Erhvervsstyrelsen

Digital sikkerhed i praksis

En analyse af danske små og mellemstore virksomheder

Marts 2022

Epinion

Indhold

ERHVERVSSTYRELSEN

Baggrund og formål

Epinion

Analysen er udført med henblik på at afdække it-sikkerhedspraksis og relevansen af forskellige tilbud om hjælp til it-sikkerhed målrettet danske SMV'er

It-sikkerhed blandt danske SMV'er

- En stor del af danske SMV'er er sårbare over for it-kriminalitet og it-sikkerhedshændelser*.
- Brud på it-sikkerheden kan have store omkostninger for den enkelte virksomhed og i yderste konsekvens betyde, at en virksomhed mister sit forretningsgrundlag og må dreje nøglen om.
- I efteråret 2020 viste segmenterings-analysen, at 27 pct. af de danske SMV'er én eller flere gange har været udsat for en it-sikkerhedshændelse.

Interesse for eksisterende tilbud

- Allerede i dag eksisterer der en række tilbud om vejledning og hjælp til it-sikkerhed i de danske virksomheder. Blandt andet på portalen sikkerdigital.dk.
- Sikkerdigital.dk er forankret i Erhvervs- og Digitaliseringsstyrelsens indsats for at tilbyde borgere, virksomheder og myndigheder viden, vejledning og konkrete værktøjer til en sikker digital hverdag.

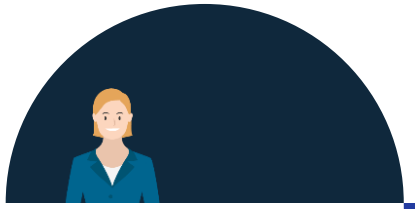
Analysen 'Digital sikkerhed i praksis'

- For at afdække it-sikkerhedspraksis samt relevansen af eksisterende tilbud har Epinion gennemført en analyse blandt danske SMV'er.
- Undersøgelsen bygger på 1.011 repræsentativt udvalgte virksomheder med 5-250 ansatte suppleret med 12 kvalitative interviews blandt målgruppen.
- Udgangspunktet for analysen er et spørgeskema, som relevante ansatte fra virksomhederne har besvaret.
- Respondenter og interviewpersoner er rekrutteret via invitationer på e-Boks i perioden 30. november 2021 til 14. december 2021.

*Note: *Begrebet it-sikkerhed skal i det følgende forstås som et begreb, der dækker over tekniske sikkerhedsforanstaltninger, men også processer og andre organisatoriske tiltag i virksomheden, som har med beskyttelse af informationer og it-systemer at gøre. Med hændelse menes derved utilsigtet eller uautoriseret adgang, ændring eller ødelæggelse af data, software, hardware eller it-systemer generelt.*

Analysen ‘Digital sikkerhed i praksis’ tager afsæt i segmenteringsanalysen, der blev lavet for Erhvervsstyrelsen i efteråret 2020

11%



De digitale

Virksomhederne med mest data og mest avancerede teknologier, og derfor også nogle af de mest it-sikre og opmærksomme grundet deres store sårbarhed. Efterspørger mere viden om konkrete brud, og hvor stor risikoen for et nedbrud er, men også trænings-værktøjer, som kan gøre medarbejderne mere opmærksomme på it-sikkerhed.

De sikkerhedsparate

Virksomheder, som er opmærksomme på it-sikkerhed, og er klar over, at de skal gøre noget herunder investere i it-sikkerhed. De mangler indblik i hvilke risici, de står overfor og hvor de skal starte. Arbejdet foregår i mindre grad på kontorer, og derfor flyttes fokus fra det digitale i hverdagen.

14%

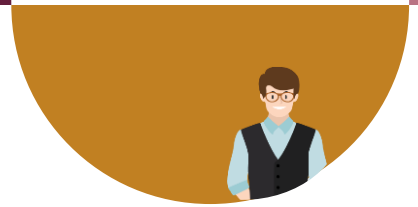
11%

De omkostnings-fokuserede

Små virksomheder, som ikke har tid eller penge til at fokusere på it-sikkerhed, men i stedet har fokus på at holde forretningen kørende. Er bevidste om it-sikkerhed, men prioriterer det ikke, da det koster tid og penge, som, for dem, er bedre brugt på forretningen. De skal se, hvilken effekt eventuelle brud kan få for deres virksomhed, og deraf værdien af it-sikkerhed.

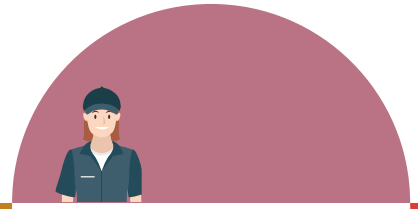
De it-erfarne

De største virksomheder, hvor it-sikkerhed er en integreret del. Mangler dog stadig at få alle medarbejdere til at efterleve de mange regler. Har en del teknologi, og holder derfor også løbende øje med trusselsbilledet, men mangler mere forståelig kommunikation fra it-branchen, da det er svært at gennemskue, hvad man skal gøre, og hvornår.



16%

20%

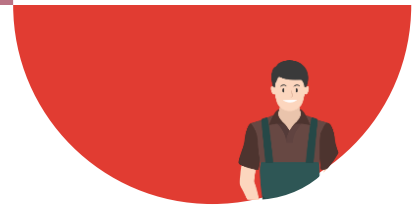


De gevinstfokuserede

Mindre virksomheder, som har svært ved at se den økonomiske gevinst ved at investere i it-sikkerhed, og som derfor ikke prioriterer dette. De skal se værdien af stærk it-sikkerhed ved at få kommunikeret, hvad det kan koste på bundlinjen ikke at være it-sikker.

