DIGITALISERINGSSTYRELSEN

Digital sikkerhed i danske SMV'er

Oktober 2023

2023

Hovedkonklusioner

Fremgang i SMV'ernes digitale sikkerhedsniveau

- SMV'erne øger fortsat deres investeringer i digital sikkerhed. I 2021 har **37 pct.** af SMV'erne øget deres investeringer i digital sikkerhed sammenlignet med 2020, hvilket er den relativt største stigning siden 2018.
- **16 pct.** af SMV'erne gennemførte *ikke* de to helt basale it-sikkerhedstiltag i 2022; opdatering af software og backup af data. Dette er en markant forbedring sammenlignet med 2021, hvor **24 pct.** af SMV'erne *ikke* gennemførte de to basale tiltag. Det er især andelen af virksomheder, der anvender backup af data, som er steget fra 2021 til 2022.
- **35 pct.** af SMV'erne har et for lavt digitalt sikkerhedsniveau set i forhold til deres risikoprofil. Igen ses der dog fremgang i forhold til **44 pct**. i det forgange år.

De helt små virksomheder (5-9 ansatte) halter fortsat efter

- Blandt de helt små virksomheder (mikrovirksomheder) med 5-9 ansatte er det blot **71 pct.** af virksomhederne, som anvender de to basale sikkerhedstiltag i 2022. Dermed er der hele **29 pct.,** som *ikke* anvender de to basale tiltag som en del af deres digitale sikkerhed. Dette gælder til sammenligning **16 pct.** blandt de øvrige SMV'er med 10-249 ansatte.
- Blandt mikrovirksomhederne findes desuden *ikke* en positiv udvikling i brug af it-sikkerhedstiltag siden den seneste undersøgelse blandt mikrovirksomhedernes digitale sikkerhed, som blev gennemført i 2019.

SMV'ernes brug af organisatoriske sikkerhedstiltag

- Blot **54 pct.** af SMV'erne gennemfører dokumentation om forholdsregler, aktiviteter og procedurer vedr. it-sikkerhed. Blandt de virksomheder, som gennemfører dokumentation af deres it-sikkerhed er det kun **36 pct**., som har opdateret denne dokumentation indenfor de seneste 12 måneder.
- Der er også plads til forbedring hvad angår ledelsen involvering i virksomhedernes digitale sikkerhed, da blot **36 pct.** af de adspurgte SMV'er svarer, at virksomhedens ledelse *i høj grad* er involveret i beslutninger om virksomhedens arbejde med digital sikkerhed (hvilket er på niveau med det forgange år).

Varetagelse af it-sikkerhedsmæssige opgaver og mangel på it-specialister

- **17 pct.** af SMV'erne har eller har forsøgt at rekruttere it-specialister i 2021. Heraf har **60 pct.** haft svært ved at besætte stillingen. Mange SMV'er har ikke en decideret it-sikkerhedsmedarbejder ansat, men anvender netop generelle it-specialister til også at varetage virksomhedens it-sikkerhedsmæssige opgaver. Derfor kan en mangel på it-specialister få negative konsekvenser for virksomhedernes digitale forsvar.
- I 2022 har hele **77 pct.** af SMV'erne (i et vist omfang) benyttet sig af ekstern hjælp til at løfte virksomhedens digitale sikkerhed (dette tal er steget fra **68 pct.** i 2020). Men **25 pct.** af de SMV'er, som anvender en ekstern leverandør, stiller *ikke* krav til leverandøren om fx behandling af data, it-sikkerhedsforanstaltninger og/eller løbende dokumentation om it-sikkerhed.

It-sikkerhedshændelser

- Samlet set har **28 pct.** af SMV'erne og **57 pct.** af de store virksomheder oplevet en it-sikkerhedshændelse i 2021 (dette tæller både utilsigtede hændelser såsom fx softwarefejl og ondsindede, forsætlige hændelser såsom fx ransomware-, phising eller Denial of Service angreb). Ses alene på de ondsindede/forsætlige hændelser har **9 pct.** af SMV'erne og **20 pct.** af de store virksomheder oplevet en it-sikkerhedshændelse i 2021.

Indhold

Introduktion

1. Introduktion

Danmark er et af Europas mest digitaliserede lande[1], hvilket bidrager til konkurrencefordele, produktivitet og vækst blandt danske virksomheder. Men selvom den digitale førerposition er en styrke, gør den samtidig virksomhederne mere sårbarhed overfor digitale angreb, hvilket forudsætter et styrket fokus på digital sikkerhed. Det kan for eksempel medføre store økonomiske omkostninger og tab af tillid, hvis uønskede aktører får adgang til virksomhedernes digitale systemer eller data.

Ifølge Center for Cybersikkehed er trusselsniveauet for cyberspionage og cyberkriminalitet meget høj for danske virksomheder[2], og danske topledere ser cybertruslen som den største bekymring for virksomheden[3]. Med den russiske invasion af Ukraine, er den digitale sikkerhed kun blevet mere aktuel, og 63 % af CXO'erne og it-fagfolkene i det private erhvervsliv er mere bekymrede for cybertruslen, end de var for 12 måneder siden, hvilket i overvejende grad skyldes konflikten mellem Rusland og Vesten[4].

Alligevel har mange virksomheder – og særligt små og mellemstore virksomheder (SMV'er) – ikke tilstrækkelig fokus på digital sikkerhed. Det skyldes blandt andet, at mange SMV'er ikke ser sig selv som interessante mål for hackerne, og derfor ikke prioritere de nødvendige ressourcer til at sikre sig. For det kræver både ressourcer i form af tid og penge og de rette kompetencer at arbejde helhedsorienteret med cybersikkerhed.

Digitaliseringsstyrelsen arbejder for at skabe større fokus på digital sikkerhed blandt danske SMV'er med henblik på at understøtte et sikkerhedsmæssigt løft af dansk erhvervsliv. Digitaliseringsstyrelsen stiller blandt andet gratis råd og vejledning om digital sikkerhed til rådighed for danske virksomheder samt koordinere offentlige-private tiltag mm. Nedenstående boks viser et samlet overblik over de erhvervsrettede indsatser for at styrke den digitale sikkerhed i danske virksomheder.

[1] Europa-Kommissionen (2022): Indekset for den digitale økonomi og det digitale samfund (DESI)
[2] Center for Cybersikkerhed (2022), Cybertuslen mod Danmark
[3] PwC (2021): CEO survey
[4] PwC (2022): Cybercrime Survey

Udvalgte tiltag for at øge den digitale sikkerhed i danske SMV'er

National Strategi for Cyber- og Informationssikkerhed (NCIS) 2022-2024
Med NCIS 2022-2024 er der afsat 270 mio. kr., som skal løfte den digitale sikkerhed på tværs af samfundet. Strategien indeholder konkrete indsatser for at styrke det offentligt-private samarbejde, og skal bl.a. sikre bedre muligheder for videns- og erfaringsudveksling om cyber- og informationssikkerhed.

Sikkerdigital.dk
På sikkerdigital.dk har Digitaliseringsstyrelsen samlet viden om informationssikkerhed til borgere, virksomheder og myndigheder. På virksomheds-sitet findes bl.a. gode råd, vejledning og værktøjer, som hjælper virksomheder til en sikker digital adfærd. Læs mere her

Cyberhotline for digital sikkerhed
Digitaliseringsstyrelsen har, i samarbejde med Center for Cybersikkerhed, oprettet en hotline, som skal hjælpe borgere og virksomheder med at få styr på den digitale sikkerhed. Virksomheder kan fx ringe til hotline og blive klogere på, hvordan de ruster deres virksomhed mod digitale trusler. Læs mere her

Cybersikkerhedspagten
Cybersikkerhedspagten er et offentligt-privat samarbejde, der skal sikre, at danske små- og mellemstore virksomheder (SMV'er) bliver de mest cybersikre i Europa. Parterne arbejder for at igangsætte nye indsatser, sikre synergi mellem nye og igangværende indsatser samt at drøfte deres fælles resultater og målsætninger. Se cybersikkerhedspagtens medlemmer og de nuværende arbejdsspor her

Brobyggerindsats
Brobyggerindsatsen skal i samarbejde med erhvervslivets interessenter bidrage til at øge den digitale robusthed i danske SMV'er ved at styrke virksomhedernes primære rådgiveres (fx revisorer, virksomhedskonsulenter mfl.) indsigt i it-sikkerhed, så de kan fungere som brobyggere, der videreformidler budskaber om it-sikkerhed til SMV'erne.

Nationalt koordinations-center for Cybersikkerhed (NCC)
NCC er et EU-initiativ delt mellem Erhvervsstyrelsen og Digitaliseringsstyrelsen, som har til formål at styrke den danske cybersikkerhedsindustri, herunder at fremme udviklingen af produkter samt styrke optaget af cybersikkerhedsløsninger i den private sektor. Det gøres bl.a. ved at understøtte innovationsprojekter og konsortiedannelse i cybersikkerhedsøkosystemet, særligt for at fremme dansk deltagelse i innovationsprogrammerne Digital Europe og Horizon Europe.

SMV:digital-pulje om digital sikkerhed
SMV'er havde i 2022 mulighed for at søge tilskud på 50.000 kr. til rådgivning om, hvordan virksomheden kan styrke den digitale sikkerhed. 552 SMV'er har i skrivende stund gennemført og evalueret it-sikkerhedspuljen med en generel tilfreds på 88 pct. Læs mere her

Cybersikkerhedsrådet
Cybersikkerhedsrådet rådgiver regeringen om, hvordan den digitale sikkerhed styrkes og bidrager til videndeling mellem myndigheder, erhvervsliv og forskningsverden. Rådet sekretariatsbetjenes af Digitaliseringsstyrelsen og Center for Cybersikkerhed. Læs mere her

1.1 Afgrænsning og datagrundlag

Datagrundlaget i rapporten er beregnet på baggrund af Danmark Statistiks årlige spørgeskemaundersøgelse "IT-anvendelse i virksomheder" (VITA). Denne rapport baserer sig på data indsamlet i 2022 blandt 4.193[5] 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 situationen i det forgange år, i dette tilfælde 2021.

Ud over den årlige VITA-undersøgelse (blandt virksomheder med 10+ ansatte) har Danmarks Statistik også gennemført en temaanalyse i 2022 blandt de helt små danske virksomheder med 5-9 ansatte (mikrovirksomheder). I undersøgelsen stilles mikrovirksomhederne blandt andet 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 1.537 virksomheder i de private, ikke-finansielle byerhverv med 5-9 fultidsansatte.

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

Eftersom Digitaliseringsstyrelsens primære målgruppe er danske SMV'er, er resultaterne i denne rapport opdelt for 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[6].

For enslydende spørgsmål om virksomhedernes arbejde med digital sikkerhed er ændringer over årene som udgangspunkt udregnet og præsenteret i rapporten.

[5] Heriblandt 3.713 SMV'er

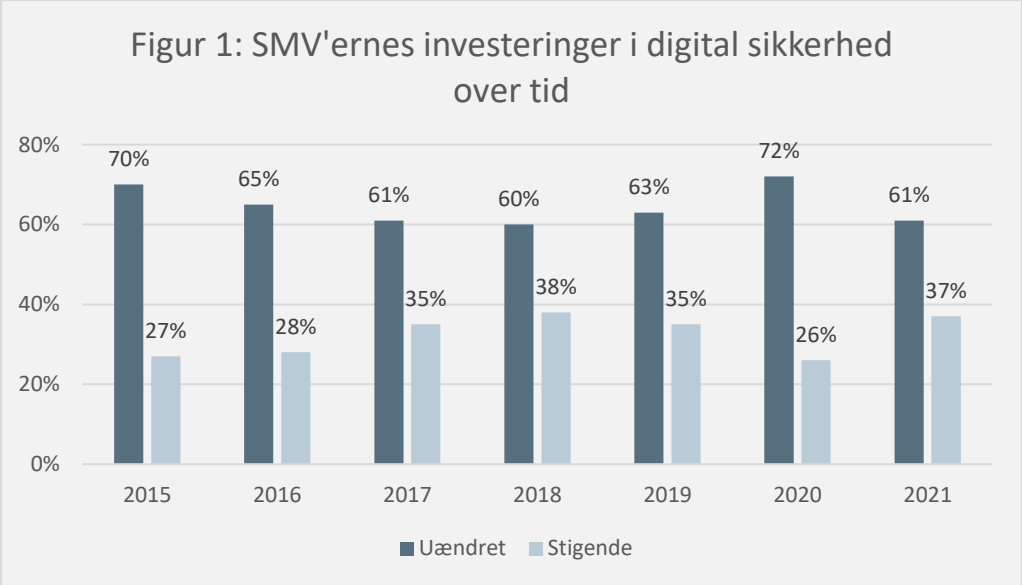
[6] I 2020, 2021 og 2022 er rapporten udarbejdet af Erhvervsstyrelsen. Men som følge af en ressortomlægning udgives rapporten af Digitaliseringsstyrelsen fra 2023 og frem.

