itnu

RAPPORT · 2026

Cybersikkerhed 2026

Det danske trusselsbillede — og hvad en mindre virksomhed faktisk kan gøre ved det.

ITNU · Personlig IT-partner for danske SMV'er

FORORD

At drive virksomhed digitalt er blevet *et grundvilkår* — og det forpligter

Cybersikkerhed er på få år gået fra at være noget, IT-afdelingen tog sig af, til at være en del af selve det at drive forretning. For de fleste danske virksomheder er spørgsmålet ikke længere *om* de bliver forsøgt ramt — men hvornår, hvordan, og om de overhovedet opdager det.

Jeg har arbejdet med IT i over 30 år, og jeg har set udviklingen tæt på. Hvor en virus engang generede en enkelt computer, kan et angreb i dag lægge en hel virksomhed ned — låse filerne, stoppe driften og koste både penge og kunder. Samtidig er angrebene blevet automatiserede. De leder ikke efter store navne. De leder efter åbne døre.

Og her er den gode nyhed: de fleste åbne døre er de samme. Svage adgangskoder. Manglende to-faktor-login. En backup, ingen har testet. En medarbejder, der aldrig har fået vist, hvordan en phishing-mail ser ud. Det er sjældent raketvidenskab. Det er disciplin — og det er noget, selv en lille virksomhed kan komme i mål med.

Denne rapport samler det danske trusselsbillede anno 2026, som det ser ud fra betroede kilder — det danske trusselsniveau fra Center for Cybersikkerhed, suppleret med de nyeste internationale 2026-rapporter fra bl.a. Verizon, Microsoft og CrowdStrike — og oversætter det til noget, en almindelig virksomhed kan handle på. Ikke for at skræmme. For at gøre klar.

2026 bliver året, hvor cybersikkerhed for alvor skal flytte sig fra bekymring til hverdag. Lad os komme i gang.

Allan Schmidt

Stifter, ITNU · Personlig IT-partner

INDHOLD

Hvad du finder i rapporten

Om tallene i rapporten

Alle nøgletal stammer fra offentligt tilgængelige, betroede kilder — bl.a. Center for Cybersikkerhed (DK), Verizon, Microsoft, CrowdStrike og UK's Cyber Security Breaches Survey. Kildehenvisninger står ved hvert tal og samlet på sidste side.

KAPITEL 01 · TRUSSELSBILLEDET 2026

Truslen er blevet *et grundvilkår*

Danske myndigheder, virksomheder og borgere udsættes for cyberangreb hver eneste dag — fra både statslige og kriminelle aktører. Truslen fra cyberkriminalitet vurderes i dag til det højeste niveau på skalaen.

MEGET HØJ

Trusselsniveauet fra cyberkriminalitet mod Danmark — det højeste på en femtrins-skala.

KILDE: STYRELSEN FOR SAMFUNDSSIKKERHED, CYBERTRUSLEN MOD DANMARK 2025

Ransomware på rekordniveau

Ransomware indgår nu i 48% af alle databrud — op fra 44% året før. Den gode nyhed: 69% af ofrene vælger ikke at betale.

KILDE: VERIZON DBIR 2026

Små virksomheder rammes også

I Storbritannien blev 42% af mikrovirksomheder og 46% af små virksomheder ramt af cyberbrud eller -angreb det seneste år. De lavere tal hos de mindste afspejler ofte, at brud ikke opdages — ikke at de udebliver.

KILDE: UK CYBER SECURITY BREACHES SURVEY 2025/26

KAPITEL 02 · TALLENE DU BØR KENDE

Seks tal, der tegner billedet

Du behøver ikke være ekspert for at forholde dig til risikoen. Her er de tal fra betroede kilder, jeg oftest bruger, når jeg taler med en ny virksomhed.

43%

af virksomheder blev ramt af cyberbrud eller -angreb inden for de seneste 12 måneder (mikro 42%, små 46%).

UK CSBS 2025/26

48.185

nye sårbarheder (CVE'er) blev registreret i 2025 — en stigning på ca. 20,6% fra året før.

CVE-PROGRAMMET / NVD, 2025

48%

ransomware indgår nu i næsten halvdelen af alle databrud.