De lavinvolverede

Små virksomheder, som på ingen måder har it-sikkerhed på dagsordenen, da de ikke ser it som en del af deres forretning. Det bliver hurtigt dyrt og koster ressourcer, hvis man skal gøre noget ved it-sikkerheden. Krav/lovgivning på området og mere viden om, at man er i risikogruppen vil kunne flytte virksomheder i dette segment.



28%

n = 1.806 virksomheder i 2020 og 1.011 virksomheder i 2021.

ERHVERVSSTYRELSEN

Hovedresultater

Epinion

Hovedresultater

1. It-sikkerhed opfattes ikke som en del af virksomheden

- Hele 75 pct. af de adspurgte SMV'er har i høj eller nogen grad udliciteret deres it-sikkerhed til en ekstern it-leverandør.
- I de kvalitative interviews er det belyst, hvordan fokus på it-sikkerhed blandt disse virksomheder i praksis er lavt, og at der derfor hersker stor tillid til it-leverandører og –supporter, som til daglig hjælper med it og it-sikkerhed i virksomheden.
- Endvidere er det fremkommet i de kvalitative interviews, at et manglende fokus på it-sikkerhed i virksomhederne skyldes, at it-sikkerhed forveksles med GDPR. Drøftelser af it-sikkerhed sker også ofte på ad hoc basis.

2. It-leverandører har en central rolle i formidling af it-sikkerhed

- It-leverandør er den kilde til information om it-sikkerhed, som virksomhederne i langt de fleste tilfælde (141 gange) selv nævner, når de bliver spurgt uhjulpet ind til kilder.
- Blandt virksomhederne er det både 60 pct., som har *modtaget* information om it-sikkerhed fra deres it-sikkerhedsrådgiver (intern eller ekstern), samt 60 pct., der *selv har opsøgt* information hos dem.
- Hele 84 pct. af virksomhederne har blot fokus på it-sikkerhed, når deres it-leverandør eller -rådgiver anbefaler at opgradere it-sikkerheden.

3. Værktøjer til risikovurdering og online test skaber interesse

- 18 pct. af de danske SMV'er er interesseret i tilbuddet om værktøjer til at lave en it-risikovurdering af virksomheden.
- 16 pct. af virksomhederne er interesseret i tilbud om online test af virksomheders it-sikkerhedsniveau og risikoprofil.
- Ud fra virksomhedernes prioriteringer af de eksisterende tilbud, finder den kvantitative analyse, at virksomheder, der er interesseret i værktøjer til risikovurdering, som regel også er interesseret i vejledningsmateriale.

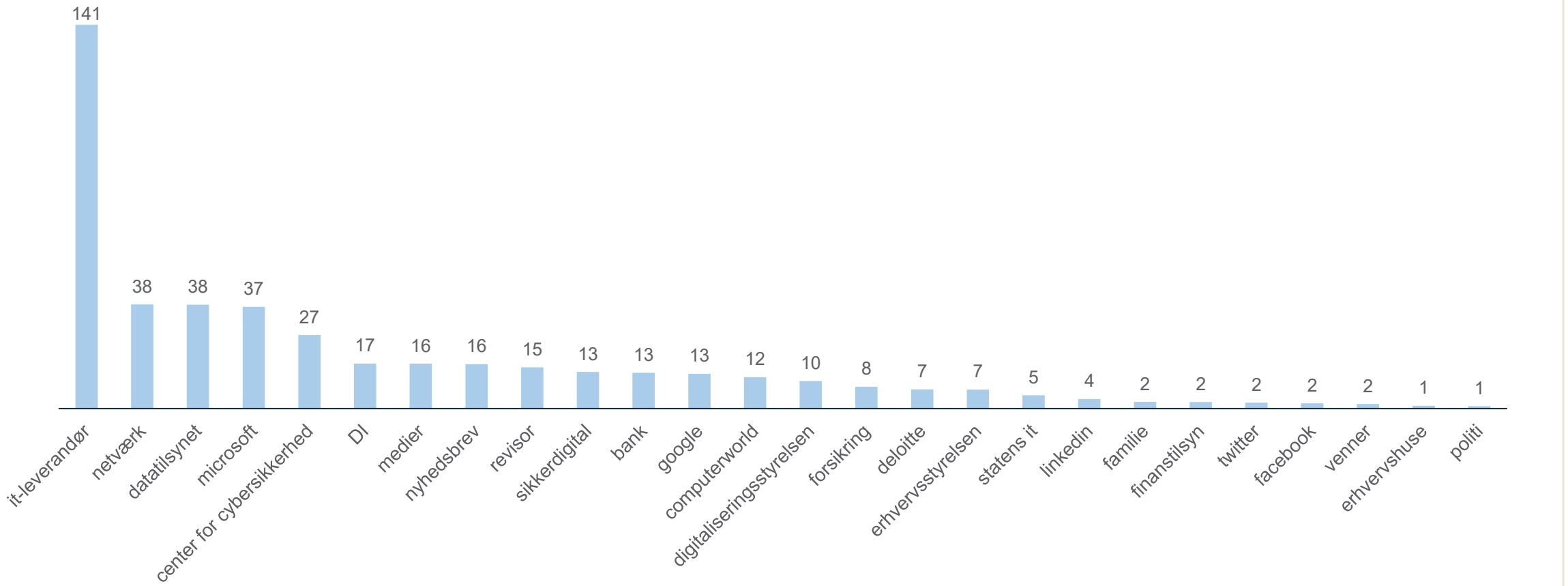
ERHVERVSSTYRELSEN

Informationskanaler

Epinion

På tværs af de danske SMV'er nævnes en række kilder til information om it-sikkerhed. De fleste virksomheder peger dog på deres it-leverandør

Hvilke kilder til information om it-sikkerhed kender du?

