Digital sikkerhed i danske SMV'er

September 2021

Erhvervsstyrelsen

Analysens hovedresultater er:

SMV'ernes digitale sikkerhedsniveau kan styrkes

- 40 pct. af de danske SMV'er har et *utilstrækkeligt* digitalt sikkerhedsniveau i forhold til deres risikoprofil.
- 24 pct. af de danske SMV'er anvendte *ikke* de to helt basale it-sikkerhedsforanstaltninger i 2019: opdatering af styresystemer og backup af data. Det er samme niveau som i 2018.
- Selv blandt SMV'er, der arbejder med digitale teknologier (cloud, IoT og big data analyse), anvender 15 pct. ikke de to basale tiltag; opdatering af styresystemer og backup af data.

Udfordringer og løsninger ift. at styrke SMV'ernes digitale sikkerhed

- 28 pct. af SMV'erne har været forhindret i, begrænset af eller oplevet udfordringer for at anvende it-sikkerhedsløsninger i 2019. Den største andel af virksomhederne fremhæver 'usikkerheden om gevinsten ved at investere i digital sikkerhed' (19 pct.) som en udfordring/begrænsning. Herefter følger udfordringerne med 'manglende it-kendskab og kompetencer til at håndtere it-sikkerhedsløsninger' (14 pct.) og 'manglende økonomiske ressourcer' (13 pct.).
- 13 pct. af SMV'erne har rekrutteret eller forsøgt at rekruttere it-specialister i 2019. Heriblandt har hele 57 pct. haft vanskeligt herved. Behovet for at rekruttere it-specialister stiger med virksomhedsstørrelse – men blandt den andel af virksomheder, som har forsøgt at rekruttere it-specialister, opleves udfordringer med at rekruttere specialisterne i samme omfang uagtet virksomhedsstørrelse.
- Hele 79 pct. af SMV'erne er enige eller helt enige i, at 'enkle og konkrete råd om it-sikkerhed' kan øge deres fokus på digital sikkerhed. Men også 'løbende varsler om aktuelle trusler' (74 pct.) og 'konkrete værktøjer' (70 pct.) topper listen af tiltag, der kan øge SMV'ernes fokus på området.

Øvrige indsigter om SMV'ernes arbejde med digital sikkerhed

- **IT-sikkerhedshændelser:** 10 pct. af SMV'erne og 32 pct. af de store virksomheder med 250+ ansatte har oplevet en it-sikkerhedshændelse i 2019. Ved sikkerhedshændelser frygter SMV'erne især de direkte, kortsigtede konsekvenser som at miste værdifulde data (69 pct.), at få lammet deres netværk og systemer (52 pct.) og/eller at miste omsætning (48 pct.). Men også en relativt stor del af SMV'erne frygter de mere indirekte, langsigtede konsekvenser såsom at miste troværdighed overfor deres kunder (39 pct.), at få et dårligt ry i branchen (19 pct.) eller en dårlig sag i pressen (16 pct.).
- **Forsikring:** 62 pct. af de danske SMV'er har tegnet en forsikring i forhold til it-sikkerhedshændelser, hvilket er en stigning fra 57 pct. i 2018. De SMV'er, som har tegnet en cyberforsikring, har implementeret flere it-sikkerhedsforanstaltninger sammenlignet med de SMV'er, som ikke har tegnet en forsikring.
- **Dataetik og digital sikkerhed:** Der findes en stærk sammenhæng mellem SMV'ernes arbejde med digital sikkerhed og dataetik. De SMV'er, som arbejder aktivt med dataetik, har blandt andet implementeret signifikant flere it-sikkerhedsforanstaltninger end de virksomheder, som ikke arbejder med dataetik.
- **Ledelsesinvolvering:** 74 pct. af SMV'erne svarer, at ledelsen 'i høj grad' er involveret i beslutninger om virksomhedens arbejde med digital sikkerhed. Dermed er ledelsen kun i nogen grad, lille grad eller slet ikke er involveret i beslutninger om virksomhedens arbejde med digital sikkerhed blandt 26 pct. af de danske SMV'er.

1. Introduktion

Cyberkriminalitet er en af de største trusler for dansk erhvervsliv. En trussel som kun bliver større i takt med, at de danske virksomheder bliver stadig mere digitale, og at de digitale angreb bliver flere og mere avancerede. Center for Cybersikkerhed vurderer, at truslen for cyberkriminalitet er 'meget høj' i Danmark for både myndigheder, borgere og virksomheder[1]. Den senest CEO undersøgelse fra PwC viser, at cybertruslen indtager en klar førsteplads på listen over danske toplederes bekymringer og dermed overgår bekymringer for pandemi, overregulering og klimaforandringer[2]. Der er også grund til bekymring, da cybersikkerhedshændelser kan medføre store omkostninger for både den enkelte virksomhed og for samfundet som helhed. Beregninger fra Dansk Erhverv viser blandt andet, at cyberangreb samlet set kostede danske virksomheder (minimum) 4 mia. kr. i 2018[3].

Selvom det ofte er hackerangreb i de største virksomheder, der bliver belyst i medierne, er der også mange små og mellemstore virksomheder (SMV'er), som årligt rammes af angreb, og også her er tendensen stigende[4]. Derfor er det vigtigt, at virksomheder i alle størrelser har fokus på digital sikkerhed, så vi har et erhvervsliv, der er modstandsdygtigt over for digitale angreb. Alligevel har mange danske SMV'er et utilstrækkeligt digitalt sikkerhedsniveau, hvilket blandt andet skyldes, at mange SMV'er ikke ser sig selv i risikozonen for digitale angreb og/eller ikke har de nødvendige ressourcer til at sikre sig. Derfor udvikler Erhvervsstyrelsen gratis vejledninger, værktøjer og awareness-aktiviteter særligt målrettet danske SMV'er med henblik på at styrke deres digitale sikkerhed. For at kunne målrette Erhvervsstyrelsen indsatser på området er formålet med denne analyse at blive klogere på de danske SMV'ers arbejde med digital sikkerhed. Analysen er således en opfølgning på Erhvervsstyrelsen analyse fra sidste år: **Digital sikkerhed i danske SMV'er, 2020**.

Analysen er opbygget i følgende afsnit:

2. Danske SMV'ers arbejde med digital sikkerhed
3. Digital sikkerhed blandt SMV'er, der arbejder med digitale teknologier
4. Sammenhæng mellem it-kompetencer og digital sikkerhed
5. Oplevede barrierer ved implementering af it-sikkerhedsløsninger
6. It-sikkerhedshændelser i danske SMV'er
7. Sammenhæng mellem SMV'ernes fokus på digital sikkerhed og dataetik
8. Fokus på digital sikkerhed blandt SMV'ernes ledelse
9. Metode

[1] Center for Cybersikkerhed (2021): Cybertruslen mod Danmark

[2] PwC (2021): CEO Survey 2021 "Topledernes agenda i en forandret verden".

[3] Dansk Erhverv (2019): Er Danmark klar til "Giganternes tid"?

[4] Center for Cybersikkerhed: https://www.metal-supply.dk/article/view/778917/advarsel_fra_center_for_cybersikkerhed_hackere_gar_efter_mindre_virksomheder

1.1 Afgrænsning og datagrundlag

Datagrundlaget for årets rapport består af to spørgeskemaundersøgelser blandt danske virksomheder. Ligesom sidste år er resultaterne i denne rapport først og fremmest baseret på Danmarks Statistiks årlige spørgeskemaundersøgelse 'IT-anvendelse i virksomhederne' (VITA). Mens resultaterne i sidste års rapport var baseret på data indsamlet i 2019 blandt 5.292 virksomheder med 5+ ansatte, er resultaterne i denne rapport baseret på data indsamlet i 2020 blandt 3.947 virksomheder med 10+ ansatte. For alle enslydende spørgsmål er udviklingen i virksomhedernes arbejde med digital sikkerhed beregnet mellem de to VITA-undersøgelser i 2019 og 2020. Eftersom mikrovirksomheder med 5-9 ansatte kun indgår i VITA 2019, er resultaterne omkodet, så de alene er baseret på besvarelser fra virksomheder med 10-249 ansatte og dermed tilsvarende målgruppen i VITA 2020. Der skal endvidere tages forbehold for, at det ikke er de samme virksomheder, som har besvaret de to VITA-undersøgelser (paneldata), hvorfor sammenligningsgrundlaget beror på det store, repræsentative datagrundlag i de to undersøgelser.

Generelt viser data dog *ikke* den store udvikling i virksomhedernes arbejde med digital sikkerhed fra VITA 2019 til VITA 2020. At der ikke ses en større udvikling, er dog interessant i sig selv og en indikator for, at der fortsat er behov for at øge SMV'ernes fokus på området. Den begrænsede udvikling kan dog også skyldes, at der kun er stillet sammenlignelige spørgsmål igennem to år hvad angår digital sikkerhed (2019, 2020). Det forventes således, at der vil ses en større udvikling i SMV'ernes arbejde med digital sikkerhed, når det foreligger sammenlignelige resultater for en længere tidsperiode. Desuden afspejler VITA 2020 virksomhedernes situation i 2019, hvorfor eventuelle Corona-effekter endnu ikke indgår i resultaterne. Da pandemien i høj grad har sat fokus på digital sikkerhed blandt virksomheder, bliver det interessant at følge udviklingen i VITA 2021, hvori eventuelle Corona-effekter vil indgå.

Udover VITA-undersøgelsen er resultaterne i årets rapport også baseret på en spørgeskemaundersøgelse gennemført af Epinion for Erhvervsstyrelsen i efteråret 2020 med svar fra 1.806 danske SMV'er i størrelsen 5-249 ansatte. Epinion-undersøgelsen indeholder flere og andre spørgsmål end VITA-undersøgelsen, og gør det blandt andet muligt at måle andelen af SMV'er, som har et utilstrækkeligt digitalt sikkerhedsniveau set i forhold til deres risikoprofil, hvilket PwC har udregnet for ERST. Derudover bibringer Epinion-undersøgelsen nye indsigter om hvilke tiltag, som kan øge SMV'ernes fokus på digital sikkerhed, hvad de frygter ved angreb, ledelsens involvering i digital sikkerhed mm.

For både VITA-undersøgelsen og Epinion-undersøgelsen gælder, at data er vægtet, således at besvarelserne afspejler et repræsentativt udsnit af de danske SMV'er[5]. Eftersom VITA-undersøgelsen og Epinion-undersøgelsen er besvaret af forskellige virksomheder på forskellige tidspunkter og indsamlet via forskellige metoder, kan resultaterne for disse to dataindsamlinger ikke sammenlignes[6]. Det vil gennem rapporten fremgå hvilken undersøgelse, som ligger til grund for de forskellige resultater/figurer. For begge datasæt gælder desuden, at SMV'erne defineres som virksomheder med op til 249 ansatte. Store virksomheder på 250 eller flere medarbejdere indgår således ikke i målgruppen, men vil løbende inddrages til sammenligning med SMV-gruppen. For en uddybning af de to undersøgelser henvises til afsnit 9. Metode.

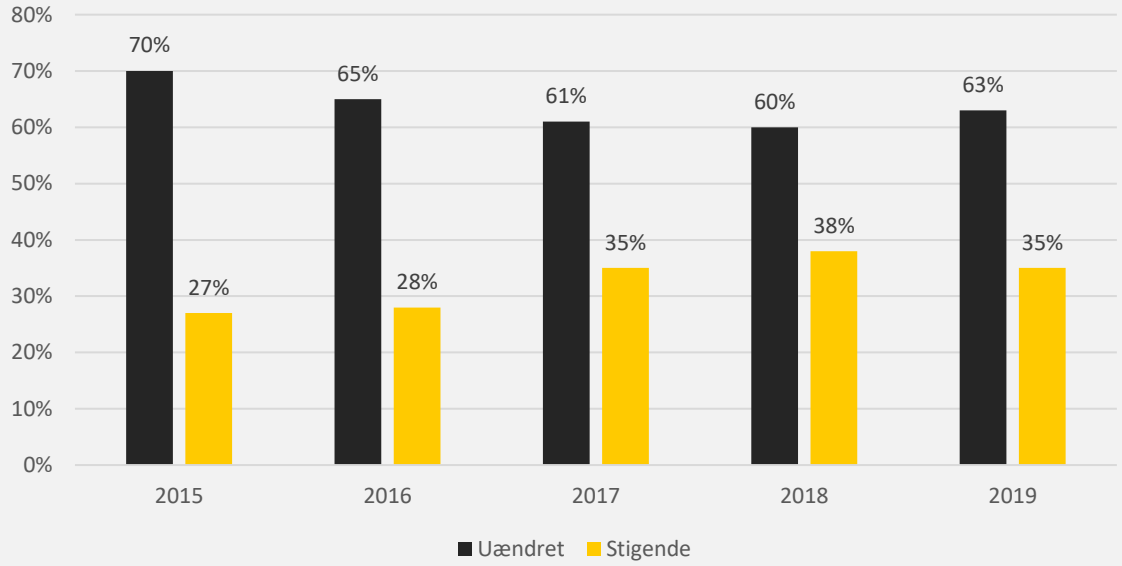
[5] På fordelinger for geografi, sektor, firmatype og antal ansatte.
[6] Fx er undersøgelsen af Danmarks Statistik obligatorisk at svare på, hvorimod undersøgelsen fra Epinion er baseret på frivillig deltagelse via invitationer sendt i e-boks.

2. Danske SMV'ers arbejde med digital sikkerhed

2.1 Stigende investeringer i digital sikkerhed

SMV'erne har årligt øget deres investeringer i digital sikkerhed fra 2015-2019. I 2019 har 35 pct. af de danske SMV'er investeret mere i digital sikkerhed i forhold til det forgange år, som illustreret i *figur 1*.

Figur 1. SMV'ernes investeringer i digital sikkerhed



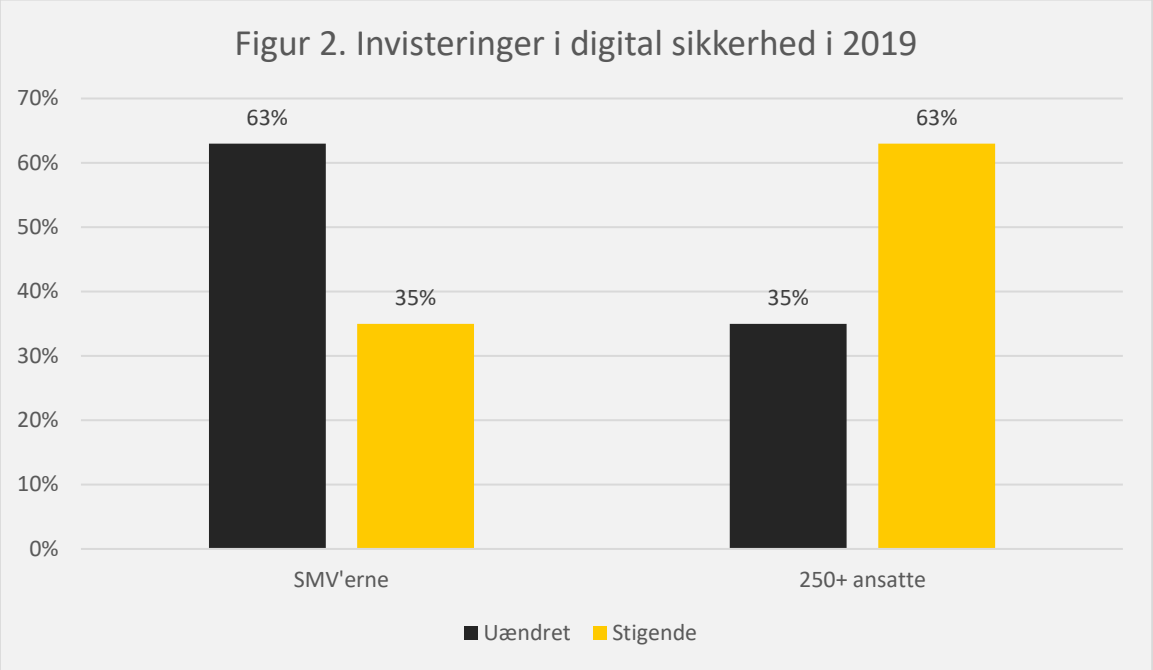
Note: Tallene summerer ikke til 100 pct. da en mindre andel af virksomhederne havde faldende udgifter på tværs af årene.
Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2020).

Copenhagen Economics har for Erhvervsstyrelsen undersøgt, hvilke effekter det har, når små og mellemstore virksomheder investerer i digital sikkerhed. De kom frem til, at investeringer i digital sikkerhed kan føre til tre overordnede effekter[7]:

- Nedsat sandsynlighed for et cyberangreb og mindre konsekvenser ved eventuelle angreb.
- At virksomhederne er mere attraktive i markedet, herunder overfor eventuelle leverandører og kunder.
- At virksomheden får et bedre overblik over deres data og digitale processer, hvilket kan bidrage til at effektivisere forretningen.

[7] Copenhagen Economics (2019): 'Værdien af Digital Sikkerhed'. Resultaterne bygger på interviews med virksomheder. Undersøgelsen er ikke offentliggjort.

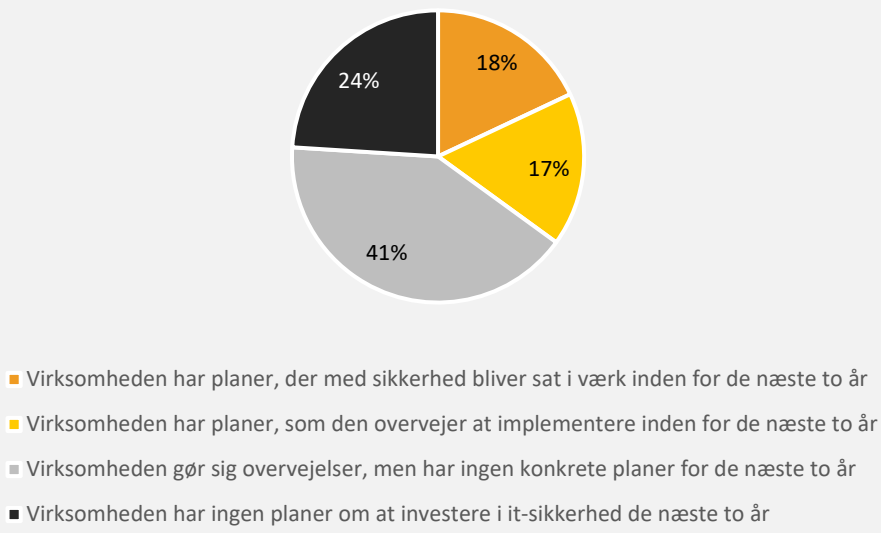
Det er således positivt, at danske virksomheder år for år øger deres investeringer i digital sikkerhed. Der ses dog en tendens til, at de større virksomheder i højere grad end SMV'erne øger deres investeringer i digital sikkerhed. Fx har hele 63 pct. af de store virksomheder med over 250 ansatte øget deres investeringer i digital sikkerhed, hvilket er markant højere end 35 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 2020).

I Epinion-undersøgelsen spørges der til, om virksomhederne har besluttet at bruge flere ressourcer (økonomi og/eller medarbejdertimer) på digital sikkerhed inden for de næste to år, altså deres fremadrettede planer på området. Som *figur 3* viser, har 18 pct. af SMV'erne helt konkrete planer om at investere flere ressourcer på digital sikkerhed de kommende to år, mens 24 pct. af SMV'erne ikke har planer om dette. De resterende 58 pct. af SMV'erne overvejer (med eller uden konkrete planer) at investere mere i digital sikkerhed de kommende år. Dette indikerer, at mange SMV'er er opmærksomme på, at der også fremadrettet vil være behov for et øget fokus på digital sikkerhed.

Figur 3. Planlagte ressourcer på digital sikkerhed de næste to år



Note: Svarkategorien 'ved ikke' er frasorteret og indgår ikke i opgørelsen.
Kilde: Egne beregninger baseret på data indsamlet af Epinion i 2020.

2.2 40 pct. af de danske SMV'er har et utilstrækkeligt digitalt sikkerhedsniveau

Et passende digitalt sikkerhedsniveau afhænger af den enkelte virksomheds risikoprofil. Man kan derfor ikke tale om ét fast niveau af digitale sikkerhedstiltag, som er tilstrækkeligt for alle danske virksomheder. Virksomheder varierer i bl.a. størrelse, teknologianvendelse, dataopbevaring og dataanvendelse, der kan have betydning for både sandsynligheden for at blive ramt af eksterne digitale angreb og evt. konsekvenser herved. Epinion-undersøgelsen fra ultimo 2020 indeholder spørgsmål, der både gør det muligt at afdække virksomhedernes digitale sikkerhedsniveau og deres risikoprofil. Derfor har Erhvervsstyrelsen fået PwC til at udarbejde et statusbillede af det digitale sikkerhedsniveau i danske SMV'er med henblik på at kortlægge, om danske SMV'er har et tilstrækkeligt it-sikkerhedsniveau i forhold til deres risikoprofil.

Baseret på dataindsamlingen fra Epinion har PwC udarbejdet:

- Et indeks over SMV'ernes sikkerhedsniveau
- Et indeks over SMV'ernes risikoprofil
- En vurdering af hvilket sikkerhedsniveau, som virksomheder med de forskellige risikoprofiler bør leve op til

Indekset for SMV'ernes digitale 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'ernes risikoprofil baserer sig på spørgsmål, der siger noget om SMV'ernes konsekvensniveau og sandsynligheden for, at de oplever en hændelse. I forhold til at vurdere matchet mellem SMV'ernes sikkerhedsniveau og deres risikoprofil anvender PwC niveauerne "lav", "middel" og "høj" til at inddele SMV'erne i tre typer (de sårbare, de tilpas sikrede og de påpasselige). Hvis fx både sikkerhedsniveau og risikoprofil er middel, vurderer PwC, at en SMV's basale it-sikkerhedsniveau er tilpas. En detaljeret beskrivelse af den metodiske fremgangsmåde - herunder hvilke konkrete spørgsmål og vægte, som danner grundlag for de to indeks samt matchet mellem disse - er beskrevet i bilag 1*: Indeksering af danske SMV'ers digitale sikkerhedsniveau og risikoprofil samt matchet mellem disse* (PwC for ERST, 2021).

Resultaterne fra PwC viser, at 40 pct. af de adspurgte SMV'er er sårbare, da de har et digitalt sikkerhedsniveau, der er lavere end deres risikoprofil, og at 44 pct. af SMV'erne er tilpas sikrede, da de har et digitalt sikkerhedsniveau, der matcher risikoprofilen. Den sidste gruppe på 16 pct. er påpasselige, i den forstand at de har et højere sikkerhedsniveau, end deres risiko angiver. Det skal i forbindelse med resultaterne gøres opmærksom på, at spørgsmålene i Epinion-undersøgelsen ikke indeholder en udtømmende liste af it-sikkerhedstiltag, men afspejler en proxy for brug af de mest basale sikkerhedstiltag, som SMV'erne bør forholde sig til[8].

Det skal endvidere gøres opmærksom på, at Monitor Deloitte har gennemført en lignende analyse for Erhvervsstyrelsen i 2018, der ligeledes matcher SMV'ernes digitale sikkerredsniveau med deres risikoprofil. Resultaterne fra PwC er i høj grad på niveau med resultaterne fra Deloittes analyse fra 2018, hvilket indikerer, at der ikke har fundet den store udvikling sted. Dog kan resultaterne i de to analyser ikke direkte sammenlignes, eftersom de beror på dataindsamlinger med forskellige spørgsmål, hvorfor SMV'ernes digitale sikkerhedsniveau og risikoprofil er operationaliseret forskelligt i de to analyser.

