Digital sikkerhed i danske SMV'er

September 2022

Erhvervsstyrelsen

Analysens hovedresultater er:

It-sikkerhedsforanstaltninger og SMV'ernes sikkerhedsniveau

- 25 pct. af de danske SMV'er anvendte *ikke* de to basale it-sikkerhedsforanstaltninger i 2020: opdatering af styresystemer og backup af data. Det er omtrent på samme niveau som i 2018 og 2019.
- 44 pct. af SMV'erne har et for lavt sikkerhedsniveau i forhold til deres sikkerhedsprofil.
- Andelen af SMV'erne som benytter mange it-sikkerhedsforanstaltninger (mellem 8-9) er steget med fire procentpoint siden 2018. Til sammenligning har andelen som benytter få it-sikkerhedsforanstaltninger (mellem 0-4) været nogenlunde stabil over samme periode.

It-sikkerhed og digitalisering i et covid-år

- Som følge af covid-19 har 68 pct. af SMV'erne et øget brug af remote løsninger. SMV'erne der har forøget sit brug af remote løsninger, er også mere digitalt sikre.
- 55 pct. af SMV'erne som har øget forbruget af to eller flere remote løsninger har implementeret mange it-sikkerhedsforanstaltninger (mellem 8-9).
- Til sammenligning har 54 pct. af SMV'erne, som ikke har et forøget brug af nogen remote løsninger, implementeret få it-sikkerhedsforanstaltninger (mellem 0-4).

Udfordringer og begrænsninger ved at øge it-sikkerhedsniveauet

- Mangel på viden og kompetencer til at håndtere it-sikkerhedsløsninger er SMV'ernes største udfordring med at hæve it-sikkerhedsniveauet, mens den største udfordring for virksomhederne med over 250 ansatte er manglende tilslutning fra medarbejderne.
- Således svarer 12 pct. af SMV'erne, at de ikke har viden og kompetencer, til at øge deres it-sikkerhed. Til sammenligning svarer kun 3 pct., at det er mangel på specifikke løsninger på markedet, der udgør en begrænsning.

It-sikkerhedshændelser

- I 2020 oplevede 17 pct. af de danske SMV'er mindst en af følgende fire it-sikkerhedshændelser: 1. blokeret adgang til it-services, 2. sletning, ødelæggelse, misbrug eller videregivelse af data (forsætligt eller utilsigtet), 3. it-relateret økonomisk svindel og 4. andre it-sikkerhedshændelser.
- Den mest udbredte it-sikkerhedshændelse er blokeret adgang til it-services (hvis man ser bort fra kategorien "andre it-sikkerhedshændelser").
- Således har 7 pct. af SMV'erne oplevet denne it-sikkerhedshændelse, mens det til sammenligning er 19 pct. af virksomhederne med over 250 ansatte.

Dataetik og it-sikkerhed

- De SMV'er som arbejder aktivt med dataetik, har implementeret flere it-sikkerhedsforanstaltninger, end de SMV'er som ikke arbejder aktivt med dataetik.

Introduktion

Danmark og danske virksomheder er i dag blandt EU's mest digitaliserede. Dette bidrager til at gøre it-sikkerhed til et vigtigt emne for det danske erhvervsliv. Center for Cybersikkerhed vurderer, at truslen fra cyberkriminalitet er meget høj. Det betyder, at det anses for meget sandsynligt, at danske virksomheder vil blive udsat for forsøg på cyberkriminalitet[1].

Et cyberangreb kan have store omkostninger for virksomhederne som følge af f.eks. tabt arbejdsfortjeneste og mistede data. Baseret på dette års VITA-data er det således 30 pct. af de danske SMV'ers egen vurdering, at de ikke ville kunne udføre deres kerneopgaver, hvis de mistede adgangen til centrale it-systemer. SMVdanmark vurderer eksempelvis, at et typisk ransomware-angreb på en virksomhed med 10-49 ansatte i gennemsnit koster 376.350 alene i tabt omsætning fra e-handel[2].

Det er derfor enormt vigtigt for både samfundet og den enkelte virksomhed at have fokus på digital sikkerhed. Ved at fokusere på og udvikle it-sikkerheden, i både SMV'er og store virksomheder, vil det danske erhvervsliv stå stærkt og modstandsdygtigt overfor fremtidens digitale angreb. Erhvervsstyrelsen udvikler derfor et sortiment af gratis vejledninger, værktøjer og awareness-aktiviteter særligt målrettet de danske SMV'er.

Med henblik på at forbedre denne indsats har Erhvervsstyrelsen udarbejdet nærværende rapport om digital sikkerhed i de danske SMV'er. Formålet med rapporten er at give et bredt indblik i de danske virksomheders arbejde med digital sikkerhed, samt kortlægge de udfordringer, som virksomhederne står overfor på it-sikkerhedsfronten.

[1] Cybertruslen mod Danmark (cfcs.dk)

[2] https://smvdanmark.dk/analyser/temaanalyser/cyberangreb-kan-blive-en-dyr-omgang-for-smverne

Afgrænsning og datagrundlag

Rapporten er bygget på data fra Danmarks Statistiks årlige spørgeskemaundersøgelse "IT-anvendelse i virksomhederne".

"IT-anvendelse i virksomhederne" er indsamlet i 2021, men beder virksomhederne forholde sig til, og besvare ud fra, året 2020. Af samme grund er dette års "Digital Sikkerhed i danske SMV'er" den første af sin slags, som præsenterer data, der beskriver et år med covid-19. Det er obligatorisk for virksomhederne at besvare spørgeskemaet, og data er indsamlet via digital indberetning.

Danmarks Statistik har til "IT-anvendelse i virksomhederne" 2021 indsamlet besvarelser fra 4144 virksomheder med 10+ ansatte. Til sammenligning bestod undersøgelsen i 2020 af besvarelser indsamlet fra 3947 virksomheder med 10+ ansatte og i 2019 af besvarelser fra 5292 virksomheder med 5+ ansatte. Undersøgelsen har en svarrate på 96 pct., hvor den til sammenligning var på 98 pct. sidste år. Forskellen forventes kun at påvirke resultaterne i et meget begrænset omfang.

Data er vægtet i overensstemmelse med Danmarks Statistiks vægtning, for at øge besvarelsernes repræsentativitet. Data er derfor vægtet i henhold til branche og størrelse for at sikre en bedre afspejling af populationen.

Virksomhederne er opdelt på størrelse efter antal ansatte med hhv. 10-19, 20-49, 50-99, 100-249 og 250+ ansatte, samt "SMV'erne" som udgøres af alle virksomheder med under 250 ansatte, altså virksomheder med 10-249 ansatte.

For enslydende spørgsmål om virksomhedernes arbejde med digital sikkerhed er ændringer fra 2020 til 2021 som udgangspunkt udregnet og præsenteret i rapporten.

1. It-sikkerhedsforanstaltninger

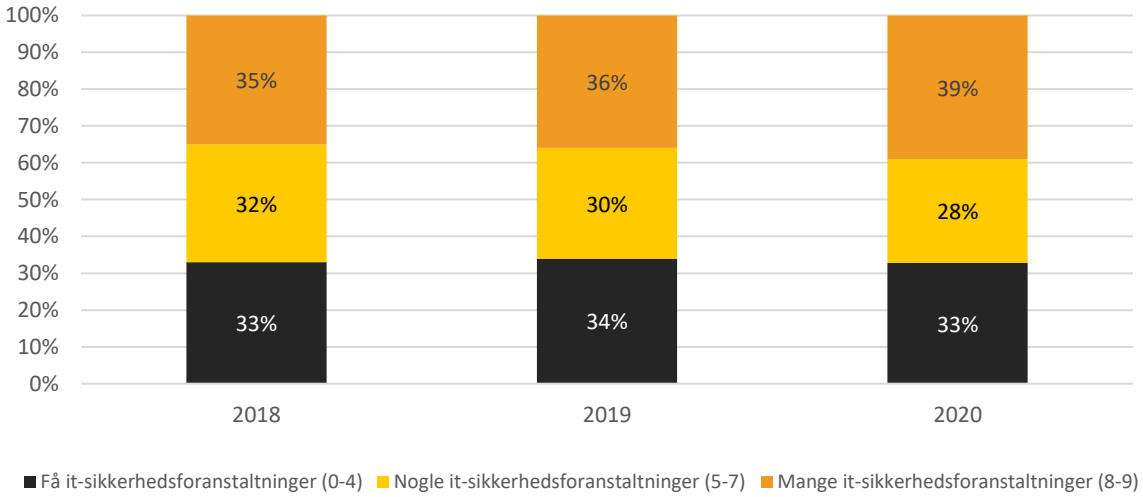
Det følgende undersøger virksomhedernes brug af it-sikkerhedsforanstaltninger. Følgende it-sikkerhedsforanstaltninger indgår i undersøgelsen[3]:

- Stærke adgangskoder
- Systematisk opdatering af software
- Kryptering af data, filer eller e-mails
- Backup af data til en alternativ geografisk placering
- Adgangskontrol til netværk
- VPN
- Lagring af log-filer
- Risikoanalyse
- Tests af it-sikkerhed

1.1 Stigning i andel SMV'er med mange it-sikkerhedsforanstaltninger

Figur 1 viser, hvordan SMV'erne fordeler sig på brugen af it-sikkerhedsforanstaltninger fra 2018 til 2020. En tendens mellem årene er, at andelen af SMV'er med få it-sikkerhedsforanstaltninger (0-4) er forholdsvis stabil, andelen med nogle it-sikkerhedsforanstaltninger (5-7) er blevet marginalt mindre, mens andelen af SMV'er med mange it-sikkerhedsforanstaltninger (8-9) er blevet marginalt større.

Figur 1: SMV'ernes brug af it-sikkerhedsforanstaltninger 2018-2020



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2021).

Data viser altså en lille positiv fremgang i andelen med mange implementerede it-sikkerhedsforanstaltninger[4].

[3] Virksomheder som ikke har backup af data og systematisk opdatering af software, kategoriseres som havende "få it-sikkerhedsforanstaltninger", da disse to foranstaltninger er helt basale for virksomhedens it-sikkerhed.

[4] Der er signifikant forskel på grupperne.

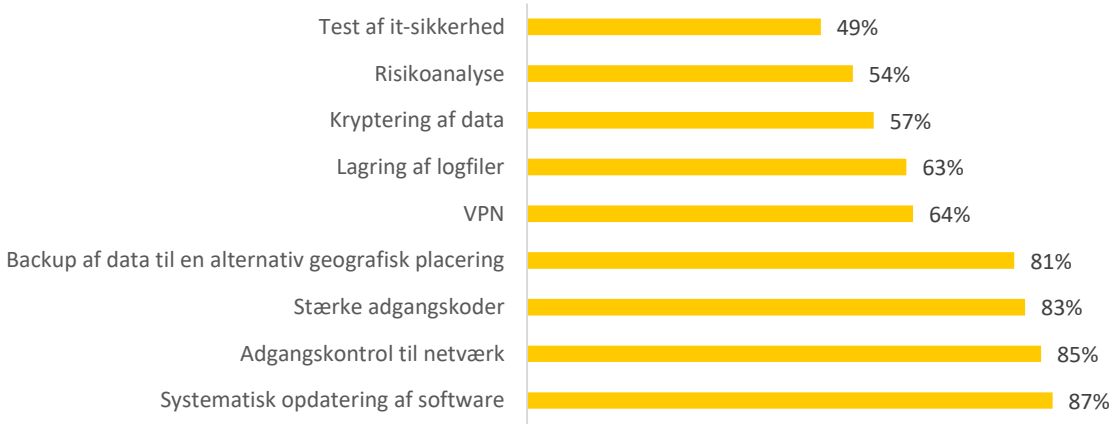
Dette kunne indikere, at SMV'er der allerede arbejder med it-sikkerhed, er mere tilbøjelige til at øge it-sikkerheden yderligere.

