

9 gode råd

om cybersikkerhed til mindre virksomheder

En praktisk vejledning til SMV'er

Cybersikkerhed behøver ikke være kompliceret. Med nogle få, velvalgte tiltag kan virksomheden mindske risikoen for cyberangreb og stå bedre rustet, hvis noget alligevel går galt.

Brug vejledningen som en praktisk tjekliste, enten internt eller i dialogen med virksomhedens IT-leverandør.

Oktober 2026

Sådan bruger I vejledningen

Det vigtigste er at skabe et grundlæggende overblik, aftale hvem der gør hvad og sikre, at de valgte løsninger faktisk virker. I behøver ikke gennemføre alle forbedringer på én gang. Begynd med de områder, der er vigtigst for virksomhedens daglige drift.

De ni råd

1. Få overblik over virksomhedens IT
2. Hold systemer og enheder opdateret
3. Brug sikre loginløsninger
4. Sørg for backup af vigtige data
5. Få styr på adgangsrettighederne
6. Brug relevante IT-sikkerhedsværktøjer
7. Arbejd sikkert uden for arbejdspladsen
8. Forbered medarbejderne på digital svindel
9. Lav en enkel beredskabsplan

1. Få overblik over virksomhedens IT

Et godt overblik gør det lettere at prioritere indsatsen og reagere hurtigt, hvis et system bliver ramt. Start derfor med at skrive ned, hvilke IT-systemer, programmer, computere, telefoner og onlinetjenester virksomheden bruger i det daglige. Notér også, hvilke løsninger og data der er særligt vigtige for driften.

Sådan kan I gøre

- Lav en enkel liste over virksomhedens computere, telefoner, programmer, systemer og onlinetjenester.
- Markér de systemer, som virksomheden er afhængig af for at kunne fungere.
- Notér, hvilke data der er særligt vigtige, og hvor de bliver opbevaret.
- Skriv ned, hvilke IT-leverandører der har ansvar for de enkelte systemer og løsninger.
- Sørg for, at virksomheden ved, hvem der skal kontaktes, hvis et system ikke fungerer eller bliver udsat for et angreb.
- Gennemgå listen med jævne mellemrum og opdatér den, når virksomheden får nye systemer, enheder eller leverandører.

Et enkelt regneark eller dokument er et fint sted at begynde. Det afgørende er, at oplysningerne findes og er tilgængelige for de personer, der skal bruge dem.

2. Hold systemer og enheder opdateret

Opdateringer indeholder ofte forbedringer af sikkerheden. Derfor er det en god idé at installere dem, når de bliver tilgængelige, både på computere, telefoner, programmer, routere og andre enheder, der er forbundet til virksomhedens netværk.

Sådan kan I gøre

- Slå automatisk opdatering til på computere, telefoner, programmer og andre relevante enheder.
- Kontrollér, at opdateringerne faktisk bliver installeret.
- Aftal, hvem der følger op på systemer, som ikke kan opdateres automatisk.
- Bed IT-leverandøren oplyse, hvordan leverandøren håndterer opdateringer, og hvad virksomheden selv har ansvar for.
- Udskift programmer og enheder, hvis leverandøren ikke længere leverer sikkerhedsopdateringer.
- Overvej et værktøj til håndtering af opdateringer, hvis virksomheden har mange computere eller systemer.

Har virksomheden en ekstern IT-leverandør, kan I bede om en kort og forståelig beskrivelse af, hvilke systemer leverandøren opdaterer, og hvordan der følges op.

3. Brug sikre loginløsninger

Et sikkert login gør det vanskeligere for uvedkommende at få adgang til virksomhedens mail, systemer og data. Brug derfor lange, unikke adgangskoder og aktivér to-faktor-login, hvor det er muligt.

Sådan kan I gøre

- Brug adgangskoder på mindst 15 tegn.
- Brug forskellige adgangskoder til forskellige systemer.
- Anvend en passwordmanager, også kaldet en kodehusker, til at oprette og gemme adgangskoder sikkert.
- Aktivér to-faktor-login på mail, økonomisystemer, fjernadgang, skyløsninger og andre vigtige konti.
- Begynd med de vigtigste konti, hvis to-faktor-login ikke kan indføres overalt på én gang.
- Bed IT-leverandøren om hjælp til opsætningen, hvis I er i tvivl.