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

		It-sikkerhedsniveau		
		Lav	Middel	Høj
Risikoprofil	Høj	De sårbare 40 %		
	Middel		De tilpas sikrede 44 %	De påpasselige 16 %
	Lav			

Note: Den metodiske fremgangsmåde for udviklingen af de to indeks samt matchet mellem disse fremgår af bilag 1: Indeksering af danske SMV'ers digitale sikkerhedsniveau og risikoprofil samt matchet mellem disse (PwC for ERST, 2021).
Kilde: Beregninger fra PwC baseret på data indsamlet af Epinion i 2020.

[8] Derfor er matchet mellem virksomhedernes digitale sikkerhedsniveau og risikoprofil udformet under antagelse af at et "højt" digitalt sikkerhedsniveau i realiteten afspejler et basalt digitalt sikkerhedsniveau. Med basale tiltag menes tiltag, som SMV'erne som minimum bør forholde sig til, om de bør implementere, selvom alle SMV'er ikke nødvendigvis bør implementere alle tiltagene.

Selvom der har været en stigning i danske SMV'er, der prioriterer digital sikkerhed i form af flere investeringer, er der således fortsat et stort potentiale for at øge den digitale sikkerhed i mange danske SMV'er, da mere end hver tredje SMV har et utilstrækkeligt digitalt sikkerhedsniveau.

Til virksomheder, der ønsker hjælp til, hvor de skal sætte ind for at styrke deres digitale sikkerhed set i lyste af deres risikoprofil, tilbyder Erhvervsstyrelsen **Sikkerhedstjekket.dk**. Sikkerhedstjekket er et online testværktøj tilpasset virksomheder og bygger på, at ikke alle virksomheder har brug for det samme sikkerhedsniveau. Sikkerhedstjekket er kort beskrevet nedenfor.

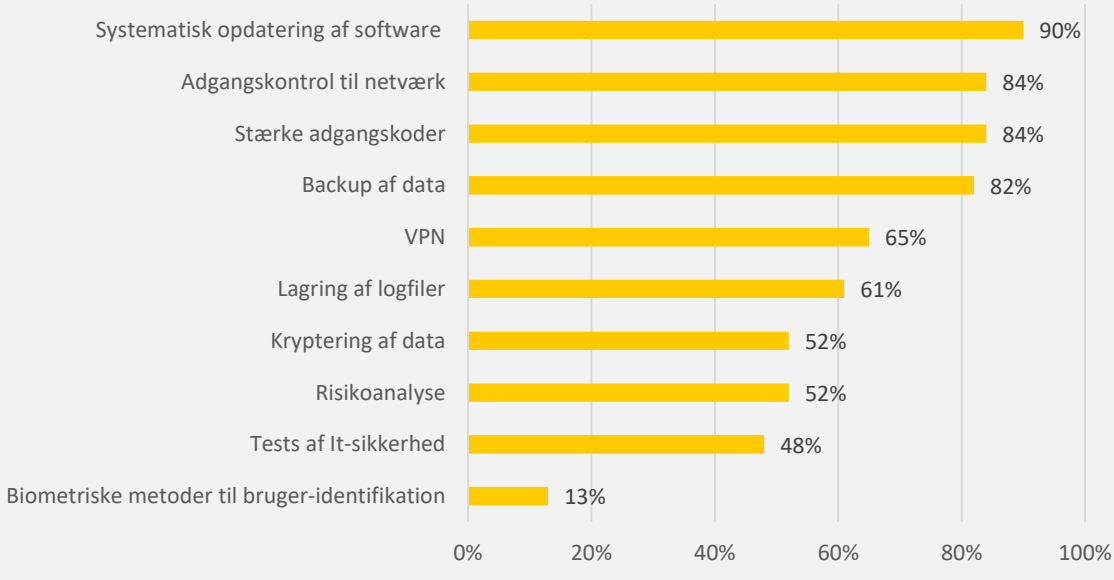
Tekstboks: Kort beskrivelse af Sikkerhedstjekket

Sikkerhedstjekket starter med 5 spørgsmål, som bruges til at finde virksomhedens risikoprofil. Efter risikospørgsmålene skal virksomheden besvare 17 testspørgsmål fordelt på 5 temaer. På baggrund af virksomhedens risikoprofil og svarene i testspørgsmålene, får man en rapport med gode råd til at matche virksomhedens digitale sikkerhed op imod dens risikoprofil.

2.3 SMV'ers brug af it-sikkerhedsforanstaltninger, herunder basale foranstaltninger

I VITA-undersøgelsen fra 2020 spørges der til, hvorvidt virksomheden har implementeret 10 forskellige it-sikkerhedsforanstaltninger i 2019[9]. En oversigt over de 10 it-sikkerhedsforanstaltninger og andelen af SMV'er der har implementeret disse, fremgår af *figur 4*.

Figur 4. SMV'ernes brug af 10 it-sikkerhedsforanstaltninger i 2019



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

[9] It-sikkerhedsforanstaltninger defineres som 'systemer og procedurer, der skal sikre konsistens, autenticitet, tilgængelighed og fortrolighed data og it-systemer'.

Som det fremgår, har 90 pct. af de danske SMV'er implementeret systematisk opdatering af software, mens 82 pct. gennemfører backup af data. 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]. Systematisk opdatering af virksomhedens software er helt essentielt for at undgå angreb. Derimod kan backup af data bidrage til at få virksomheden hurtigt op at køre igen, hvis den har været udsat for et angreb. Derfor bør stort set *alle* virksomheder som minimum anvende disse to basale foranstaltninger. På trods af dette, har blot 76 pct. af SMV'erne implementeret *begge* de to basale sikkerhedsforanstaltninger. Det vil sige, at hele 24 pct. af de danske SMV'er *ikke* anvender de to basale it-sikkerhedsforanstaltninger som en del af deres digitale sikkerhed. Til sammenligning brugte 22 pct. af SMV'erne ikke de to basale sikkerhedstiltag i 2018[11] - så der ses ikke engang en positiv udvikling på området.

I sammenligning med de øvrige 27 EU-medlemslande indtager Danmark en delt 4. plads, når det kommer til andelen af SMV'er, som tager backup af data og en delt 9. plads, når det kommer til andelen af SMV'er, der opdaterer deres styresystemer[12]. Resultaterne peger således på, at der ligger et fortsat potentiale i at få danske SMV'er til at få øjnene op for selv helt basale sikkerhedstiltag, der kan øge deres digitale sikkerhed.

En forklaring på, at så mange virksomheder ikke anvender selv basale sikkerhedstiltag, kan være, at mange SMV'er ikke ser sig selv som mål for it-kriminelle, fordi de ikke mener, at de har informationer, der kan interessere andre. Men de fleste virksomheder er i besiddelse af systemer og data, der er vigtige for den daglige drift, som fx kundekartoteker og e-mails, og hvis data er værdifulde for en virksomhed, kan det udnyttes af it-kriminelle.

På **sikkerdigital.dk/virksomhed** har Erhvervsstyrelsen 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 og få styr på deres backup-rutiner.

Foruden de to basale sikkerhedstiltag er der også en betydelig andel af SMV'erne, som ikke benytter sig af øvrige grundlæggende it-sikkerhedsforanstaltninger. Fx er det blot omkring halvdelen af SMV'erne, der gennemfører en risikoanalyse. Det kan blandt andet skyldes, at mange SMV'er ikke ved, hvordan de skal gøre, og hvor de skal starte. Derfor har Erhvervsstyrelsen i foråret 2021 lanceret et **risikovurderingsværktøj**, som guider SMV'er til at få overblik over deres systemer og hjælper dem med at vurdere, hvor virksomheden har risici forbundet med deres digitale systemer.

Samlet sat danner de ovenstående sikkerhedsforanstaltninger i *figur 4* baggrund for analysens operationalisering i hhv. 'få', 'nogle' og 'mange' it-sikkerhedsforanstaltninger, som beskrevet i *tabel 2*.
De 9 it-sikkerhedstiltag skal dog ikke ses som en udtømmende liste af nødvendige sikkerhedsforanstaltninger, men anses samlet set for en god proxy for SMV'ernes brug af de mest basale sikkerhedstiltag. Det må således forventes, at fx store og/eller teknologitunge virksomheder har flere og mere avancerede sikkerhedstiltag, som denne analyse ikke har med.

---

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

[11] OBS. dette tal afviger fra resultatet i rapporten sidste år, fordi det kun inkluderer virksomheder med 10-249 ansatte for sammenlignelighedens skyld (da vi ikke har svar fra mikrovirksomheder med 5-9 ansatte i år, jf. indledningen).

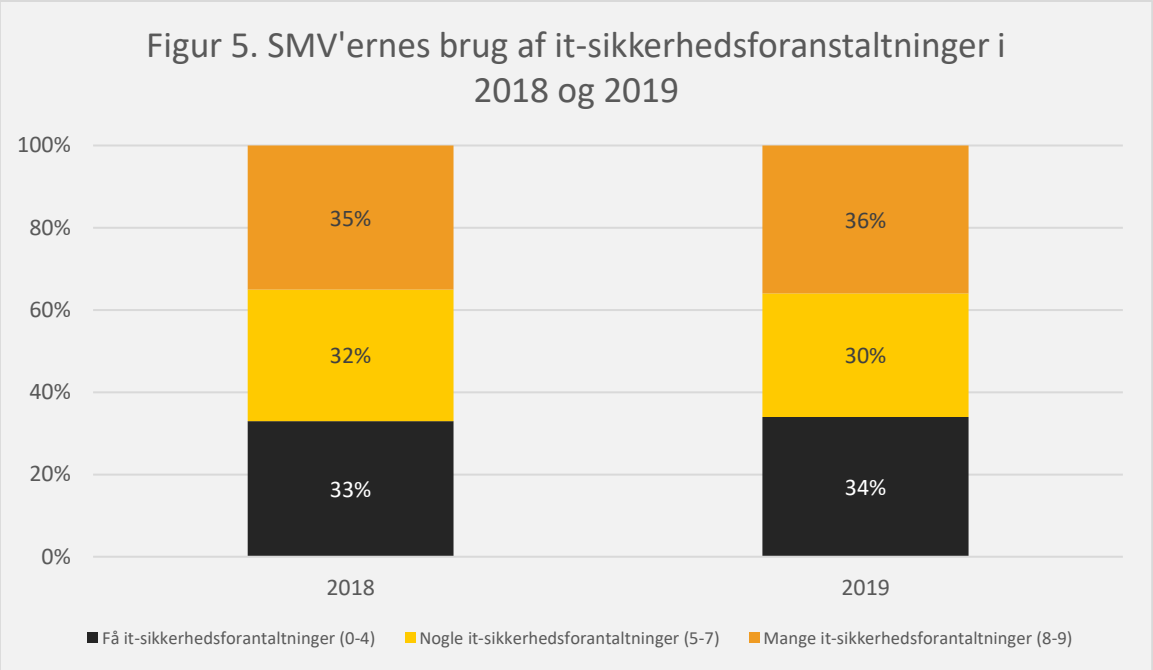
[12] OBS. Denne sammenligning mellem EU-landene beror på data indsamlet i 2019, som afspejler situationen i 2018, og er ikke tilgængelig for data indsamlet i 2020: https://ec.europa.eu/eurostat/databrowser/view/isoc_cisce_ra/default/table?lang=en

Tabel 2: Operationalisering af virksomheders brug af it-sikkerhedsforanstaltninger (indeks)

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

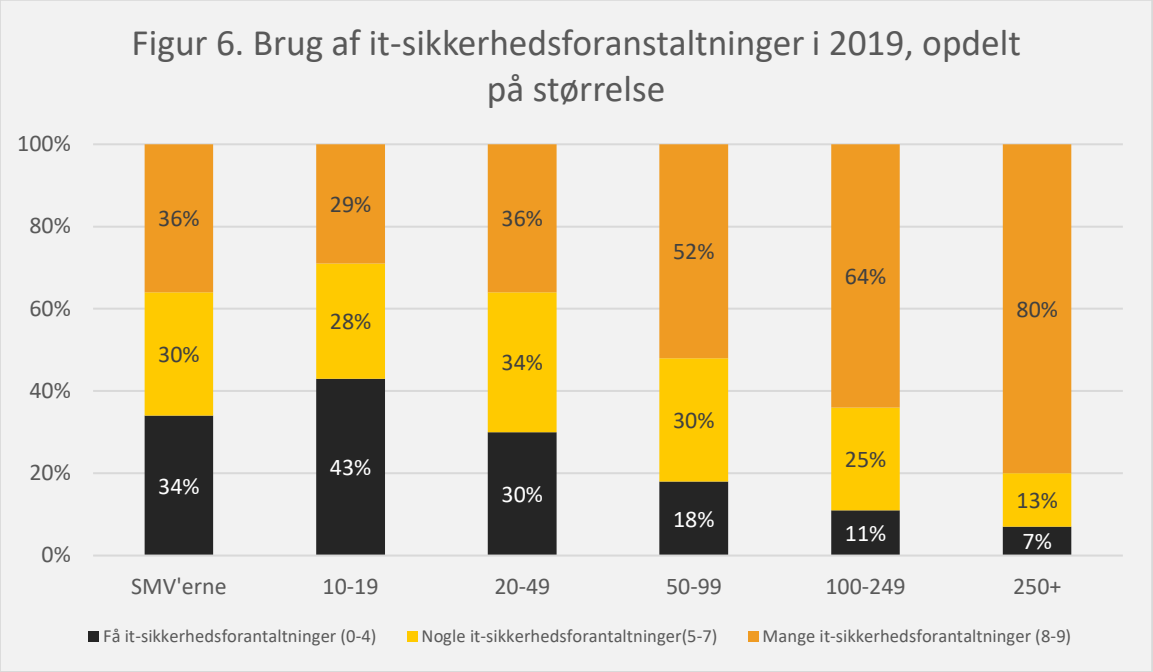
Note: En nærmere forklaring af denne operationalisering fremgår af afsnit 9. Metode.
Note: Som begrundet i afsnit 9. Metode er foranstaltningen 'biometriske metoder til brugeridentifikation' taget ud af det samlede indeks, som derfor består af de 9 resterende sikkerhedsforanstaltninger

Figur 5 viser SMV'ernes brug af de 9 it-sikkerhedsforanstaltninger i hhv. 2018 og 2019. I 2019 anvendte 34 pct. af SMV'erne blot 'få' (0-4) it-sikkerhedsforanstaltninger og dermed under halvdelen af de 9 anbefalede it-sikkerhedsforanstaltninger, mens 30 pct. brugte 'nogle´ (5-7) og 36 pct. brugte 'mange' (8-9) af de 9 anbefalede it-sikkerhedsforanstaltninger. Som det også fremgår af figuren, er der ikke betydelig forskel fra SMV'ernes brug af it-sikkerhedsforanstaltninger fra 2018 til 2019.



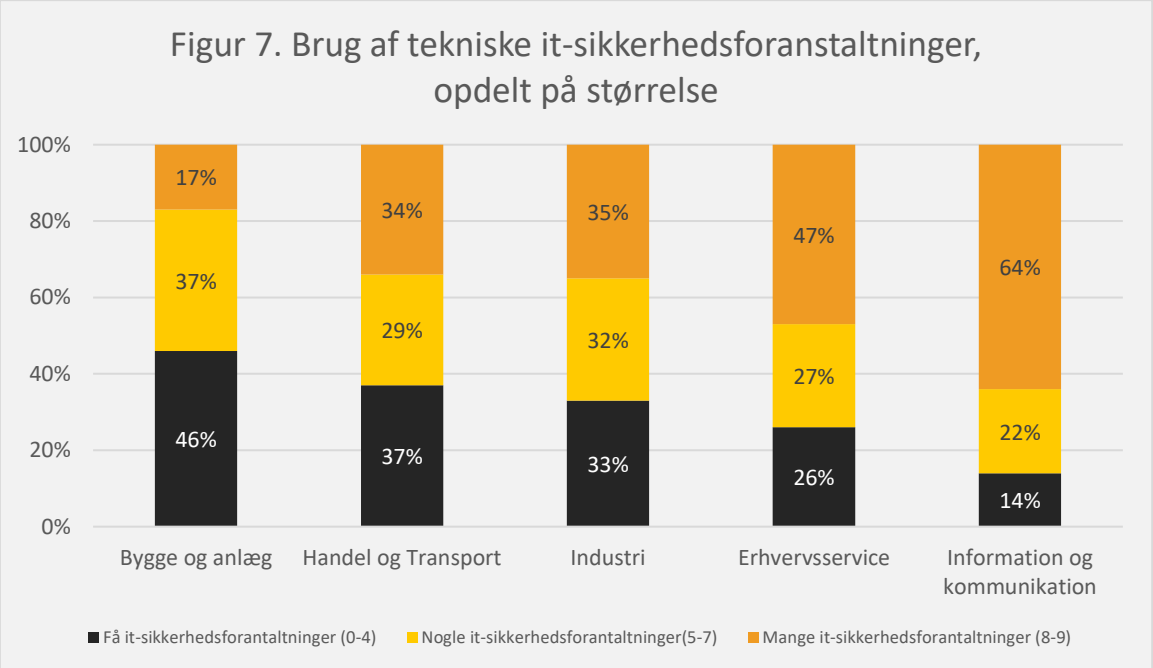
Note: Se tabel 1 og metodeafsnittet for definitioner på hhv. få, middel og mange it-sikkerhedsforanstaltninger.
Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2020).

Figur 6 illustrerer SMV'ernes brug af de 9 it-sikkerhedsforanstaltninger i 2019 opdelt på virksomhedsstørrelse. I lighed med sidste år er tendensen klar - jo mindre virksomhed, jo færre it-sikkerhedsforanstaltninger har den typisk implementeret.



Note: Se tabel 1 og metodeafsnittet for definitioner på hhv. få, middel og mange it-sikkerhedsforanstaltninger.
Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2020).

Ser vi nærmere på anvendelsen af it-sikkerhedsforanstaltninger for SMV'erne inden for de forskellige brancher, ses der også betydelige forskelle, *jf. figur 7*. Branchen 'Bygge og Anlæg' har generelt implementeret færrest it-sikkerhedstiltag efterfulgt af branchen 'Handel og Transport'. Dette er ikke overraskende, da en relativt stor andel af medarbejderne inden for disse brancheralt andet lige må forventes at arbejde mindre digitalt end SMV'er inden for branchen 'Information og kommunikation', da en stor andel af medarbejderne inden for denne branche ofte vil være i besiddelse af kundedata osv., hvilket må forventes at være i højere risiko for digitale angreb.



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

Der er også forskel på SMV'ernes brug af it-sikkerhedsforanstaltninger alt efter hvilket erhvervshusområde, de tilhører. Denne geografiske forskel forsvinder dog ved kontrol for virksomhedsstørrelse og branche. De geografiske forskelle er således blot et udtryk for forskellige virksomhedssammensætninger (størrelse, branche osv.) inden for de forskellige erhvervshusområder. At der ikke findes geografiske forskelle, var dog også at forvente, da hackerne arbejder virtuelt og kan nå deres ofre fra hele verden modsat "traditionel" fysisk kriminalitet.

2.4 Især de store virksomheder informerer deres medarbejdere om deres rolle og ansvar ift. digital sikkerhed

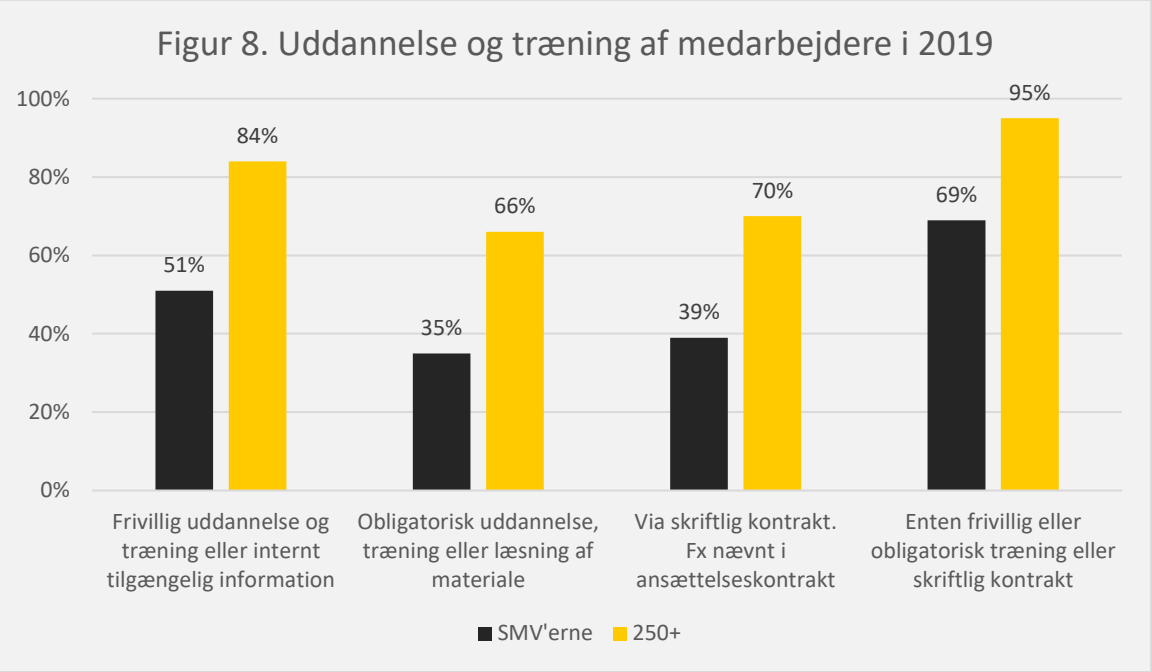
Foruden de tekniske it-sikkerhedsforanstaltninger spiller medarbejderne en vigtig rolle i forhold til virksomhedernes digitale sikkerhed. Mange sikkerhedsbrud sker på grund af manglende viden blandt medarbejdere. De kan fx blive narret til at klikke på et usikkert link eller til at udlevere deres adgangskode.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

Samlet set informerer 69 pct. af SMV'erne deres medarbejdere om deres rolle og ansvar ift. digital sikkerhed gennem enten frivillig træning, obligatorisk træning eller via skriftlig kontrakt i 2019. Denne andel ligger på niveau med 2018, hvis man sammenligner SMV'erne i størrelsen 10-249 ansatte i de to VITA-undersøgelser.

Figur 8 viser træning af medarbejderne i SMV'er med 10-249 ansatte i 2019 sammenlignet med de store virksomheder med 250+ ansatte. For alle virksomhedsstørrelser gælder, at virksomheder, der arbejder med medarbejder-awareness gennem ét af de tre tiltag, også anvender flere it-sikkerhedsforanstaltninger. Der findes således en stærk sammenhæng mellem virksomheder, der fokuserer på de tekniske og organisatoriske sikkerhedstiltag.

Data fra Eurostat baseret på VITA-undersøgelsen fra 2019 viser, at Danmark er godt med, hvad angår medarbejdertræning sammenlignet med de øvrige EU-medlemslande. Danmark ligger nemlig på hhv. 2 og 4 pladsen, hvis man ser på andelen af SMV'er, som gennemfører obligatorisk og frivillig uddannelse og træning for deres medarbejdere om deres rolle og ansvar ift. digital sikkerhed[13].

