Digital sikkerhed i danske SMV'er

November 2019

ERHVERVSSTYRELSEN

Digital sikkerhed i danske SMV'er

1. Introduktion

Boks 1: Hovedresultater

- Digital sikkerhed fylder mere hos danske SMV'er end tidligere. I 2018 øgede mere end hver tredje SMV deres investeringer i digital sikkerhed.
- Knap hver fjerde SMV har ikke implementeret grundlæggende tekniske sikkerhedstiltag som fx antivirus, firewall og backup.
- Knap halvdelen af de mest digitaliserede SMV'er i Danmark har ikke et grundlæggende teknisk og organisatorisk sikkerhedsniveau[1]
- 12 pct. af danske SMV'er, der benytter nye teknologier som Big Data, maskinlæring eller IoT har ikke implementeret grundlæggende tekniske it-sikkerhedstiltag, og knap halvdelen af disse virksomheder har ikke sørget for et grundlæggende teknisk og organisatorisk sikkerhedsniveau.

Danmark er et af Europas mest digitaliserede lande, og digitale teknologier integreres mere og mere i danske virksomheder[2]. Virksomheders brug af nye teknologier og data kan være en kilde til konkurrencefordele og vækst, men dette forudsætter, at virksomheder tænker digital sikkerhed ind i deres brug af disse nye teknologier. Den øgede digitalisering blandt danske virksomheder medfører, at virksomheder ofte er dybt afhængige af teknologiske løsninger og data, hvorfor det kan medføre store økonomiske udfordringer og tab af tillid, hvis uønskede aktører får adgang til disse.

Alligevel har mange danske virksomheder ikke tilstrækkeligt styr på deres digitale sikkerhed, og problemet er særligt stort blandt de små og mellemstore virksomheder (SMV'er). Dette skyldes blandt andet manglende involvering fra ledelsen, viden hos medarbejdere og prioritering af ressourcer[3].

For at kunne målrette indsatsen for at øge SMV'ers digitale sikkerhedsniveau, vil vi i denne analyse undersøge, hvordan danske SMV'er arbejder med digital sikkerhed. Analysen skal gøre status på, hvor mange danske SMV'er, der prioriterer at investere i digital sikkerhed, og hvilke digitale sikkerhedstiltag de vælger at investere i.

Analysens hovedresultater understreger, at selvom flere danske SMV'er arbejder aktivt med digital sikkerhed end tidligere, er der stadig behov for at øge fokus på grundlæggende it-sikkerhedstiltag hos en stor del af danske virksomheder. Selv blandt de mest digitaliserede og teknologitunge

[1] Et grundlæggende teknisk og organisatorisk sikkerhedsniveau indeholder grundlæggende tekniske sikkerhedstiltag, formuleret it-sikkerhedspolitik og retningslinjer til medarbejdere.
[2] European Commission: The Digital Economy and Society Index (DESI)
[3] Monitor Deloitte for Erhvervsstyrelsen (2018): IT-sikkerhed og datahåndtering i danske SMV'er

virksomheder, der ligger inde med store mængder data, er der stadig mange virksomheder, der ikke har implementeret grundlæggende tekniske og organisatoriske it-sikkerhedstiltag.

Erhvervsstyrelsen arbejder allerede løbende for at skabe større fokus på digital sikkerhed blandt danske SMV'er med henblik på, at understøtte et sikkerhedsmæssigt løft af dansk erhvervsliv. Erhvervsstyrelsen gennemfører kampagner, udvikler information, vejledninger og værktøjer, der kan hjælpe SMV'er, der gerne vil styrke deres digitale sikkerhed.

Boks 2: Eksempler på Erhvervsstyrelsens arbejde med Digital Sikkerhed

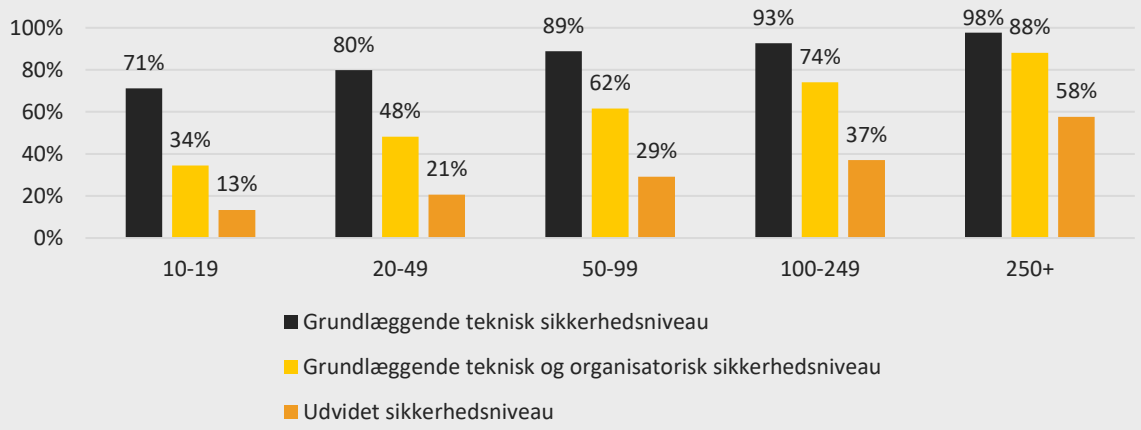
- Sikkerdigital.dk, der er en online informationsportal, som samler viden, vejledninger og værktøjer, der kan understøtte virksomheders arbejde med digital sikkerhed.
- Sikkerhedstjekket.dk, hvor virksomheder kan teste deres sikkerhedsniveau ud fra deres risikoprofil og blive klogere på, hvor de skal starte deres arbejde med digital sikkerhed.
- PrivacyKompasset er en online test, der kan hjælpe virksomheder i gang med at efterleve databeskyttelsesreglerne og få svar på helt basale spørgsmål i forhold til ansvarlig datahåndtering.
- Indberetningsløsning på virk.dk, hvor virksomheder og myndigheder kan indberette sikkerhedshændelser.