Investeringer i digital sikkerhed og brug af it-sikkerhedstiltag

2. Investeringer i digital sikkerhed og brug af it-sikkerhedstiltag

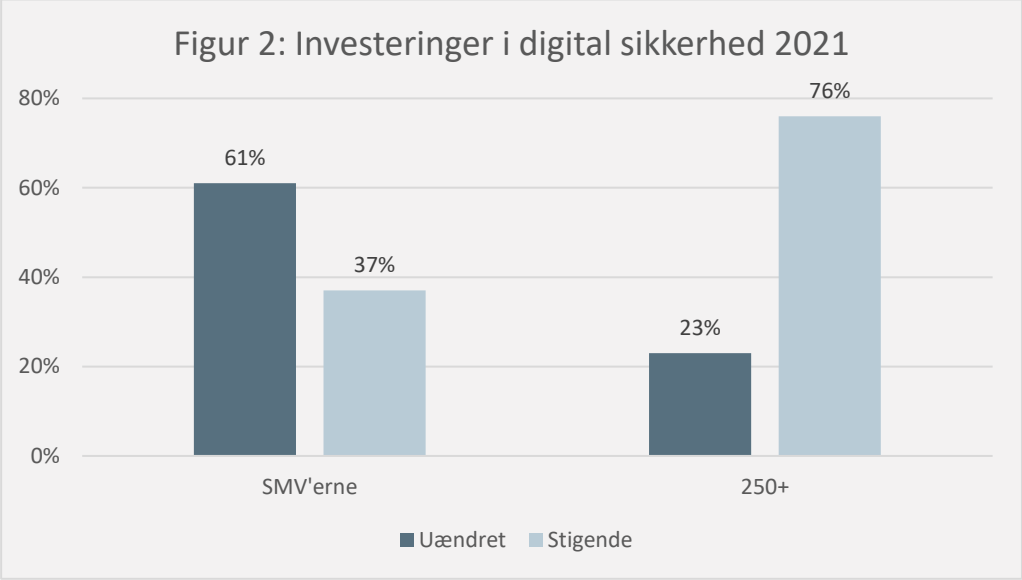
2.1 Stigende investeringer i digital sikkerhed

I 2021 har 37 pct. af de danske SMV'er investeret mere i digital sikkerhed i forhold til det forgange år, som illustreret i *figur 1*. Dette er en positiv fortsættelse af de seneste års tendens med øgede investeringer i digital sikkerhed. I 2021 finder vi endda den største andel virksomheder, som har øget deres investeringer i digital sikkerhed siden 2018. Der spørges dog ikke ind til, hvor meget virksomhederne har øget deres investeringer i digital sikkerhed.



Note: Tallene summerer ikke til 100 pct. da en mindre andel af virksomhederne havde faldende udgifter på tværs af årene.
Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2022).

Der ses dog en tendens til, at de større virksomheder i højere grad end SMV'erne øger deres investeringer i digital sikkerhed. Fx har 76 pct. af de store virksomheder med over 250 ansatte øget deres investeringer i digital sikkerhed, hvilket er markant højere end 37 pct. blandt SMV'erne, jf. *figur 2*.



Note: Tallene summerer ikke til 100 pct. da en mindre andel af virksomhederne havde faldende udgifter.
Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2022).

Selvom investeringer i digital sikkerhed er en omkostning for virksomheden, kan det være en fordelagtig investering målt op imod omkostningerne ved et eventuelt angreb. En undersøgelse fra IBM viser, at et it-sikkerhedsbrud gennemsnitligt koster omkring 14 mio. kr. for virksomheder i Skandinavien[7]. Dette tal er dog ikke opgjort for SMV'er alene.

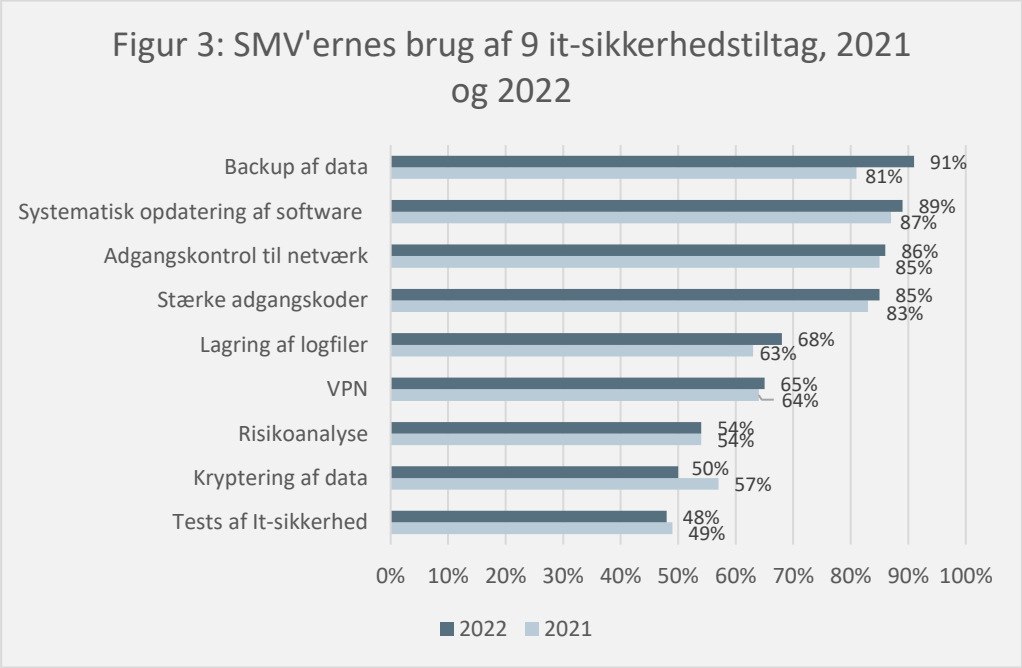
Udover at sikre sig mod cyberangreb og mindske omkostninger herved, kan investeringer i digital sikkerhed også føre øvrige fordele med sig. En undersøgelse gennemført af Analyse & Tal for Industriens Fond i 2022[8] viser nemlig, at der findes en positiv sammenhæng mellem antallet af anvendte it-sikkerhedstiltag (såsom backup, opdatering, medarbejdertræning osv.) og oplevede konkurrencefordele for virksomhederne. Det vil sige, at it-sikkerhedstiltag udover at beskytte mod udefrakommende cybertrusler *også* kan bidrage til at skabe fx effektivitet og nytænkning i SMV'erne samt øge tilliden til virksomhederne fra eksempelvis kunder, investorer osv.

De kommende afsnit fokuserer derfor på hvilke og hvor mange it-sikkerhedstiltag, som SMV'erne anvender. Der vil først sættes fokus på virksomhedernes brug af tekniske it-sikkerhedstiltag og dernæst deres brug af organisatoriske it-sikkerhedstiltag.

[7] IBM Security (2022): Cost of a Data Breach. Data består af kvalitative interviews med 3.600 personer blandt 550 organisationer, der har oplevet et brud på datasikkerheden, heraf 20 organisationer i Skandinavien).
[8] Cyberbarometer.dk

2.2 SMV'ers brug af tekniske it-sikkerhedstiltag

I VITA-undersøgelsen 2022 spørges der til, hvorvidt virksomheden anvender 9 forskellige tekniske it-sikkerhedsforanstaltninger[9]. En oversigt over andelen af SMV'er, som har anvendt disse 9 it-sikkerhedsforanstaltninger i hhv. 2021 og 2022, fremgår af *figur 3*.



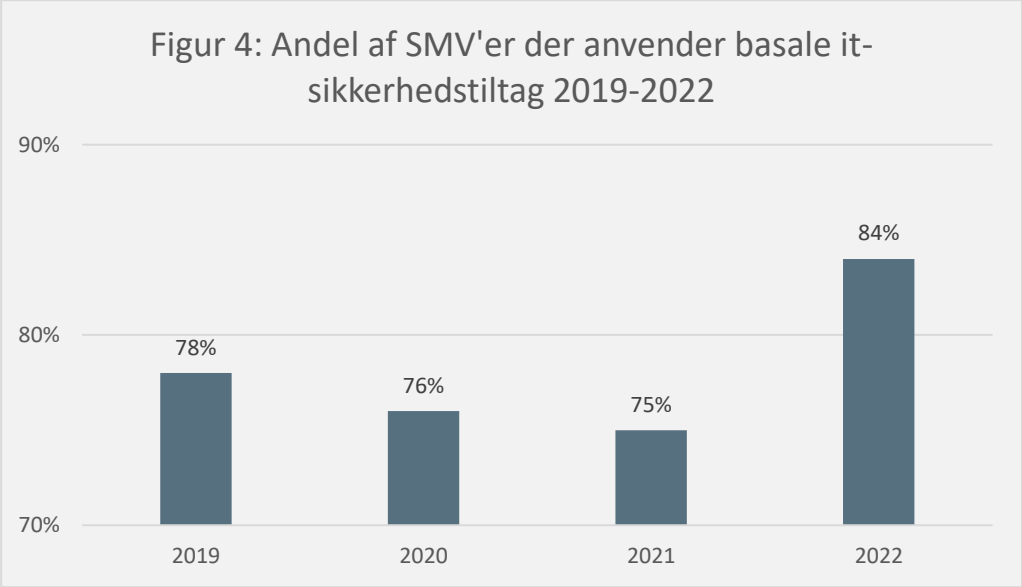
Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2022).

Som det fremgår af figuren tog 91 pct. af de danske SMV'er backup af data i 2022, mens 89 pct. gennemførte systematisk opdatering af software. Disse to sikkerhedsforanstaltninger anses som værende helt basale og nødvendige for en virksomheds digitale sikkerhed, da de udover at være relevante i forhold til at afværge mange it-sikkerhedsangrebstyper også er relativt simple at indføre for virksomheden[10]. Derfor bør alle virksomheder som minimum anvende disse to basale foranstaltninger.

Det er derfor positivt, at der i 2021 er sket en betydelig fremgang ift. andelen af SMV'er, der anvender begge disse to basale sikkerhedsforanstaltninger som en del af deres digitale sikkerhed. Som *figur 4* viser, anvendte 75 pct. af SMV'erne de to basale tiltag i 2021, hvilket er steget til 84 pct. i 2022. Det er især andelen af virksomheder, der anvender backup af data, som er steget fra 2021 til 2022 (jf. *figur 3* ovenfor).

[9] It-sikkerhedsforanstaltninger defineres som 'systemer og procedurer, der skal sikre konsistens, autenticitet, tilgængelighed og fortrolighed af data og it-systemer'.
[10] Monitor Deloitte for Erhvervsstyrelsen (2018): IT-sikkerhed og datahåndtering i danske SMV'er.

På **sikkerdigital.dk** har Digitaliseringsstyrelsen samlet syv gode råd om digital sikkerhed målrettet de danske SMV'er, heriblandt de to basale tiltag. På sitet kan virksomheder således få simple råd til at opdatere deres styresystemer, få styr på deres backup-rutiner mm.



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2022).

Der kan selvfølgelig være flere årsager til den positive fremgang i SMV'ernes brug af basale it-sikkerhedstiltag. Én forklaring kan være, at der i takt med den stigende cybertrussel og opmærksomheden herpå er opstået en generel forståelse i SMV-laget om vigtigheden i at have den helt basale sikkerhed på plads. Blandt andet som følge af Ruslands invasion på Ukraine. Desuden har flere virksomheder offentligt peget på, at netop mangel på backup har medført store omkostninger for virksomheden efter et angreb[11]. En anden forklaring kan være, at virksomhederne generelt har fået et større fokus på cybersikkerhed i kølvandet på Corona, som har sat ekstra skub i den digitale omstilling og i forlængelse heraf også sat mere fokus på cybersikkerhed eller mangel på samme. En tredje forklaring kan være, at man fra politisk side har øget ambitionsniveauet for indsatsen på cyberområdet de seneste år. Fx ved at lancere den første nationale strategi for cyber- og informationssikkerhed i 2018[12], 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[13] (se evt. rapportens introduktion for et samlet overblik over Digitaliseringsstyrelsens virksomhedsrettede initiativer rettet mod at styrke virksomhedernes digitale sikkerhed).

[11] Se fx: https://globalrevision.dk/husk-at-tage-backup-af-elektroniske-oplysninger/ og https://www.version2.dk/artikel/maersk-ciso-jeg-stoler-ikke-paa-den-indbyggede-sikkerhed-i-cloud
[12] https://www.regeringen.dk/media/5227/5-publikation-digitale-muligheder-a5s-dk-maj-web.pdf
[13] https://fm.dk/media/25359/national-strategi-for-cyber-og-informationssikkerhed_web-a.pdf

Foruden fremgangen i brug af de to basale sikkerhedstiltag viser *figur 3* også en smule fremgang i SMV'ernes brug af yderlige it-sikkerhedstiltag, herunder stærke adgangskoder og lagring af logfiler, mens der findes et fald i SMV'ernes brug af kryptering af data og test af it-sikkerhed. Nogle af disse forskelle er dog så små, at det også kan skyldes tilfældig variation i virksomhedsbesvarelserne mellem årene.

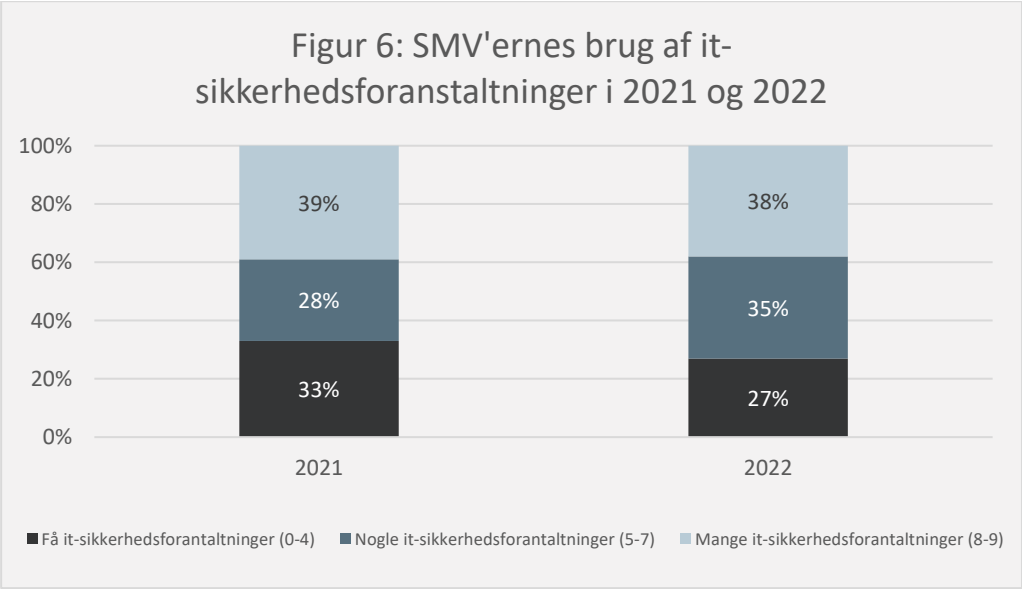
De 9 tekniske it-sikkerhedsforanstaltninger i *figur 3* er omdannet til et indeks, der angiver om en virksomhed anvender hhv. 'få', 'nogle' eller 'mange' tekniske it-sikkerhedsforanstaltninger, som beskrevet i *tabel 1*.