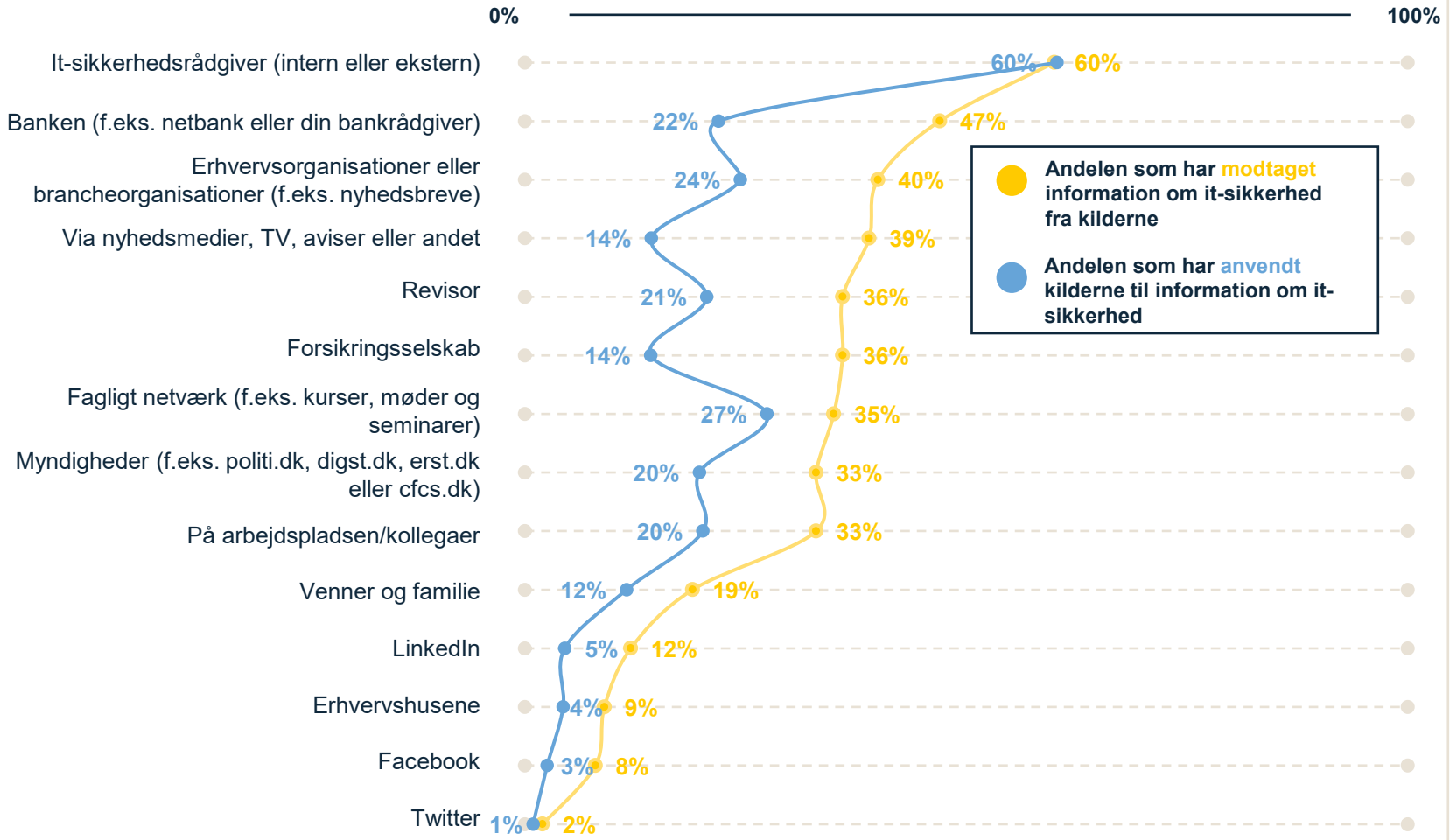


n = 612 virksomheder kender én eller flere kilder til information om it-sikkerhed.

It-sikkerhedsrådgivere er den største kilde til både *modtaget* og *anvendt* information om it-sikkerhed. Hernæst bank og erhvervsorganisationer

- For at tage højde for, at virksomheder både kan blive eksponeret for information om it-sikkerhed (f.eks. via mail eller reklamer) og selv opsøge det, har vi både spurgt ind, hvilke kilder de generelt *modtager* og *anvender*.
- Ca. 60% af virksomhederne angiver således, at de enten har modtaget eller gjort brug af it-sikkerhedsrådgivere til at få information om it-sikkerhed.
- På tværs af kilder er andelen, som har modtaget information om it-sikkerhed, højere end andelen som har gjort brug af kilden som information om it-sikkerhed.
- Det er cirka hver tredje virksomhed, som har modtaget information om it-sikkerhed fra myndigheder. Derimod har lidt over hver fjerde virksomhed faktisk anvendt kilder fra myndighederne i arbejdet med it-sikkerhed.

Fra hvilke af nedenstående kilder har du modtaget eller anvendt information om it-sikkerhed?