VERIZON DBIR 2026

62%

af databrud involverer en menneskelig faktor — et klik, en fejl, et stjålet kodeord.

VERIZON DBIR 2026

$4,44 mio.

global gennemsnitsomkostning ved ét databrud.

IBM, 2025

29 min

gennemsnitstiden fra angriberen er inde, til spredningen begynder.

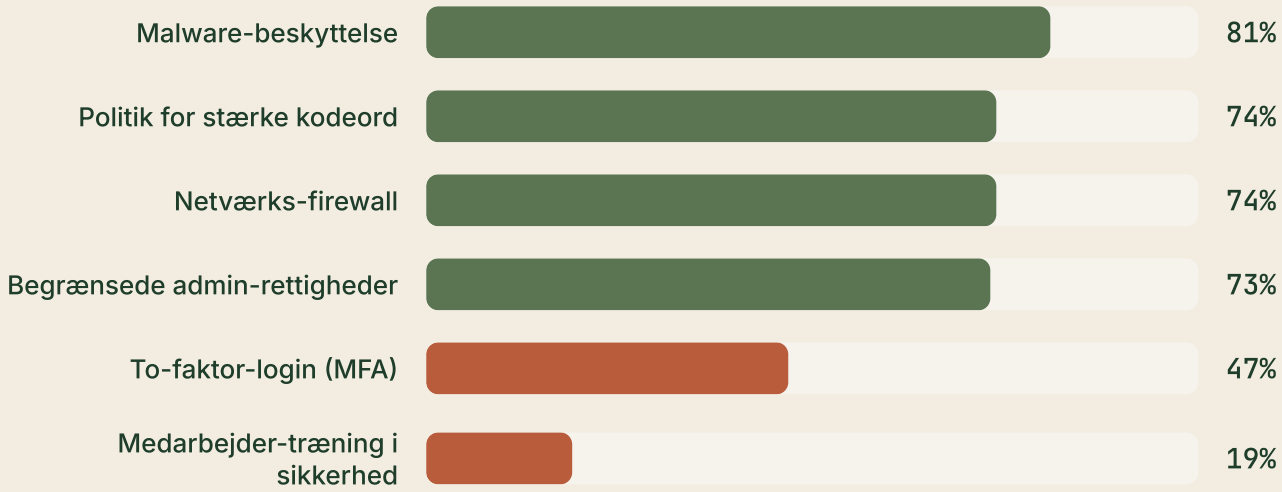
CROWDSTRIKE 2026

Tallene er ikke til for at skræmme. De er til for at prioritere — så indsatsen lander der, hvor risikoen faktisk er.

KAPITEL 03 · HVOR LANGT ER VIRKSOMHEDERNE NÅET?

Det grundlæggende er på vej — men ikke i mål

Blandt virksomheder generelt er de basale kontroller udbredte — men de to vigtigste menneskelige tiltag halter.



KILDE: UK GOVERNMENT (DSIT) — CYBER SECURITY BREACHES SURVEY 2025/26

Allans bemærkning

Læg mærke til de to orange søjler. To-faktor-login bruges kun af knap halvdelen, og medarbejder-træning er endda faldet siden sidste år. Det er præcis de to ting, der koster mindst — og forhindrer mest. Mønsteret er det samme hos danske SMV'er.

KAPITEL 04 · VI ER FOR SMÅ TIL AT VÆRE INTERESSANTE

"Vi er for små til at *være interessante*"

Det er den sætning, jeg oftest hører på et første møde. Og det er den, der koster danske virksomheder mest.

For ti år siden gav den måske mening. I dag gør den ikke. De fleste angreb er automatiserede og leder efter *svagheder* — ikke firmastørrelse. En offentligt tilgængelig login-portal, en genbrugt adgangskode, en server der ikke er opdateret, eller en konto uden ejer der både er gemt og glemt. Det er nok.

