CENTER FOR CYBERSIKKERHED

KROMANN REUMERT

INDUSTRIENS FOND FREMMER DANSK KONKURRENCEEVNE
The Danish Industry Foundation

BESTYRELSESFORENINGEN
Fokus på værdiskabelse, ledelse og governance

Bestyrelsesforeningens
Center for Cyberkompetencer

Anbefalinger til styrkelse af cyberkompetencer i bestyrelser

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 anbefalinger til (yderligere) investering.

2. Risikoappetit og strategi

Det anbefales, at

- bestyrelsen mindst én gang om året fastsætter virksomhedens risikoappetit indenfor cyber- og informationssikkerhed baseret på en afvejning af virksomhedens forretningsmål og digitaliseringsstrategi, risikoprofil, eksisterende sikkerhedsbudget og investeringsvilje.

Udførelse

3. Planer, processer og beredskab

Det anbefales, at

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

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 bestyrelsesmøde med bl.a. risikovurdering, resultater af sikkerhedstest, sikkerhedshændelser, resultater fra audits, sikkerhedsbudget, forsikringsdækning, resultater fra awareness aktiviteter og anbefalede tiltag og investeringer.

Mennesker

5. Kultur og mennesker

Det anbefales, at

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

6. Kompetencer og organisering

Det anbefales, at

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

CENTER FOR CYBERSIKKERHED

KROMANN REUMERT

INDUSTRIENS FOND FREMMER DANSK KONKURRENCEEVNE
The Danish Industry Foundation

BESTYRELSESFORENINGEN
Fokus på værdiskabelse, ledelse og governance
Bestyrelsesforeningens Center for Cyberkompetencer

Tjekliste til centrale overvejelser i et bestyrelseslokale

1. Risikovurdering og sårbarheder

- ❑ Hvad betyder det for forretningen, hvis vigtige værdier ændres, stjæles eller 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/teknikker 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 sikkerhedshændelser?
- ❑ 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?
- ❑ Bliver planerne øvet og testet regelmæssigt?
- ❑ Hvad er resultatet af seneste test, og har det ført til ændringer?
- ❑ Bliver planerne justeret i lyset af angreb, der har ramt andre virksomheder?
- ❑ Er der indgået aftale med eksterne, som kan tilkaldes for at støtte interne teams?

4. Rapportering og kontrol

- ❑ Modtager bestyrelsen med faste intervaller rapporter om virksomhedens cybersikkerhed (risici, status, investeringer, anbefalinger mv.) fra direktionen?
- ❑ Har bestyrelsen implementeret cybersikkerhed som en fast del af et 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 positiv sikkerhedskultur?

6. Kompetencer og organisering

- ❑ Har mindst ét bestyrelsesmedlem kompetencer og 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?
- ❑ Er cyber- og informationssikkerhed et fast punkt på dagsordenen på bestyrelsesmøderne?
- ❑ 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 informationssikkerhed?
- ❑ Hvem rapporterer denne sikkerhedsfunktion til?
- ❑ Er der allokeret tilstrækkelige ressourcer med de rette tekniske kompetencer til at løfte opgaven?
- ❑ Har virksomheden de rette tekniske kompetencer inhouse eller er der behov for ekstern hjælp?