Digital Sikkerhed i Danske SMV'er

August 2020

Erhvervsstyrelsen

1. Introduktion

Danmark er et af de mest digitaliserede lande i Europa. Det er vigtigt, at danske virksomheder innoverer deres produkter med ny teknologi, så de kan fastholde og udbygge deres markedsposition. Men selvom digitaliseringen og den teknologiske udvikling giver mange muligheder for de danske virksomheder, medfører det også nye sikkerhedsrisici. Det er derfor også vigtigt, at virksomheder har et stærkt og vedvarende fokus på digital sikkerhed, så brugere og samarbejdspartnere bevarer tilliden til de ydelser, der leveres.

Center for Cybersikkerhed vurderer, at truslen fra cyberkriminalitet er 'meget høj' i Danmark, og at truslen er rettet mod alle[1]. Under COVID-19-pandemien har vi også set nye metoder for hackerangreb mod virksomheder, som udgør et nyt element i det samlede trusselsbillede. Samtidig kan de ændrede arbejdsvilkår for mange virksomheder og deres medarbejdere øge risikoen for, at hackerne lykkedes med deres angreb. Pandemien har således understreget et behov for øget fokus på digital sikkerhed i takt med den fortsatte digitalisering og udviklingen af eventuelle nye, vedvarende arbejdsformer som følge af Corona-krisen. Uafhængigt af Corona-krisen ses også en stigende trussel fra målrettede ransomware-angreb mod danske virksomheder[2]. Men mange danske virksomheder har ikke nok fokus på deres digitale sikkerhed, og problemet er særligt stort blandt de små og mellemstore virksomheder (SMV'er)[3][4].

Erhvervsstyrelsen arbejder for, at erhvervslivet, med særlig fokus på SMV'erne, får løftet deres digitale sikkerhed gennem oplysning og konkrete værktøjer. For at kunne målrette denne indsats undersøger vi med denne analyse, hvordan danske SMV'er arbejder med digital sikkerhed. Herunder de danske SMV'ers investeringer i digital sikkerhed, hvilke sikkerhedsforanstaltninger de anvender, og hvilke barrierer de støder på ved implementeringen af digitale sikkerhedstiltag. Analysen vil udgives løbende med henblik på at følge udviklingen i virksomhedernes indsats for at sikre sig mod digitale angreb.

Analysens hovedresultater viser, at opmærksomheden på digital sikkerhed generelt er stigende i de danske virksomheder, der fra 2015-2018 årligt har øget deres investeringer i digital sikkerhed. Til trods for den øgede opmærksomhed, viser analysen, at der stadig er et væsentligt potentiale for at forbedre virksomhedernes it-sikkerhedstiltag. Dette gør sig gældende blandt danske SMV'er generelt såvel som SMV'er, der arbejder med nye teknologier, hvor en relativ stor del af virksomhederne ikke har implementeret selv essentielle sikkerhedstiltag. Derudover viser analysen, at der forekommer en generel mangel på kompetencer inden for cybersikkerhed på tværs af virksomhedsstørrelse. SMV'erne oplever blandt andet 'manglende it-kendskab og kompetencer til at håndtere it-sikkerhedsløsninger' som den største udfordring for at implementere it-sikkerhedsløsninger.

[1] Center for Cybersikkerhed: Trusselsvurdering: Cybertruslen mod Danmark under COVID-19- pandemien

[2] Center for Cybersikkerhed: Trusselsvurdering: Cybertruslen mod Danmark under COVID-19-pandemien

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

[4] Data i denne analyse er indsamlet før COVID-19-pandemien. Der kan således være sket en del på området siden dataindsamlingen, hvilket der må tages højde for ved læsning af rapportens resultater.

Analysen består af følgende afsnit:

2. Danske SMV'ers arbejde med digital sikkerhed
3. Digital sikkerhed hos virksomheder med høj risikoprofil
4. Sammenhæng mellem it-kompetencer og digital sikkerhed
5. Barrierer ved implementering af it-sikkerhedsløsninger
6. It-sikkerhedshændelser i danske SMV'er
7. Metode

Analysens hovedresultater er:

- 38 pct. af de danske SMV'er har øget deres investeringer i it-sikkerhed i 2018, hvilket er en større andel end de forgange år.
- 26 pct. af de danske SMV'er har ikke implementeret de to helt essentielle it-sikkerhedsforanstaltninger; opdatering af styresystemer og backup af data. Det gælder for knap hver tredje virksomhed med 5-9 ansatte.
- 40 pct. af de danske SMV'er har et lavt digitalt sikkerhedsniveau, hvilket i analysen operationaliseres som virksomheder, der har implementeret 0-4 ud af 9 it-sikkerhedsforanstaltninger[6]. 31 pct. af SMV'erne har et middel sikkerhedsniveau, hvilket er defineret som virksomheder, der har implementeret 5-7 sikkerhedsforanstaltninger, mens de resterende 29 pct. har et højt digitalt sikkerhedsniveau med implementeringen af 8-9 sikkerhedsforanstaltninger. Tendensen er klar - jo mindre virksomhed, desto færre digitale sikkerhedsforanstaltninger har den implementeret.
- Selv blandt SMV'er, der arbejder med nye teknologier (herunder IoT, maskinlæring og Big Data), har 15 pct. af virksomhederne ikke implementeret de to essentielle sikkerhedsforanstaltninger, og 22 pct. har, ifølge analysens definition, et lavt digitalt sikkerhedsniveau.
- 7 pct. af de danske SMV'er har hverken egne ansatte eller eksterne leverandører til at varetage it-sikkerhedsmæssige aktiviteter. Det digitale sikkerhedsniveau er signifikant lavere for denne gruppe af virksomheder sammenlignet med virksomheder, der har egne medarbejdere, eksterne leverandører eller begge dele til at varetage it-sikkerhedsmæssige aktiviteter. At nogle virksomheder ikke har medarbejdere til at varetage it-sikkerhedsmæssige opgaver kan skyldes, at 33 pct. af de små og mellemstore virksomheder ikke føler sig i risikozonen for digitale angreb. Modsat er det digitale sikkerhedsniveau signifikant højere blandt virksomheder, der både har egne medarbejdere og eksterne leverandører til at varetage it-sikkerhedsmæssige opgaver[7].
- Virksomheder, der har oplevet en it-sikkerhedshændelse i 2018, øgede ligeledes deres investeringer i it-sikkerhed i samme år. Det tyder således på, at en oplevet it-sikkerhedshændelse øger SMV'ernes fokus på it-sikkerhed.
- De store virksomheder har – sammenlignet med SMV'erne – et højere digitalt sikkerhedsniveau, da 82 pct. i følge analysens definition har et højt digitalt sikkerhedsniveau, mens blot 7 pct. har et lavt niveau. Hele 96 pct. af de store virksomheder har ligeledes implementeret to af de helt essentielle sikkerhedstiltag; opdatering af styresystemer og backup af data. Flere store virksomheder har dog også

[6] Disse er: 1) Systematisk opdatering af software, 2) Backup af data, 3) Adgangskontrol til netværk, 4) Stærke adgangskoder 5) Lagring af logfiler, 6) brug af VPN, 7) Kryptering af data, 8) Risikoanalyse, 9) Tests af It-sikkerhed

[7] Der findes signifikant forskel ved kontrol for virksomhedernes størrelse og branche.

oplevet en eller flere sikkerhedshændelser i 2018, ligesom en større andel af de store virksomheder arbejder med nye teknologier (såsom Big Data, Maskinlæring og IoT). En højere risikoprofil blandt de store virksomheder kan således være én forklaring på, at de har et skærpet fokus på it-sikkerhed.

1.1 Afgrænsning

Virksomhedernes digitale niveau måles af Danmarks Statistik via den årlige undersøgelse 'IT-anvendelse i virksomhederne' (VITA). Denne rapport baserer sig på data indsamlet i 2019 med svar fra 5.292 virksomheder[8]. Analysen skal understøtte Erhvervsstyrelsens arbejde med at øge digital sikkerhed i små og mellemstore virksomheder, som udgør 99 pct. af danske virksomheder. Derfor er målgruppen danske virksomheder med 5-249 ansatte blandt de private, ikke-finansielle byerhverv (samlet betegnelse=SMV'erne). Store virksomheder på 250 eller flere medarbejdere indgår således ikke i målgruppen, men de inddrages løbende til sammenligning med SMV-gruppen.

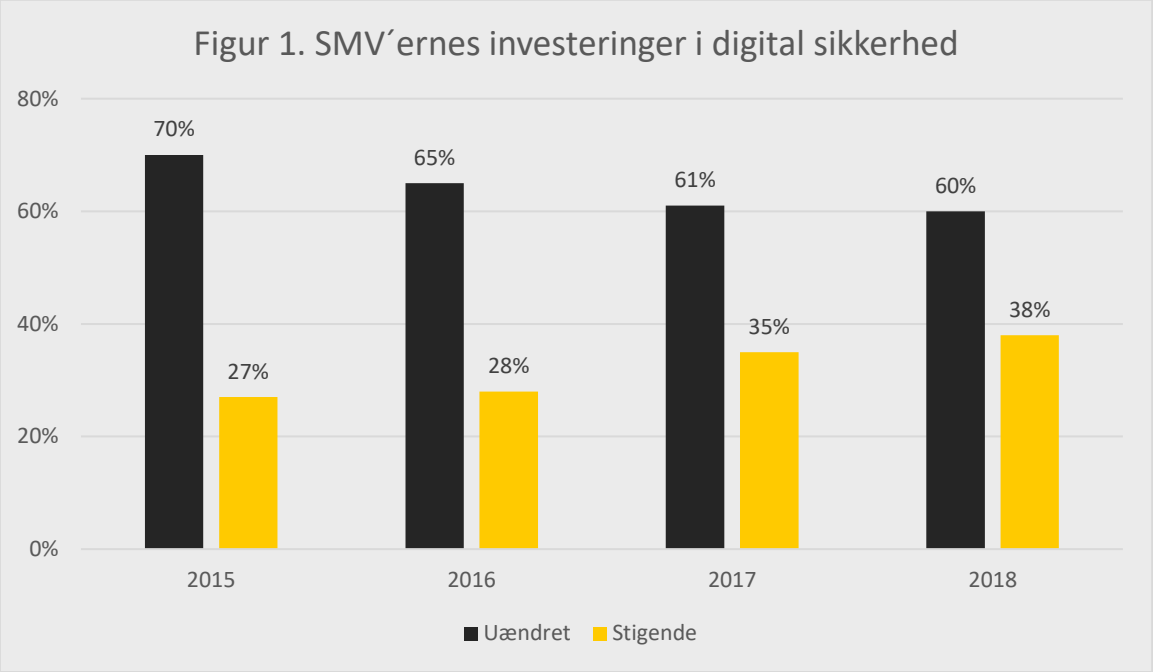
VITA-undersøgelsen blev i 2015-2018 kun gennemført blandt virksomheder med minimum 10 ansatte. Mikrovirksomheder med 5-9 ansatte er således med for første gang i 2019. Dette kan have betydning for de samlede resultater for SMV'erne, og derfor kan rapportens resultater for SMV'erne samlet set ikke direkte sammenlignes med tidligere år. For eksempel kan man forvente, at sikkerhedsniveauet generelt er lavere i 2019, hvor virksomheder med 5-9 ansatte er med i analysen, da både undersøgelsen i 2018 og 2019 viser, at jo færre ansatte virksomheden har, jo færre sikkerhedstiltag har den implementeret. Herudover er det ikke muligt at sammenligne dette års resultater med sidste års resultater på en række specifikke spørgsmål, da både spørgsmålsformuleringer og svarkategorier er blevet ændret i 2019.