[13] Denne sammenligning mellem EU-landene beror på data indsamlet i 2019, som afspejler situationen i 2018, og er ikke tilgængelig for data indsamlet i 2020. Kilde: https://ec.europa.eu/eurostat/databrowser/view/isoc_cisce_ra/default/table?lang=en



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

3. Digital sikkerhed blandt virksomheder, der arbejder med digitale teknologier

Flere og flere virksomheder benytter digitale teknologier som blandt andre IoT, cloud og big data analyse. Denne digitalisering skaber mange nye muligheder for danske virksomheder, men brug af digitale løsninger kan også indebære en række nye udfordringer og sikkerhedstrusler, hvilket kan stille endnu større krav til virksomhedernes digitale sikkerhed.

Virksomheders brug af digitale teknologier kan fx introducere nye sårbarheder, skabe flere angrebsflader og større konsekvenser ved eventuelle angreb.

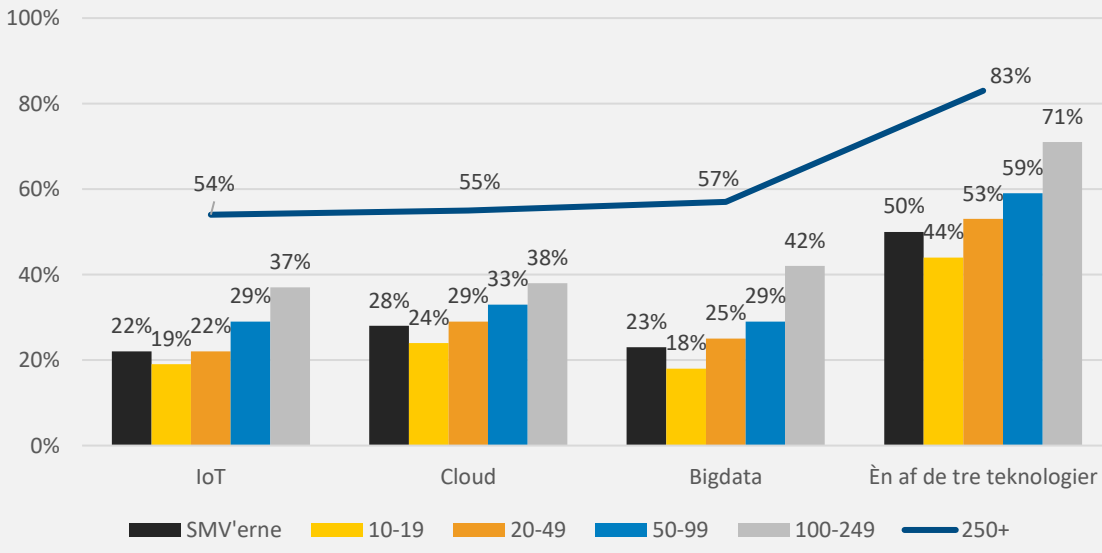
Mere konkret vil virksomheder, som arbejder med big data analyse, som navnet antyder, være i besiddelse af store digitale datamængder og derfor også være mere sårbare overfor eventuelle angreb. Brugen af cloud-tjenester kan også betyde, at man på nogle områder har mindre kontrol over sine data og systemer end ved traditionelle indkøb eller udlicitering af it, og det er derfor vigtigt, at virksomhederne er opmærksomme på, hvordan deres data er beskyttet i deres cloudløsning. Endelig bruger mange virksomheder internetforbundne sensorer (IoT-enheder) til fx at videoovervåge et kontor, fjernstyre temperaturen i en bygning eller se, hvornår en maskine skal serviceres. Men mange virksomheder ser i den forbindelse deres IoT-enheder som fysiske produkter og glemmer, at de er koblet til nettet og derfor kan hackes og udgøre et alvorligt sikkerhedsproblem for dem selv og andre. Hackerne kan blandt andet bruge dårligt beskyttede IoT-enheder som springbræt til at få adgang til virksomhedens øvrige computernetværk. Det kan fx betyde, at en virksomheds produktion går i stå, eller at it-kriminelle kan udføre ransomware-angreb eller lække virksomhedens data.

3.1 Især de store virksomheder arbejder med digitale teknologier

Figur 9 viser danske virksomheders brug af hhv. cloud, big data analyse og IoT i 2019. Brugen af cloud defineres i denne analyse udelukkende som virksomheder, der køber cloud services til infrastruktur til drift af egne it-programmer. Det skyldes en vurdering af, at virksomheder, som køber cloud til drift af egne systemer, har et væsentligt større ansvar ift. sikkerheden sammenlignet med virksomheder, der køber cloud services til "færdige" systemer som fx CRM, Outlook, regnskabssystemer mm., hvor ansvaret for sikkerheden i høj grad ligger hos leverandøren. Af samme årsag defineres brugen af big data analyse udelukkende som virksomheder, der selv har gennemført big data analyse (dvs. eksklusiv virksomheder, der har fået en ekstern leverandør til at gennemføre big data for dem)[14].

Baseret på ovenstående definitioner anvendes cloud af 28 pct. af SMV'erne, mens big data analyse og IoT anvendes af hhv. 23 pct. og 22 pct. af de danske SMV'er. Samlet set anvender 50 pct. af SMV'erne én af de tre teknologier, hvilket til sammenligning gælder 83 pct. af de store virksomheder med 250+ ansatte. Også blandt SMV-gruppen ses en tendens til, at især de større virksomheder arbejder med de tre digitale teknologier. Én forklaring på, at større virksomheder har et højere sikkerhedsniveau er således, at de i højere grad arbejder med nye teknologier og dermed er mere udsatte for eventuelle sikkerhedsangreb. Det er ikke muligt at sammenligne SMV'ernes brug af digitale teknologier i 2019 med 2018, da forskellige teknologier og spørgsmålsformuleringer indgår i de to VITA-undersøgelser.

Figur 9: Brug af digitale teknologier opdelt på størrelse, 2019



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

I følgende afsnit ser nærmere på den digitale sikkerhed blandt virksomheder, der arbejder med digitale teknologer, for at afdække, om den digitale udvikling og den digitale sikkerhed går hånd i hånd.

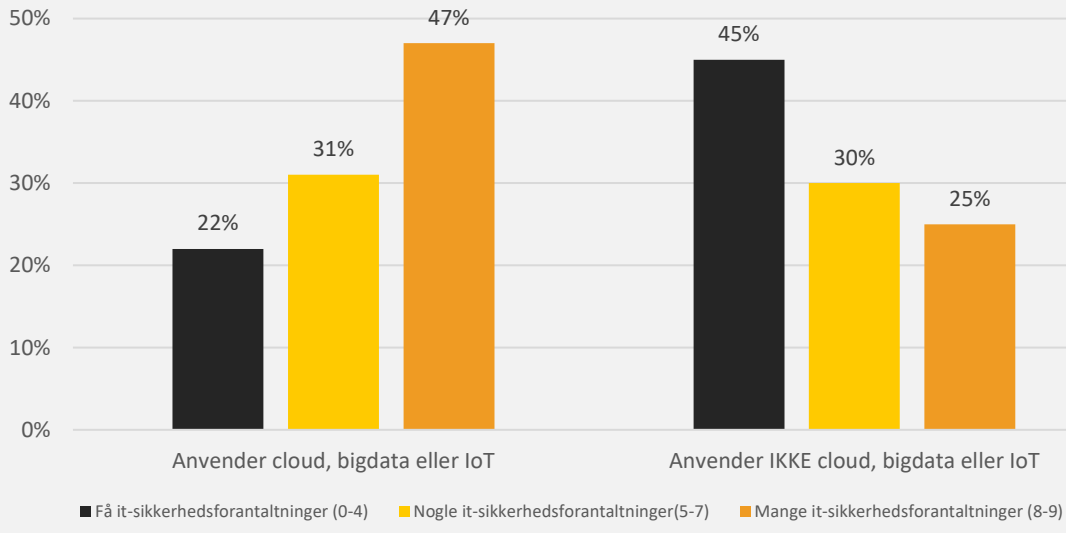
[14] En nærmere definition på virksomhedernes brug af de tre teknologier findes uddybet i afsnit 9. Metode.

3.2 Blandt SMV'er der arbejder med digitale teknologier har 15 pct. ikke implementeret de to basale sikkerhedstiltag

Figur 10 sammenligner brugen af it-sikkerhedsforanstaltninger alt efter om SMV'erne arbejder med én af de tre teknologier eller ej. Som det fremgår, anvender de SMV'er der arbejder med cloud, IoT eller big data analyse generelt flere it-sikkerhedstiltag end de SMV'er, som ikke arbejder med én af de tre teknologier, hvilket er positivt. Men taget virksomhedernes risiko i betragtning, må det siges at være en betydelig andel, at 22 pct. blandt SMV'er der arbejder med én af de digitale teknologier ikke har implementeret mere end 4 ud af de 9 anbefalede it-sikkerhedsforanstaltninger. For virksomheder der arbejder med nye teknologier, skal først og fremmest have styr på de traditionelle sikkerhedstiltag såsom stærke adgangskoder, risikoanalyse mfl.[15].

Desuden har hele 15 pct. af de virksomheder, som arbejder med én af de tre teknologier, *ikke* implementeret selv de to basale sikkerhedstiltag (opdatering af styresystemer og backup af data) på trods af at virksomheder, der fx arbejder med big data ved brug af kunstig intelligens er i besiddelse af store digitale datamængder, som kan give flere angrebsflader, nye angrebstyper og større konsekvenser ved angreb[16]. Virksomhedernes risiko taget i betragtning ligger der således et fortsat potentiale for at løfte den digitale sikkerhed i denne gruppe af SMV'er, hvor interessen fra hackerne kan være særlig høj.

Figur 10. Brug af digitale teknologier og it-sikkerhedsforanstaltninger, 2019



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

Foruden de to basale it-sikkerhedstiltag er det særligt vigtigt for virksomheder, der arbejder med digitale teknologier, at gennemføre en risikovurdering inden anskaffelse af teknologien for at vurdere, om løsningen (enheden, programmet, systemer osv.) lever op til virksomhedens

[15] Se fx: Boston Consulting Group (2020): Analyse af kunstig intelligens i et sikkerhedsperspektiv og Alexandra Instituttet (2020): Kan dit IoT produkt hackes

[16] Boston Consulting Group (2019): Analyse af kunstig intelligens i et sikkerhedsperspektiv

sikkerhedsmæssige krav. Det kan fx være krav til fortrolighed, beskyttelse mod uautoriseret adgang eller backup. Efter anskaffelse er det ligeledes vigtigt at gennemføre løbende risikovurderinger for at se, om den anskaffede løsning faktisk leverer den sikkerhed, som virksomheden efterspørger. På trods af dette er det blot 62 pct. af SMV'erne, der arbejder med cloud, IoT eller bigdata, som løbende gennemfører en risikoanalyse. Som beskrevet i afsnit 2, kan virksomheder hente hjælp til at foretage en risikovurdering ved hjælp af Erhvervsstyrelsen **risikovurderingsværktøj**.

Desuden er det særligt vigtigt for virksomheder, der arbejder med digitale teknologier, at stille krav til deres leverandør om sikkerheden i produkterne, hvad enten det drejer sig om systemer/produkter inden for IoT, big data analyse, cloud mv., da ansvaret i sidste ende vil ligge i virksomheden. Man bør i den forbindelse sikre, at sikkerhedsroller og ansvar er tydeligt mellem virksomheden og leverandøren. Men også her er der rum til forbedring eftersom 11 pct. af de SMV'er, der arbejder med én af de tre teknologier, ikke stiller minimum ét krav til deres leverandør om fx behandling af data, brug af it-sikkerhedsforanstaltninger og/eller løbende dokumentation af it-sikkerheden.

3.3 Guides til sikker brug af digitale teknologier i virksomheder

Erhvervsstyrelsen har i foråret 2021 lanceret en ny temasektion på **Sikkerdigital.dk 'Sikkerhed i digitale teknologier'** der består af guides til virksomheder, som arbejder med forskellige digitale teknologer. I skrivende stund findes følgende tre guides:

Tabel 3. Guides til sikker brug af digitale teknologier

IoT: Beskyt virksomhedens internetforbundne enheder	Sikker brug af cloud-løsninger i virksomheden	Sikker brug af kunstig intelligens
Dette er en online IoT-tjekliste med 16 punkter, der guider virksomheder til køb og sikker brug af IoT-produkter. Der er også en tilhørende artikel, der beskriver de vigtigste råd. Tjeklisten henvender sig både til virksomheder, der anvender IoT og til virksomheder, som skal til at købe IoT-produkter.	Dette er en online guide med seks trin, der kan hjælpe virksomheder med at være opmærksom på it-sikkerhed ved køb og brug af cloud-baserede tjenester. Guiden kan bl.a. bruges til cloud-tjenester som samarbejdsværktøjer og dokumenthåndtering (f.eks. Microsoft 365) eller fildelingsværktøjer (f.eks. Dropbox). Der er også en tilhørende artikel, der forklarer de seks trin.	Denne vejledning sætter fokus på, hvordan man som virksomhed selv kan styrke sikkerheden ved brug af kunstig intelligens og indeholder 16 konkrete tiltag. Vejledningen er baseret på en analyse af kunstig intelligens i et sikkerhedsperspektiv. Vejledningen såvel som analysen er gennemført af BCG for ERST og DIGST.
Link til IoT-artikel **Link til IoT-tjekliste**	**Link til cloud-artikel** **Link til trin-for-trin-guide**	**Link til analyse** **Link til vejledning**

4. Sammenhæng mellem it-kompetencer og digital sikkerhed

Mangel på kompetencer er en stor udfordring for SMV'erne ift. at løfte deres digitale sikkerhed[17]. Dette afsnit vil derfor belyse forholdet mellem varetagelse af it-sikkerhedsmæssige opgaver i de danske SMV'er sammenholdt med deres brug af digitale sikkerhedstiltag.

4.1 Ca. 2/3 dele af SMV'erne udliciterer hele eller dele af deres it-sikkerhed

VITA-undersøgelsen fra 2020 viser, at 68 pct. af SMV'erne udliciterede hele eller dele af deres it-sikkerhed til en ekstern leverandør i 2019, hvilket er samme niveau som i 2018. Denne andel er også nogenlunde ens på tværs af virksomhedsstørrelse, som vist i *figur 11*.

Det kan være mange fordele ved at udlicitere sin it-sikkerhed. Fx hvis man er en mindre virksomhed, som ikke har behov for eller ressourcer til at ansætte en it-sikkerhedsansvarlig/it-afdeling. Men selvom man vælger at udlicitere hele eller dele af sin it, er det fortsat vigtigt, at man som virksomhed forholder sig til og tager ansvar for sin digitale sikkerhed blandt andet ved at stille krav til sin leverandør. Det gælder fx krav om databehandling, backup og andre grundlæggende sikkerhedsforanstaltninger. På trods af dette har kun 89 pct. af de SMV'er, som udliciterer deres digitale sikkerhed, stillet krav til deres leverandør om enten behandling af data, it-sikkerhedsforanstaltninger og/eller løbende dokumentation om fx it-sikkerhedsforanstaltninger[18]. Det betyder, at 11 pct. af virksomhederne *ikke* har stillet minimum ét af de tre krav til sin leverandør.

På **sikkerdigital.dk/virksomhed** kan virksomheder downloade et dialogværktøj, der indeholder et skema med konkrete spørgsmål til it-leverandøren. Virksomheder kan sende skemaet til sin it-leverandør og bede dem besvare spørgsmålene for at få et overblik over leverandørens digitale sikkerhed i løsningerne, som virksomheden benytter sig af.

4.2 Større virksomheder benytter i højere grad egne ansatte til at varetage it-sikkerhedsmæssige aktiviteter

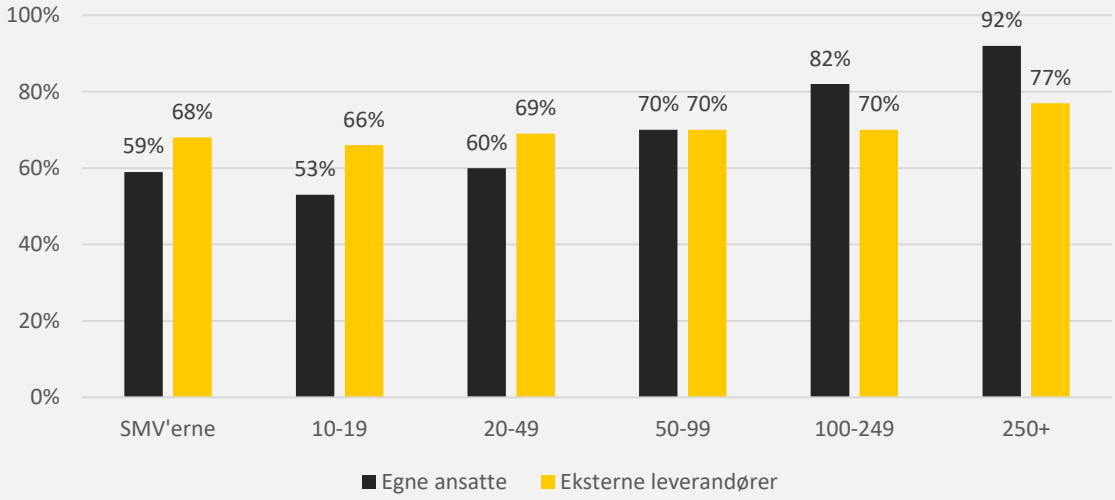
59 pct. af SMV'erne fik varetaget it-sikkerhedsmæssige aktiviteter af egne medarbejdere i 2019, hvilket ligeledes er på niveau med 2018. Dette spørgsmål er bredt formuleret og kan både tælle medarbejdere, der er ansat som it-sikkerhedsspecialister, men også ansatte, som varetager de it-sikkerhedsmæssige opgaver ved siden af andre arbejdsopgaver. Hvad angår virksomheder, der udliciterer sin digitale sikkerhed, er der betydelig forskel på virksomhedens størrelse. Fx har 53 pct. egne medarbejdere til at varetage it-sikkerhedsmæssige opgaver blandt virksomheder med 10-19 ansatte, mens det gælder hele 82 pct. blandt virksomheder med 100-249 ansatte. Til sammenligning har langt de fleste store virksomheder (92 pct.) egne ansatte til at udføre it-sikkerhedsmæssige opgaver.

[17] Højbjerre Brauer Schultz (2019): Arbejdsmarkedet for informationssikkerhedskompetencer i Danmark
[18] Blandt SMV'er, der udliciterer deres it-sikkerhed, stiller 76 pct. krav om behandling af data, 76 pct. stiller krav om it-sikkerhedsforanstaltninger og 60 pct. stiller krav om løbende dokumentation (89 pct. stiller minimum ét ud af de tre krav)

Som *figur 11* illustrerer, benytter størstedelen af virksomheder med op til 49 medarbejdere *eksterne* leverandører til at varetage it-sikkerhedsmæssige aktiviteter, hvorimod størstedelen af virksomheder med 100 ansatte eller derover i anvender *egne* medarbejdere til at varetage it-sikkerhedsmæssige aktiviteter.

Tal fra Eurostat viser, at Danmark er ét af de lande i EU (kun overgået af Finland), hvor it-sikkerheds-mæssige opgaver oftest varetages af SMV'ernes egne ansatte. Derimod ligger Danmark på en 6. plads, når det kommer til andelen af SMV'er, der udliciterer it-sikkerhedsmæssige opgaver[19].

Figur 11. Udførelse af it-sikkerhedsmæssige opgaver opdelt på størrelse, 2019



Note: Tallene summerer ikke til 100 pct., da nogle virksomheder både benytter egne ansatte og eksterne leverandører til udførelse af it-sikkerhedsmæssige aktiviteter.
Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2020).

4.3 Lav digital sikkerhed blandt SMV'er, der hverken har egne ansatte eller eksterne leverandører til at varetage it-sikkerhedsmæssige opgaver

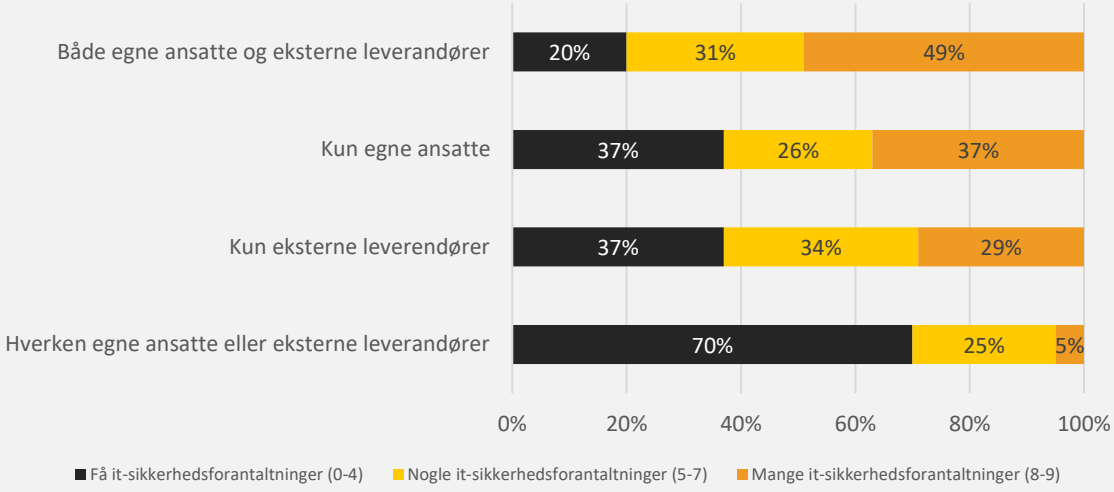
Samlet set har 32 pct. af SMV'erne *både* egne ansatte og eksterne leverandører til at varetage it-sikkerhedsaktiviteter, 36 pct. har *kun* eksterne leverandører og 27 pct. har *kun* egne ansatte til at varetage it-sikkerhedsaktiviteter, mens 5 pct. *hverken* har egne ansatte eller eksterne leverandører ansat til at varetage it-sikkerhedsaktiviteter.

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

[19] Denne sammenligning mellem EU-landene beror på data indsamlet i 2019, som afspejler situationen i 2018, og er ikke tilgængelig for data indsamlet i 2020. Kilde: https://ec.europa.eu/eurostat/databrowser/view/isoc_cisce_ra/default/table?lang=en

sikkerhedsforanstaltninger end øvrige virksomheder, jf. *figur 12*[20]. Der er midlertidig ikke signifikant forskel på virksomhedernes brug af it-sikkerhedsforanstaltninger alt efter om det er egne ansatte eller eksterne leverandører, som varetager de it-sikkerhedsmæssige aktiviteter.