N = 1.011 virksomheder

Erhvervsstyrelsen

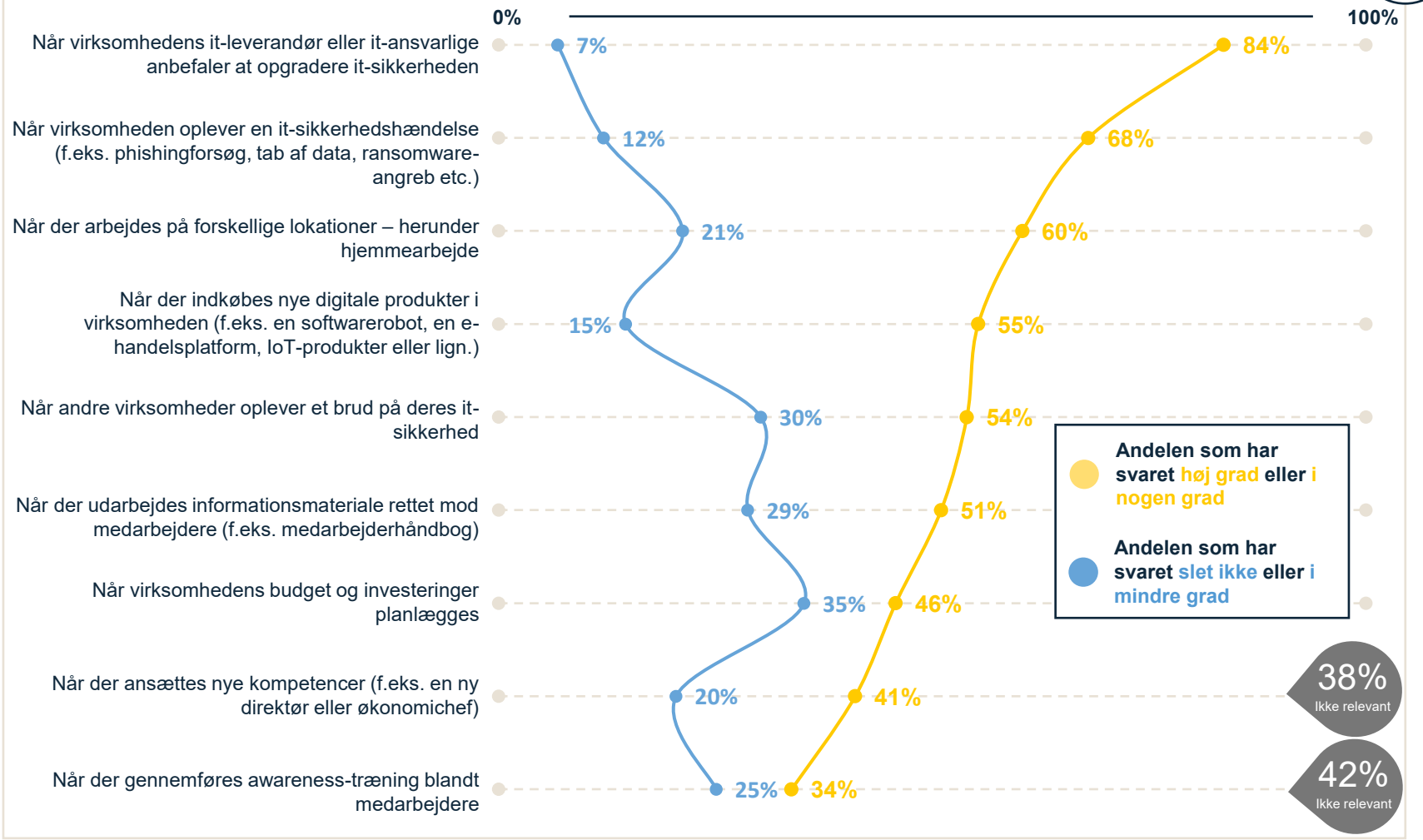
Forståelse og håndtering af it-sikkerhed

Epinion

Mere end 4 ud af 5 har fokus på it-sikkerhed, når it-leverandør eller -ansvarlig anbefaler at opgradere it-sikkerhed. Færrest har fokus ved awareness-træning

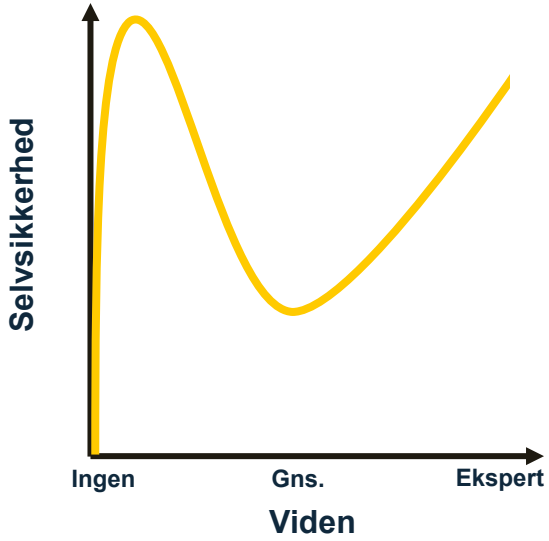
- På tværs af virksomhederne er der særligt fokus på it-sikkerhed, når virksomhedens it-leverandører eller it-ansvarlige anbefaler at opgradere sikkerheden. Mange virksomheder har også fokus på it-sikkerhed, hvis virksomheden eller andre virksomheder oplever en it-sikkerhedshændelse.
- Samtidig fører arbejde på tværs af lokationer også til fokus på it-sikkerhed.
- Omkring halvdelen af virksomhederne har fokus på it-sikkerhed, når der indkøbes nye digitale produkter, planlægges budget/investeringer, og når der udarbejdes informationsmateriale til medarbejderne.
- Færrest har fokus på it-sikkerhed, når der ansættes nye medarbejdere, eller når der gennemføres awareness-træning. Mange svarer imidlertid "ikke relevant", hvilket peger på, at en del virksomheder ikke arbejder med f.eks. awareness-træning.