2. Danske SMV'ers arbejde med digital sikkerhed

2.1 Stigende investeringer i digital sikkerhed

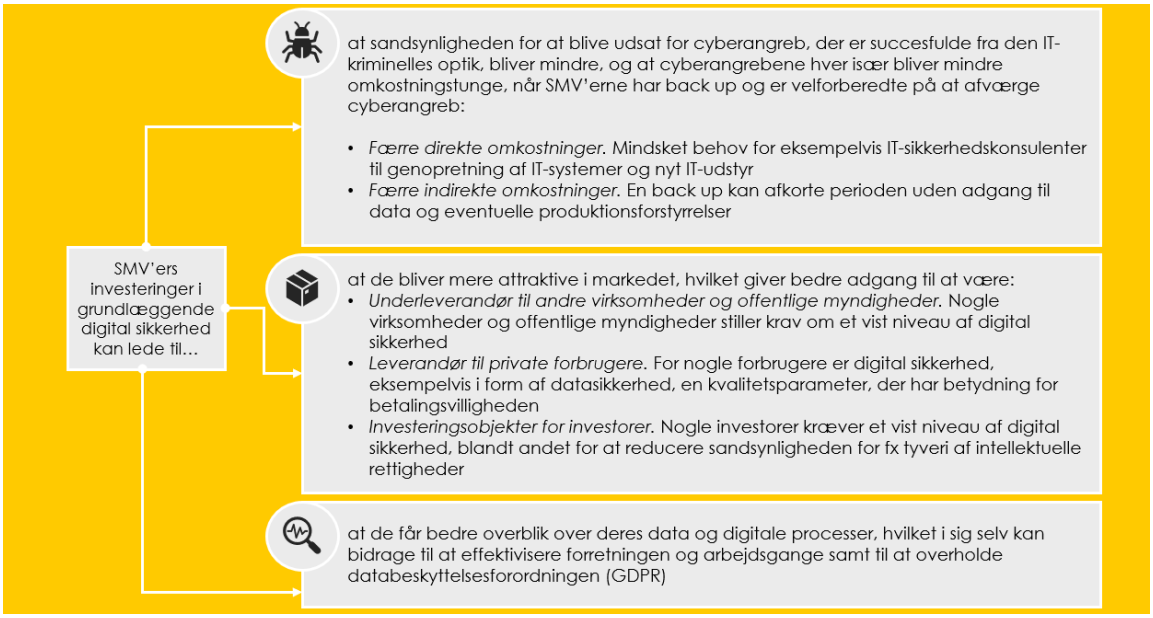
Stadig flere SMV'er investerer i digital sikkerhed. 38 pct. af danske SMV'er har øget deres investeringer i digital sikkerhed i 2018, hvilket er en større andel end de forgangne år, som illustreret i *figur 1*.

[8] Analysen fokuserer primært på de små og mellemstore virksomheder med 5-149 ansatte, som udgør 4.802 af besvarelserne i datasættet.



Note: Resultatet for 2018 er i denne figur beregnet blandt virksomheder med 10-249 ansatte med henblik på at kunne sammenligne resultatet med tidligere år. Inkluderer man mikrovirksomheder med 5-9 ansatte i SMV-gruppen har hhv. 61 pct. uændret og 37 pct. stigende investeringer i 2018.
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.

Figur 2: Effekter ved investeringer i digital sikkerhed



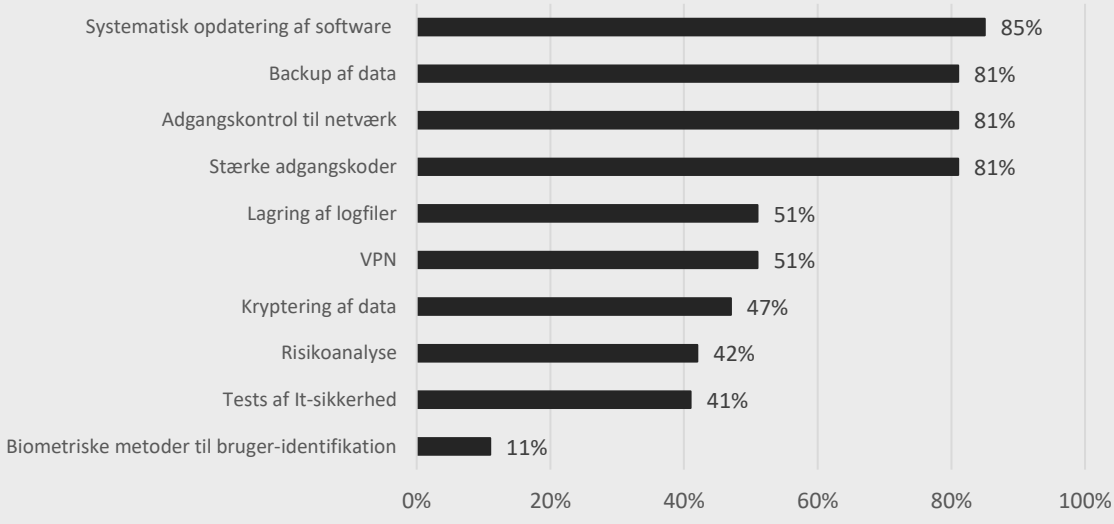
Kilde: Copenhagen Economics i en dataindsamling for Erhvervsstyrelsen (2019): 'Værdien af Digital Sikkerhed'. Resultaterne bygger på interviews med virksomheder. Dataindsamlingen er ikke offentliggjort.

Copenhagen Economics har for Erhvervsstyrelsen undersøgt, hvilke effekter det har, når små og mellemstore virksomheder investerer i digital sikkerhed. Ovenstående *Figur 2* opsummerer de tre overordnede effekter, som de er kommet frem til. Som nærmere beskrevet i figuren kan investeringer i digital sikkerhed føre til 1) nedsat sandsynlighed for et cyberangreb og mindre konsekvenser herved, 2) at virksomhederne er mere attraktive i markedet, herunder overfor eventuelle leverandører og kunder, og 3) at virksomheden får et bedre overblik over deres data og digitale processer, hvilket kan bidrage til at effektivisere forretningen.

2.2 Det digitale sikkerhedsniveau kan løftes i danske SMV'er

Selvom der har været en stigning i antallet af danske SMV'er, der prioriterer digital sikkerhed, er der fortsat potentiale for at øge den digitale sikkerhed i mange danske SMV'er. I VITA-undersøgelsen 2019 spørges der til, hvorvidt virksomheden har implementeret 10 forskellige it-sikkerhedsforanstaltninger[9]. En oversigt over de 10 sikkerhedsforanstaltninger og andelen af SMV'er, der har implementeret disse, fremgår af *figur 3*.

Figur 3. Implementering af forskellige it-sikkerhedstiltag, andel virksomheder 2018



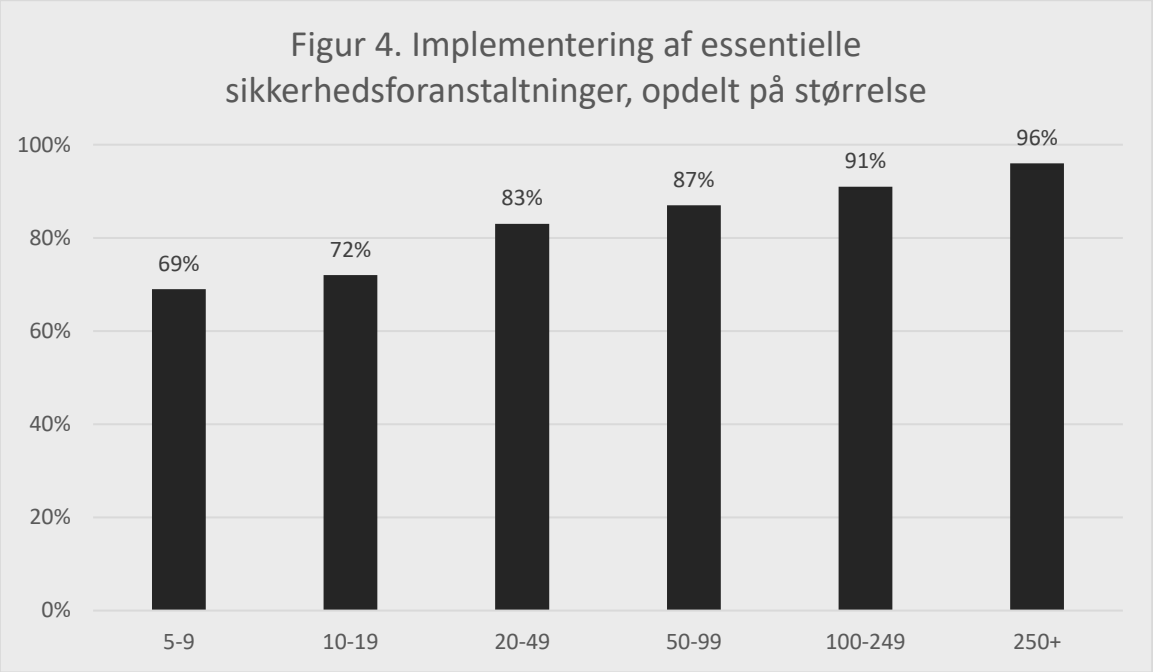
Kilde: Egne beregninger baseret på tal fra Danmarks Statistik.

Som det fremgår af *figur 3,* har 85 pct. af de danske SMV'er implementeret systematisk opdatering af software, mens 81 pct. gennemfører backup af data. Disse to sikkerhedsforanstaltninger anses som værende essentielle 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]. Begge disse tiltag indgår desuden i de gode råd om digital sikkerhed fra Erhvervsstyrelsen på sikkerdigital.dk/virksomhed.

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

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

Ser man på de to tiltag samlet set, har 26 pct. af de danske SMV'er ikke implementeret begge disse essentielle it-sikkerhedsforanstaltninger som en del af deres digitale sikkerhed. Det gælder for knap hver tredje virksomhed blandt mikrovirksomheder med 5-9 ansatte. Til sammenligning har blot 4 pct. af de store virksomheder med 250+ ansatte ikke implementeret de to essentielle foranstaltninger.



Note: Essentielle sikkerhedstiltag defineres som virksomheder, der både har implementeret 'systematisk opdatering af software' og 'Backup af data'. *Kilde:* Egne beregninger baseret på tal fra Danmarks Statistik

Der er også en betydelig del af SMV'erne, som ikke har implementeret øvrige grundlæggende it-sikkerhedsforanstaltninger. Fx er det blot lidt over 40 pct. af virksomhederne, der gennemfører en risikoanalyse eller tester deres it-sikkerhed. I deres vejledning 'Cyberforsvar der virker' anbefaler Center for Cybersikkerhed og Digitaliseringsstyrelsen de danske virksomheder at gennemføre netop en risikoanalyse samt at teste deres sikkerhedsniveau løbende.

Samlet set danner de ovenstående it-sikkerhedsforanstaltninger i *figur 3* baggrund for analysens operationalisering af hhv. lavt, middel og højt digitalt sikkerhedsniveau. Dette er beskrevet i *tabel 1*.

Tabel 1: Operationalisering af digitalt sikkerhedsniveau

Lavt digitalt sikkerhedsniveau	Middel digitalt sikkerhedsniveau	Højt digitalt sikkerhedsniveau
Implementering af 0-4 sikkerhedsforanstaltninger. Inklusive virksomheder der ikke har implementeret de to essentielle sikkerhedstiltag.	Implementering af 5-7 sikkerhedsforanstaltninger. På nær virksomheder der ikke har implementeret de to essentielle sikkerhedstiltag.	Implementering af 8-9 sikkerhedsforanstaltninger. På nær virksomheder der ikke har implementeret de to essentielle sikkerhedstiltag.

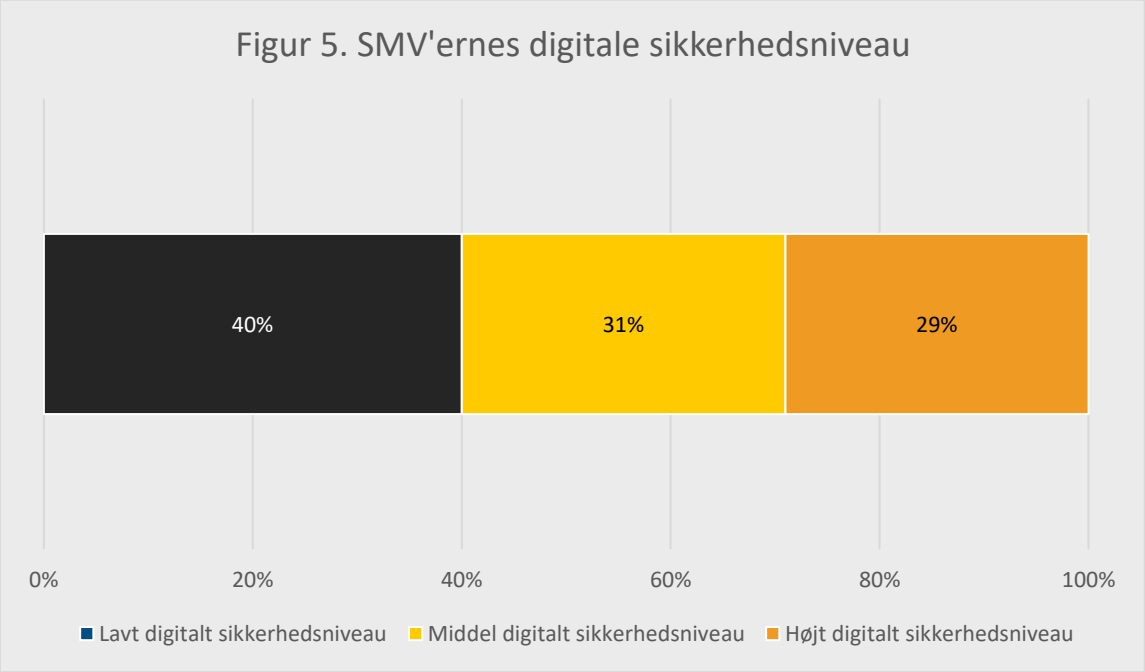
Note: Som begrundet i afsnit 7. Metode er sikkerhedsforanstaltningen 'biometriske metoder til brugeridentifikation' taget ud af det samlede indeks, som derfor består af de 9 resterende sikkerhedsforanstaltninger.
Note: En nærmere forklaring af denne operationalisering fremgår af afsnit 7. Metode.

