SMVdanmark

Cyberangreb kan blive en dyr omgang for SMV'erne

TEMAANALYSE

Et ransomware angreb koster 376.350 kr. alene i tabt omsætning fra e-handel for en virksomhed med 10-49 ansatte. I lyset af at truslen for cyberkriminalitet er på sit højeste, skal flere SMV'er have hjælp til at øge deres IT-sikkerhed. Særligt efter en hård tid under COVID-19, som har tvunget virksomhedernes fokus væk fra IT-sikkerhed.

Cyberangreb kan blive en dyr omgang for SMV'erne

Truslen for cyberangreb er på sit højeste. Det vurderer Center for Cybersikkerhed, da sanktionerne mod Rusland kan føre til gengældelse fra russiske hackere. Samtidig har Danmark den højeste digitaliseringsgrad i EU. Det skyldes blandt andet, at Danmark er det land i EU, hvor flest SMV'er har en grundlæggende digitaliseringsgrad. Det betyder, at SMV'erne er europamestre i at implementere digitale værktøjer. Det kommer blandt andet til udtryk ved, at danske SMV'er er langt foran, når det f.eks. gælder brugen af e-handel, kunstig intelligens og digital informationsdeling. Desværre findes der også en bagside af medaljen. Den høje digitaliseringsgrad blandt SMV'erne, åbner nemlig samtidig for flere indgange, som hackerne kan benytte. Særligt i en tid, hvor cybertruslen er på sit højeste.

Hovedpointer fra undersøgelsen

- De økonomiske konsekvenser ved et cyberangreb er høje. Et ransomware angreb koster i gennemsnit 376.350 kr. for den gennemsnitlig virksomhed med 10-49 ansatte, alene i tabt omsætning fra e-handel.
- Det er ikke kun de store virksomheder, hvis digitale sikkerhed er udsat. SMV'er rammes i høj grad også af brud på IT-sikkerheden. I 2020 oplevede hver tiende virksomhed brud på IT-sikkerheden.
- Flere og flere virksomheder får foretaget en risikoanalyse af virksomhedens IT-systemer.
- Tidligere har en stigende andel af SMV'er hævet virksomhedens investeringer i IT-sikkerhed. Coronakrisen har dog tvunget virksomhedernes fokus væk fra IT-sikkerhed.

I gns. oplever en virksomhed digital mørklægning som følge af ransomware angreb i:

18 dage

Det koster dyrt for virksomhederne når IT-systemet rammes

Når virksomheders IT-system rammes af et ransomware angreb, resulterer det i gennemsnit i 18 dages digital mørklægning[1]. Et ransomware angreb er en computervirus, som krypterer enten hele eller dele af virksomhedens harddiske, hvorefter der kræves en løsesum hos den pågældende virksomhed for at få låst filerne op igen.. Samtidig steg antallet af ransomware angreb med 150 pct. i 2020 på globalt plan[2]. Nedenstående figur viser, det gennemsnitlige tab i omsætning fra e-handel, for virksomheder som rammes af et ransomware angreb på netop 18 dage. En virksomhed med 10-49 ansatte vil i gennemsnit tabe 376.530 kroner i tilfælde af et angreb på 18 dage, hvor ingen e-handler kan gennemføres. I samme tilfælde, vil en virksomhed med 50-99 ansatte i gennemsnit tabe knap 2 millioner kroner.

Omkostningerne, som figuren angiver, kan dog være endnu højere, da det interne IT-system i virksomheden ligeledes kan være ramt og forårsage yderligere omkostninger i forbindelse med et angreb. Dertil kommer virksomheden omdømme, som også vil blive beskadiget.

