Appendiks 5. Sikker kommunikation i bestyrelsen

Som led i at styrke de strategiske cyberkompetencer i danske virksomheder, er en sikker kommunikation i bestyrelseslokalet en vigtig forudsætning for at modvirke eventuelle sårbarheder, som kan skade virksomheden, dens kunder og/eller ansatte.

En velovervejet og gensidig forståelse for sikker kommunikation i bestyrelsen, er en forudsætning for en fortrolig kommunikation i bestyrelseslokalet og ikke mindst for virksomheden generelt.

I takt med udviklingen på digitaliseringsområdet og større digital kompleksitet er der en række områder, som de cyberkriminelle er særlig interesseret i.

I bestyrelseslokalet handler det bl.a. om at beskytte:

► *Data*

► *Omdømme*

► *Immaterielle rettigheder*

► *Strukturelle ændringer som f.eks. ejerskifte, generationsskifte, fusioner*

► *Sensitiv information, f.eks. om virksomhedens risikolandskab, medarbejdere og kunder*

► *Produktnyheder, f.eks. produkter, services og ydelser, som virksomheden ønsker at lancere*

Generelle anbefalinger til sikker kommunikation i bestyrelsen:

1. Mobile elektroniske enheder i lokalet

› Bestyrelsen bør overveje at begrænse mobile elektroniske enheder, når bestyrelsesmøder afholdes. Dette for at begrænse, at digitale medier, via applikationer, smartwatch eller andre elektroniske enheder, kan kompromitteres før-under-efter mødet.

2. Elektronisk kommunikation

› Bestyrelsen bør overveje at undgå brugen af e-mails til at udveksle sensitiv information samt anvende bitlockere, som krypterer og kræver kode for at få adgang til filer. Bestyrelsen kan f.eks. udveksle information og opbevare filer på en board management platform. Eksempel på overblik over forskellige board management software muligheder: https://www.capterra.com/board-management-software/

3. Overvågning i bestyrelseslokalet

› Bestyrelsen bør overveje at begrænse møder i lokaler med lyd- eller videoovervågning i rummet, idet dette begrænser risikoen for at sensitive information lækkes.

4. Tredjeparter i bestyrelsen

› Tredjeparter, som deltager i bestyrelsesmøder eller som modtager sensitive informationer, bør screenes inden deltagelse i bestyrelsesmøder, herunder i forhold til sociale platforme m.v. Dette samme gælder for nye bestyrelsesmedlemmer.

5. Fysisk placering af bestyrelsesmøder

› Bestyrelsen kan overveje at skifte mødelokale fra gang til gang og at booke lokale under et anonymiseret navn for at begrænse mønsteret i bestyrelsens mødeårshjul. Dette gælder særligt, hvis bestyrelsen skal drøfte sensitive emner.

6. Sikker destruktion af sensitive materialer

› Bestyrelsen bør begrænse medbragte sensitive informationer i papirformat og destruere sensitivt materiale efterfølgende, f.eks. efter anvisninger i en arkiverings- og sletningspolitik.