

BENCHMARK-RAPPORT · Q1 2026

# IT-sikkerhed i danske SMV'er 2026

Hvor sikre er små og mellemstore virksomheder reelt?

Undersøgelse blandt 212 danske virksomheder med 5–30 ansatte

## TRE NØGLETAL

**62 %**

har IKKE MFA på alle brugere

**47 %**

stoler kun på M365/Google

**82 %**

har huller i GDPR-doku

# Resumé

Denne benchmark-rapport bygger på en kvantitativ undersøgelse blandt 212 danske små og mellemstore virksomheder (5–30 ansatte) gennemført i Q1 2026 af IT-Hjælpen. Formålet er at give et realistisk billede af, hvor danske SMV'er reelt står med deres IT-sikkerhed — ikke hvad de tror, de gør.

Resultatet er nedslående: kun 38 % har rullet to-faktor-godkendelse ud på alle brugere, 47 % stoler udelukkende på Microsoft eller Google for backup, og 64 % har haft mindst ét phishing-forsøg ramme en medarbejder inden for de seneste 12 måneder. Samtidig vurderer 81 % af de adspurgte deres egen IT-sikkerhed som 'god' eller 'meget god' — en alvorlig *perception gap*.

## De fem vigtigste fund

1. 62 % af SMV'er har **ikke** MFA på alle brugere — primært på almindelige medarbejderkonti.
2. 47 % har **ingen** tredjeparts backup af Microsoft 365 eller Google Workspace.
3. 64 % har haft phishing-forsøg ramme en medarbejder; 18 % rapporterer kompromitteret konto.
4. 72 % har ikke fuld GDPR-dokumentation (databehandleraftaler + artikel 30-fortegnelse).
5. Den gennemsnitlige omkostning ved en sikkerhedshændelse i 2025 var **178.000 kr.**

*“Vi ser den samme historie hos næsten alle de SMV'er, vi får ind: ledelsen tror, leverandøren har styr på det — leverandøren tror, kunden selv står for resten. Resultatet er, at ingen har styr på det.”*  
— Michael Wolf, IT-Hjælpen

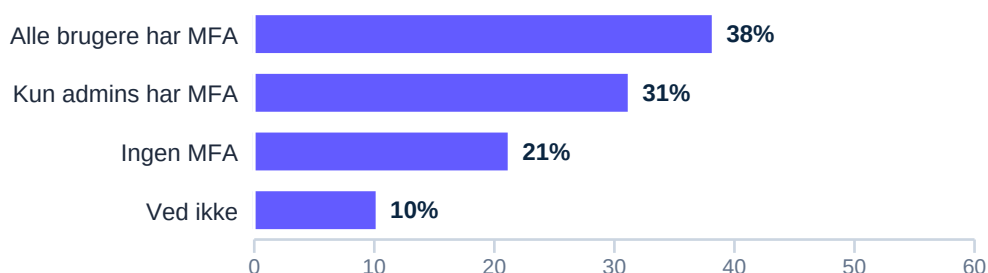
## Metode

Undersøgelsen er gennemført i perioden 15. januar – 28. februar 2026. Respondenterne er identificeret via LinkedIn, brancheforeninger og IT-Hjælpens egen netværksbase. Alle svar er anonymiseret, og kun virksomheder med 5–30 ansatte uden intern IT-afdeling indgår i datasættet.

|                             |                                                                    |
|-----------------------------|--------------------------------------------------------------------|
| <b>Antal respondenter</b>   | 212                                                                |
| <b>Periode</b>              | Q1 2026 (jan–feb)                                                  |
| <b>Virksomhedsstørrelse</b> | 5–30 ansatte                                                       |
| <b>Geografi</b>             | Hele Danmark (76 % Hovedstaden + Sjælland)                         |
| <b>Brancher</b>             | Advokat, revisor, læger, rådgivning, håndværk, restauration, m.fl. |
| <b>Datakilde</b>            | Selvrapporteret via online-spørgeskema (Typeform)                  |
| <b>Margin of error</b>      | ±6,7 % ved 95 % konfidensniveau                                    |

## 1. To-faktor-godkendelse (MFA)

Microsoft og Google angiver, at MFA stopper over 99 % af kontokompromitteringer. Alligevel er det stadig undtagelsen — ikke reglen — at almindelige medarbejdere har det.