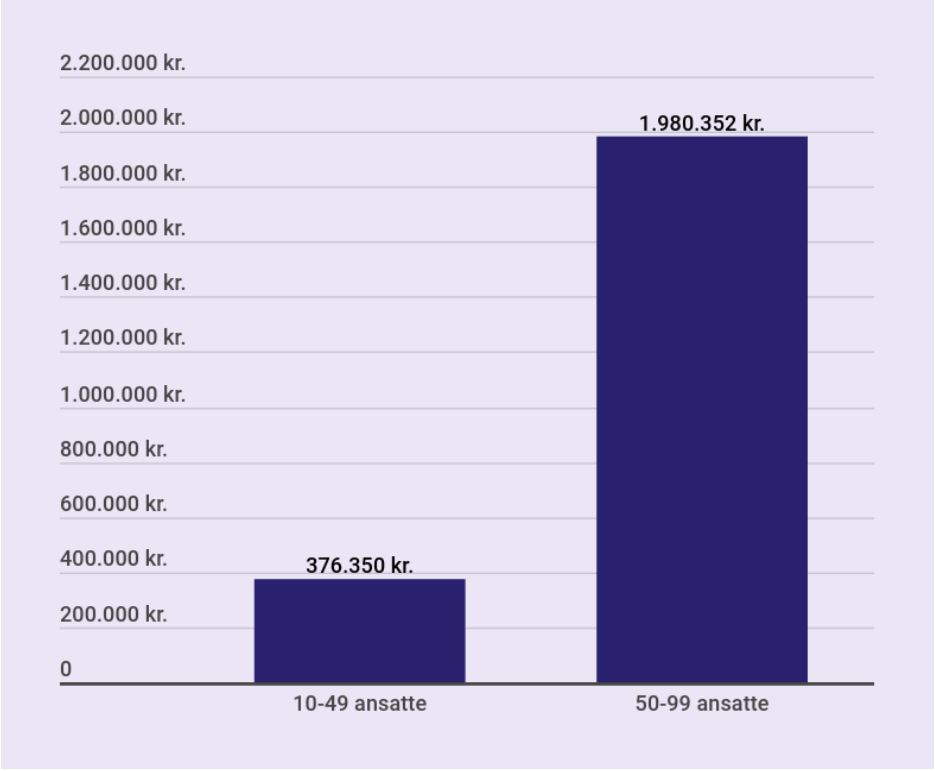
Sådan har vi gjort

I rapporten "Ransomware Uncovered 2020-2021" som er publiceret af GROUP-IB (Et af verdens førende modstandscentre for cyberkriminalitet og partner med både Interpol og Europol) fremgår det, at et gennemsnitligt ransomware angreb tvinger en virksomhed i 18 dages digital mørklægning.

En gennemsnitlig virksomhed med 10-49 ansatte har en omsætning på 2.688.214 kr. over 18 dage. 14 pct. af denne omsætning sker via e-handel, hvilket svaret til et omsætningstab via e-handel, som følge af digital mørklægning, på 376.350 kr. Disse tal er baseret på tal fra Regnskabsregistret og DST-ITAV13.

[1] Ransomware Uncovered 2020-2021, GROUP-IB

Gennemsnitlig tabt omsætning ved lukket e-handel i 18 dage fordelt på antal ansatte



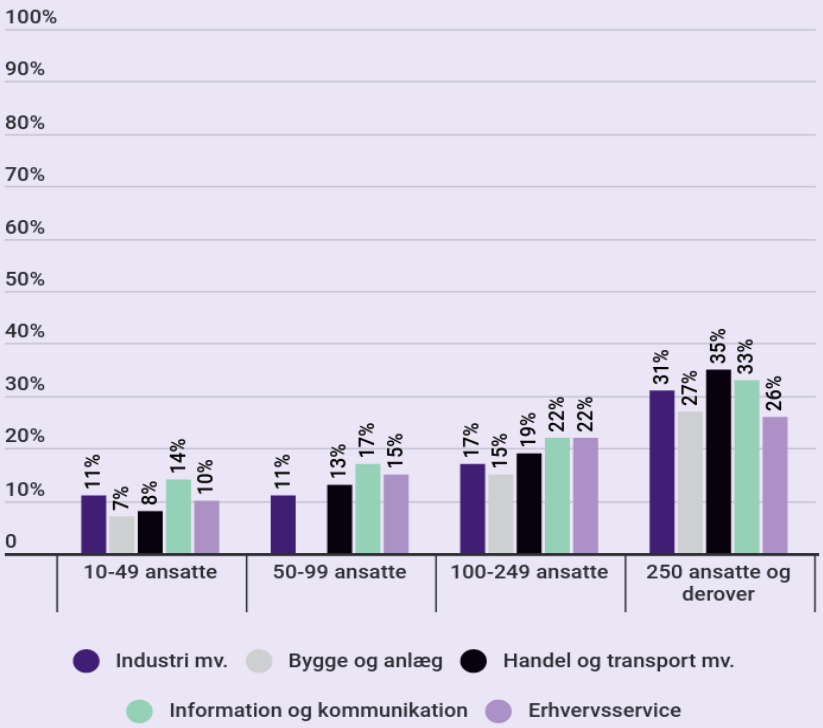
Kilde: Group-IB, Danmarks Statistiks forskeradgang Figur 4
Anm.: I beregningerne er det antaget, at ingen e-handler kan gennemføres i tilfælde af digital mørklægning.