For angriberen er en mindre virksomhed ofte et nemmere mål: der er færre øjne på loggene, færre processer og hurtigere afkast. Du bliver ikke valgt, fordi du er stor. Du bliver valgt, fordi du er åben. Og de mindste er ikke beskyttet af deres størrelse: kun 21% af mikrovirksomheder har overhovedet en nedskrevet beredskabsplan. (KILDE: UK CSBS 2025/26)

Maskiner scanner alt

Angreb begynder sjældent med et menneske, der vælger dig. De begynder med en bot, der scanner internettet for kendte svagheder — døgnet rundt, uden at skelne.

Færre øjne, hurtigere vej ind

I en lille virksomhed er der sjældent nogen, der holder øje med loggene. Det gør vejen fra kompromittering til skade kortere — og opdagelsen langsommere.

Sikkerhed handler ikke om at være stor nok. Det handler om at have syn, sans og styr på sit eget.

KAPITEL 05 · DE OTTE HULLER

De otte huller, jeg ser *igen og igen*

På tværs af de virksomheder jeg arbejder med, går de samme svagheder igen. Den gode nyhed: de er alle sammen til at lukke — uden et stort budget.

01 **Svage og genbrugte adgangskoder**
Den samme kode på flere tjenester betyder, at ét læk åbner mange døre.

02 **To-faktor-login mangler — eller kun delvist**
MFA på ledelsens konti, men ikke på fællespostkasser og servicekonti.

03 **Backup, ingen har testet**
En backup, der aldrig er gendannet, er en forhåbning — ikke en sikkerhed.

04 **Manglende, systematisk patching**
Kendte sårbarheder — især på internetvendte systemer — er nu angribernes vigtigste vej ind: 31% af databrud starter her, og udnyttelsen sker i snit, før en patch overhovedet findes.

05 **For mange administrator-rettigheder**
Når alle er administratorer, kan ét klik kompromittere hele huset.

06 **Ingen logning eller overvågning**
Uden øjne på miljøet opdages et brud først, når kunden ringer.

07 **Ingen awareness blandt medarbejdere**
Folk klikker på det, de aldrig har lært at genkende som farligt.

08 **Ingen afprøvet beredskabsplan**
Når skærmene bliver sorte, er det for sent at finde ud af, hvem der gør hvad.

KAPITEL 06 · TO-FAKTOR I DYBDEN

To-faktor-login er stadig *den billigste forsikring*

47%

Knap halvdelen af virksomhederne bruger i dag to-faktor-login. Det betyder, at over halvdelen stadig kan kompromitteres med ét stjålet kodeord.

KILDE: UK CSBS 2025/26

Hvorfor det virker så godt

De fleste angreb mod konti handler ikke om at "knække" en kode — men om at bruge en, der allerede er lækket eller gættet. To-faktor-login lukker den dør, fordi koden alene ikke længere er nok. Det stopper langt de fleste automatiserede forsøg på stedet. Microsoft opgør, at 97% af identitetsangreb er password-angreb — og at phishing-resistent MFA stopper over 99% af dem.

Den vigtigste pointe: ingen konto må stå udenfor. Brugere og administratorer skal have MFA, fællespostkasser skal have blokeret direkte login, og servicekonti skal gennemgås med færrest mulige rettigheder — især den gamle administrator, ingen rigtig bruger længere. Det er typisk dér, hullet sidder.

Gør det i denne uge

Slå MFA til på alle brugere og administratorer i jeres Microsoft 365, blokér direkte login på fællespostkasser, og gennemgå servicekonti med færrest mulige rettigheder. Det er den enkeltstående ændring, der flytter mest.

KAPITEL 07 · TEST OG OVERVÅGNING

Du kan kun beskytte *det, du kan se*

Mange virksomheder føler sig trygge, fordi de har investeret i sikkerhed. Men uden test og overvågning er det kun en følelse. Moderne angreb er sjældent et stort brag — de forløber stille, i flere trin, og ligner helt almindelig drift. Og de går hurtigt: gennemsnitstiden fra første adgang til spredning er nede på 29 minutter, og 82% af angreb bruger slet ikke malware — de bruger gyldige konti og legitime værktøjer.