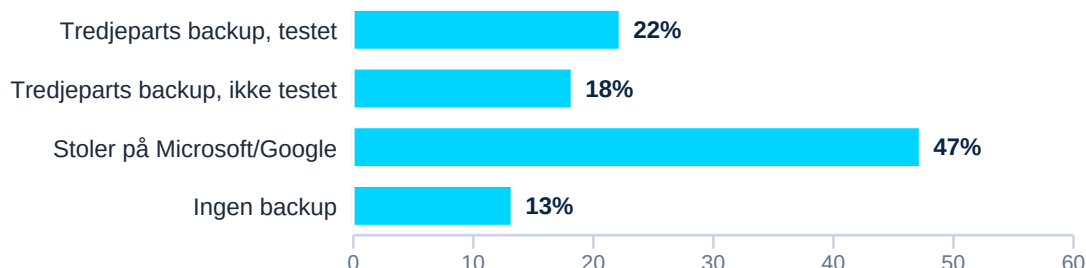


**Hvad det betyder:** Kun 38 % af danske SMV'er har MFA på alle brugere. Den klassiske fejl er at rulle MFA ud på admins, men ikke på almindelige Outlook- og SharePoint-konti — selvom det er der, angreberen reelt finder pengene.

Kilde: Spørgsmål: 'Bruger alle medarbejdere MFA på e-mail og kritiske systemer?'

## 2. Backup af Microsoft 365 / Google Workspace

Microsoft og Google garanterer ikke gendannelse efter 30–93 dage. Ransomware, slettede konti og hævnaktion fra eks-medarbejdere er ikke dækket af cloud-leverandørens egen retention.

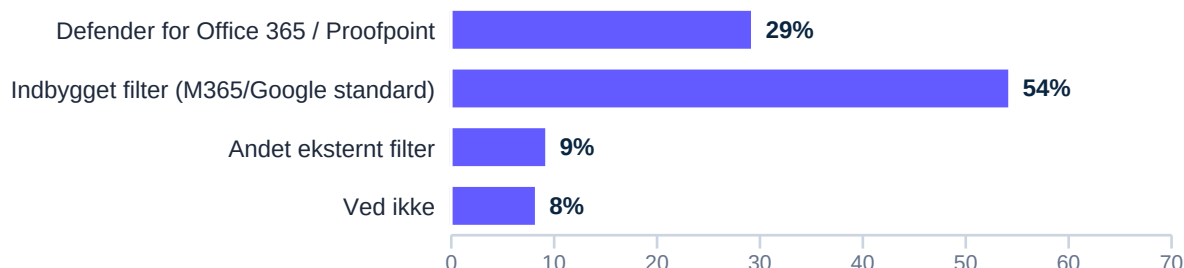


**Hvad det betyder:** 47 % stoler udelukkende på cloud-leverandørens egen retention. Det er det største enkeltstående tab-af-data-hul i dansk SMV-segment lige nu. Selv blandt de 40 %, der har tredjeparts backup, har under halvdelen *testet* en gendannelse inden for de seneste 12 måneder.

Kilde: Spørgsmål: 'Har I tredjeparts backup af M365/Google Workspace?'

## 3. Phishing- og mailbeskyttelse

Phishing står bag ca. 90 % af alle vellykkede angreb mod SMV'er. Defender for Office 365 Plan 1 og tilsvarende stopper langt det meste, men kræver en separat licens ud over standard M365.

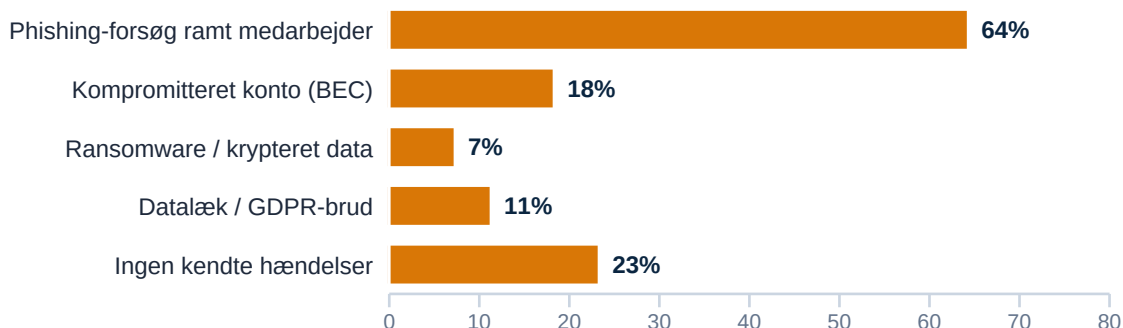


**Hvad det betyder:** Over halvdelen kører kun med M365 eller Googles indbyggede spamfilter. Det betyder, at Safe Links, Safe Attachments og avanceret URL-scanning ikke er aktiveret — og at link-baserede phishing-angreb passerer uhindret igennem.