Zoomer man ind på brugen af de to basale sikkerhedstiltag, systematisk opdatering af software og backup af data, har 25 pct. af SMV'erne ikke indført de to tiltag. Til sammenligning var tallet i 2018 på 22 pct. og 24 pct. i 2019. Forskellen på 2019 og 2020 er på kanten af den statistiske usikkerhed, men tallene tyder på, at der har været en negativ udvikling siden 2018 på netop disse sikkerhedstiltag.

Da det virker usandsynligt, at SMV'erne er begyndt at afvikle allerede etablerede it-sikkerhedstiltag, ligger en del af forklaringen formentlig i, at andelen af mindre SMV'er udgør en større andel af populationen end i 2018. I de vægtede tal udgør SMV'erne med mellem 10-19 ansatte således 51 pct. af stikprøven i 2020, mens de i 2018 udgjorde 46 pct.. Da de mindre SMV'er generelt betragtet har færre it-sikkerhedsforanstaltninger, kan en sådan ændring i sammensætningen af SMV'erne betyde, at andelen uden de basale it-sikkerhedsforanstaltninger bliver større.

Figur 2 viser hvor stor en andel af SMV'erne, som har indført hvert af de ni tiltag. Det ene af de basale tiltag, systematisk opdatering af software, er den mest udbredt it-sikkerhedsforanstaltning, mens tests af it-sikkerhed (eksempelvis penetrationstests) er den mindst udbredte it-sikkerhedsforanstaltning blandt SMV'erne.

Figur 2: SMV'ernes brug af ni it-sikkerhedsforanstaltninger i 2020

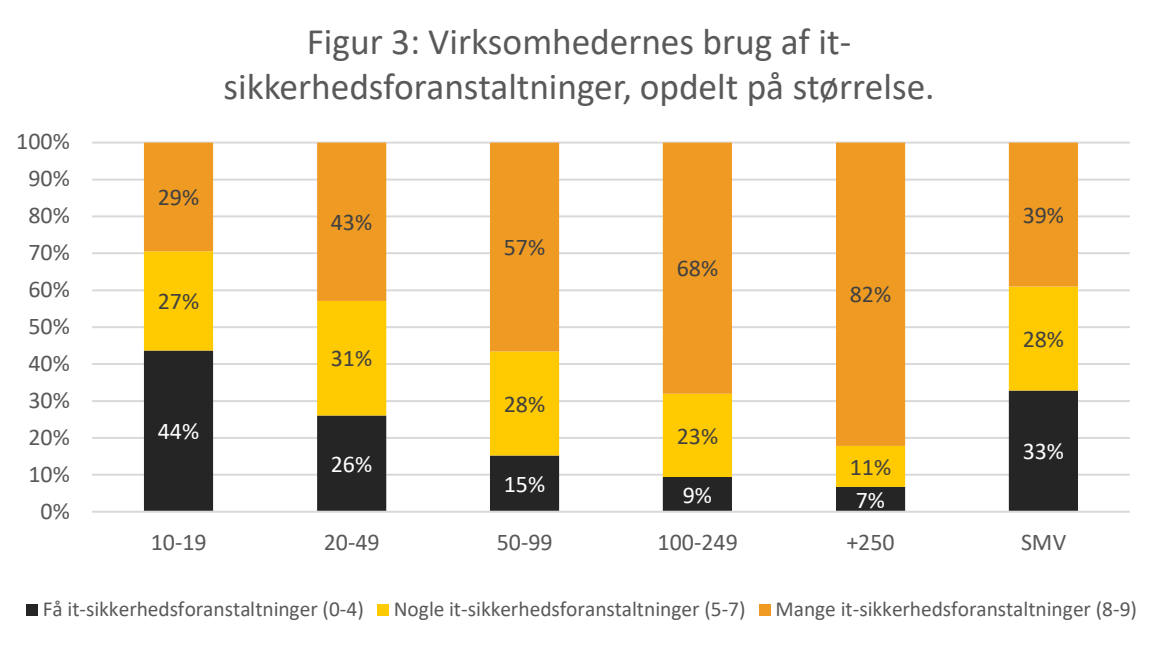


Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2021).

Adgangskontrol til netværk, backup af data, systematisk opdatering af software og brug af stærke adgangskoder er, som sidste år, de mest udbredte sikkerhedstiltag blandt SMV'erne med en andel på mellem 81 pct. og 87 pct..

1.2 Større virksomheder har flere it-sikkerhedsforanstaltninger, samt it-sikkerhedsforanstaltninger opdelt på branche

Figur 3 viser virksomhedernes brug af it-sikkerhedsforanstaltninger fordelt på virksomhedsstørrelse. Den viser en tydelig positiv sammenhæng mellem antallet af ansatte og antal sikkerhedsforanstaltninger.



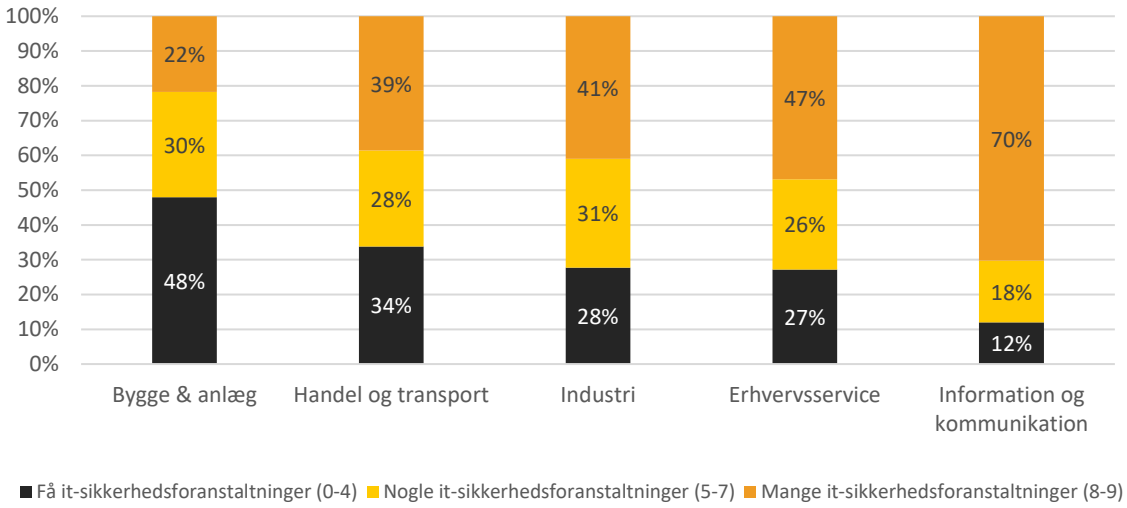
Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2021).

Således har 44 pct. af virksomhederne med 10-19 ansatte kun indført mellem 0 og 4 it-sikkerhedsforanstaltninger. Til sammenligning var samme tal for virksomheder med 100-249 ansatte på 9 pct..

Forskellen mellem SMV'erne og virksomhederne med +250 ansatte understreger samme tendens. Kun 7 pct. af virksomhederne med +250 ansatte har få it-sikkerhedsforanstaltninger, mens det er 33 pct. af SMV'erne; en forskel på 26 procentpoint.

Figur 4 viser SMV'ernes brug af it-sikkerhedsforanstaltninger opdelt på branche. Branchen med den største andel med få it-sikkerhedsforanstaltninger er bygge og anlægsbranchen (48 pct.). I den modsatte ende ligger information og kommunikationsbranchen med 12 pct..

Figur 4: SMV'ernes brug af it-sikkerhedsforanstaltninger, opdelt på branche



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2021).

I information og kommunikationsbranchen har 70 pct. mange it-sikkerhedsforanstaltninger, hvilket er 23 procentpoint mere end nr. 2 (erhvervsservice) på 47 procentpoint.

Det tyder altså på, at en mindre andel af SMV'erne har implementeret de to basale it-sikkerhedsforanstaltninger sammenlignet med 2018. Videre indikerer data, at der er sket en større udvikling blandt de SMV'er, der har nogle (5-7) eller mange (8-9) it-sikkerhedsforanstaltninger end i gruppen med få it-sikkerhedsforanstaltninger. Sidst tenderer antal it-sikkerhedsforanstaltninger til at korrelere positivt med virksomhedsstørrelse.

2. It-sikkerhed og digitalisering i et covid-år

Som følge af covid-19 sendte regeringen d. 13. marts 2020 elever og studerende på alle uddannelsesinstitutioner hjem, lukkede alle indendørs kulturinstitutioner, sendte alle ikke-kritiske offentligt ansatte hjem og opfordrede det private arbejdsmarked til at arbejde mest muligt hjemmefra.

Dermed begyndte en omstilling fra fysisk fremmøde til online hjemmearbejde.

Hjemarbejde er interessant fra et it-sikkerhedsperspektiv, da hjemarbejde kan skabe et behov for digitale løsninger. Digitale løsninger åbner samtidig for sårbarheder, som it-kriminelle kan benytte, samt potentielt også konsekvenserne ved at blive udsat for en it-sikkerhedshændelse.

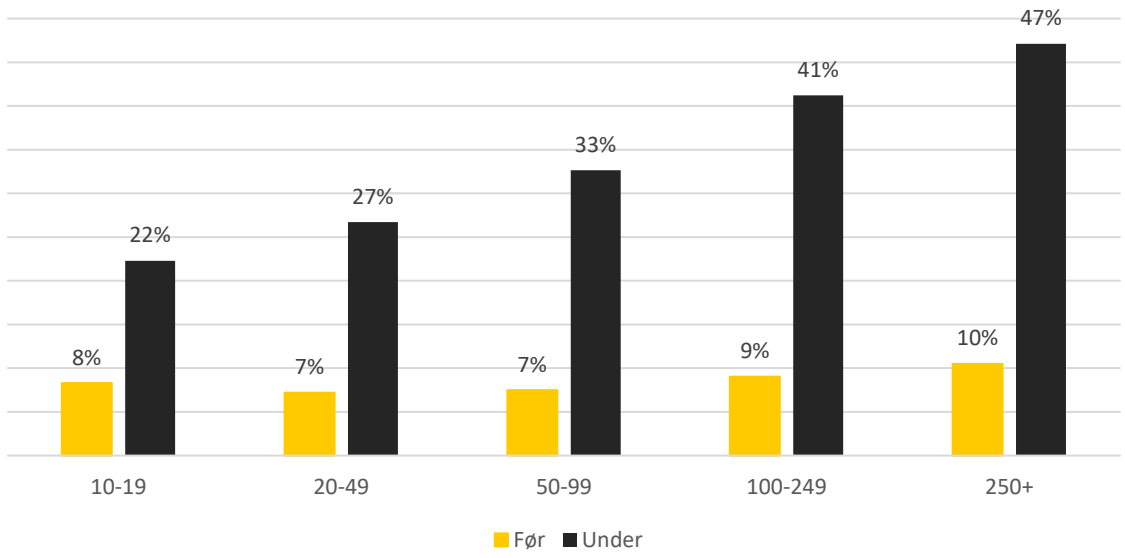
Spørgsmålet er derfor, om der er en relation mellem covid-19 og brug af digitale løsninger, og dernæst om disse løsninger også samvarierer med bedre it-sikkerhed.

I dette kapitel undersøges hjemarbejde under covid-19, brug af digitale løsninger under covid-19, samt forholdet mellem disse digitale løsninger og it-sikkerhedsforanstaltninger.

2.1 Stigning i hjemmearbejde under covid-19

Som det ses i figur 5, er andelen af medarbejdere med mindst én hjemarbejdsdag steget markant under pandemien.

Figur 5: Gennemsnitlig andel af virksomhedernes medarbejdere med hjemmearbejde mindst en dag om ugen før/under covid-19



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2021).

