

Virksomhederne mangler rådgivning om digital sikkerhed

TEMAANALYSE

Virksomhederne mangler den korrekte rådgivning til at følge med inden for digitaliseringen. 2 ud af 5 SMV'er har ikke en digital sikkerhed, som matcher deres risikoprofil. Problemet skyldes i høj grad, at virksomhederne ikke ved hvor de skal finde den relevante rådgivning.



Virksomhederne mangler rådgivning om digital sikkerhed

Dato: 22. december 2021

Danmark er et af de mest digitaliserede lande i verden, men den digitale udvikling medfører også til øget sårbarhed, hvor vi skal justere og beskytte os imod nye trusler og problemer. Mange af SMV'erne mangler mere digital sikkerhed, hvor tal fra SMVdanmark viser at 1 ud af 6 SMV'er ikke har certificeret deres hjemmesider. Problemet skyldes i høj grad, at virksomhederne ikke ved hvor de skal finde den relevante rådgivning og den rådgivning de får, ikke matcher deres behov.

Hovedpointer fra undersøgelsen

- 34 pct. af virksomhederne ved ikke, hvor de finder rådgivning inden for digitalisering.
- 1 ud af 6 SMV'er mangler at certificere deres hjemmesider, så de mindsker deres risiko for nye trusler.

Så mange
SMV'er ved
ikke hvor de
finder råd-
givning

34%

Hver tredje SMV'er mangler rådgivning

SMVdanmark har i perioden 3. august til 20. august 2021 gennemført en analyse blandt medlemsvirksomheder om digitalisering. Hele undersøgelsen er udsendt til ca. 1.452 virksomheder.

Undersøgelsen viser, at hver tredje SMV'er ikke ved, hvor de finder den relevante rådgivning inden for digitalisering. En [analyse fra SMVdanmark](#) viser, at Danmark er det EU-land med den højeste procentdel af webshops i Europa, hvor 32 pct. af de danske virksomheder har salg via deres egen webshop, apps eller markedsplads. Danmark er derfor et af de lande som lægger sig i front, når det gælder brugen af digitale løsninger.

Danske virksomheder er altså i førertrøjen når det kommer til brugen af digitale redskaber som f.eks. webshops, men den store digitale udvikling øger også truslerne, som består af den digitale sårbarhed der opstår ved brug af f.eks. webshops. Det er derfor vigtigt at virksomhederne ved, hvor de kan finde den korrekte rådgivning, til at sikre sig imod nyskabte digitale trusler. Konsekvensen af den manglende fokus på digital sikkerhed øger risikoen for digital kriminalitet i takt med, at de digitale løsninger som f.eks. webshops bliver mere og mere udbredt.

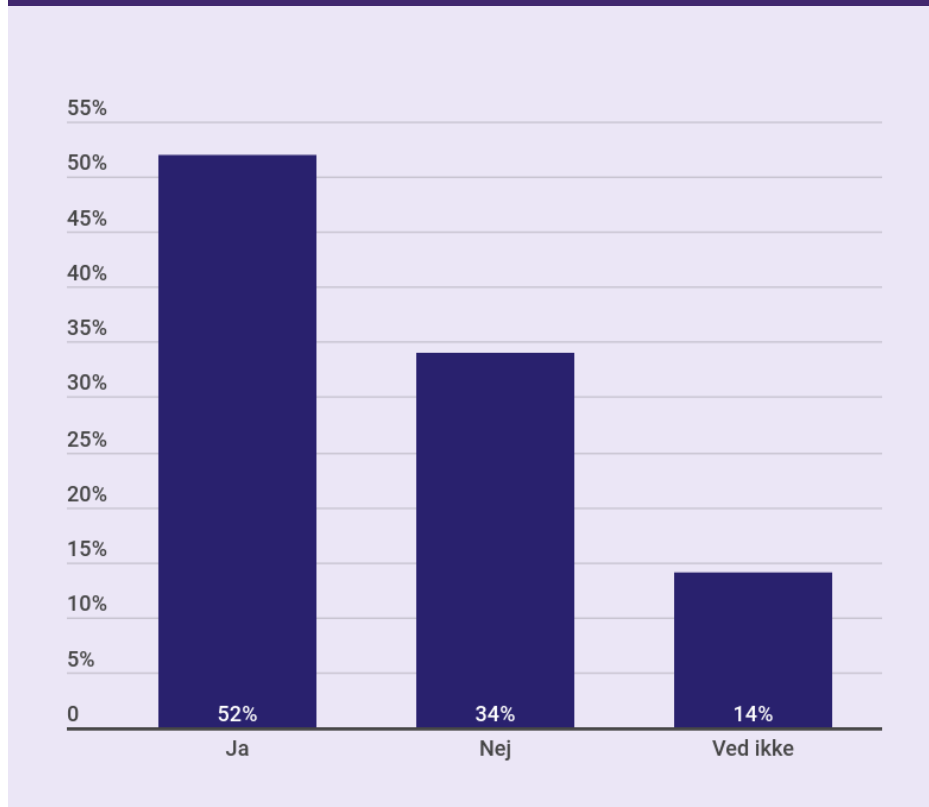
Ifølge [Center for Cybersikkerhed](#) vurderes det, at truslen fra cyberkriminalitet er så høj, at virksomheder bliver udsat for en vedvarende og aktiv trussel fra cyberkriminelle.

