IT-sikkerhed i SMV’er

- Vejen til handling

Publiceret: 25. februar 2025

Af: Leif Vessty Dixon Kildelund og Martin Edwin Schjødt Nielsen

Forestil dig, at din virksomhed en morgen står stille. Ingen kan få adgang til systemerne, filerne er låst, og en løsesum kræves for at få dem tilbage. Det lyder som en fjern trussel for mange små og mellemstore virksomheder (SMV’er), men det er virkeligheden for flere end nogensinde før.

Cyberkriminalitet er en voksende global industri, der i 2025 forventes at omsætte for svimlende 10,5 billioner dollars. Det gør cyberkriminalitet til verdens tredjestørste industri (Cybersecurity Ventures, 2024). Danmark er verdens næstmest digitaliserede land (Ritzau, 2023), og derfor er vi et oplagt mål for den voksende cyberkriminalitet.

I 2022 kostede alene ransomware-angreb danske SMV’ere med 10-49 ansatte gennemsnitligt 376.350 kr. i tabt omsætning fra e-handel (SMVdanmark, 2022). På trods af de store økonomiske tab viser tal at kun 8% af SMV’erne benytter sig af efteruddannelsestilbud inden for IT-sikkerhed og at 51% af virksomhedsejere i SMV’ere ikke er klar over, at der findes relevante tilbud for dem og deres medarbejdere.

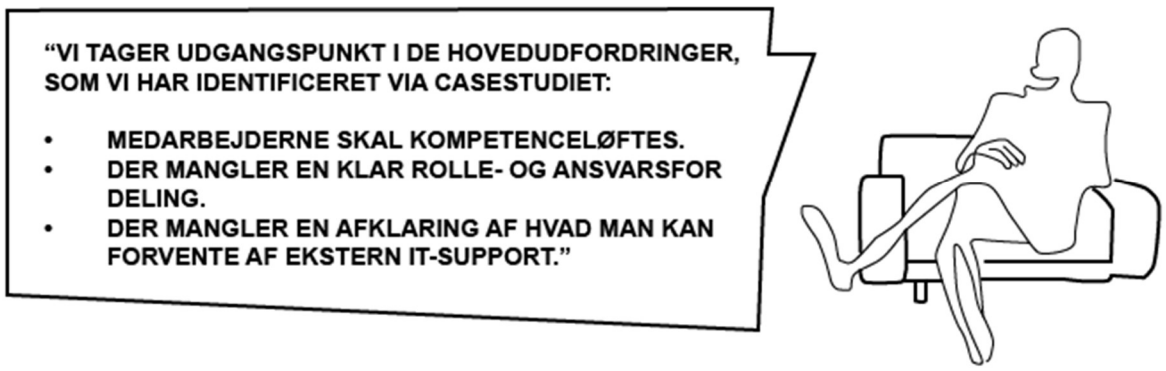
I denne kronik belyser vi SMV’ernes vigtigste udfordringer med IT-sikkerhed og præsenterer konkrete løsninger, der kan hjælpe virksomheder med at beskytte sig effektivt mod trusler.

Hvorfor vi undersøgte SMV'ernes IT-sikkerhed

Som IT-undervisere har vi undret os over SMV'ernes lave interesse for IT-sikkerhed, særligt når manglen på IT-sikkerhed har så store økonomiske konsekvenser. Det skabte en nysgerrighed hos os som ledte til nogle spørgsmål: Arbejder SMV'ere aktivt med IT-sikkerhed? Hvilke barrierer findes der for, at de engagerer sig i IT-sikkerhed? Og hvordan kan SMV’ere starte arbejdet med IT-sikkerhed?

For at undersøge disse spørgsmål nærmere har vi udført et mindre casestudie i en dansk virksomhed, hvor vi har undersøgt dens IT-sikkerhedspraksisser. Casestudiet har givet os indblik i, hvordan en SMV konkret arbejder med IT-sikkerhed og de specifikke barrierer, som virksomheden støder på i arbejdet med IT-sikkerhed. Denne viden kan være nyttig for andre SMV'er, sandsynligvis står overfor lignende udfordringer.

Da projektet bygger på et casestudie, giver det ikke et fuldstændigt billede af alle SMV'eres udfordringer, men det giver et indblik i, hvilke barrierer SMV'ere møder i arbejdet med IT-sikkerhed. Som læser kan du måske genkende nogle af de barrierer og udfordringer, der beskrives i casestudiet fra din egen virksomhed.



Vi tager udgangspunkt i de hovedudfordringer, som vi har identificeret via casestudiet:

- Medarbejderne skal kompetenceløftes.
- Der mangler en klar rolle- og ansvarsfordeling.
- Der mangler en afklaring af hvad man kan forvente af ekstern it-support.

For hver udfordring præsenterer vi konkrete løsninger, der kan hjælpe dig med at styrke IT-sikkerheden i din virksomhed.

Medarbejderne skal kompetenceløftes

Selv hvis du investerer i de bedste teknologier, kan din investering være værdiløs, hvis ikke dine medarbejdere ved, hvordan de skal bruge dem. F.eks. hjælper en stærk adgangskontrol til arbejdscomputere ikke, hvis de er efterladt ulåste.

