

Styrket cybersikkerhed:

# NIS2-kravene til kapitalselskaber og offentlige myndigheders ledelse



## HVAD ER LEDELSENS ANSVAR?

Uagtet om der er tale om en kapitalvirksomhed eller en offentlig myndighed, har ledelsen ansvar for:

- At godkende foranstaltninger til styring af cybersikkerhedsrisici.
- At føre tilsyn med gennemførelsen.
- At følge kurser, så ledelsen opnår tilstrækkelige kundskaber og færdigheder vedr. cybersikkerhedsrisici.

## HVEM ER OMFATTET, OG HVEM ER ANSVARLIG FOR AT HÅNDHÆVE REGLERNE?

**Kapitalselskaber** er omfattet af direktivet, hvis de har over 50 ansatte, en årlig omsætning og/eller balance på over 10 mio. euro og opererer inden for bestemte sektorer. Det er bestyrelsen og/eller direktionen, som er ansvarlige for og har beføjelser til at træffe afgørelser og føre kontrol på selskabets vegne.

**Offentlige myndigheder** er omfattet uanset størrelse, hvis der er tale om en statslig myndighed, hvor anvendelsen på regioner og kommuner afhænger af den nationale implementering. Den præcise afgrænsning og ansvarsfordeling, herunder hvorvidt ansvaret både gælder den administrative og politisk udpegede ledelse, udestår fortsat.

## HVAD KAN LEDELSEN HOLDES ANSVARLIG FOR?

### Kapitalselskaber:

- Pligtforsømmelser, jf. selskabsloven og sektorspecifik regulering.
- Overtrædelser, jf. NIS2-reglerne (administrativt og evt. civil- og strafferetligt alt efter implementeringslovgivningen).
- Ledelsen kan forbydes at udøve ledelsesfunktioner i selskabet, jf. NIS2-reglerne.

### Offentlige myndigheder:

- Overtrædelser, jf. NIS2-reglerne (administrativt og evt. civil- og strafferetligt alt efter implementeringslovgivningen).
- Pligtforsømmelser, jf. straffelovens § 155, 156 og 157 samt tjenestemandsløven, iht. overenskomst og/eller kontrakter.
- Medlemmer af Folketinget, regionsråd og kommunalbestyrelser er undtaget. Her gælder ministeransvarsloven, kommunestyrelsesloven og regionsloven.