Bestyrelsesforeningens Center for Cyberkompetencer

KROMANN REUMERT

CENTER FOR CYBERSIKKERHED

INDUSTRIENS FOND

# Anbefalinger til bestyrelsen

Vejledning i sin helhed findes bl.a. på Bestyrelsesforeningen.dk

Strategi

## 1. Risikovurdering og sårbarheder

Det anbefales, at

- bestyrelsen mindst to gange om året modtager og forholder sig til en opdateret risikovurdering på cyberområdet baseret på virksomhedens vigtigste værdier, teknologilandskab, primære sårbarheder, sandsynlige trusler, mulige tab ved angreb og anbefaling til (yderligere) investering.

## 2. Risikoappetit og strategi

Det anbefales, at

- bestyrelsen så ofte som relevant og mindst én gang om året fastsætter virksomhedens risikoappetit indenfor cyber- og informationssikkerhed baseret på en afvejning af virksomhedens forretningsmål og digitaliserings-strategi, risikoprofil, eksisterende sikkerhedsbudget og investeringsvilje.

Udførelse

## 3. Planer, processer og beredskab

Det anbefales, at

- bestyrelsen fører kontrol med, at cyber- og informationssikkerhedsrisici er fastlagt i politikker og håndteret i processer for it/fysisk sikkerhed og digital adfærd.
- bestyrelsen fører kontrol med, at virksomheden har testede beredskabs- og kommunikationsplaner for håndtering i tilfælde af alt fra hackerangreb til strømnedbrud.

## 4. Rapportering og kontrol

Det anbefales, at

- bestyrelsen implementerer cybersikkerhed som en fast del af sit årshjul, og har cybersikkerhed på agendaen på hvert bestyrelsesmøde.
- bestyrelsen modtager relevant rapportering forud for hvert bestyrelses-møde med bl.a. aktuelt trusselsbillede, sikkerhedshændelser, resultater af sikkerhedstest og awareness aktiviteter, resultater fra revisionsgen-nemgange, evt. forslag til supplerende tiltag ift. forsikringsdækning og investeringer.

Mennesker

## 5. Kultur og mennesker

Det anbefales, at

- virksomheden har et træningsprogram for bestyrelse, direktion og medarbejdere i relation til cyber- og informationssikkerhed.
- bestyrelsen går forrest i at understøtte en stærk og bevidst cyber- og informationssikkerhedskultur i virksomheden.

## 6. Kompetencer og organisering

Det anbefales, at

- mindst ét medlem af bestyrelsen har relevant viden om eller erfaring med cyber- og informationssikkerhed og er i stand til at tilegne sig indsigt i virksomhedens tekniske og sikkerhedsmæssige fundament.
- virksomhedens sikkerhedsorganisation er direkte forankret på et direktionsniveau, der rapporterer direkte til bestyrelsen.

Bestyrelsesforeningens Center for Cyberkompetencer

KROMANN REUMERT

CENTER FOR CYBERSIKKERHED

INDUSTRIENS FOND

# Relevante overvejelser for bestyrelsesmedlemmer og virksomhedsledere

**1. Risikovurdering og sårbarheder**

- ☐ Hvad betyder det for forretningen, hvis vigtige værdier ændres, stjæles, lækkes eller hvis kritiske systemer eller andre it-services er utilgængelige i kortere eller længere tid?
- ☐ Hvem er de sandsynlige angribere, hvad er deres mål, og hvilke redskaber/teknik- ker bruger de til at opnå disse mål?
- ☐ På hvilke områder er virksomheden mest sårbar overfor angreb (teknologi, personale, processer), og hvor sandsynligt er angreb indenfor disse områder?
- ☐ Hvad er virksomhedens plan for risikohåndtering, inkl. investeringer?

**2. Risikoappetit og strategi**

- ☐ Hvor stort er budgettet for cyber- og informationssikkerhed?
- ☐ Hvor ligger virksomhedens sikkerhedsniveau- og budget sammenlignet med andre forretningsområder? Med andre virksomheder?
- ☐ Hvad er de potentielle omkostninger forbundet med at investere i en opgradering af sikkerhedsniveauet?
- ☐ Baseret herpå, hvad er virksomhedens tolerance for at påtage sig cyberrisici?

**3. Planer, processer og beredskab**

- ☐ Har virksomheden nedskrevne it-sikkerhedspolitikker, som direktionen aktivt støtter, og som medarbejderne er trænet i?
- ☐ Foreligger der beredskabs- og kommunikationsplaner til at håndtere sikkerheds- hændelser?
- ☐ Beskriver planerne hvordan forretningen kan fortsætte i tilfælde af manglende adgang til de vigtigste it-systemer og it-services, hvem der skal involveres i en krisesituation, og hvordan der sker reetablering af it-systemer og it-services?
- ☐ Angiver planerne en handlingsplan for de første 24 timer efter en sikkerheds-hændelse, herunder hvem der har ansvaret for at føre minutrapport?
- ☐ Bliver planerne øvet og testet regelmæssigt?
- ☐ Hvad er resultatet af seneste test, og har det ført til ændringer?

**4. Rapportering og kontrol**

- ☐ Modtager bestyrelsen med faste intervaller rapporter om virksomhedens cybersikkerhed (risici, status, investeringer, anbefalinger mv.) fra direktionen?
- ☐ Er cyber- og informationssikkerhed et fast punkt på dagsordenen på bestyrelsesmøderne?
- ☐ Har bestyrelsen implementeret cybersikkerhed som en fast del af sit årshjul?

**5. Kultur og mennesker**

- ☐ Er der et trænings- og uddannelsesprogram for, at medlemmer af bestyrelse, direktionen og medarbejdere løbende modtager cybersikkerheds- og awareness træning, herunder træning i krisehåndtering og disaster recovery?
- ☐ Foregår der et samarbejde på tværs af organisationen, hvor der deles viden?
- ☐ Opfordrer virksomheden sine tekniske specialister til at udveksle viden og erfaringer med medarbejdere fra lignende organisationer?
- ☐ Går bestyrelsen forrest i at understøtte en stærk og bevidst cybersikkerhedskultur,
  f.eks. ved selv at anvende VPN, password managers og flerfaktor godkendelse?

**6. Kompetencer og organisering**

- ☐ Har mindst ét bestyrelsesmedlem kompetencer og relevant erfaring indenfor cyber- og informationssikkerhed? Hvis ikke, får bestyrelsen intern eller ekstern rådgivning og/eller sparring på området? F.eks. fra rådgivere eller en komité?
- ☐ Deltager bestyrelsen aktivt i diskussioner om cyber- og informationssikkerhed?
- ☐ Er bestyrelsen opmærksom på, at dens medlemmer selv kan være et oplagt mål
  for cyberangreb?
- ☐ Hvor i organisationen (person/funktion) ligger ansvaret for cyber- og informations-
  sikkerhed?