I hvilken grad er der fokus på it-sikkerhed i virksomheden ved følgende situationer?



n = 1.011 virksomheder

Virksomheder forstår it-sikkerhed som et greb, der er med til at beskytte personfølsomme oplysninger



It-sikkerhed i kontekst af GDPR

- Analysen viser, at flere af de små virksomheder eller virksomhederne fra de mindre it-kyndige segmenter til tider blander GDPR og it-sikkerhed sammen. De har svært ved at adskille de to fra hinanden.
- Yderligere peger analysen på, at flere af virksomhederne forstår it-sikkerhed som noget, der ligger rundt om GDPR, og at et af formålene med at have den rette it-sikkerhed er, at det er med til at beskytte de personfølsomme oplysninger, som virksomheden besidder.

"Jamen, der er to ting i det [vi forbinder med it-sikkerhed]. Den ene er selvfølgelig den der helt, helt simple it-sikkerhed, der ligger i at vi har nogle patenter og får noget viden her i huset, som vi jo ikke ønsker at dele. Og så har vi selvfølgelig nogle personfølsomme oplysninger, som vi ikke ønsker at dele, og nogenlunde salgsmæssige."

- Direktør, 11-49 ansatte

Barrierer ift. it-sikkerhed

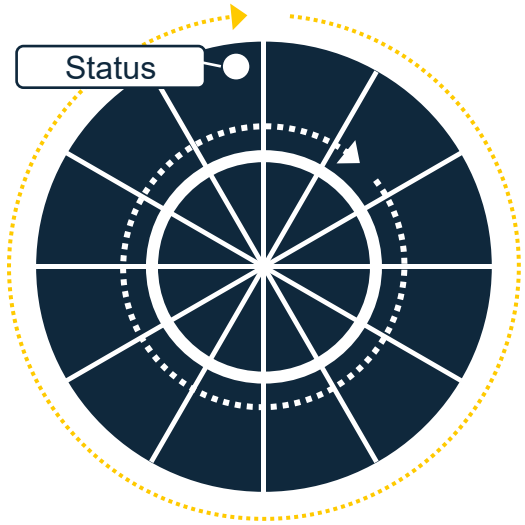
- Analysen peger på, at der er et mismatch mellem virksomhedernes viden om it-sikkerhed og deres egen forståelse: Flere virksomheder, som tilhører et segment med mindre fokus på it-sikkerhed, er meget selvsikre i deres beskrivelser af deres it-sikkerhed.
- Omvendt beskriver de virksomheder, som har stor viden om it-sikkerhed, hvordan de hele tiden må være opmærksomme på nye tendenser og sikkerhedsbrud, ligesom de anerkender, at de må hive eksperter ind for at være "up to date".

"Det er et meget varmt emne og det er et emne, der hele tiden bliver taget op. Man hører jo hele tiden om i medierne, hvordan den ene, den anden og den tredje virksomhed lige pludselig har været udsat for en eller anden sikkerhedsbrist. Så derfor har vi jo hele tiden fokus på at sørge for, at vi forhåbentlig ikke ryger i samme situation, og derfor er det hele tiden noget, vi snakker og sparrer med vores leverandører om: Er der noget, vi kan gøre endnu bedre, end vi gør i dag?"

- It-chef, 50-99 ansatte

n = 12 kvalitative interviews

Der findes virksomheder, for hvem it-sikkerhed ikke drøftes kontinuerligt på ledelsesdagsorden, men vendes ad hoc eller på et årligt statusmøde med leverandører

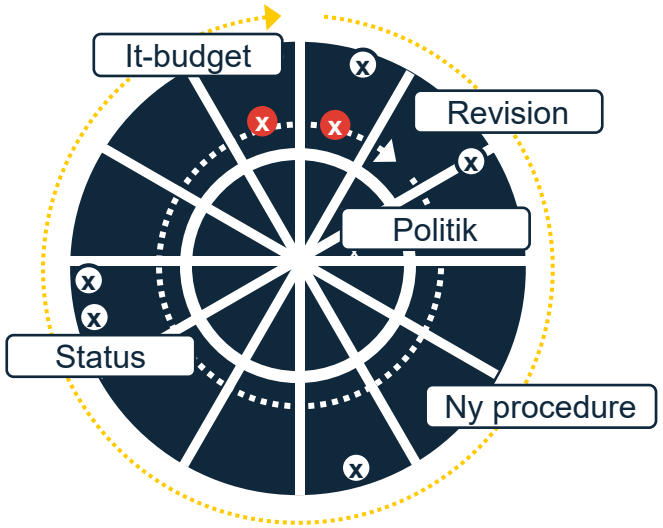


It-sikkerhed ad hoc

- For de fleste virksomheder i de kvalitative interview, er sikkerhedspraksis ikke skitseret i et fast årshjul
- Ofte et til to årlige statusmøder enten internt i organisationen eller med it-leverandør, hvor nye sikkerhedspraksisser og/eller behov for nye investeringer diskuteres og anbefales.
- Ligger ofte i forbindelse med it-budgetter.
- It-sikkerhed justeres ad hoc fx ved nyt udstyr, hændelser i medierne, sikkerhedsbrud, ansættelser eller fordi it-leverandør anbefaler ændringer.