1.1 Afgrænsning

Virksomhedernes digitale niveau måles via den årlige undersøgelse 'IT-anvendelse i virksomhederne' (VITA). Undersøgelsen blev i 2015-2018 kun gennemført blandt virksomheder med minimum 10 årsværk ansat blandt de private ikke-finansielle byerhverv. Det betyder, at mikrovirksomheder med under 10 medarbejdere ikke er med i undersøgelsen, selvom disse udgør langt størstedelen af de danske virksomheder.

Som det fremgår af *Figur 1* er der en klar sammenhæng mellem virksomhedsstørrelse og deres digitale sikkerhedsniveau. Når de allermindste virksomheder ikke indgår i analysen, er der derfor stor sandsynlighed for, at vi overestimerer det overordnede it-sikkerhedsniveau i Danmark.

Figur 1: Digital sikkerhed fordelt på størrelse



Note: *Grundlæggende teknisk sikkerhedsniveau* er fx regelmæssig opdatering og patching af styresystemer, antivirus, firewall og backup samt styring af databrugerrettigheder.

Grundlæggende teknisk og organisatorisk sikkerhedsniveau kræver at virksomhederne har implementeret grundlæggende sikkerhedstiltag, at virksomheden har en it-sikkerhedspolitik og retningslinjer for it-sikkerhed og databeskyttelse for medarbejderne.

Udvidet sikkerhedsniveau kræver foruden alle de grundlæggende tiltag også, at virksomheden foretager risikoanalyser af sig selv, stiller krav til leverandører angående it-sikkerhed og uddanner og træner egne medarbejdere i digital sikkerhed.
Kilde: Egne beregninger baseret på tal fra Danmarks Statistik

I kapitel 5 kigger vi nærmere på disse mikrovirksomheder med foreløbige resultater fra VITA2019 som, modsat tidligere undersøgelser, indeholder data for virksomheder med under 10 medarbejdere. Selvom der benyttes andre mål for digital sikkerhed i VITA2019, understøtter resultaterne, at mikrovirksomheder i mindre grad end selv små SMV'er på 10-19 ansatte, implementerer sikkerhedstiltag.

Store virksomheder på 250 eller flere ansatte indgår heller ikke i denne undersøgelse. Som det fremgår af *Figur 1* har de store virksomheder, uanset operationalisering, implementeret flere digitale sikkerhedstiltag end de mindre virksomheder. Dette kan både skyldes, at større virksomheder ofte har flere ressourcer til rådighed, men også at større virksomheder i gennemsnit har højere risikoprofil, dvs. er mere afhængige af IT-systemer og data[4]. Desuden har større virksomheder i sagens natur flere ansatte, hvilket øger risikoen for menneskelige fejl.

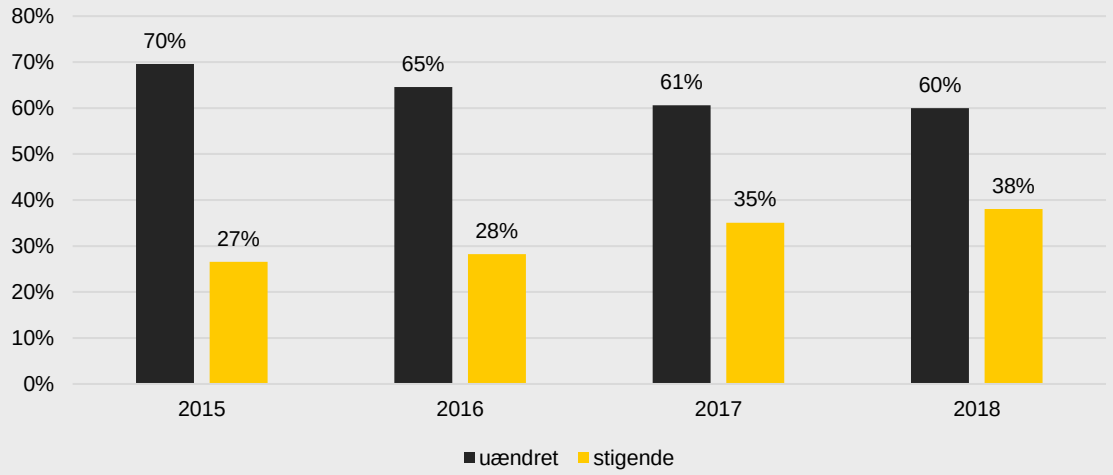
Denne analyse skal give viden om it-sikkerhed i danske SMV'er for at kunne kvalificere Erhvervsstyrelsens indsats for at øge fokus på it-sikkerhed i netop denne målgruppe. Der fokuseres i denne analyse alene på danske SMV'er (10-249 ansatte).

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

2. Danske SMV'ers arbejde med digital sikkerhed

Selvom der stadig er lang vej endnu, før alle danske SMV'er har etableret tilstrækkelige sikkerhedstiltag, går udviklingen den rigtige vej, og stadig flere virksomheder er begyndt at arbejde med digital sikkerhed. Knap 40% af alle danske SMV'er har investeret mere i digital sikkerhed i 2018, hvilket er en større andel end i de forgangne år.

Figur 2: SMV'ernes investeringer i digital sikkerhed



Note: Udviklingen kan være påvirket af, at SMV'erne i samme periode havde svagt stigende investeringer i drift og immaterielle anlæg. Tallene summerer ikke til 100 pct. da ca. 2pct. havde faldende udgifter på tværs af årene.
Kilde: Egne beregninger baseret på tal fra Danmarks Statistik

Selvom der har været en stigning i danske SMV'er der prioriterer digital sikkerhed, er der stadig et stort potentiale for at øge den digitale sikkerhed i mange danske SMV'er.

Boks 3: De økonomiske konsekvenser ved it-sikkerhedsbrud

It-sikkerhedsbrud har oftest store omkostninger for de virksomheder, der bliver ramt. Når en virksomhed bliver hacket, kræver det ofte direkte udgifter til it-specialister til udbedring og efterforskning af sikkerhedsbruddet. Dertil kommer de indirekte økonomiske tab fx i form af manglende drift, tabte forretningsmuligheder og tab af tillid fra kunder.