Figur 12. Udførelse af it-sikkerhedsmæssige aktiviteter og brug af it-sikkerhedsforanstaltninger, 2019

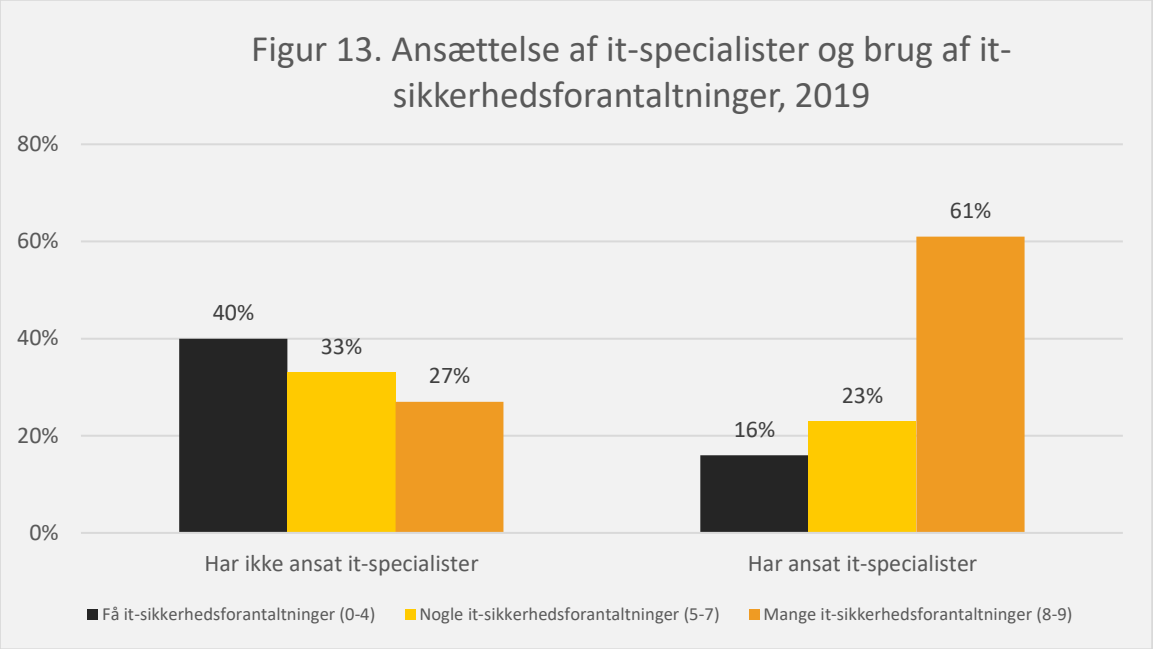


Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2020).

4.4 Højere digital sikkerhed blandt SMV'er, der beskæftiger it-specialister

Figur 13 viser, at SMV'er, der har ansat én eller flere it-specialister, bruger flere it-sikkerhedsforanstaltninger end virksomheder, der ikke beskæftiger it-specialister. Denne forskel er statistisk signifikant kontrolleret for virksomhedsstørrelse og branche. Ser man på de to essentielle sikkerhedstiltag (systematisk opdatering og backup af data) har hele 87 pct. af virksomhederne, som har it-specialister ansat, implementeret disse, hvilket gælder 72 pct. af de virksomheder, der ikke har ansat specialister.

[20] Der findes signifikant forskel på tværs af virksomhedsstørrelse og branche. Sammenhængen skyldes således ikke blot, at flere store virksomheder både har egne ansatte og eksterne leverandører og et højere digitalt sikkerhedsniveau.



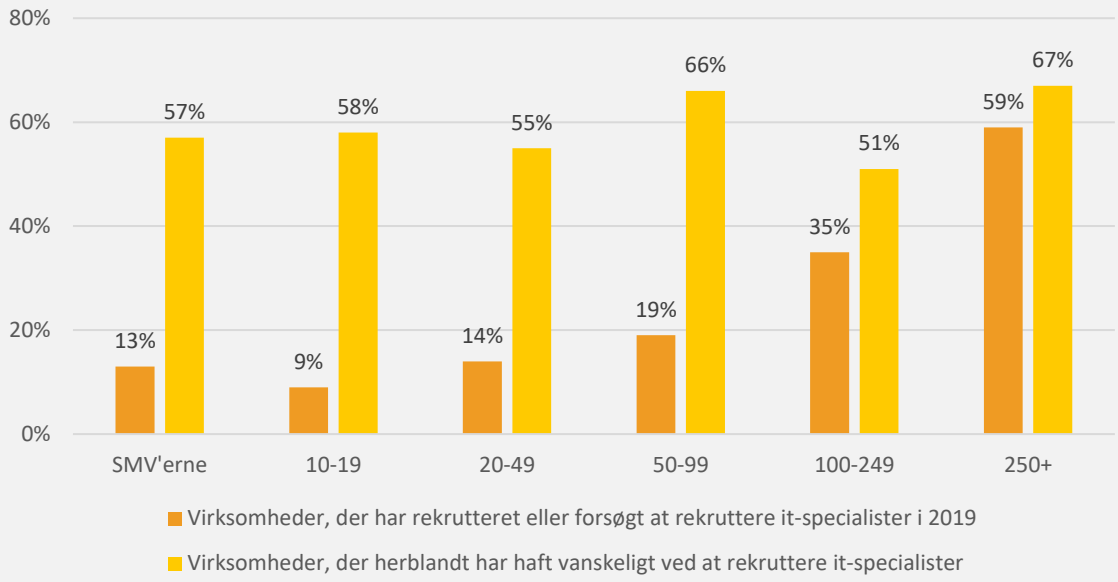
Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2020).

4.5 Svært at rekruttere it-specialister på tværs af virksomhedsstørrelse

It-kompetencer spiller således en nøglerolle i forhold til at styrke den digitale sikkerhed blandt de danske SMV'er. Men desværre er det i disse år ikke nemt at rekruttere disse it-specialister. Som *figur 14* viser, har 13 pct. af SMV'erne rekrutteret eller forsøgt at rekruttere it-specialister i 2019. Heriblandt har hele 57 pct. haft vanskeligt herved. Både andelen af SMV'er, der har rekrutteret eller forsøgt at rekruttere it-specialister såvel som andelen af virksomheder, der har haft problemer herved, er på niveau med i 2018.

Som figur 14 også viser, stiger andelen af virksomheder, der har rekrutteret eller forsøgt at rekruttere it-specialister med virksomhedsstørrelse. Fx har 9 pct. af SMV'er med 10-19 ansatte rekrutteret/forsøgt at rekruttere it-specialister, hvilket gælder 35 pct. blandt SMV'er med 100-249 ansatte (og 59 pct. blandt de store virksomheder med 250+ ansatte). Blandt den andel af virksomheder, som har forsøgt at rekruttere it-specialister, opleves udfordringer med at rekruttere specialisterne dog stort set i samme omfang blandt alle virksomhedsstørrelser.

Figur 14: Rekruttering af it-specialister og udfordringer herved



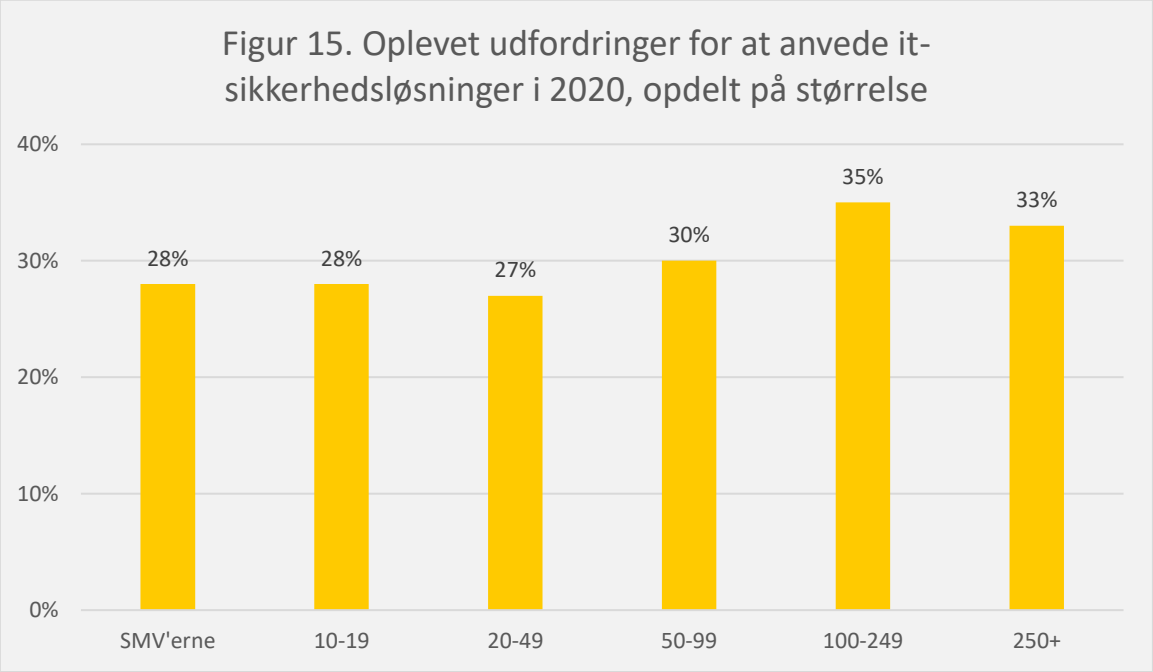
Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2020).
Note: Andelen af virksomheder, der har haft vanskeligt ved at rekruttere specialister er udelukkende beregnet blandt virksomheder, der har rekrutteret eller forsøgt at rekruttere it-specialister.

5. Oplevede barrierer ved implementering af it-sikkerhedsløsninger

28 pct. af SMV'erne angiver samlet set, at de har været forhindret i, begrænset af eller oplevet udfordringer for at anvende it-sikkerhedsløsninger i 2019, som vist i *figur 15*. Som det ligeledes fremgår af figuren, er der ikke stor forskel på virksomhedsstørrelse og andelen af virksomheder, der oplever udfordringer for at anvende it-sikkerhedsløsninger.

Andelen af virksomheder, der oplever udfordringer for anvendelse af it-sikkerhedsløsninger i 2019, er markant højere end i 2018, hvor blot 7 pct. af SMV'erne angav, at de havde oplevet udfordringer for at anvende it-sikkerhedsforanstaltninger. Resultaterne kan dog ikke sammenlignes direkte pga. ændret spørgsmålsformulering mellem de to år[21].

[21] I VITA 2019 blev virksomhederne først spurgt til, om de havde oplevet udfordringer for at anvende it-sikkerhedsløsninger (ja/nej), før de blev præsenteret for eksempler på udfordringer. I VITA 2020 blev virksomhederne spurgt til. om de have oplevet nogle af de listede udfordringer (manglende it-kendskab og kompetencer, manglende økonomi osv.).

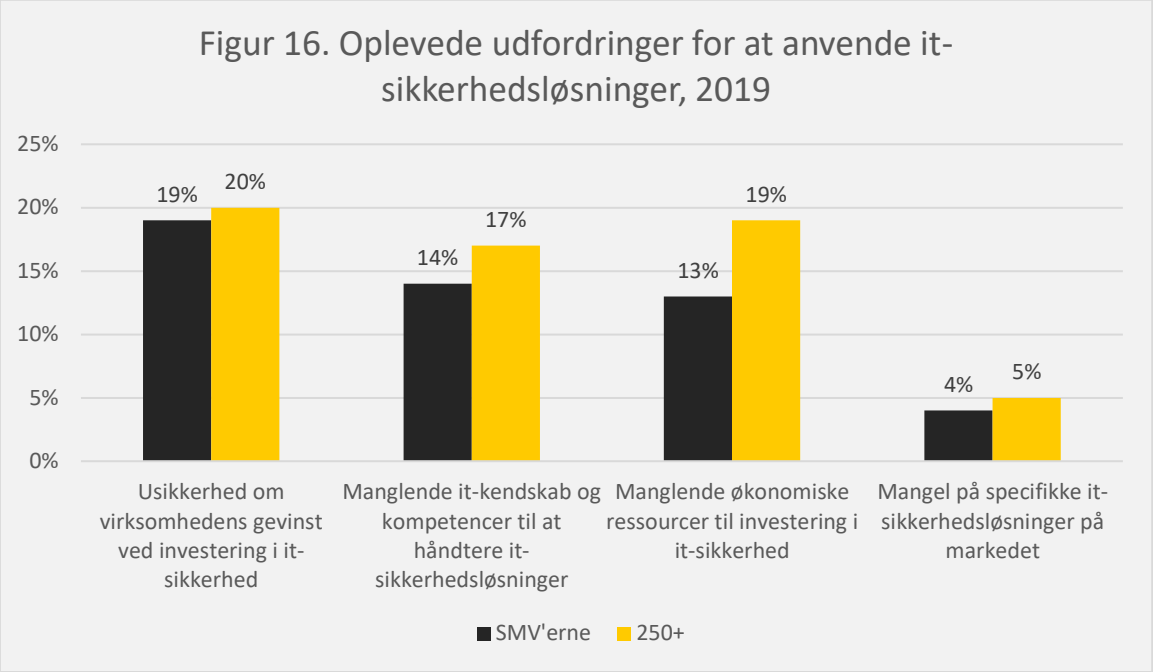


Kilde: Egne beregninger baseret på data indsamlet af Epinion i 2020.

5.1 Usikkerheden om gevinsten ved investeringer i digital sikkerhed opleves som den største barriere

Figur 16 viser, hvilke væsentlige forhindringer, begrænsninger eller udfordringer, virksomhederne typisk oplever for at anvende it-sikkerhedsløsninger. Blandt SMV'erne såvel som de store virksomheder opleves 'usikkerheden om gevinsten ved at investere i digital sikkerhed' som den største udfordring/barriere. Herefter følger en udfordring med 'manglende it-kendskab og kompetencer til at håndtere it-sikkerhedsløsninger', hvilket understøtter resultaterne i afsnit 4 om, at virksomhedernes digitale sikkerhed i høj grad afhænger af de rette kompetencer. Endelig opleves 'manglende økonomiske ressourcer' også som en væsentlig barriere for at anvende it-sikkerhedsløsninger. Virksomhederne oplever kun i mindre grad 'mangel på specifikke it-sikkerhedsløsninger i markedet' som en udfordring for at anvende it-sikkerhedsløsninger.

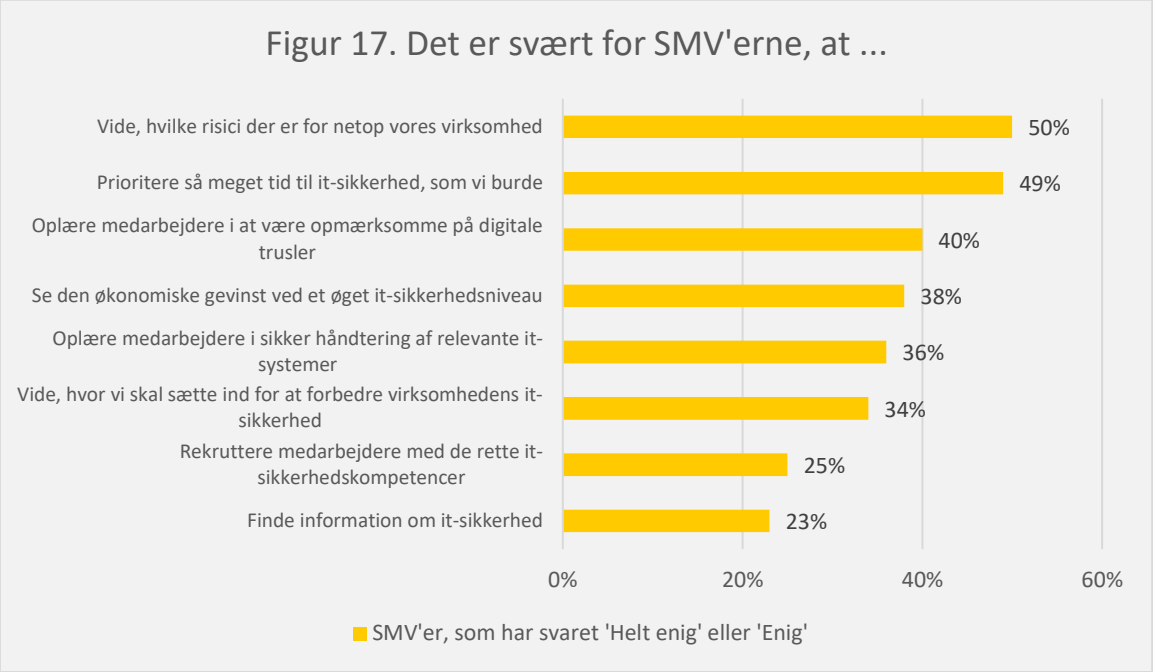
Overordnet set peger resultaterne fra VITA-undersøgelsen således på, at SMV'erne især mangler incitament til at investere i og arbejde med digital sikkerhed frem for specifikke it-sikkerhedsløsninger. Hertil skal dog bemærkes, at de udvalgte kategorier i *figur 16* ikke nødvendigvis er udtømmende, og at det ikke har været muligt for virksomhederne at svare 'andet'. Der kan således være andre væsentlige barrierer, som denne analyse ikke har med.



Note: Tallene summerer ikke til 100 pct., da virksomheden har kunne angive ingen eller flere svarmuligheder.
Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2020).

I Epinion-undersøgelsen spørges SMV'erne ligeledes ind til, hvad de har svært ved i forhold til deres behov for digital sikkerhed. Hertil svarer halvdelen af SMV'erne (50 pct.), at det er svært for dem at vurdere de konkrete risici for netop deres virksomhed. Mange danske SMV'er er desuden 'helt enige' eller 'enige' i, at de har svært ved at prioritere nok tid til digital sikkerhed (49 pct.) samt at oplære deres medarbejdere i at være opmærksom på digitale trusler (40 pct.).

Resultaterne indikerer, at det skal være nemt for virksomhederne at finde frem til og implementere sikkerhedsløsninger, og at de har behov for, at nogen tager dem i hånden og lærer dem og deres medarbejdere, hvad de skal gøre.

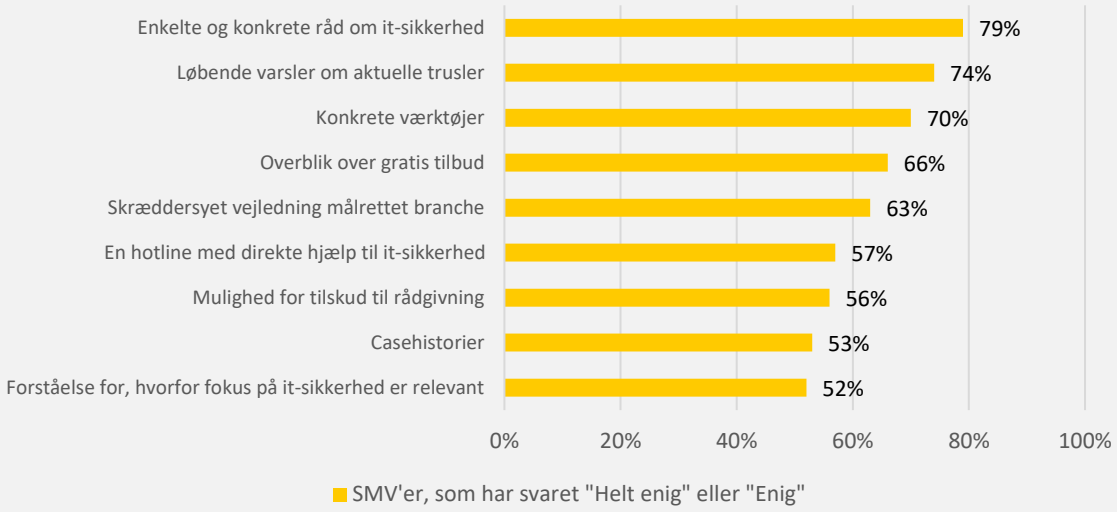


Note: De øvrige svarkategorier er "hverken enig eller uenig", "uenig" og "helt uenig". Svarkategorien "ikke relevant" er frasorteret og indgår ikke i opgørelsen.
Kilde: Egne beregninger baseret på data indsamlet af Epinion i 2020.

5.2 Enkle og konkrete råd vil øge SMV'ernes fokus på digital sikkerhed

I Epinion-undersøgelsen spørges der også ind til hvilke tiltag, der vil øge SMV'ernes fokus på digital sikkerhed. Øverst på listen findes 'enkle og konkrete råd om it-sikkerhed', som hele 79 pct. af SMV'erne enten er 'enige' eller 'helt enige' i kan bidrage til at styrke deres fokus på digital sikkerhed. Men også 'løbende varsler om aktuelle trusler' (74 pct.) og 'konkrete værktøjer' (70 pct.) topper listen af tiltag, der kan øge SMV'ernes fokus på området. Der spørges dog ikke nærmere ind til, hvilke konkrete råd, varsler og værktøjer, som virksomhederne efterspørger.

Figur 18. Tiltag der vil øge SMV'ernes fokus på digital sikkerhed, 2020



Note: De øvrige svarkategorier er "hverken enig eller uenig", "uenig" og "helt uenig". Svarkategorien "ikke relevant" er frasorteret og indgår ikke i opgørelsen. *Kilde:* Egne beregninger baseret på data indsamlet af Epinion i 2020.

For virksomheder der efterspørger konkrete råd, værktøjer og et overblik over gratis tilbud er der hjælp at hente på **Sikkerdigital.dk/virksomhed**, som kort uddybet i nedenstående boks.

Tabel 4. Overblik over udvalgte tilbud til virksomheder på Sikkerdigital.dk

Syv gode råd	Test og værktøjer	Overblik over gratis tilbud
På Sikkerdigital.dk har Erhvervsstyrelsen udarbejdet syv basale råd om it-sikkerhed, som er et godt sted at starte for virksomheder, der ønsker at styrke sikkerheden **Læs de syv råd her**	På Sikkerdigital.dk findes en række gratis online testværktøjer, som kan styrke it-sikkerheden og persondatahåndtering. **Se test og værktøjer her**	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). **Se de gratis tilbud her**

6. It-sikkerhedshændelser i danske SMV'er

Flere og flere virksomheder rammes af cyberangreb. I deres årlige trusselsvurderinger fra 2021 beskriver Center for Cybersikkerhed blandt andet en stigende trussel fra målrettede ransomware-angreb mod danske virksomheder[22]. Disse simple angreb er en trussel mod alle virksomheder, også de små.

[22] Center for Cybersikkehed (2021): Cybertruslen med Danmark 2021

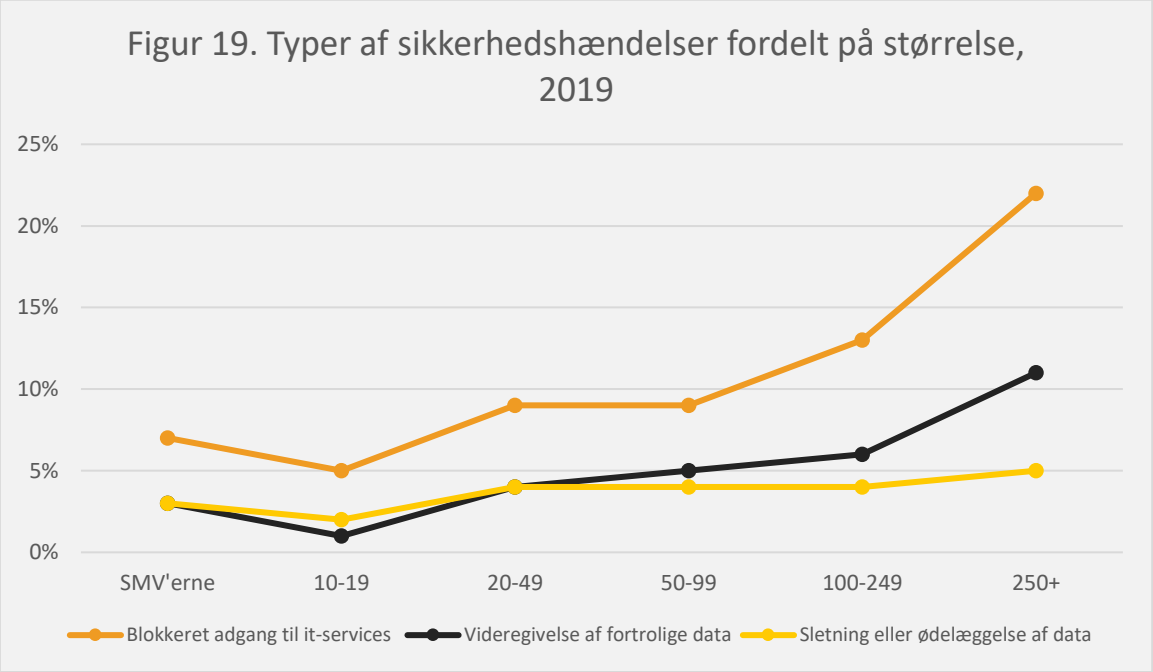
På baggrund af en undersøgelse blandt deres medlemmer er Dansk Erhverv kommet frem til, at danske virksomheder oplever omkostninger i intervallet 10.000-100.000 kr. ved et cyberangreb, og at cyberangreb samlet set kostede danske virksomheder (minimum) 4 mia. kr. i 2018[23]. Cyberangreb kan således have stor betydning for såvel de enkelte virksomheders bundlinje og for samfundsøkonomien som helhed.