Tabel 1: Operationalisering af virksomheders brug af tekniske it-sikkerhedsforanstaltninger

Få it-sikkerhedsforanstaltninger	Nogle it-sikkerhedsforanstaltninger	Mange it-sikkerhedsforanstaltninger
Brug af 0-4 it-sikkerhedsforanstaltninger + virksomheder, der ikke har implementeret de to basale sikkerhedstiltag	Brug af 5-7 sikkerhedsforanstaltninger, forudsat at virksomhederne har implementeret de to basale tiltag.	Brug af 8-9 sikkerhedsforanstaltninger, forudsat at virksomhederne har implementeret de to basale tiltag.

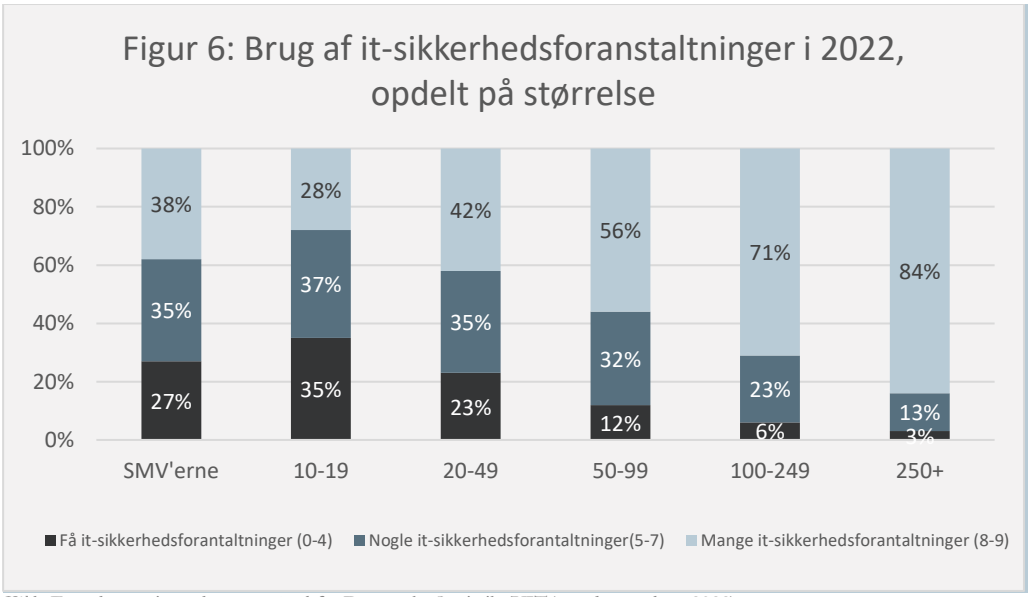
Note: En nærmere forklaring af denne operationalisering fremgår af kapitel 9, Metode.

Figur 5 viser SMV'ernes brug af de 9 it-sikkerhedsforanstaltninger i hhv. 2021 og 2022. I 2022 anvendte 27 pct. 'få' (0-4) it-sikkerhedsforanstaltninger, mens 35 pct. har anvendt 'nogle' (5-7) og 38 pct. har anvendt 'mange' (8-9) tekniske it-sikkerhedsforanstaltninger. Sammenligner man SMV'ernes brug af sikkerhedsforanstaltninger i 2021 og 2022 har en mindre andel af virksomheder flyttet sig fra 'få' til 'nogle' sikkerhedsforanstaltninger, hvorimod der ikke findes en udvikling blandt de SMV'er, som allerede har arbejdet med digital sikkerhed i form af 5 it-sikkerhedstiltag eller flere.



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2022).

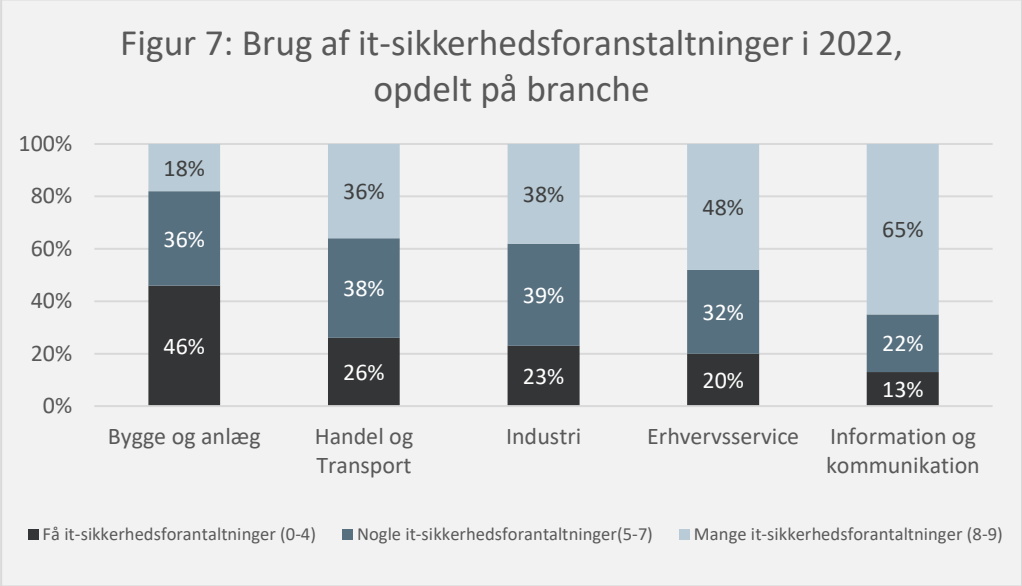
Som *figur 6* illustrerer, er der i lighed med tidligere år en klar tendens: jo mindre virksomhed, jo færre it-sikkerhedsforanstaltninger har den typisk implementeret. Dette er ikke overraskende, da mindre virksomheder generelt er mindre digitale end større virksomheder[14], og derfor må forventes at være i mindre risiko for digitale angreb. Det vender vi tilbage til i kapitel 3, når virksomhedens risikoprofil skal findes.



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2022).

Ligeledes findes der også (igen i år) betydelige forskelle i SMV'ernes digitale sikkerhedsniveau alt efter hvilken branche, som virksomheden arbejder indenfor, jf. *figur 7*. Dette findes heller ikke overraskende, da branchen "kommunikation og kommunikation" - hvor virksomhederne i gennemsnit har implementeret flest it-sikkerhedstiltag - også har i gennemsnit har flere ansatte der arbejder digitalt med adgang til kundedata osv., og derfor også bør have et endnu større fokus på digital sikkerhed. Igen et parameter, som vi kommer tilbage til i kapitel 3 i forbindelse med kortlægning af virksomheden risikoprofil.

[14] Erhvervsstyrelsen (2022): Årsrapport SMV:Digital 2021



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2022).

I en europæisk kontekst klarer danske SMV'er sig godt hvad angår brug af disse tekniske it-sikkerhedstiltag. I Danmark finder vi nemlig den højeste andel af SMV'er, som har anvendt hhv. minimum 3 og minimum 5 af de konkrete it-sikkerhedstiltag på tværs af europiske lande, mens vi har en anden plads i andelen af virksomheder, som har anvendt minimum 7 it-sikkerhedstiltag (kun overgået af Finland)[15].

Mens dette afsnit har fokuseret på de tekniske it-sikkerhedstiltag, vil det kommende afsnit fokusere på SMV'ernes arbejde med organisatoriske it-sikkerhedstiltag såsom medarbejdertræning og ledelsesinvolvering.

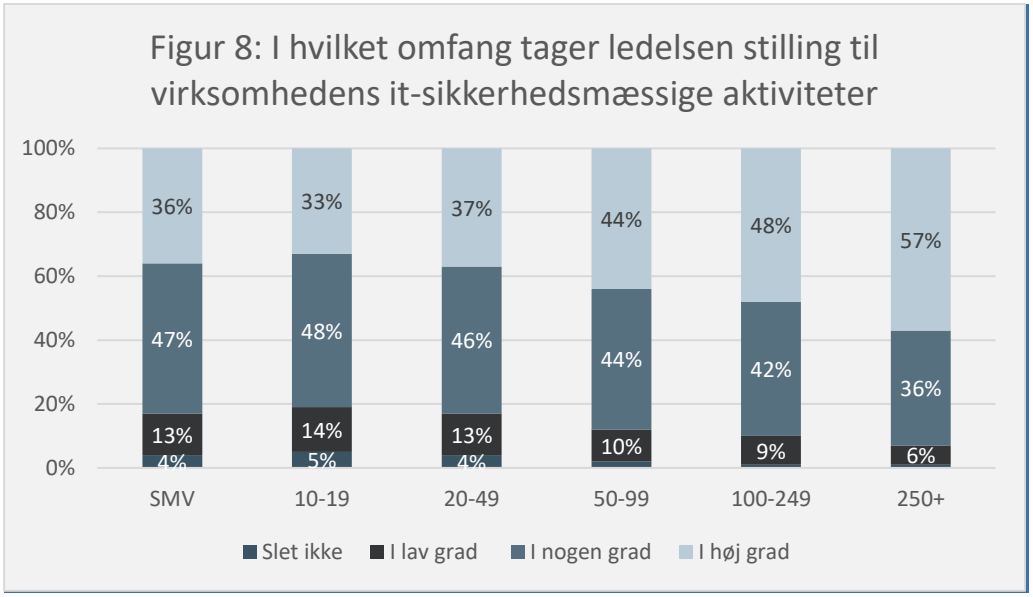
2.3 SMV'ers brug af organisatoriske it-sikkerhedstiltag

I sidste ende er det ledelsen i de enkelte virksomheder, der har ansvar for virksomhedens digitale sikkerhed. Et helt centralt organisatorisk tiltag er derfor, i hvilket omfang virksomhedens øverste ledelse tager stilling til virksomhedens it-sikkerhedsmæssige aktiviteter.

Figur 8 viser sammenhængen mellem virksomhedsstørrelse, og i hvilket omfang at ledelsen har taget stilling til virksomhedens it-sikkerhedsmæssige aktiviteter. Blandt de adspurgte SMV'er svarer 38 pct., at virksomhedens ledelse *i høj grad* er involveret i beslutninger om virksomhedens arbejde med digital sikkerhed. Det gælder til sammenligning 57 pct. blandt de store virksomheder med 250+ ansatte.

[15] Eurostat (2022): security policy measures, risk and staff awareness

Dermed er 64 pct. af danske SMV'ers ledelser kun *i nogen grad, lille grad* eller *slet ikke* involveret i virksomhedens arbejde med digital sikkerhed (hvilket er på niveau med det forgange år). Det er dog positivt, at blot 4 pct. af SMV'erne svarer, at ledelsen *slet ikk*e tager stilling til virksomhedens it-sikkerhedsmæssige aktiviteter.



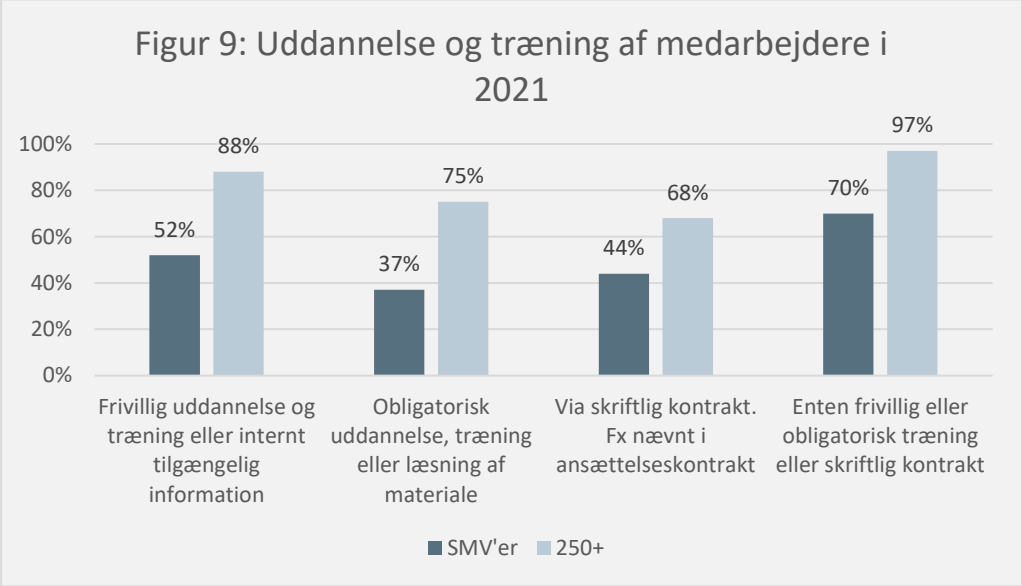
Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2022).

Foruden ledelsens involvering spiller medarbejderne en vigtig rolle i forhold til virksomhedernes digitale sikkerhed. Mange sikkerhedsbrud sker på grund af manglende viden blandt medarbejdere. De kan fx blive narret til at klikke på et usikkert link eller til at udlevere deres adgangskode. Derfor er det afgørende, at virksomhedens medarbejdere løbende bliver mindet om de gode digitale vaner.

