ANBEFALINGER OG TJEKLISTE

Til styrkelse af strategiske cyberkompetencer i danske bestyrelser

Bestyrelsesforeningens Center for Cyberkompetencer

INDUSTRIENS FOND

KROMANN REUMERT

Dubex:

FE CENTER FOR CYBERSIKKERHED

1. Risikovurdering
- værdier og trusler

Det anbefales, at

- bestyrelsen så ofte som relevant og mindst én gang om året modtager og forholder sig til en opdateret risikovurdering på cyberområdet baseret på virksomhedens vigtigste værdier, it-infrastruktur, forretningsmodel, primære sårbarheder, sandsynlige trusler, mulige tab ved angreb samt mulige konkurrencemæssige vurderinger.

2. Risikoappetit
- risikoafvejning og risikovillighed

Det anbefales, at

- bestyrelsen så ofte som relevant og mindst én gang om året fastsætter virksomhedens cybersikkerhedsstrategi, herunder risikoappetit, baseret på en afvejning af virksomhedens generelle forretningsstrategi, forretningsmål, it-infrastruktur, generelle risikoappetit, sikkerhedsbudget og investeringsvilje m.v.

3. Politikker, processer og beredskab
- delegering og operationalisering

Det anbefales, at

- bestyrelsen fører kontrol med, at cybersikkerhedsstrategien er operationaliseret i politikker, processer og forretningsgange.
- bestyrelsen fører kontrol med, at virksomheden har implementeret passende cyberhygiejne, herunder en relevant backup, der løbende er testet,
- bestyrelsen fører kontrol med, at virksomheden har testede beredskabs- og kommunikations-planer i tilfælde af alt fra hackerangreb til strømnedbrud.

4. Rapportering
- kontrol og tilsyn

Det anbefales, at

- bestyrelsen implementerer cybersikkerhed som en fast del af sit årshjul på linje med øvrige væsentlige risici,
- bestyrelsen har cybersikkerhed på agendaen på hvert møde, og modtager relevant rapportering forud for mødet med bl.a. aktuelt trusselsbillede, sikkerhedshændelser, resultater af sikkerhedstest, awareness aktiviteter og revisionsgennemgange, samt evt. forslag til supplerende tiltag.

5. Kultur
- mennesker og træning

Det anbefales, at

- medlemmer af bestyrelse og direktion regelmæssigt følger specifikke kurser for at opnå tilstrækkelig viden og færdigheder til at forstå og vurdere cybersikkerhedsrisici, styringspraksisser og deres indvirkning på virksomhedens drift,
- virksomheden regelmæssigt har tilpassede uddannelses- og træningsprogrammer for bestyrelse, direktion og medarbejdere i relation til cybersikkerhed,
- bestyrelsen og daglig ledelse går forrest i at understøtte en stærk og bevidst cybersikkerhedskultur.

6. Governance
- kompetencer og organisering

Det anbefales, at

- bestyrelsen forholder sig til, om den har tilstrækkelige kompetencer og erfaring med risikostyring af it- og cyberrisici,
- virksomhedens sikkerhedsorganisation fagligt er direkte forankret på direktionsniveau, og rapporterer direkte til bestyrelsen,
- styrke virksomhedens cybersikkerhed gennem etablering af uafhængige risikostyringskontroller (lines of defence).

1. Risikovurdering – værdier og trusler

- ❑ Hvad er vores vigtige License to Operate (LtO) aktiver? (dvs. hvad vil vi gerne beskytte, hvad er vigtigt for vores forretning, hvad er kronjuvelerne?)
- ❑ Hvad truer vores vigtige LtO aktiver (trusselsvurdering)?
- ❑ Hvorfor skulle dette kunne ske (sårbarhedsvurdering)?
- ❑ Hvad er sandsynligheden for, at det sker?
- ❑ Hvad er konsekvensen af, at det sker (konsekvensanalyse)?
- ❑ Hvad har vi gjort for at reducere risikoen (i form af forebyggelse og beredskab)?