Det skal indledningsvist understreges, at et passende it-sikkerhedsniveau afhænger af den enkelte virksomheds risikoprofil. Man kan derfor ikke tale om ét fast niveau af it-sikkerhedstiltag, som er

tilstrækkeligt for alle danske virksomheder. Virksomheder varierer bl.a. i størrelse, forretningsmodeller, teknologianvendelse mm. En mindre tømrervirksomhed har fx ikke samme digitale sikkerhedsbehov som et stort softwarefirma. Derfor siger denne analyse således noget generelt om virksomhedernes sikkerhedsniveau uden at konkludere, hvorvidt dette sikkerhedsniveau er tilstrækkeligt. Ønsker man som virksomhed at blive klogere på dette, tilbyder Erhvervsstyrelsen alle virksomheder en målrettet vurdering af deres risikoprofil på sikkerhedstjekket.dk. På hjemmesiden kan man teste sin virksomhed og få gode råd til at matche sin it-sikkerhed op imod sin risikoprofil.

Figur 5 illustrerer SMV'ernes digitale sikkerhedsniveau. Som det fremgår af figuren, har 40 pct. af SMV'erne implementeret under halvdelen af de 9 sikkerhedsforanstaltninger og har dermed et lavt digitalt sikkerhedsniveau, mens 31 pct. har et middel sikkerhedsniveau, og 29 pct. har et højt sikkerhedsniveau ifølge operationaliseringen i denne analyse.

En forklaring på, at mange SMV'er har et lavt digitalt sikkerhedsniveau, kan være, at de ikke ser sig selv som potentielle ofre for digitale angreb. I en dataindsamling, som PwC har gennemført for Erhvervsstyrelsen i 2019, svarer 33 pct. af virksomhederne, at de ikke føler sig i risikozonen for cyberangreb[11]. Derudover angiver 46 pct. af virksomhederne i samme analyse, at de ikke selv mener, at deres data eller it-systemer rummer noget af særlig værdi for it-kriminelle.



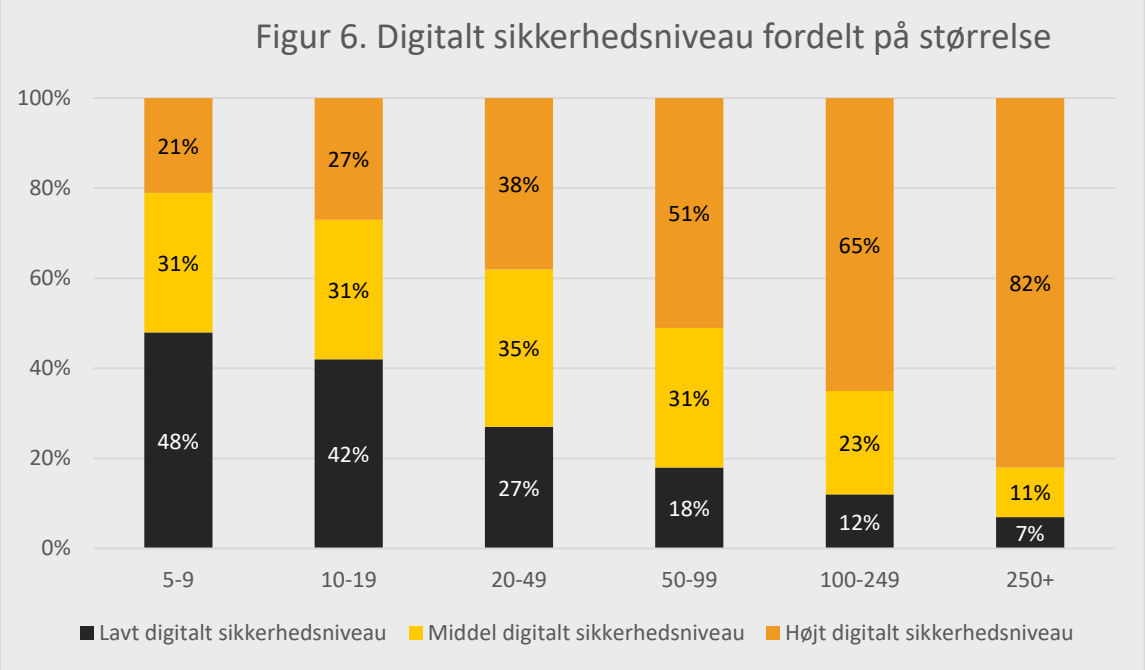
Kilde: Egne beregninger baseret på tal fra Danmarks Statistik

2.3 Jo mindre virksomhed, desto lavere digital sikkerhed

Figur 6 viser det digitale sikkerhedsniveau i danske virksomheder på tværs af virksomhedsstørrelse. Tendens er klar - jo mindre virksomhed, jo lavere digital sikkerhed. For eksempel har knap halvdelen

[11] Dataindsamlingen baserer sig på 1.252 kvalitative web- og telefoninterviews og 30 kvalitative interviews blandt SMV'er. Dataindsamlingen er ikke offentliggjort.

af mikrovirksomhederne med 5-9 ansatte et lavt digitalt sikkerhedsniveau, mens blot 21 pct. kan kategoriseres med et højt niveau. Til sammenligning har kun 7 pct. af de store virksomheder med over 250 ansatte et lavt digitalt sikkerhedsniveau, mens hele 82 pct. har et højt digitalt sikkerhedsniveau. Dette kan både skyldes, at større virksomheder ofte har flere ressourcer til rådighed, men også at større virksomheder i gennemsnit har en højere risikoprofil, dvs. er mere afhængige af it-systemer og data[12].



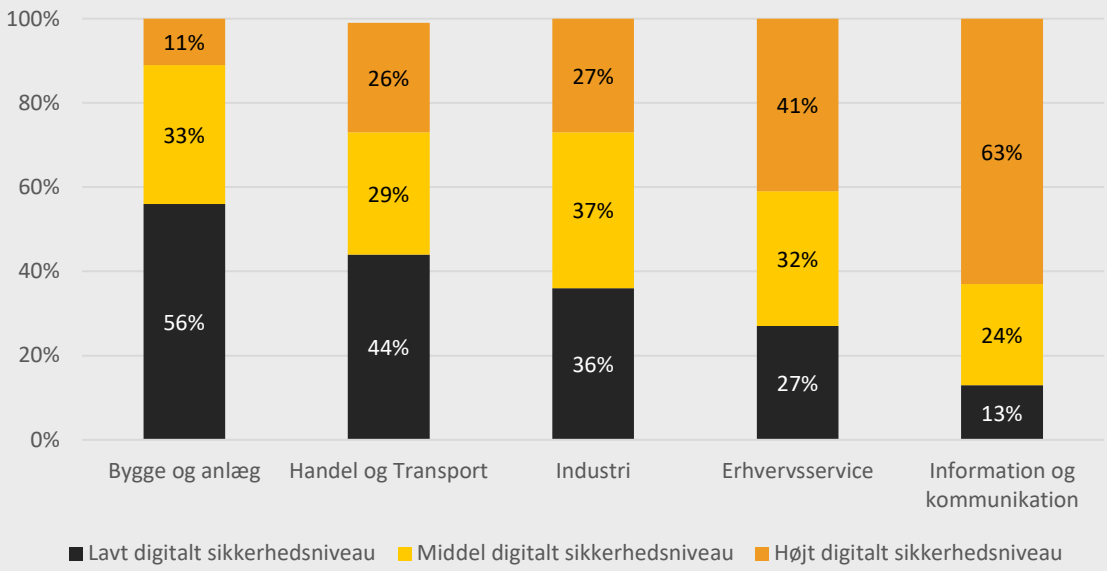
Note: Se tabel 1 og metodeafsnittet for definitioner på hhv. lavt, middel og højt digitalt sikkerhedsniveau.
Kilde: Egne beregninger baseret på tal fra Danmarks Statistik

2.4 Stor forskel på SMV'ernes digitale sikkerhedsniveau på tværs af brancher

Ser vi nærmere på det digitale sikkerhedsniveau for SMV'erne inden for de forskellige brancher, findes der også betydelige forskelle. Branchen 'Bygge og Anlæg' har generelt det laveste digitale sikkerhedsniveau efterfulgt af branchen 'Handel og Transport'. Dette kan eventuelt skyldes de to branchers karakter, hvor en del medarbejdere er ude på byggepladsen eller i butikken frem for at sidde bag deres computere og blive udsat for digitale angreb. Information og kommunikationsbranchen har generelt det højeste digitale sikkerhedsniveau, hvilket heller ikke er overraskende, da man i denne branche vil have en stor andel af medarbejdere, som arbejder digitalt og samtidig ofte vil være i besiddelse af kundedata osv. Som vi vender tilbage til i afsnit 3, er der ligeledes en større andel af virksomheder indenfor 'Information og kommunikation', der arbejder med nye teknologier såsom Big Data, maskinlæring og IoT, og som derfor også må forventes at være i højere risiko for digitale angreb.

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

Figur 7. Digitalt sikkerhedsniveau fordelt på branche



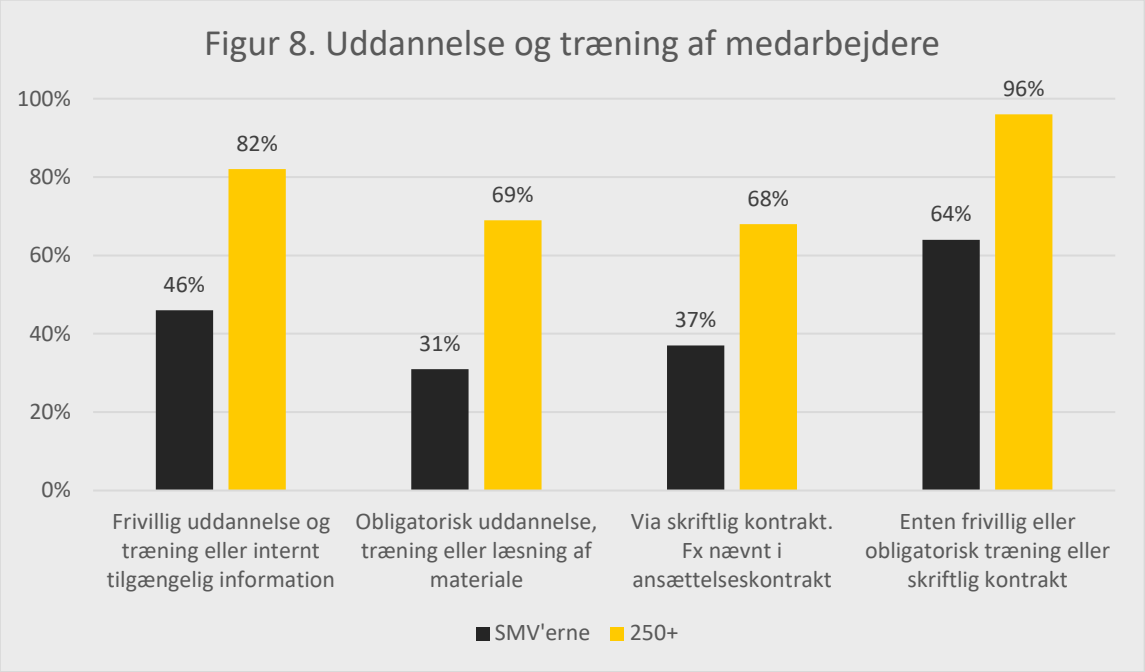
Kilde: Egne beregninger baseret på tal fra Danmarks Statistik

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

Foruden de grundlæggende tekniske it-sikkerhedsforanstaltninger er medarbejderne en vigtig kilde til digital sikkerhed. Mange sikkerhedsbrud sker på grund af fejl og manglende viden blandt medarbejdere. De kan fx blive narret til at klikke på et usikkert link eller udlevere deres adgangskode gennem fx malware eller virusangreb. Derfor er det afgørende, at virksomhedens medarbejdere løbende bliver mindet om de gode digitale vaner.

