitalt sikkerhedsniveau.

8.1 Måling af tekniske og essentielle it-sikkerhedstiltag

Til afdækning af virksomhedernes brug af tekniske sikkerhedstiltag anvendes de ni nedenfor listede it-sikkerhedsforanstaltninger. Alle spørgsmålene besvares med ja/nej og der måles således ikke på intensiteten, eller i hvilken grad virksomhederne benytter den givende teknologi. Analysen siger således intet om, hvorvidt de valgte teknologier eller sikkerhedstiltag benyttes korrekt og i tilstrækkelig grad. Blot om de benyttes eller ej.

Tekniske it-sikkerhedstiltag

Bruger virksomheden følgende it-sikkerhedsmæssige foranstaltninger?

- Stærke adgangskoder til autentificering. Dvs. minimumslængde på 12 blandede karakterer og at koden ikke bruges flere steder.
- Systematisk opdatering af software (inkl. styresystemer).
- Kryptering af data, filer eller e-mails.
- Backup af data til en alternativ geografisk placering. Herunder backup som cloud computing service.
- Adgangskontrol til netværk. Fx styring af brugerrettigheder i virksomhedens netværk
- VPN (virtuelt privat netværk). VPN-teknologi skaber en sikker forbindelse til udveksling af data via internettet.
- Lagring af logfiler. Fx til analyse efter it-sikkerhedshændelser.
- Risikoanalyse. Periodevis vurdering af sandsynlighed og konsekvenser for it-sikkerhedsmæssige hændelser.
- Tests af It-sikkerhed. Fx penetrationstest, test af it-sikkerhedsalarmer og backup systemer samt evaluering af it-sikkerhedsmæssige forhold.

De ni ovenstående it-sikkerhedstiltag skal *ikke* ses som en udtømmende liste af it-sikkerhedstiltag, men derimod en liste med mere basale tiltag, som er gode at overveje for en stor andel af virksomhederne. Virksomheder med en høj risikoprofil må således forventes at gøre brug af yderligere it-sikkerhedstiltag.

Foruden måling af de enkelte sikkerhedstiltag er der i analysen udviklet et samlet indeks, som måler virksomhedernes brug af de ni tekniske it-sikkerhedstiltag. Dette indeks er bygget op omkring, hvor mange sikkerhedsforanstaltninger virksomhederne anvender. Der ses på antallet af foranstaltninger, fordi der ikke foreligger en entydig definition på, hvilke der er vigtigst for virksomhederne. I denne analyse er de ni sikkerhedstiltag opdelt i følgende tre kategorier: få, nogle og mange tekniske it-sikkerhedsforanstaltninger pba. følgende operationalisering:

Få it-sikkerhedstiltag	Nogle it-sikkerhedstiltag	Mange it-sikkerhedstiltag
Brug af 0-4 it-sikkerhedstiltag + virksomheder, der ikke har implementeret de to essentielle sikkerhedstiltag	Brug af 5-7 it-sikkerhedstiltag. På nær virksomheder, der ikke har implementeret de to essentielle sikkerhedstiltag	Brug af 8-9 it-sikkerhedstiltag. På nær virksomheder, der ikke har implementeret de to essentielle sikkerhedstiltag

Essentielle it-sikkerhedstiltag

To it-sikkerhedstiltag anses som værende helt centrale[20], ligesom de også indgår i langt de fleste anbefalinger for it-sikkerhed. Disse sikkerhedstiltag er 'Backup af data' og 'Systematisk opdatering af software'. En backup-procedure gør det muligt for virksomheden at få sine systemer relativt hurtigt op at køre igen efter et eventuelt sikkerhedsangreb. Samtidig er systematisk opdatering af software central for virksomhedens sikkerhed, da systemer og programmer løbende repareres for fejl og "sikkerhedshuller", og derved reduceres muligheden for digitale sikkerhedsangreb. Disse to sikkerhedsforanstaltninger er derfor udvalgt til at 'diskvalificere' en virksomheds digitale sikkerhedsniveau. Det vil sige, at virksomheden automatisk defineres med et lavt digitalt sikkerhedsniveau, uanset hvilket digitalt sikkerhedsniveau denne virksomhed måtte have, hvis virksomheden mangler ét af de to centrale sikkerhedstiltag. Dette er i tråd med en tidligere analyse, som Deloitte har udarbejdet[21]. De to sikkerhedstiltag (backup af data og systematisk opdatering af software) rapporteres som 'essentielle sikkerhedstiltag' igennem rapporten.