"Vi har møde 2 gange om året, hvor vi har vores infrastruktur oppe at vende. Vi kommer også omkring it-sikkerheden og GDPR - hvor vi lige vender og ser, hvor er vi egentlig henne? Det ligger omkring sommertid lige omkring her, hvor vi går på sommerferie. Enten før eller efter. Fordi her er der bedst tid"

- It-vejleder, 11-49 ansatte



It-sikkerhed i et fast årshjul

- It-sikkerheden ligger i et fast årshjul med flere møder spredt gennem året, f.eks. faste statusmøder, budget, audit eller lignende, hvor der er fokus på revidering og nye tiltag samt huller i eksisterende sikkerhed
- For andre virksomheder er it-sikkerheden ikke skitseret i et fast årshjul, men er månedligt på ledelsesdagsorden. It-sikkerheden har her karakterer af at være skitseret fast, fordi den genbesøges hyppigt

"Altså dels har vi jo bygget en lang række politikker og procedurer. Vi har nogle årshjul, så vi til stadighed genbesøger både politikker og procedurer. […] De fordeler sig ud over året, så man ikke skal have 30 opgaver på én måned og nul den næste. Det ligger bare fordelt hen over året, sådan at de alle sammen er indenfor det samme år og afsluttet i december, da vi har vores it revision i januar."

- Direktør, 0-10 ansatte

n = 12 kvalitative interviews

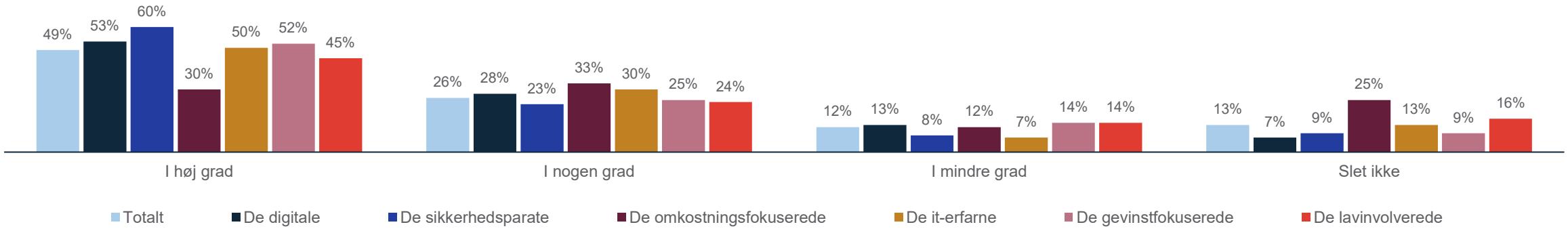
Næsten halvdelen har i høj grad udliciteret deres it-sikkerhed – tendensen er størst blandt de sikkerhedsparate

- I de kvalitative interviews er der variation i, om it-sikkerheden er udliciteret. Flere virksomheder påtaler, at de har udliciteret hele eller dele af it-sikkerheden til eksterne leverandører. Blandt flere af disse virksomheder er kendskabet til it-sikkerhed i praksis lavt, og der hersker som følge stor tillid til it-leverandører og –supporter, der til daglig hjælper med it og it-sikkerhed i virksomheden.
- Andre virksomheder italesætter, at de selv internt står for ansvaret med it-sikkerheden. Mens nogle af disse virksomheder har en velopbygget infrastruktur og overblik over it-sikkerheden på leverancesystemet, så har andre af virksomhederne ikke en dybere forståelse eller opmærksomhed på it-sikkerheden.

"Min rolle er egentlig, at jeg er ansvarlig for it-sikkerhed her, men der er rigtig meget af det, der ligger hos nogle der hedder [leverandør]. Man kan sige, at rigtig meget er outsourcet til dem, og så bruger vi også et eksternt firma til at hjælpe os med de forskellige ting, der er, idet vi er underlagt ledelsesbekendtgørelser og andet lovgivning, som stiller nogle krav."

- Udviklingschef, 100+ ansatte

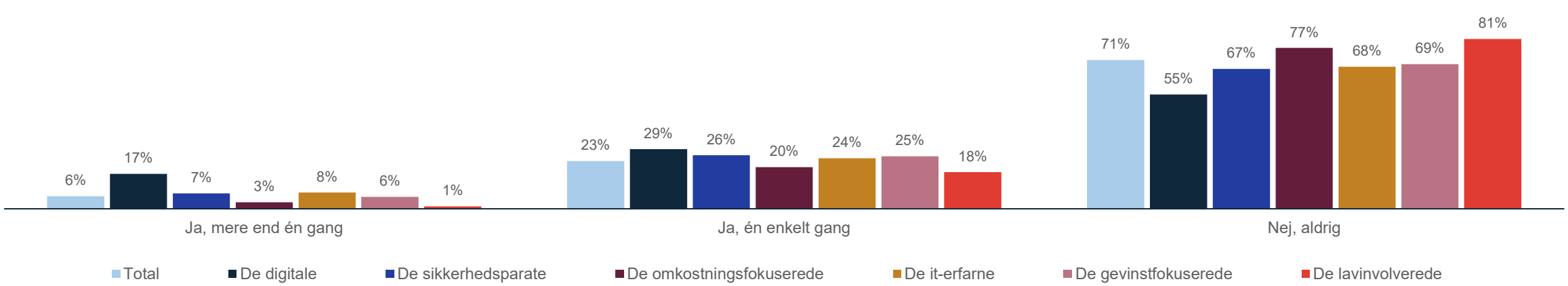
I hvilken grad har virksomheden udliciteret it-sikkerheden (både hosting og drift) til en eller flere eksterne leverandører?



n = 1.011, hvoraf 27 virksomheder svarer "Ved ikke" til spørgsmålet om udlicitering + 12 kvalitative interviews.