I alt informerer 64 pct. af SMV'erne deres medarbejdere om deres rolle og ansvar ift. digital sikkerhed gennem enten frivillig træning, obligatorisk træning eller via skriftlig kontrakt. Heraf gennemfører 31 pct. af virksomhederne *obligatorisk* træning og uddannelse for deres medarbejdere.

Figur 8 viser fordelingen af træning i digital sikkerhed af medarbejdere i SMV'erne med 5-249 ansatte sammenlignet med de store virksomheder med 250+ ansatte. Blandt alle virksomhedsstørrelser gælder det, at virksomheder, der arbejder med medarbejder-awareness gennem ét af de tre tiltag, også har et betydeligt højere sikkerhedsniveau, hvad angår de tekniske it-sikkerhedsforanstaltninger (fx har 41 pct. af dem, der træner deres ansatte, et højt digitalt sikkerhedsniveau, mens dette blot gælder 9 pct. blandt de SMV'er, som ikke træner deres medarbejdere). Der findes således en stærk sammenhæng mellem virksomheder, der fokuserer på de tekniske og organisatoriske sikkerhedstiltag og deres digitale sikkerhedsniveau.



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik

I følgende afsnit ser vi nærmere på den digitale sikkerhed hos virksomheder, der er i højere risiko for at blive angrebet, herunder virksomheder der arbejder med nye teknologier.

3. Digital sikkerhed hos virksomheder med høj risikoprofil

Nye teknologier og digitale løsninger medfører mange nye muligheder for de danske virksomheder, men de indebærer også en række nye udfordringer og sikkerhedstrusler, hvilket stiller endnu større krav til den digitale sikkerhed. Fx vil virksomheder, der arbejder med Big Data og maskinlæring, ofte være i besiddelse af store digitale datamængder, som kan give flere angrebsflader, nye angrebstyper og større konsekvenser ved angreb[13]. Ligeledes peger eksperter på, at det er vigtigt med fokus på digital sikkerhed ved brug af 'Internet of Things' (IoT) uanset graden af anvendelse, da selv simple løsninger kan hackes og udnyttes[14]. Jo flere digitale systemer, vi anvender og kobler sammen, desto flere steder kan vi blive angrebet. Et cyberangreb på en IoT-enhed kan påvirke enhedens funktion eller medføre en kompromittering af det netværk, som enheden er installeret i. Det anslås, at IoT-enheder er blandt den type af enheder på internettet, der bliver udsat for flest cyberangreb[15].

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

[14] Alexandra Instituttet (2020): Kan dit IoT produkt hackes.

[15] https://fe-ddis.dk/cfcs/publikationer/Documents/Cybertruslen-mod-Danmark-2019.pdf

Især antallet af DDoS angreb (Distributed Denial of Service) vurderes at stige på grund af usikre IoT-enheder[16]. Et af de mest berømte angreb er Mirai-angrebet, som er det første og største IoT-botnet af sin slags[17].

Boks 1. Mirai-angrebet kort fortalt:

Mirai-angrebet lagde i 2016 store dele af nettet ned, herunder tjenester som HBO, Netflix og Spotify. Angrebet blev udløst af ca. 300.000 inficerede IoT-enheder, som alle på samme tid begyndte at sende forespørgsler til de førnævnte tjenester, som ikke kunne følge med. I angrebet udnyttede bagmændene sårbarheder i IoT-enheder ved at afprøve de mest kendte standard kombinationer af brugernavne og kodeord på IoT-enheder. Bagmændene lykkedes den vej igennem at hacke sig ind i primært webkameraer, routere og videooptagere. Angrebet kunne blandt andet lade sig gøre, fordi det var rettet mod billige IoT-gadgets med lav sikkerhed. Mirai-angrebet var første gang, at man så et denial-of-service-angreb i en så massiv skala[18]. Siden er der opstået varianter af dette botnet, som stadig er aktive[19].

Note: DDoS går ud på, at hackere overbelaster offerets infrastruktur i et så stort omfang, at den bliver utilgængelig[20].

3.1 Flere store virksomheder arbejder med nye teknologier

Figur 9 viser danske virksomheders brug af hhv. maskinlæring, Big Data og IoT i 2018[21]. På tværs af virksomhedsstørrelse er IoT den mest anvendte blandt disse nye teknologier. IoT anvendes samlet set af 38 pct. af SMV'erne, mens Big Data og maskinlæring anvendes af hhv. 16 pct. og 6 pct. af de danske SMV'er. Der ses en tendens til, at en større andel blandt de store virksomheder arbejder med de nye teknologier. Blandt de store virksomheder med 250+ ansatte er det interessant at bemærke, at over halvdelen af virksomhederne arbejder med Big Data, og næsten to tredjedele anvender IoT-enheder til et eller flere formål. Statistisk kan vi se, at en del af forklaringen, på at store virksomheder har et højere sikkerhedsniveau, er, at de i højere grad arbejder med nye teknologier og dermed er mere udsatte for eventuelle sikkerhedsangreb.

[16] https://www.cert.dk/da/news/2018-09-13/ddos

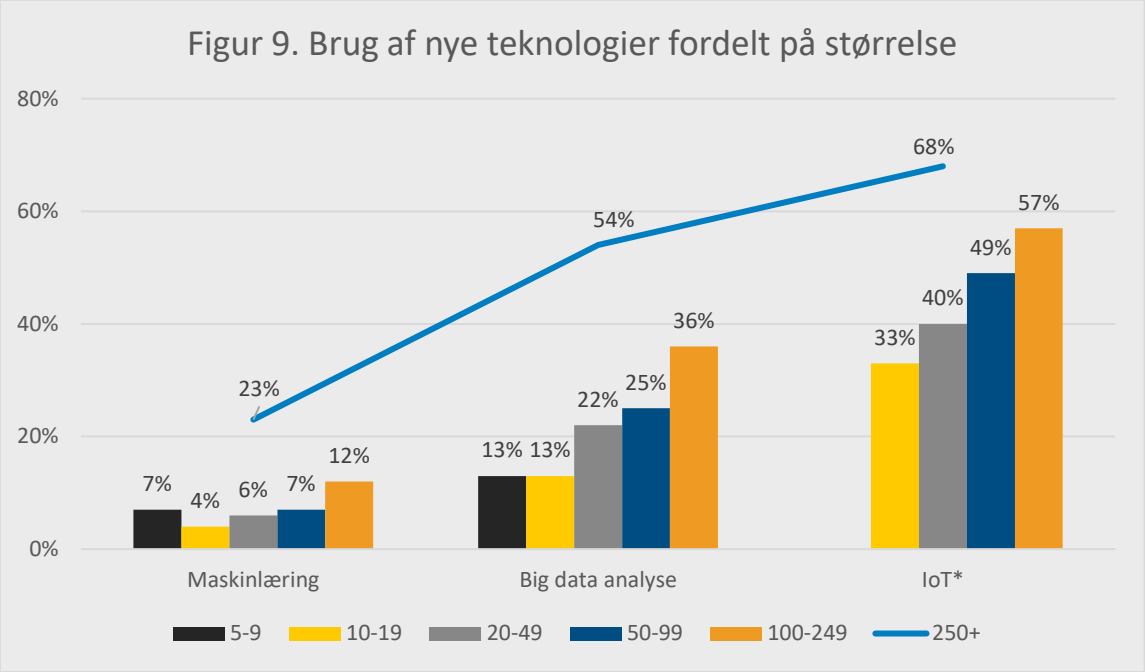
[17] https://www.version2.dk/artikel/it-skurke-slog-store-dele-nettet-ud-med-heftige-botnet-nu-arbejder-de-fbi-1086480

[18] https://alexandra.dk/dk/aktuelt/nyheder/2020/iot-udviklingen-er-som-formel-1-racer-uden-sikkerhedsudstyr

[19] https://fe-ddis.dk/cfcs/publikationer/Documents/Trusselsvurdering-for-telesektoren-2019.pdf

[20] https://www.version2.dk/artikel/it-skurke-slog-store-dele-nettet-ud-med-heftige-botnet-nu-arbejder-de-fbi-1086480

[21] Analysens definitioner på de tre teknologier findes i afsnit 7. Metode.

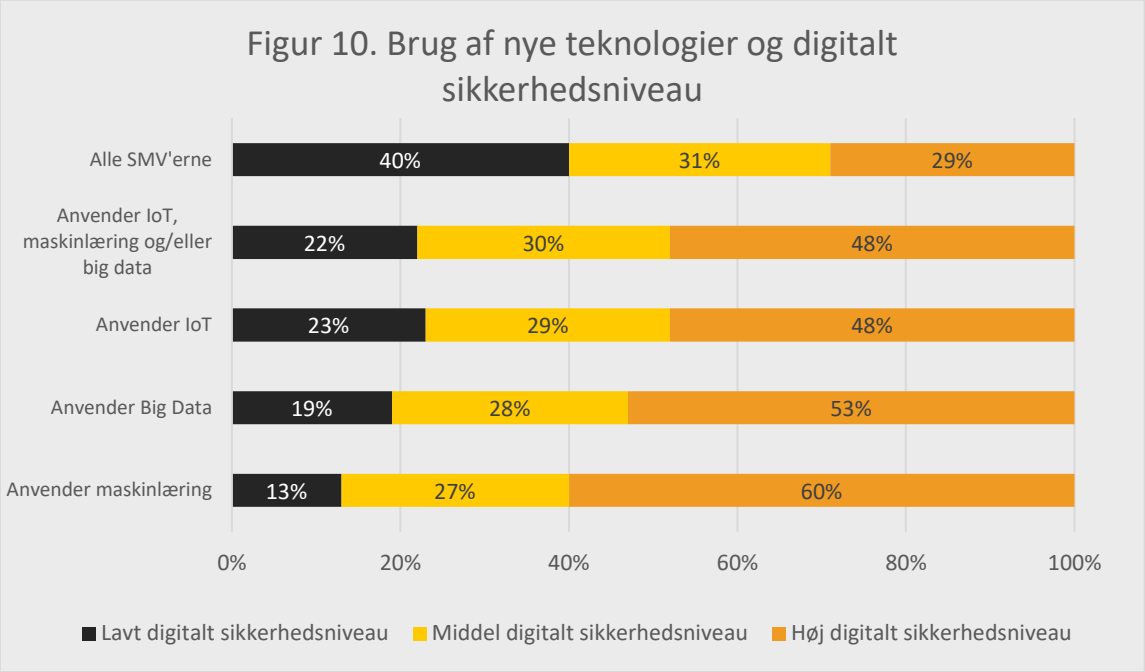


Note: *Mikrovirksomhederne har ikke besvaret spørgsmålet vedr. brug af IoT og er derfor ikke med i denne opgørelse.
Kilde: Egne beregninger baseret på tal fra Danmarks Statistik

Også ved brug af nye teknologier er der betydelige forskelle på brancherne. I tråd med forventningen gør virksomhederne inden for branchen 'Information og kommunikation' mere brug af nye teknologier sammenlignet med de øvrige brancher. Dette understøtter således forklaringen om, at denne branche har et højere sikkerhedsniveau, fordi risikoprofilen i disse virksomheder er højere.

3.2 Blandt SMV'er, der arbejder med nye teknologier, har 15 pct. ikke implementeret essentielle sikkerhedstiltag

Som det fremgår af *figur 10*, har 22 pct. af SMV'erne, der arbejder med IoT, Big Data eller maskinlæring, et lavt digitalt sikkerhedsniveau, mens 30 pct. har et middel digitalt sikkerhedsniveau, og 48 pct. kan kategoriseres med et højt digitalt sikkerhedsniveau. Til sammenligning har 7 pct. af de store virksomheder, der arbejder med IoT, Big Data eller maskinlæring, et lavt digitalt sikkerhedsniveau, mens 9 pct. har et middel, og 84 pct. har et højt digitalt sikkerhedsniveau.



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

Som *figur 10* viser, har virksomheder, der arbejder med nye teknologier, generelt et højere digitalt sikkerhedsniveau sammenlignet med det gennemsnitlige niveau blandt alle SMV'erne. Men taget virksomhedernes risikoprofil i betragtning, må det siges at være en betydelig andel, at 22 pct. af SMV'erne og 7 pct. af de store virksomheder ikke har implementeret flere end 4 ud af de 9 it-sikkerhedsforanstaltninger. For selvom nye teknologier kan give nye sårbarheder og flere angrebsflader, skal virksomheder, der arbejder med nye teknologier, først og fremmest have styr på de traditionelle sikkerhedstiltag såsom stærke adgangskoder, risikoanalyse mfl.[22]. Ser man på de to helt essentielle sikkerhedstiltag (backup af data og opdatering af styresystemer), har 15 pct. af SMV'erne, der arbejder med de nye teknologier, ligeledes *ikke* implementeret disse[23]. Dette kan i særlig grad udgøre et problem, hvis disse virksomheder udsættes for en it-sikkerhedshændelse. Det gælder 5 pct. blandt de store virksomheder med 250+ ansatte.