Mens andelen af medarbejdere med mindst én hjemarbejdsdag var forholdsvis ensartet på tværs af virksomhedsstørrelse før covid-19 (mellem 7-10 pct.), har der under pandemien været en klar tendens til, at andelen af medarbejdere med mindst én hjemarbejdsdag stiger med virksomhedsstørrelse.

Dette kan indikere, at de større virksomheder i højere grad har kunnet omstille sig til hjemmearbejde. Men det kan også være udtryk for, at mindre virksomheder, i kraft af sine færre medarbejdere, bedre har kunnet fortsætte med fysisk fremmøde, uden at bryde covid-19 retningslinjerne.

2.2 Stigning i remote løsninger som følge af covid-19

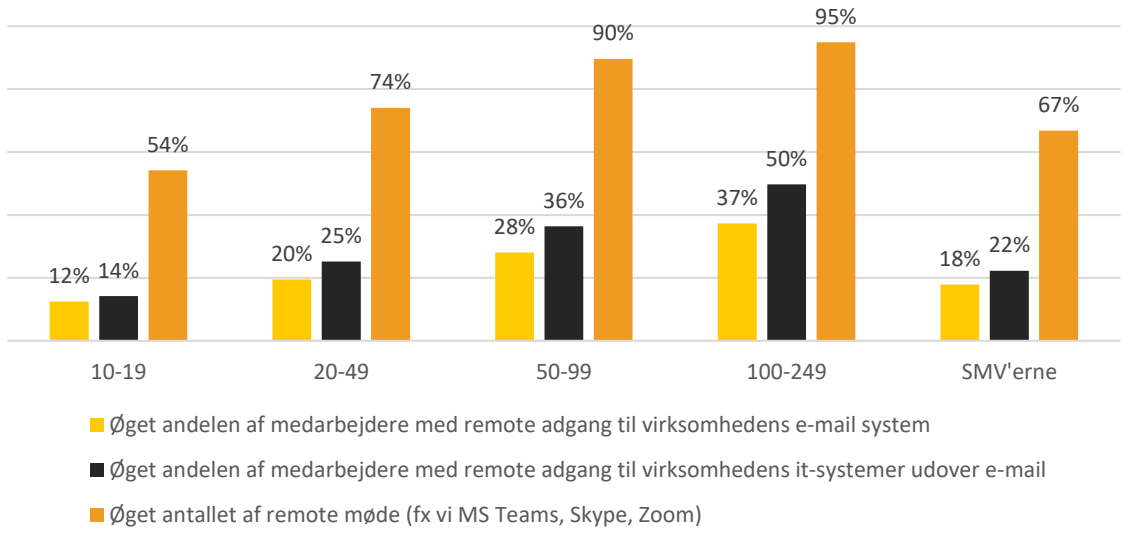
Pandemien har affødt en højere grad af hjemmearbejde. I det følgende afsnit undersøges brugen af digitale teknologier under covid-19.

Figur 6 viser om virksomhedernes andel af medarbejdere med 1. remote adgang til virksomhedens email-system, 2. remote adgang til virksomhedens it-systemer og 3. antallet af remote møder, er øget som følge af covid-19.

Den overordnede tendens er, at jo større virksomhederne er, jo større forøgelse i brugen af remote løsninger.

Dette hænger formentlig sammen med figur 5 ovenfor; de mindre SMV'er har en mindre andel medarbejdere med hjemmearbejde end de store SMV'er.

Figur 6: Har virksomheden i løbet af 2020 gjort følgende grundet COVID-19:



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2021).

Den største udvikling for SMV'erne har været andelen af remote møder, hvor 67 pct. har øget andelen af møder over tjenester som MS Teams, Skype og Zoom.

Videre har 18 pct. af SMV'erne øget andelen af medarbejdere med remote adgang til virksomhedens e-mail-system som følge af covid-19.

Ligeledes har op til 22 pct. af SMV'erne en højere andel af medarbejdere med remote adgang til virksomhedens it-systemer udover mail.

I alt har 68 pct. af SMV'erne øget én eller flere remote løsninger.

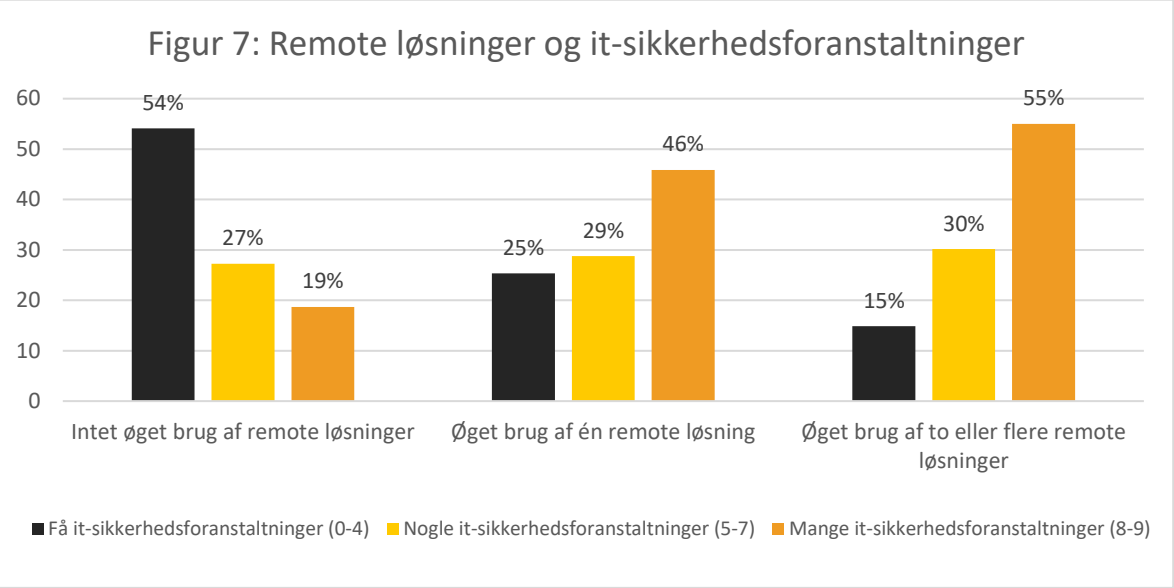
2.3 En større forøgelse i brug af remote løsninger hænger sammen med et højere antal it-sikkerhedsforanstaltninger

Figur 7 nedenfor viser forholdet mellem SMV'ernes brug af remote løsninger som følge af covid-19 og it-sikkerhedsforanstaltninger.

Tendensen er, at jo større en forøgelse i brug af remote løsninger, jo flere it-sikkerhedsforanstaltninger[5].

Andelen af SMV'er med mange it-sikkerhedsforanstaltninger bliver den største gruppe, så snart vi kigger på gruppen af SMV'er, som har øget sit brug af remote løsninger (hhv. 46 pct. og 55 pct.).

[5] Sammenhængen er signifikant ved kontrol for virksomhedsstørrelse, branche og digitaliseringsgrad.



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2021).

Omvendt har 54 pct. af de SMV'er, som *ikke* har et øget brug af remote løsninger, også kun få it-sikkerhedsforanstaltninger, mens det er 15 pct. af SMV'erne med et øget brug af to eller flere remote løsninger.

Det er overordnet set positivt, at de SMV'er, som bruger flere remote løsninger, også er mere sikre.

En hyppigt benyttet teknologi til at sikre hjemmearbejdsløsningerne er VPN. VPN er samtidig en væsentlig it-sikkerhedsforanstaltning.

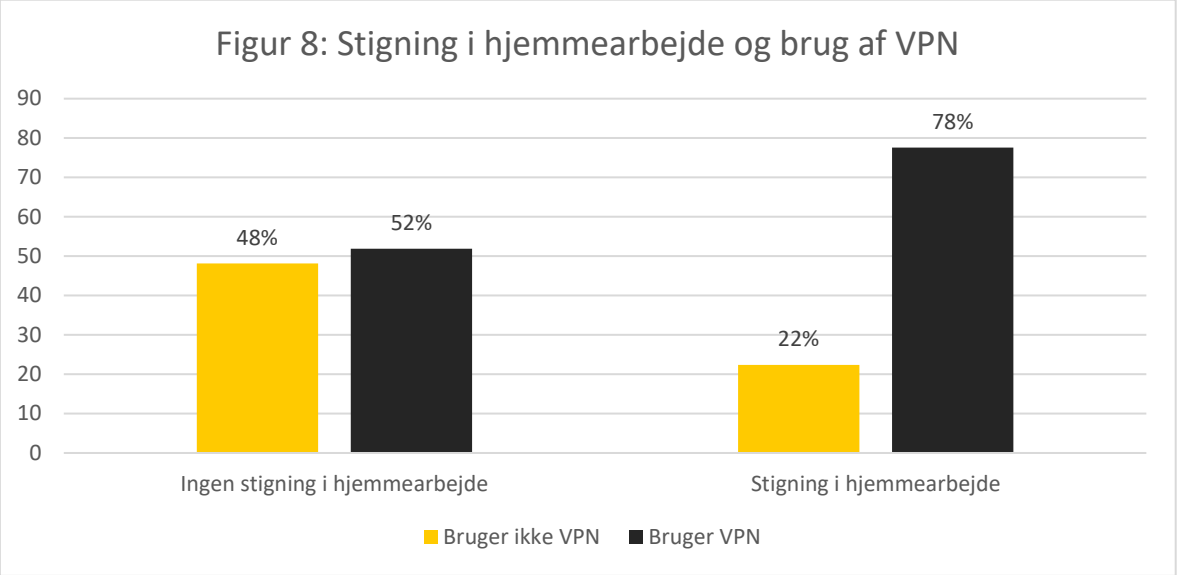
2.4 En stigning i hjemmearbejde hænger sammen med at benytte sig af VPN

Figur 8 viser forholdet mellem brug af VPN, kombineret udviklingen i hjemmearbejde efter covid-19 brød ud.

SMV'erne er inddelt i dem, som har haft en stigning i andelen af medarbejdere med hjemmearbejde mindst én dag om ugen efter covid-19 brød ud, og de hvor andelen af medarbejdere med hjemmearbejde mindst én dag om ugen er enten faldet eller uændret efter covid-19 brød ud.

Indenfor disse opdelinger viser figur 8 andelen af virksomheder med og uden VPN.

Den tydelige tendens er, at virksomheder som har haft en stigning i hjemmearbejde, også i langt højere grad benytter sig af VPN.

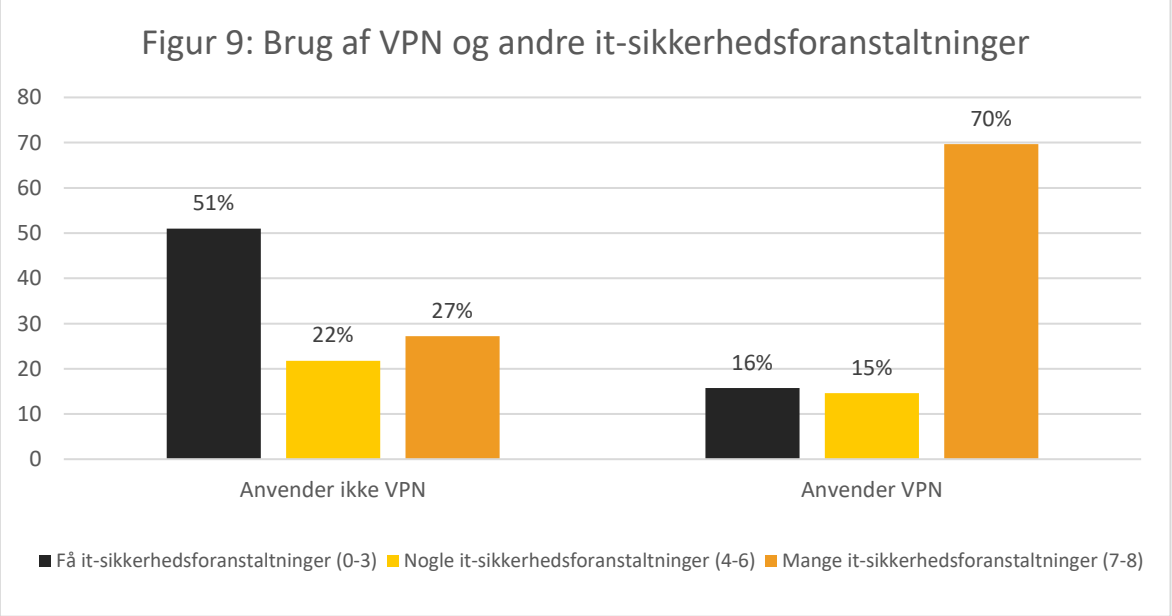


Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2021).