8.2 Måling af digitalt sikkerhedsniveau og risikoprofil

I det følgende beskrives metoden til at indeksere de danske SMV'ers digitale sikkerhedsniveau og risikoprofil samt matchet mellem dem. Den bygger på en metode udviklet af PwC.

[20] Monitor Deloitte for Erhvervsstyrelsen (2018): IT-sikkerhed og datahåndtering i danske SMV'er.
[21] Monitor Deloitte for Erhvervsstyrelsen (2018): IT-sikkerhed og datahåndtering i danske SMV'er.

Metodikken står også beskrevet i tidligere "Digital Sikkerhed i danske SMV'er" (2021 og 2022), men genbeskrives for gennemsigtighed og grundet forskelle i spørgsmålsformuleringer.

Derfor vil store dele af metodens beskrivelse være ensartet, men vil adskille sig på visse punkter. Forskellene mellem de to indeks vil blive kommenteret for sin potentielle påvirkning på sammenlignelighed.

Sammenlignelighed mellem it-sikkerhedsniveau/risikoprofil-tal 2022 og 2023 samt metodiske forbehold

Metoden bygger på et overordnet framework, som er beskrevet nedenfor, hvor en række spørgsmål samlet udgør et mål for virksomhedernes it-sikkerhedsniveau og deres risikoprofil, med en mulighed for at sammenholde disse to. Årets tal bruger samme overordnede framework, og bruger samme metode som de seneste to år, mens nogle af spørgsmålene, også kaldet indikatorerne, varierer en smule.

Variationer i spørgsmålsformuleringer kan påvirke respondenters svar. Der er dog tale om relativt små variationer i spørgsmålsformuleringer mellem årets og sidste års rapport.

Den præcise effekt af disse variationer er imidlertid svær præcist at vurdere. Som nævnt, er det de samme fænomener som måles, men de måles med små variationer i indikatorerne. Der skal derfor tages et forbehold herfor, når tallene sammenlignes på tværs af årene.

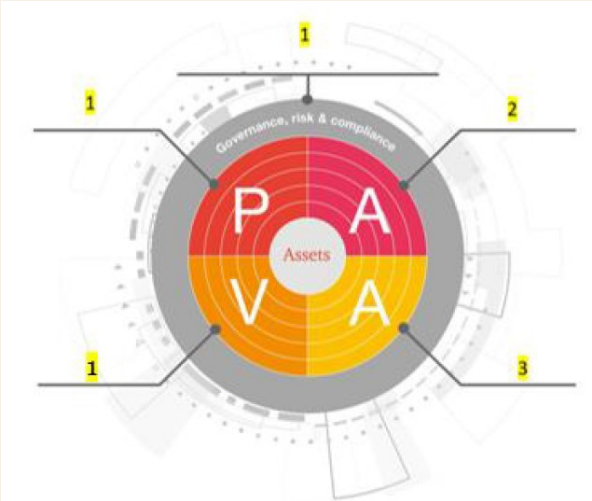
Metode og fremgangsmåde

Indekset for SMV'ernes it-sikkerhedsniveau baserer sig på spørgsmål, der siger noget om, hvilke sikkerhedstiltag SMV'erne har implementeret – fx i hvilken grad virksomhedens ledelse er inde over beslutninger om it-sikkerheden, samt om virksomheden anvender en række tekniske it-sikkerhedstiltag, fx backup af data. Indekset for SMV'ernes risikoprofil baserer sig på spørgsmål, der siger noget om SMV'ernes konsekvensniveau og sandsynligheden for, at de oplever en hændelse. I forhold til at vurdere matchet mellem SMV'ernes sikkerhedsniveau og deres risikoprofil anvendes niveauerne "lav", "middel" og "høj" til at inddele SMV'erne i tre typer. Hvis fx både sikkerhedsniveau og risikoprofil er middel, vurderes virksomheden til at have et tilpas it-sikkerhedsniveau.