Cyberkriminalitet dækker over flere typer berigelseskriminalitet, herunder både tyveri, bedrageri og afpresning. Det sidstnævnte dækker blandt andet over de såkaldte ransomware-angreb, som i stigende grad bliver brugt af hackere på blandt andet de danske virksomheder. Gennem de seneste år har der ifølge Center for Cybersikkerhed været en kraftig vækst i antallet af ransomware-angreb mod de danske virksomheder, hvor en stikprøve viser at 78 pct. af virksomhederne i 2020 er blevet angrebet. Det præcise antal ransomware-angreb i Danmark er dog ukendt, da mange virksomheder ikke vil skilte med sårbarhederne i deres digitale systemer, og derfor findes der et stort mørketal vi ikke kender til.

Ved et ransomware-angreb bliver data og systemer gjort utilgængelige for virksomheden der bliver hacket. Derefter kræver hackeren en løsesum, som oftest skal betales i kryptovaluta, for at give virksomhederne adgang til deres data igen.

Over hver tredje virksomhed ved ikke hvor de skal finde rådgivning til digitalisering

Andel af virksomheder der ved hvor de finder rådgivning inden for digitalisering, pct.



Antal respondenter: 516

Figur 1

Kilde: SMVdanmark

Spg.: "Ved du, hvor du søger rådgivning inden for digitalisering?"

Virksomhederne søger mere lavpraktiske løsninger

For at mindske risikoen for cyberangreb kan man som virksomhedsejer beskytte sin websites med velegnede SSL-certifikater. Disse certifikater beskytter besøgendes personlige informationer, samt giver hjemmesiden et valideringsmærkat, som kan hjælpe til at sikre, man ikke besøger falske hjemmesider. Uden et SSL-certifikat risikerer virksomhedernes

hjemmesider, at de ikke dukker op når man søger på dem, da google kan vurdere hjemmesider uden SSL-certifikat for risikable.

Faktaboks

SSL står for Secure Sockets Layer, hvilket er en online sikkerhedsteknologi, der sikrer forbindelsen imellem en web browser og den server hvor hjemmesiden ligger på. Med et SSL-certifikat bliver alt data, der sendes digitalt imellem browseren og serveren, krypteret. Det beskytter dermed sensitiv information som kreditkortoplysninger, login-informationer og data transaktioner, og gør det langt sværere for cyberkriminelle.

Udover at miste trafik på virksomhedens hjemmeside, hvilket går udover omsætning så kan angrebet også få skadet virksomhedens ry og renommé.

En [publikation fra efteråret 2021 fra Erhvervsstyrelsen](#) påpeger, at 40 pct. af SMV'erne ikke havde en digital sikkerhed, som matchede deres risikoprofil.