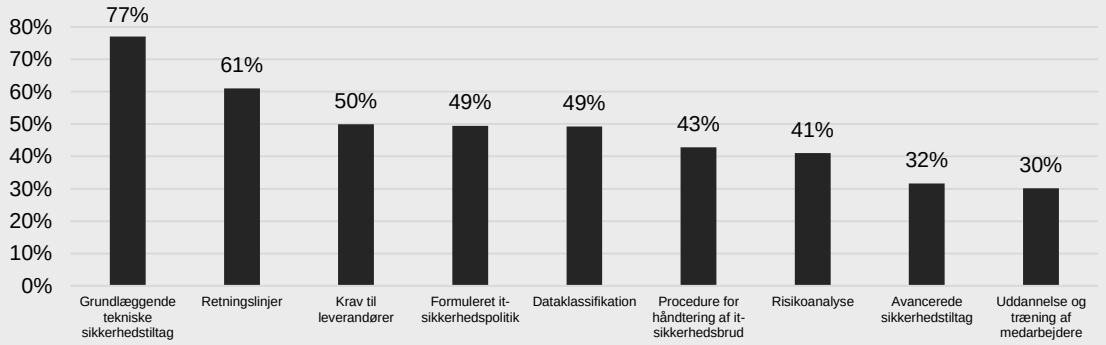
Deloitte har i en undersøgelse af danske SMV'er opgjort, at de direkte omkostninger af et sikkerhedsbrud i gennemsnit ligger på ca. 40.000 kr. Derudover har sikkerhedsfirmaet Kaspersky i en international undersøgelse opgjort, at de direkte og indirekte omkostninger lagt sammen ved et sikkerhedsbrud i gennemsnit ligger på 570.000 kr. for SMV'er

Note: Disse omkostningsestimater er dog præget af mørketal, da der kan være oplysninger som virksomheder ikke ønsker at dele, og fordi virksomheder ofte ikke har overblik over det fulde omfang af konsekvenser.
Kilde: Monitor Deloitte for Erhvervsstyrelsen (2018): IT-sikkerhed og datahåndtering i danske SMV'er, https://erhvervsstyrelsen.dk/sites/default/files/2019-03/it-sikkerhed_og_datahaandtering_i_danske_smver.pdf og Kaspersky Lab (2016): Measuring the Financial Impact of IT Security on Businesses

Blandt danske SMV'er har knap hver fjerde virksomhed ikke implementeret helt grundlæggende tekniske sikkerhedstiltag dvs. tiltag såsom opdatering af antivirusprogrammer, firewall og backup, styring af databrugerrettigheder osv.

Ydermere har hver tredje virksomhed ikke retningslinjer om it-sikkerhed for deres medarbejdere, og mere end 2 ud af 3 SMV'er har ingen uddannelse eller træning af deres medarbejdere inden for it-sikkerhed og databeskyttelse. Dette er vel at mærke blandt virksomheder, som har minimum 10 ansatte, hvor man kan forvente, at der er flere medarbejdere, der har adgang til virksomhedens systemer og data. Der er derfor stor risiko for, at der begås menneskelige fejl i virksomheden, som kan kompromittere virksomhedens it-sikkerhed fx ved phishing mail-angreb, og som kunne være undgået, hvis medarbejderne var trænet og uddannet i it-sikkerhed.

Figur 3: Implementering af forskellige IT-sikkerhedstiltag, andel virksomheder, 2017



Note: Viser andelen af danske private ikke-finansielle byerhverv med minimum 10 årsværk som har implementeret forskellige it-sikkerhedstiltag.
Kilde: Egne beregninger baseret på tal fra Danmarks Statistik

Hvornår virksomheder har et passende it-sikkerhedsniveau afhænger af den enkelte virksomhed. Man kan derfor ikke tale om ét fast niveau af it-sikkerhedstiltag, som er tilstrækkeligt for alle danske virksomheder. Virksomheder varierer i bl.a. størrelse, forretningsmodeller, teknologianvendelse og graden af dataopbevaring. Derfor bør man, når man skal vurdere om en virksomhed har en tilstrækkelig it-sikkerhed, se på, hvilken risikoprofil den enkelte virksomhed har og ud fra denne vurdere hvilke sikkerhedstiltag virksomheden bør have implementeret for at have en passende it-sikkerhed. En tidligere undersøgelse lavet for Erhvervsstyrelsen viser, at 26 pct. af danske SMV'er har en lav risikoprofil, 45 pct. har en middel risikoprofil og 28 pct. har en høj risikoprofil. Undersøgelsen viser

ligeledes, at 39 pct. af danske SMV'er ikke har et digitalt sikkerhedsniveau, der matcher deres risikoprofil[5].

Der er dog en række it-sikkerhedstiltag, der vurderes at være relevante for alle danske SMV'er, og som det vil være hensigtsmæssigt, at alle SMV'er har arbejdet med. I denne analyse arbejder vi med tre forskellige niveauer, som vist ved *tabel 1*. Det grundlæggende tekniske niveau indeholder kun grundlæggende tekniske sikkerhedstiltag. Det grundlæggende tekniske og organisatoriske niveau indeholder som tidligere nævnt tre simple sikkerhedstiltag, som det vil være hensigtsmæssigt, at stort set alle danske SMV'er har implementeret. Det udvidede niveau er mere omfattende og indeholder yderligere tre sikkerhedstiltag, og det vil således være relevant for danske SMV'er, der er meget digitaliserede og dermed er afhængige af IT-systemer og som bruger teknologier, der er baseret på store mængder data[6].