(KILDE: CROWDSTRIKE GLOBAL THREAT REPORT 2026)

Overvågning

Et usædvanligt login midt om natten, en ny mail-regel, et stort download fra et cloud-drev. Hver for sig ser de harmløse ud. Værdien opstår, når nogen ser mønsteret — og når alarmen lyder, før skaden vokser.

Test

Sikkerhedsværktøjer, politikker og awareness har alle en værdi. Men uden at teste dem antager man bare, at de virker. En test giver fakta i stedet for følelser — og viser hullerne, før en angriber gør.

Sådan kommer en mindre virksomhed nemt i gang

01 **Start med de vigtigste kilder**
Microsoft 365, brugeridentiteter, endpoint-beskyttelse og firewall. Det er her, det meste sker.

02 **Definér få, skarpe alarmer**
Login fra nye lande uden for arbejdstid, oprettelse af admin-konti, ændringer i MFA-opsætning, nye mail-regler, masse-download fra cloud og mistænkelige OAuth-app-godkendelser.

03 **Aftal roller på forhånd**
Hvem spærrer adgang, hvem kontakter brugeren, hvem dokumenterer — og hvornår eskaleres der?

KAPITEL 08 · MENNESKER SOM FORSVARSLINJE

Den vigtigste firewall sidder *ved tastaturet*

62%

af alle databrud involverer en menneskelig faktor — et klik, en fejl, en genbrugt adgangskode.

KILDE: VERIZON DBIR 2026

19%

af virksomhederne tilbyder nogen form for medarbejder-træning i sikkerhed — og andelen er faldende.

KILDE: UK CSBS 2025/26

Når godt seks ud af ti brud har en menneskelig faktor, men kun cirka hver femte virksomhed træner sine folk, ligger der en åbenlys mulighed. Awareness handler ikke om en årlig PowerPoint, ingen husker. Det handler om små, gentagne vaner. Og det handler ikke kun om e-mail: sms, QR-koder, Teams-beskeder og telefonopkald er i dag lige så vigtige kanaler — mobil-phishing har ca. 40% højere klikrate end e-mail. Microsoft registrerede ca. 8,3 mia. phishing-trusler alene i 1. kvartal 2026.

(KILDER: VERIZON DBIR 2026; MICROSOFT Q1 2026)

Gør det til et ritual

Korte, hyppige drys af viden slår én lang seance. Fem minutter en gang om måneden husker folk — to timer en gang om året gør de ikke.

Træn uden at skamme

Phishing-simulationer virker, når de lærer i stedet for at udstille. Målet er en kultur, hvor folk tør melde en fejl — ikke skjuler den.

Teknologi stopper det meste. Mennesker stopper resten — hvis de er klædt på til det.

KAPITEL 09 · AI PÅ GODT OG ONDT

Når angriberne også får *nye værktøjer*

AI hjælper virksomheder med at arbejde hurtigere. Men de samme værktøjer giver også angriberne mere fart, præcision og omfang. Samtidig flytter angriberne sig mod kanaler hvor AI gør angrebene hurtigere, mere målrettede og mere troværdige.

QR-kode-phishing

+146%

i 1. kvartal 2026

MICROSOFT, Q1 2026

Mobil-phishing

+40%

højere klikrate end e-mail

VERIZON DBIR 2026

AI forstærker begge sider

AI er ikke ond. Den forstærker bare både det gode og det onde. Angriberne får stærkere værktøjer til troværdig phishing og deepfakes — men forsvaret får også nye muligheder. Forskellen ligger i, hvem der bruger teknologien klogest. Verizon DBIR 2026 finder, at generativ AI nu understøtter 15 forskellige angrebsteknikker — AI opfinder sjældent nye angreb, men gør de kendte hurtigere, billigere og mere skalerbare.

Men dømmekraften er stadig menneskets

AI kan fejlvurdere trusler og falde bagud, når angriberne skifter taktik. Den er et stærkt supplement — men kan ikke erstatte et menneske, der forstår konteksten og kan handle hurtigt, når det gælder.