En passwordmanager betyder, at medarbejderne kun behøver at huske én stærk hovedadgangskode. To-faktor-login giver et ekstra lag sikkerhed, også hvis en adgangskode bliver opsnappet.

4. Sørg for backup af vigtige data

En fungerende backup gør det muligt at genskabe virksomhedens data efter eksempelvis et cyberangreb, et systemnedbrud eller en menneskelig fejl. Det er ikke tilstrækkeligt, at der bliver taget backup. Virksomheden skal også vide, at den virker.

Sådan kan I gøre

- Find ud af, hvilke data virksomheden ikke kan undvære.
- Sørg for, at der løbende bliver taget backup af disse data.
- Aftal, hvor ofte der skal tages backup. Behovet afhænger af, hvor ofte data ændres.
- Opbevar mindst to sæt af virksomhedens data.
- Sørg for, at mindst én sikkerhedskopi er adskilt fra virksomhedens daglige IT-system.
- Test jævnligt, at data kan genskabes fra backuppen.
- Notér, hvem der har ansvaret for backup og gendannelse.
- Bed IT-leverandøren dokumentere, hvilke data der sikkerhedskopieres, og hvordan en gendannelse foregår.

Backup kan være inkluderet i virksomhedens IT- eller cloudløsning, men det bør ikke blot forudsættes. Bed leverandøren forklare løsningen i et forståeligt sprog og gennemfør en praktisk test.

5. Få styr på adgangsrettighederne

Medarbejdere og eksterne leverandører bør som udgangspunkt kun have adgang til de systemer og oplysninger, de har brug for i deres arbejde. Det gør IT-miljøet mere overskueligt og kan begrænse konsekvenserne, hvis en konto bliver misbrugt.

Sådan kan I gøre

- Lav en oversigt over, hvem der har adgang til virksomhedens vigtigste systemer.
- Sørg for, at medarbejderne kun har de adgange, der er nødvendige for deres arbejde.

- Gennemgå adgangene mindst én gang om året og ved ændringer i organisationen.
- Fjern adgangen med det samme, når en medarbejder stopper eller skifter arbejdsopgaver.
- Husk også at lukke konti og adgange for tidligere konsulenter og leverandører.
- Find ud af, hvem der har administratorrettigheder, og begræns dem til personer og leverandører, der reelt har brug for dem.
- Brug almindelige brugerkonti til det daglige arbejde og administratorkonti til særlige administrative opgaver.

Gør gerne gennemgangen af adgange til en fast del af proceduren, når en medarbejder begynder, skifter funktion eller stopper.

6. Brug relevante IT-sikkerhedsværktøjer

Tekniske sikkerhedsværktøjer kan hjælpe med at opdage og blokere skadelige mails, programmer og forsøg på uautoriseret adgang. Mange løsninger har allerede indbyggede sikkerhedsfunktioner, som giver en god grundbeskyttelse, når de er slået til og holdes opdateret.

Sådan kan I gøre

- Sørg for, at virksomhedens enheder er beskyttet med antimalware eller antivirus.
- Brug firewall på virksomhedens netværk og enheder.
- Aktivér phishing- og spamfiltre i mailsystemet.
- Bevar de anbefalede sikkerhedsindstillinger, medmindre der er en konkret, fagligt begrundet årsag til at ændre dem.
- Kontrollér, at sikkerhedsværktøjerne bliver opdateret automatisk.
- Aftal, hvem der reagerer, hvis et sikkerhedsværktøj viser en advarsel.
- Bed IT-leverandøren om en oversigt over de sikkerhedsværktøjer, der allerede er aktiveret.
- Søg rådgivning, hvis virksomheden har særlige systemer, følsomme data eller er meget afhængig af IT.

Virksomheden behøver ikke nødvendigvis købe mange produkter. Begynd med at få overblik over den beskyttelse, der allerede er inkluderet i virksomhedens systemer og abonnementer.

7. Arbejd sikkert uden for arbejdspladsen

Når medarbejdere arbejder hjemmefra, hos kunder eller under transport, bruges virksomhedens udstyr og oplysninger uden for de sædvanlige rammer. Nogle enkle vaner kan gøre arbejdet mere sikkert.