Flere SMV'er oplever brud på IT-sikkerheden

Nedenstående figur angiver hvor mange procent, der i 2020 oplevede brud på IT-sikkerheden fordelt på brancher. Det ses således, at det ikke alene er store virksomheder som oplever brud på IT-sikkerheden, men i høj grad også de små og mellemstore virksomheder. 9 pct. af virksomhederne med 10-49 ansatte oplevede i 2020 brud på it-sikkerheden. Tallet er 13 pct. for virksomheder med 50-99 ansatte. Dykker man ned på brancheniveau ses det, at det i særlig høj grad er Information- og kommunikationsbranchen som er udsat. I denne branche har 14 pct. og 17 pct. af virksomhederne med hhv. 10-49 ansatte og 50-99 ansatte været udsat for brud på IT-sikkerheden. Det indebærer f.eks. malware (ondsindet software), herunder særligt ransomware, spoofing og Ddos-angreb. Alle sammen kritiske hackerangreb, som øger risikoen for, at SMV'erne mister deres forretningsgrundlag og i yderste konsekvens må dreje nøglen om.

Flere SMV'er oplever brud på IT-sikker-heden.

Andelen af virksomheder med brud på IT-sikkerheden i 2020 fordelt på brancher og antal ansatte



Kilde: DST- ITAV15 Figur 1

Anm: Private ikke-finansielle byerhverv

Coronakrisen har reduceret andelen af SMV'er som øger investeringer i IT-sikkerhed

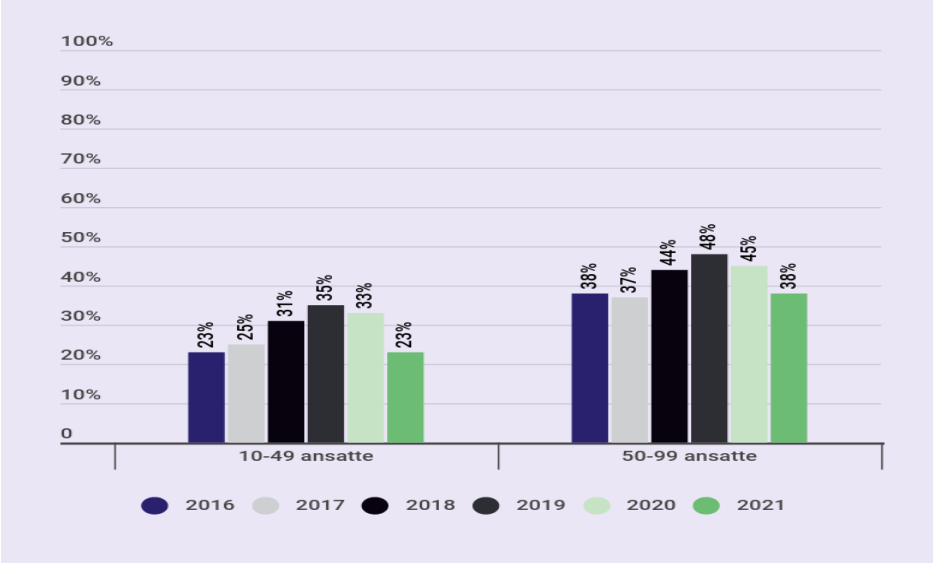
Færre SMV'er har øget investeringerne i IT-sikkerhed i 2021 sammenlignet med tidligere jf. nedenstående figur. Siden 2016 har der været en generel tendens til, at flere SMV'er har øget investeringerne i IT-sikkerhed.

Investeringerne for virksomhederne med 10-49 ansatte er faldet med 10 pct. point fra 2020 til 2021. Dermed er niveauet faldet til 2016-nivauet, som er det laveste for perioden. Faldet for virksomheder med 50-99 ansatte er på 7 pct. point og er ligeledes faldet til 2016-nivauet.

De relativt markante fald i andelen af virksomheder, som har øget investeringerne i IT-sikkerhed, skal ses i lyset af coronakrisen, hvor flere virksomheder har været økonomisk udfordret og derfor har været nødsaget til at prioritere anderledes end tidligere.

Færre SMV'er øger investeringerne i IT-sikkerhed sammenlignet med tidligere.

Andelen af virksomheder med stigende niveau af investering i IT-sikkerhed fordelt på antal ansatte