I VITA-undersøgelsen har 10 pct. af SMV'erne angivet, at de har oplevet en it-sikkerhedshændelse i løbet af 2019, hvilket er på samme niveau som i 2018. Til sammenligning har 32 pct. af de store virksomheder med 250+ ansatte oplevet en it-sikkerhedshændelse. Disse estimater må dog anses som konservative resultater, da it-sikkerhedshændelser ofte er behæftet med væsentlige "mørketal". Det skyldes blandt andet, at virksomheder ikke er forpligtet til at indrapportere alle typer af it-sikkerhedshændelser, og at mange virksomheder ikke ønsker at dele, hvis de bliver ramt af en hændelse, da de frygter, at det kan skade deres omdømme over for kunder, leverandører og samarbejdspartnere. Desuden kan der være virksomheder, som slet ikke ved, at de har været udsat for en hændelse (fx hvis der fx er tale om spyware, der ligger gemt i virksomhedens systemer). Hverken Erhvervsstyrelsen eller andre myndigheder har således det fulde overblik over antallet af angreb mod danske virksomheder. Derfor er det også mere interessant at se på hvilke virksomheder, som rammes af it-sikkerhedshændelser samt hvilke hændelser, som de rammes af.

6.1 'Blokeret adgang til it-service' er den hyppigste it-sikkerhedshændelse på tværs af virksomhedsstørrelse

Figur 19 viser hvilke sikkerhedshændelser, virksomhederne har oplevet i 2019. På tværs af virksomhedsstørrelse oplevede størstedelen af virksomhederne blokeret adgang til it-service (fx Denial of Service-angreb, ransomware-angreb, hardware- eller softwarefejl). Sammenlignet med SMV'erne oplevede de store virksomheder i højere grad 'videregivelse af fortrolige data, fx på grund af uautoriseret indtrængen, pharming, phishing-angreb eller handlinger fra ansatte'. Eftersom store virksomheder i sagens natur har flere ansatte, der kan 'lokkes' til at trykke på et forkert link eller komme til at videregive deres adgangskode, er dette resultat ikke overraskende og bekræfter blot, at det er vigtigt med en vedvarende medarbejder-awareness træning for at styrke virksomhedens digitale forsvar.

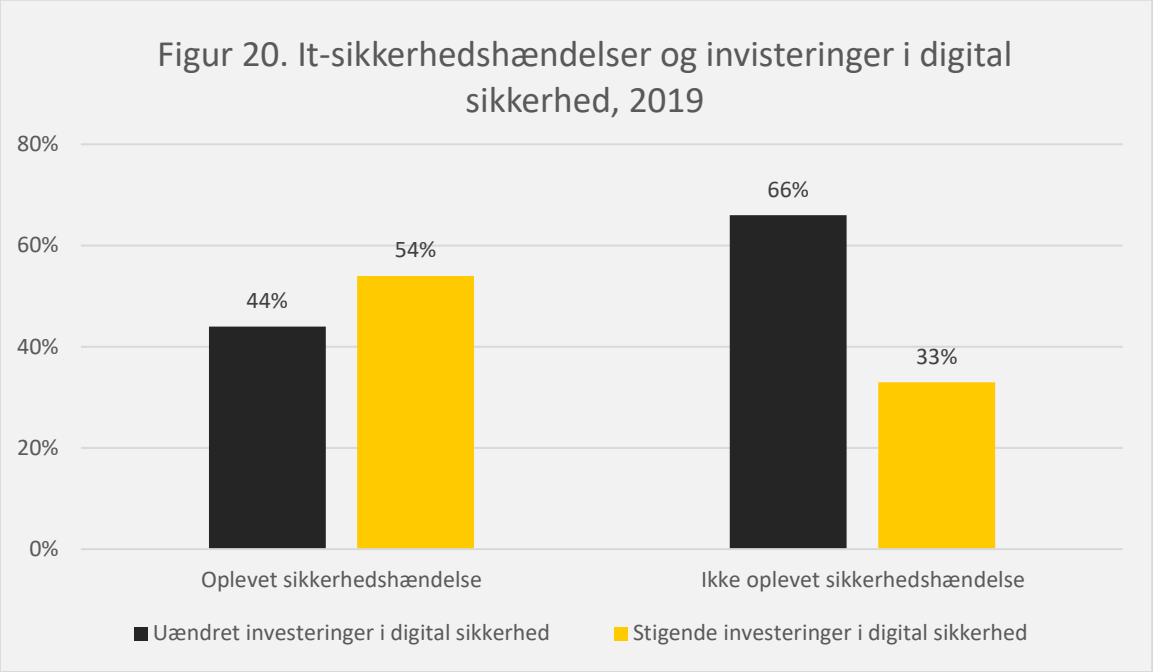
[23] Dansk Erhverv (2019): Er Danmark klar til "Giganternes tid"?



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

6.2 SMV'er der oplever it-sikkerhedshændelser, investerer mere i digital sikkerhed og finder det mere sandsynligt, at de rammes igen

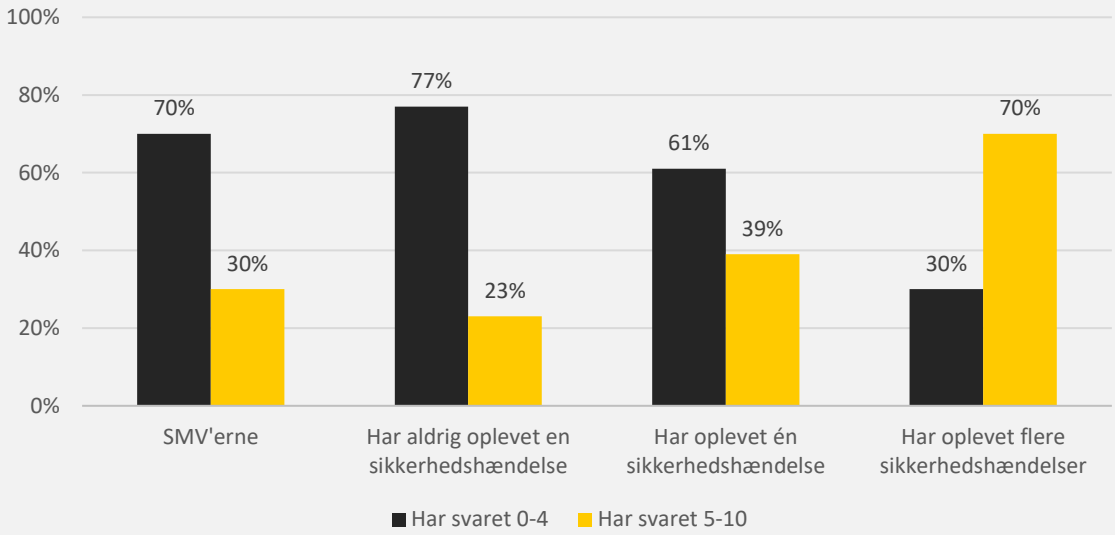
De SMV'er, som har oplevet en it-sikkerhedshændelse i 2019, har også investeret mere i digital sikkerhed i samme år, som illustreret i nedenstående *figur 20*. Denne sammenhæng er signifikant og gælder på tværs af virksomhedsstørrelse/branche. Det tyder således på, at virksomheder skal mærke de negative konsekvenser ved en it-sikkerhedshændelse, før digital sikkerhed prioriteres. Der ligger således fortsat et arbejde i at få virksomhedernes øjnene op for eventuelle konsekvenser ved angreb, så de får implementeret forebyggende tiltag, før skaden er sket.



Note: Tallene summerer ikke til 100 pct. da en lille andel af virksomhederne havde faldende udgifter.
Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2020).

Resultater fra Epinion-undersøgelsen peger ligeledes på, at de SMV'er, som allerede har oplevet én eller flere sikkerhedshændelser, i højere grad frygter, at deres virksomhed vil rammes igen. Dette fremgår af *figur 21,* som viser virksomhedernes selvvurderede sandsynlighed for at blive ramt af en sikkerhedshændelse på en skala fra 0-10. For SMV-gruppen samlet set er det hele 70 pct., som vurderer sandsynligheden for at blive ramt af en sikkerhedshændelse som 0-4 og 30 pct. som vurderer sandsynligheden for at blive ramt som 5-10. Omvendt ser det ud for de SMV'er, som allerede har oplevet flere sikkerhedshændelser, hvor 70 pct. vurderer sandsynligheden som 5 eller derover og 30 pct. vurderer sandsynligheden som 4 eller derunder.

Figur 21. Selvvurderet sandsynlighed for at virksomheden rammes af en sikkerhedshændelse på en skala fra 0-10, 2020

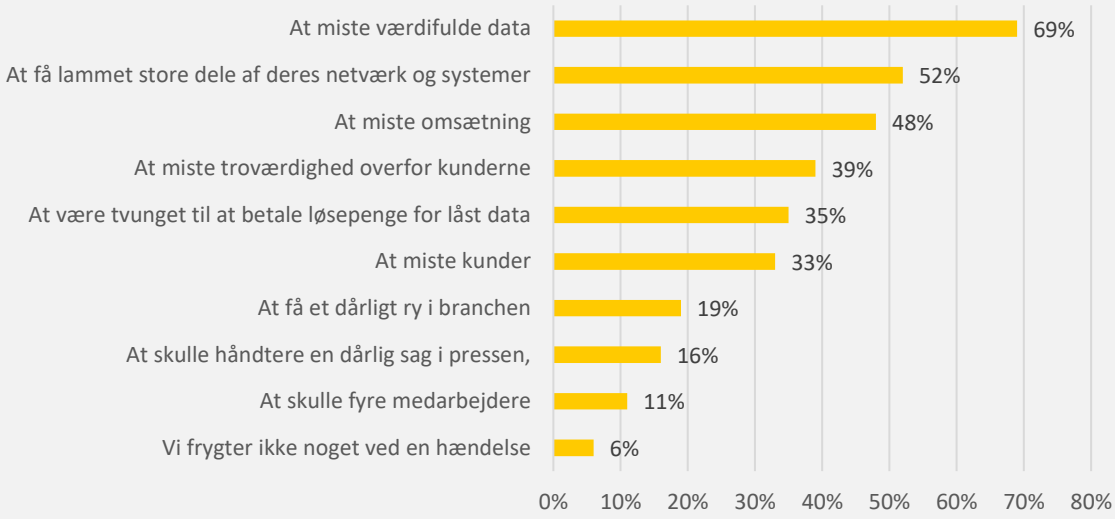


Kilde: Egne beregninger baseret på data indsamlet af Epinion i 2020.

6.3 Virksomheder frygter især at miste værdifulde data ved en sikkerhedshændelse

I Epinion-undersøgelsen svarer SMV'erne endvidere på, hvad de frygter ved en sikkerhedshændelse. Resultaterne fremgår af *figur 22* og viser, at størstedelen af SMV'erne frygter de kortsigtede, direkte konsekvenser ved en sikkerhedshændelse; herunder at miste værdifulde data (69 pct.), at få lammet deres netværk og systemer (52 pct.) og/eller at miste omsætning (48 pct.). Men også en relativt stor del af SMV'erne frygter de mere langsigtede, indirekte konsekvenser såsom at miste troværdighed overfor deres kunder (39 pct.), at få et dårligt ry i branchen (19 pct.) og/eller en dårlig sag i pressen (16 pct.). Dermed kan man med fordel appellere til både direkte og indirekte konsekvenser, hvis man skal gøre SMV'erne opmærksomme på eventuelle konsekvenser ved cyberangreb i fx awareness- eller casekampagner.

Figur 22. Hvad frygter virksomheden ved en sikkerhedshændelse? 2020



Kilde: Egne beregninger baseret på data indsamlet af Epinion i 2020

6.4 62 pct. af de danske SMV'er har tegnet en forsikring i forhold til it-sikkerhedshændelser

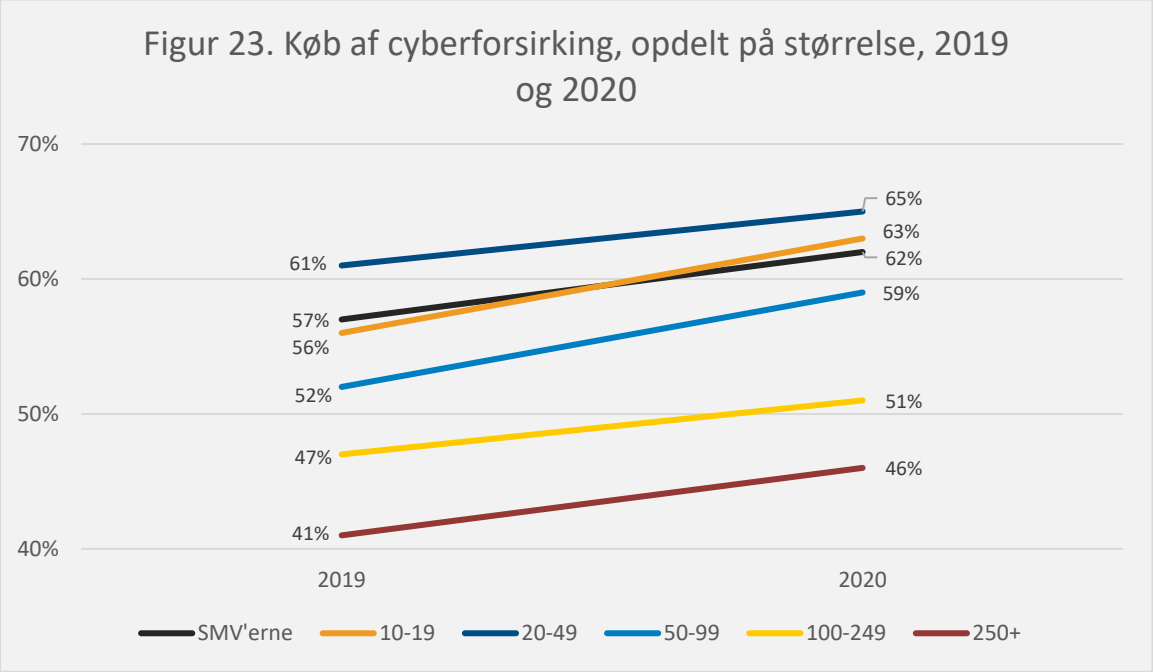
62 pct. af de danske SMV'erne har angivet, at de har tegnet en forsikring i forhold til it-sikkerhedshændelser. Data fra Eurostat baseret på VITA-undersøgelsen i 2019 viser desuden, at Danmark er det land i EU med den største andel af virksomheder, som har tegnet en forsikring i forhold til it-sikkerhedshændelser. Danmark er også det eneste land i EU, hvor en større andel blandt SMV'er end store virksomheder har tegnet en forsikring i forhold til it-sikkerhedshændelser[24]. At en så stor andel af SMV'erne har angivet, at de har tegnet en forsikring i forhold til it-sikkerhedshændelser kan dog skyldes, at det kan være svært for virksomhederne at skelne mellem forskellige forsikringsprodukter, og hvad de dækker. Det gælder især ift. cyberforsikringer, netbanksforsikringer og kriminalitetsforsikringer[25]. Der kan således være nogle virksomheder, som tror, de er dækket i forhold til it-sikkerhedshændelser uden at være det.

Figur 23 viser andelen af virksomheder, der har tegnet en forsikring i forhold til it-sikkerhedshændelser i hhv. 2019 og 2020 opdelt på virksomhedsstørrelse. For det første viser figuren, at det særligt er de mindre virksomheder med op til 50 ansatte, som har valgt at tegne en forsikring. For det andet viser figuren en relativt høj udvikling i køb af forsikringer, der dækker it-sikkerhedshændelser fra 2019 til 2020 blandt alle virksomhedsstørrelser. Dette er positivt, da it-sikkerhedshændelser, som beskrevet i afsnit 6, kan være meget omkostningsfulde for den enkelte virksomhed. Derudover skal virksomheder leve op til en række it-sikkerhedsforanstaltninger for at kunne tegne en cyberforsikring, herunder de to basale tiltag med at tage backup af data og opdatere virksomhedens programmer

[24] OBS. Denne sammenligning mellem EU-landene beror på data indsamlet i 2019, som afspejler situationen i 2018, og er ikke tilgængelig for data indsamlet i 2020. Kilde: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_security_in_enterprises#Problems_due_to_ICT_related_security_incidents

[25] Rådet for Digital Sikkerhed, DI og Forsikring og Pension (2020): Vejledning til SMV'er om cyberforsikringer

og styresystemer[26]. Cyberforsikringer kan således også have en forebyggende effekt ved at foranledige at virksomheder får implementere basale sikkerhedstiltag.

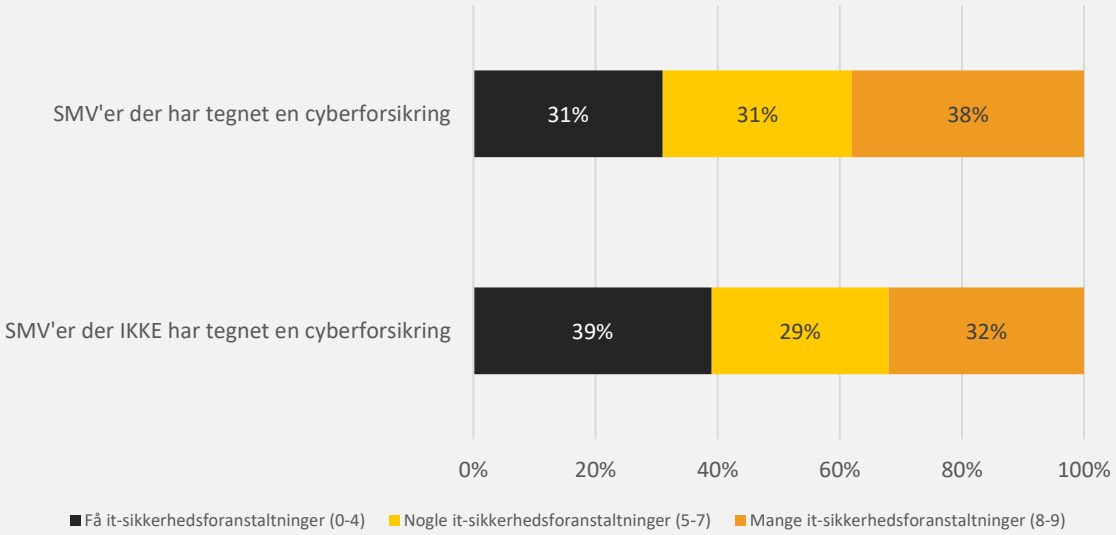


Kilde: Egne beregninger baseret på tal fra Danmarks Statistik (VITA-undersøgelsen 2020).

Figur 24 viser i forlængelse af ovenstående, at de SMV'er, som har tegnet en cyberforsikring, også har implementeret flere it-sikkerhedsforanstaltninger sammenlignet med de SMV'er, som ikke har tegnet en forsikring. Denne forskel er signifikant kontrolleret for virksomhedsstørrelse og branche. Det er dog ikke muligt at undersøge, om denne sammenhæng skyldes, at virksomhederne øger deres digitale sikkerhed for at leve op til de krav, der er for at tegne en forsikring, eller om det skyldes, at virksomheder med fokus på digital sikkerhed er mere tilbøjelige til at tegne cyberforsikringer (eller en kombination heraf).

[26] Rådet for Digital Sikkerhed, DI og Forsikring og Pension (2020): Vejledning til SMV'er om cyberforsikringer

Figur 24. Køb af cyberforsikring krydset med brug af it-sikkerhedsforanstaltninger



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

7. Sammenhæng mellem SMV'ernes fokus på digital sikkerhed og dataetik

At virksomheder behandler data ansvarligt, er en nødvendighed for at bevare tilliden til digitale løsninger og realisere gevinsterne ved virksomheders stigende digitalisering. Udover at sikre virksomheder bedst muligt mod udefrakommende cyberangreb, indebærer ansvarlig dataanvendelse også et fokus på dataetik, herunder at virksomhederne selv bruger data ansvarligt og ikke deler data uden samtykke.

En analyse om 'Danske virksomheders arbejde med dataetik' gennemført af Rambøll for Erhvervsstyrelsen i 2020 viser, at mange SMV'er har svært ved at skelne mellem områderne 'digital sikkerhed' og 'dataetik'. Ud fra virksomhedsbesvarelserne i analysen er det fx tydeligt, at SMV'erne blander begreber inden for dataetik og digital sikkerhed sammen[27].

Flere steder ses også initiativer, hvor datetik og digital sikkerhed tænkes sammen. Et eksempel er **D-mærket**, som er en dansk kommende mærkningsordning for it-sikkerhed og ansvarlig dataanvendelse, der forventes at blive lanceret i efteråret 2021[28]. Formålet med D-mærket er at tydeliggøre, hvilke virksomheder, der beskytter og behandler data ansvarligt, herunder at gøre sikker og ansvarlig databehandling til et konkurrenceparameter for danske virksomheder. For at opnå D-mærket skal virksomhederne både leve op til en række kriterier inden for it-sikkerhed og ansvarlig dataanvendelse, der passer til deres risikoprofil.

[27] Rambøll for Erhvervsstyrelsen (2020): "Danske virksomheders arbejde med dataetik" *Ikke udgivet*

[28] D-mærket er stiftet af Dansk Industri, Dansk Erhverv, SMVdanmark, samt Forbrugerrådet Tænk og støttes af Erhvervsstyrelsen og finansieres af Industriens fond.

Eftersom VITA-undersøgelsen både indeholder spørgsmål om digital sikkerhed og dataetik, vil dette afsnit se nærmere på, om der findes en positiv sammenhæng mellem SMV'ernes arbejde med digital sikkerhed og dataetik. Indledningsvist gives en kort introduktion til dataetik.