I gruppen af SMV'er som har haft en stigning i hjemmearbejde, bruger 78 pct. af SMV'er også VPN, mens tallet for SMV'erne uden stigning i hjemmearbejde er 52 pct. En forskel på 26 procentpoint. Ligeledes er det blot 22 pct. af SMV'erne med en stigning i hjemmearbejde, som ikke har VPN, mens tallet er over dobbelt så stort i gruppen uden en stigning i hjemmearbejde.

Den samlede andel SMV'er som bruger VPN, var i 2020 64 pct., mens tallet i 2019 var 65 pct.. Dette indikerer, at der ikke har været en substantiel stigning i brug af VPN som følge af hjemmearbejde, men at virksomheder som bruger VPN, også er mere tilbøjelige til at bruge mere hjemmearbejde.

Figur 9 viser brug af VPN og andre it-sikkerhedsforanstaltninger. Den overordnede tendens er, at SMV'er, som bruger VPN, også tenderer mod at have flere it-sikkerhedsforanstaltninger end SMV'er, der ikke gør.



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2021).

27 pct. af SMV'erne, som *ikke* anvender VPN, benytter mange it-sikkerhedsforanstaltninger, mens det er 70 pct. af SMV'erne, som anvender VPN. Dette tyder på, at én it-sikkerhedsforanstaltning sjældent kommer alene. Generelt viser data, at alle it-sikkerhedsforanstaltningerne samvarierer positivt med hinanden.

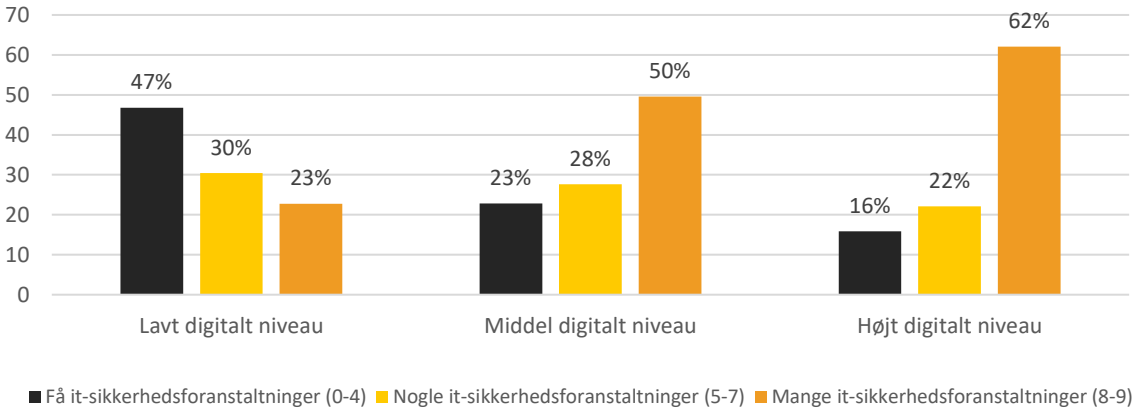
Ovenstående indikerer, at covid-19 har medført mere hjemmearbejde samt flere remote løsninger. Data tyder videre på, at disse remote løsninger hænger sammen med flere implementerede it-sikkerhedsforanstaltninger[6].

Dette betyder ikke, at der kan sluttes en entydig kausal sammenhæng mellem covid-19 og it-sikkerhedsforanstaltninger, men indikerer trods alt en sammenhæng[7]. Det er eksempelvis muligt, at virksomheder med flere it-sikkerhedsforanstaltninger, også er mere rolige ved at benytte sig af digitale løsninger, eller at virksomheder med flere it-sikkerhedsforanstaltninger i højere grad har de tekniske færdigheder til at bruge flere digitale løsninger. Som nævnt udgør digitale løsninger en risiko, så uanset årsagen er det positivt, at de digitale løsninger SMV'erne har benyttet under covid-19, ser ud til at følges med et øje på it-sikkerheden.

2.5 SMV'er med en højere digitaliseringsgrad bruger også flere it-sikkerhedsforanstaltninger

Som det ses i figur 10 nedenfor, genfinder man samme tendens, hvis man undersøger forholdet mellem it-sikkerhedsforanstaltninger og digitalisering generelt; et højere digitalt niveau korrelerer med flere it-sikkerhedsforanstaltninger[8].

Figur 10: Digitaliseringsgrad og it-sikkerhedsforanstaltninger



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2021). Note: Digitaliseringsniveau er målt som et indeks baseret på 5 indikatorer: 1) ERP-system, 2) CRM-system, 3) brug af min. én avanceret teknologi (IoT, KI/ML, Industrirobotter, Servicerobotter) 4) e-salg og 5) e-eksport. For hver indikator gives 1 point. Lavt niveau: 0-1 point. Middel niveau: 2- 3 point. Højt niveau: 4-5 point.

[6] It-sikkerhedsforanstaltningerne lagring af log-filer, tests af it-sikkerhed og risikoanalyse korrelerer særligt stærkt med hinanden.

[7] Sammenhængen mellem hjemarbejde og it-sikkerhedsforanstaltninger er signifikant efter kontrol for størrelse og branche.

[8] Sammenhængen er fortsat positiv og signifikant, hvis der kontrolleres for størrelse og branche.

Således har 47 pct. af SMV'erne med et lavt digitalt niveau også få it-sikkerhedsforanstaltninger, mens andelen blot er 16 pct. for SMV'erne med et højt digitalt niveau. Videre har 23 pct. af SMV'erne med et lavt digitalt niveau mange it-sikkerhedsforanstaltninger, mens det til sammenligning er 62 pct. af SMV'erne med et højt digitalt niveau.

Data viser derfor at SMV'ernes brug af digitale løsninger, gerne følges med flere it-sikkerhedsforanstaltninger, både hvad angår løsninger brugt ifm. covid-19, men også på et mere generelt plan.

Næste kapitel vil undersøge, SMV'ernes it-sikkerhedsniveau i forhold til deres risikoprofil.

3. SMV'ernes it-sikkerhedsniveau i forhold til deres risikoprofil.

3.1 44 pct. af virksomhederne har et for lavt sikkerhedsniveau i forhold til deres 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, sektor 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.

Resultaterne i tabel 1 viser, at 44 pct. af SMV'erne er sårbare, og at de dermed har et for lavt sikkerhedsniveau i forhold til deres risikoprofil.

Tabel 1: Match mellem SMV'ernes digitale sikkerhedsniveau og risikoprofil

		It-sikkerhedsniveau		
		Lav	Middel	Høj
Risikoprofil	Høj	De sårbare 44 pct.		
	Middel		De tilpas sikrede 48 pct.	
	Lav			De påpasselige 8 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 2021).

48 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 angiver, og tæller altså 8 pct.

PwC har for Erhvervsstyrelsen udviklet metoden til at estimere forholdet mellem virksomhedernes it-sikkerhedsniveau og deres risikoprofil. Grundet ændringer i spørgsmålsformuleringer siden Erhvervsstyrelsens rapport, "Digital Sikkerhed i Danske SMV'er" fra sidste år, kan tallene ikke sammenlignes 1

til 1 på tværs af de to rapporter. Det skyldes, bl.a. at ændringer i spørgsmålsformuleringer kan give støj i tallene, selvom den overordnede metode er den samme[9].

I sidste års rapport havde 40 pct. af SMV'erne et utilstrækkeligt sikkerhedsniveau ift. deres risikoprofil, men grundet ovenstående kan man pba. årets tal ikke konkludere, at andelen af sårbare virksomheder er steget med 4 procentpoint.

Der er en længere beskrivelse af PwC's metode, hvormed forholdet mellem virksomhedernes sikkerhedsniveau og risikoprofil er kalkuleret, i slutningen af denne rapport.

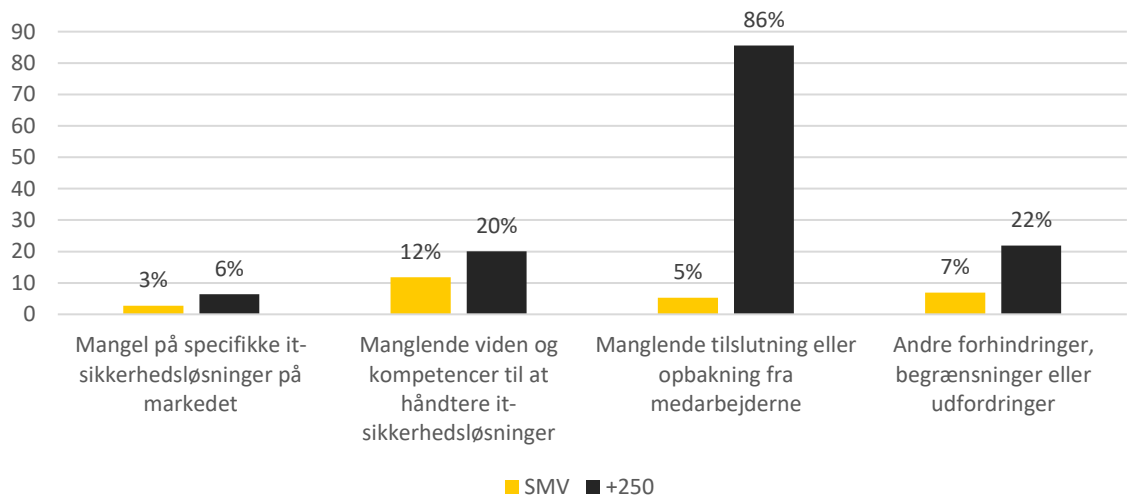
3.2 Mangel på viden og kompetencer er SMV'ernes største udfordring ved at øge it-sikkerheden

Afsnittet ovenfor viser, at forholdsvis mange SMV'er har et for lavt it-sikkerhedsniveau i forhold til deres risikoprofil. Videre viste afsnit 1, at mange SMV'er ikke har implementeret de to basale it-sikkerhedsforanstaltninger. I dette afsnit undersøges virksomhedernes udfordringer med at øge it-sikkerheden.

Samlet set svarer 17 pct. af SMV'erne, at de i 2020 har oplevet udfordringer og/eller begrænsninger med at øge it-sikkerheden. Sidste år var tallet 28 pct., men ændringer i spørgsmålsformuleringen gør, at tallene ikke kan sammenlignes 1 til 1[10]. For virksomhederne med over 250 medarbejdere svarer 37 pct., at de har oplevet udfordringer og/eller begrænsninger med at øge it-sikkerheden.

Figur 11 indikerer, at den største begrænsning for SMV'erne er manglende viden og kompetencer til at håndtere it-sikkerhedsløsninger. For virksomheder med over 250 ansatte er den suverænt mest udbredte udfordring manglende tilslutning eller opbakning fra medarbejdere.

Figur 11: Oplevede udfordringer med at øge it-sikkerheden



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2021).

[9] For uddybning se metodeafsnittet.