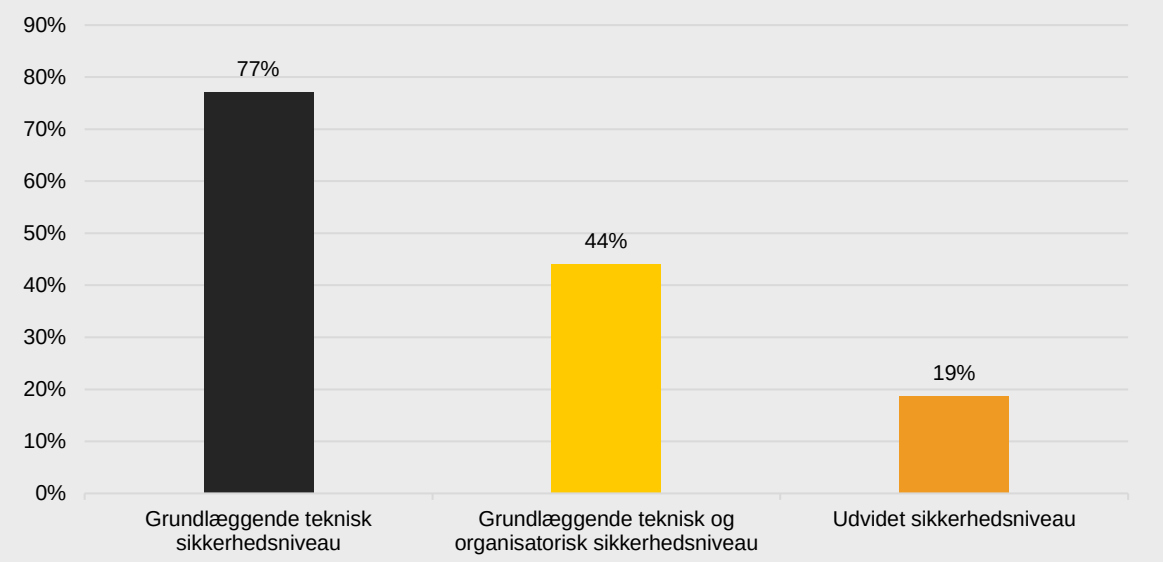
Tabel 1: Niveauer af digital sikkerhed

		Udvidet sikkerhedsniveau
		Uddannelse og træning af medarbejdere indenfor it-sikkerhed og databeskyttelse
		Risikoanalyse
	Grundlæggende teknisk og organisatorisk sikkerhedsniveau	Krav til leverandører vedr. it-sikkerhed og databeskyttelse
	Formuleret it-sikkerhedspolitik	Formuleret it-sikkerhedspolitik
Grundlæggende teknisk sikkerhedsniveau	Retningslinjer vedr. it-sikkerhed og databeskyttelse til medarbejderne	Retningslinjer vedr. it-sikkerhed og databeskyttelse til medarbejderne
Grundlæggende tekniske sikkerhedstiltag. Fx, antivirus og backup.	Grundlæggende tekniske sikkerhedstiltag. Fx, antivirus og backup.	Grundlæggende tekniske sikkerhedstiltag. Fx, antivirus og backup.

I *Figur 4* præsenteres fordelingen af SMV'er, der på nuværende tidspunkt lever op til kravene for henholdsvis det grundlæggende og udvidede minimumsniveau. *Figur 4* illustrerer, at lidt under halvdelen af de danske SMV'er har et grundlæggende teknisk og organisatorisk niveau af digital sikkerhed, og kun en femtedel har implementeret det udvidede niveau af sikkerhedstiltag på trods af, at 28 pct. af danske SMV'er har en høj risikoprofil.

Figur 4: Andel SMV'er der lever op til grundlæggende og udvidet sikkerhedsniveau

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



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik

3. Digital sikkerhed hos virksomheder med høj risikoprofil

Den stigende digitalisering og brug af nye teknologier medfører et stigende ansvar for at prioritere digital sikkerhed, da virksomheders risiko for at blive angrebet ofte stiger i takt med, at de bliver mere digitale og dataafhængige. Det skyldes, at digitalisering og nye teknologier ofte kræver, at data og information lagres digitalt, hvorfor det skaber risiko for, at udefrakommende ønsker at få fat i dette. For eksempel kan en webshop benytte maskinlæring til at udvælge og præsentere produkter for hver enkelt kunde baseret på deres tidligere adfærd på nettet. Denne udvælgelse er baseret på en algoritme, der bygger på store mængder data om deres kunder, og som derfor kan bruges til at forudsige den enkelte kundes adfærd.

Meget digitale virksomheder og virksomheder, der benytter nye teknologier, vil derfor typisk have en høj risikoprofil, hvilket betyder større krav til deres implementering af it-sikkerhedstiltag.

Figur 5: Digitalt sikkerhedsniveau hos en række forskellige typer SMV'er

Note: Anvendelsen af udvalgte digitale teknologier fungerer her som en proxy for virksomhedernes risikoprofil
Kilde: Egne beregninger baseret på tal fra Danmarks Statistik

Blandt SMV'er, der bruger Big Data, Maskinlæring eller IoT, og som derfor forventeligt er i besiddelse af store mængder data, har 12 pct. ikke sikret grundlæggende tekniske sikkerhedstiltag, fx firewall, antivirus og backup. 53 pct. af disse virksomheder har sikret et grundlæggende teknisk og organisatorisk sikkerhedsniveau og 26 pct. har sikret det udvidede sikkerhedsniveau, som man typisk vil forvente af virksomheder med denne type teknologier, der kræver så store mængder data. Dette kan være en indikation på, at investeringer i nye teknologier ikke i tilstrækkelig grad følges op af en sideløbende investering i digital sikkerhed. Det kan potentielt udgøre en substantiel sikkerhedsrisiko – ikke kun for virksomhederne selv, men også for andre virksomheder og organisationer i værdikæden. I den forstand kan manglende sikkerhed hos disse SMV'er udgøre en samfundsmæssig sikkerhedsrisiko.

Figur 5 viser også, at SMV'er, der har valgt at ansætte en eller flere it-specialister, har et højere niveau af digital sikkerhed. Dette peger på, at uddannelsesniveau og kompetencer spiller en nøglerolle i forhold til at styrke it-sikkerheden blandt danske SMV'er.