Foruden de essentielle sikkerhedstiltag er risikoanalyse en helt afgørende sikkerhedsforanstaltning for virksomheder, der arbejder med Big Data, maskinlæring og IoT, da den danner hele udgangspunktet for at vide, hvordan man sikrer sin brug af de respektive teknologier[24]. Brugen af disse nye teknologier kan introducere nye sårbarheder og øge antallet af angrebsflader, hvilket kan ændre virksomhedernes overordnende risikoprofil. Risikoanalysen kan kaste lys over sandsynligheden for og de største risici ved digitale angreb ved brug af teknologierne - og derefter sørge for at man som virksomhed tager de passende forholdsregler for at forhindre potentielle angreb. På trods af dette laver blot 60 pct. af SMV'erne, der arbejde med IoT, 66 pct. af SMV'erne, der arbejder med Big Data, og 68 pct. af SMV'erne, der arbejder med maskinlæring, løbende risikoanalyser.

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

[23] Det gælder 16 pct. af virksomhederne, der anvender IoT, 12 pct. blandt virksomheder der arbejder med Big Data og 6 pct. blandt virksomheder der arbejder med maskinlæring.

[24] Se fx: Boston Consulting Group (2020): Vejledning: Tiltag til at sikre brugen af kunstig intelligens og Alexandra Instituttet (2020): Kan dit IoT produkt hackes.

Det er især virksomheder, der arbejder med IoT, som *ikke* har implementeret de essentielle sikkerhedstiltag, *ikke* gennemfører risikoanalyse, og som har et lavt digitalt sikkerhedsniveau. Én forklaring kan være, at virksomheder ofte har svært ved at placere ansvaret for IoT-sikkerheden i organisationen. Der er stor forskel på, hvordan virksomheder i praksis placerer denne opgave. Mange har stor tiltro til, at producenterne af IoT-enhederne har styr på it-sikkerheden, men de mangler ofte forudsætninger for at gå i dialog om dette og dermed vurdere sikkerheden i produkterne[25].

Det er positivt, at der overordnet set er højere digital sikkerhed blandt virksomheder, der arbejder med nye teknologier. Men tallene viser også, at der er potentiale for at løfte niveauet for den digitale sikkerhed i denne gruppe af virksomheder, som har mange angrebsflader, og hvor interessen kan være særlig høj for hackerne.

4. Sammenhæng mellem it-kompetencer og digital sikkerhed

Undersøgelser viser, at mangel på kompetencer er en af virksomhedernes største udfordringer i forhold til at styrke deres digitale sikkerhed[26]. Følgende afsnit belyser forholdet mellem varetagelse af it-sikkerhedsmæssige aktiviteter i de danske SMV'er sammenholdt med deres digitale sikkerhedsniveau.

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

VITA-data 2019 viser, at 70 pct. af SMV'erne udliciterer hele eller dele af deres it-sikkerhed til en ekstern leverandør. Denne andel ser nogenlunde ens ud på tværs af virksomhedsstørrelse, som vist i *figur 11*. En årsag til at SMV'erne vælger outsourcing kan være, at de ikke har de tilstrækkelige kompetencer på området til selv at kunne etablere og drive den nødvendige infrastruktur. Det gælder fx hos de mindre SMV'er, som ikke altid har etableret en it-afdeling eller kan forsvare udgiften til en intern specialiseret sikkerhedsekspert[27].

Selvom man vælger at outsource hele eller dele af sin it, er det fortsat vigtigt, at man som virksomhed forholder sig til og tager ansvar for sin digitale sikkerhed. Som virksomhed bør man stille krav til sin leverandør, fordi leverandøren bliver afgørende for, at virksomhedens systemer og data er sikre. I forbindelse med outsourcing er der således en række forhold, som man skal tage stilling til og aftale i en skriftlig kontrakt, så der er klarhed om, hvad leverandøren skal levere og under hvilke betingelser. Fx bør virksomheden ved indgåelse af kontrakt stille krav om databehandling, backup og andre grundlæggende sikkerhedsforanstaltninger samt fastlægge et passende niveau for kontrol af leverancerne.

[25] Alexandra Instituttet (2020): Kan dit IoT produkt hackes.

[26] Højbjerre Brauer Schultz (2019): Arbejdsmarkedet for informationssikkerhedskompetencer i Danmark og https://www.version2.dk/artikel/rapport-syv-ud-ti-nordiske-it-virksomheder-mangler-kvalificerede-sikkerhedsfolk-1089748

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

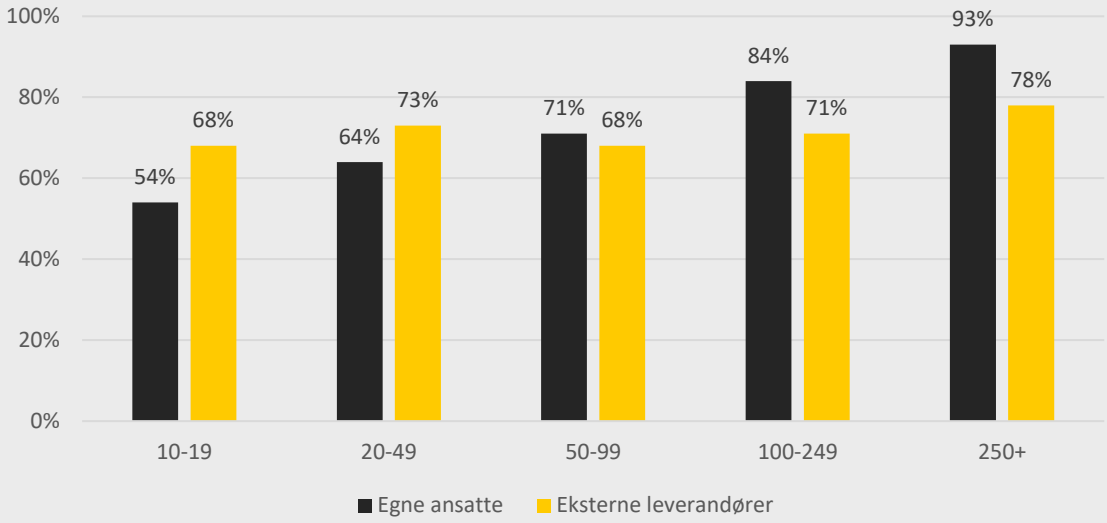
På trods af dette har kun 86 pct. af SMV'erne, der udliciterer deres digitale sikkerhed, stillet krav til deres leverandør om enten behandling af data, it-sikkerhedsforanstaltninger og/eller løbende dokumentation om fx it-sikkerhedsforanstaltninger[28]. Det betyder, at 14 pct. af virksomhederne *ikke* har stillet minimum ét af de tre krav til deres leverandør. Der er således en betydelig gruppe, som ikke får den nødvendige indsigt i, om leverandøren lever op til sine forpligtelser, og om deres digitale sikkerhed er i orden. På sikkerdigital.dk/virksomhed kan virksomheder downloade et dialogværktøj, der indeholder et skema med konkrete spørgsmål til it-leverandøren. Virksomheder kan sende skemaet til deres it-leverandør og bede dem besvare spørgsmålene for at få et overblik over leverandørens digitale sikkerhed i de løsninger, som virksomheden benytter sig af.

4.2 Flere store virksomheder har egne ansatte til at varetage it-sikkerhedsmæssige aktiviteter

61 pct. af SMV'erne får varetaget it-sikkerhedsmæssige aktiviteter af egne medarbejdere. Dette spørgsmål er bredt formuleret og kan både inkludere medarbejdere, der er ansat som it-sikkerhedsspecialister, men også ansatte, som varetager de it-sikkerhedsmæssige opgaver ved siden af andre arbejdsopgaver. Her er der i modsætning til outsourcing forskel på virksomhedens størrelse. Fx har blot 54 pct., blandt virksomheder med 10-19 ansatte, deres egne medarbejdere til at varetage it-sikkerhedsmæssige opgaver, mens det gælder hele 84 pct. blandt virksomheder med 100-249 ansatte. Til sammenligning har langt de fleste store virksomheder (93 pct.) egne ansatte til at udføre it-sikkerhedsmæssige opgaver. Forskellen kan, som tidligere beskrevet, skyldes, at de mindre virksomheder ikke har de tilstrækkelige ressourcer til at ansætte en it-ansvarlig, men det kan også skyldes manglende ledelsesprioritering i og med, at de mindre virksomheder ikke føler sig i risikogruppen for cyberangreb og ikke anser sig selv som et interessant mål for hackerne.

[28] Blandt SMV'er, der udliciterer sin it-sikkerhed, stiller 81 pct. krav om behandling af data, 77 pct. stiller krav om it-sikkerhedsforanstaltninger og 61 pct. stiller krav om løbende dokumentation (86 pct. stiller minimum ét ud af de tre krav)

Figur 11. Udførelse af it-sikkerhedsmæssige aktiviteter, fordelt på størrelse



Note: Tallene summerer ikke til 100 pct., da nogle virksomheder både benytter egne ansatte og eksterne leverandører til udførelse af it-sikkerhedsmæssige aktiviteter.
Note: Dette spørgsmål er ikke besvaret af mikrovirksomheder med under 10 ansatte, som derfor ikke er med i opgørelsen.
Kilde: Egne beregninger baseret på tal fra Danmarks Statistik.

Der er ligeledes stor forskel på, hvordan de forskellige brancher vælger at placere deres it-sikkerhedsmæssige opgaver. Inden for branchen 'Bygge og anlæg' ser vi en tendens til, at mange virksomheder vælger at udlicitere deres it-sikkerhedsmæssige opgaver (76 pct.), hvorimod blot 43 pct. har egne ansatte til dette. Det modsatte gør sig gældende inden for branchen 'Information og kommunikation', hvor hele 95 pct. af SMV'erne har egne ansatte til at varetage it-sikkerhedsmæssige opgaver, og blot 53 pct. vælger at udlicitere disse opgaver til en ekstern leverandør.

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 38 pct. af SMV'erne *både* egne ansatte og eksterne leverandører til at varetage it-sikkerhedsaktiviteter, 32 pct. har *kun* eksterne leverandører, og 23 pct. har *kun* egne ansatte til at varetage it-sikkerhedsaktiviteter, mens 7 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, har (kontrolleret for størrelse og branche) et signifikant højere digitalt sikkerhedsniveau end alle øvrige virksomheder, mens den mindre gruppe af virksomheder, der *hverken* har egne ansatte eller eksterne leverandører, har et signifikant lavere digitalt sikkerhedsniveau end øvrige virksomheder[29]. Blandt denne mindre gruppe af virksomheder, som hverken har egne eller eksterne til at varetage it-sikkerhedsmæssige opgaver, har over halvdelen (60 pct.) af virksomhederne

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

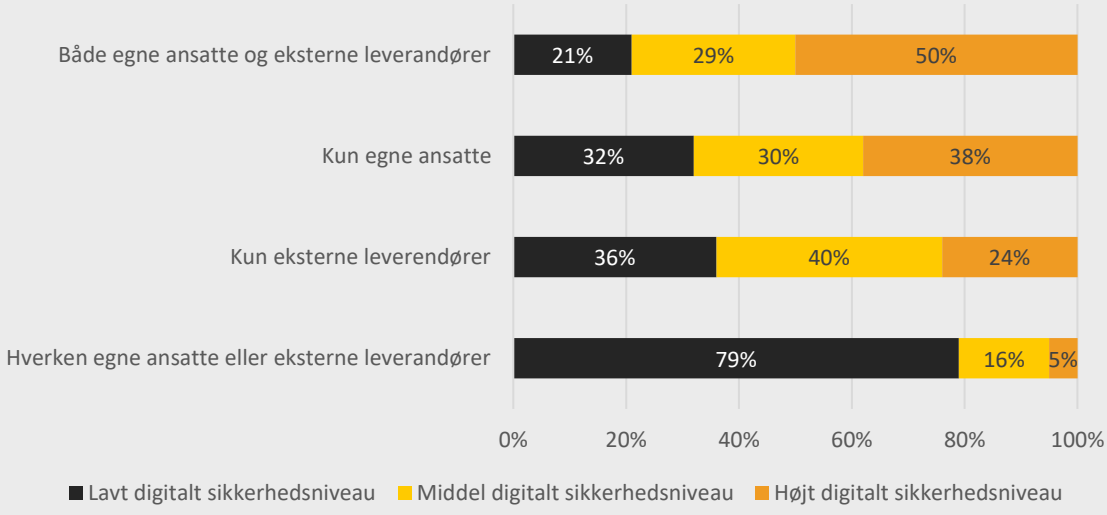
ikke implementeret de to helt essentielle sikkerhedstiltag, mens hele 79 pct. har et lavt digitalt sikkerhedsniveau ifølge analysens operationalisering, jf. *figur 12*.