Figur 9 viser træning og uddannelse af medarbejdere i SMV'er med 10-249 ansatte sammenlignet med de store virksomheder med 250+ ansatte. Samlet set har 70 pct. af SMV'erne informeret deres medarbejdere om deres rolle og ansvar i forhold til digital sikkerhed gennem enten frivillig træning, obligatorisk træning eller via skriftlig kontrakt i 2022. Denne andel ligger på niveau med tidligere år - det bør dog også være en løbende proces at træne virksomhedens medarbejdere i digital sikkerhed, da cybertruslen løbende udvikler sig.

Sammenlignet med andre EU lande har Danmark en relativ høj andel af SMV'er, som gennemfører medarbejdertræning. Vi ligger nemlig på en fjerdeplads efter Tjekkiet, Irland og Tyskland[16].

[16] Eurostat (2022): security policy measures, risk and staff awareness



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2022).

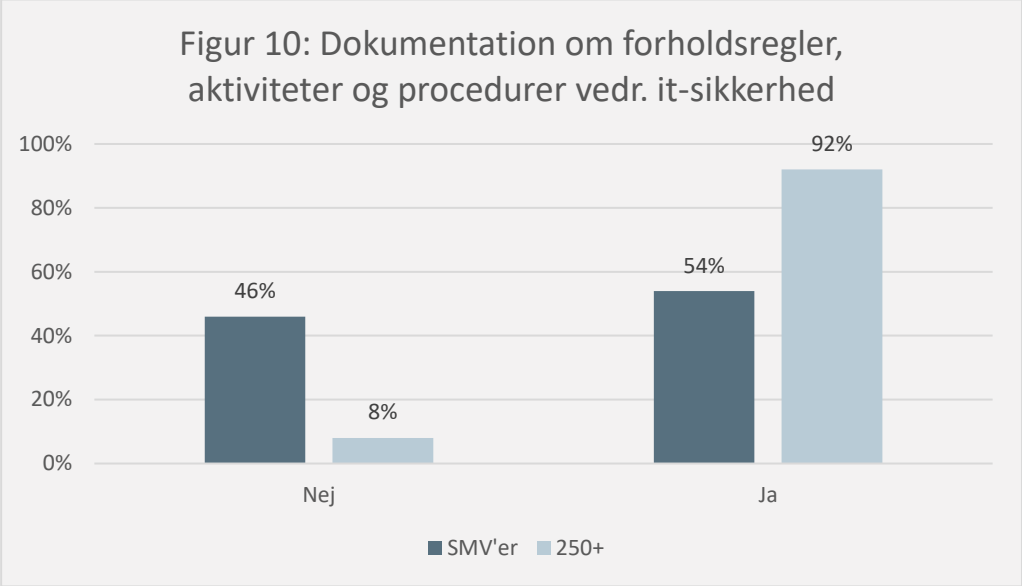
Endelig spørger VITA-undersøgelsen ind til virksomhedernes dokumentation af deres it-sikkerhed. Som illustreret i *figur 10*, er det blot lidt over halvdelen (54 pct.) af SMV'erne, som gennemfører dokumentation om forholdsregler, aktiviteter og procedurer vedr. it-sikkerhed (fx risikovurdering, evaluering af it-sikkerhedshændelser mv). Blandt de virksomheder, som gennemfører dokumentation af deres it-sikkerhed, er det blot 36 pct., som har opdateret denne indenfor de seneste 12 måneder.

Sammenligner vi os med de øvrige europæiske lande er Danmark godt med igen, da vi ligger i top tre hvad angår andelen af SMV'er som gennemfører dokumentation om forholdsregler, aktiviteter og procedurer vedr. it-sikkerhed - kun overgået af Finland (56 pct.) og Sverige (65 pct.)[17].

På **Sikkerdigital.dk** kan danske virksomheder få hjælp til at gennemføre dokumentation om forholdsregler, aktiviteter og procedurer vedr. it-sikkerhed. Blandt andet findes:

- Et værktøj og en vejledning, som gør det nemmere at arbejde struktureret med virksomhedens **risikovurdering**.
- En **beredskabsplan**, som kan bidrage til at sikre at virksomheden reagerer hurtigt, målrettet og tilstrækkeligt, hvis den oplever en it-sikkerhedshændelse
- En nedskrevet **it-sikkerhedspolitik**, som kan bidrage til at skabe klare retningslinjer om, hvad der forventes af både leder og medarbejder, når det gælder it-sikkerhed.

[17] Eurostat (2022): security policy measures, risk and staff awareness



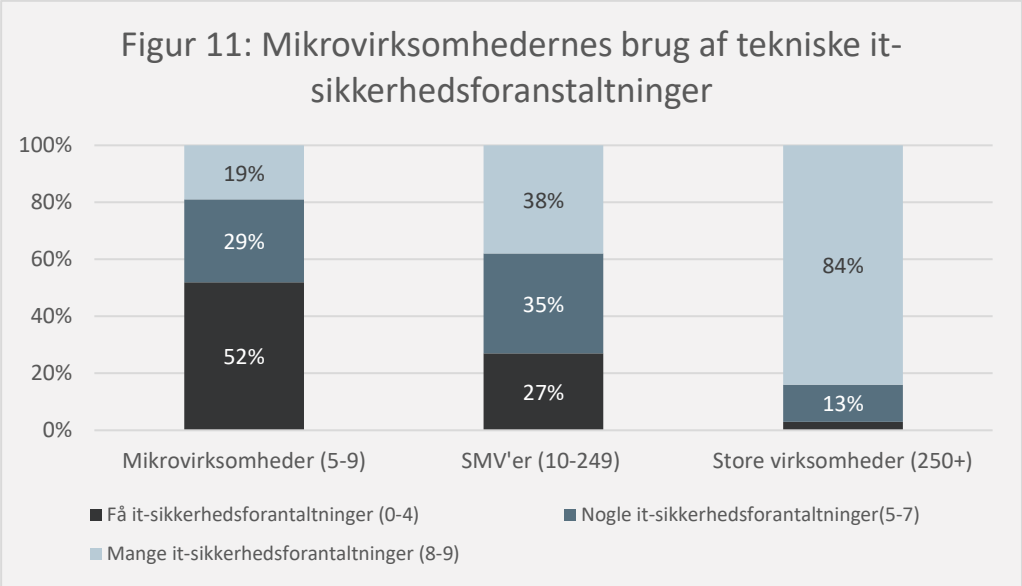
Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2022).

Kantrolleret for virksomhedsstørrelse og branche gælder, at virksomheder der arbejder med hhv. medarbejder-awareness, ledelsesinvolvering og dokumentation af procedure vedr. it-sikkerhed også anvender flere tekniske it-sikkerhedsforanstaltninger. Der findes således en stærk sammenhæng mellem virksomheder, der arbejder med tekniske og organisatoriske it-sikkerhedstiltag.

2.4 De mindste virksomheder har lavt fokus på it-sikkerhed

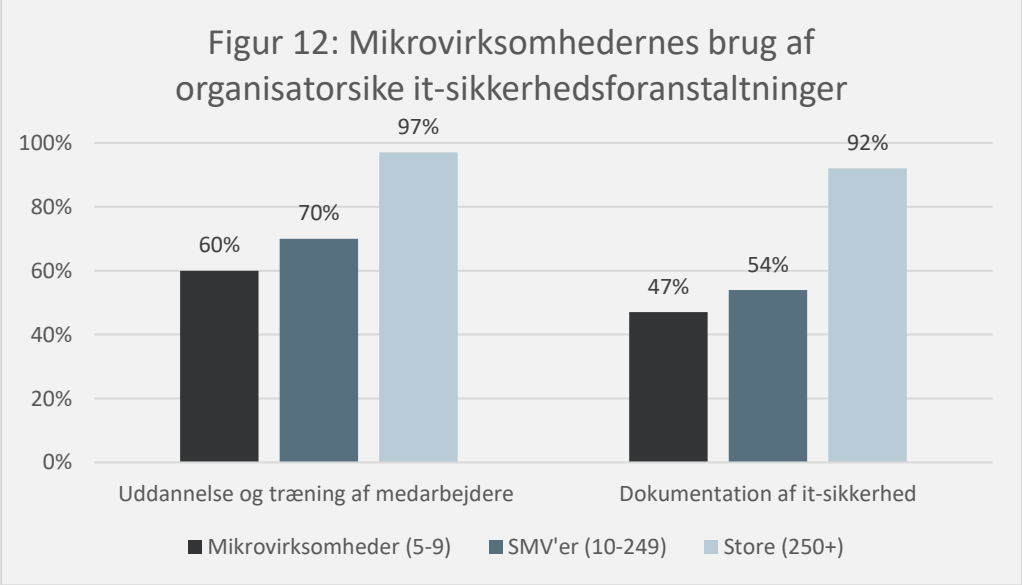
Ud over den årlige VITA-undersøgelse (blandt virksomheder med 10+ ansatte) har Danmarks Statistik også gennemført en temaanalyse i 2022 blandt de helt små danske virksomheder med 5-9 ansatte (mikrovirksomheder). Stikprøven består af gennemførte besvarelser fra i alt 1.537 virksomheder i de private, ikke-finansielle byerhverv med 5-9 fultidsansatte. I undersøgelsen stilles mikrovirksomhederne blandt andet udvalgte it-sikkerhedsspørgsmål, herunder til deres brug af de 9 tekniske it-sikkerhedsforanstaltninger. *Figur 11* 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 over halvdelen af denne virksomhedsgruppe blot anvender "få" tekniske it-sikkerhedstiltag. Her finder vi heller ikke en positiv udvikling siden seneste analyse blandt mikrovirksomhederne i 2019. Ser vi på de to helt basale tiltag (backup af data og opdatering af styresystemer) er det blot 71 pct. af mikrovirksomhederne, som anvender disse. Der er således hele 29 pct. af mikrovirksomhederne, som *ikke* anvender de to helt basale tiltag sammenlignet med 16 pct. i den samlede SMV-gruppe med 10-249 ansatte.



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (It-anvendelse i virksomheder 2022 og Aktiviteter i små virksomheder 2022).

Samme billeder gør sig gældende hvad angår de organisatoriske tiltag, hvor mikrovirksomhederne har særlig lav fokus på uddannelse og træning af medarbejdere og dokumentation af it-sikkerhed sammenlignet med de øvrige SMV'er og store virksomheder (der er ikke spurgt til ledelsesinvolvering i temaanalysen blandt mikrovirksomhederne).



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA 2022 og Aktiviteter i små virksomheder 2022).

Dette kapitel har således 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. For eksempel er der stor forskel

i behovet for digital sikkerhed i en lille frisørvirksomhed og et stort softwarefirma, ligesom nogle brancher i højere grad end andre arbejder med kritisk infrastruktur og derfor bør have særlig høj fokus på digital sikkerhed. Derfor kan der ikke fastlås ét fælles niveau for, hvornår det digitale sikkerhedsniveau er tilstrækkeligt på tværs af virksomheder. I næste afsnit ser vi derfor på, i hvilken grad virksomhederne har et digitalt sikkerhedsniveau, som matcher deres risikoprofil.

SMV'ernes sikkerheds-niveau i forhold til risi-koprofil

3. SMV'ernes sikkerhedsniveau i forhold til risikoprofil

Hvor sårbar en virksomhed er overfor it-sikkerhedshændelser, er en helhedsvurdering. Hvad der udgør et passende sikkerhedsniveau for den ene virksomhed, er ikke nødvendigvis et passende niveau for den anden.

Variationer i virksomhedernes teknologianvendelse, typen af data der opbevares, virksomhedens afhængighed af forskellige systemer, antal ansatte, branche osv., har betydning for både sandsynligheden for at blive ramt, og konsekvensen hvis man bliver ramt. Hvad der udgør et passende sikkerhedsniveau, afhænger altså af virksomhedens risikoprofil.

Med udgangspunkt i PwC's PAVA-model har Digitaliseringsstyrelsen derfor udregnet 1) et indeks over SMV'ernes it-sikkerhedsniveau og 2) et indeks over SMV'ernes risikoprofil. Indekset for SMV'ernes it-sikkerhedsniveau baserer sig på spørgsmål, der siger noget om, hvilke sikkerhedstiltag SMV'erne har implementeret – fx om virksomhedens ledelse tager stilling til it-sikkerhedsmæssige aktiviteter, virksomhedens brug af tekniske tiltag mm. Indekset for SMV'erne risikoprofil baserer sig på spørgsmål, der siger noget om SMV'ernes konsekvensniveau og sandsynligheden for, at de oplever en hændelse (fx antal ansatte, branche, tekniske angrebsflader, opbevaring af persondata mfl.).

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 9) gives en detaljeret redegørelse for den metodiske fremgangsmåde for hver af de to indeks og matchet mellem disse.

Resultaterne i tabel 2 viser, at 35 pct. af SMV'erne er sårbare, da de har et lavt sikkerhedsniveau ift. deres risikoprofil. 52 pct. af SMV'erne vurderes at være tilpas sikre, og har dermed et digitalt sikkerhedsniveau, som matcher deres risikoprofil. Den sidste gruppe er de SMV'er, der vurderes at have et højere sikkerhedsniveau, end deres risikoprofil tilsiger, og tæller altså 13 pct.

Tabel 2: Match mellem SMV'ernes digitale sikkerhedsniveau og risikoprofil

		It-sikkerhedsniveau		
		Lav	Middel	Høj
Risiko-profil	Høj	De sårbare 35 pct.		
	Middel		De tilpas sikrede 52 pct.	
	Lav			De påpasselige 13 pct.

Note: Den metodiske fremgangsmåde for udviklingen af de to indeks samt matchet mellem disse, fremgår af metodeafsnittet og er baseret på metoden udviklet af PwC for Erhvervsstyrelsen. *Kilde:* Egne beregninger baseret på tal fra Danmarks statistik (VITA-undersøgelsen 2022).