Figur 6: Digital sikkerhed og SMV'ers digitale niveau (DII-score)

Note: DII-scoren består af 12 digitale teknologier. Anvender virksomheden mellem 0-6 af disse teknologier, vurderes virksomheden til at have et lavt digitaliseringsniveau. Anvender virksomheden mellem 7-12 af disse teknologier, vurderes virksomheden til at have et højt digitaliseringsniveau.
Kilde: Egne beregninger baseret på tal fra Danmarks Statistik

En anden indikator for virksomhedernes digitale niveau er EU's digitaliseringsindikator DII-scoren (Digital Intensity Index). *Figur 6* illustrerer sammenhængen mellem digitaliseringsniveau ud fra denne score og virksomhedernes digitale sikkerhedsniveau.

Figur 6 viser, at selv blandt de mest digitale SMV'er i Danmark har nap halvdelen ikke et grundlæggende teknisk og organisatorisk sikkerhedsniveau, og tre ud af 4 af disse SMV'er har ikke det udvidede sikkerhedsniveau, som man eller kunne forvente af sådanne digitale virksomheder.

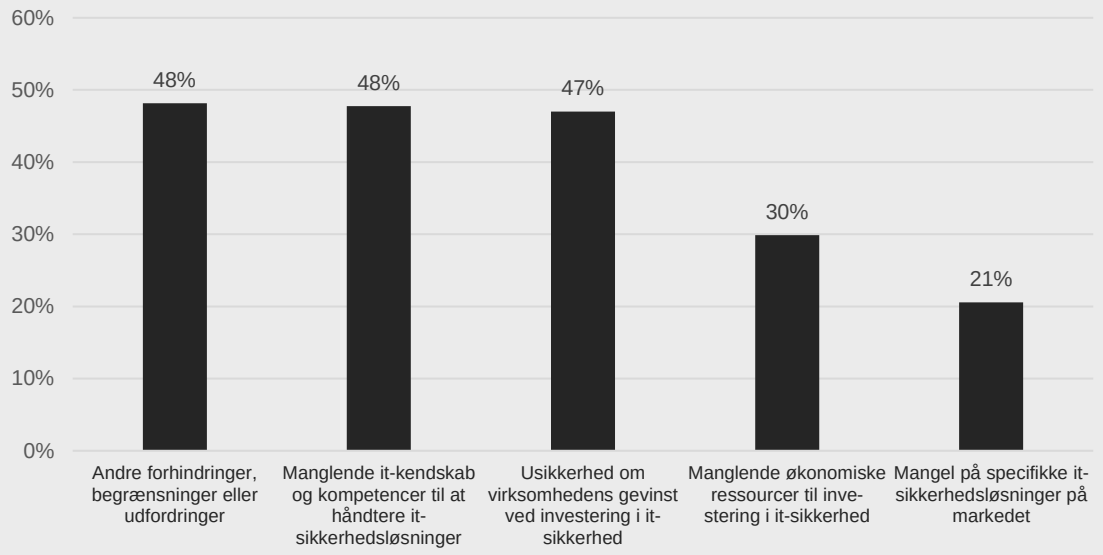
Selv om andelen af SMV'er, der har det grundlæggende og udvidede sikkerhedsniveau, er lavt, er det dog positivt, at figuren illustrerer en tendens til, at jo mere digitaliserede SMV'er er, jo flere sikkerhedstiltag har de implementeret.

4. Oplevede barrierer ved implementeringen af digital sikkerhed

Men hvorfor har flere virksomheder så ikke etableret de nødvendige sikkerhedstiltag? Selvom analysen peger på, at mange danske SMV'er ikke har et tilstrækkeligt niveau af digital sikkerhed, er det kun 6 pct. af danske SMV'er, der indikerer, at de har oplevet udfordringer ved at anvende it-sikkerhedsløsninger. Dette kan skyldes, at det hovedsageligt er virksomheder, der arbejder fokuseret med

implementering af sikkerhedsløsninger, der støder på udfordringer. Det er særligt større virksomheder, der har oplevet udfordringer. Det er er interessant, da det også er de store virksomheder, der har højst niveau af digital sikkerhed. Dette kan skyldes, at virksomheder er nødt til at have beskæftiget sig med digital sikkerhed for at støde på udfordringer for at anvende it-sikkerhedsløsninger. Tallene kan derfor afspejle, at den store udfordring fremadrettet stadig ligger i, at få virksomhederne til at få øjnene op for emnet.

Figur 7: Udfordringer ved implementering af it-sikkerhedsløsninger



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik

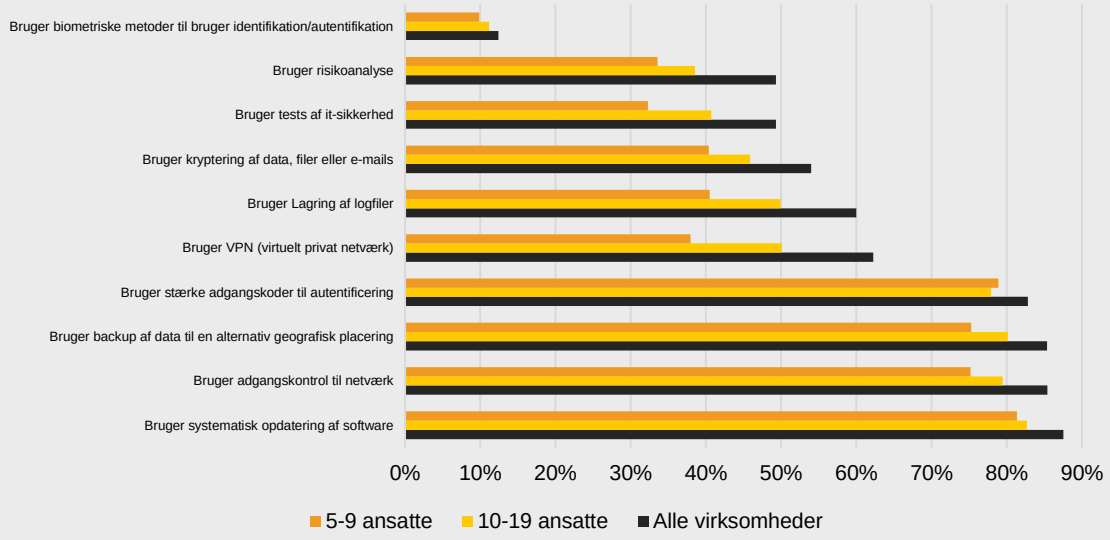
Blandt de 6 pct., der har oplevet udfordringer, er det primært udfordringer med manglende kompetencer og kendskab til it-sikkerhed samt usikkerhed om den økonomiske gevinst i at investere i digital sikkerhed, de nævner. Det peger på, at der stadig er behov for at udbrede viden om digital sikkerhed til danske SMV'er. Denne viden skal ud fra figur 7 både omhandle, hvorfor det er vigtigt at SMV'er forholder sig til digital sikkerhed, men også at der er et behov for mere konkret viden og værktøjer, der kan hjælpe SMV'er med at gå i gang med implementering af sikkerhedsforanstaltninger.

