# It-sikkerhed: Sikker køb og brug af cloud-tjenester

Denne guide har til formål at gøre virksomheder klogere på, hvordan de tænker digital sikkerhed ind i køb og anvendelse af cloud-tjenester.

**Hvad er en cloud-tjeneste?**
Cloud-tjenester er en betegnelse, der dækker over software, som stilles til rådighed via internettet. Herunder er en række eksempler på tjenester og værktøjer hos virksomheder, som kan fungere som cloud-tjenester:

- Samarbejdsværktøjer og dokumenthåndtering (fx Microsoft 365)
- HR-værktøj (fx SAP)
- Fildelingsværktøjer (fx Dropbox)
- CMS-system (fx Wordpress)

**Hvem kan bruge guiden?**
Guiden henvender sig både til virksomheder, der endnu ikke bruger cloud-tjenester, og virksomheder, der allerede bruger en eller flere cloud-tjenester.

**Hvordan bruges guiden?**
Guiden indeholder seks anbefalinger, der kan guide virksomheder til køb og brug af en cloud-tjeneste. Dokumentet har ikke svaret på, hvordan I teknisk opsætter jeres cloud-løsning korrekt, men det kan være en guide, I kan støtte jer til, så I kan beskytte jeres virksomhed, uanset hvilken løsning I vælger.

# **Trin-for-trin-guide:** Sikker køb og brug af cloud-tjenester

## 1. Opbyg viden om emnet med en cloud-ansvarlig

Når I som virksomhed skal købe en cloud-løsning, er det vigtigt, at I har sat jer ind i emnet. Udpeg derfor en cloud-ansvarlig, der skal opbygge viden om emnet og sætte sig ind i jeres virksomheds behov. Den cloud-ansvarlige kan efterfølgende dele relevant viden med resten af virksomheden. Den cloud-ansvarlige kan også indhente ekstern hjælp, hvis vedkommende har brug for det.

Med en cloud-ansvarlig sikrer I, at der bliver taget aktivt stilling til, hvordan cloud-tjenester påvirker virksomhedens arbejde, og hvad det betyder for den digitale sikkerhed.

**Det er vigtigt at få undersøgt:**

- den digitale sikkerhed hos forskellige cloud-leverandører
- hvor ofte leverandøren udruller sikkerhedsopdateringer
- hvordan leverandøren kommunikerer med jer og håndterer den daglige dialog
- hvordan jeres virksomhed informeres, hvis cloud-løsningen bliver hacket eller oplever et nedbrud

### Viden og værktøjer til inspiration:

- Læs en udførlig gennemgang af cloud-tjenester i **Digitaliseringsstyrelsens og Center for Cybersikkerheds vejledning om cloud-services**

## 2. Lav en risikovurdering af cloud-løsningen inden køb

I bør foretage en risikovurdering inden køb af cloud-løsning, hvor I vurderer, hvorvidt løsningen lever op til virksomhedens sikkerhedsmæssige krav. Det kan fx være krav til oppetid, fortrolighed, beskyttelse imod uautoriseret adgang eller backup.

Hvis I ikke har de nødvendige kompetencer internt til at foretage denne vurdering, kan I søge hjælp hos en ekstern rådgiver. Når risikovurderingen er lavet, bør den revideres jævnligt. Der skal også tages højde for, at virksomheden altid er ansvarlig for at overholde GDPR.

### Viden og værktøjer til inspiration:

- I kan benytte denne risikovurderingsmodel til at foretage en **risikovurdering** af jeres virksomhed. Hent en vejledning til modellen **her**.

**Trin-for-trin-guide:** Sikker køb og brug af cloud-tjenester

## 3. Stil krav til cloud-leverandøren

Danske virksomheder er ofte ikke store nok til at kræve særlige tilpasninger af globale cloud-leverandører, da deres standardiserede "hyldevare-løsninger" har mange millioner brugere, men for nogle er det muligt at indgå dialog og stille krav.

Det er ofte også muligt at tilkøbe yderligere sikkerhedsrelaterede ydelser til cloud-løsningen. Hvis dette ikke er tilstrækkeligt for at imødekomme virksomhedens sikkerhedsbehov, bør I vælge en anden leverandør, som bedre matcher jeres behov.

Husk altid at gemme den aftale, I indgår med leverandøren.

### Viden og værktøjer til inspiration:

- Få hjælp til at tage dialogen med cloud-leverandøren med dette **leverandørværktøj**

## 4. Sørg for at løsningen er opsat korrekt

Mange cloud-løsninger har indbyggede sikkerhedsfunktioner, men det er ofte virksomheden selv, der skal aktivere de rette indstillinger. Derfor er det afgørende, at I sætter jer ind i, hvad indstillingerne betyder og tager et aktivt valg om, hvordan indstillingerne sættes op. I bør fx nøje overveje, hvem der har adgang til at foretage ændringer, hvilken proces I har for ændringer og jævnligt tjekke, at indstillingerne er korrekte.

Hvis jeres virksomhed ikke har de nødvendige kompetencer internt til at vurdere dette, bør I indhente hjælp til opgaven udefra.

# **Trin-for-trin-guide:** Sikker køb og brug af cloud-tjenester

## 5. Tænk cloud-løsningen ind i det løbende arbejde med sikkerhed

Som virksomhed har I ansvaret for jeres data og it-systemer. Det gælder også, selvom I bruger en cloud-leverandør. På de områder, hvor cloud-løsningen ikke lever op til virksomhedens krav til sikkerhed, skal I selv sørge for at løse det - fx med indkøb af tillægssikkerhedsløsninger.

I kan skrive jer op til nyhedsbreve og information fra cloud-leverandøren for at holde jer opdaterede om løsningens sikkerhed.

I bør også lade virksomhedens cloud-ansvarlige sørge for at holde øje med de sikkerhedsleverancer, I får fra cloud-leverandøren, så I er sikre på, at de overholder den aftale, I har indgået.

En metode til at holde øje kan fx være gennemgang af de opsamlede sikkerheds-logs, der bruges til at sikre, at I er i stand til at reagere fornuftigt på eventuelle sikkerhedshændelser. Overvågningen af logs kan også identificere eventuelle forhold, der bør forbedres.

### Viden og værktøjer til inspiration:

- Få løbende opdateringer på it-sikkerhedshændelser på **Center For Cybersikkerhed hjemmeside** og **Twitter-profil**

## 6. Vær opmærksom på sikkerheden ved ophør eller skift af cloud-leverandør

I forbindelse med afslutning eller overdragelse af kontraktforholdet med en cloud-leverandør er det vigtigt, at sikkerheden bevares i hele afslutningsfasen, uanset om driften overdrages til en anden leverandør, ophører eller hjemtages.

Ved ophør eller skift bør I genlæse den oprindelige aftale med cloud-leverandøren jf. punkt 3.

### Viden og værktøjer til inspiration:

- Læs eller genlæs, hvordan I laver en exit-strategi, når kontrakten indgås med leverandøren, på **Digitaliseringsstyrelsens og Center for Cybersikkerheds vejledning om cloud-services (side 19 og 36)**