2. Risikoappetit – risikoafvejning og risikovillighed

- ❑ Hvad er virksomhedens overordnede digitale strategi og forretningsmål?
- ❑ Hvad er virksomhedens holdning til at prioritere beskyttelse – f.eks. helst at *forebygge* at hændelser kan opstå og/eller at bruge ressourcerne på et stærkt *beredskab*?
- ❑ Er cybersikkerhed en fast del af virksomhedens kvalitetssikringsprocesser (udvikling, indkøb, salg, outsourcing mv.)?
- ❑ Er der mellem forretningen og risiko-/kontrolfunktioner en fælles forståelse for cybersikkerhed og prioriteringer?
- ❑ Er der klarhed over, hvem der er ejer af de enkelte cyber risici?
- ❑ Kunne virksomheden med fordel indgå samarbejdsaftaler omkring cybersikkerhed eller afdække en del af risikoen via forsikring?
- ❑ Ud fra en samlet afvejning af risici >< omkostninger, hvad er virksomhedens tolerance for at påtage sig cyberrisici, herunder toleranceværdien for de enkelte risici, f.eks. risikotype, produkttype, kunder, strategi, målsætninger mv.?

3. Politikker, processer og beredskab – delegering og operationalisering

- ❑ Hvilke processer og værktøjer anvender virksomheden til at identificere sårbarheder og trusler?
- ❑ Har virksomheden et opdateret overblik over systemer og infrastruktur?
- ❑ Har virksomheden implementeret basal cyberhygiejne?
- ❑ Har virksomheden overvågning til at opdage, hvis der sker noget?
- ❑ Har virksomheden logning, og - hvis ja - hvad logger den på og hvor længe?
- ❑ Har virksomheden backup - og er backup beskyttet?
- ❑ Har virksomheden håndteret cybersikkerhedsrisici i kontrakter med leverandører, kunder mv.?

4. Rapportering – kontrol og tilsyn

- ❑ Har bestyrelsen implementeret cybersikkerhed som en fast del af sit årshjul?
- ❑ Er cybersikkerhed et fast punkt på dagsordenen på bestyrelsesmøderne?
- ❑ Modtager bestyrelsen relevant rapportering fra direktionen om virksomhedens cybersikkerhed forud for hvert møde (med bl.a. risici, status, testresultater, investeringer, anbefalinger mv.)?
- ❑ Får virksomheden og/eller dens leverandører udarbejdet ekstern kontrol, f.eks. revisionserklæringer, på it-sikkerhed?

5. Kultur – mennesker og træning

- ❑ Følger medlemmer af bestyrelse og direktion regelmæssigt specifikke kurser for at opnå tilstrækkelig viden og færdigheder til at forstå og vurdere cybersikkerhedsrisici, styringspraksisser og deres indvirkning på virksomhedens drift?
- ❑ Er der et trænings- og uddannelsesprogram for medlemmer af bestyrelse, direktionen og medarbejdere, så de løbende modtager cybersikkerheds- og awareness træning, herunder træning i krisehåndtering og disaster recovery?
- ❑ Går bestyrelse og direktion forrest i at understøtte en stærk og bevidst cybersikkerhedskultur?

6. Governance – kompetencer og organisering

- ❑ Har medlemmer af bestyrelse og direktion tilstrækkelige kompetencer og erfaring med risikostyring af it- og cybersikkerhedsrisici?
- ❑ Holder bestyrelse og direktion sig løbende orienteret om de cybertrusler og aktører, der truer virksomheden, deres metoder og motivation?
- ❑ Har virksomheden en sikkerhedsorganisation, der er fagligt forankret direkte på direktionsniveau, f.eks. CEO, CFO eller CIO?
- ❑ Hvor i organisationen (person/funktion) ligger ansvaret for cybersikkerhed, og rapporterer denne til de rette på ledelsesniveau?
- ❑ Hvem har risikostyringsansvaret?
- ❑ Hvem kontrollerer hvad (lines of defense)? – Kontrollerer risikoejeren sig selv?
- ❑ Hvem holder styr på risikoeksponeringen fra leverandører?
- ❑ Er der allokeret tilstrækkelige ressourcer med de rette tekniske kompetencer til at løfte opgaven?
- ❑ Hvor meget af sikkerheden står virksomheden selv for, og hvor meget er lagt ud til tredjepart?