5. Mikrovirksomheders digitale sikkerhedsniveau

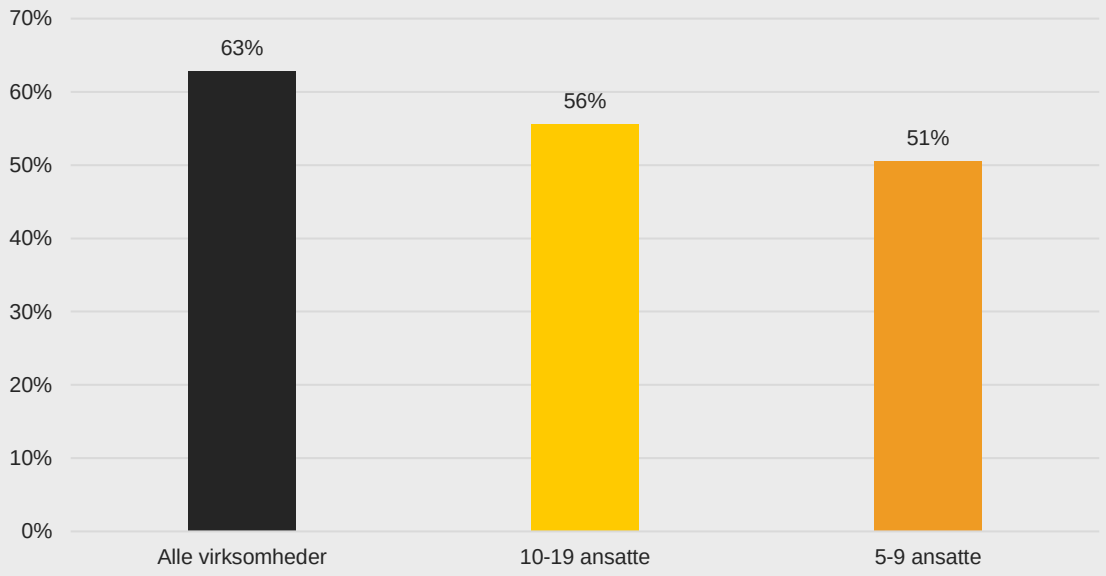
Som nævnt tidligere i analysen omhandler resultaterne kun danske SMV'er med 10-250 ansatte. Det er som nævnt forventningen, at mikrovirksomheder med under 10 ansatte arbejder mindre med it-sikkerhed end de større SMV'er. Pga. manglende data om mikrovirksomhederne i de tidligere VITA undersøgelser af it-anvendelse i danske virksomheder, er det på nuværende tidspunkt ikke muligt at måle it-sikkerhed med de samme it-sikkerhedstiltag, som vi har brugt til at konstruere det 'Grundlæggende' og 'Udvidede' sikkerhedsniveau.

De foreløbige resultater fra den nyere VITA undersøgelse fra 2019, giver os dog mulighed for at sammenligne mirkovirksomheder med de øvrige SMV'er på en række nye sikkerhedstiltag[7]. Som det fremgår af *Figur 8/Figur 9* har færre mikrovirksomheder implementeret de forskellige sikkerhedstiltag end større virksomheder.

Figur 8: Implementerede IT-sikkerhedstiltag, VITA2019



Figur 9: Implementerede IT-sikkerhedstiltag - Tværsnit, VITA2019

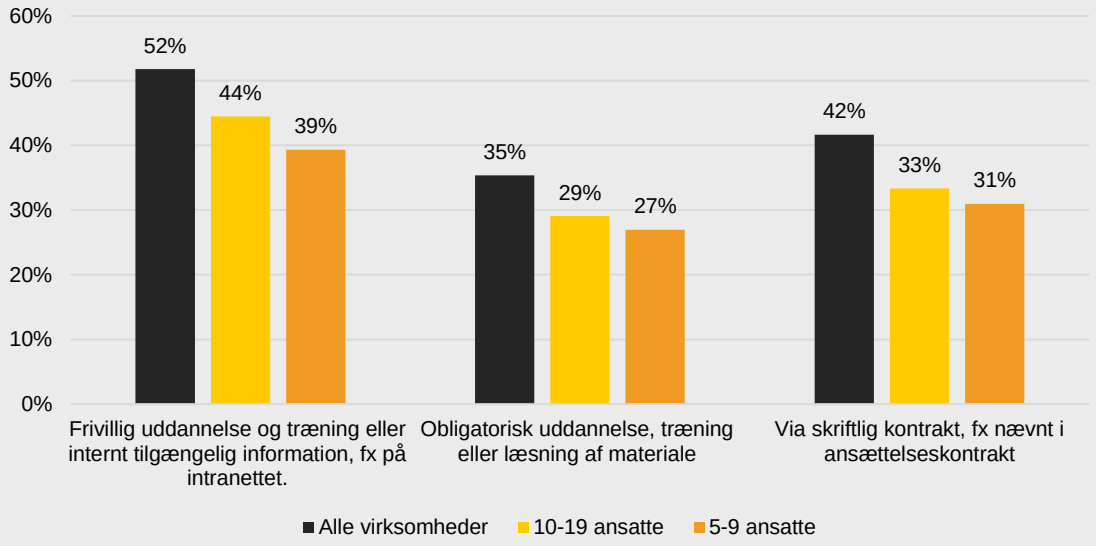


[7] I VITA2019 indgår der spørgsmål om IT-sikkerhed som er strømlinet på tværs af EU, modsat spørgsmålene i tidligere VITA undersøgelser.