Mikrovirksomheder med under 10 ansatte har ikke besvaret dette spørgsmål, så resultaterne gælder for virksomheder med 10 ansatte eller derover. Man må dog forvente, at samme tendens gør sig gældende blandt mikrovirksomhederne, da særligt de mindre virksomheder med 10-19 ansatte hverken har egne eller eksterne til at varetage it-sikkerhedsmæssige aktiviteter.

At nogle virksomheder ikke har medarbejdere til at varetage it-sikkerhedsmæssige opgaver kan skyldes, at flere af de små og mellemstore virksomheder, som tidligere beskrevet, ikke føler sig i risikogruppen for angreb og ikke anser sig selv som et interessant mål for hackerne. Dette underbygges af et virksomhedsinterview, som PwC har gennemført for Erhvervsstyrelsen ifm. en dataindsamling om SMV'ers viden om digital sikkerhed. Heri forklarer respondenten, at virksomheden ikke fokuserer på eller ved meget om it-sikkerhed, fordi den ikke har nogle it-ansatte, og at virksomheden heller ikke er et interessant mål for it-kriminelle. Det handler derfor om at gøre virksomhederne opmærksomme på, at alle kan rammes, hvis sikkerhedsniveauet i denne gruppe skal løftes.

Ser man på, hvorvidt virksomheder har egne ansatte *eller* eksterne leverandører til at varetage it-sikkerhedsmæssige opgaver, er der langt flere blandt de mindre SMV'er, der udelukkende benytter eksterne leverandører. Det gælder fx 38 pct. af virksomhederne med 10-19 ansatte, og 14 pct. af virksomhederne med 100-249 ansatte. Omvendt anvender de større SMV'er i højere grad egne ansatte. Men selv ved kontrol for størrelse og branche findes der ikke en signifikant forskel på virksomhedernes sikkerhedsniveau, alt efter om det er egne ansatte eller eksterne leverandører, som varetager de it-sikkerhedsmæssige aktiviteter. At der *ikke* er en signifikant forskel, er dog i sig selv interessant og kan tyde på, at det ikke handler om, hvorvidt virksomheden selv udfører deres it-sikkerhedsopgaver, eller om disse udliciteres, så længe it-sikkerhed prioriteres, og der er en eller flere personer, der har ansvaret for dette i eller uden for virksomheden.

Figur 12. Udførelse af it-sikkerhedsmæssige aktiviteter og digitalt sikkerhedsniveau



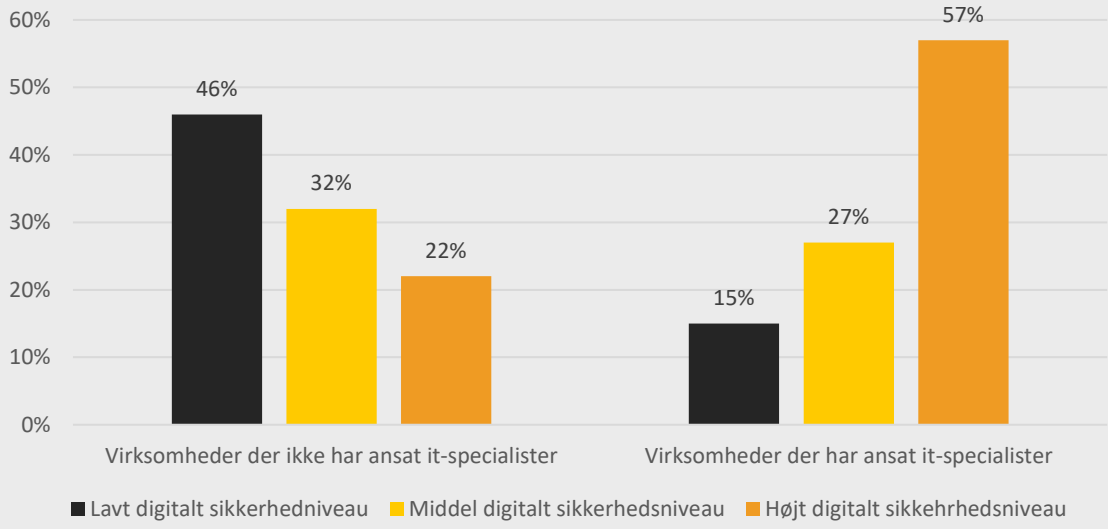
Note: Dette spørgsmål er ikke besvaret af mikrovirksomheder med under 10 ansatte, som derfor ikke er med i opgørelsen.
Kilde: Egne beregninger baseret på tal fra Danmarks Statistik

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, har et højere niveau af digital sikkerhed end virksomheder, der ikke beskæftiger it-specialister. Denne forskel er statistisk signifikant kontrolleret for virksomhedsstørrelse og branche. Der ses især en forskel på andelen af virksomheder med et højt sikkerhedsniveau, da niveauet opnås af hele 57 pct. af SMV'erne med it-specialister ansat, i kontrast til 22 pct. af SMV'erne, der ikke har it-specialister ansat. Ser man på de to essentielle sikkerhedstiltag (systematisk opdatering og backup af data), har hele 88 pct. af virksomhederne, som har it-specialister ansat, implementeret disse, hvilket blot gælder for 71 pct.af virksomhederne, der ikke har ansat it-specialister.

Et markant højere sikkerhedsniveau blandt virksomheder, der har ansat it-specialister, kan muligvis forklares med, at virksomheder, der generelt er meget digitale, og virksomheder med en højere risikoprofil for angreb har et større incitament til at ansætte it-specialister. Det kan dog også skyldes, at it-specialister i højere grad er opmærksomme på it-sikkerhed og har kompetencerne til at implementere it-sikkerhedstiltag.

Figur 13. Ansættelse af it-specialister og digitalt sikkerhedsniveau



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik

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 ikke nemt at rekruttere disse specialister. I VITA-besvarelserne fra 2019 har 13 pct. af SMV'erne rekrutteret eller forsøgt at rekruttere it-specialister i 2018. Heriblandt har hele 59 pct. haft vanskeligt herved. Sammenligner man med de store virksomheder med over 250 ansatte, har 61 pct. rekrutteret eller forsøgt at rekruttere it-specialister i 2018, hvoraf 67

pct. har haft vanskeligt ved at rekruttere it-specialister til deres ledige stillinger. Der tegner sig således et kompetencebehov på tværs af alle virksomhedsstørrelser.

Dette resultat understøttes af en undersøgelse fra 2019, som viser, at hver femte organisation på tværs af det private og det offentlige, der har forsøgt at rekruttere en person med informationssikkerhedskompetencer, herunder it-sikkerhed, enten ikke har kunnet ansætte en it-specialist eller har måttet ansætte en profil, som ikke havde alle de ønskede kompetencer [30].

5. Oplevede barrierer ved implementering af it-sikkerhedsløsninger

Blot 7 pct. af SMV'erne angiver, at de har været forhindret i, begrænset af eller oplevet udfordringer for at anvende it-sikkerhedsløsninger i 2018.

Det er primært de store virksomheder med et højt digitalt sikkerhedsniveau, som har oplevet disse udfordringer. En forklaring kan være, at jo mere 'modne' virksomheder er ift. deres digitale sikkerhed, des mere støder de på forhindringer i forhold til at implementere sikkerhedsløsninger. Tallene kan derfor afspejle, at de fleste virksomheder ikke har oplevet udfordringer, fordi de ikke har implementeret it-sikkerhedsforanstaltninger. Den store udfordring ligger i så fald i, at få virksomhederne til at få øjnene op for emnet.

5.1 Mangel på viden og kompetencer opleves som de største barrierer

Figur 14 viser, hvilke udfordringer virksomhederne typisk oplever. Som det fremgår, er den største udfordring 'manglende it-kendskab og kompetencer til at håndtere it-sikkerhedsløsninger'. Det understøtter resultaterne i afsnit 4 om, at virksomhedernes it-sikkerhed i høj grad afhænger af de rette kompetencer til at varetage virksomhedens digitale sikkerhed. Her er det også interessant at sammenligne resultaterne fra 2017 til 2018, som indikerer, at netop mangel på viden og kompetencer er en udfordring, der ser ud til at stige med årene.

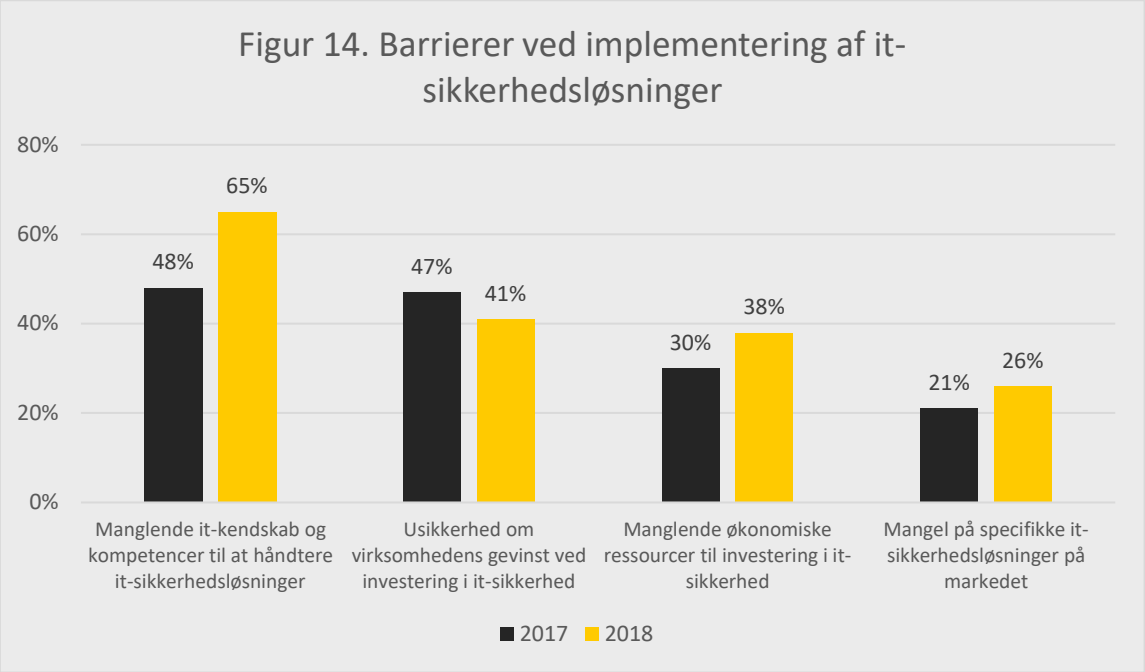
Det skal dog bemærkes, at de udvalgte kategorier ikke nødvendigvis er udtømmende, og at det ikke har været muligt for virksomhederne at svare 'andet' i 2019[31]. Der kan således være andre væsentlige barrierer, som denne analyse ikke har med. Andre lignende analyser er blandt andet kommet frem til, at ledelsens stillingtagen til it-sikkerhed og medarbejderkulturen i virksomheden kan være barrierer i forhold til at implementere digitale sikkerhedstiltag[32]. Fx angiver 17 pct. af SMV'erne, i data indsamlet af PwC for Erhvervsstyrelsen, at der ikke er nok ledelsesmæssigt fokus på it-sikkerhed[33].

[30] Højbjerre Brauer Schultz (2019): Arbejdsmarkedet for informationssikkerhedskompetencer i Danmark

[31] En stor andel virksomheder svarede 'andet' i 2018. Noget tyder derfor på, at kategorierne ikke er udtømmende.

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

[33] Analysen baserer sig på 1252 kvalitative web- og telefoninterviews og 30 kvalitative interviews blandt SMV'er. Analysen er ikke offentliggjort.



Note: Mikrovirksomheder med 5-9 ansatte har ikke besvaret dette spørgsmål. Resultaterne i 2018 er derfor sammenlignelige med resultaterne i 2017, da populationen i begge år er beregnet for SMV'er med 10-249 ansatte.
Note: I 2017 indgik også svarmuligheden 'andet' med en svarprocent på 48 pct.
Note: Tallene summerer ikke til 100 pct., da virksomheden har kunne angive flere svarmuligheder.
Kilde: Egne beregninger baseret på tal fra Danmarks Statistik

Overordnet set peger resultaterne i dette afsnit på et behov for at udbrede viden om digital sikkerhed til danske SMV'er samt hjælpe dem med at rekruttere de rette kompetencer til at implementere it-sikkerhedsforanstaltninger.