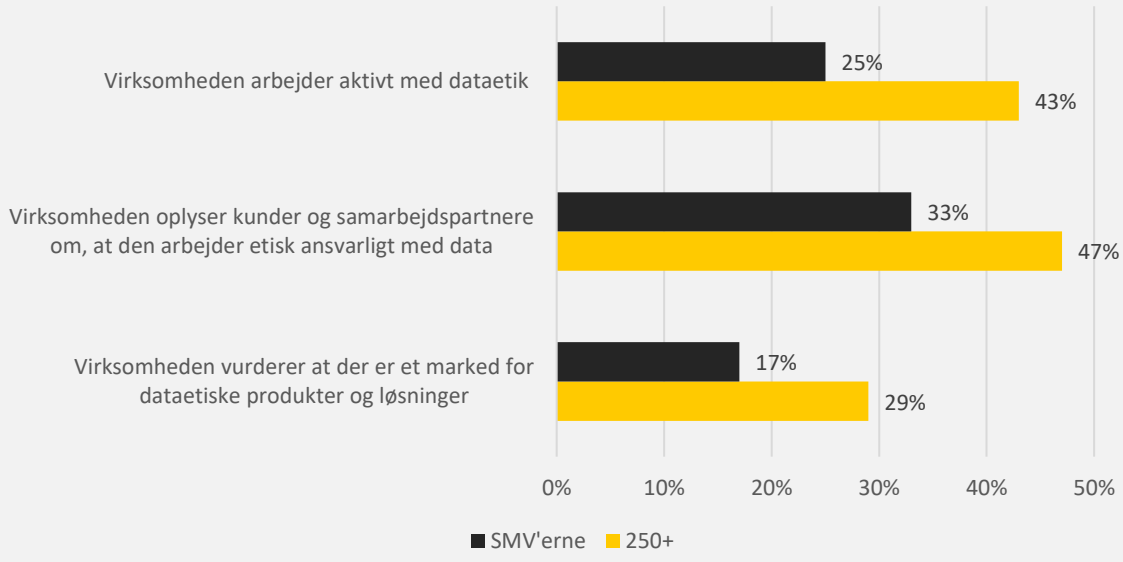
Tekstboks: Kort beskrivelse af dataetik

Dataetik handler om ansvarlig og bæredygtig brug af data i virksomhedens 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 virksomhedens 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.

Bliv klogere på dataetik på Virksomhedsguiden.dk

Figur 25 viser de danske SMV'ers arbejde med dataetik inden for tre konkrete spørgsmål. I lighed med virksomhedernes arbejde med digital sikkerhed, har virksomhedsstørrelse også betydning for arbejdet med dataetik. Fx er der flere store virksomheder med 250+ ansatte end SMV'er, som 1) arbejder aktivt med dataetik, 2) ser et marked for dataetiske produkter og løsninger og 3) oplyser samarbejdspartnere og kunder om deres arbejde med dataetik.

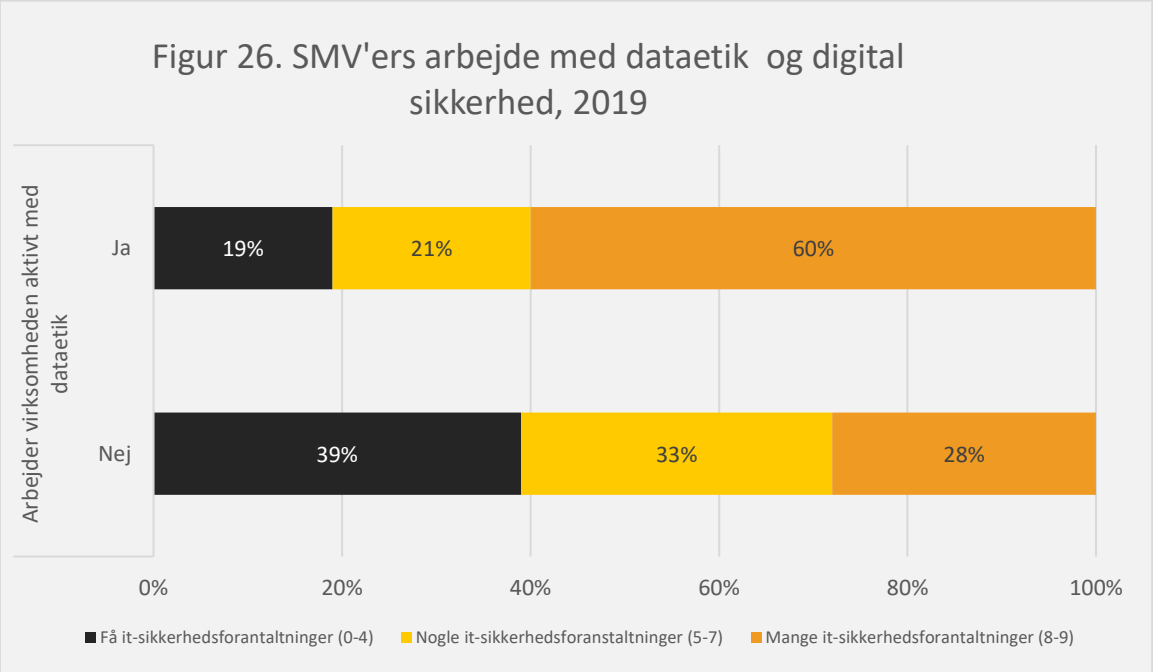
Figur 25. Virksomheders arbejde med dataetik, 2019



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

Figur 26 viser sammenhængen mellem, hvorvidt SMV'erne arbejder aktivt med dataetik eller ej, og hvor mange ud af de 9 anbefalede it-sikkerhedsforanstaltninger, som de anvender. Der ses en tydelig tendens til at de SMV'er, der arbejder aktivt med dataetik, også har implementeret flere it-sikkerhedsforanstaltninger. Fx har 60 pct. af de virksomheder, der arbejder aktivt med dataetik, implementeret 'mange' it-sikkerhedsforanstaltninger, hvilket kun gælder 28 pct. af de virksomheder, der ikke

arbejder med dataetik. Denne forskel er signifikant kontrolleret for størrelse og branche[29]. Det er således plausibelt, at et øget fokus på digital sikkerhed også kan øge virksomhedens fokus på dataetik og vice versa.



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

Sideløbende med indsatsen for at løfte SMV'ernes digitale sikkerhed arbejder Erhvervsstyrelsen også for at understøtte SMV'ernes arbejde med dataetik. Det har blandt andet resulteret i en række værktøjer, der kan understøtte ansvarlig brug af data i virksomheder, som kort beskrevet i *tabel 5*.

Tabel 5. Test og værktøjer til at understøtte virksomheder arbejde med dataetik

Beskyttelse af data	Test din algoritme	Test din algoritme for bias
Brugdata.dk tilbyder en nem adgang til at finde information om reglerne for anvendelse 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 algoritmetesten kan man ved at besvare 6 spørgsmål teste og højne gennemsigtigheden i sit datadrevne system – det gør det nemmere at spore og forklare beslutninger, der tages af systemet. Tag algoritmetesteren her	Med biastesten kan man ved at besvare 6 spørgsmål, teste bias I sit datadrevne system – det gør det nemmere at finde og sætte fokus på eventuelle etiske skævheder i dit datadrevne system. Tag biastesten her

[29] Forskellen er således ikke blot er udtryk for at flere store virksomheder eller specifikke brancher i højere grad fokuserer på begge områder end andre virksomhedsstørrelser og brancher.

Resultaterne i dette afsnit understøtter derfor, at man med fordel kan tænke digital sikkerhed og dataetik sammen i fremadrettede initiativer, der har til formål at øge SMV'ernes samlede fokus på ansvarlig og sikker dataanvendelse.

8. Fokus på digital sikkerhed blandt SMV'ernes ledelse

Det er vigtigt, at ledelsen i de enkelte virksomheder har fokus på deres ansvar for at skabe en digitalt sikker virksomhed. Andre analyser er blandt andet kommet frem til, at ledelsens manglende stillingtagen til digital sikkerhed og medarbejderkulturen i virksomheden kan være barrierer i forhold til at implementere digitale sikkerhedstiltag[30]. Derfor vil dette afsnit se nærmere på ledelsens fokus på digital sikkerhed blandt de danske SMV'er.

I Epinion-undersøgelsen fra 2020 har SMV'erne vurderet, i hvilken grad virksomhedens ejer/øverste ledelse er involveret i beslutninger om virksomhedens arbejde med digital sikkerhed. Af resultaterne fremgår det, at 74 pct. af de adspurgte SMV'er vurderer, at virksomhedens ledelse *i høj grad* er involveret i beslutninger om virksomhedens arbejde med digital sikkerhed. Dermed er 26 pct. af danske SMV'ers ledelser kun *i nogen grad, lille grad* eller *slet ikke* involveret i beslutninger om virksomhedens arbejde med digital sikkerhed. Det er dog positivt, at blot 2 pct. svarer, at ledelsen *slet ikk*e er involveret i arbejdet med digital sikkerhed.

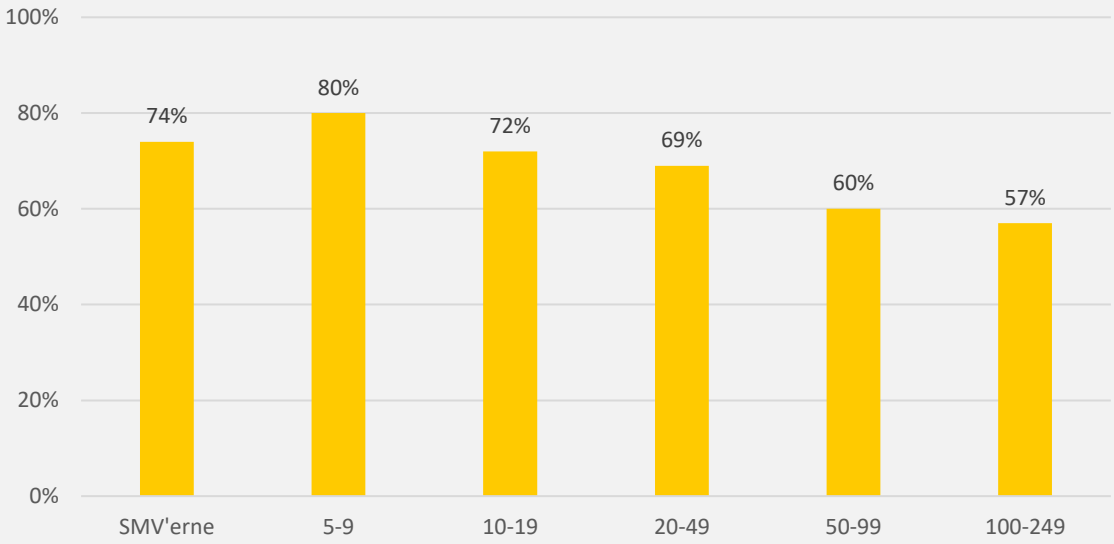
Blandt svarpersoner i undersøgelsen er både ledere[31] (62 pct.) og ikke-ledere (38 pct.) i de danske SMV'er. Det er her interessant, at de adspurgte ledere generelt vurderer deres egen involvering i beslutninger om virksomhedens digital sikkerhed højere, end de adspurgte ikke-ledere vurderer ledelsens involvering. En forklaring herpå kan være, at ledelsen overvurderer sin egen involvering i virksomhedens beslutninger om digital sikkerhed. En anden forklaring kan dog være, at ledelsen i virksomheder med høj ledelsesinvolvering vil være mere tilbøjelige til at besvare et spørgeskema om digital sikkerhed, end ledelsen i virksomheder med lav ledelsesinvolvering i digital sikkerhed.

Figur 27 viser sammenhængen mellem virksomhedsstørrelse og ledelsens involvering i beslutninger om arbejdet med virksomhedens digitale sikkerhed i 2020. Som det fremgår, er ledelsen langt mere involveret i beslutninger om virksomhedens arbejde med digital sikkerhed i mindre SMV'er, end i større SMV'er. Dette resultat er dog ikke overraskende, da ledere i mindre virksomheder generelt kan forventes at være "tættere" på beslutningerne inden for flere forretningsområder end ledelsen i store virksomheder.

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

[31] Ledere er her defineret som virksomhedens ejer, medejer, direktør, økonomichef, økonomidirektør, COO, CFO, CTO, administrativ leder, driftsleder, daglig leder, administrationschef, driftschef, hotelchef, finansdirektør, fabrikschef eller leder.

Figur 27. SMV'er, hvor ledelsen 'i høj grad' er involveret i beslutninger om virksomhedens arbejde med digital sikkerhed, 2020



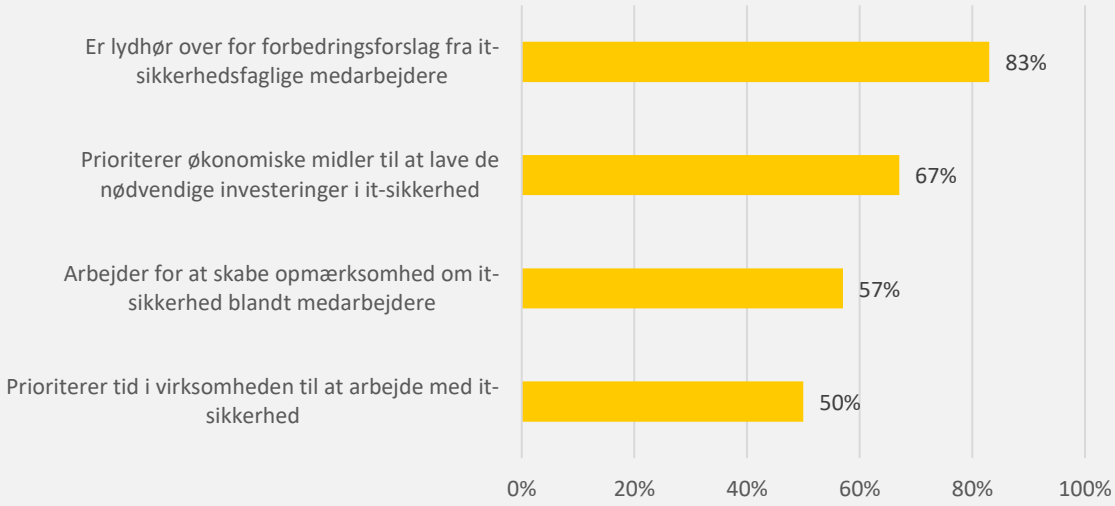
Note: De øvrige svarkategorier er 'slet ikke', 'i mindre grad' og 'i nogen grad'.
Kilde: Egne beregninger baseret på data indsamlet af Epinion i 2020.

Figur 28 viser andelen af danske SMV'er, som er 'enige' eller 'helt enige' i en række udsagn om ledelsens involvering i virksomhedens digitale sikkerhed. Det ses, at blot halvdelen af virksomhederne angiver, at deres ledelse prioriterer tid til at arbejde med virksomhedens digitale sikkerhed. Desuden angiver kun 57 pct. af SMV'erne, at ledelsen arbejder for at skabe opmærksomhed på digital sikkerhed blandt virksomhedens medarbejdere. Endelig er der også rum til forbedring, hvad angår andelen af SMV'er, som mener, at ledelsen prioriterer de nødvendige økonomiske midler til digital sikkerhed (67 pct.) og andelen af SMV'er som mener, at ledelsen er lydhør overfor forbedringsforslag fra it-sikkerhedsfaglige medarbejdere (83 pct.).

Blandt de SMV'er, hvor ledelsen i høj grad er involveret i beslutninger om virksomhedens arbejde med digital sikkerhed, er ledelsen - ikke overraskende – også mere tilbøjelig til at prioritere de økonomiske midler, være lydhør over for forbedringsforslag fra it-sikkerhedsfaglige medarbejdere, sætte fokus på digital sikkerhed blandt virksomhedens medarbejdere og prioritere tid til digital sikkerhed.

Resultaterne i dette afsnit viser generelt et potentiale for at øge fokus på digital sikkerhed blandt SMV'ernes ledelser. En forklaring på, at mange ledelser ikke prioriterer tilstrækkelig tid og ressourcer på digital sikkerhed kan være, at de ofte vælger at udlicitere arbejdet med digital sikkerhed til en leverandør (jf. afsnit 4), og derfor ikke ser det som deres ansvar. Men i sidste ende er det virksomhedens, herunder ledelsens, ansvar.

Figur 28. SMV'er, som er 'helt enige' eller 'enige' i, at virksomhedens ledelse:



Note: De øvrige svarkategorier er 'Hverken enig eller uenig', 'Uenig' og 'Helt uenig'.
Kilde: Egne beregninger baseret på data indsamlet af Epinion i 2020.

9. Metode

Resultaterne i denne rapport er baseret på to forskellige spørgeskemaundersøgelser gennemført blandt danske virksomheder. For det første er resultaterne – tilsvarende sidste år – baseret på den årlige undersøgelse 'IT-anvendelse i virksomhederne' (VITA). I alt indgår 3.947 virksomheder[32] i denne undersøgelse, som er indsamlet i 2020 og som gennemføres af Danmarks Statistik. Virksomhederne i VITA-undersøgelsen har minimum 10 årsværk og tilhører de private ikke-finansielle byerhverv. Selvom dataindsamlingen i VITA-undersøgelsen er gennemført i 2020, spørges virksomhederne til deres situation i 2019.

Resultaterne for VITA 2020 er løbende sammenlignet med resultaterne for VITA 2019 med henblik på at følge udviklingen imellem de to år (ved alle sammenlignelige spørgsmål). I VITA 2019 indgår i alt 5.292 virksomheder med 5+ ansatte. Eftersom mikrovirksomheder med 5-9 kun indgår i VITA-undersøgelsen 2019, er resultaterne omkodet, så de alene er baseret på besvarelser fra virksomheder med 10-249 ansatte og dermed tilsvarende målgruppen i 2020. For det andet er resultaterne i denne rapport baseret på en undersøgelse gennemført af Epinion for Erhvervsstyrelsen. Besvarelserne i Epinion-undersøgelsen er indsamlet i oktober og november 2020 og afspejler virksomhedernes situation på indsamlingstidspunktet. I alt indgår 1.806 virksomheder i denne undersøgelse, som udelukkende er gennemført blandt SMV'er med 5-249 ansatte.

I analysen benyttes vægtet data for begge undersøgelser således, at stikprøverne afspejler den fulde population af danske virksomheder. Men eftersom VITA-undersøgelsen og Epinion-undersøgelsen er indsamlet via forskellige metoder blandt forskellige virksomheder på forskellige

[32] Analysen fokuserer primært på de små og mellemstore virksomheder med 10-249 ansatte, som udgør 3.452 af besvarelserne i datasættet.

tidspunkter, kan virksomhedernes besvarelser i de to undersøgelser, herunder udviklingen mellem de to undersøgelser, ikke sammenlignes direkte. For eksempel er et generelt billede, at SMV'erne i Epinion-undersøgelsen har implementeret færre tekniske sikkerhedstiltag end SMV'erne i VITA-undersøgelsen. Da de to undersøgelser samtidig indeholder forskellige spørgsmål, giver de samlet set et mere nuanceret billede af SMV'ernes arbejde med digital sikkerhed.

Det skal herudover bemærkes, at begge undersøgelser er baseret på selvrapporterede besvarelser fra virksomhederne. Selvevaluering siger noget om udfylderens egen opfattelse af virksomhedens digitale sikkerhed, hvilket kan variere fra dens reelle niveau. Dette er dog en metodisk udfordring i samtlige analyser, der baserer sig på selvrapporteret survey data. I indeværende 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.

9.1 Definition: Digitalt niveau og matchet med risikoprofil

Den metodiske fremgangsmåde for udviklingen af de to indeks til afdækning af SMV'ernes digitale sikkerhedsniveau og risikoprofil og matchet mellem disse fremgår af ilag 1: Indeksering af danske SMV'ers digitale sikkerhedsniveau og risikoprofil samt matchet mellem disse (PwC for ERST, 2021).

9.2 Definition: Brug af it-sikkerhedsforanstaltninger

I VITA-undersøgelsen spørges der til, hvorvidt virksomhederne har implementeret 10 it-sikkerhedsforanstaltninger, som gengivet nedenfor. Alle spørgsmålene besvares med ja/nej. Det skal bemærkes, at der ikke måles på intensiteten eller i hvilken grad virksomhederne benytter den givende teknologi.

Spørgsmål om digital sikkerhed i VITA 2020

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 brug af it-sikkerhedsforanstaltninger. Sikkerhedsforanstaltningen 'biometriske metoder til brugeridentifikation' er dog taget ud af det samlede indeks, der måler virksomhedernes brug af it-sikkerhedstiltag. Dette skyldes bl.a. at det er det eneste tiltag, der ikke i sig selv beskrives af Center for Cybersikkerhed og Digitaliseringsstyrelsen som nødvendigt tiltag i deres tekniske minimumskrav eller i deres vejledning "Cyberforsvar der virker"[33]. Derudover kan man diskutere, om brug af biometriske metoder til brugeridentifikation er mere sikkert end brug af to-faktorgodkendelse, hvorfor dette ikke nødvendigvis altid er den sikreste løsning. Indekset er således baseret på de 9 resterende it-sikkerhedsforanstaltninger. De 9 sikkerhedstiltag skal ikke ses som en udtømmende liste af nødvendige sikkerhedsforanstaltninger, men anses samlet set for en god proxie for SMV'ernes brug af de mest nasale sikkerhedstiltag. Det må dog forventes at fx store og teknologitunge virksomheder har flere og mere avancerede sikkerhedstiltag, som denne analyse ikke har med.

I denne analyse er indekset for de 9 it-sikkerhedstiltag opdelt i følgende tre kategorier: få, nogle og mange it-sikkerhedsforanstaltninger baseret på, hvor mange it-sikkerhedstiltag, som virksomhederne anvender, som beskrevet i *tabel 7*. Der ses på antallet af foranstaltninger fordi, der ikke findes en entydig definition på, hvilke der er vigtigst for virksomhederne og eftersom dette også kan variere fra virksomhed til virksomhed.

Tabel 7: Operationalisering af virksomheders brug af it-sikkerhedsforanstaltninger (indeks)

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

Note: Analysens operationalisering af digitalt sikkerhedsniveau baseret på 9 anbefalede tekniske it-sikkerhedsforanstaltninger.

[33] Center for Cybersikkerhed og Digitaliseringsstyrelsen (2017): Cyberforsvar der virker og Center for Cybersikkerhed og Digitaliseringsstyrelsen (2019): Tekniske minimumskrav til it-sikkerheden hos statslige myndigheder

9.3 Definition: De to basale it-sikkerhedsforanstaltninger

To ud af de 9 it-sikkerhedsforanstaltninger anses som helt centrale[34], ligesom de indgår i langt de fleste anbefalinger for it-sikkerhed. Disse sikkerhedstiltag er 'backup af data' og 'systematisk opdatering af software'. En backup-procedure gør det muligt for virksomheden at få sine systemer relativt hurtigt op at køre igen efter et eventuelt sikkerhedsangreb. Samtidig er systematisk opdatering af software central for virksomhedens sikkerhed, da systemer og programmer løbende repareres for fejl og "sikkerhedshuller" og derved reducerer muligheden for digitale sikkerhedsangreb[35]. Disse to sikkerhedsforanstaltninger er derfor udvalgt til at 'diskvalificere' en virksomheds digitale sikkerhedsniveau således, at virksomheden automatisk defineres med lavt digitalt sikkerhedsniveau, uanset hvilket digitalt sikkerhedsniveau denne virksomhed måtte have. De to sikkerhedstiltag (backup af data og systematisk opdatering af software) rapporteres som 'basale sikkerhedstiltag' gennem rapporten.

9.4 Definitioner: Brug af digitale teknologier

Afsnit 3 ser på virksomheder, der arbejder med digitale teknologier. Til at afdække hvorvidt virksomhederne arbejder med digitale teknologier er der i analysen taget udgangspunkt i følgende tre teknologier; big data anlyse, IoT og Cloud. Nedenfor gennemgås analysens definitioner på de tre teknologier og virksomhederne brug heraf.