Note: Figur 8 viser fordelingen mellem mikro-virksomheder, små virksomheder og landsgennemsnittet i implementeringen af 10 forskellige sikkerhedstiltag. Figur 9 viser den gennemsnitlige implementeringsgrad på tværs af de 10 sikkerhedstiltag fordelt på de samme virksomhedsgrupper.
Kilde: Danmarks Statistik

På samme måde er mikrovirksomhederne grundlæggende også mindre aktive omkring information til deres ansatte om ansvar og roller i forhold til IT-sikkerhed, i hvert fald når man ser på andelen af virksomheder, der på forskellig vis forsøger at gøre det.

Figur 10: Virksomhedens ansatte bliver informeret om deres rolle og ansvar i forhold til It-sikkerhed på følgende måder



Kilde: Danmarks Statistik

Alt i alt tyder det således på, at mikrovirksomheder generelt arbejder mindre med digital sikkerhed end de øvrige virksomheder, og de udfordringer omkring digital sikkerhed som analysen har afdækket for SMV'er på 10-249 ansatte, må forventes også at gøre sig gældende for mikrovirksomhederne.

Bilag 1: Metode

Virksomhedernes digitale niveau måles via den årlige undersøgelse 'IT-anvendelse i virksomhederne' (VITA). I denne analyse bruges primært data indsamlet i VITA 2018. Analysens resultater repræsenterer situationen i de danske virksomheder i 2017.

I alt indgår 3954 virksomheder i undersøgelsen, som foretages af Danmarks Statistik. Virksomhederne i undersøgelsen har minimum 10 årsværk ansat og tilhører de private ikke-finansielle byerhverv. Der benyttes vægtet data således, at stikprøven afspejler den fulde population af virksomheder med minimum 10 årsværk inden for de private ikke-finansielle byerhverv.

Stikprøvens afgrænsning betyder, at undersøgelsen ikke reflekterer virksomheder med under 10 årsværk, som ellers udgør langt den største andel af danske virksomheder. Såfremt mikrovirksomheder (2-9 årsværk) følger den samme tendens som alle øvrige virksomheder, må det forventes, at jo mindre en virksomhed er, desto færre digitale sikkerhedstiltag har den implementeret. Den store andel af danske virksomheder, der mangler de helt grundlæggende sikkerhedstiltag, må derfor forventes at være større end anslået i denne analyse. Dette understøttes af resultaterne i kapitel 5.

Måling af digital sikkerhed

I VITA 2018 spørges der ind til, hvorvidt virksomhederne har implementeret en eller flere af følgende digitale sikkerhedstiltag. Alle spørgsmålene besvares med ja/nej. Det skal bemærkes, at der ikke måles på intensiteten eller i hvilken grad virksomhederne benytter den givende teknologi. Analysen siger således intet om, hvorvidt de valgte teknologier eller sikkerhedstiltag benyttes korrekt og i tilstrækkelig grad. Blot om de benyttes eller ej.

Undersøgelsen baserer sig ligeledes på selvrapportering, hvormed der må forventes en mindre usikkerhed om de nøjagtige resultater i analysen. De overordnede tendenser og resultater står dog stadig til troende.

Boks 4: Spørgsmål om digital sikkerhed i VITA 2018

Har virksomheden implementeret følgende it-sikkerhedsmæssige foranstaltninger?

- Formuleret it-sikkerhedspolitik.
  Dvs. en beskrivelse af virksomhedens sikkerhedsniveau samt de organisatoriske rammer og planer for it-sikkerheden.
- Retningslinjer vedr. it-sikkerhed og databeskyttelse til medarbejderne.
- Uddannelse og træning af medarbejdere indenfor it-sikkerhed og databeskyttelse.
  Fx informationsarrangementer, træningsforløb, online kurser.
- Procedure for håndtering af it-sikkerhedsbrud.
  Fx en beredskabsplan.
- Dataklassifikation.
  Dvs. vurdering af forskellige datatypers følsomhed og fastlæggelse af adgangsrettigheder hertil.
- Risikoanalyse.
  Dvs. løbende vurdering af sandsynlighed og konsekvenser af it-sikkerhedsmæssige hændelser.
- Grundlæggende tekniske sikkerhedstiltag.
  Fx regelmæssig opdatering og patching af styresystemer, antivirus, firewall og backup samt styring af databrugerrettigheder.
- Avancerede tekniske sikkerhedstiltag.
  Fx kryptering af mails og filer, penetrationstest, honeypot systemer.
- Krav til leverandører vedr. it-sikkerhed og databeskyttelse.
- Andre it-sikkerhedsmæssige foranstaltninger.

Foruden måling af implementering af det enkelte tiltag, bruges der i analysen også en række indeks, som måler på tværs af de forskellige sikkerhedstiltag. indeksene er teoretisk konstrueret og er alle bygget op ud fra den samme tankegang, nemlig at man for en given type virksomhed kan forvente, at de som minimum har implementeret en række tiltag for at have et grundlæggende niveau af digital sikkerhed.

I analysen benyttes indeksene: Grundlæggende og Udvidet.

Indekset Grundlæggende teknisk og organisatorisk består af tre tiltag som virksomheden skal have implementeret. De 3 tiltag er 'Grundlæggende tekniske sikkerhedstiltag', 'Formuleret it-sikkerhedspolitik' og 'Retningslinjer vedr. it-sikkerhed og databeskyttelse til medarbejderne'. Det er forventningen, at det vil være hensigtsmæssigt for stort set alle danske virksomheder at leve op til kravene i indekset.

Indekset Udvidet består af de samme tiltag som *Grundlæggende organisatorisk og teknisk*, men har derudover også krav om implementeringen af 'Risikoanalyse', 'Krav til leverandører vedr. it-sikkerhed og databeskyttelse' samt 'Uddannelse og træning af medarbejdere indenfor it-sikkerhed og databeskyttelse'. Udvidet er det forventede minimum hos virksomheder, der anslås at være meget digitale, og dermed har en høj risikoprofil.