I sidste års rapport om digital sikkerhed i danske SMV'er havde 44 pct. et for lavt sikkerhedsniveau ift. deres risikoprofil, og blev altså kategoriseret som sårbare. Andelen af sårbare virksomheder er derfor faldet med 9 procentpoint. Der skal dog tages forbehold for mindre ændringer i spørgsmålsformuleringer, hvorfor sammenligningen kan være behæftet med en vis usikkerhed[18].

Tallene tyder dog på, at der har været en forbedring i it-sikkerheden sammenlignet med sidste års rapport. Årsagerne til dette kan (som også beskrevet i kapitel 2) være flere, det kan være en øget opmærksomhed på den stigende cybertrussel, eller at covid-19 var med til at sætte ekstra fokus på sikkerhed ved hjemmearbejde. En tredje mulig årsag er, at man politisk har sat større fokus på området, og også har lanceret strategier for Cyber- og Informationssikkerhed, som indeholder initiativer målrettet det private erhvervsliv, herunder SMV'erne.

[18] Se metodeafsnittet for en uddybning af metodikken.

Udførelse af it-sikkerhedsmæssige opgaver og mangel på kompetencer

4. Udførelse af it-sikkerhedsmæssige opgaver og mangel på kompetencer

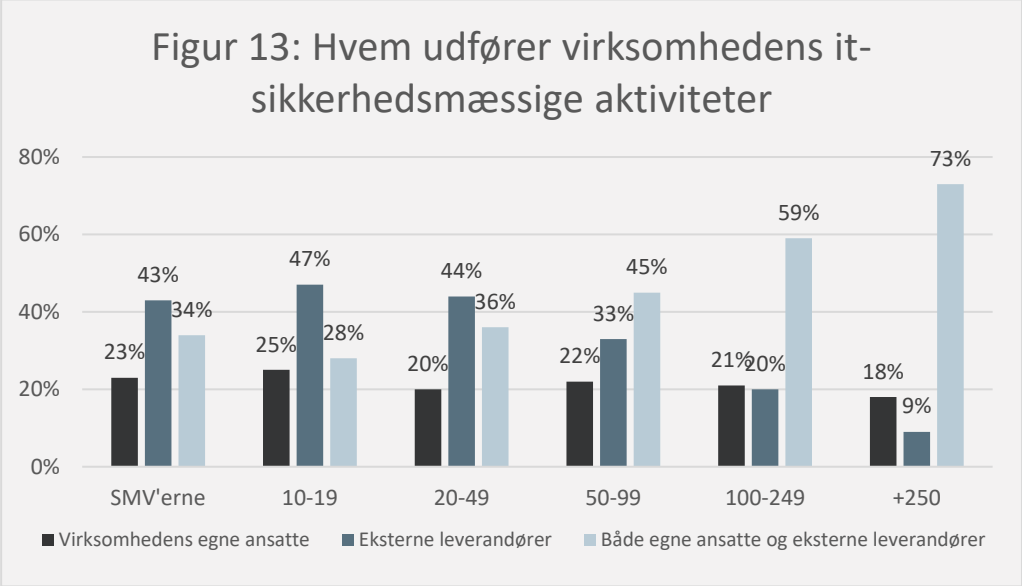
Det er vigtigt at forankre arbejdet med digital sikkerhed hele vejen rundt i virksomheden. Ud over medarbejdertræning og ledelsens fokus på digital sikkerhed er det også nødvendigt med de rette it- og cyberkompetencer til at håndtere de øgede trusler fra cyberkriminalitet. Dette afsnit vil derfor se på, hvem der varetager de it-sikkerhedsmæssige aktiviteter i SMV'erne samt virksomhedernes udfordringerne med at rekruttere it-specialister.

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

Figur 13 viser hvor stor en andel af danske virksomheder som har egne medarbejdere, eksterne leverandører eller begge dele til at varetage virksomhedens it-sikkerhedsmæssige aktiviteter. Som det fremgår udliciterer 43 pct. af SMV'erne alle virksomhedens it-sikkerhedsmæssige aktiviteter, mens 34 pct. udliciterer dele af de it-sikkerhedsmæssige aktiviteter til en ekstern leverandør. Samlet set benytter hele 77 pct. af SMV'erne sig således (i et vist omfang) af ekstern hjælp til at løfte virksomhedens digitale sikkerhed i 2022. Dette tal er desuden steget fra 68 pct. siden 2020.

Der kan være mange fordele for en virksomhed i at udlicitere dens it-sikkerhedsmæssige aktiviteter til eksterne leverandører – for eksempel har mange af de mindre SMV'er hverken behov for eller ressourcer til at ansætte en decideret it-sikkerhedsekspert eller en it-afdeling. Men selvom virksomheden udliciterer den digitale sikkerhed, er det fortsat vigtigt, at virksomhederne stiller krav til, at der er styr på sikkerheden hos leverandøren. Her viser resultaterne dog plads til forbedring, da 25 pct. af de SMV'er, som anvender en ekstern leverandør, *ikke* stiller krav til leverandøren om fx behandling af data, it-sikkerhedsforanstaltninger og/eller løbende dokumentation om it-sikkerhed.

Der er dog hjælp at hente på **Sikkerdigital.dk,** hvor der ligger et **leverandørværktøj** til rådighed, som kan ruste virksomheder til at have en kvalificeret dialog med it-leverandøren omkring sikkerheden i den respektive løsning.



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2022).
Note: En mindre del af SMV'erne (6 pct.) har hverken egne medarbejdere eller eksterne leverandører til at varetage it-sikkerhedsmæssige aktiviteter. Procentandelen i figuren er alene udregnet blandt de 94 pct. som har egne ansatte, eksterne leverandøren eller begge dele til at varetage it-sikkerhedsmæssige opgaver.

Figur 13 viser også, at de mindre virksomheder *enten* benytter egne medarbejdere eller eksterne leverandører til at varetage den digitale sikkerhed, mens de store virksomheder *både* anvender egne medarbejdere og eksterne leverandører. Anvender virksomheden udelukkende egne ansatte til at varetage it-sikkerhedsmæssige opgaver, er det særligt vigtigt, at disse medarbejdere har de rette kompetencer. I det følgende ser vi derfor på hvilke medarbejderprofiler, som typisk varetager de it-sikkerhedsmæssige opgaver i SMV'erne.

4.2 Mange SMV'er ansætter ikke it-sikkerhedsspecialister, men uddelegerer opgaven til øvrige medarbejderprofiler

I et antropologisk studie blandt 30 forskellige SMV'er, som Aalborg Universitet har gennemført for Digitalisringsstyrelsen i 2022[19][20], blev det blandt andet undersøgt hvilke medarbejderprofiler, som typisk varetager de it-sikkerhedsmæssige aktiviteter i SMV'erne. Resultaterne viser, at *ingen* af de 30 SMV'er har en decideret it-sikkerhedseksperter ansat, men at ansvaret for it-sikkerheden typisk bliver delegeret til én af følgende tre medarbejderprofiler: 1) it-specialister 2) bogholdere eller 3) compliance- og kommunikationsspecialister. Ud over de tre medarbejderprofiler bekræfter også denne undersøgelse, at mange SMV'er udliciterer deres it-sikkerhed til eksterne leverandører.

[19] AAU (2022): "Good" Organizational Reasons for "Bad" Cybersecurity: Ethnographic Study of 30 Danish SMEs
[20] OBS: AAU undersøgelsen blev i gangsat af Erhvervsstyrelsen - men det kontor, som fik udarbejdet analysen, blev ressortoverflyttet til Digitaliseringsstyrelsen før opgavens afslutning.

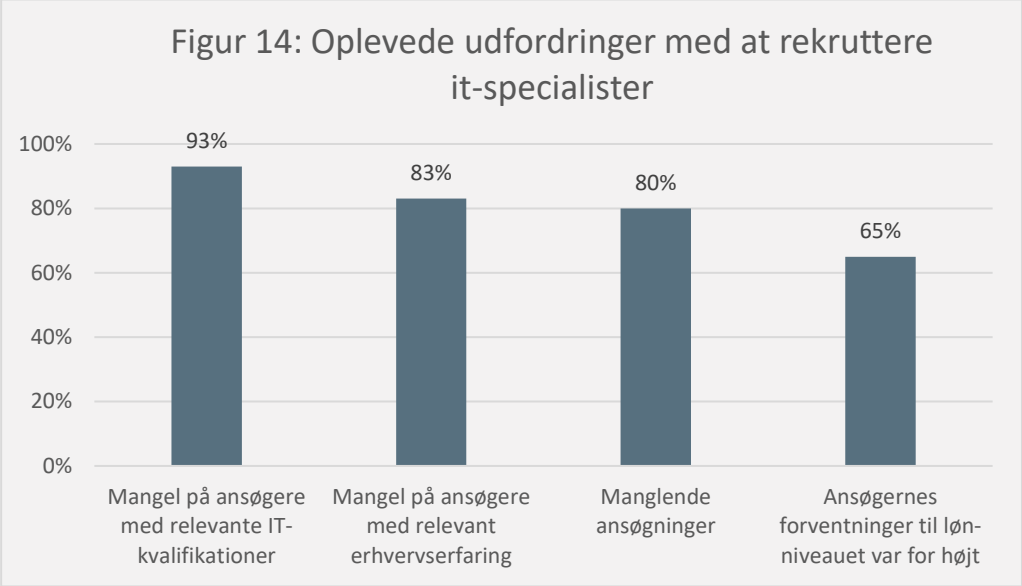
Undersøgelsen nuancerer desuden, hvorledes disse tre medarbejderprofiler typisk har hver deres tilgang til it-sikkerhed, herunder forskellige styrker og svagheder i forhold til at varetage opgaven. It-specialisterne har ofte den fordel, at de kender de tekniske systemer i virksomheden, hvilket dog samtidig kan være en ulempe i forhold til at skulle kunne "kritisere" systemernes it-sikkerhed. Bogholderne har den fordel, at de arbejder tæt på direktøren og ofte har en stor berøringsflade med medarbejdere i virksomheden, men også den ulempe at de ofte mangler de tekniske kompetencer (bogholderne har derfor ofte større fokus på organisatoriske frem for tekniske it-sikkerhedstiltag). Endelig har kommunikationsspecialisterne den fordel at de dygtige til at lave kommunikationsværktøjer og strategier, men samtidig den ulempe at de ofte har mindre indsigt i, hvad der er praksis i virksomhedens produktion og administration og derfor har svært ved at tage højde for de lokale forhold i virksomheden. Dette gælder i øvrigt også for eksterne it-sikkerhedsleverandører. Det kan således på forskellig vis være "huller" eller behov for efteruddannelse ift. SMV'ernes digitale sikkerhed, afhængigt af hvilke medarbejderprofiler, som løfter opgaven.

Da mange SMV'er får varetaget it-sikkerheden af deres it-specialister, vil det kommende afsnit se på virksomhedernes udfordringer med at rekruttere disse specialister.

4.3 Over halvdelen af danske SMV'er, som ønsker at ansætte it-specialister, oplever udfordringer med at rekruttere dem

Efterspørgslen efter it-specialister er stor og udbuddet matcher ikke denne efterspørgsel. Data viser nemlig, at 17 pct. af SMV'erne har rekrutteret eller forsøgt at rekruttere it-specialister i 2021. Heraf har 60 pct., har haft svært ved at besætte deres stillinger. Det gælder til sammenligning 75 pct. af de store virksomheder med 250+ ansatte, hvor hele 68 pct. af virksomhederne har eller har forsøgt at rekruttere it-specialister.

Figur 14 viser hvilke udfordringer, som SMV'erne har oplevet i forbindelse med at rekruttere it-specialister. Som det fremgår, oplevede virksomhederne især mangel på ansøgere med relevante it-kvalifikationer (93 pct.), mangel på ansøgere med relevant erhvervserfaring (83 pct.) samt generel mangel på ansøgninger (80 pct.). Men også ansøgernes forventning til løn var en betydelig udfordring (65 pct). Disse oplevede udfordringer går igen på tværs af virksomhedsstørrelse, hvor der ikke findes nævneværdige forskelle.



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2022).
Note: Virksomhederne har haft mulighed for at angive flere svarmuligheder (multible choice)

Dette kapitel har beskrevet, at de generelle it-specialister også ofte sidder med de konkrete it-sikkerhedsmæssige opgaver i SMV'erne, hvorfor mangel på disse generelle it-specialister kan gå ud over virksomhedernes digitale forsvar. Dertil kommer, at også andre medarbejderprofiler (fx bogholder og kommunikationsspecialister) også varetager it-sikkerhedsmæssige aktiviteter og dermed kan en eventuel mangel på disse medarbejderprofiler også påvirke i hvilken grad SMV'erne formår at løfte de it-sikkerhedsmæssige opgaver – ligesom disse medarbejdertyper kan mangle kompetencerne til at sikre de nødvendige (især tekniske) it-sikkerhedstiltag.

It-sikkerhedshændelser i danske virksomheder

5. It-sikkerhedshændelser i danske virksomheder

I VITA-undersøgelsen 2022 spørges der til, om virksomhederne har oplevet én eller flere it-sikkerhedshændelser i 2021 (dvs. at referenceperioden for it-sikkerhedshændelser er det foregående kalenderår). I 2022 har Danmarks Statistik omformuleret spørgsmålet om it-sikkerhedshændelser, således at svarmulighederne både indeholder ondsindede/tilsigtede it-sikkerhedshændelser såsom CEO fraud og utilsigtede it-sikkerhedshændelser såsom hardware- eller softwarefejl (modsat kun ondsindede/tilsigtede hændelser i tidligere år). Derfor kan resultaterne i dette afsnit ikke sammenlignes med tidligere år.