I de følgende afsnit gives en detaljeret redegørelse for den metodiske fremgangsmåde for hver af de to indeks, og matchet mellem disse.

It-sikkerhedsniveau

SMV'ernes it-sikkerhedsniveau vurderes ud fra otte spørgsmål inden for emnerne Governance, Processer, Adfærd, Validering og Arkitektur, jf. PwC's PAVA-model nedenfor.



PAVA-modellen benyttes til at tildele spørgsmålene forskellig vægtning. Vægtningen er udtrykt i en sårbarhedseffekt fra 1-3, hvor 3 er den største sårbarhedseffekt, og 1 er den laveste sårbarhedseffekt. Vægtningen er baseret på en betragtning om, at en svaghed i sikkerhedstiltag i de forskellige områder, udgør en forskelligartet effekt. Således vil sårbarheder inden for fx Arkitektur (kategori 3). påvirke den reelle sikkerhed i højere grad end fx sårbarheder inden for Governance (kategori 1).

Hvert spørgsmål har også fået tildelt en pointscore, som går fra 0 til 5 – baseret på spørgsmålets svarmulighed. De otte udvalgte spørgsmål samt deres scorer og vægt fremgår af tabellen nedenfor.

#	Spørgsmål	Score	Vægt
	Governance, risk & compliance		
1	I hvilket omfang tager virksomhedens øverste ledelse og/eller bestyrelse stilling til virksomhedens it-sikkerhedsmæssige aktiviteter	0-5	1
2	I hvilken grad stiller virksomheden krav om it-sikkerhed til eksterne it-leverandører om fx behandling af data, it-sikkerhedsforanstaltninger (fx backup af data) og/eller løbende dokumentation om it-sikkerhed?	0-5	1
3	Har virksomheden i 2020 tilbudt opkvalificering af it-færdigheder til følgende: a) it-specialister, b) øvrige ansatte.	0-5	1

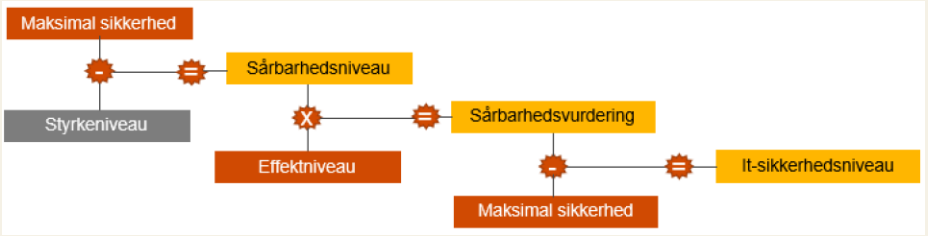
#	Spørgsmål	Score	Vægt
	Processer		
4	Hvem udførte virksomhedens it-funktioner i 2021? (egne ansatte eller eksterne leverandører)	0-5	1
5	Bruger virksomheden følgende it-sikkerhedsmæssige foranstaltninger: risikoanalyse?	0-5	1
	Validering		
7	Har virksomheden haft følgende it-sikkerhedshændelser i 2022? a) Utilgængelighed af it-tjenester på grund af angreb udefra, fx ransomware-angreb, Denial of Service-angreb, b) Ødelæggelse eller korruption af data på grund af infektion af ondsindet software eller uautoriseret indtrængen, c) Videregivelse af fortrolige data på grund af indtrængen, phrarming, phishing-angreb, forsætlige handlinger fra egne medarbejdere, d) it-relateret økonomisk svindel, e) Andre it-sikkerhedshændelser.	1-4	1
	Arkitektur		
8	Bruger virksomheden følgende it-sikkerhedsmæssige foranstaltninger? a) stærke adgangskoder til autentificering, b) systematisk opdatering af software, c) kryptering af data, filer eller e-mails, d) backup af data til en alternativ geografisk placering, e) adgangskontrol til netværk, f) VPN (virtuelt privat netværk), g) lagring af log-filer h) test af it-sikkerhed	0-5	3