[10] I VITA 2020 blev virksomhederne spurgt ind til udfordringer ved at anvende it-sikkerheds*løsninger*, mens der i år spørges ind til udfordringer ved at hæve it-sikkerheds*niveauet*. Videre er svarkategorierne anderledes, eksempelvis var det sidste år ikke muligt at svare, at manglende tilslutning fra medarbejderne var en udfordring.

Således svarede 12 pct. af de danske SMV'er ja til, at de oplevede, at manglende viden og kompetencer, begrænsede dem i at øge deres it-sikkerhedsniveau. Mens hele 86 pct. af virksomhederne med over 250 ansatte har oplevet manglende tilslutning eller opbakning fra medarbejderne.

Ganske mange af virksomhederne med 250+ ansatte, angiver dog også mangel på viden og kompetencer som en barriere for øget it-sikkerhed (20 pct.). Det kan skyldes, at store virksomheder typisk er mere digitaliserede, hvorfor deres it-sikkerhedsudfordringer kan være mere komplekse.

Fælles for SMV'erne og de store virksomheder er, at mangel på specifikke it-sikkerhedsløsninger er den mindst udbredte udfordring. Hhv. 3 pct. af SMV'erne og 6 pct. af de store virksomheder svarede, at de havde oplevet denne udfordring i 2020.

For virksomheder, der efterspørger konkrete råd, værktøjer og et overblik over gratis tilbud, er der hjælp at hente på Sikkerdigital.dk/virksomhed.

Syv gode råd	**Test og værktøjer**	**Overblik over gratis tilbud**
På Sikkerdigital.dk har Erhvervsstyrelsen udarbejdet syv basale råd om at it-sikkerhed, som er et godt sted at starte for virksomheder, der ønsker at styrke sikkerheden. Syv råd om it-sikkerhed (sikkerdigital.dk)	På sikkerdigital.dk findes en række gratis onlineværktøjer, som kan styrke it-sikkerheden og persondatahåndtering. Eksempelvis IT-risikovurderingsværktøjet og sikkerhedstjekket. Test og værktøjer (sikkerdigital.dk)	Erhvervsstyrelsen har samlet et overblik over en række gratis tilbud fra aktører, som kan styrke virksomhedens digitale sikkerhed (fx online test, kurser, e-læring og apps) Gratis tilbud fra andre aktører (sikkerdigital.dk)

3.3 Ledelsens involvering i it-sikkerhed

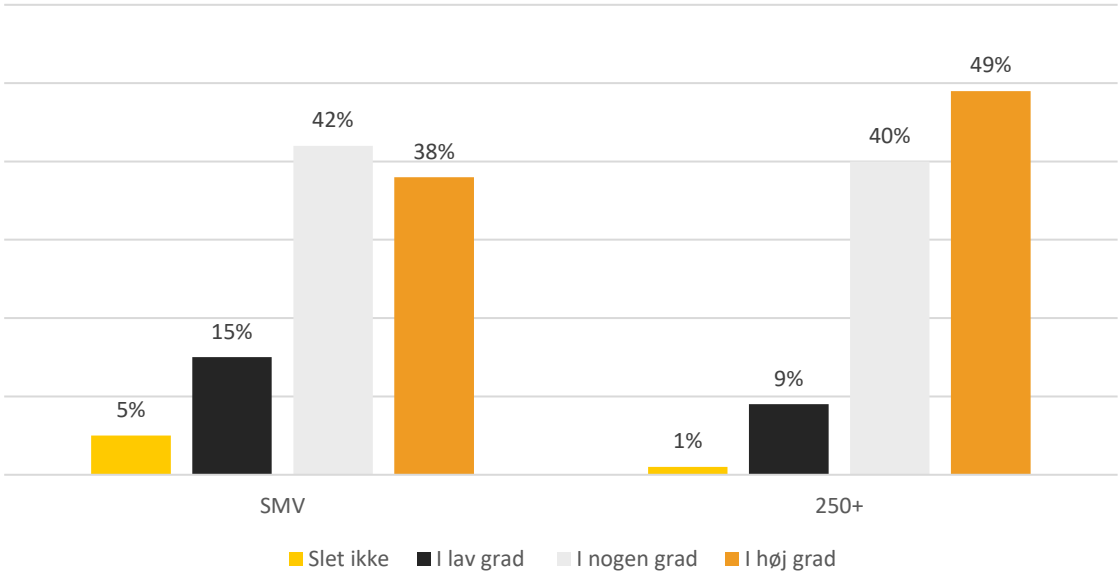
I forlængelse af virksomhedernes udfordringer med at øge it-sikkerhedsniveauet, er det værd at undersøge ledelsens involvering. En manglende stillingtagen til digital sikkerhed i ledelsen kan fungere som en barriere for at implementere digitale sikkerhedstiltag[11].

Figur 13 viser, i hvor høj grad ledelsen og bestyrelsen i virksomhederne tager stilling til virksomhedens it-sikkerhedsmæssige aktiviteter.

Her er der en lille tendens til, at ledelsen og bestyrelsen i de større virksomheder i højere grad tager stilling til sikkerhedsmæssige aktiviteter.

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

Figur 12: I hvilket omfang tager virksomhedens topledelse og/eller bestyrelse stilling til virksomhedens it-sikkerhedsmæssige aktiviteter?



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2021).

49 pct. af virksomhederne med 250+ ansatte svarede, at topledelsen og/eller bestyrelsen i høj grad tog stilling til virksomhedens it-sikkerhedsmæssige aktiviteter. Til sammenligning var dette tal for SMV'erne 38 pct. Forskellen mellem SMV'erne og de store virksomheder er generelt betragtet ikke særligt stor, når det gælder ledelsens involvering.

3.4 It-specialister hænger sammen med flere it-sikkerhedsforanstaltninger

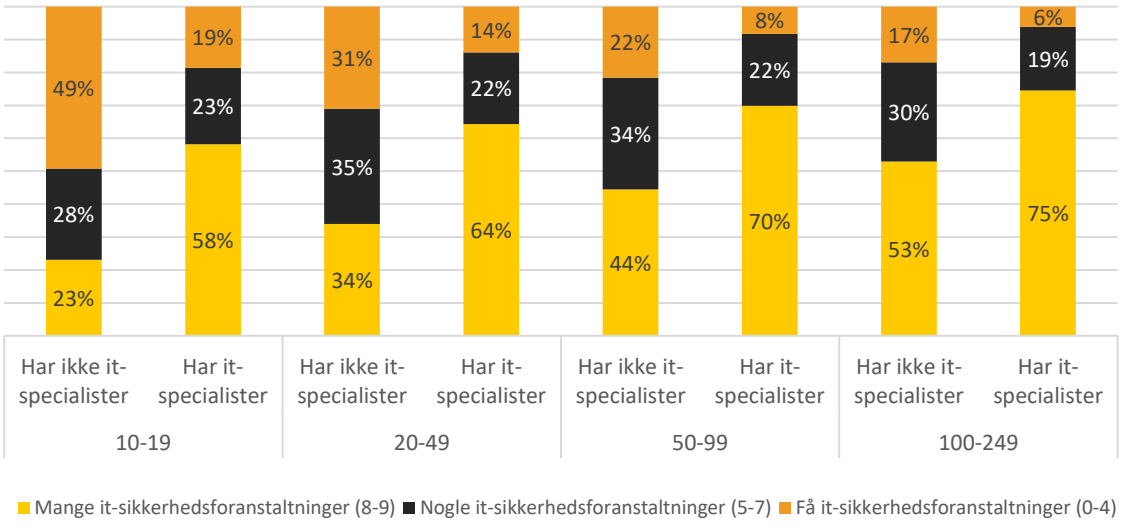
Mangel på it-kompetencer i virksomheden er en af virksomhedernes hovedudfordringer. Den mest oplagte måde at øge virksomhedens it-kompetencer, er ved at ansætte it-specialister, eller ved at videreuddanne medarbejderne.

Helt overordnet beskæftiger større virksomheder i højere grad it-specialister end små virksomheder. I kategorien 10-19 ansatte er det således kun 18 pct., der beskæftiger it-specialister. Til sammenligning er det for 250+ virksomheder hele 90 pct.. Samlet set er det 28 pct. af SMV'erne som beskæftiger it-specialister.

Figur 13 nedenfor viser forholdet mellem it-sikkerhedsforanstaltninger, og hvorvidt virksomheden har it-specialister ansat. Søjlerne er ydermere inddelt på virksomhedsstørrelse.

En tendens på tværs af virksomhedsstørrelse er, at en større andel af SMV'erne med it-specialister ansat har implementeret mange it-sikkerhedsforanstaltninger (8-9).

Figur 13: It-specialister og it-sikkerhedsforanstaltninger

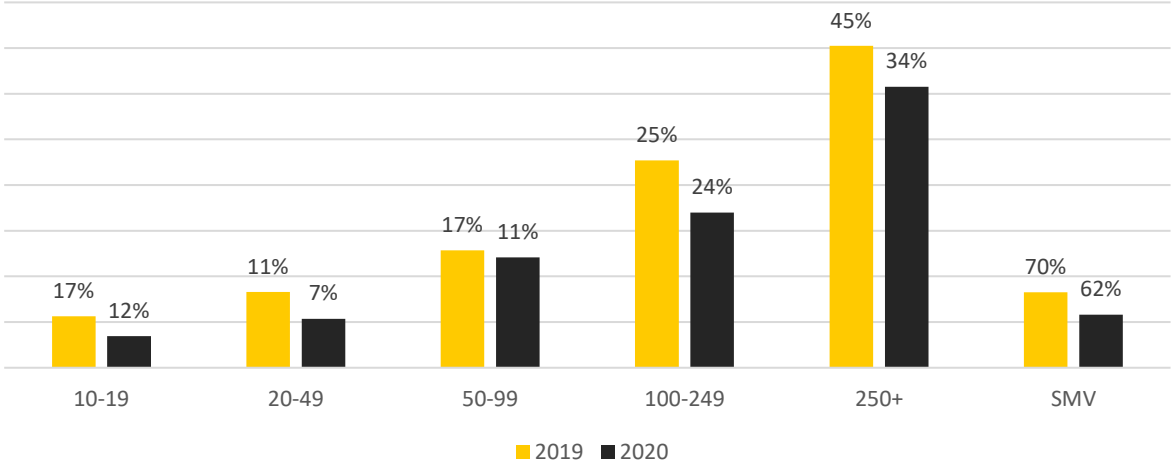


For SMV'erne med 10-19 ansatte, har 23 pct. af dem uden it-specialister ansat, implementeret mange it-sikkerhedsforanstaltninger, mens tallet for virksomhederne med it-specialister ansat er 58 pct.. På tværs af virksomhedsstørrelse er der en gennemsnitlig forøgelse i andelen med mange it-sikkerheds-foranstaltninger på 28 procentpoint, når virksomheden har en it-specialist ansat.

Der er altså en samvariation mellem it-kompetencer i virksomheden og it-sikkerhedsforanstaltninger. Af denne grund, er det også interessant at undersøge, om virksomhederne prioriterer at opkvalificere medarbejdernes it-kompetencer.

Figur 14 viser, om virksomheden har tilbudt opkvalificering af it-specialisters it-færdigheder i 2019 og 2020.

Figur 14: Har virksomheden tilbudt opkvalificering af it-specialister i it-færdigheder?