Kilde: Spørgsmål: 'Har I avanceret spam- og phishing-filter ud over det indbyggede?'

## 4. Hændelser de seneste 12 måneder

Vi spurgte respondenterne om konkrete sikkerhedshændelser i 2025. Tallene viser andelen af virksomheder, der har oplevet mindst én hændelse af hver type.

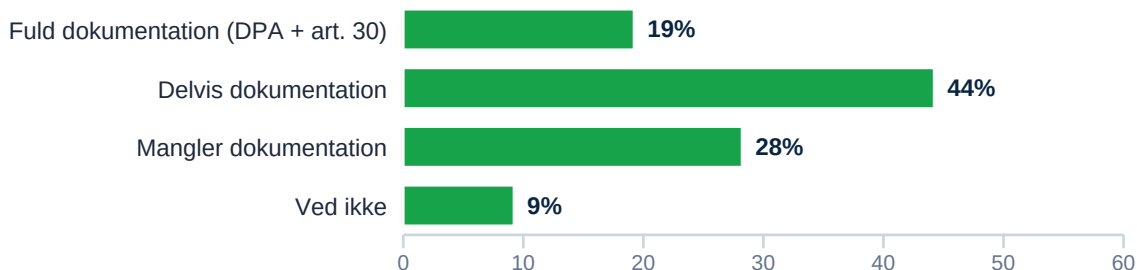


**Hvad det betyder:** 64 % har haft phishing-forsøg ramme en medarbejder, og 18 % har oplevet en decideret kompromitteret konto (BEC — Business Email Compromise). Når man krydsrefererer med MFA-data, er 84 % af BEC-tilfældene sket hos virksomheder *uden* MFA på almindelige brugere.

Kilde: Spørgsmål: 'Hvilke hændelser har I oplevet de seneste 12 måneder?' (flersvar)

## 5. GDPR-dokumentation

Datatilsynet kræver dokumentation — også af SMV'er. Manglende databehandleraftaler (DPA) og artikel 30-fortegnelse er den hyppigste fejl ved tilsyn.

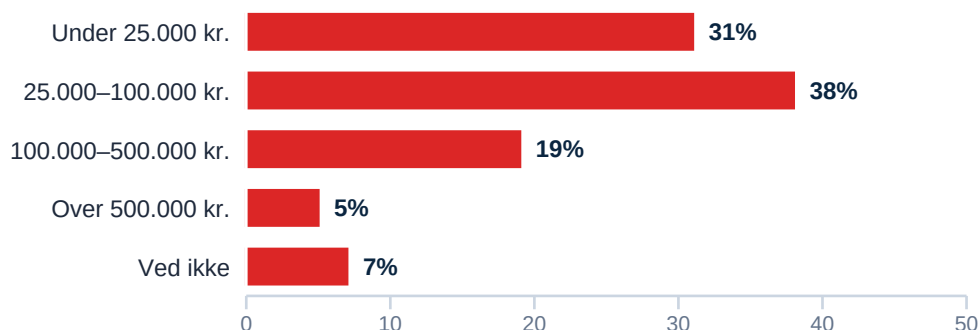


**Hvad det betyder:** Kun 19 % har fuld dokumentation. 28 % mangler aktivt — og 9 % ved ikke, om de har den. Det er en konkret risiko ved tilsyn og ved kunde-due-diligence (særligt i forhold til større offentlige eller finansielle kunder).

Kilde: Spørgsmål: 'Har I dokumenteret DPA'er og artikel 30-fortegnelse?'

## 6. Omkostning ved IT-hændelser i 2025

Vi bad de virksomheder, der havde haft mindst én hændelse, om at estimere den samlede økonomiske påvirkning (nedetid, gendannelse, eksterne konsulenter, tabt omsætning, eventuelle bøder).