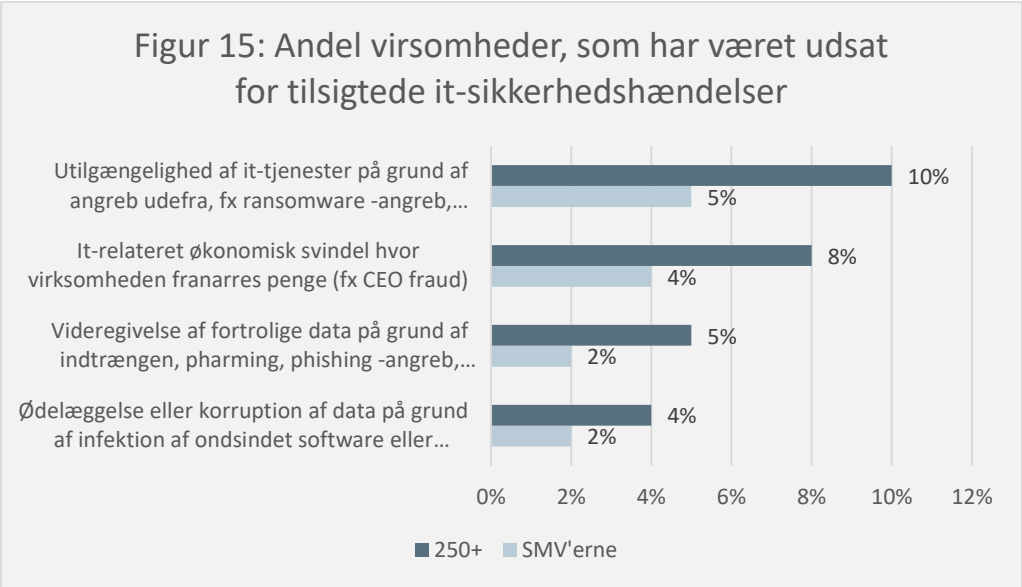
Tabel 3 nedenfor opsummerer de 7 nye svarkategorier og andelen af hhv. SMV'er og store virksomheder med 250+ansatte, som har oplevet disse it-sikkerhedshændelser i 2021.

Tabel 3: It-sikkerhedshændelser i danske virksomheder i 2021

It-sikkerhedshændelser	SMV'er	250+
A. Ødelæggelse eller korruption af data på grund af infektion af ondsindet software eller uautoriseret indtrængen	2%	4%
B. Videregivelse af fortrolige data på grund af indtrængen, pharming, phishing -angreb, forsætlige handlinger fra egne medarbejdere	2%	5%
C. Videregivelse af fortrolige data på grund af utilsigtede handlinger foretaget af egne medarbejdere	2%	9%
D. Ødelæggelse eller korruption af data på grund af hardware- eller softwarefejl	3%	12%
E. It-relateret økonomisk svindel (hvor virksomheden franarres penge (fx CEO fraud)	4%	8%
F. Utilgængelighed af it-tjenester på grund af angreb udefra, fx ransomware -angreb, Denial of Service-angreb	5%	10%
G. Utilgængelighed af it-tjenester på grund af hardware- eller softwarefejl	22%	48%
I ALT	**28%**	**57%**

Kilde: Danmarks Statistik (VITA-undersøgelsen 2022).

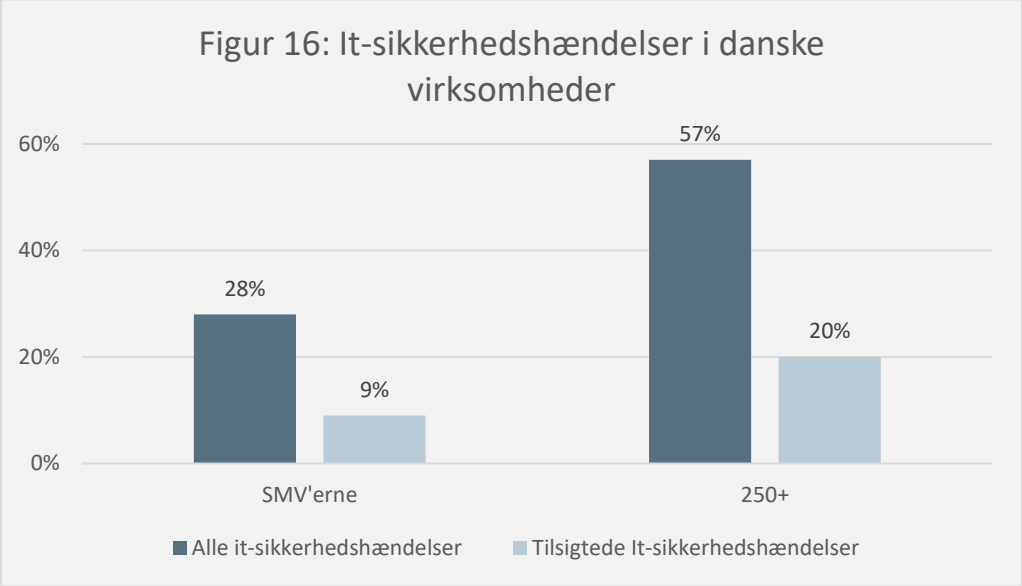
Det findes dog relevant – som i tidligere år – også at se isoleret på de ondsindede/forsætlige it-sikkerhedshændelser (kategorierne A, B, E og F i *tabel 3*). *Figur 15* viser disse tilsigtede it-sikkerhedshændelser og andelen af virksomheder, som har været udsat for dem i 2021. Som figuren viser, har flest SMV'er såvel som store virksomheder været udsat for *"utilgængelighed af it-tjenester på grund af angreb udefra, fx ransomware -angreb, Denial of Service-angreb"*. Dernæst er *"It-relateret økonomiske svindel, fx CEO fraud"* den hyppigst oplevede it-sikkerhedshændelse for begge virksomhedsgrupper.



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2022).
Note: Virksomhederne har haft mulighed for at angive flere it-sikkerhedshændelser (multiple choice svar).

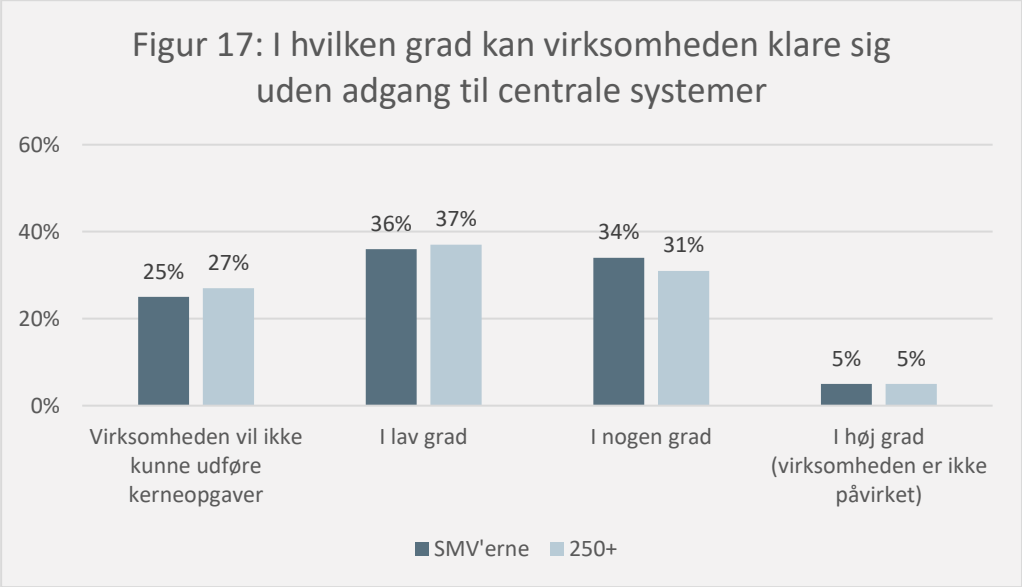
Samlet set har 28 pct. af SMV'erne og 57 pct. af de store virksomheder oplevet en it-sikkerhedshændelse i 2021, hvoraf 9 pct. af SMV'erne og 20 pct. af de store virksomheder har oplevet en ondsindet, tilsigtet it-sikkerhedshændelser, som vist i *figur 16*.

Disse tal må dog antages at være konservative resultater, da der ofte er mørketal forbundet med selvrapporterede svar om it-sikkerhedshændelser. Det skyldes, at virksomheder ikke er forpligtet til at rapportere alle former for it-sikkerhedshændelser og ofte ikke ønsker at dele, hvis de har været ramt af et cyberangreb (fx for ikke at miste tillid fra kunder og samarbejdspartnere) eller ikke ved, at de faktisk har været udsat for en it-sikkerhedshændelse. Det er heller ikke usandsynligt at en andel af de virksomheder, som tror at de har oplevet en utilsigtet hardware- eller softwarefejl muligvis har oplevet en ondsindet handling udefra. Hverken Digitaliseringsstyrelsen eller andre organisationer har således det fulde overblik over antallet af it-sikkerhedshændelser blandt danske virksomheder.



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2022).
Note: Sikkerhedshændelser med forsætlig handling defineres som kategorierne A, B, E og F i tabel 3.

En konsekvens ved et vellykket cyberangreb kan være, at virksomheden midlertidig mister adgang til centrale it-systemer. Her viser resultaterne (ikke overraskende), at størstedelen af virksomhederne er meget afhængige af deres systemer, da 61 pct. af de danske SMV'er i lav grad eller slet ikke kan udføre deres kerneopgaver, hvis virksomheden mister adgangen til centrale interne it-systemer (fx ordresystem, lagersystem, økonomisystem, kommunikationsmidler, kundedatabase, intranet osv.).



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2022).

SMV’ernes fokus på datetik og sammenhæng til digital sikkerhed

6. SMV'ernes fokus på dataetik og sammenhæng til digital sikkerhed

Det er afgørende, at danske virksomheder udviser digital ansvarlighed for at bevare forbrugernes tillid til de digitale løsninger. Digital ansvarlighed handler ikke kun om at skabe digitalt sikre produkter, men også om ansvarlig brug af data, herunder at indsamle, bearbejde og anvende data på ansvarlig vis. Med andre ord dækker digital ansvarlighed både over digital sikkerhed og dataetik. Flere steder tænkes dataetik og digital sikkerhed også sammen. Et eksempel er **D-mærket**, som er en dansk mærkningsorden for it-sikkerhed og ansvarlig dataanvendelse, der guider virksomhederne til nemmere at få overblik over, hvad de skal leve op til inden for datasikkerhed, databeskyttelse og dataetik. Et andet eksempel er Digitaliseringsstyrelsens **guide og tjekliste**, som kan hjælpe bestyrelser med at tage hul på diskussioner om digital ansvarlighed, herunder at drøfte forskellige temaer inden for dataetik og digital sikkerhed.

Derfor handler dette afsnit om sammenhængen mellem virksomheder der arbejde med digital sikkerhed og dataetik. Først introduceres begrebet dataetik:

Tekstboks: Kort beskrivelse af dataetik

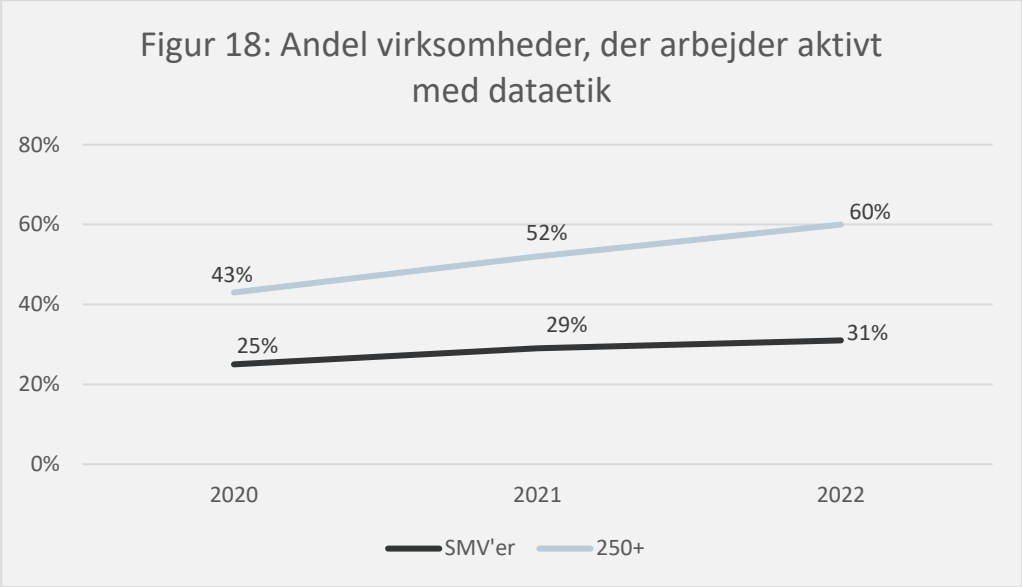
Begrebet dataetik forstås overordnet som den etiske dimension af forholdet mellem på den ene side teknologi og på den anden side borgernes grundlæggende rettigheder, retssikkerhed og grundlæggende samfundsmæssige værdier, som den teknologiske udvikling giver anledning til at overveje.

Dataetik vedrører dermed de etiske overvejelser, som den enkelte virksomhed bør gøre sig i forbindelse med ansvarlig brug af data og nye teknologier.

Dataetik er relevant for anvendelsen af alle former for data. Det går videre end gældende krav til data- og privatlivsbeskyttelse i snæver forstand, fx reglerne i databeskyttelsesforordningen og databeskyttelsesloven.