Sådan kan I gøre

- Undgå trådløse netværk, som ikke kræver adgangskode.
- Brug telefonens internetdeling, hvis der ikke er adgang til et netværk, I har tillid til.
- Brug virksomhedens VPN-løsning, hvis en sådan er stillet til rådighed.
- Sørg for, at computer og telefon er opdateret og beskyttet med adgangskode eller anden skærmlås.

- Lås skærmen, når udstyret ikke er under opsyn.
- Vær opmærksom på, om andre kan se med på skærmen i tog, lufthavne, caféer og andre offentlige steder.
- Undgå at drøfte fortrolige oplysninger, hvis andre kan lytte med.
- Spørg IT-leverandøren, hvordan medarbejderne skal logge sikkert på virksomhedens systemer udefra.

Lav gerne en kort vejledning, der beskriver, hvordan medarbejderne logger på, hvilke netværk de må bruge, og hvem de skal kontakte, hvis noget virker usædvanligt.

8. Forbered medarbejderne på digital svindel

Medarbejderne er en vigtig del af virksomhedens sikkerhed. Målet er ikke, at alle skal være IT-eksperter, men at de kan genkende noget usædvanligt og ved, hvordan de skal reagere.

Sådan kan I gøre

- Tal jævnligt om svindelmails, falske sms'er og mistænkelige telefonopkald.
- Bed medarbejderne være særligt opmærksomme på uventede links, vedhæftede filer og anmodninger om betaling.
- Brug en fast godkendelsesprocedure ved pengeoverførsler og ændringer af betalingsoplysninger.
- Kontrollér ændringer af kontonumre via en anden kanal end den, hvor ændringen blev modtaget.
- Kontakt eksempelvis kunden eller leverandøren på et allerede kendt telefonnummer.
- Gør det tydeligt, hvem medarbejderne skal kontakte, hvis de er i tvivl.
- Skab en åben kultur, hvor hændelser og fejl bliver meldt hurtigt.
- Brug konkrete og relevante eksempler i den løbende træning.

Skab en kultur, hvor det er naturligt at spørge en kollega eller leder, hvis en mail, sms eller telefonsamtale virker mistænkelig. En hurtig henvendelse kan forhindre, at en fejl udvikler sig.

9. Lav en enkel beredskabsplan

Hvis virksomheden bliver ramt af en IT-sikkerhedshændelse, er det en stor fordel på forhånd at have aftalt, hvem der gør hvad. Planen behøver ikke være lang. Den skal først og fremmest indeholde de vigtigste handlinger, roller og kontaktoplysninger.

Sådan kan I gøre

- Aftal, hvem der har ansvaret for at koordinere indsatsen.
- Skriv ned, hvem der skal kontaktes, eksempelvis IT-leverandør, ledelse, bank og forsikringsselskab.
- Beskriv kort, hvordan medarbejderne skal reagere ved mistanke om et cyberangreb.
- Aftal, hvem der må træffe beslutning om at lukke systemer eller afbryde forbindelser.
- Find ud af, hvordan de vigtigste arbejdsopgaver kan fortsætte, hvis IT-systemerne midlertidigt er utilgængelige.

- Opbevar planen, så den også kan tilgås, hvis virksomhedens netværk eller mail ikke virker.
- Print gerne en kopi og opbevar den et kendt sted.
- Gennemgå og øv planen med ledere og medarbejdere.
- Opdatér planen, når kontaktpersoner, leverandører eller systemer ændres.

En kort øvelse kan gennemføres som en samtale: Hvad gør vi, hvis vi ikke kan tilgå mail, kundedata eller økonomisystemet i morgen tidlig? Formålet er at opdage mangler, inden planen skal bruges.

En enkel måde at komme i gang på

10. Udpeg én person, der koordinerer arbejdet.
11. Gennemgå de ni råd sammen med virksomhedens IT-leverandør.
12. Notér for hvert råd, hvad der allerede er på plads.
13. Vælg de vigtigste mangler, og aftal konkrete handlinger.
14. Skriv ned, hvem der har ansvaret, og hvornår der følges op.
15. Gennemgå sikkerheden igen, når virksomheden ændrer systemer, leverandører eller arbejdsgange.

På den måde bliver cybersikkerhed en overskuelig del af den almindelige drift frem for en særskilt teknisk opgave.