Digital ansvarlighed på bestyrelsens dagsorden

I en tid, hvor samfundet og erhvervslivet er mere digitaliseret end nogensinde, er virksomheder i stigende omfang sårbare over for uhensigtsmæssige hændelser som it-angreb og datalæk. Det kalder på digital ansvarlighed blandt virksomheder. Og det starter faktisk hos jer – i bestyrelsen.

Hvad er digital ansvarlighed?

Digital ansvarlighed dækker over dataetik og it-sikkerhed og er en nødvendighed på bestyrelsens agenda. Dataetik drejer sig om, hvorvidt jeres virksomhed indsamler, bearbejder og anvender data på ansvarlig og bæredygtig vis.

It-sikkerhed handler imidlertid om, hvordan jeres virksomhed bedst beskytter it-systemer og data.

Forretningsrisiko og konkurrencefordel

Prioriterer I ikke digital ansvarlighed, udsætter I virksomheden for risiko – på bundlinjen, kundeforholdene og omdømmet. I kan fx opleve et it-angreb med læk og misbrug af kunde- og forretningsdata, hvis it-sikkerheden ikke er høj nok.

Omvendt kan jeres overvejelser om virksomhedens dataskik rumme forretningsudvikling og vækstmuligheder, mener Mikael Jensen, der er direktør for D-mærket – en mærkningsordning for digital ansvarlighed.

”Dataetiske overvejelser kan kaste nye produkter eller løsninger af sig, og så har de stor betydning som led i virksomhedens risikostyring og i forhold til at opbygge tillid til interessenter. Virksomheder bliver klogere på deres egen forretning, når de forholder sig til, hvor de indsamler data, og hvordan de håndterer og bruger dem,” siger Mikael Jensen.

Digital ansvarlighed kan altså potentielt åbne nye markeder for jer – fx til virksomheder og organisationer, der stiller høje krav til samarbejdspartneres digitale handlemåder. Derfor er det vigtigt at stille skarpt på i bestyrelseslokalet. Virksomhedens digitale ansvarlighed hviler nemlig på jeres skuldre.

En løbende proces

I tænker måske, at det er et spørgsmål om alt eller intet: At I enten er 100 procent dækket ind mod it-angreb og datalæk eller fuldkomment blottet for selv samme. Sådan forholder det sig dog sjældent. Digital ansvarlighed er en trinvis proces, der skal vedligeholdes løbende i takt med et skiftende risikobillede.

Hvordan håndteres dataetiske dilemmaer? Hvor stor er virksomhedens risiko for it-angreb? Og hvilke data er forretningskritiske? Spørgsmålene kan være mange.

Bestyrelsens tjekliste til digital ansvarlighed

Denne tjekliste giver jer et overblik over de overvejelser, I som bestyrelse skal afklare med virksomhedens direktion og den ansvarlige for it-sikkerhed. 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. 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 der en løbende dialog om behovet for opkvalificering af ledelsens kompetencer inden for it-sikkerhed og dataetik?
- ☐ Modtager bestyrelsen løbende rapportering om virksomhedens it-sikkerhed (trusler, risici, angreb, investeringer) og dataetiske overvejelser?
- ☐ Er digital ansvarlighed en fast del af bestyrelsens årshjul?

2. Risiko og sårbarheder

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

☑ Overvej:

- ☐ Er der en oversigt over hvilke it-systemer, der er mest kritiske for den daglige drift (fx faktureringssystem, webshop, ERP-system, lagerstyring)?
- ☐ Hvilke typer af data indsamler, opbevarer og behandler virksomheden? Og hvilke data er forretningskritiske?
- ☐ 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, målrettet og tilstrækkeligt, hvis uheldet er ude.

☑ Overvej:

- ☐ Har virksomheden en fysisk liste over, hvem der skal kontaktes i tilfælde af angreb (fx medarbejdere, eksterne it-leverandører, politiet)?
- ☐ 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?

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)?
- ☐ 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?
- ☐ Indgår overvejelser om it-sikkerhed i virksomhedens produktudvikling, vækst, markedsføring og overordnede strategi?

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. Som en del af ledelsen skal I også overveje, hvordan I ønsker at indsamle, anvende og dele data. Disse dataetiske overvejelser har til formål at værne om tilliden mellem virksomhedens kunder, leverandører og samarbejdspartnere.

☑ Overvej:

- ☐ Er virksomhedens data til fx markedsføring indsamlet på en ansvarlig måde – også af underleverandører?
- ☐ Hvilke dataetiske overvejelser skal ligge til grund for indkøb af nye produkter og/eller tjenester, som bruger data?
- ☐ Hvilke dataetiske overvejelser vil I have, når I selv udvikler nye produkter og/eller tjenester, som bruger data?

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)?

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

---

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 ansvarlighed 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.