9.4.1 Big data analyse:

I VITA-undersøgelsen defineres big data som: brug af teknologier, teknikker eller software-værktøjer som data- eller tekstmining, maskinlæring m.m. til analytisk behandling af big data fra virksomhedens egne kilder eller andre kilder. Big data har typisk disse træk:

- Stor volumen: Big data er typisk meget store mængder data
- Stor kompleksitet og variation, fx i dataformater (tekst, video, billeder, sensordata, logs, click stream data, GPS-koordinater mv.)
- Højt tempo: Big data genereres typisk konstant og hastigheden hvormed data opdateres og nye informationer er tilgængelige er derfor meget høj.

I rapporten defineres brug af big data som virksomheder, der *selv* har analyseret big data i 2020 fra minimum én af følgende kilder (virksomheder, der har fået udført big data fra eksterne leverandører medregnes således ikke):

- Virksomhedens egne data fra smart devices og sensorer. *fx digitale sensorer, RFID-tags eller anden maskine-til-maskine kommunikation*
- Geolokations-data fra brugen af mobile enheder. *fx mobile enheder, der anvender mobilnet, trådløse forbindelser eller GPS*
- Data fra sociale medier. *fx sociale netværk, blogs osv.*
- Andre big datakilder

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

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

9.4.2 Internet of Things

Internet of Things (IoT) defineres i VITA-undersøgelsen som: (smarte) enheder eller systemer, der er forbundet via internettet. De indsamler/udveksler data og kan overvåges eller fjernstyres via internettet (eksempler: styring af indeklima og forbrug, lagerstyrring, flåder/kørsel).

I rapportens medregnes virksomheder, som overvåger eller fjernstyrer virksomheden ("smarte") enheder eller systemer via internettet (IoT), fx fra smartphones eller computere. Det kan være via følgende enheder/systemer:

- Internetforbundne sensorer er sensorer, der er selvstændigt forbundet med internettet og kan opsamle Intelligente termostater, intelligent belysning eller trådløse målere til fjernaflæsning for at optimere virksomhedens energiforbrug? *Fx i lokaler til lager, produktion eller distribution*
- Sensorer, RFID tags eller IP kameraer for at forbedre kundernes oplevelse eller følge deres aktiviteter. *Fx for at tilbyde målrettede rabatter eller self-service-checkout.*
- Sensorer til overvågning af køretøjers kørsel eller vedligeholdelsesbehov. *Fx. ved en serviceaftale for vedligeholdelse af køretøjer.*
- Sensorer eller RFID-tags til at overvåge vareproduktion, styre logistik eller spore varerne i produktionsprocessen.
- Andre (smarte) enheder eller systemer der kan overvåges eller fjernstyres via internettet (IoT).

9.4.3 Cloud computing (internetbaseret it-service)

Cloud computing defineres i VITA-undersøgelsen som: virksomhedens køb af it-services som benyttes via internettet Det omfatter fx adgang til software, computerkraft, lagerkapacitet mv., hvor ydelsen:

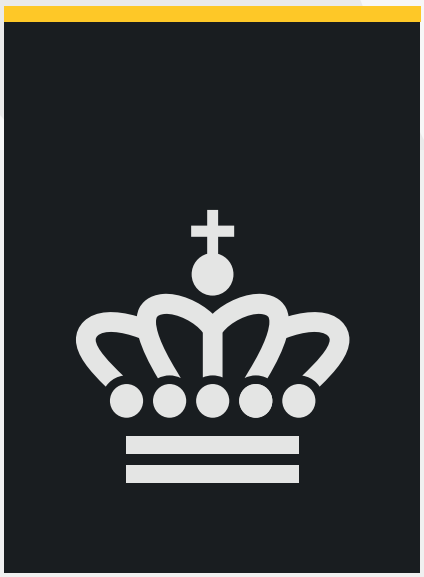
- Leveres fra computer-ressourcer hos leverandøren
- Let kan skaleres op og ned efter behov (fx antal brugere eller ændring af kapacitet)
- Er med selvbetjening, uden daglig kontakt til leverandøren (efter opsætning)
- Kan afregnes efter faktisk forbrug eller forudbetalt.

Brug af cloud defineres i rapporten som virksomheder:

- Der er køber cloud computing til virksomhedens Infrastuktur (herunder computerkraft) til drift af eget it-programmer.

Virksomheder der køber cloud computing til fx e-mail, CRM, økonomisystemer osv. medtages *ikke* i denne analyse, da det vurderes, at virksomheden har et større ansvar for sikkerheden, hvis cloud computing anvendes til egne systemer fremfor at købe "færdige" systemer til fx Outlook og CRM, hvor ansvaret for sikkerheden i højere grad ligger hos leverandøren.

Bilag 1: Indeksering af danske SMV'ers digitale sikkerhedsniveau og risikoprofil samt matchet mellem disse:



ERHVERVSSTYRELSEN

Langelinie Allé 17
2100 København Ø

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

Erhvervsstyrelsen

Indeksering af danske SMV'ers digitale sikkerhedsniveau og risikoprofil samt matchet mellem disse

16. august 2021

pwc

Indholdsfortegnelse

Ledelsesresume

PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab (PwC) har udarbejdet et statusbillede af it-sikkerhedsniveauet i danske SMV'er. Dette er sket med henblik på at kortlægge, om danske SMV'er har et tilstrækkeligt it-sikkerhedsniveau i forhold til deres risikoprofil.

34% har et lavt it-sikkerhedsniveau, mens 25 % har en høj risikoprofil
Undersøgelsen viser, at størstedelen af virksomhederne (43 %) har et middel it-sikkerhedsniveau, mens 34 % har et lavt it-sikkerhedsniveau, og 23 % har et højt it-sikkerhedsniveau. Undersøgelsen viser desuden, at det særligt er på arkitekturområdet, som omfatter stærke adgangskoder, backup mv., at SMV'erne med fordel kan højne it-sikkerhedsniveauet. Ser man på SMV'ernes risikoprofil, placerer størstedelen (66 %) sig i middelintervallet, mens 9 % har en lav risikoprofil og 25 % har en høj risikoprofil. For langt over halvdelen af SMV'erne vil en sikkerhedshændelse altså have en mærkbar indflydelse på deres forretning, og for en fjerdedel vil påvirkningen være særligt kritisk.

40 % af virksomhederne har et utilstrækkeligt sikkerhedsniveau
40 % af de adspurgte virksomheder er sårbare, da de har et it-sikkerhedsniveau, der er lavere end deres risikoprofil. Knap halvdelen har et basalt it-sikkerhedsniveau, der matcher risikoprofilen. Den sidste gruppe på 16 % er påpasselige, i den forstand at de har et højere sikkerhedsniveau, end deres risiko angiver. Vi gør dog opmærksom på, at datasættet kun er tilstrækkeligt til at vurdere basale it-sikkerhedstiltag, hvorfor matchet mellem virksomhedernes it-sikkerhedsniveau og risikoprofil er udformet, under antagelse af at et "højt" it-sikkerhedsniveau i realiteten afspejler et basalt niveau.

<table>
<tr><td colspan="2" rowspan="2"></td><td colspan="3">It-sikkerhedsniveau</td></tr>
<tr><td>Lav</td><td>Middel</td><td>Høj</td></tr>
<tr><td rowspan="3">Risikoprofil</td><td>Høj</td><td rowspan="2">De sårbare 40 %</td><td></td><td></td></tr>
<tr><td>Middel</td><td>De tilpas sikrede
44 %</td><td rowspan="2">De påpasselige
16 %</td></tr>
<tr><td>Lav</td><td></td><td></td></tr>
</table>

Indledning og baggrund

Team Digital Sikkerhed i Erhvervsstyrelsen ("ERST") arbejder for, at særligt SMV'erne får løftet deres digitale sikkerhedsniveau gennem oplysning og konkrete værktøjer. For at målrette denne indsats og for at følge virksomhedernes udvikling på området undersøger ERST løbende danske SMV'ers arbejde med digital sikkerhed. Tidligere analyser viser, at 39 % af SMV'erne ikke har et tilstrækkeligt sikkerhedsniveau, set i forhold til deres risikoprofil. I den forbindelse ønsker ERST en tidssvarende analyse af:

- danske SMV'ers digitale sikkerhedsniveau
- danske SMV'ers risikoprofil
- hvilket niveau af digital sikkerhed, der er passende for virksomheder med de forskellige risikoprofiler, og dermed hvor mange danske SMV'er der har et henholdsvis tilstrækkeligt og utilstrækkeligt digitalt sikkerhedsniveau.

De to ovenstående indeks og matchet mellem disse er baseret på et datasæt, som Erhvervsstyrelsen allerede råder over med besvarelser fra 1.806 danske SMV'er, indsamlet af Epinion i ultimo 2020.

Formål

Formålet med denne rapport er at vise et opdateret resultat for, hvor mange danske SMV'er der har et henholdsvis tilstrækkeligt og utilstrækkeligt sikkerhedsniveau. Rapporten vil på baggrund af det datasæt, som ERST har leveret, præsentere en analyse af:

- et indeks over SMV'ernes sikkerhedsniveau
- et indeks over SMV'ernes risikoprofil
- en vurdering af, hvilket sikkerhedsniveau virksomheder med de forskellige risikoprofiler bør leve op til.

Metode og fremgangsmåde

PwC's analyse og udarbejdelse af de to indeks tager udgangspunkt i spørgeskemadata leveret af ERST. 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.

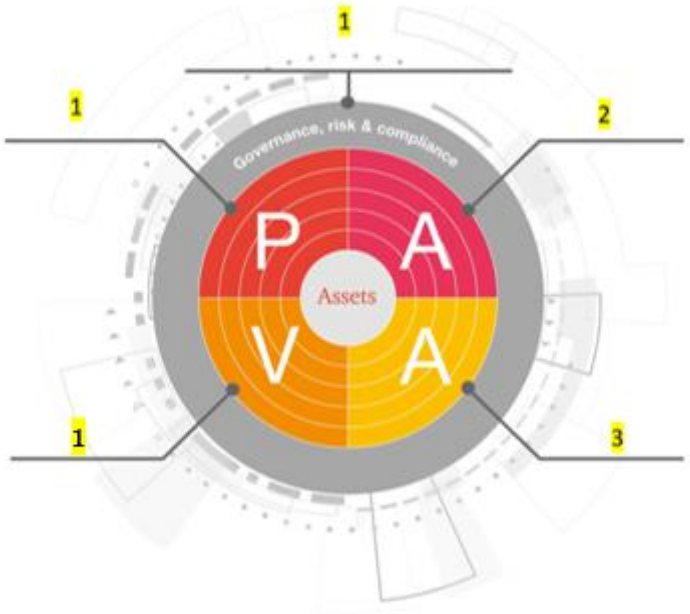
I de følgende afsnit gives en detaljeret redegørelse for PwC's metodiske fremgangsmåde for hver af de to indeks og matchet mellem disse.

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.[1]

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).

Figur 1. PAVA-effektniveauer



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 tabel 1 nedenfor.

[1] PAVA-modellen er et generisk kommunikations-, vurderings- og rapporterings koncept, som virksomheder kan bruge til bl.a. at vurdere og rapportere deres sikkerhedsniveau i relation til forskellige typer af risici og standarder.

Tabel 1. Score og vægt – It-sikkerhedsniveau

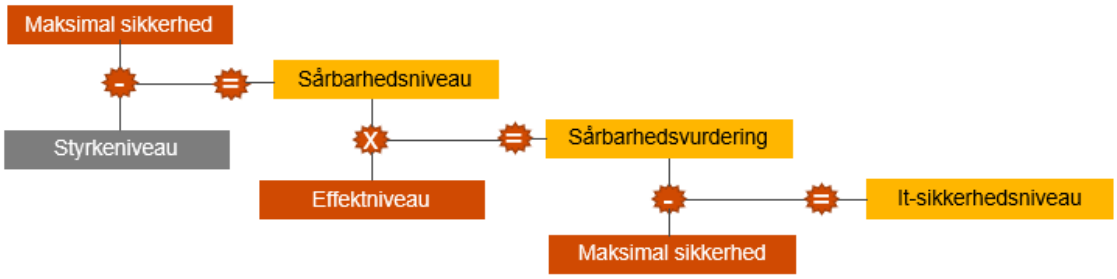
#	Spørgsmål	Score	Vægt
	Governance, risk & compliance		
1	**Spørgsmål Q10:** I hvilken grad … (_1) er virksomhedens ejer/øverste ledelse involveret i beslutninger om, hvordan virksomheden arbejder med it-sikkerhed? (_2) er virksomhedens bestyrelse involveret i større beslutninger om virksomhedens it og it-sikkerhed?	0-5	1
2	**Spørgsmål Q13:** For så vidt angår de eksterne leverandører af it-sikkerhed, har virksomheden så sat krav om: (_1) behandling af data (herunder personoplysninger)? (_2) it-sikkerhedsforanstaltninger?	0-5	1
3	**Spørgsmål Q17:** Virksomhedens ejer/øverste ledelse … (_1) arbejder for at skabe opmærksomhed om it-sikkerhed blandt medarbejdere (_2) er lydhør over for forbedringsforslag fra it-sikkerhedsfaglige medarbejdere (_3) prioriterer tid i virksomheden til at arbejde med it-sikkerhed (_4) prioriterer økonomiske midler til at lave de nødvendige investeringer i it-sikkerhed.	0-5	1
	Processer		
4	**Spørgsmål Q11:** I hvilken grad har virksomheden udliciteret it-sikkerheden (både hosting og drift) til en eller flere eksterne leverandører? ** Det er PwC's erfaring at sikkerhedsniveauet hos eksterne leverandører af hosting/drift er forbedret inden for de seneste år. Generelt er de hurtigere til at få patchet systemer og er mere opmærksomme på nye sårbarheder, sammenlignet med mindre virksomheder der selv står for it-sikkerheden. SMV'er der udliciterer antages derfor, som generelt mere sikre.*	0-5	1
5	**Spørgsmål Q12:** Har virksomheden … (_1) en plan for, hvordan I håndterer personoplysninger? (_2) en plan for, hvordan I håndterer et brud på it-sikkerhed? (_3) en it-sikkerhedspolitik? (_4) lavet en risikovurdering af it-sikkerheden i virksomheden?	0-5	1
	Adfærd		
6	**Spørgsmål Q15:** Det er svært … (_1) at rekruttere medarbejdere med de rette it-sikkerhedskompetencer (_2) at vide, hvor vi kan finde information om it-sikkerhed (_3) at oplære alle medarbejdere i virksomheden i sikker håndtering af relevante it-systemer (_4) at oplære alle medarbejdere i virksomheden i at være opmærksomme på digitale trusler (_5) at vide, hvor vi skal sætte ind for at forbedre virksomhedens it-sikkerhed (_6) at prioritere så meget tid til it-sikkerhed, som vi burde (_7) at vide, hvilke risici der er for netop vores virksomhed (_8) at se den økonomiske gevinst ved et øget it-sikkerhedsniveau. ** Normalt tillægger PwC adfærd vægt 2. Da datasættet er mangelfuldt ift. adfærdsspørgsmål, er parameteren adfærd fjernet fra beregningen af it-sikkerhed. I praksis gøres dette ved at tildele adfærd vægt 0.* *Adfærdsspørgsmål anses som utilstrækkelige, da kun Q15 relaterer sig til adfærd, og da fortolkning af Q15 er uklar i forhold til sikkerhed. Fx er det uklart om en virksomhed, der angiver, at det er svært at skaffe medarbejdere med de rette sikkerhedskompetencer skal score højt, fordi de er opmærksomme på det eller lavt, fordi det netop er svært.*	0-5	0

	Validering		
7	**Spørgsmål Q26:** Har virksomheden været udsat for en sikkerhedshændelse? ** Validering kan kun score 1-4 grundet usikkerheden indbygget i spørgsmålet. Fx er det muligt at en virksomhed har været udsat for en hændelse uden at være vidende om det.*	1-4	1
	Arkitektur		
8	**Spørgsmål Q14:** Hvilke af nedenstående it-sikkerhedstiltag har virksomheden implementeret?	0-5	3

Metode 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 i figur 2, 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 fra Epinion.

Figur 2. Formel til beregning af it-sikkerhedsniveau

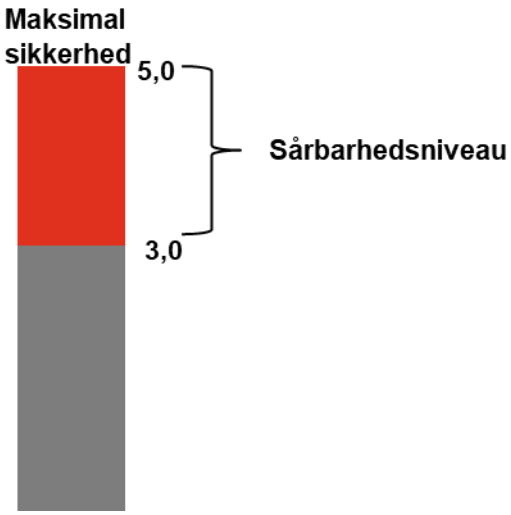


Styrkeniveau
PAVA anvendes til at finde styrken i SMV'ernes sikkerhedstiltag. Ved at bruge PAVA vil der for hvert af områdernes sikkerhedstiltag blive foretaget en vurdering ved anvendelse af en målestok fra 0 til 5.

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, jf. figur 3. Sårbarhedsniveauet består af fem værdier (én værdi inden for hvert PAVA-område), der fordeler sig på en skala fra 0 til 5.

Figur 3. Sårbarhedsniveau



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 sårbarhedsniveauet for hvert enkelt PAVA-område og ganger med det effektniveau, der dækker det enkelte område. Sårbarhedsvurderingen består af én værdi på en skala fra 0 til 5.

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

Figur 4 og 5 viser et eksempel på den samlede beregning af it-sikkerhedsniveauet.

Figur 4. Eksempel på beregning af sårbarhedsvurdering

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	Æ
SME	Maksimal sikkerhed					-	Styrkeniveau					=	Sårbarhedsniveau					*	Effektniveau (vægte)					=	Sårbarhedsvurdering (max 5)
	G	P	Ad	V	Ar	-	G	P	Ad	V	Ar	=	G	P	Ad	V	Ar	*	G	P	Ad	V	Ar	=	
1	5.0	5.0	5.0	5.0	5.0	-	4.7	3.0	2.0	3.0	0.0	=	0.3	2.0	3.0	2.0	5.0	*	1.0	1.0	2.0	1.0	3.0	=	3.16
2	5.0	5.0	5.0	5.0	5.0	-	3.3	3.0	3.0	3.0	0.0	=	1.7	2.0	2.0	2.0	5.0	*	1.0	1.0	2.0	1.0	3.0	=	3.09
3	5.0	5.0	5.0	5.0	5.0	-	3.7	3.0	3.0	3.0	0.0	=	1.3	2.0	2.0	2.0	5.0	*	1.0	1.0	2.0	1.0	3.0	=	3.04
4	5.0	5.0	5.0	5.0	5.0	-	4.3	3.0	1.0	3.0	0.0	=	0.7	2.0	4.0	2.0	5.0	*	1.0	1.0	2.0	1.0	3.0	=	3.46
5	5.0	5.0	5.0	5.0	5.0	-	4.0	0.0	1.0	3.0	0.0	=	1.0	5.0	4.0	2.0	5.0	*	1.0	1.0	2.0	1.0	3.0	=	3.88
6	5.0	5.0	5.0	5.0	5.0	-	4.0	0.0	2.0	3.0	0.0	=	1.0	5.0	3.0	2.0	5.0	*	1.0	1.0	2.0	1.0	3.0	=	3.63
7	5.0	5.0	5.0	5.0	5.0	-	3.7	3.0	2.0	3.0	0.0	=	1.3	2.0	3.0	2.0	5.0	*	1.0	1.0	2.0	1.0	3.0	=	3.29
8	5.0	5.0	5.0	5.0	5.0	-	4.7	0.0	2.0	3.0	0.0	=	0.3	5.0	3.0	2.0	5.0	*	1.0	1.0	2.0	1.0	3.0	=	3.54

Figur 5. Eksempel på beregning af it-sikkerhedsniveau

A	B	C	D	E	F
SME	Maksimal sikkerhed	-	Sårbarhedsvurdering	=	IT-sikkerhedsniveau (max 5)
1	5	-	3.16	=	1.84
2	5	-	3.09	=	1.91
3	5	-	3.04	=	1.96
4	5	-	3.46	=	1.54
5	5	-	3.88	=	1.13
6	5	-	3.63	=	1.38
7	5	-	3.29	=	1.71
8	5	-	3.54	=	1.46

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, vurderer PwC, 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.

Tabel 2. Inddelingen af SMV'er i niveauer på baggrund af it-sikkerhedsscoren

It-sikkerhedsscore	**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.

Figur 6. Udregning af risikoscore

Risikoscore = sandsynlighed x konsekvens

Metode for beregning af sandsynlighedscore

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 (Q4), da det for hver enkelt SMV ville kræve en kvalitativ vurdering af typen af det digitale produkt (angivet med tekst i Q5) i forhold til sektor og sandsynlighed.

Tabel 3. Score – Sandsynlighed

#	Spørgsmål	Score
	Sektor	
1	**Kolonne B i dataset (metadata):** Sektor	1 (lidt udsat sektor) – 3 (meget udsat sektor)
	Størrelse	
2	**Spørgsmål Q3:** Hvor mange fuldtidsansatte er der i virksomheden?	1 (få) – 5 (mange)
	Teknisk angrebsflade	
3	**Spørgsmål Q8:** Anvender virksomheden nogen af nedenstående tjenester og/eller teknologier?	1 (få eller ingen anvendte teknologier) – 5 (de fleste af de angivne teknologier)

I forhold til Q3 antages det, at flere ansatte medfører flere brugere/adgange, og i forhold til Q8 antages det, at flere teknologier medfører en større angrebsflade. Størrelsen af virksomheden og den tekniske angrebsflade scores fra 1-5. Sektoren scores fra 1-3, da PwC på baggrund af datasættet ikke kan vurdere en større spredning mellem de angivne sektorer. Tildelingen af scoren beror på en ekspertvurdering fra PwC.

Sandsynlighedsscoren udregnes som summen af scoren for de tre ovenstående spørgsmål og falder i intervallet 3-13. En højere score angiver en større sandsynlighed.

Tabel 4. Sektorscoring

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 fire spørgsmål, der angiver, hvor store datamængder virksomheden ligger inde med, samt typen af disse data, og hvor afhængig virksomheden er af gemte data og anvendte teknologier.

Tabel 5. Spørgsmål til vurdering af konsekvens

#	Spørgsmål	Score
	Datamængder og -typer	
1	**Spørgsmål Q6**: Hvor mange individer (fx kunder, brugere og ansatte) gemmer virksomheden data på?	1 (ingen data) -5 (mange og/eller følsomme data)
2	**Spørgsmål Q7**: Udover eventuelle persondata hvilke andre typer af data har virksomheden da gemt?	1 (ingen andre data) -5 (særligt fortrolige virksomhedsdata)
	Afhængighed af data og teknologi	
3	**Spørgsmål Q27:** Hvilke typer data/informationer vil virksomheden ikke kunne undvære i opretholdelsen af den daglige drift?	1 (ingen afhængighed) - 5 (afhængig af særligt fortrolige virksomhedsdata)
4	**Spørgsmål Q29**: Hvilke tjenester eller teknologier vil virksomheden ikke kunne undvære i opretholdelsen af den daglige drift?	1 (ingen/meget lille afhængighed) -5 (meget stor afhængighed)

Hver af de fire ovenstående konsekvensspørgsmål scores i intervallet 1-5. Specifikt for konsekvensspørgsmålene tildeles scoren på baggrund af udfaldet med højeste konsekvens. Fx i Q29: Hvis der er en af de angivne teknologier, som virksomheden ikke kan undvære i under én time, så tildeles scoren 5, uanset afhængigheden af andre teknologier.