Kilde: DST-ITAV15 Figur 2

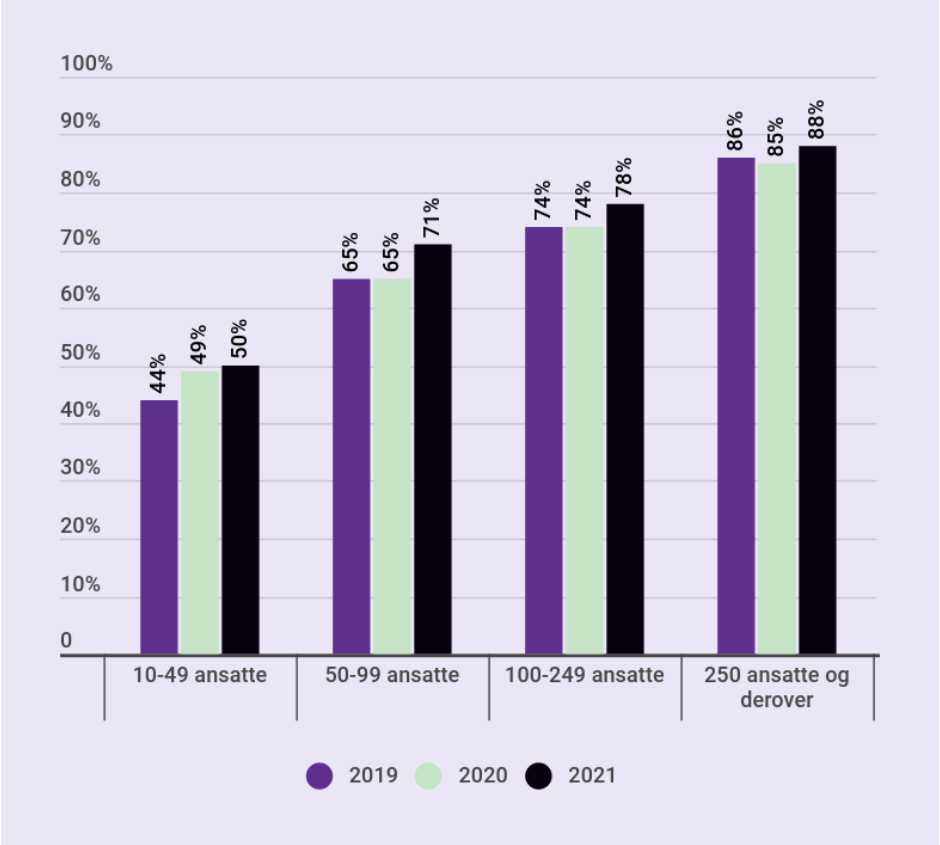
Anm.: Andelen af virksomheder med et faldende niveau for investeringer i IT-sikkerhed har ligget nogenlunde konstant over den angivne tidsperiode. Private ikke-finansielle byerhverv.

Halvdelen af de små virksomheder har i 2021 foretaget en risikoanalyse af virksomhedens IT

50 pct. af virksomhederne med 10-49 ansatte foretog i 2021 en risikoanalyse af deres IT-systemer. Det er en stigning på 6 pct. point sammenlignet med andelen i 2019. Den samme stigning ses for virksomhedsgruppen med 50-99 ansatte. Det fremgår altså, at virksomhederne i højere grad analyserer deres sårbarheder i forbindelse med IT-kriminalitet sammenlignet med tidligere. Denne tendens ses særligt blandt SMV'erne.

Halvdelen af de små virksomheder har foretaget en risikoanalyse i 2021.

Andel af virksomheder, som har fortaget en risikoanalyse vedr. deres IT-sikkerhed



Kilde: DST-ITAV15 Figur 2

Anm.: Andelen af virksomheder med et faldende niveau for investeringer i IT-sikkerhed har ligget nogenlunde konstant over den angivne tidsperiode. Private ikke-finansielle byerhverv.

Konklusion og politikforslag

Et ransomware angreb koster 376.350 kr. alene i tabt omsætning fra e-handel for en lille virksomhed med 10-49 ansatte. Coronakrisen har samtidig sat en kæp i hjulet for de mange virksomheder, som hvert år øgede deres investeringer i IT-sikkerhed. I lyset af, at truslen for cyberkriminalitet er på sit højeste, skal flere SMV'er have hjælp til at øge deres IT-sikkerhed. I 2020 steg antallet af ransomware angreb med 150 pct. på globalt plan.

I SMVdanmark forslår vi, at midlerne til SMV:Digital øges markant. Det er en tilskudspulje, hvor efterspørgslen i forvejen er stor, og som virksomhederne er begejstret for. Den 28. marts 2022 åbner SMV:Digital for en pulje, som er tilegnet rådgivning inden for digital sikkerhed. I øvrigt bør åbningen af denne pulje fremrykkes således, at virksomhederne har mulighed for gå øge deres IT-sikkerhed hurtigst muligt.

Hvis flere virksomheder kunne få del i netop denne pulje, ville det give et samlet løft til SMV'ernes digitale sikkerhed. Det vil reducere risikoen for cyberangreb og dermed stille danske SMV'er stærkere i det aktuelle trusselsbillede.

Kontakt

Konsulent Lasse Lundqvist, tlf. 41 29 20 09, lundqvist@SMVdanmark.dk.
Juniorkonsulent Anna Dose Stenild, stenild@smvdanmark.dk
SMVdanmark, marts 2021.