5.2 Vejledninger til styrkelse af digital sikkerhed

Nedenstående boks giver et overblik over nogle af de tilbud, som virksomhederne kan benytte med henblik på at styrke deres digitale sikkerhed.

Tabel 2. Vejledninger, som kan styrke den digitale sikkerhed i virksomheder (gratis)

Sikkerdigital.dk/virksomhed	Sikkerhedstjekket.dk	Varslingsapp: mit digitale selvforsvar
På sitet kan virksomhederne få viden, vejledning og konkrete værktøjer, som styrker den digitale sikkerhed. Der sættes fx fokus på de største trusselstyper, hvordan man forebygger cyberangreb, vigtigheden af god digital medarbejderadfærd og operationelle råd, som styrker virksomhedens digitale sikkerhed - både teknisk og organisatorisk. Se mere på sikkerdigital.dk/virksomhed	Sikkerhedstjekket starter med 5 spørgsmål, som bruges til at finde virksomhedens risikoprofil. Herefter kommer 17 testspørgsmål fordelt på 5 temaer. På baggrund af virksomhedens risikoprofil og svarene i testspørgsmålene, får virksomheden en individuel rapport, som viser, hvor det er vigtigst at sætte ind for at forbedre virksomhedens digitale forsvar. Tag testen HER	Forbrugerrådet TÆNK tilbyder den gratis app Mit Digitale Selvforsvar, som hjælper dig med at være sikker online og holder dig opdateret på digitale trusler. Se mere om Mit Digitale Selvforsvar

6. It-sikkerhedshændelser i danske SMV'er

Samlet set har 9 pct. af SMV'erne angivet, at de har oplevet en it-sikkerhedshændelse i løbet af 2018. Dette tal stiger med virksomhedsstørrelse og spænder bredt fra 7 pct. blandt virksomheder med 5-9 ansatte til 18 pct. blandt virksomheder med 100-249 ansatte. Til sammenligning har 27 pct. af de store virksomheder med 250+ ansatte oplevet en it-sikkerhedshændelse i 2018.

Tallenes nøjagtighed er dog forbundet med en høj grad af usikkerhed, og forskellige undersøgelser har vist et bredt spænd af oplevede it-sikkerhedshændelser fra 9 pct. til 51 pct. i danske virksomheder[34]. Én af forklaringerne er, at der ofte er mørketal betonet med sikkerhedshændelser, da mange virksomheder er tilbageholdende med at dele, hvis de har været udsat for en sikkerhedshændelse. Ligeledes vil der være virksomheder, som ikke har opdaget, at de har oplevet en it-sikkerhedshændelse, hvis der fx er tale om spyware, der ligger gemt i virksomhedens systemer. Disse mørketal kan derfor betyde, at analysen underestimerer problemets omfang.

Herudover er svarkategorierne for it-sikkerhedshændelser ikke helt udtømmende i denne analyse. Selvom svarkategorierne er brede og således indfanger mange former for it-sikkerhedshændelser, spørges der ikke til betalingssvindel herunder CEO fraud, hvor formålet for de kriminelle er at franarre oplysninger eller store pengeoverførsler fra ansatte ved at udgive sig som virksomhedens direktør. Ifølge PwC's cybercrime survey 2019 er dette én af de hyppigste sikkerhedshændelser blandt danske virksomheder[35]. Endelig kan omfanget af it-sikkerhedshændelser afhænge af målgruppen og spørgsmålsformuleringerne i de forskellige analyser.

I stedet for at hæfte sig ved andelen af virksomheder, der oplever sikkerhedsbrud, er det derfor mere interessant at se på, hvilke brud virksomhederne oplever samt konsekvenserne heraf.

[34] Tal baseret på denne undersøgelse og PwCs Cybercrime survey 2019.

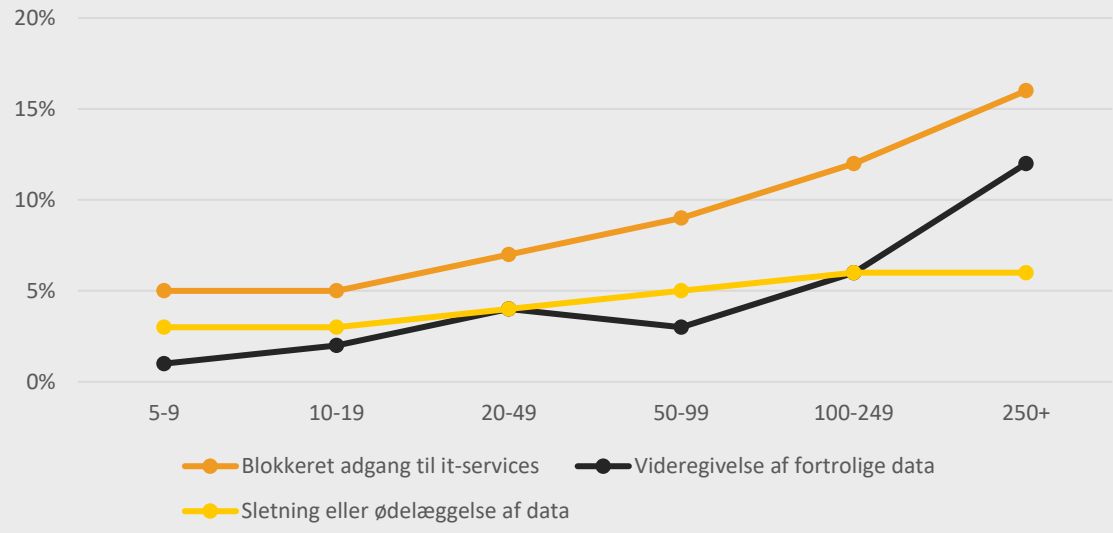
[35] PWC: Cybercrime Survey 2019.

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

Figur 15 viser, hvilke sikkerhedshændelser virksomhederne oplever. På tværs af virksomhedsstørrelse oplever størstedelen af virksomhederne blokeret adgang til it-service (fx Denial of Service-angreb, ransomware-angreb og hardware- eller softwarefejl). Det er problematisk, da virksomhederne er meget afhængige af deres systemer og dataadgang for at kunne varetage kerneopgaver. For eksempel viser data indsamlet af PwC for Erhvervsstyrelsen i 2019, at 41 pct. af virksomhederne kun kan varetage virksomhedens primære opgaver under en halv arbejdsdag uden adgang til virksomhedens it-systemer og/eller data. Det gælder for hele 58 pct. af virksomhederne inden for branchen 'information og kommunikation'[36].

Sammenlignet med SMV'erne oplever 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. Det understreger blot behovet for kontinuerlig træning af virksomhedens medarbejdere. Som vi så *i figur 8* i afsnit 2, gennemfører 31 pct. af SMV'erne og 69 pct. af de store virksomheder obligatorisk træning og uddannelse af deres medarbejdere. Der er således potentiale for at øge denne træning blandt SMV'erne såvel som hos de store virksomheder.

Figur 15. Typer af it-sikkerhedshændelser fordelt på virksomhedsstørrelse



Kilde: Egne beregninger baseret på tal fra Danmarks Statistik

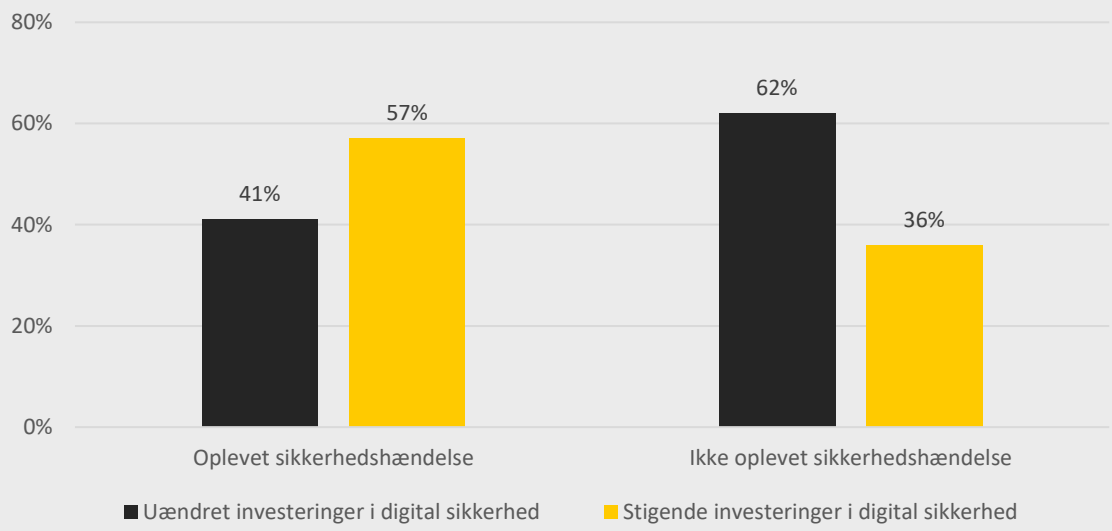
[36] Dataindsamlingen baserer sig på 1.252 kvalitative web- og telefoninterviews og 30 kvalitative interviews blandt SMV'er. Dataindsamlingen er ikke offentliggjort.

6.2 Virksomheder, der har oplevet en it-sikkerhedshændelse, investerer mere i it-sikkerhed

De virksomheder, som har oplevet en it-sikkerhedshændelse i 2018, har også investeret mere i it-sikkerhed i samme år, som illustreret i nedenstående *figur 16*. Denne sammenhæng er signifikant og gælder på tværs af virksomhedsstørrelser. Dette resultat understøttes af en række case interviews, som Deloitte har gennemført i en tidligere analyse for Erhvervsstyrelsen. Heri beskriver de deltagende virksomheder, hvordan et it-sikkerhedsbrud gjorde konsekvenserne meget håndgribelige for ledelsen og medarbejderne, og det blev klart, hvordan det påvirkede virksomheden, og dermed understregede vigtigheden af it-sikkerhed[37].

Resultatet stemmer også overens med data, som PwC har indsamlet for Erhvervsstyrelsen i 2019[38], der viser, at flere virksomheder generelt føler sig sikre, fordi de endnu ikke har oplevet digitale sikkerhedsbrud. De virksomheder, der har været udsat for cyberangreb eller forsøg herpå, føler sig derimod mere i risikogruppen og italesætter, at alle virksomheder er i risikogruppen.

Figur 16. It-sikkerhedshændelser og investeringer i it-sikkerhed



Note: Tallene summerer ikke til 100 pct., da 2 pct. havde faldende udgifter.
Kilde: Egne beregninger baseret på tal fra Danmarks Statistik

En sikkerhedshændelse kan således fungere som en drivkraft for at øge den digitale sikkerhed i virksomheden. Optimalt set skal virksomhederne dog få øjnene op for eventuelle konsekvenser og forebygge disse angreb, før skaden er sket. Resultatet peger derfor på et behov for at øge virksomhedernes opmærksomhed på konsekvenserne ved et angreb og nødvendigheden ved at implementere forebyggende tiltag i tide. Som beskrevet er der mange SMV'er, der ikke føler sig i risikogruppen for

[37] Monitor Deloitte for Erhvervsstyrelsen (2018): IT-sikkerhed og datahåndtering i danske SMV'er
[38] Analysen baserer sig på 1.252 kvalitative web- og telefoninterviews og 30 kvalitative interviews blandt SMV'er. Analysen er ikke offentliggjort.

cyberangreb. Derfor ligger der også et potentiale i at udbrede forståelsen for, at alle virksomheder kan rammes af sikkerhedsbrud. Blandt andet derfor har Erhvervsstyrelsen i samarbejde med Industriens Fond samlet en række cases på mindre virksomheder, der på forskellig vis fik øget fokus på digital sikkerhed efter et angreb. Historierne kan ses og læses på: Sikkerdigital.dk/virksomhed.

7. Metode

Virksomhedernes digitale niveau måles via den årlige undersøgelse 'IT-anvendelse i virksomhederne' (VITA). I alt indgår 5.292[39] virksomheder i undersøgelsen, som gennemføres af Danmarks Statistik. Virksomhederne i undersøgelsen har minimum 5 årsværk og tilhører de private, ikke-finansielle byerhverv.