Forskelle mellem spørgsmål i 2022 og 2023: Der er små forskelle i spørgsmålsformuleringerne i sikkerhedsniveau-indekset fra undersøgelsen i 2022 til 2023. Der er dog tale om minimale forskelle. For eksempel er spørgsmålet vedrørende krav til eksterne gået fra at være et ja/nej spørgsmål til et skala spørgsmål (slet ikke, i lille grad, i nogen grad, i høj grad). Derudover er der variation i svarmulighederne hvad angår, om virksomhederne har oplevet en it-sikkerhedshændelse. I 2022 indgik også en række utilsigtede it-sikkerhedshændelser som fx "utilgængelighed af it-tjenester på grund af hardware- eller softwarefejl". Disse utilsigtede svarmuligheder indgår ikke i indekset, men

kan alligevel påvirke resultaterne. Desuden var der en andet-kategori i 2023, hvilket der ikke var i 2022. Endelig er stærke adgangskoder defineret på forskellig vis i de to år[22] .

Model for beregning af it-sikkerhedsniveau

Scoringsværdien for SMV'ernes it-sikkerhedsniveau fastlægges ved at anvende metoden i figuren nedenfor. It-sikkerhedsniveauet består af en numerisk værdi, og som det ses nedenfor, foregår der flere beregninger, før man kommer frem til et sikkerhedsniveau. Figuren er opdelt i tre farver, hvor de orange kasser er statiske værdier, og de gule farver er delresultater af beregningerne. Den grå kasse afspejler værdier, der bliver indsamlet gennem spørgeskemaet.



PAVA anvendes til at finde styrken i SMV'ernes sikkerhedstiltag. Ved at bruge PAVA vil der for hvert af områdernes sikkerhedstiltag, blive foretaget en vurdering ved anvendelse af en målestok fra 0 til 5.

Maksimal sikkerhed

Eftersom SMV'erne maksimalt kan score 5 i styrke, defineres 5 som maksimal sikkerhed.

Beregning af sårbarhedsniveau

I formlen er sårbarhedsniveauet et udtryk for afstanden fra det aktuelle styrkeniveau til den maksimale sikkerhed. Sårbarhedsniveauet består af fem værdier (én værdi for hvert PAVA-område), der fordeler sig på en skala fra 0 til 5.

Effektniveau

Der er til hvert område i PAVA-konceptet knyttet en effektværdi, som beskrevet tidligere.

[22] Definition i 2022: *Dvs. minimumslængde på 8 blandede karakterer og periodevis ændring af adgangskode.*
Definition i 2023: *Dvs. minimumslængde på 12 blandede karakterer og at koden ikke bruges flere steder*

Beregning af sårbarhedsvurdering

For at foretage en sårbarhedsvurdering tager man udgangspunkt i sårbarhedsniveau for hvert enkelt PAVA-område og ganger med det effektniveau, der dækker det enkelte område. Sårbarhedsvurderingen består af én værdi på en skala fra 0 til 5.

Beregning af it-sikkerhedsniveau

For at beregne sikkerhedsniveauet fratrækkes sårbarhedsniveauet endnu engang fra det maksimale sikkerhedsniveau, så man ender med en restværdi, der afspejler sikkerhedsniveauet.

Konvertering af it-sikkerhedsniveauet til niveauer

Scoren for it-sikkerhedsniveauet falder i intervallet 0-5, som angiver, hvor godt en virksomhed lever op til basal it-sikkerhed for SMV'er. 3 er en middelværdi, og da skalaen kun måler basal sikkerhed, vurderes det, at 3 er minimumsgrænsen for at ramme middelniveauet, og at en SMV's sikkerhedsscore skal løfte sig væsentligt over middel for at blive karakteriseret som høj.