Næsten hver tredje virksomhed har været udsat for en it-sikkerheds-hændelse, og særligt de digitale har været udsat for mere end én hændelse

Har virksomheden nogensinde været udsat for en it-sikkerhedshændelse?



"En af mine kolleger (på anden institution) blev udsat for et angreb, hvor alt gik frygtelig galt og de mistede både deres primære servere og deres backup server, så de startede simpelthen var fra nul. Det er jo sådan en et skrækscenarie. Det hele var bare tabt (…). I forlængelse af den episode, så fik jeg hyret en it-rådgiver(…), som så står for det meste af vores it."
- Rektor, 50-99 ansatte

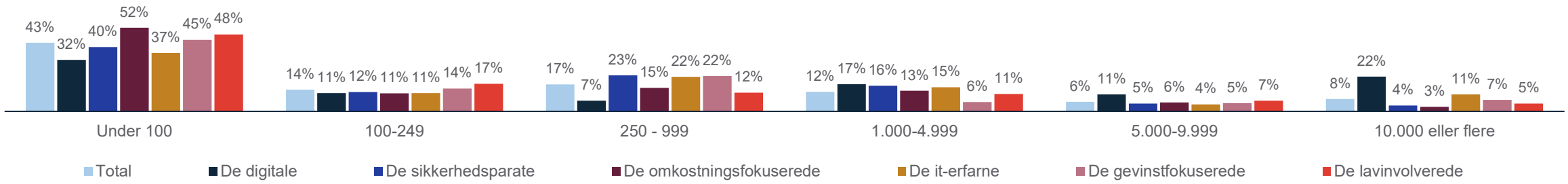
"Ikke endnu (…), men det er jo klart hvis du er på en skala, så kommer du aldrig længe op end 85% (it-sikker) fordi der altid er nogle der vil kunne prøve at lave rav i den, og få dine systemer til at gå ned. (…) Hvis der er nogle ondsindede hackere, som vil have vores system går ned, jamen så kan de jo vælge at gøre det, fordi de fx bare kan skyde så meget på serveren, at den til sidst ikke kan følge med."
- COO, 1-9 ansatte

N = 1.011, hvoraf 76 virksomheder svarer "Ved ikke" til spørgsmålet om sikkerhedshændelse + 12 kvalitative interviews.

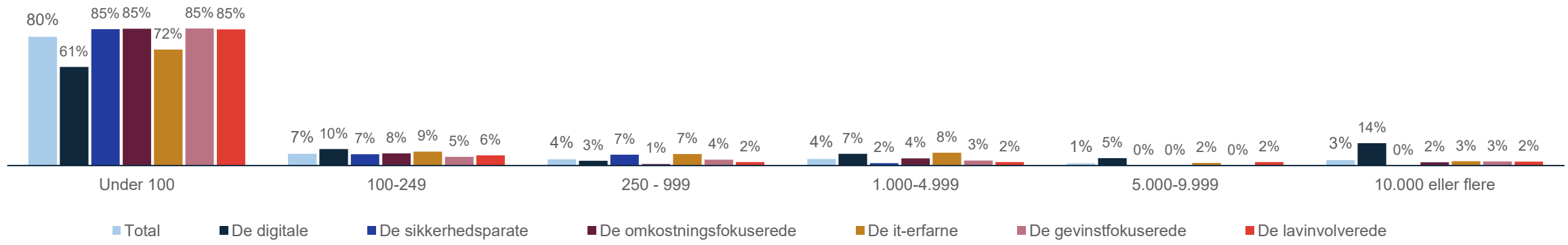
Mængden af almindelige personoplysninger varierer, mens langt størstedelen af virksomhederne har kun følsomme personoplysninger på under 100 individer

Hvor mange individer (f.eks. kunder, brugere, ansatte, m.v.) gemmer virksomheden data på?

Almindelige personoplysninger



Følsomme/særlige personoplysninger



N = 1.011, hvoraf henholdsvis 72 og 115 virksomheder svarer "Ved ikke" til, hvor mange individer virksomheden gemmer data på.