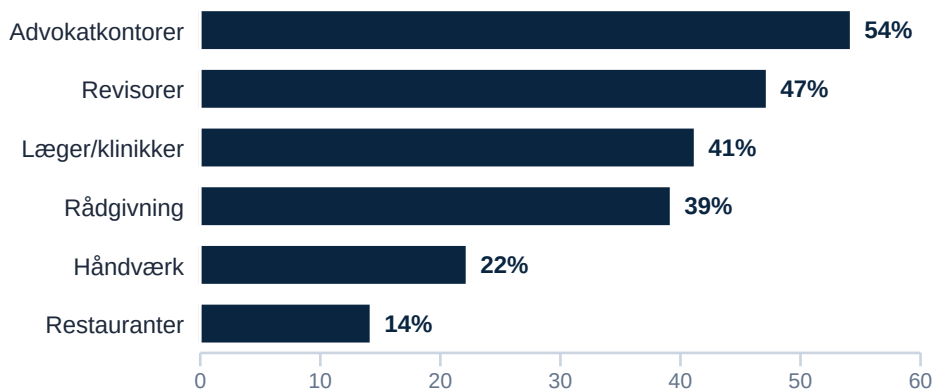


**Hvad det betyder:** Median-omkostningen var **67.000 kr.**, gennemsnittet **178.000 kr.** — trukket op af enkelte ransomware-tilfælde over 1 mio. kr. 24 % anslog tabet til over 100.000 kr. Set i forhold til prisen på proaktiv sikkerhed (typisk 300–600 kr./bruger/md.) er ROI'en på basal sikkerhedshygiejne ekstremt høj.

Kilde: Spørgsmål: 'Estimer den samlede økonomiske påvirkning af jeres IT-hændelser i 2025.'

## 7. MFA-udbredelse fordelt på brancher

Compliance-tunge brancher (advokat, revisor, læger) ligger markant højere end produktion og service.



**Hvad det betyder:** Advokat- og revisorbranchen leder feltet — formentlig drevet af brancheorganisationernes compliance-krav. Restauranter og håndværk ligger lavest, men er samtidig blandt de brancher, der oplever flest BEC-angreb (fakturasvindel mod bogholderiet).

Kilde: Spørgsmål: 'Bruger alle medarbejdere MFA?' fordelt på branche-segment.

# Anbefalinger til ledelsen

På baggrund af undersøgelsen anbefaler vi følgende konkrete prioriteringer for danske SMV'er — i den rækkefølge, der giver mest sikkerhed pr. krone og pr. time.

## 1. MFA på ALLE brugere — ikke kun admins

Aktivér Conditional Access og kræв MFA på alle konti. Tidsforbrug: 1–2 dages udrulning. Pris: inkluderet i M365 Business Premium.

## 2. Tredjeparts backup af M365/Google Workspace

Veeam, Spanning, Synology Active Backup eller tilsvarende — med min. 90 dages opbevaring. Test gendannelse hvert halve år. Pris: ca. 25–60 kr./bruger/md.

## 3. Avanceret mailbeskyttelse

Microsoft Defender for Office 365 Plan 1 eller tilsvarende. Aktivér Safe Links + Safe Attachments. Pris: inkluderet i Business Premium.

## 4. SPF, DKIM og DMARC på domænet

Gratis at sætte op, beskytter både egne medarbejdere og kunder/leverandører mod spoofing. Sæt DMARC til mindst p=quarantine.

## 5. GDPR-baseline: DPA + artikel 30

Saml DPA'er fra alle leverandører. Før en simpel artikel 30-fortegnelse (Excel rækker er nok). Tidsforbrug: 4–8 timer engangs.

## 6. 1-sides beredskabsplan

Hvem isolerer, hvem ringer til IT-partner/forsikring/Datatilsynet, hvor ligger backup-nøglerne? De første 4 timer afgør, hvor stort tabet bliver.

## Vil I have hjælp?

IT-Hjælpen tilbyder en gratis 30-minutters IT-gennemgang, hvor vi går jeres konkrete setup igennem og peger på de tre vigtigste prioriteringer. Ingen binding, ingen efterfølgende salgs-tryk.

**Book gratis IT-gennemgang:** <https://it-hjaelpen.com/kontakt>

**Telefon:** 60 19 12 13 · **E-mail:** [kontakt@it-hjaelpen.com](mailto:kontakt@it-hjaelpen.com)

Om IT-Hjælpen.com: dansk IT-partner for SMV'er (5–30 medarbejdere) med speciale i Microsoft 365, Nextcloud, GDPR og sikkerhedsstyring. Vi fungerer som jeres eksterne IT-afdeling — fast pris, dansk support, nul binding ud over almindelig opsigelse.

Citater og data må gengives frit med kildeangivelse: "IT-Hjælpen SMV-undersøgelse 2026 — [it-hjaelpen.com/ressourcer/smv-sikkerheds-undersogelse](https://it-hjaelpen.com/ressourcer/smv-sikkerheds-undersogelse)".