It-sikkerhedsniveau	Niveau
< 3	Lav
3-4	Middel
> 4-5	Høj

Risikoprofil

SMV'ernes risikoscore udregnes som produktet af sandsynlighed for og konsekvens ved at blive ramt af en sikkerhedshændelse. Risikoscoren inddeles i tre intervaller, hvori virksomhederne kategoriseres som havende en lav, middel eller høj risikoprofil.

Sandsynlighedsscoren angiver, hvor sandsynligt det er, at en virksomhed udsættes for en sikkerhedshændelse, mens konsekvensscoren betegner, hvor stor en negativ påvirkning en sikkerhedshændelse kan/vil have for virksomheden. Risiko er en beregning af sandsynligheden for, at en hændelse forekommer, multipliceret med konsekvensen af hændelsen. Risikoscoren er således et udtryk for forholdet mellem sandsynligheden for og konsekvensen af, at en hændelse indtræffer.

Risikoscore = sandsynlighed x konsekvens

Metode for beregning af sandsynlighedsscore

Sandsynlighedsscoren for hver SMV vurderes i forhold til 1) sektoren, den opererer i, 2) størrelsen af virksomheden og 3) størrelsen af virksomhedens tekniske angrebsflade.

#	Spørgsmål	Score
	Sektor	
1	Sektorkoder (DB07) inddelt i sektorer efter udsathed.	1 (lidt udsat sektor) – 3 (meget udsat sektor)
	Størrelse	
2	Hvor mange fuldtidsansatte er der i virksomheden?	1 (få)-5 (mange)
	Teknisk angrebsflader	
3	Anvender virksomheden: IoT, AI, CRM/ERP software, industrirobotter, servicerobotter og/eller cloud-tjenester.	1 (få eller ingen anvendte teknologier) – 5 (de fleste af de angivne teknologier)

I forhold til spørgsmål 2 (størrelse) antages det, at flere ansatte medfører flere brugere/adgange, og i forhold til spørgsmål 3 (teknisk angrebsflade) antages det, at flere teknologier medfører en større angrebsflade. Størrelsen af virksomheden og den tekniske angrebsflade scores fra 1-5.

Tildelingen af sektorscoren beror på en ekspertvurdering fra PwC. I Danmarks Statistisk data er virksomhederne inddelt i sektorer efter DB07-nomenklaturet. DB07 er en mere findelt inddeling, hvorfor virksomhederne efterfølgende er fordelt i de sektorer PwC's ekspertvurdering angår.

Sektorerne ses nedenfor:

Sektor	Score
Anden sektor	1
Industrisektor	2
Sundhedssektor	3

Sektor	Score
Handelssektor	1
Uddannelsessektor	1
Finanssektor	3
Energisektor	3
Telesektor	3
Byggesektor	1
Transportsektor	2
Fødevaresektor	2
Drikkevandssektor	2

Forskel mellem 2022 og 2023: Mens der ikke er forskel på spørgsmålene vedr. sektor og antal ansatte mellem årene, findes der nævneværdige forskel på spørgsmålene vedr. tekniske angrebsflader. For eksempel blev der blot spurgt til, hvorvidt virksomheden anvendte AI i 2022 (ja/nej), mens der i 2023 blev spurgt ti,l om de anvender en række konkrete AI teknologier (definitionen af AI er dog den samme mellem årene). Ligeledes findes der variation i den måde hvorpå, der bliver spurgt til virksomhedens brug af CRM, hvor der i 2023 blot bliver spurgt til anvendelsen heraf, mens der i 2022 bliver spurgt til forskellige måder at anvende CRM på (kundeinformationer, markedsføring). Endelig er der også mindre ændringer i definitionen af IoT - ligesom eksempler på brug af IoT i virksomheder blev tilføjet spørgsmålet i 2023. Disse forskelle vurderes igen at kunne have en mindre effekt på de overordnede resultater.

Metode for beregning af konsekvensscore
Konsekvensen vurderes ud fra tre spørgsmål, der angiver, hvilke datatyper virksomheden ligger inde med, virksomhedens afhængighed af data, samt virksomhedens afhængighed af dens it-systemer.