Konsekvensscoren udregnes som summen af scoren for de fire spørgsmål og falder i intervallet 4-20. En højere score angiver en større konsekvens.

Konvertering af risikoscore til risikoprofil

Sandsynlighedscoren falder i intervallet 3-13, og konsekvensscoren falder i intervallet 4-20. Den lavest mulige risikoscore er 3 x 4 = 12, og den højest mulige er 13 x 20 = 260. Risikoscoren falder derfor i intervallet 12-260.

Den midterste værdi for sandsynlighedsintervallet er 8 – alle værdier herover regnes for høj sandsynlighed. Intervallet 3-8, inddeles i to intervaller af samme størrelse for lav (3-5,5) og middel (5,5-8) sandsynlighed.

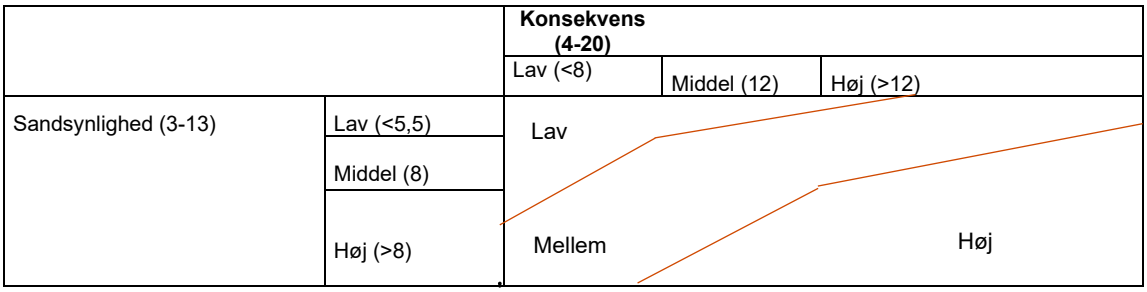
Den midterste værdi for konsekvensintervallet er 12, alle værdier herover regnes for høj konsekvens. Intervallet 4-12, inddeles i to intervaller af samme størrelse for lav (4-8) og middel (8-12) konsekvens.

Middelintervallet for risikoscoren udregnes ved at gange grænseværdierne for middelintervallerne for sandsynlighed og konsekvens med hinanden – det vil sige 5,5 x 8 = 44 og 8 x 12 = 96. En risikoscore i intervallet 44-96 giver derfor en middel risikoprofil, og en risikoscore under 44 og over 96 giver henholdsvis en lav og høj risikoprofil.

Tabel 6. Oversigt over grænseværdier i udregning af risikoprofil

Sandsynlighedsscore (3-13)	Konsekvensscore (4-20)	Risikoscore (12-260)	Risikoprofil
3-<5,5	4-<8	12-<44	Lav
5,5-8	8-12	44-96	Middel
>8-13	>12-20	>96-260	Høj

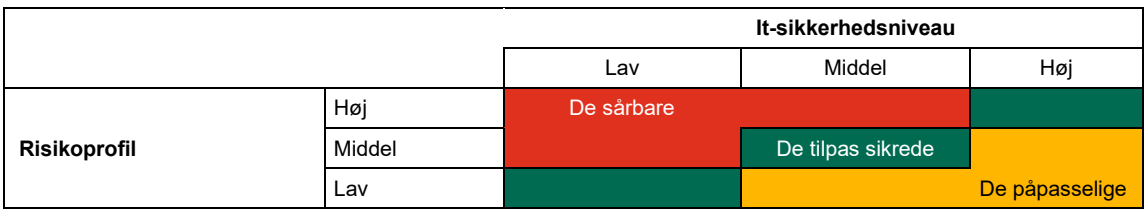
Figur 7. Visualisering – Inddeling af risikoscore i risikoprofil



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.

Figur 8. Match mellem it-sikkerhedsniveau og risikoprofil



De røde felter i figur 8 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 i figur 8 de påpasselige SMV – dvs. dem med et it-sikkerhedsniveau, der overstiger deres risikoprofil. Disse virksomheder har implementeret flere/mere avancerede it-sikkerhedstiltag, end hvad der anses tilstrækkeligt i forhold til den forventede konsekvens og sandsynligheden for en hændelse. De tilpas sikre SMV'er har et it-sikkerhedsniveau, der svarer til deres risikoprofil.

Afgræsninger

I forbindelse med analysen af spørgeskemaundersøgelsen har PwC foretaget en udvælgelse og kvantificering af hvert enkelt spørgsmål for at vurdere, hvilke spørgsmål der anses som relevante og fyldestgørende i forhold til opgaven. PwC har på den baggrund fravalgt særlige spørgsmålstyper, der vurderes svære at kvantificere:

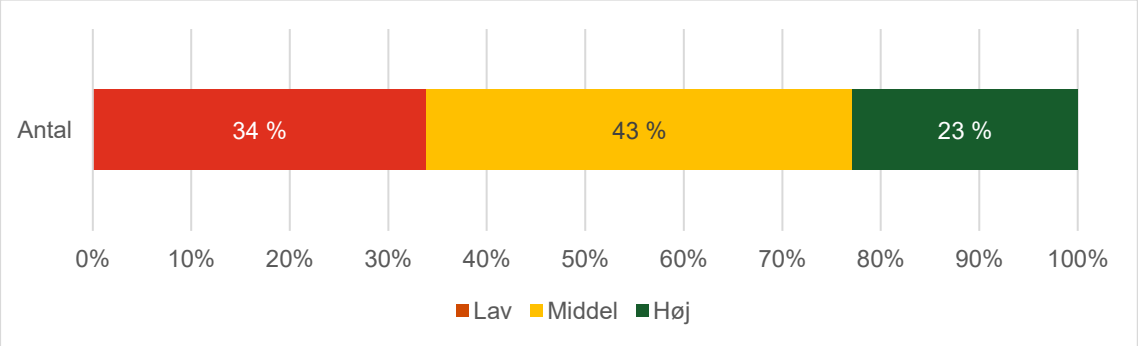
1) Spørgsmål, der tager form som uddybende tekstfelter (fx Q5)
2) Baggrundsspørgsmål, der ikke kan benyttes i forbindelse med en sandsynlighedsvurdering (fx Q1 og Q1a)
3) Spørgsmål, der mangler kontekst (fx Q2)

I forhold til inddelingen af SMV'erne i typer baseret på matchet mellem it-sikkerhedsniveauet og risikoprofilen bør det pointeres, at typen "de tilpas sikrede" er et udtryk for, at en virksomhed lever op til de basale krav for at opnå, hvad der anses som basissikkerhed for SMV'er jf. Erhvervsstyrelsens anbefalinger. Datagrundlaget er ikke tilstrækkeligt til at vurdere, om SMV'er generelt har et højt it-sikkerhedsniveau. Et "højt" it-sikkerhedsniveau afspejler derfor i denne undersøgelse et basalt it-sikkerhedsniveau. Uanset graden af en virksomheds vurderede it-sikkerhedsniveau og forholdet til dennes risikoprofil er det ikke en garanti imod at blive ramt af en it-sikkerhedshændelse.

Indeks over SMV'ernes sikkerhedsniveau

Undersøgelsen viser, at størstedelen af virksomhederne (43 %) har et middel it-sikkerhedsniveau. Dette fremgår af figur 9. Til sammenligning har 34 % et lavt it-sikkerhedsniveau, og 23 % har et højt it-sikkerhedsniveau.

Figur 9. Indeks over SMV'ernes sikkerhedsniveau

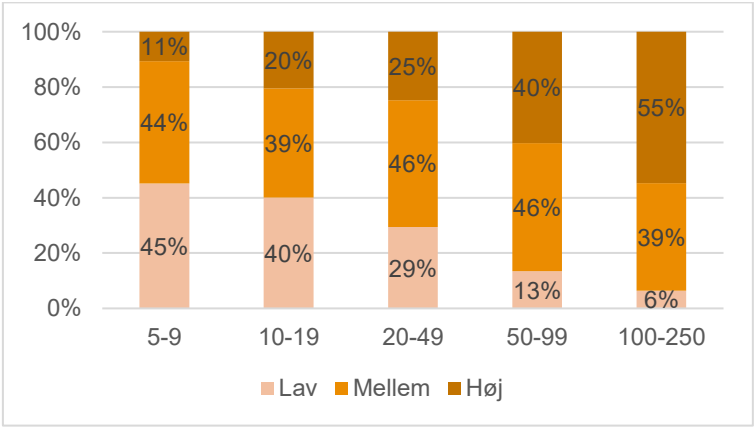


Datasættet indeholder ikke information om sikkerhedstiltag, der ligger ud over det basale. Resultatet viser altså, at lige over en tredjedel af de adspurgte SMV'er ikke lever op til basale it-sikkerhedsforanstaltninger.

Undersøgelsen viser desuden, at det særligt er på arkitekturområdet, som omfatter stærke adgangskoder, backup mv., at SMV'erne med fordel kan højne it-sikkerhedsniveauet. 32 % af SMV'erne scorer lavt (under 3) på arkitekturområdet.

Af figur 10 fremgår der en klar korrelation mellem størrelsen af SMV'erne målt på antal medarbejdere og it-sikkerhedsniveauet. 45 % af SMV'erne med 5-9 ansatte har et lavt it-sikkerhedsniveau og kun 11 % af disse et højt. For de største af SMV'erne (100-250) er billedet modsat, da 55 % af dem har et højt niveau, men kun 6 % har et lavt niveau.

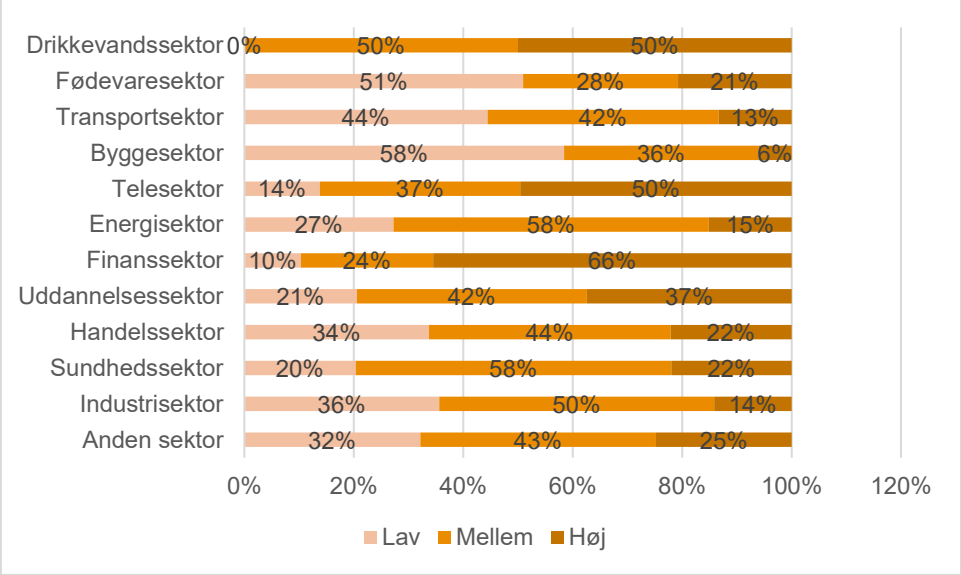
Figur 10. Sammenhæng mellem antal medarbejdere og it-sikkerhedsniveau.



Betragter man it-sikkerhed ift. sektor, kan det af figur 11 ses, at SMV'er i finanssektoren, telesektoren og uddannelsessektoren har det højeste basale it-sikkerhedsniveau. Henholdsvis 66

%, 50 % og 37 % har et højt niveau. Omvendt har byggesektoren, fødevarer og transportsektoren størst andele af SMV'er med et lavt niveau.

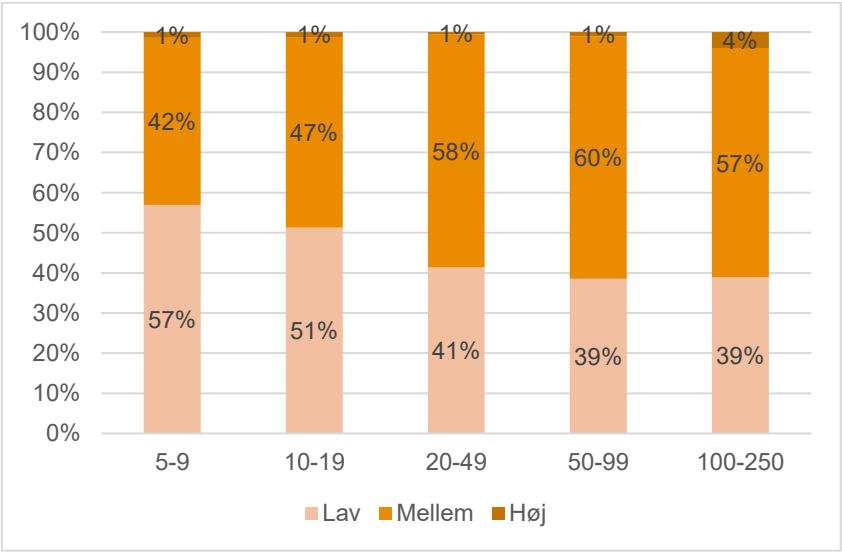
Figur 11. Sammenhæng mellem sektor og it-sikkerhedsniveau.



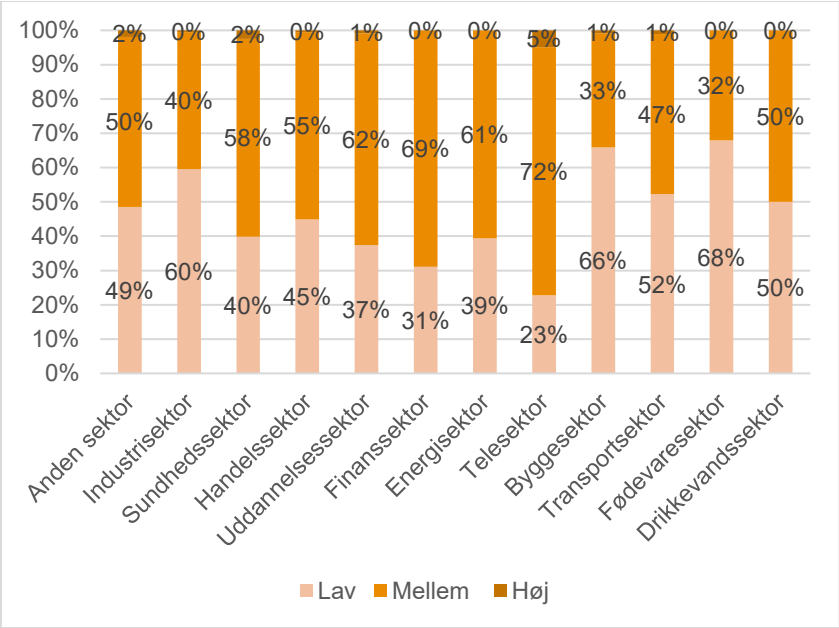
**Der er kun 6 SMV'er der har angivet, at de er i drikkevandssektoren. Resultatet er derfor usikkert.*

Selvom adfærd ikke indgår i beregningen af SMV'erne sikkerhedsniveau, så er det fortsat en vigtig parameter i it-sikkerhed. På baggrund af adfærdsscoren beregnet efter tidligere beskrevne antagelse (se tabel 7), fremgår det af figur 12 at andelen af SMV'er med en dårlig adfærd er lavere, jo større virksomheden er. Tilsvarende har finans-, tele- og uddannelsessektoren den laveste andel med lavt adfærdsniveau, og bygge-, fødevare-, (industri-) samt transportsektoren har den højeste andel (figur 13). Dette svarer til ovenstående billede, hvor antal medarbejdere og sektor vurderes ift. it-sikkerhedsniveauet.

Figur 12. Sammenhæng mellem antal medarbejdere og adfærdsniveau.



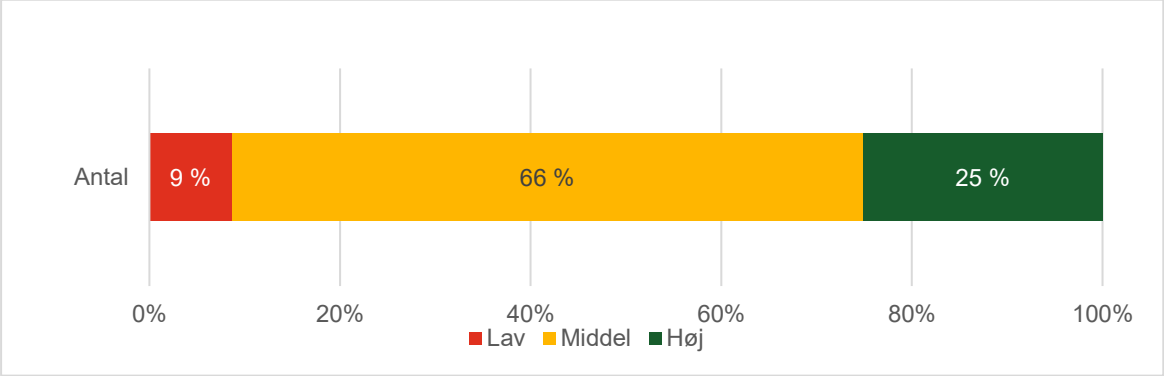
Figur 13. Sammenhæng mellem sektor og adfærdsniveau.



Indeks over SMV'ernes risikoprofil

Ser man på SMV'ernes risikoprofil, placerer størstedelen (66 %) sig i middelintervallet. 9 % placerer sig i lav og 25 % i høj.

Figur 14. Indeks over SMV'ernes risikoprofil



For langt over halvdelen af SMV'erne vil en sikkerhedshændelse altså have en mærkbar indflydelse på deres forretning, og for en fjerdedel vil påvirkningen være særligt kritisk. Risikoprofilen, der er en inddeling af produktet af sandsynlighed og konsekvens, kan forstås ved at kigge på de to parametre i tabel 7.

Tabel 7. Fordeling af SMV'ernes i niveauerne for konsekvens og sandsynlighed

Niveau	Sandsynlighed	Konsekvens
Lav	39 %	3 %
Middel	47 %	48 %
Høj	14 %	49 %

I forhold til sandsynligheden for, at en hændelse indtræffer, vurderes denne som lav for 39 % af SMV'erne og middel for 47 % af SMV'erne. Kigger man på datasættet, ses det, at knap 64 % af de adspurgte SMV'er befinder sig i en sektor, der ikke generelt er særligt udsat (scorer 1 i sektor), 83 % har under 50 ansatte, altså maksimalt en middelstørrelse, og 94 % anvender maksimalt tre forskellige teknologier, hvilket vil sige, at de har en begrænset angrebsflade. Overordnet set er der altså meget få SMV'er, der har en høj grad af sandsynlighed for en hændelse.

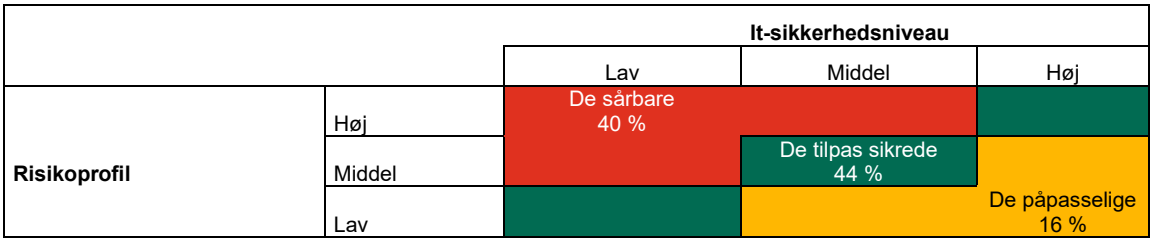
Ser man omvendt på konsekvensen af en hændelse, vurderes den høj for 49 % af SMV'erne og lav for kun 3 % af SMV'erne. Det skyldes, at de fleste SMV'er har en mængde data eller særligt sensitive data, der løfter konsekvensen op over det lave niveau. Kun 13 % af virksomhederne har ingen afhængighed af de adspurgte data, og knap halvdelen anvender en teknologi, de ikke kan undvære i den daglige drift i mere end maksimalt fire timer. Dvs. at konsekvensen af en hændelse er høj for en stor andel af virksomhederne.

Den lille andel af SMV'er med en lav risikoprofil er et udtryk for, at konsekvensen af en hændelse vurderes som lav for kun 3 % af SMV'erne. Dvs. at kun meget få virksomheder opnår en lav risikoscore. Årsagen til, at størstedelen af SMV'erne vurderes til en middel risikoprofil, er, at de mange høje konsekvensscorer afbalanceres af de mange lave sandsynlighedsscorer og ligeledes omvendt.

Vurdering af SMV'ernes sikkerhedsniveau over for risikoprofil

Matchet mellem it-sikkerhedsniveaet og risikoprofilen medfører, at SMV'erne inddeles i tre typer. Af figur 15 fremgår det, at 40 % af de adspurgte virksomheder er sårbare, da de har et it-sikkerhedsniveau, der er lavere end deres risikoprofil. 44 % har et basalt it-sikkerhedsniveau, der matcher risikoprofilen, hvorfor niveauet er tilpas. Den sidste gruppe på 16 % er påpasselige, i den forstand at de har et højere sikkerhedsniveau, end deres risiko angiver.

Figur 15. Match mellem it-sikkerhedsniveau og risikoprofil



Som tidligere nævnt er datasættet kun tilstrækkeligt til at vurdere basale it-sikkerhedstiltag, og ovenstående matrice er udformet under antagelse af, at inddelingen af det basale sikkerhedsniveau er overensstemmende med inddelingen af risikoprofilen. Altså at fx et middel basalt sikkerhedsniveau er i stand til at matche en middel risikoprofil én-til-én.

Enhver person, der er ikke er adressat af denne rapport, eller som ikke har underskrevet og returneret en aftale om ansvarsfrihed til PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab ("PwC") er ikke bemyndiget til at have adgang til denne rapport ("Ubemyndiget person")

Hvis en Ubemyndiget person skulle få adgang til og læse denne rapport, accepterer den Ubemyndigede person, (1) at det af PwC udførte arbejde er udført i henhold til instrukser fastlagt af adressaten af denne rapport og udelukkende er udført til adressatens eget brug, (2) at anerkende, at denne rapport er udarbejdet efter adressatens anvisninger og omfatter givet vis ikke alle forhold, som den Ubemyndigede person måtte finde nødvendige, (3) at PwC, dets partnere og medarbejdere hverken påtager sig eller accepterer nogen form for forpligtelse eller ansvar for denne rapport, og (4) at PwC ikke kan holdes ansvarlig for tab, skader eller omkostninger af nogen art forårsaget af den Ubemyndigede persons brug af denne rapport eller som konsekvens af den Ubemyndigede persons adgang til rapporten. Endvidere accepterer den Ubemyndigede person, at denne rapport ikke må distribueres uden PwC's skriftlige samtykke.