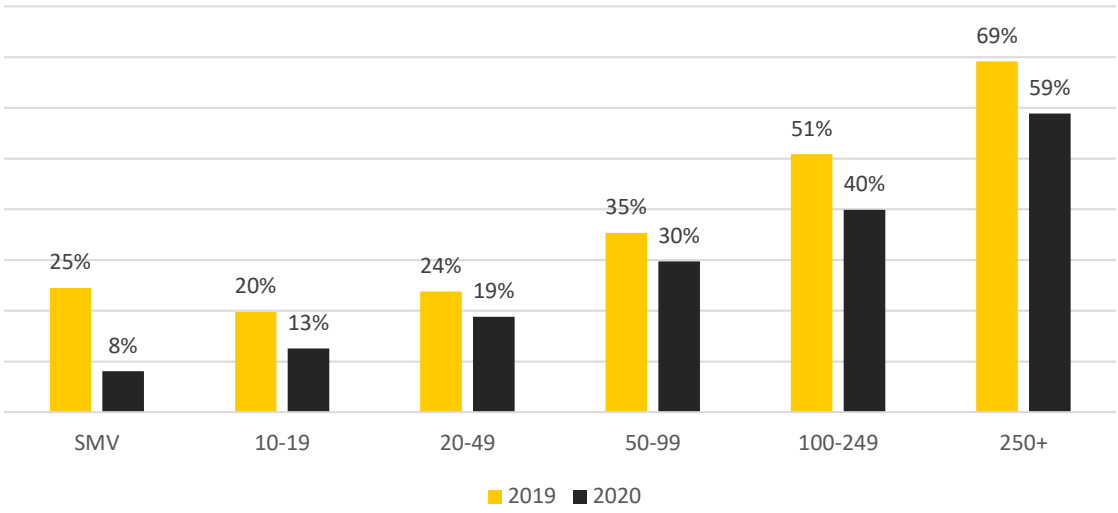


Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2020 og 2021).

For alle kategorier af virksomhedsstørrelse har der været et fald i oplæring fra 2019 til 2020. Årsagen kan være, at det har været praktisk svært for virksomhederne at afholde oplæringsforløb under covid-19. En anden årsag kan være, at mange virksomheder har måttet prioritere ressourcer over på andre problemstillinger, som eksempelvis håndtering af covid-19 retningslinjer, løse leveranceudfordringer el. lign.

Figur 15 viser andelen af virksomheder, der har tilbudt oplæring i it-færdigheder til ansatte, der *ikke* er it-specialister for 2019 og 2020. Her er tendensen den samme, hvor mængden af virksomheder med oplæring af ansatte stiger med virksomhedsstørrelse.

Figur 15: Har virksomheden tilbudt opkvalificering af øvrige ansatte i it-færdigheder



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2020 og 2021).

Generelt var der blandt SMV'erne i 2020 8 pct., der tilbød oplæring i it-færdigheder. Til sammenligning var det samme tal for 250+ 69 pct., hvilket er en forskel på 61 procentpoint. Andelen af virksomheder, der tilbød oplæring i it-færdigheder faldt også markant fra 2019 til 2020.

Igen er en mulig forklaring, at fokus under corona har ligget andetsteds, eller at den øgede mængde af hjemmearbejde har gjort det svært at lave oplæringsforløb til medarbejderne.

Generelt betragtet tyder resultaterne ovenfor på, at større virksomheder både ansætter og udvikler it-sikkerhedskompetencer i højere grad end de mindre virksomheder, og at der i 2020 har været tilbudt mindre opkvalificering end i 2019.

4. It-sikkerhedshændelser i danske SMV'er

I det følgende afsnit præsenteres data om it-sikkerhedshændelser i danske virksomheder. Der skal i den forbindelse tages nogle forbehold.

For det første er ikke alle it-sikkerhedshændelser, nogle man som virksomhed nødvendigvis erkender som værende en it-sikkerhedshændelse. Eksempelvis kan ens servere være en del af at botnet, uden at man som virksomhed er opmærksom på det.

Videre kan frygt for at stille ens virksomhed i et dårligt lys betyde, at man som respondent lader være med at angive, at man har været udsat for en it-sikkerhedshændelse.

Modsat er spørgsmålet formuleret således, at software- og hardware fejl tælles med, da årsagen bag disse i nogle tilfælde kan være en it-sikkerhedshændelse. Det vil dog ikke altid være tilfældet, sommetider er der blot tale om en fejl, dette vil alt andet lige trække tallet mod et overestimat.

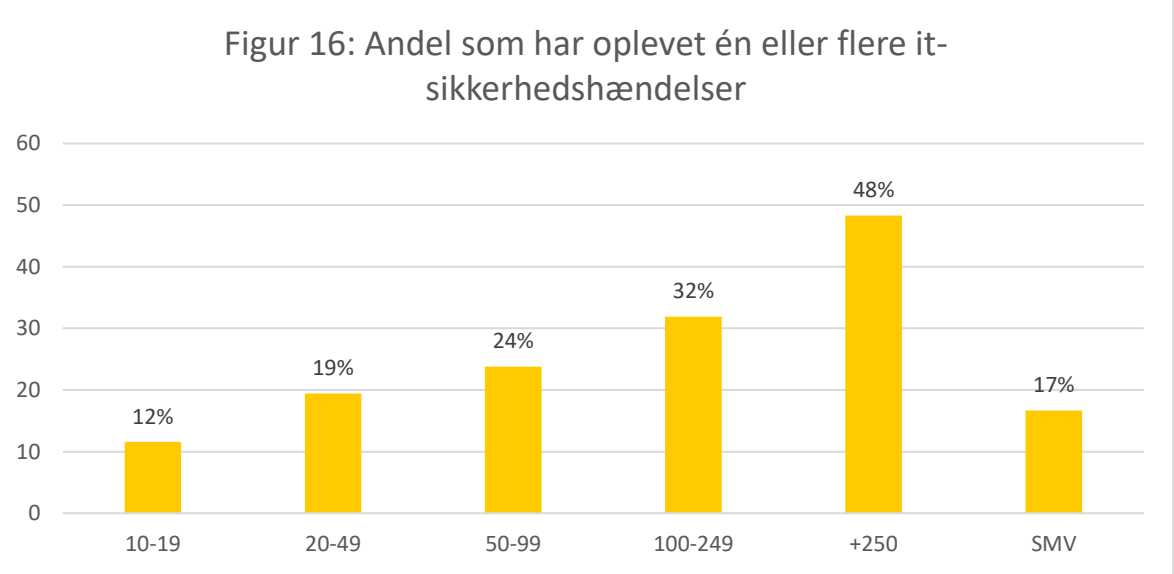
Der skal derfor tages forbehold for disse opmærksomhedspunkter i fortolkningen af tallene.

4.1 En større andel af store virksomheder har oplevet en it-sikkerhedshændelse

I årets VITA-undersøgelse dækker it-sikkerhedshændelser over følgende:

1. Blokeret adgang til it-services	2. Sletning eller ødelæggelse af data	3. It-relateret økonomisk svindel	4. Andre it-sikkerhedshændelser
Distributed denial of service-angreb (DDoS). Ransomware-angreb. Hardware- eller softwarefejl.	Eksempelvis grundet ondsindet software, hardware eller softwarefejl.	Situationer hvor virksomheden franarres penge.	Denne kategori er med for at sikre, at kategorierne samlet set er udtømmende.

Figur 16 nedenfor viser andelen, som har oplevet én eller flere it-sikkerhedshændelser. Tendensen er, at jo større virksomheder, jo større en andel har oplevet en it-sikkerhedshændelse.

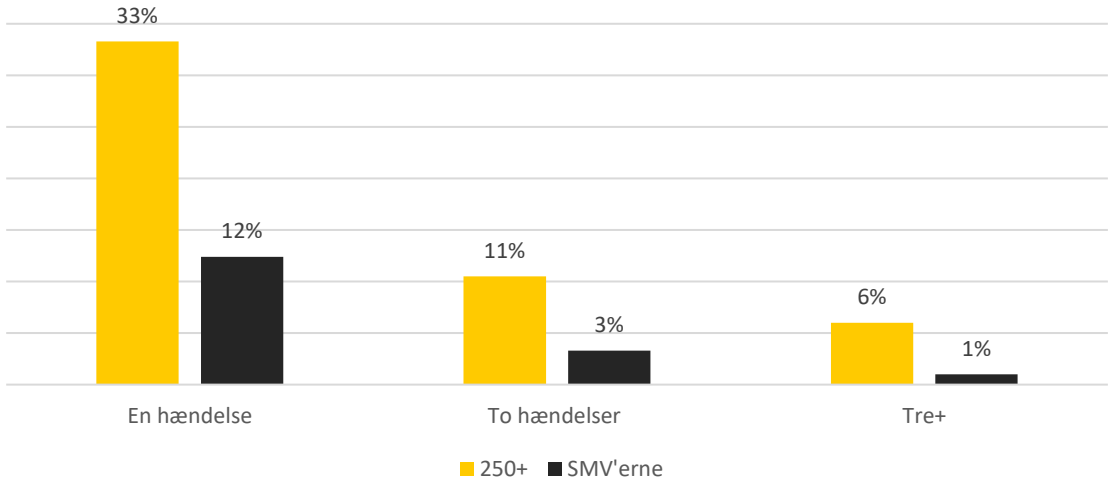


Samlet set har 17 pct. af SMV'erne oplevet én eller flere af de ovenstående it-sikkerhedshændelser. Til sammenligning svarer 48 pct. af virksomhederne med over 250 ansatte, at de har oplevet én eller flere it-sikkerhedshændelser.

Figur 17 nedenfor viser, hvor mange af de fire typer sikkerhedshændelser de adspurgte virksomheder i 2020 har oplevet fordelt på segmenterne SMV'er og 250+.

Overordnet er tendensen, at de store virksomheder oplever flere forskellige typer it-sikkerhedshændelser end SMV'erne.

Figur 17: Antal it-sikkerhedshændelser i SMV'erne og 250+



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2021).

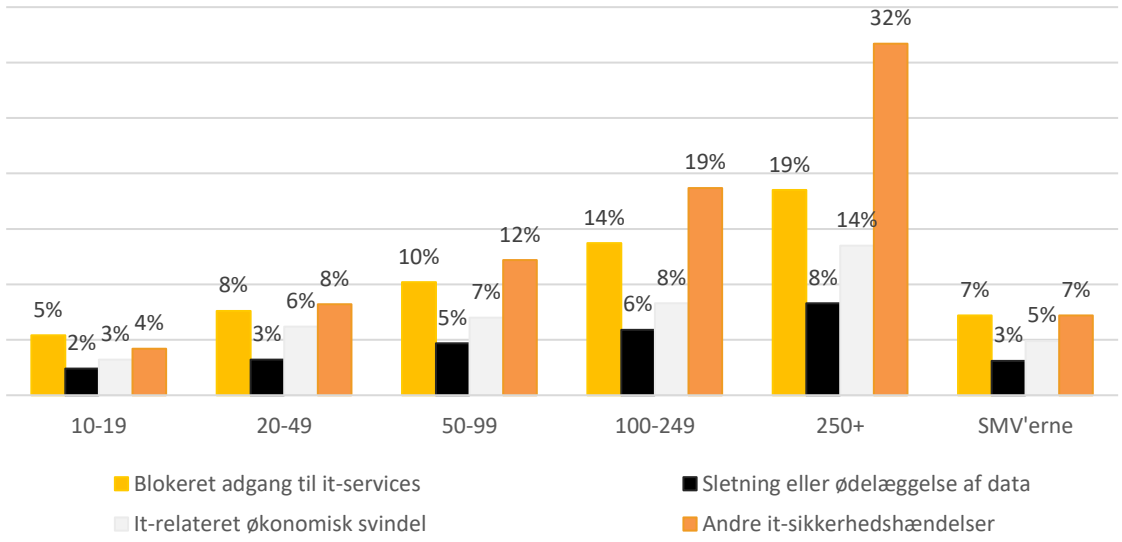
Cirka 12 pct. af de danske SMV'er har oplevet minimum én sikkerhedshændelse. Her er det primært de større virksomheder i SMV-segmentet, der trækker tallet op. I virksomheder med 100-249 ansatte er det f.eks. 22 pct., der har oplevet minimum én sikkerhedshændelse.