I analysen benyttes vægtet data således, at stikprøven afspejler den fulde population af virksomheder med minimum 5 årsværk inden for de private, ikke-finansielle byerhverv. Analysen er gennemført på grundlag af det nyeste tilgængelige data indsamlet i VITA 2019, som repræsenterer situationen i de adspurgte virksomheder i 2018. Det skal hertil bemærkes, at cybertrusler og digital sikkerhed er områder i hastig udvikling generelt – og særligt i lyset af det udvidet fokus på cybersikkerhed, som der har været i forbindelse med Corona-pandemien. Der kan derfor være sket en del på området siden dataindsamlingen i 2019, hvilket der må tages forbehold for ved læsning af analysens resultater.

Det skal herudover bemærkes, at VITA-data er baseret på selvrapporterede besvarelser. Selvevaluering siger noget om udfylderens egen opfattelse, af fx deres digitale sikkerhed, hvilket kan variere fra deres reelle niveau. Dette er dog en metodisk udfordring i samtlige analyser, der baserer sig på selvrapporteret survey data. I denne analyse mindskes denne udfordring ved, at besvarelserne er anonyme, således at virksomhedens svar, og dermed sikkerhedsniveau, ikke er tilgængelige for kunder, leverandører, samarbejdspartnere osv. Herudover er spørgsmålene formuleret meget konkrete, så der er mindst muligt overladt til svarpersonens egen fortolkning. Fx bliver der spurgt til implementeringen af 10 konkrete tekniske it-sikkerhedstiltag (fx om virksomheden gennemfører backup af data), frem for om virksomheden har et 'tilstrækkeligt' digitalt sikkerhedsniveau.

7.1 Måling af digital sikkerhed

I VITA 2019 spørges der ind til, hvorvidt virksomhederne har implementeret 10 digitale 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. Analysen siger således intet om, hvorvidt de valgte teknologier eller sikkerhedstiltag benyttes korrekt og i tilstrækkelig grad. Blot om de benyttes eller ej.

Spørgsmål om digital sikkerhed i VITA 2019

Bruger virksomheden følgende it-sikkerhedsmæssige foranstaltninger?

[39] Analysen fokuserer primært på de små og mellemstore virksomheder med 5-249 ansatte, som udgør 4.802 af besvarelserne i datasættet.

- Stærke adgangskoder til autentificering. *Dvs. minimumslængde på 8 blandede karakterer og periodevis ændring af adgangskode.*
- Systematisk opdatering af software (inkl. styresystemer).
- Biometriske metoder til bruger-identifikation og autentifikation. *Fx baseret på fingeraftryk, stemmegenkendelse eller ansigtsscanning.*
- Kryptering af data, filer eller e-mails.
- Backup af data til en alternativ geografisk placering. *Herunder backup som cloud computing service.*
- Adgangskontrol til netværk. *Styring af adgang fra digitale enheder og brugere af virksomhedens netværk.*
- VPN (virtuelt privat netværk). *VPN-teknologi skaber en sikker forbindelse til udveksling af data via internettet.*
- Lagring af logfiler. *Fx til analyse efter it- sikkerhedshændelser.*
- Risikoanalyse. *Periodevis vurdering af sandsynlighed og konsekvenser for it-sikkerhedsmæssige hændelser.*
- Tests af It-sikkerhed. *Fx penetrationstest, test af it-sikkerhedsalarmer og backup systemer samt evaluering af it-sikkerhedsmæssige forhold.*

Foruden måling af de enkelte sikkerhedstiltag bruges der i analysen et samlet indeks, som måler virksomhedernes digitale sikkerhedsniveau på tværs af de forskellige tiltag. Sikkerhedsforanstaltningen 'biometriske metoder til brugeridentifikation' er taget ud af den samlede liste af it-sikkerhedstiltag, som virksomhederne er spurgt ind til. Dette skyldes bl.a., at det er det eneste tiltag, der ikke beskrives som et nødvendigt tiltag af Center for Cybersikkerhed og Digitaliseringsstyrelsen i deres tekniske minimumskrav eller i deres vejledning "Cyberforsvar der virker"[40]. I de tekniske minimumskrav nævnes biometrisk identifikation kun på grund af, at der stilles krav om *enten* minimum længde og anvendelse af numerisk kode eller biometrisk identifikation til beskyttelse af telefoner. Det kan også være én af årsagerne til, at netop denne sikkerhedsforanstaltning blot anvendes af 11 pct. af virksomhederne. Indekset er således baseret på de 9 resterende tekniske sikkerhedsforanstaltninger. De 9 sikkerhedstiltag i denne analyse skal ikke ses som en udtømmende liste af sikkerhedsforanstaltninger, men de skal i stedet anses som en proxy for virksomhedernes digitale niveau.

Det samlede indeks, til måling af virksomhedernes digitale sikkerhedsniveau, er bygget op omkring, hvor mange sikkerhedsforanstaltninger virksomhederne anvender. Der ses på antallet af foranstaltninger, fordi der ikke findes en entydig definition på, hvilke der er vigtigst for virksomhederne. Dog anses to sikkerhedsforanstaltninger som værende helt centrale[41], ligesom de også indgår i langt de fleste anbefalinger for it-sikkerhed. Disse sikkerhedstiltag er 'Backup af data' og 'Systematisk opdatering af software'. En backup-procedure gør det muligt for virksomheden at få sine systemer relativt hurtigt op at køre igen efter et eventuelt sikkerhedsangreb. Samtidig er systematisk opdatering

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

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

af software central for virksomhedens sikkerhed, da systemer og programmer løbende repareres for fejl og "sikkerhedshuller", og derved reduceres muligheden for digitale sikkerhedsangreb[42]. Disse to sikkerhedsforanstaltninger er derfor udvalgt til at 'diskvalificere' en virksomheds digitale sikkerhedsniveau. Det vil sige, at virksomheden automatisk defineres med et lavt digitalt sikkerhedsniveau, uanset hvilket digitalt sikkerhedsniveau denne virksomhed måtte have hvis virksomheden mangler et af de to centrale sikkerhedstiltag. Dette er i tråd med en tidligere analyse, som Deloitte har udarbejdet for Erhvervsstyrelsen[43]. De to sikkerhedstiltag (backup af data og systematisk opdatering af software) rapporteres som 'essentielle sikkerhedstiltag' igennem rapporten.

Der findes heller ikke en entydig definition på, hvor mange sikkerhedsforanstaltninger en virksomhed bør implementere, hvilket ligeledes afhænger af den enkelte virksomhed og dens risikoprofil. I denne analyse er de 9 sikkerhedstiltag opdelt i følgende tre kategorier: lavt, middel og højt digitalt sikkerhedsniveau. Et lavt digitalt sikkerhedsniveau defineres som virksomheder, der har implementeret under halvdelen af de 9 anbefalede sikkerhedstiltag. Et middel digitalt sikkerhedsniveau defineres som virksomheder, der har implementeret 5-7 af de tekniske sikkerhedstiltag, mens et højt niveau defineres som virksomheder, der har implementeret 8-9 af de tekniske sikkerhedstiltag, som er anbefalet til virksomhederne. Dermed ser operationaliseringen for digitalt sikkerhedsniveauet således ud:

Lavt digitalt sikkerhedsniveau	Middel digitalt sikkerhedsniveau	Højt digitalt sikkerhedsniveau
Implementering af 0-4 sikkerhedsforanstaltninger + virksomheder, der ikke har implementeret de to essentielle sikkerhedstiltag	Implementering af 5-7 sikkerhedsforanstaltninger. På nær virksomheder, der ikke har implementeret de to essentielle sikkerhedstiltag	Implementering af 8-9 sikkerhedsforanstaltninger. På nær virksomheder, der ikke har implementeret de to essentielle sikkerhedstiltag

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

Ud fra VITA-data er det ikke muligt at beregne virksomhedernes risikoprofil (dvs. hvor alvorlig en it-sikkerhedshændelse vil være for virksomheden, og hvor stor sandsynlighed der er for, at virksomheden bliver ramt). Derfor siger analysen således noget om virksomhedernes digitale sikkerhedsniveau uden at konkludere, hvorvidt dette niveau er tilstrækkeligt. I afsnit 3 fungerer virksomhedernes brug af nye teknologier som en proxy for virksomhedens risikoprofil, da man vil forvente, at virksomheder, der arbejder med maskinlæring, Big data og IoT, ofte vil være i besiddelse af store digitale datamængder, som kan give nye angrebsflader og større konsekvenser ved angreb, som uddybet i afsnittet.

7.2 Definitioner på nye teknologier og brug heraf

Til at afdække hvorvidt virksomhederne arbejder med nye teknologier, er der i analysen taget udgangspunkt i følgende tre teknologier; Big Data, IoT og Maskinlæring. Som ved it-sikkerhedstiltag spørges der *ikke* ind til, i hvilken grad disse teknologier anvendes, men blot om de anvendes

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

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

(virksomhederne svarer ja/nej til en række parametre). Det er således ikke muligt at måle, i hvilken grad virksomhederne anvender de respektive teknologier. Nedenfor gennemgås analysens definitioner på de tre teknologier og virksomhedernes brug heraf.

1. Big Data:

Big Data defineres i undersøgelsen som:

- Big Data er brugen af teknikker, teknologier og software værktøjer til analytisk behandling af big data, der kan stamme fra virksomhedens egne kilder eller fra andre kilder.
- Big Data genereres ved aktiviteter, der foregår elektronisk, og ved maskine-til-maskine kommunikation, fx data fra brug af sociale medier eller fra produktionsprocesser.
- Big Data er typisk karakteriseret ved:
    - 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, geolokationsdata mv.).
    - Høj hastighed: Big data genereres typisk konstant og hastigheden, hvormed data opdateres, og nye informationer er tilgængelige, er derfor meget høj.

Brug af bigdata tæller virksomheder, der har anvendt Big Data fra minimum én af følgende kilder:

- 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.

2. Internet of Things

Internet of Things (IoT) defineres i undersøgelsen som:

- Internetforbundne sensorer, der er selvstændigt forbundet med internettet og kan opsamle og videregive informationer ad den vej samt evt. selv handle på baggrund af de samme informationer.
- Sensorer, der eksempelvis måler, registrerer eller styrer tryk, bevægelse, temperatur, fugtighed, lyd, vibrationer, hastighed, position og nærhed.
- Sensorer, der ikke er koblet på internettet, er ikke omfattet af denne undersøgelse.

Brug af IoT tæller virksomheden, der anvender sensorer, der er koblet til internettet til følgende formål:

- Sikkerheds- og adgangskontrol. *Fx sensorer, der monitorerer adgang til bestemte områder og via internettet videregiver informationer om ikke-autoriseret adgang, herunder indbrud.*

- Måling, registrering eller styring af vareproduktion. *Fx sensorer, der monitorerer industrimaskiner og via internettet videresender informationer om funktionsfejl.*
- Måling, registrering eller styring af temperatur, tryk og luft. *Fx sensorer, der monitorerer og via internettet videresender informationer om temperaturniveau og -ændringer.*
- Måling, registrering eller styring af lagre. *Fx sensorer, der monitorerer og via internettet videresender informationer om lager- eller varebeholdning.*
- Overvågning af varer og logistikkontrol. *Fx sensorer, der monitorerer og via internettet videresender informationer om en bestemt vares placering eller rystelser mv. i forbindelse med transport af varer.*
- Forbedring af eksisterende produkter og services. *Fx på baggrund af indsamling og analyse af data fra sensorer, der via internettet videresender informationer om brugeradfærd, performance mv. fra et bestemt produkt eller en service i anvendelse.*
- Udvikling af nye produkter og services. *Fx på baggrund af indsamling og analyse af data fra sensorer, der via internettet videresender informationer om brugeradfærd, performance mv. fra et bestemt produkt eller en service i anvendelse.*
- Andre formål.

3. Maskinlæring og kunstig intelligens

Maskinlæring og kunstig intelligens defineres i undersøgelsen som:

- Maskinlæring (Machine Learning) og kunstig intelligens er software til dataanalyse, der finder mønstre og sammenhænge i data. Eksempler kan være automatiseret markedsføring, autogenerering af årsrapport, chatbots mm. baseret på tekst, billede, lyd eller numeriske data.

Brug af maskinlæring og kunstig intelligens inkluderer virksomheder, der anvender maskinlæring og kunstig intelligens fra følgende datakilder:

- Intern data fra virksomhedens egne systemer. *Fx sensordata fra virksomhedens maskiner, data for kundeadfærd og regnskabsdata.*
- Offentlige data. *Fx data fra offentlige myndigheder om geografiske forhold, vejr, virksomheder, indkomster, bopæl, mv.*
- Data fra internettet. *Fx data fra sociale medier som Google+, Twitter, Facebook og lign.*

Erhvervsstyrelsen

Langelinie Allé 17
2100 København Ø

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