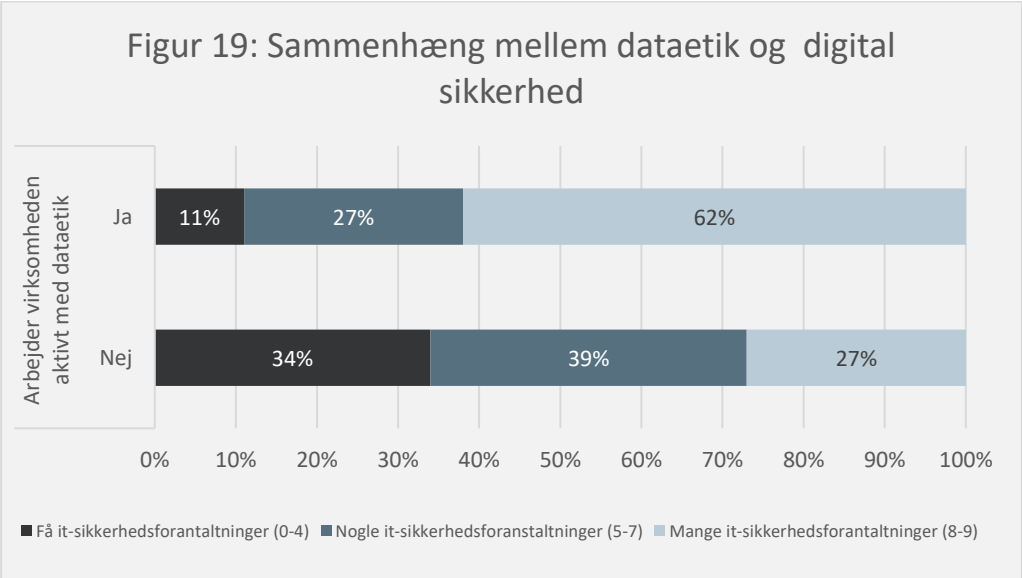
Bliv klogere på dataetik på Virksomhedsguiden.dk

Figur 18 viser andelen af virksomheder, der arbejder aktivt med dataetik fra 2020 til 2022. I lighed med virksomhedernes arbejde med digital sikkerhed, har virksomhedsstørrelse også betydning for arbejdet med dataetik. Der er flere store virksomheder med 250+ ansatte end SMV'er, som arbejder aktivt med dataetik, ligesom der også findes den største stigning i virksomheder, der arbejder med dataetik blandt de store virksomheder, jf. *figur 18*.



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2022).

Figur 19 viser sammenhængen mellem, hvorvidt SMV'erne arbejder aktivt med dataetik eller ej og hvor mange tekniske it-sikkerhedstiltag, som virksomheden anvender. Som det fremgår er der en tydelig tendens til, at virksomheder, der har fokus på digital sikkerhed også har fokus på dataetik og vice versa. Fx er det hele 62 pct. af dem, som arbejder med dataetik, der anvender mange it-sikkerhedstiltag, hvilket kun gælder 27 pct. af de virksomheder, som ikke arbejder med dataetik. Denne forskel er signifikant kontrolleret for størrelse og branche.



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2022).

Sideløbende med indsatsen for at løfte SMV'ernes digitale sikkerhed arbejder Digitaliseringsstyrelsen også for at understøtte SMV'ernes arbejde med dataetik. Det har blandt andet resulteret i vejledning og værktøjer, som kan hjælpe virksomheder i gang eller videre med ansvarlig datahåndtering og dataetik, som beskrevet i *tabel 4*.

Vejledning om dataetisk redegørelse i årsrapport	**Dataetisk dilemmaspil**	**Dataetiske retningslinjer**	**Tjekliste til bestyrelsen**
Vejledningen henvender sig til virksomheder, som vil i gang med at arbejde med dataetik, udforme en dataetisk redegørelse og have input til en dataetisk politik. Det kan både give konkurrencefordele og sikre at virksomheden kommer på forkant med fremtidig regulering.	Dataetiske dilemmaspil kan bruges til at få startet samtalen om, hvordan virksomheden vil forholde sig til dataetik. Igennem spillet bliver medarbejdere i virksomheden konfronteret med dilemmaer og spørgsmål, der kan være startskuddet for en beslutning om, hvordan virksomheden gerne vil arbejde med dataetik.	Hvis virksomheden gerne vil implementere dataetik, er et godt sted at starte at formulere nogle dataetiske retningslinjer. Retningslinjerne gør det nemmere for virksomhedens medarbejdere at agere, når der opstår dataetiske dilemmaer, og de kan bruges strategisk over for kunder.	Det kan være svært at tage hul på diskussionen om digital ansvarlighed i ledelsen eller bestyrelsen. Med denne tjekliste til digital ansvarlighed, kan ledelsen eller bestyrelsen få en guide til hvordan de kan drøfte forskellige temaer inden for digital ansvarlighed.
Vejledning om dataetiks redegørelse til årsrapport	Spil dataetisk dilemmaspil	Kom i gang med at udforme dataetiske retningslinjer	Tjekliste: Få digital ansvarlighed ind i ledelsen

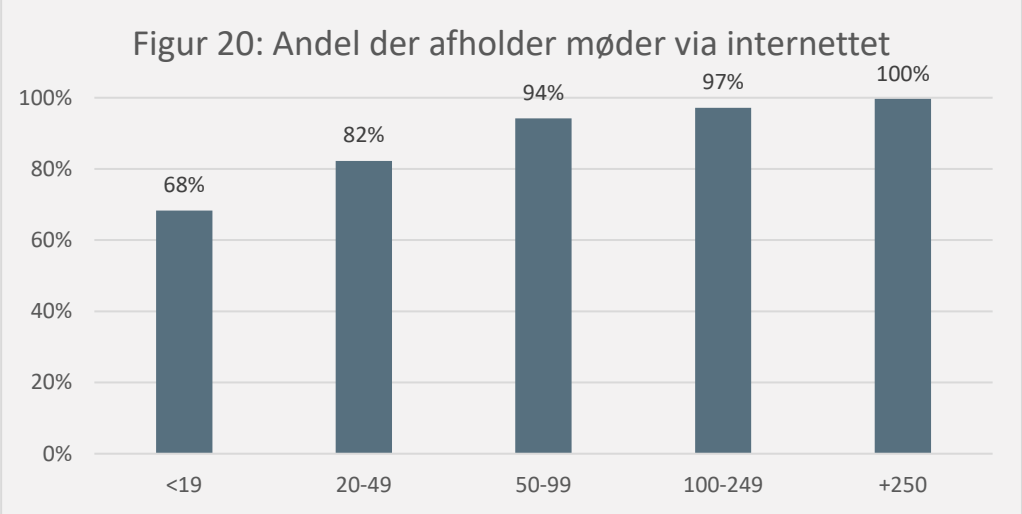
Hjemmearbejde og it-sikkerhed

7. Hjemmearbejde og it-sikkerhed

I sidste års rapport fandt vi en stigning i brugen af digitale løsninger til hjemmearbejde og undersøgte i forlængelse heraf, om sikkerheden også fulgte med, når virksomhederne i højere grad bruger flere digitale løsninger. I dette års VITA-undersøgelse er der blevet spurgt ind til virksomhedernes brug af digitale hjemmearbejdsløsninger, og om virksomhederne har retningslinjer for it-sikkerhed, når de bruger deres digitale hjemmearbejdsløsninger.

7.1 It-sikkerhed og onlinemøder

Figur 20 viser hvor stor en andel af virksomhederne, der afholdte møder via internettet i 2021. Tallene er inddelt i virksomhedsstørrelse, og det er tydeligt, at møder over internettet er udbredte både blandt SMV'erne og de store virksomheder. Der er herudover en tendens til, at større virksomheder i højere grad anvender onlinemøder.

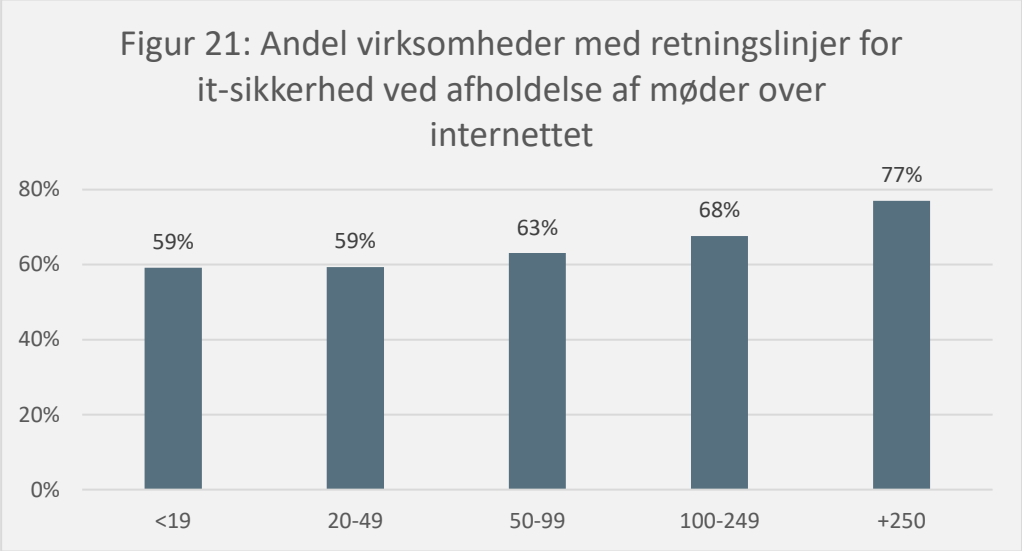


Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2022).

De mindste virksomheder er ofte de mindst digitaliserede, hvilket også er tilfældet her, men det er alligevel en bemærkelsesværdig stor andel af selv de mindste virksomheder, som afholder møder via internettet. Når løsningen er så udbredt, er det også vigtigt, at virksomhederne forholder sig til, om der er sikkerhedsrisici forbundet med at afholde møder over internettet.

Figur 21 viser andelen af virksomhederne, som afholder møder over internettet, som også har retningslinjer for it-sikkerheden for møder afholdt over internettet. Tabellen er igen inddelt i virksomhedsstørrelse, og der er samme tendens, hvor en større

andel af større virksomheder har retningslinjer for it-sikkerheden ved afholdelse af møder over internettet.

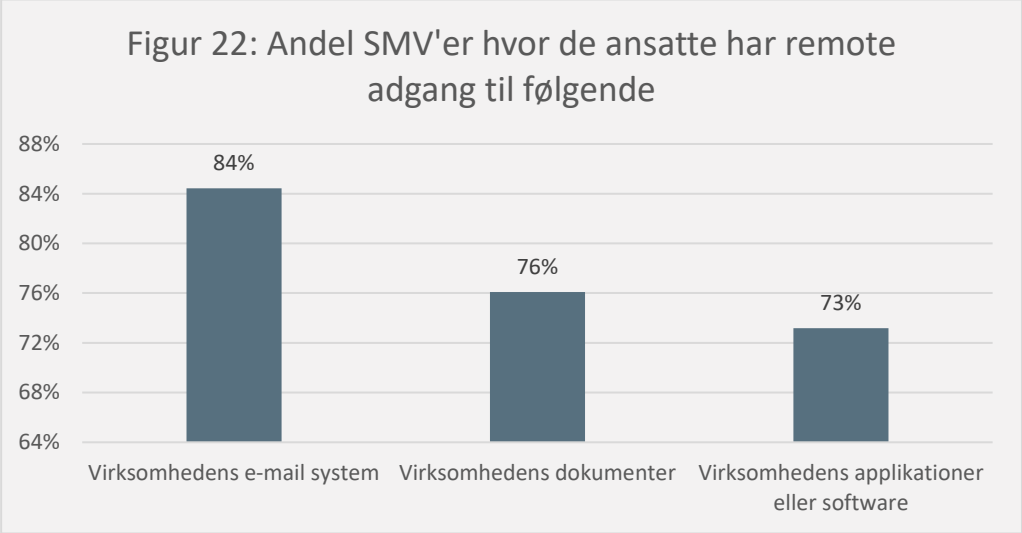


Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2022).

For virksomheder med under 49 ansatte har 41 pct. ingen retningslinjer for it-sikkerheden ved afholdelse af møder over internettet. En del af forklaringen på dette tal kan være, at mange virksomheder betragter onlinemøder som et lukket rum. Center for Cybersikkerhed anbefaler i stedet, at virtuelle mødeplatforme betragtes som åbne fora. Center for Cybersikkerhed har lavet en vejledning om sikkerhed på virtuelle mødeplatforme (**råd om sikkerhed på virtuelle mødeplatforme, CFCS.dk)**, som med fordel kan konsulteres, hvis man ønsker at øge sikkerheden i sine møder afholdt over internettet.

7.2 It-sikkerhed og remote adgang

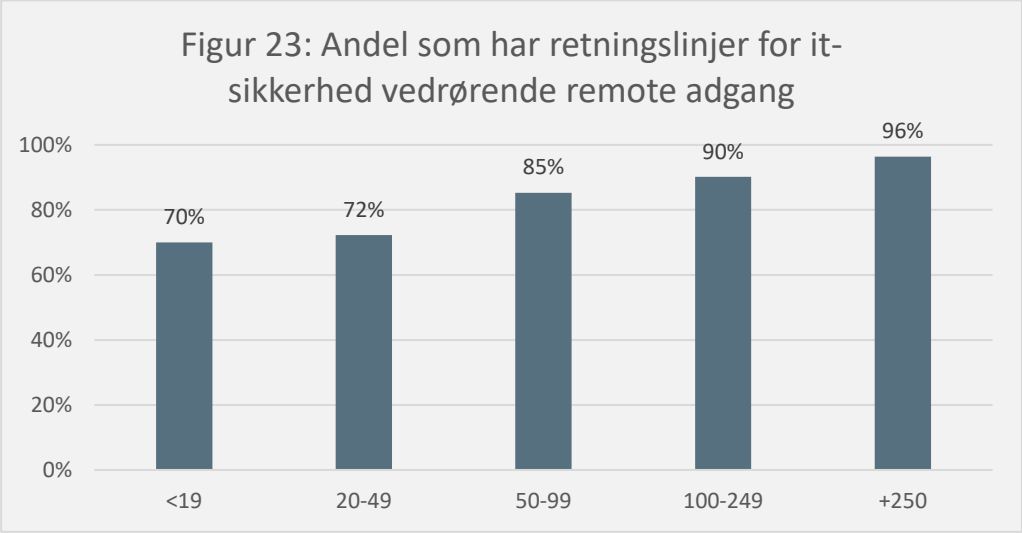
Figur 22 viser hvor stor en andel af SMV'erne, der understøtter, at ansatte har remote adgang til en række funktioner i virksomheden (e-mail system, dokumenter og applikationer/software). Det overordnede billede er, at remote adgang er meget udbredt blandt SMV'erne, uanset hvilken funktionalitet der er tale om.