#	Spørgsmål	Score
	Datatyper	

#	Spørgsmål	Score
1	Opbevarer eller behandler virksomhedens systemer persondata med særlig risiko dvs. følsomme persondata, CPR-numre mv., som ikke omhandler virksomhedens egne ansatte.	1-5
	Afhængighed af data og teknologi	
2	Opbevarer eller behandler virksomhedens systemer data, som er forretningskritiske? Fx forretningshemmeligheder eller kundedatabaser	1-5
3	I hvilken grad vil virksomheden være i stand til at udføre dens kerneopgaver, hvis virksomheden mister adgangen til centrale interne it-systemer?	1-5

Hver af de ovenstående spørgsmål scores i intervallet 1-5, på samme vis som var tilfældet sidste år. Det betyder også at flere af indikatorerne er reskalerede. Konsekvensscoren udregnes som summen af de tre spørgsmål og falder i intervallet 3-15. Der er igen kun tale om minimale forskelle i spørgsmålsformuleringerne sammenlignet med sidste års rapport.

Konvertering af risikoscore til risikoprofil
Sandsynlighedsscoren falder i intervallet 3-11, og konsekvensscoren falder i intervallet 3-15. Den lavest mulige risikoscore er 3 x 3 = 9, og den højest mulige er 11 x 15 = 165. Risikoscoren falder derfor i intervallet 9-165.

Den midterste værdi for sandsynlighedsintervallet er 7 – alle værdier herover regnes for høj sandsynlighed. Intervallet 3-7, inddeles i to intervaller af samme størrelse for lav (3-5) og middel (5-7) sandsynlighed.

Den midterste værdi for konsekvensintervallet er 9, alle værdier herover regnes for høj konsekvens. Intervallet 3-9, inddeles i to intervaller af samme størrelse for lav (3-6) og middel (6-9) konsekvens.

Middelintervallet for risikoscoren udregnes ved at gange grænseværdierne for middelintervallerne for sandsynlighed og konsekvens med hinanden – det vil sige 5 x 5 = 30 og 7 x 9=63. En risikoscore i intervallet 30-63 giver derfor en middel risikoprofil, og en risikoscore under 30 og over 63 giver henholdsvis en lav og høj risikoprofil.

Sandsynlighedsscore (3-11)	Konsekvensscore (3-15)	Risikoscore (9-165)	Risikoprofil
3-5	3-6	9-30	Lav
5-7	6-9	30-63	Middel
7-11	9-15	63-165	Høj

Match mellem it-sikkerhedsniveau og risikoprofil
SMV'erne inddeles i tre typer – de sårbare, de tilpas sikrede og de påpasselige – baseret på matchet mellem virksomhedernes it-sikkerhedsniveau og risikoprofil.

It-sikkerhedsniveau				
		Lav	Middel	Høj
Risikoprofil	Høj	De sårbare 40 pct.		
	Middel		De tilpas sikrede 48 pct.	
	Lav		De påpasselige 12 pct.	

Felterne øverst til venstre i tabellen angiver de SMV'er, der har et utilstrækkeligt it-sikkerhedsniveau i forhold til deres risikoprofil. Fx vil en SMV med et middel it-sikkerhedsniveau, men en høj risikoprofil, placere sig her. For disse SMV'er vurderes konsekvensen af en it-sikkerhedshændelse, samt sandsynligheden for, at en sådan finder sted, til at overstige det nuværende it-sikkerhedsniveau, og derfor kategoriseres de som "sårbare". Omvendt angiver felterne nederst til højre de påpasselige SMV'er – dvs. dem med et it-sikkerhedsniveau, der vurderes at overstige deres risikoprofil. Disse virksomheder har implementeret flere/mere avancerede it-sikkerhedstiltag, end hvad der vurderes tilstrækkeligt i forhold til den forventede konsekvens og sandsynlighed for en hændelse. De tilpas sikre SMV'er har et it-sikkerhedsniveau, der svarer til deres risikoprofil.