KonsensIT
En del af CapMon A/S

NIS2

- Beskyt virksomhedens værdier!

Nye konkrete og skærpede krav til informationssikkerhed stiller øgede krav til bestyrelsen og ledelsen. Det nye direktiv vil du komme til at kende som NIS2.

Hvorfor NIS2

Med den eksplosive udvikling af digitaliseringen bliver stort set alt bundet sammen - også på tværs af landegrænser. Truslen stiger tilsvarende fra mange forskellige fronter.

For at sikre en ensartet og tilstrækkelig beskyttelse fastsætter NIS2 direktivet regler for cyber- og informationssikkerhed, som vi skal leve op til. Direktivet gælder for både offentlig og privat virksomhed

Sund fornuft eller bureaukrati

Direktivet stiler mon en højere grad af sikkerhed i virksomhederne, dels fordi der er store værdier på spil ved angreb, og dels fordi der er den store sammenhæng - når én falder, kan det trække flere med i faldet. NIS2 er derfor sund fornuft - ikke et bureaukratisk påfund.

Den 13. maj 2022 blev NIS2 direktivet vedtaget i EU, og inden for kort tid kommer de danske regler. Herefter er der 21 måneder for virksomhederne til at implementere reglerne.

Hvad er NIS2

NIS2 er en hjælp til at opsætte rammerne for sikkerhed. I forhold til tidligere (NIS1) er langt flere virksomheder og sektorer nu omfattet af reglerne.

Det skal ske via en række risikobaserede foranstaltninger bl.a. forebyggelse og håndtering af sikkerhedshændelser, sikkerhed i dataopbevaring og databehandling samt planer for håndtering af hændelser, hvis der sker et cyberangreb.

NIS2 er ikke noget som løses i IT-afdelingen men er et ledelsesanliggende for at beskytte virksomhedens værdier!

Virksomheder opdeles i væsentlige enheder (fx energi, regioner, datacentre) og vigtige enheder (fx fødevarer, pharma, optisk udstyr, transport).

Der er nogle overordnede lister med omfattede virksomhedstyper, men det forventes, at disse bliver detaljeret yderligere.

Skærpede krav

Konkret betyder NIS2, at virksomhederne skal træffe passende og forholdsmæssige tekniske og organisatoriske foranstaltninger; herunder en række af de krav, der bla. skal være styr på:

- Risikoanalyser og sikkerhedspolitikker.
- Krisehåndtering
- Værdikædesikring og sikkerhedsrelaterede aspekter vedrørende forbindelserne mellem virksomhe den og dens leverandører
- Driftskontinuitet
- Hændelseshåndtering (forebyggelse, opdagelse og reaktion på hændelser).
- Kryptering
- Politikker og procedurer (test og revision) til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici.

>>2

Indrapportering til myndigheder
Et af de nye krav er, at virksomhederne indenfor 24 timer skal informere myndighederne om enhver sikkerhedshændelse og cybertrussel, der har en væsentlig indvirkning på levering af deres tjenester.

Fokus på ledelsens ansvar
Et andet og nyt krav er, at ledelsen/bestyrelsen **SKAL** involveres i styring, godkendelse og tilsyn med cyber- og informationssikkerhedsrisici, og de kan blive stillet direkte til ansvar for brud på NIS2.

Væsentlige brancher	Vigtige brancher
Energi	Fødevare
Regioner	Pharma
Datacentre	Optisk udstyr
	Transport

NIS2 omfatter langt flere brancher end NIS1. Ovenfor er en overordnet opdeling i væsentlige og vigtige enheder. Opdelingen forventes at blive yderligere detaljeret.

Hvornår skal du i gang

Da GDPR skulle implementeres fik de, der ikke var forberedte meget travlt. I første omgang med at forstå reglerne og derefter med at finde ud af, hvordan de skulle efterleve dem.

For at undgå at komme i en presset situation, hvor både tid og adgang til rådgivere kan blive knap, vil det være rettidig omhu at begynde arbejdet **NU**.

Myndigheder skal i lighed med GDPR føre tilsyn og udstede påbud eller bøder, som kan være helt op til 10.000.000 EUR eller 2 % af den samlede globale årsomsætning.

Anbefalede fokusområder

Få styr på hvad I har i dag, læg en plan for at få det som mangler på plads. Etablér en drift i forhold til overvågning, rapportering og deling.

- Beredskabsplaner; skal løbende testes (skal kunne dokumenteres)
- Ledelse/bestyrelse skal involveres (godkendelse og rapportering).
- Procedure til at identificere sikkerhedshændelser og indrapportere til myndigheder.
- Etablér en operationel krisestyringsorganisation og plan.

Hvordan kan vi hjælpe

KonsensIT's konsulenter har bred erfaring med styring af sikkerhedsprojekter, herunder bl.a. GDPR compliance, risikovurdering, beredskabsplaner.

Vi bruger vores erfaring fra eksisterende NIS2 opgaver og vil i samarbejde med Jer hjælpe med at skabe et overblik over de forskellige opgaver og herefter udarbejde en plan som skal sikre overholdelse af NIS2 reglerne.

Kontakt:
Mail: jt@konsensit.dk
Tel.: +45 4485 5070
Mobil.: +45 2689 0088

*"Ledelsesorganerne for væsentlige og vigtige enheder **godkender** de foranstaltninger til styring af cybersikkerhedsrisici, som disse enheder har truffet for at overholde artikel 18. De fører **tilsyn** med gennemførelse og er **ansvarlige** for enhedernes manglende overholdelse af forpligtelserne."*