Bestyrelsens tjekliste til digital ansvarlighed

Denne tjekliste giver jer et overblik over de overvejelser, I som bestyrelse skal afklare med virksomhedens direktion. Tjeklisten er især målrettet bestyrelser, der ikke har dataetik og digital sikkerhed som kernekompetence, og skal benyttes som en hjælp til at komme i gang med at sikre virksomheden og dens data.

1. Forankring i ledelsen

Virksomhedens digitale ansvarlighed starter fra toppen, og det er jeres ansvar som bestyrelse at sætte emnet på virksomhedens dagsorden og sikre en løbende opfølgning. Derefter hviler det på direktionens skuldre at få de dataetiske og it-sikkerhedsmæssige beslutninger ud at leve i virksomheden.

☑ Overvej i samarbejde med direktionen:

- ☐ Er it-sikkerhed og dataetik en fast del af bestyrelsens årshjul?
- ☐ Er der lagt en strategi for it-sikkerhed og dataetik?
- ☐ Er der en løbende dialog om behovet for opkvalificering af ledelsens kompetencer inden for it-sikkerhed og dataetik?
- ☐ Bliver it-sikkerhed og dataetik tænkt ind i etablering af nye samarbejder, forretningsudvikling og ved implementering af nye teknologier (fx kunstig intelligens)?

2. Risiko og sårbarheder

Det er nødvendigt, at direktionen vurderer, hvilke digitale risici virksomheden kan blive udsat for, og hvor virksomheden er mest sårbar overfor cyberangreb. På den måde får I et overblik over, hvor virksomheden er mest sårbar, hvor højt sikkerhedsniveauet bør være, herunder hvad virksomhedens risikoappetit er, og hvad I kan gøre for at reducere it-sårbarheden.

☑ Overvej:

- ☐ Modtager bestyrelsen løbende rapportering om virksomhedens it-sikkerhed og risici?
- ☐ Er der en oversigt over hvilke it-systemer, der er mest kritiske for den daglige drift og opretholdelse af forretningen (fx faktureringssystem, webshop, ERP-system, lagerstyring)?
- ☐ Har I et overblik over, hvilke typer af data virksomheden indsamler, opbevarer og behandler? Og hvilke data der er vigtige for virksomhedens drift og forretning?
- ☐ Man kan ikke beskytte sig mod alt, har I derfor taget stilling til virksomhedens risikoappetit?
- ☐ Hvor lang tid kan virksomheden fungere uden adgang til it-systemer (fx e-mail, lagersystemer, kundedatabase, hjemmeside)?
- ☐ Opdateres risikovurderingen, når der indkøbes eller udvikles nye it-produkter og systemer?

Hvis I ikke har foretaget en it-risikovurdering i jeres virksomhed, kan direktionen få hjælp her: Identificer din virksomheds risici

3. Beredskab

Med en it-beredskabsplan kan direktionen kortlægge, hvem der gør hvad i tilfælde af en it-sikkerhedshændelse. Beredskabsplanen sikrer, at virksomheden kan reagere hurtigt og målrettet, hvis uheldet er ude.

☑ Overvej:

- ☐ Har virksomheden en opdateret fysisk liste over hvem, der skal kontaktes i tilfælde af uforudsete hændelser eller cyberangreb (fx medarbejdere, samarbejdspartnere, eksterne it-leverandører, politiet), og hvordan de skal kontaktes?
- ☐ Beskriver beredskabet, hvordan arbejdsgangene (fx produktion) fortsætter uden adgang til de påvirkede it-systemer?
- ☐ Har I en strategi for ekstern og intern kommunikation i tilfælde af en it-sikkerhedshændelse?
- ☐ Øves beredskabet, og testes back-up af systemer og data?

Hvis I ikke har en it-beredskabsplan, kan direktionen få hjælp her: Vær beredt med en it-sikkerhedspolitik og beredskabsplan

4. Politik for it-sikkerhed

En nedskrevet it-sikkerhedspolitik giver både ledelsen og medarbejderne retningslinjer for, hvad der forventes i forhold til, at alle i virksomheden bidrager til it-sikkerheden. For ingen kæde er stærkere end det svageste led.