AI-risikoen kommer heller ikke kun udefra: når medarbejdere bruger AI-værktøjer uden aftale, kan kundedata og personoplysninger ende steder, virksomheden ikke har styr på. Hver femte virksomhed har haft brud relateret til uautoriseret AI-brug. (KILDE: IBM, 2025)

KAPITEL 10 · ALLANS TJEKLISTE

Otte spørgsmål, enhver leder bør *stille sig selv*

Du behøver ikke kunne svaret på det hele. Men du bør vide, hvem der kan. Hvis du tøver ved et af disse, er det et godt sted at begynde.

01 **Er MFA slået til på alle konti, der kan logge ind — og er direkte login blokeret på fællespostkasser?**

02 **Hvornår testede vi sidst, om vores backup faktisk kan gendannes?**

03 **Ved vi, hvem der opdager det — og hvordan — hvis vi bliver ramt nu?**

04 **Har vores medarbejdere fået vist, hvordan en phishing-mail ser ud?**

05 **Hvor mange har administrator-rettigheder — er de navngivne, nødvendige og adskilt fra daglige konti?**

06 **Opdateres vores systemer systematisk, eller når vi det "når vi kan"?**

07 **Findes der en beredskabsplan — og er den nogensinde blevet afprøvet?**

08 **Ved vi, hvilke AI-værktøjer medarbejderne bruger til virksomhedsdata?**

Hjemmebanefordel

Den positive nyhed er, at du kender dit eget system bedre end nogen angriber. Det er aldrig for sent at begynde at arbejde målrettet med de huller, du har. Start simpelt — og start nu.

FIRE RÅD TIL AT KOMME I GANG

Fra bekymring til *hverdag*

1 Luk de billige huller først

To-faktor på alt, en testet backup og systematisk opdatering. Det koster mindst og forhindrer mest.

2 Få øjne på miljøet

Få overvågning og få, skarpe alarmer på plads, så et brud opdages af jer — ikke af jeres kunder.

3 Klæd menneskene på

Korte, gentagne awareness-vaner slår en årlig seance. Gør det til et ritual, ikke en engangsforestilling.

4 Skriv planen, før I får brug for den

En enkel beredskabsplan med klare roller — afprøvet mindst én gang — er din interne forsikring.

Usikker på, hvor I står? Få et gratis IT-tjek.

— Allan

RING TIL ALLAN
6084 6320

SKRIV EN MAIL
as@itnu.dk

KILDER & METODE

Hvor tallene kommer fra

Denne rapport bygger udelukkende på offentligt tilgængelige, betroede kilder. Vi har samlet og oversat dem til en form, en mindre virksomhed kan handle på.

01 **Styrelsen for Samfundssikkerhed (Center for Cybersikkerhed)** — "Cybertruslen mod Danmark 2025". Det nationale trusselsniveau.

02 **Verizon** — "Data Breach Investigations Report 2026". Ransomware, den menneskelige faktor, mobil-phishing og AI-understøttede angrebsteknikker.

03 **Microsoft** — "Digital Defense Report 2025" og "Email threat landscape: Q1 2026". Identitetsangreb, MFA-effekt, QR-kode-phishing og phishing-volumen.

04 **CrowdStrike** — "Global Threat Report 2026". Spredningstid og malware-frie angreb.

05 **Mandiant / Google Cloud** — "M-Trends 2026". Udnyttelse af sårbarheder som indgang.

06 **IBM** — "Cost of a Data Breach Report 2025". Gennemsnitsomkostning og brud relateret til uautoriseret AI-brug.

07 **UK Government (DSIT)** — "Cyber Security Breaches Survey 2025/26". Andel ramte virksomheder, basale kontroller, MFA, træning og beredskabsplaner.

08 **CVE-programmet / NVD** — CVE-volumen 2025 (via Jerry Gamblins "2025 CVE Data Review").

En note om tallene. Det danske trusselsniveau bygger på Center for Cybersikkerhed. De øvrige tal er de nyeste internationale 2025/2026-rapporter og bruges som pejlemærker — de beskriver ikke danske SMV'er én-til-én, men viser udviklingen i angrebsmetoder, sårbarheder og forsvar.

itnu

ITNU ApS · CVR 45557510 · Hesselrødvej 34, 2980 Kokkedal
Personlig IT-partner for danske SMV'er · itnu.dk · 6084 6320