IT-sikkerhed handler ikke kun om teknologi. Det handler lige så meget om adfærd og uddannelse. Det betyder f.eks., at dine medarbejdere skal vide, at de ikke skal klikke på mistænkelige links i e-mails. Hvis medarbejderne ikke forstår risikoen eller deres ansvar, og de ikke ved, hvordan de skal handle, når en farlig eller kritisk situation opstår, så er din virksomhed sårbar – uanset hvor gode (eller dyre) dine indkøbte systemer er.

Virksomhedsejeren vi interviewede, sagde:

"Jeg har et par gange tænkt, at det ville være klogt at samle medarbejderne omkring det her […] der skal jo bare være ét svagt led, jo ik'?"

Selvom mange SMV'ere erkender vigtigheden af IT-sikkerhed, tøver de med at tage næste skridt, da de enten ikke ved, hvordan sagen kan gribes an eller ikke anser sig som interessante mål for hackerne. Der mangler ofte viden om ansvar og rollefordeling, hvilket kan efterlade din virksomhed eksponeret og sårbar. Men hvor skal den viden komme fra? Her er det vigtigt, at

man som ledelse støtter op om efteruddannelse og skaber en stærk vidensdelingskultur, hvor medarbejderne kontinuerligt opdaterer og deler deres viden om IT-sikkerhed.

IT-sikkerhed bør ikke være noget, der kun diskuteres én gang om året; det skal være en integreret del af virksomhedens kultur og rutiner. IT-sikkerhed kan således være et fast tilbagevendende emne – enten månedligt eller kvartalsvist – hvor alle medarbejdere har mulighed for at opdatere deres viden, diskutere aktuelle trusler og løsninger, og hvor der løbende er fokus på kompetenceløft. Ved at fremme regelmæssig efteruddannelse og åbne diskussioner om IT-sikkerhed kan virksomheden sikre, at alle medarbejdere er rustet til at håndtere de udfordringer, som cybertruslerne medfører.

En fælles opmærksomhedskultur

Når medarbejderne har tilegnet sig grundlæggende IT-sikkerhedskompetencer, og en løbende dialog er etableret i virksomheden, opstår der et fundament for at drøfte ansvar og rollefordeling. Hvad er f.eks. Jyttes ansvar og rolle i marketing-afdelingen? Hvad er Michaels rolle i IT-afdelingen?

Det er vigtigt, at den enkelte medarbejder selv reflekterer over, hvad deres ansvar og rolle er, så de er klar til at tage deres del af ansvaret, hvis der skulle opstå en kritisk situation. Dette kræver en grundlæggende forståelse af IT-sikkerhed og dens betydning for virksomhedens data, processer og daglige drift.

Selvom IT-sikkerhed kan kræve tekniske løsninger, som ofte varetages af specialister eller IT-leverandører, er det vigtigt, at alle medarbejdere er en del af løsningen. En opmærksomhedskultur kan være en af de mest effektive forsvarsmekanismer mod cybertrusler.

Ledelsen skal sikre klare tekniske krav og rammer, og at medarbejderne er klædt på til at:

- Genkende og håndtere phishingmails og anden hverdagssvindel.
- Bruge stærk adgangskontrol, f.eks. Multifaktor autentificering.
- Rapportere mistænkelig aktivitet hurtigt og til de rette personer.

Derudover er det også lederens ansvar at skabe de rette betingelser for medarbejderne, herunder at de:

- Besidder de nødvendige grundlæggende IT-sikkerhedskompetencer og løbende har mulighed for at udvikle dem.
- Deltager i en åben og kontinuerlig dialog om IT-sikkerhed i virksomheden.
- Forstår deres specifikke rolle og det ansvar, der følger med.

Samspillet mellem ledelse og medarbejdere er afgørende for at skabe en stærk IT-sikkerhedskultur. Når IT-sikkerhed bliver en integreret del af den daglige drift, står virksomheden stærkere mod både nuværende og fremtidige cybertrusler.

Hvem har ansvaret for din backup?

De fleste virksomheder opbevarer kritiske data i deres IT-systemer – f.eks. kundeordrer, arbejdstider og leverandørbestillinger – som er uundværlige for den daglige drift. Men hvad

sker der, hvis disse data pludselig bliver utilgængelige? Backup er løsningen, men det kræver, at virksomhederne sikrer, at data er kopieret og gemt pålideligt flere steder.

En backup-løsning bør altid være en central del af virksomhedens IT-strategi, især når data er kritiske for forretningsdriften. Men hvordan sikrer man, at backup-løsningen fungerer efter behov? Som virksomhedsejeren forklarede i interviewet:

"Den ligger i skyen, og det betaler vi jo en hel del penge for, og den bliver opdateret hele tiden. Og der stoler vi på, at det sker […] Det kan I roligt regne med, at den gør, siger vores leverandør."