Det skal understreges at virksomheder som har oplevet den samme type it-sikkerhedshændelse flere gange, kun vil tælle med som én i figuren, da figuren viser andelen som har oplevet en, to eller tre+ *typer* hændelser.

4.2 "Blokeret adgang til it-services" og "andre it-sikkerhedshændelser" er de mest udbredte it-sikkerhedshændelser

Figur 18 viser andelen, der har oplevet hver af de fire typer sikkerhedshændelser i 2020.

Figur 18: Typer af sikkerhedshændelser fordelt på størrelse



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2021).

De mest udbredte it-sikkerhedshændelser er "Blokeret adgang til it-services" og "Andre it-sikkerhedshændelser". Herudover ses det at andelen af virksomheder, som har oplevet en hændelse, stiger med virksomhedsstørrelse. Denne tendens er tilfældet med alle kategorier af it-sikkerhedshændelser, dog er tendensen stærkest for "andre it-sikkerhedshændelser", hvor blot 4 pct. af virksomhederne med 10-19 ansatte har oplevet en sådan, mens tilfældet er 32 pct. for virksomheder med over 250 ansatte.

Der kan være flere årsager til, at store virksomheder i højere grad oplever it-sikkerhedshændelser. F.eks. kan større virksomheder være mere udsatte for cyberkriminalitet, da kendskabet til virksomhederne er større. Det kan også skyldes, at større virksomheder har flere angrebsflader end små virksomheder eksempelvis i kraft af sine mange ansatte, men også som følge af en højere digitaliseringsgrad og brug af eksempelvis IoT-produkter.

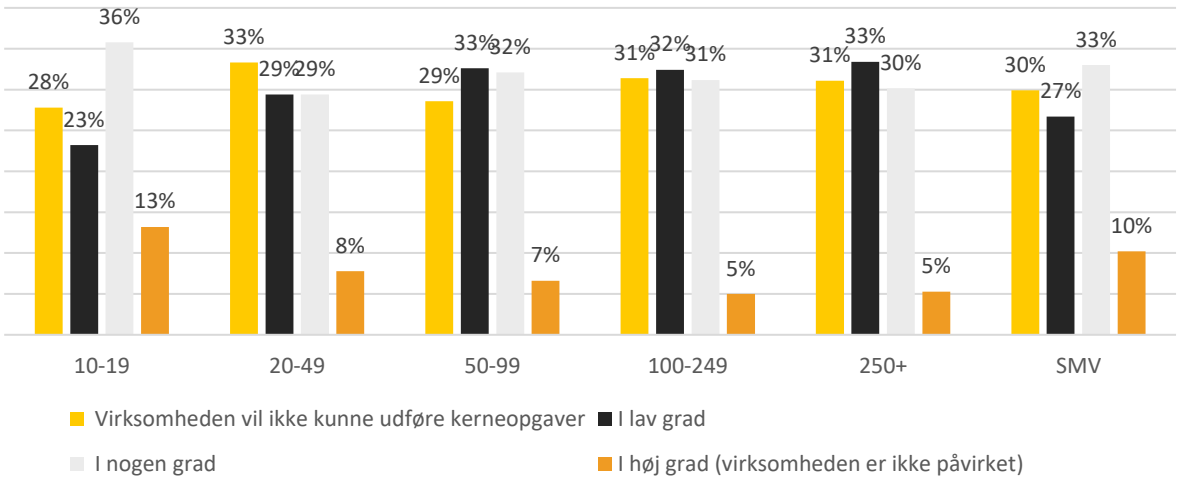
Som nævnt ovenfor, kan der også være en variation i, hvor gode virksomhederne er til at opdage it-sikkerhedshændelser. Dette er særligt relevant, når der er tale om hændelser, som ikke direkte påvirker virksomhedens daglige gang. Da sådanne hændelser ville falde i kategorien "andre it-sikkerhedshændelser", kan dette være en del af forklaringen på, at "andre it-sikkerhedshændelser" optræder så markant oftere i de store virksomheder.

4.3 30 pct. af de danske SMV'er ville ikke kunne udføre deres kerneopgaver, hvis de mistede adgang til centrale it-systemer

Figur 19 viser, i hvor høj grad virksomhederne vil kunne udføre deres kerneopgaver, hvis de mister adgang til centrale interne it-systemer.

Skalaen går fra 1-4, hvor 1 er ensbetydende med, at virksomheden ikke ville kunne udføre dens kerneopgaver. Omvendt vil en score på 4 betyde, at virksomheden i høj grad vil kunne udføre dens kerneopgaver, og dermed ikke ville være påvirket.

Figur 19: I hvilken grad vil virksomheden være i stand til at udføre dens kerneopgaver, hvis virksomheden mister adgangen til centrale interne it-systemer?



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2021).

30 pct. af de danske SMV'er vil ikke kunne udføre deres kerneopgaver, hvis de mister adgangen til centrale interne it-systemer.

Cirka 10 pct. af SMV'erne vil ikke være påvirket og vil dermed fortsat kunne udføre deres kerneopgaver. Til sammenligning er det kun ca. 5 pct. af 250+ virksomhederne, der vil være upåvirkede.

På tværs af størrelse bliver virksomhederne i store træk påvirket i sammenlignelig grad, hvis de mister adgangen til deres centrale interne it-systemer. Virksomheder med 10-19 ansatte vil dog blive påvirket i en smule mindre grad end de større.

Dette hænger formentlig sammen med, at større virksomheder tenderer mod at være mere digitaliserede, og at flere af virksomhedens kerneprocesser derfor er digitaliserede.

Resultaterne i dette afsnit viser, at mange virksomheder, vil have store udfordringer med at udføre deres kerneopgaver, såfremt de mister adgang til deres centrale it-systemer.

Det viser, at it-systemer ofte er et vigtigt element i udførslen af kerneopgaver, hvorfor beskyttelse af disse systemer blot er af mere central karakter.

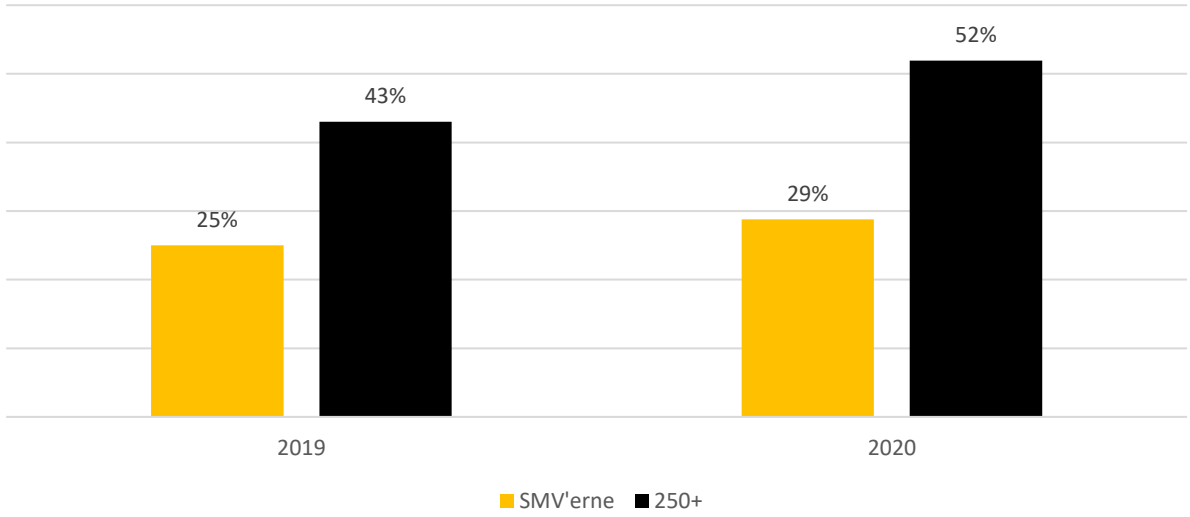
5. Dateetik

Virksomhedernes arbejde og brug af data har i dag stor betydning for kunderne og deres tillid til virksomhederne. Virksomhederne skal dels behandle kundernes oplysninger og andet data ansvarligt, og skal derudover sikre disse bedst muligt mod cyberangreb. Ansvarlig brug af data omhandler også fokus på dataetik, herunder ikke at dele data uden samtykke og kun at indsamle nødvendige data.

Dataetik handler om ansvarlig og bæredygtig brug af data i virksomhedernes datahåndtering, hvor man arbejder for at sikre, at dataanvendelse ikke sker på et uetisk grundlag eller leder til uønskede samfundsmæssige konsekvenser. Dataetik er bl.a. vigtigt i forhold til at bevare og højne tilliden blandt virksomhedernes kunder. Dataetik er ikke bare et spørgsmål om at overholde lovgivning, men om at behandle andres data med respekt og gøre det rigtige, selv når ingen kigger.

Figur 20 viser, hvor stor en andel af SMV'erne og virksomheder med 250+, der arbejder aktivt med dataetik i 2019 og 2020. Der er fremgang for begge segmenter, hvor specielt andelen i 250+ segmentet er steget.

Figur 20: Arbejder virksomheden aktivt med dataetik?



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2021).

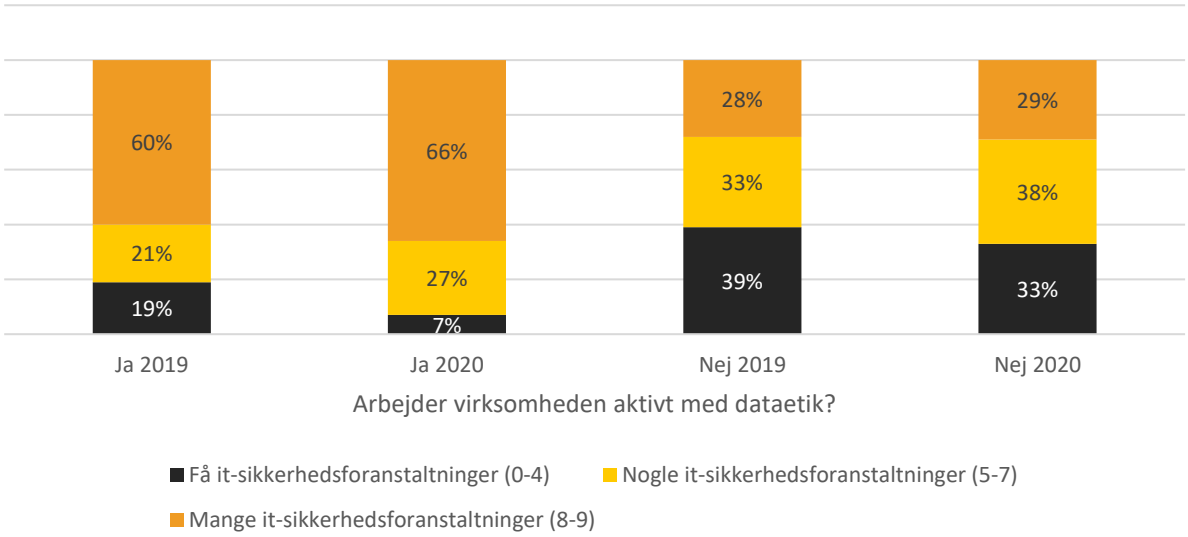
Blandt SMV'erne arbejder cirka en tredjedel af virksomhederne aktivt med dataetik, hvor det til sammenligning er cirka halvdelen af 250+ virksomhederne. Dette indikerer, at dataetik ligesom f.eks. mængden af it-sikkerhedsforanstaltninger og beskæftigelse af it-specialister, har en positiv sammenhæng med virksomhedsstørrelse.

Figur 21 viser virksomhedernes arbejde med dataetik kombineret med antallet af sikkerhedsforanstaltninger for 2019 og 2020.