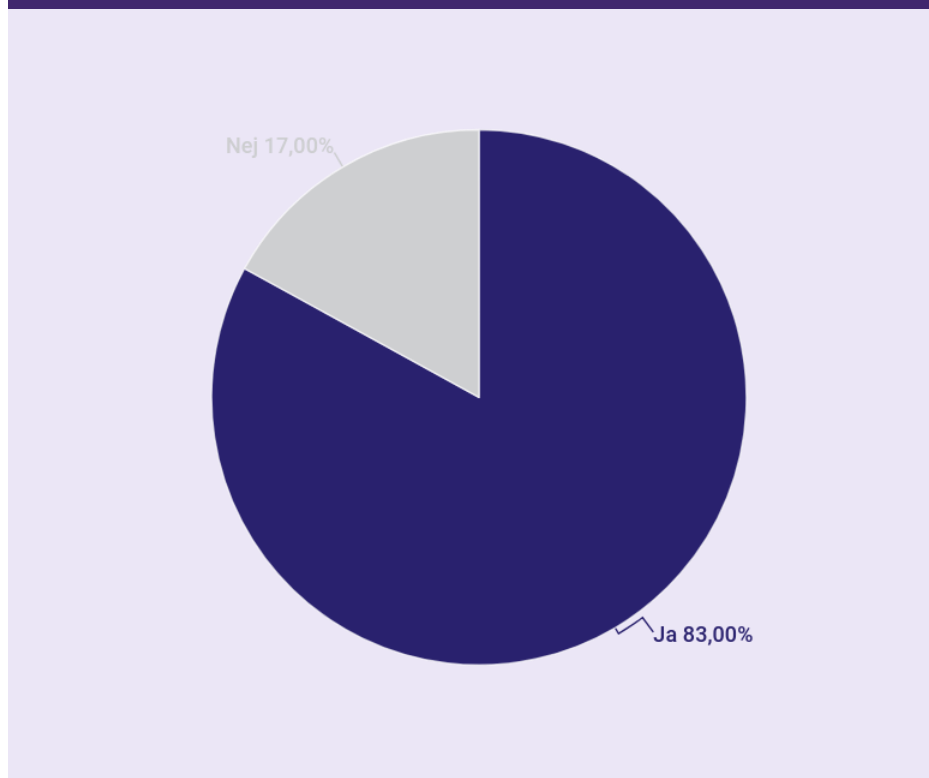
Det kan være et særligt alvorligt problem for SMV'er, som ofte ikke har ressourcer til aktivt at overvåge deres tilstedeværelse på internettet for at opdage domænehamstring og beskytte deres omdømme.

En undersøgelse lavet af SMVDanmark baseret på en stikprøve af 5.623 SMV'er viser, at 17 pct. af de små eller mellemstore virksomhed ikke har certifikatsikret deres hjemmeside. Det vil sige at omkring hver 6 virksomhed, hvis hjemmeside aktivt bliver brugt og kan indeholde en masse informationsrig viden om deres virksomhed, bliver sat i stor risiko for cyberangreb.

Hvis en virksomhed uden sikkerhedscertifikat bliver udsat for et angreb, kan det være farligt for virksomhedens omdømme. [En undersøgelse](#) viser at 46 pct. af danskerne vil stoppe med at handle med deres foretrukne virksomhed, hvis virksomheden har svag it-sikkerhed og bliver involveret i et cyberangreb. Derudover viser undersøgelsen også, at forbrugeren er klar til at stille virksomheden til ansvar, hvis ikke de beskytter deres kunder.

En ud af seks
SMV'er har
ikke sikret
deres hjem-
mesider

Andel af virksomheder der har et SSL-certifikat på deres hjemmeside, pct.



Antal respondenter: 5623

Kilde: SMVdanmark

Figur 2

Konklusion og politikforslag

SMV'erne mangler den korrekte rådgivning når det handler om digitaliseringen. Der er alt for stor andel af SMV'erne som ikke er beskyttet imod digitale trusler, og SMVdanmarks egen analyse viser at 1 ud af 6 SMV'er mangler et SSL-certifikat, som øger deres risiko.

Den rådgivning der allerede findes omkring digitalisering, mangler en SMV-vinkel, så de små og mellemstore virksomheder kan relatere til strategien om digitaliseringen og den rådgivning der bliver stillet. Det skal være en mere målrettet rådgivning, hvor der skal være konkrete og relaterbare digitale løsninger, så SMV'erne også kan se idéen og fordelene ved digitaliseringen.

SMVdanmark forslår, at Erhvervsstyrelsen øger indsatsen for vidensdeling og rådgivning indenfor digital sikkerhed. Rådgivningen skal tage udgangspunkt i konkrete problemer. Samtidig er ønsket at midlerne til SMV:digital øges i lyset af, at kun ca. end 3.800 virksomheder har fået del af puljen, hvilket er en dråbe i havet sammenlignet med antallet af digitaliseringsparate SMV'er, men samtidig ville flere midler også give mulighed for at hjælpe mange af de lavpraktiske sikkerhedsbrister, som mange SMV'er slet ikke er klar over. Mange flere SMV'er har brug for hjælp til et kompetenceløft når det gælder digital sikkerhed.

Kontakt

Konsulent Lasse Lundqvist,
tlf. 41 29 20 09, lundqvist@SMVdanmark.dk.
SMVdanmark, oktober 2021

Juniorkonsulent Maximilian Hueg,
tlf. 60 22 42 82, hueg@SMVdanmark.dk.
SMVdanmark, oktober 2021