☑ Overvej:

- ☐ Har I en oversigt over de tekniske sikkerhedsforanstaltninger, der er implementeret (fx backup af data, firewall, automatisk opdatering og logning)?
- ☐ Bruges der to-faktorsikkerhed – fx ved ekstern adgang til virksomhedens systemer?
- ☐ Bruger virksomheden adgangsstyring, og er der udpeget en medarbejder med ansvar for at tildele adgang til virksomhedens systemer og informationer?
- ☐ Stiller I krav til samarbejdspartnere og leverandørers it-sikkerhedsforanstaltninger?

Hvis I ikke har en it-sikkerhedspolitik, kan direktionen få hjælp her: Vær beredt med en it-sikkerhedspolitik og beredskabsplan

5. Politik for dataetik

Digital ansvarlighed indebærer mere end at beskytte sig mod udefrakommende aktører. I bør derfor overveje, hvordan virksomheden skal indsamle, anvende og dele data. Disse dataetiske overvejelser kan med fordel beskrives i principper og sammenfattes i en dataetisk politik, der afspejler virksomhedens værdier. Formålet er at forholde sig til dataetik for at værne om tilliden mellem virksomheden og deres kunder, leverandører og samarbejdspartnere. Dataetik er mere end beskyttelse af personoplysninger, som der er fokus på med GDPR, men der er en tæt sammenhæng. Har virksomheden forståelse for forskellen på GDPR og dataetik? *Læs mere om, hvad dataetik er her.*

☑ Overvej:

- ☐ Er der et overblik over virksomhedens data, hvordan der indsamles, bearbejdes og anvendes data, og om det sker på en ansvarlig og etisk måde?
- ☐ Hvordan sikres det, at eventuelle dataetiske retningslinjer bliver efterlevet og forankret i virksomheden?
- ☐ Inddrager virksomheden kunder, samarbejdspartnere eller interessenter i processen for virksomhedens forretnings- og produktudvikling til at identificere dataetiske problemstillinger?
- ☐ Stilles der krav til samarbejdspartnere og underleverandørers dataetiske foranstaltninger?

5. Politik for dataetik - fortsat

☑ Overvej:

- ☐ Bruger I kunstig intelligens til at indsamle eller bearbejde data, og hvilke dataetiske problemstillinger kan dette foranledige?
- ☐ Overvejer I hvilke data, der bruges til at træne og validere kunstig intelligens, og om der genereres profilering eller faglige vurderinger, som er dataetisk uhensigtsmæssige?

Hvis I ikke har en dataetisk politik, kan direktionen få hjælp her: Kom i gang med at udforme dine dataetiske retningslinjer

6. Medarbejdere

Medarbejdernes digitale adfærd er et vigtigt værn mod angreb som fx ransomware via phishingmails. Samtidig danner medarbejdernes dataetiske handlinger grundlaget for, at virksomheden agerer digitalt ansvarligt.

☑ Overvej:

- ☐ Bliver nye medarbejdere oplært i virksomhedens it-sikkerhed og dataetik (fx krav til adgangskoder, usikre links og retningslinjer for behandling af data)?
- ☐ Er der løbende opkvalificering af medarbejderne i virksomhedens it-sikkerhed og dataetik (fx med awareness-kampagner og oplæg)?
- ☐ Bliver der indsamlet og anvendt digital medarbejderdata som ledelsesværktøj? Og bliver medarbejderne informeret herom?

Hvis I mangler materialer og værktøjer til sikker digital adfærd, kan I finde hjælp her: Værktøjer der styrker medarbejdernes it-sikkerhedsadfærd

Denne tjekliste skal ikke anses som en komplet løsning på virksomhedens digitale ansvarlighed, da antallet og omfanget af it-sikkerhedsforanstaltninger og dataetiske overvejelser afhænger af den enkelte virksomhed. Tjeklisten udgør og erstatter ikke professionel rådgivning, og bestyrelsen skal ikke nødvendigvis kunne svare direkte på alle overvejelserne.

Det kan fx være en god idé at få en relevant oplægsholder ind for at fortælle nærmere om digital sikkerhed og dataetik og få hjælp til implementeringen af en relevant rådgiver.

Ønsker I som bestyrelse at gå mere i dybden med digital sikkerhed, kan I læse mere på Bestyrelsesforeningens hjemmeside.