Måling af digitalt niveau

Foruden måling af digital sikkerhed bruges der i analysen også forskellige mål for graden af digitalisering. *Figur 5* består af følgende spørgsmål.

Boks 5: Digitale teknologier

IT-specialister	Big Data, Maskinlæring eller IoT	E-eksport
Beskæftiger virksomheden it-specialister? *It-specialister er ansatte, der primært arbejder med it-udvikling, it-drift eller andre it-opgaver.*	Har virksomheden i 2017 analyseret Big data fra nogle af de følgende kilder? Hvilke kilder? *Medtag også big data analyse udført for virksomheden af andre.* Anvender virksomheden sensorer, der er koblet til internettet til følgende formål? Hvilke formål? Anvender virksomheden maskinlæring eller kunstig intelligens? *Inkl. services der omfatter dette, som leveres af eksterne leverandører.*	Har virksomheden modtaget ordrer i 2017 som er afgivet via hjemmesider eller apps? *Medtag ikke ordrer afgivet via almindelig e-post.* Modtog virksomheden i 2017 ordrer via hjemmeside eller apps fra kunder i: - Danmark - Andre EU-lande - Resten af verdenen Har virksomheden modtaget ordrer i 2017 som er afgivet som EDI? Modtog virksomheden i 2017 EDI-ordrer fra kunder i: Danmark - Andre EU-lande - Resten af verdenen

I analysen benyttes også EU's digitaliseringsindikator 'Digital Intensity Index' (DII). Scoren består af 12 spørgsmål om anvendelsen af teknologi (også fra VITA). Alt efter hvor mange teknologier virksomheden har implementeret, kategoriseres den som værende meget lavt digital (0-3 teknologier), lavt digital (4-6 teknologier), højt digital (7-9 teknologier) og meget højt digital (10-12 teknologier). I denne analyse lægges de to laveste og to højeste niveauer sammen så der blot ses på lavt (0-6) og højt (7-12) digitale virksomheder.

Følgende spørgsmål indgår i DII-scoren:

Tabel 2: Spørgsmål der indgår i DII-scoren

1) Hvor stor en del af alle ansatte i virksomheden anvender computer med internetadgang til arbejdsbrug (skal være mindst 50%)?

2) Har virksomheden en hjemmeside?

3) Beskæftiger virksomheden it-specialister?
It-specialister er ansatte, der primært arbejder med it-udvikling, it-drift eller andre it-opgaver.

4) Annoncerer virksomheden på internettet?
Dvs. betalt annoncering på søgemaskiner, sociale medier eller andre hjemmesider.

5) Har virksomheden modtaget ordrer i 2017 som er afgivet via hjemmesider eller apps?
+
Har virksomheden modtaget ordrer i 2017 som er afgivet som EDI?

6) Hvad er virksomhedens hurtigste fastnet internetforbindelse (skal være minimum 30 Mbit/sek)?

7) Anvendes hjemmesiden til følgende formål?
- Produktbeskrivelser, prislister m.m.
- Besøgende kan tilpasse eller designe produkter
- Mulighed for at følge ordrer på hjemmesiden
- Individuelt tilpasset indhold (dvs. genkendelse af brugeren)

8) Hvilke af følgende services køber virksomheden som cloud computing?
-Opbevaring af virksomhedens database(r)
-Økonomi- og regnskabssystemer
-Behandling af kundedata
-Infrastruktur (herunder computerkraft) til drift af eget it-programmel

9) Hvor stor en andel af alle medarbejdere er forsynet med bærbart udstyr til mobil internetadgang til arbejdsbrug?
Dvs. mobiltelefon, bærbar pc eller lignende med mobil internetforbindelse (skal være mere end 20%).

10) Anvendes hjemmesiden til følgende formål?
-Henvisning til virksomhedens profil på sociale medier

11) Har virksomheden udstedt/-sendt følgende typer fakturaer i 2017?
- Fakturaer i et elektronisk format, der kan databehandles automatisk.
Fx EDIFACT, XML, NemHandel.
Medtag ikke fakturaer sendt i PDF-format

12) Udgør virksomhedens B2C websalg mere end 10% af det samlede websalg[8]

[8] Ikke et selvstændigt spørgsmål, men udregnes på baggrund af forskellige spørgsmål i VITA2018

Særligt for kapitel 5

I kapitel 5 benyttes data fra VITA2019 som indeholder et særudtræk af mikrovirksomheder med 5-9 ansatte. Det er således muligt at teste tesen om, at SMV'er med færre ansatte end 10 er lige så eller mindre digitalt sikre som de mindste SMV'er på 10-19 ansatte.

I VITA 2019 blev 1216 mikrovirksomheder adspurgt. Derudover blev yderligere 4076 SMV'er adspurgt hvoraf 1060 af dem havde 10-19 ansatte. Alle resultaterne i kapitel 5 er vægtet.

I VITA2019 spørges der ind til nogle andre sikkerhedstiltag end i de foregående VITA undersøgelser. Det er således ikke muligt at lave en direkte sammenligning. Boks 6 viser de anvendte spørgsmål.

Boks 6: Spørgsmål om digital sikkerhed i VITA 2019

Bruger virksomheden følgende it-sikkerhedsmæssige foranstaltninger (figur 8)?

- 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.

Bliver virksomhedens ansatte informeret om deres rolle og ansvar i forhold til It-sikkerhed på nogen af de følgende måder (figur 10)?

- Frivillig uddannelse og træning eller internt tilgængelig information – fx på intranettet.
- Obligatorisk uddannelse, træning eller læsning af materiale.
- Via skriftlig kontrakt.
  Fx nævnt i ansættelseskontrakt.

Årsagen til at VITA2019 ikke anvendes for hele analysen skyldes, at Erhvervsstyrelsen inden for projektperioden ikke har adgang til data på mikro-niveau, og dermed fx ikke kan undersøge forholdet mellem digital sikkerhed og virksomhedernes digitale niveau.

ERHVERVSSTYRELSEN

Langelinie Allé 17
2100 København Ø
T: 3529 1000
@: erst@erst.dk
W: erhvervsstyrelsen.dk