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2022).

Blandt SMV'erne er det mest udbredt, at medarbejderne har adgang til virksomhedens e-mail system. 84 pct. af SMV'erne har denne mulighed, hvilket formentlig hænger sammen med, at mange bruger e-mail systemer som eksempelvis Microsoft Outlook, som uden problemer kan tilgås fra telefon og computer hjemmefra.

Figur 23 viser hvor stor en andel af virksomhederne, som har retningslinjer for it-sikkerhed vedrørende remote adgang. Tabellen er inddelt i virksomhedsstørrelse og tendensen er, at en større andel af større virksomheder har retningslinjer vedrørende remote adgang. Herudover gælder det generelt for en stor del af virksomhederne, at de har retningslinjer for it-sikkerhed vedrørende remote løsninger.



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2022).

For de mindste virksomheder har 30 pct. af dem, som bruger remote løsninger, ingen retningslinjer for it-sikkerheden.

Der er en risiko forbundet med distancearbejde, da remote adgang til virksomhedens informationer kan betyde, at noget information ender steder det ikke skal. Center for Cybersikkerhed har lavet en guide til, hvordan man som virksomhed arbejder sikkert fra distancen: **Beskyt organisationen: Opdater sikkerhedspolitikkerne til en »ny normal« (cfcs.dk)**.

Dette afsnit viser samlet set, at digitale hjemmearbejdsløsninger er meget udbredte uanset virksomhedsstørrelse. Det viser også, at retningslinjer for it-sikkerhed ved brugen af disse løsninger er relativt udbredte, omend særligt de mindste virksomheder halter lidt bagefter.

Metode

8. Metode

Virksomhedernes arbejde med digital sikkerhed måles via den årlige undersøgelse 'IT-anvendelse i virksomhederne' (VITA). I alt indgår 4.193 virksomheder i undersøgelsen, som gennemføres af Danmarks Statistik. Virksomhederne i undersøgelsen har minimum 10 årsværk og tilhører de private, ikke-finansielle byerhverv. Analysen fokuserer primært på de små og mellemstore virksomheder med 10-249 ansatte, som udgør 3.713 af besvarelserne i datasættet.

Ud over den årlige VITA-undersøgelse (blandt virksomheder med 10+ ansatte) har Danmarks Statistik også gennemført en temaanalyse i 2022 blandt de helt små danske virksomheder med 5-9 ansatte (mikrovirksomheder), som indgår i rapportens afsnit 2.4. Dette datasæt består af gennemførte besvarelser fra i alt 1.537 virksomheder i de private, ikke-finansielle byerhverv med 5-9 fultidsansatte.

I analysen benyttes vægtet data således, at stikprøven afspejler den fulde population af virksomheder inden for de private, ikke-finansielle byerhverv. Analysen er gennemført på grundlag af det nyeste tilgængelige data indsamlet i VITA 2022.

Ved læsning af analysens resultater skal der dog 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 2022. Særligt i lyset af at der ved flere spørgsmål – fx hvad angår antallet af it-sikkerhedshændelser – spørges til situationen i 2021, hvilket for eksempel ligger før Ruslands invasion af Ukraine.

Det skal herudover bemærkes, at VITA-data er baseret på selvrapporterede besvarelser. 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 selvrapporteret survey data. I denne analyse 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 10 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 it-sikkerhedstiltag og basale it-sikkerhedstiltag

Til afdækning af virksomhedernes brug af tekniske sikkerhedstiltag anvendes de 9 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 8 blandede karakterer og periodevis ændring af adgangskode.
- Systematisk opdatering af software (inkl. styresystemer).
- Biometriske metoder til bruger-identifikation og autentifikation. Fx baseret på fingeraftryk, stemmegenkendelse eller ansigtsscanning.
- Kryptering af data, filer eller e-mails.
- Backup af data til en alternativ geografisk placering. Herunder backup som cloud computing service.
- Adgangskontrol til netværk. Styring af adgang fra digitale enheder og brugere af 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.

Foruden måling af de enkelte sikkerhedstiltag bruges der i analysen et samlet indeks, som måler virksomhedernes digitale sikkerhedsniveau på tværs af de ovenstående 9 forskellige tekniske sikkerhedsforanstaltningen. Disse 9 sikkerhedstiltag skal ikke ses som en udtømmende liste af sikkerhedsforanstaltninger, men de skal i stedet anses som en proxy for virksomhedernes digitale niveau.

Det samlede indeks, til måling af virksomhedernes digitale sikkerhedsniveau, er bygget op omkring, hvor mange sikkerhedsforanstaltninger virksomhederne anvender. Der ses på antallet af foranstaltninger, fordi der ikke findes en entydig definition på, hvilke der er vigtigst for virksomhederne. I denne analyse er de 9 sikkerhedstiltag opdelt i følgende tre kategorier: få, nogle og mange tekniske it-sikkerhedsforanstaltninger pba følgende operationalisering:

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

Basale it-sikkerhedstiltag

To sikkerhedsforanstaltninger anses som værende helt centrale, ligesom de også indgår i langt de fleste anbefalinger for it-sikkerhed. Disse sikkerhedstiltag er 'Backup af data' og 'Systematisk opdatering af software'[21]. 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 et af de to centrale sikkerhedstiltag. Dette er i tråd med en tidligere analyse, som Deloitte har udarbejdet[22]. De to sikkerhedstiltag (backup af data og systematisk opdatering af software) rapporteres som 'basale sikkerhedstiltag' igennem rapporten.

8.2 Måling af hhv. it-sikkerhedsniveau og risikoprofil

Det følgende er en beskrivelse metoden, til at Indeksere de danske SMV'ers digitale sikkerhedsniveau og risikoprofil samt matchet mellem dem. Den bygger på en metode udviklet af PwC.

Metodikken står også beskrevet i "Digital Sikkerhed i danske SMV'er" (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.

Den opsummerede effekt af disse forskelle på sammenligneligheden mellem tallet for denne rap-port, og det tilsvarende tal i den tilsvarende rapport fra sidste år, beskrives i afsnittet nedenfor, sammen med andre metodiske forbehold.

Sammenlignelighed mellem it-sikkerhedsniveau/risikoprofil-tal 2020 og 2021 samt metodiske forbehold

Metoden bygger på et overordnet framework, som er beskrevet nedenfor, hvor en række spørgsmål samlet skal udgøre 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 sidste år, mens nogle af spørgsmålene, også kaldet indikatorerne, varierer.

---

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

Variationer i spørgsmålsformuleringer kan påvirke respondenters svar, ligeledes kan variationer i spørgeskemaet som helhed. Der er dog tale om relativt små variationer i spørgsmålsformuleringer mellem årets og sidste års rapport. Spørgeskemaet som helhed har ændret sig mere substantielt.

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 lille forbehold herfor, når tallene sammenlignes på tværs af årene.

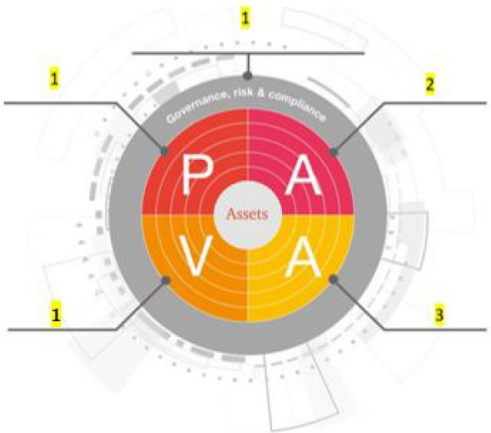
Metode og fremgangsmåde

Indekset for SMV'ernes it-sikkerhedsniveau baserer sig på spørgsmål, der siger noget om, hvilke sikkerhedstiltag SMV'erne har implementeret – fx om virksomhederne har en plan for, hvordan de håndterer personoplysninger, og om de har implementeret backup af data. Indekset for SMV'erne 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, Pro-cesser, 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 sårbarhedsef-fekt, hvilket er vist i figur 1. Vægtningen er baseret på en betragtning om, at en svaghed i sikker-hedstiltag 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).

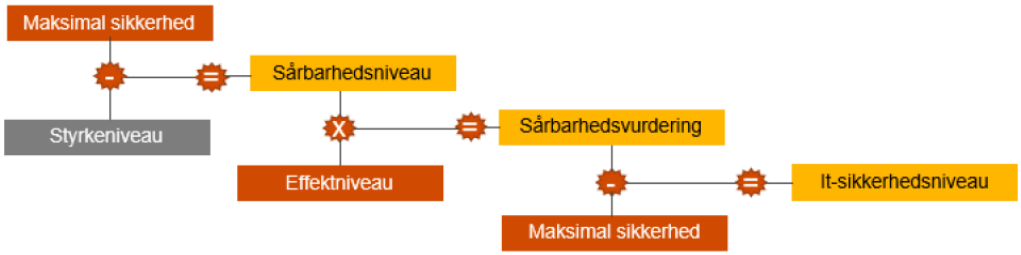
Hvert spørgsmål har også fået tildelt en pointscore, som går fra 0 til 5 – baseret på spørgsmålets svarmulighed. De otte udvalgte spørgsmål samt deres scorer og vægt fremgår af tabellen nedenfor.

#	Spørgsmål	Score	Vægt
	Governance, risk & compliance		
1	I hvilket omfang tager virksomhedens topledelse og/eller bestyrelse stilling til virksomhedens it-sikkerhedsmæssige aktiviteter	0-5	1
2	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 2021 tilbudt opkvalificering af it-færdigheder til følgende: a) it-specialister, b) øvrige ansatte	0-5	1
	Processer		
4	Hvem udførte virksomhedens it-funktioner i 2021	0-5	1
5	Bruger virksomheden følgende it-sikkerhedsmæssige foranstaltninger: risikoanalyse?	0-5	1
	Validering		
7	Har virksomheden haft følgende it-sikkerhedshændelser i 2021? a) utilgængelighed af it-tjenester på grund af angreb udefra, fx. Ransomwareangreb, 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, pharming, phishing-angreb forsætlige handlinger fra egne medarbejdere d) it-relateret økonomisk svindel.	1-4	1
	Arkitektur		
8	Bruger virksomheden følgende it-sikkerhedsmæssige foranstaltninger? A) stærke adgangskoder til autentificering, b) systematisk opdatering af software (inkl. Styresystemer), c) kryptering af data, filer eller e-mails, d) backup af data til en separat placering, e) adgangskontrol til netværk, f) VPN (virtuelt privat netværk), g) lagring af log-filer h) test af it-sikkerhed	0-5	3

Der er små forskelle i spørgsmålsformuleringerne i sikkerhedsniveau-indekset fra rapporten i 2022, og indekset brugt i årets rapport. Der er dog tale om minimale forskelle eks. er "(inkl. Styresystemer)" tilføjet til svarmulighed b) under arkitektur om systematisk opdatering af software. Forskelle af denne størrelse vurderes at have en lille til ingen effekt.

Model for beregning af it-sikkerhedsniveau

Scoringsværdien for SMV'ernes it-sikkerhedsniveau fastlægges ved at anvende metoden jf. figur 2. 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 maksi-male 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.

Beregning af sårbarhedsvurdering
For at foretage en sårbarhedsvurdering tager man udgangspunkt i sårbarhedsniveau for hvert en-kelt PAVA-område og ganger med det effektniveau, der dækket det enkelte område. Sårbarheds-vurderingen 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 sikkerheds-score 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 og konsekvens. 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 sikker-hedshændelse, mens konsekvensscoren betegner, hvor stor en negativ påvirkning en sikkerheds-hændelse kan/vil have for virksomheden. Risiko er en beregning af sandsynligheden for, at en hæn-delse 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 sektor-scoren beror på en ekspertvurdering fra PwC. I Dansk 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
Handelssektor	1
Uddannelsessektor	1
Finanssektor	3
Energisektor	3
Telesektor	3
Byggesektor	1
Transportsektor	2
Fødevaresektor	2
Drikkevandssektor	2

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	
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? Og vil medføre væsentlige problemer, hvis de bliver delt eller hacket? 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 sand-synlighed. 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 risikosco-re i intervallet 30-63 giver derfor en middel risikoprofil, og en risikoscore under 30 og over 63 giver henholdsvis en lav og høj risikoprofil.

Sandsynligheds-score (3-11)	**Konsekvens-score (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.

<table>
<tr><td colspan="2"></td><td colspan="3">It-sikkerhedsniveau</td></tr>
<tr><td colspan="2"></td><td>Lav</td><td>Middel</td><td>Høj</td></tr>
<tr><td rowspan="3">Risikopro-fil</td><td>Høj</td><td rowspan="2">De sårbare 35 pct.</td><td colspan="2"></td></tr>
<tr><td>Middel</td><td>De tilpas sikrede 52 pct.</td><td rowspan="2">De påpasselige 13 pct.</td></tr>
<tr><td>Lav</td><td></td><td></td></tr>
</table>

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.

digst.dk