Her er det tydeligt at se, at de virksomheder der arbejder aktivt med dataetik, også har implementeret væsentligt flere af de 9 anbefalede it-sikkerhedsforanstaltninger.

For 2020 er det fx hele 66 pct. af de virksomheder, der arbejder aktivt med dataetik, som har implementeret 8-9 it-sikkerhedsforanstaltninger. Til sammenligning er det for de virksomheder, der ikke arbejder aktivt med dataetik kun 29 pct., der har indført 8-9 it-sikkerhedsforanstaltninger.

Figur 21: SMV'ernes arbejde med dataetik og digital sikkerhed, 2019 og 2020



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2021).

Det tyder dermed på, at fokus på digital sikkerhed er positivt korreleret med fokus på dataetik og vice versa. Erhvervsstyrelsen arbejder aktivt for at understøtte de danske SMV'ers arbejde med dataetik. Dette har blandt andet resulteret i en række værktøjer, som fremgår herunder.

Beskyttelse af data	Start en dataetisk samtale	Find inspiration
Brugdata.dk tilbyder en nem ad-gang til at finde information om reglerne foranvendelse af data. På siden kan man få svar på konkrete spørgsmål om bl.a. sikring af data, databaser og online platforme. Få svar på spørgsmål om beskyttelse af data	Med Dataetisk Dilemmaspil kan du få startet den dataetiske samtale i virksomheden. Igennem spillet bliver du og dine kollegaer konfronteret med dilemmaer og spørgsmål, der kan hjælpe jer på vej i forhold til, hvordan netop din virksomhed gerne vil arbejde med dataetik. Spil Dataetisk Dilemmaspil her	På Virksomhedsguidens temaside om dataetik kan du finde konkrete værktøjer til jeres arbejde med dataetik. Du kan også læse andre virksomheders erfaringer med at implementere dataetik i deres arbejde. Find inspiration og værktøjer på Virksomhedsguidens tema

Metode

It-sikkerhedsniveau / Risikoprofil

Det følgende er en beskrivelse af PwC's metode, for en "Indeksering af danske SMV'ers digitale sikkerhedsniveau og risikoprofil samt matchet mellem disse" fra d. 16. august 2021. Metoden står også beskrevet i "Digital Sikkerhed i danske SMV'er" (2021), men genbeskrives, her grundet ændringer i nogle indikatorer, som følge af forskelle i spørgsmålsformuleringer mellem "it-anvendelse i virksomheder" (2021) og data indsamlet af Epinion for Erhvervsstyrelsen i 2020.

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 indekseringen af de it-sikkerhedsniveau og risikoprofil.

Den opsummerede effekt af disse forskelle på sammenligneligheden mellem tallet for denne rapport, 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.

Sidste års it-sikkerhedsniveau/risikoprofil-tal er målt med en bestemt metode udviklet af PwC. Denne bygger på et overordnet framework, som er beskrevet nøjere 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, mens flere af spørgsmålene, også kaldet indikatorerne, varierer mellem de to år.

Variationer i spørgsmålsformuleringer kan påvirke respondenters svar, ligeledes kan variationer i spørgeskemaet som helhed.

Videre har variationer i stikprøven også en betydning. Rekrutteringen af respondenterne i stikprøverne er ganske forskellige, mens spørgeskemaet bag årets tal fra Danmarks Statistik, har været obligatorisk for virksomhederne at besvare, var spørgeskemaet bag sidste års tal frivilligt at besvare. Dette kan betyde at respondenterne i sidste års datasæt, har været systematisk mere interesserede i it-sikkerhed, end respondenternes i årets datasæt. På den ene side, kan det betyde at respondenterne repræsenterer virksomheder, med større interesser for it-sikkerhed, hvilket betyder en øget risiko for at overestimere virksomhedernes sikkerhedsniveau. Modsat kan større it-kundskaber blandt respondenterne betyde, at de har en større viden om virksomhedernes it-sikkerhedsniveau, hvilket ville betyde relativt mere præcise svar.

Den præcise effekt af disse variationer er, imidlertid svær at vurdere. Den simple konklusion som følge af disse variationer er derfor, at tallet fra sidste år ikke kan sammenlignes med tallet fra i år.

Årets tal er desuden kendetegnet ved, samlet set at bestå af færre indikatorer end sidste års tal. Som nævnt er det de samme fænomener som måles, men de måles med færre datapunkter, hvorfor evnen til at indfange fænomenerne er mindre finmasket og resultatet mindre nuanceret. Der skal derfor tages forbehold herfor.

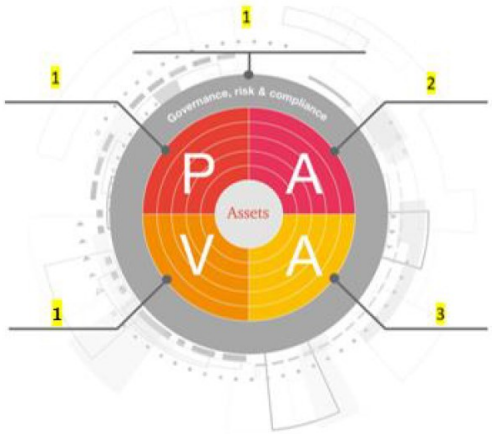
Metode og fremgangsmåde

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 anvender PwC niveauerne "lav", "middel" og "høj" til at inddele SMV'erne i tre typer. Hvis fx både sikkerhedsniveau og risikoprofil er middel, vurderer PwC, at en SMV's basale it-sikkerhedsniveau er tilpas.

I de følgende afsnit gives en detaljeret redegørelse for PwC's 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, hvilket er vist i figur 1. 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 udover en vægtning 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	**Spørgsmål:** I hvilket omfang tager virksomhedens topledelse og/eller bestyrelse stilling til virksomhedens it-sikkerhedsmæssige aktiviteter	0-5	1
2	**Spørgsmål:** 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	**Spørgsmål:** Har virksomheden i 2020 tilbudt opkvalificering af it-færdigheder til følgende: a) it-specialister, b) øvrige ansatte	0-5	1
	Processer		
4	Hvem udførte virksomhedens it-funktioner i 2020	0-5	1
5	Bruger virksomheden følgende it-sikkerhedsmæssige foranstaltninger: risikoanalyse?	0-5	1
	Validering		
7	Har virksomheden haft følgende it-sikkerhedshændelser i 2020? a) blokeret adgang til it-services, b) sletning, ødelæggelse, misbrug eller videregivelse af data (forsætligt eller utilsigtet), c) it-relateret økonomisk svindel (hvor virksomheden franarres penge) d) andre it-sikkerhedshændelser.	1-4	1
	Arkitektur		
8	**Spørgsmål:** 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

Der er en række forskelle på spørgsmålene brugt i sikkerhedsniveau-indekset fra rapporten i 2021, og indekset brugt i årets rapport.

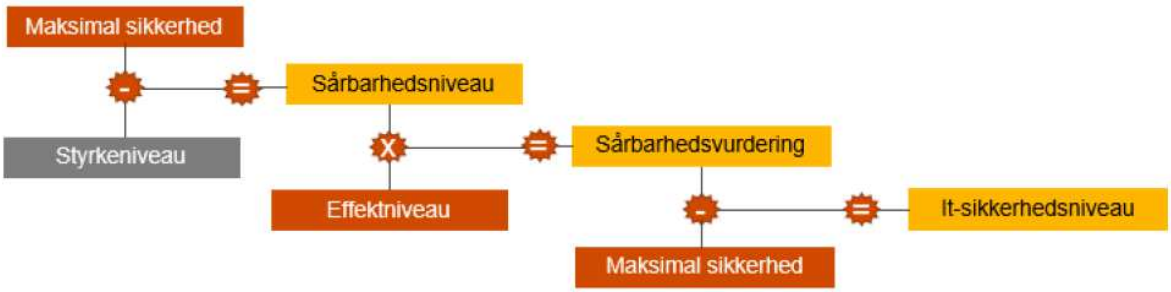
Eksempelvis er spørgsmål 1 i rapporten fra 2021 delt i to separate spørgsmål, hvor der først spørges til ejerens/den øverste ledelses og dernæst til bestyrelsens involvering i it-sikkerhedsspørgsmål. I årets rapport er disse to slået sammen til et enkelt spørgsmål. Dette betyder et mindre finmasket estimat af ledelsens og bestyrelsens involvering, men indfanger derudover det samme. Effekten af dette er, at resultaterne er mindre nuancerede. På den måde kan data fremstille virksomhederne mere karikerede, hvorfor man skal tage forbehold herfor.

Ligeledes er spørgsmålene brugt i årets rapport flere steder simplere end sidste år, eksempelvis havde spørgsmål 5 fire underspørgsmål, hvori en risikovurdering er blandt, men også eksempelvis om virksomheden har en it-sikkerhedspolitik. Det betyder at nogle virksomheder potentielt vil vurderes til at have et lavt it-sikkerhedsniveau i år, som ville have været vurderet højere sidste år, og modsat at nogle virksomheder vurderes til at have et højt it-sikkerhedsniveau i år, som ville have været vurderet lavere med sidste års indikatorer. Ligeledes vil der, lig med spørgsmål 1, mangle nuancer i data, som konsekvens af, at det bagvedliggende fænomen data skal indfange, indfanges med færre indikatorer end sidste år.

Da forskellene mellem sidste års og dette års indikatorer ikke systematisk trækker i én retning, vurderes effekten af disse forskelle at være lille. I denne vurdering lægges der, udover manglen på systematik i forskellene, særligt vægt på at alle overemnerne (governance, processer, validering, arkitektur) er repræsenteret i indikatorerne brugt i dette års indeks..

Model for beregning af it-sikkerhedsniveau

Scoringsværdien for SMV'ernes it-sikkerhedsniveau fastlægges ved at anvende PwC's formel 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.



Styrkeniveau

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.

Beregning af sårbarhedsvurdering

For at foretage en sårbarhedsvurdering tager man udgangspunkt i sårbarhedsniveau for hvert enkelt PAVA-område og ganger med det effektniveau, der dækket 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 og konsekvens. Risikoscoren inddeles i tre intervaller, som karakteriserer virksomheder med en henholdsvis lav, middel og 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. Sandsynlighedsscoren vurderes ikke i forhold til, hvilke sektorer en virksomhed leverer digitale produkter til, da det for hver enkelt SMV ville kræve en kvalitativ vurdering af typen af det digitale produkt i forhold til sektor og sandsynlighed.

#	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, industriro-botter, servicerobotter og/eller cloud-tjenester.	1 (få eller ingen an-vendte 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 er beskrevet 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?	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. Sidste års rapport havde også et spørgsmål om antallet af individer, som virksomheden opbevarer data på. Denne indgår ikke i indekset, hvilket betyder at risikovurderingen af virksomhedens data er mindre præcis. Hvorfor der skal tages forbehold herfor når man læser rapportens konklusioner.

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.

<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">Risikoprofil</td><td>Høj</td><td rowspan="2">De sårbare 44 pct.</td><td></td><td></td></tr>
<tr><td>Middel</td><td>De tilpas sikrede 48 pct.</td><td rowspan="2">De påpasselige 8 pct.</td></tr>
<tr><td>Lav</td><td></td><td></td></tr>
</table>

De sorte felter 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 overstiger konsekvensen af en it-sikkerhedshændelse og sandsynligheden for, at en sådan finder sted, det nuværende it-sikkerhedsniveau, og derfor kategoriseres de som "sårbare".

Omvendt angiver de gule felter de påpasselige SMV'er – dvs. dem med et it-sikkerhedsniveau, der overstiger deres risikoprofil. Disse virksomheder har implementeret flere/mere avancerede it-sikkerhedstiltag, end hvad der for 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.

Erhvervsstyrelsen

Langelinie Allé 17
2100 København Ø

T: 3529 1000
@: erst@erst.dk
W: erhvervsstyrelsen.dk