

Digital sikkerhed

Hvad kan du som rådgiver gøre, for at styrke IT-sikkerheden i de virksomheder, du rådgiver?

For at styrke små og mellemstore virksomheders robusthed over for IT-nedbrud eller angreb fra IT-kriminelle, skal IT-sikkerhed tænkes ind som en naturlig del af den digitale omstilling. IT-sikkerhed er relevant for alle dele af den digitale omstilling, uanset om det omhandler cykelsmedens kundedatabase eller servicevirksomhedens lønsystem.

Det er derfor vigtigt, at du som rådgiver har fokus på digital sikkerhed, når du rådgiver små og mellemstore virksomheder i deres digitale omstilling. Denne oversigt har til formål at give et overblik over, hvordan IT-sikkerhed kan indtænkes i dit rådgivningsarbejde.

Vejledning om IT-sikkerhed bør altid tage udgangspunkt i virksomhedens forhold: Hvor digital er virksomheden, arbejder man aktivt med IT-sikkerhed allerede, eller skal det grundlæggende på plads?

Digitaliseringsstyrelsen har en række værktøjer og vejledninger, der kan anvendes, enten af virksomheden selv eller som en del af rådgivningsarbejdet. Det vil komme an på en konkret vurdering, hvilke værktøjer det er relevant at bruge. Det kunne være:

- **De 7 råd om IT-sikkerhed** – Syv råd der hjælper virksomheder med at styrke deres grundlæggende IT-sikkerhed.
- **Sikkerhedstjekket** – Få overblik over virksomhedens IT-sikkerhedsniveau og mulige indsatspunkter.
- **Leverandørpakken** – Hjælper virksomheden med at stille sikkerhedskrav til deres IT-leverandør.
- **IT-risikovurdering** – Skabelon og online værktøj der hjælper virksomheden med at lave en IT-risikovurdering.

Læs mere om de forskellige værktøjer på de næste sider.

De 7 råd om IT-sikkerhed

Vejledning til, hvordan virksomheder opnår en bedre grundlæggende IT-sikkerhed. Rådene er særligt målrettet de virksomheder, som ikke selv har en IT-sikkerhedsansvarlig ansat i virksomheden, og som derfor selv må håndtere den digitale sikkerhed.

Som rådgiver kan du gennemgå rådene med virksomheden, og få dem til at fokusere på eventuelle huller.

1. Få overblik over vigtige data og systemer
2. Opdater programmer løbende
3. Køb antivirus og firewall
4. Tag backup af data
5. Lær at spotte mistænkelige mails
6. Lav stærke adgangskoder og brug to-faktor login
7. Stil sikkerhedskrav til IT-leverandøren

Find de syv råd på www.sikkerdigital.dk/7raad

Sikkerhedstjekket

Sikkerhedstjekket er et digitalt værktøj, der vil skabe en større forståelse for vigtigheden af IT-sikkerhed for virksomhedens forretning. Når virksomheden har gennemført det, får de en række konkrete anbefalinger, der er tilpasset deres risikoprofil og andre forhold. Anbefalingerne fra sikkerhedstjekket kan fx tydeliggøre, hvad ledelsen bør gøre for at forankre IT-sikkerheden i virksomheden.

Det kan være relevant at drøfte anbefalingerne fra Sikkerhedstjekket med virksomheden og lægge en handlingsplan for at gå videre med dem.

Sikkerhedstjekket giver en konkret vurdering af følgende seks områder:

- Din virksomhed
- Ledelse og risikohåndtering
- Sikkerhedsprocedurer
- Medarbejdere
- Tekniske sikkerhedsløsninger
- Samarbejdspartnere

Du kan finde vores værktøjer på <https://sikkerdigital.dk/vaerktoejer>

IT-risikovurderingsværktøj

IT-risikovurderingsværktøjet er henvendt til små og mellemstore virksomheder og de IT-faglige personer med kendskab til virksomhedens IT-setup. Det kan være virksomhedens egen IT-ansvarlige eller en leverandør.

Gennem værktøjet bliver man præsenteret for en række risikoscenarier, der skal få virksomheden til at reflektere over deres IT-setup, samt hvilke risici der er forbundet med dette. Med værktøjet får virksomheden konkret hjælp til at vurdere følgende fem områder af deres IT-setup og håndtering heraf:

- Enheder
- Applikationer og tjenester
- Brugere
- Netværk
- Data

Resultatet fra svarene er en IT-risikovurdering, som virksomheden efterfølgende kan downloade som regneark. Risikovurderingen indikerer, hvor virksomheden har de største risici, og indeholder en vejledning til, hvad de kan gøre for at håndtere de forskellige risici.

Find materialer til IT-risikovurdering på www.sikkerdigital.dk/IT-risikovurdering

Leverandørpakken

Fordi mange virksomheder outsourcer deres IT-drift, kan du være med til at gøre dem opmærksomme på at stille sikkerhedskrav til leverandøren.

For at afdække, om IT-leverandøren har tilstrækkelig fokus på IT-sikkerhed, er det en god ide, at tale med leverandøren om nedenstående punkter. Kravene til sikkerhed kan naturligvis variere alt efter, hvor kritiske og følsomme virksomhedens data er:

- Hvad gør IT-leverandøren for at beskytte mod uønsket adgang?
- Hvad gør IT-leverandøren for at sikre tilgængelighed og høj opetid?
- Hvad gør IT-leverandøren for at dokumentere deres sikkerhed?
- Hvad gør IT-leverandøren for at passe på persondata (GDPR)?
- Hvad er ansvarsfordeling mellem jer som kunde og IT-leverandøren

Du kan finde leverandørpakken og vejledningen på www.sikkerdigital.dk/leverandørpakken