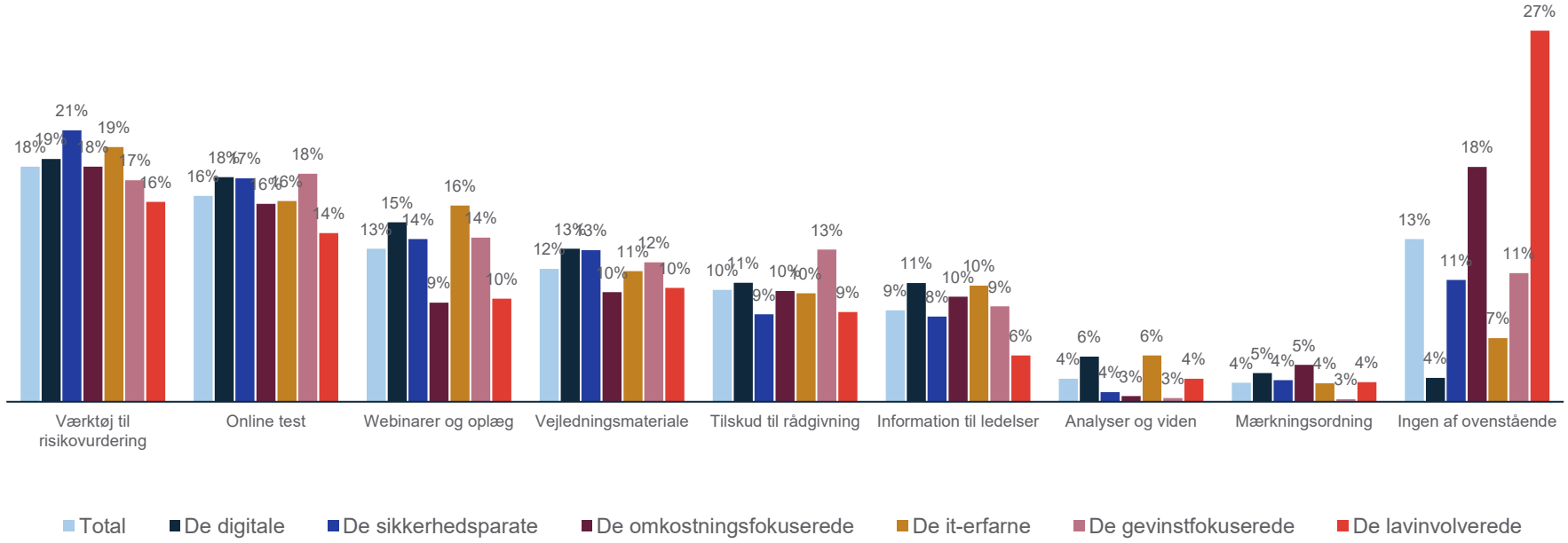
ERHVERVSSTYRELSEN

Nuværende indsatser

Epinion

Hvor de lavinvolverede ikke er interesseret i tilbud, så er det i høj grad de digitale og it-erfarne, som ønsker forskellige tilbud om hjælp til it-sikkerhed

Hvilke af de forskellige indsatser kunne jeres virksomhed være interesseret i at gøre brug af?



- Til venstre ses en opgørelse over, hvilke tilbud danske SMV'er generelt vælger, at de kunne være interesseret i.
- Generelt er virksomhederne mest interesseret i tilbuddet om værktøj til it-risikovurdering, hvor specielt de sikkerhedsparate vælger det til.
- De gevinstfokuserede skiller sig ud ved at være relativt mere interesseret i tilskud til uvildig rådgivning, og de lavinvolverede viser ikke den store interesse.

n = 1.011 virksomheder

ERHVERVSSTYRELSEN

Metodebilag

Epinion

Resultaterne beror på en gennemprøvet metodisk tilgang, hvor virksomheder rekrutteres via e-Boks, inddeles i segmenter og til sidst vejes op mod populationen

Indsamling

Både respondenter og interviewpersoner er rekrutteret via invitation på e-Boks. Første kontakt er taget tirsdag den 30. november 2021, hvor invitationer blev sendt ud til 6.000 juridiske enheder blandt danske små og mellemstore virksomheder fra KOB/Experians virksomhedsdatabase. Brutto sample blev udtrukket simpelt tilfældigt fra populationen af danske SMV'er. Én uge senere blev der sendt et påmindelsesbrev på e-Boks efterfulgt af en påmindelsesmail til e-mailadresserne fra udtrækket. Mandag den 13. december blev sidste påmindelse sendt til virksomhederne i form af en SMS til telefonnumre fra udtrækket.

Segmenter

Gyldige besvarelser bliver herefter kategoriseret i de seks virksomhedstyper, som blev identificeret under segmenteringsanalysen i efteråret 2020. Det gøres på baggrund af fire diskriminantspørgsmål, som blev fundet særdeles velegnet til at inddele virksomheder i de seks segmenter. Det drejer sig om spørgsmål angående sikkerhedstiltag, digitale produkter, kritiske sektorer, sandsynlighed for sikkerhedshændelse samt opmærksomhed på it-sikkerhed blandt ledelsen. Algoritmen for inddeling af virksomheder i segmenter kan afprøves her: https://epinionglobal.shinyapps.io/erst_app/. På baggrund af segmentnøglen bliver alle virksomheder således tildelt et segment, hvor de deler grundlæggende karakteristika med andre virksomheder i segmentet.

Datarens

I alt har 1.752 virksomheder tilgået spørgeskemaet i løbet af perioden. Ud af disse er 1.066 besvarelser registreret som fuldførte og indgår i den efterfølgende databehandling. Her sikrer Epinion ved en rens af data, at analysen beror på højkvalitetsbesvarelser. For det første bliver gengangere ekskluderet således, at én virksomhed ikke kan deltage flere gange (*dubletter*). Derudover frasorteres interviews, som er gennemført usandsynlig hurtigt – her defineret som 40 pct. hurtigere end median gennemførselstiden (*speeders*). Slutteligt ekskluderes interview, hvis respondenten svarer hyppigere i én kategori end én standardafvigelse fra gennemsnittet, samt at interviewet er gennemført hurtigere hen 50 pct. fra medianen *(flatliners)*. Det efterlader 1.011 gyldige besvarelser til analysen.

Vægt

Eventuelle mindre skævheder ift. at opnå en repræsentativ stikprøve er efterfølgende vejet på plads (*post-stratificering*). Stikprøven er vejet efter fordelingerne i det samlede udtræk fra KOB/Experians virksomhedsdatabase – det vil sige populationen af danske SMV'er. Vejestrategien følger den, som blev brugt under segmenteringsanalysen. Således er stikprøven repræsentativ på følgende dimensioner: antal ansatte, region og sektor. Derudover er der også vejet efter fordelingen mellem segmenter fra efteråret 2020. Resultaterne præsenteres derfor som vægtede procenttal – det vil sige vægtede procentdele af danske SMV'er eller vægtede procentdele af de seks segmenter i stikprøven.