NIS2

Overholder jeres virksomhed kravene til det nye cyber-direktiv NIS2?

MODENHEDSANALYSE OG ANBEFALINGER I FORHOLD TIL KRAV FRA NIS2-DIREKTIVET

ER I SOM ORGANISATION OMFATTET?

Få foretaget en konkret vurdering om I er omfattet som væsentlig eller vigtig enhed.

Såfremt I er omfattet af direktivet skal I være opmærksom på, at der sættes betydelige krav til jeres organisation.

Herunder jeres governance, nedskrevne politikker og processer samt reaktion ved IT-hændelser.

LOVKRAV TIL VIRKSOMHEDER

NIS2-direktivet regulerer virksomheder og myndigheder forhold indenfor cybersikkerhed, som har betydning for samfundet.

Reguleringen skal håndhæves af medlemslandene fra medio 2024

LEDELSESMÆSSIG FORANKRING

NIS2-direktivet stiller betydelige krav til ledelsens indsigt i og organisationens risikostyring, forretningskontinuitet og rapportering til myndighederne. Ledelse bliver direkte ansvarlig og kan ikke delegere dette ansvar.

Vi anbefaler, at I som organisation kommer i gang nu.

UDVALGTE KRAV I NIS2

- Krav om ledelsesmæssig forankring (art. 17)
- Effektiv risikostyring (art. 18)
- Håndtering af sikkerhedshændelser (art. 20)

Få en gratis og uforpligtende samtale med Partner, Michael Gadgaard

+45 53 54 53 34

Michael@salamon.dk

SALAMON&COMPANY

VI ER MED HELE VEJEN IGENNEM

PROCESSEN

FASE 1

VURDERING

Identificere, hvorvidt I vil blive omfattet af NIS2-direktivet, og i givet fald hvordan (essentiel eller vigtig enhed)

WORKSHOP

Analyse og indsigt i jeres nuværende tekniske, operationelle og organisatoriske foranstaltninger. (As Is analyse)

MODENHEDSANALYSE

Identificere mangler i forhold til kravene i direktivet og anbefalinger fra Center for Cybersikkerhed

ANBEFALING

Konkret anbefaling til tekniske, operationelle og organisatoriske foranstaltninger

FASE 2

IMPLEMENTERING (OPTION)

Implementering af både organisatoriske og tekniske krav i jeres organisation

Etablere de kapabiliteter, der er nødvendige for at varetage forpligtelsen i jeres organisation