Det er naturligt at have tillid til en leverandør, men det er vigtigt at sikre, at aftalen afspejler virksomhedens behov og forventninger – og det kræver, at man stiller de rette spørgsmål. At købe IT-ydelser og-systemer er ikke som at købe en bil, hvor man forventer, at grundlæggende funktioner som fastmonterede hjul er en selvfølge. IT-systemer og -ydelser kræver mere opmærksomhed og stillingtagen fra køberens side. For at sikre at IT-sikkerhedsløsningen lever op til virksomhedens behov, bør indkøberen stille konkrete krav til leverandøren. Her bør fokus både være på at beskytte virksomhedens drift og for at værne om kundernes data. En god begyndelse er at vurdere værdien af virksomhedens data og afgøre, hvor længe virksomheden kan klare sig uden dem.

Lad os tage udgangspunkt i et kendt eksempel og se på, hvilke spørgsmål man med fordel kunne stille til leverandøren.

Stil de rigtige spørgsmål til din IT-leverandør

Mange har hørt om Chili Klaus, der mistede adgang til sin webshop, da hans IT-leverandør blev udsat for et hackerangreb, hvor al data blev utilgængelig. Det betød, at kunderne ikke kunne benytte Chili Klaus' hjemmeside, og det resulterede i tabt omsætning og en ukendt tidsramme for genopretning.

For at undgå en lignende situation kunne Chili Klaus, stille sin (formodentlig nye) IT-leverandør følgende spørgsmål:

- Hvad gør IT-leverandøren for at beskytte webshoppen mod uønsket adgang til data?
- Hvad er ansvarsfordelingen mellem virksomhed og IT-leverandør?

- Hvad gør IT-leverandøren for at sikre webshoppen tilgængelighed for kunderne? Kan kunderne stadig få adgang til hjemmesiden?.

Desuden bør svarene være specifikke og tidsbestemte, når man stiller nedenstående spørgsmål:

- ”Hvor ofte tages der backup?”
- ”Hvad tages der backup af?”
- ”Hvor ofte tester I backuppen?”.

En overvejelse, der kan hjælpe Chili Klaus med at konkretisere disse spørgsmål yderligere, kunne være:

- Hvor meget data kan vi tåle at miste?
- Hvis vores system bliver angrebet kl. 12:30, kan vi så acceptere kun at kunne gendanne kundeordre frem til kl. 12:00?

Ovenstående overvejelser er afgørende for at fastlægge kravene til backup-systemet.

Vær opmærksom på, hvad der konkret aftales. Man skal f.eks. ikke acceptere, at en IT-leverandør fortæller, at de tager backup ”regelmæssigt”, ”hele tiden” eller ”jævnligt”. Det skal konkretiseres, så det f.eks. bliver defineret som ”ugentligt, månedligt eller halvårligt”. Ved at stille de rigtige spørgsmål og definere klare krav kan ledelsen beskytte virksomheden bedre mod fremtidige trusler.

Sådan kommer du i gang

Enhver virksomhed bør følge op på de officielle retningslinjer fra sider som sikkerdigital.dk, som tilbyder enkle råd om alt fra phishing-beskyttelse til backup-strategier. Det er Ministeriet for Samfundssikkerhed og Beredskab, der i samarbejde med en række partnere, står bag Sikkerdigital.dk.

For at få en fornemmelse af virksomhedens sårbarhed, kan man gennemføre simulerede phishing-kampagner med et link og på den måde øge opmærksomheden på IT-sikkerhed i organisationen. Antallet af klik på det simulerede link, kan give konkret indsigt i, hvordan medarbejderne forholder sig til risiciene ved at klikke på ukendte links. Resultaterne af en sådan test giver et billede af organisationens nuværende opmærksomhedsniveau. Det giver indblik og mulighed for at følge op med målrettede oplysningskampagner, der styrker medarbejdernes forståelse og bevidsthed. Det kan også fungere som et dialogværktøj mellem dig og medarbejderne, så de "svage led" bliver styrket i forhold til IT-sikkerhed. Når der er en åben dialog mellem ledelsen og de ansatte om IT-sikkerhed, kan det hjælpe med at opbygge en kultur, hvor medarbejderne er bedre rustet til at navigere sikkert i deres e-mails.

Endelig er der mange puljer, som man kan søge til opkvalificering af medarbejdere. Selv små tiltag, som f.eks. at opdatere sin software regelmæssigt og efteruddannelse af ens medarbejderne i sikker IT-adfærd kan gøre en forskel. Der er mange gode ressourcer at finde online, nedenfor følger et lille udpluk:

- SMVDigital som tilbyder løbende tilskud til styrkelsen af cybersikkerhed.
- NC3 Erhverv tilbyder, at man kan bestille en IT-ekspert til ens virksomhed og har særligt fokus på IT-sikkerhed for SMV'ere.
- CFCS har flere forskellige lavpraktiske vejledninger til, hvordan man kan komme i gang med at arbejde med IT-sikkerhed.

Cybertrusler er en realitet, og fremtiden bliver kun mere digital – både for muligheder og trusler. Men ved at starte processen nu, hjælper du med at beskytte din virksomhed og bidrage til en mere sikker digital økonomi.

Lad os alle tage ansvar for en tryg digital fremtid, ét lille skridt ad gangen.