6 HURTIGE OM NIS2

FOCUS ADVOKATER

1 Hvad er NIS2, og hvorfor er det relevant?

NIS2 er et kommende EU-direktiv, der sigter på at øge cybersikkerheden i net- og informationssystemer i de kritiske infrastruktursektorer. NIS2 fastsætter en række sikkerhedskrav og sanktioner, der skal sikre, at en lang række organisationer i EU sætter cybersikkerheden på dagsordenen og implementerer passende cybersikkerhed.

NIS2 vil bl.a. bidrage til at:

1. øge **sikkerheden** og **robustheden** i de omfattede organisationers net- og IT-systemer
2. **cybersikkerheden indtænkes i organisationers strategier**, hvor der skal gennemføres tiltag, som sikrer hurtig og effektiv reaktion på sikkerhedshændelser
3. give **økonomiske**, samt **sikkerheds-** og **konkurrencemæssige fordele** i form af bl.a.:
   - øget modstandsdygtighed mod angreb
   - fokus på en ansvarlig digitalisering i organisationen
   - større tillid fra kunder/borgerer til organisationer, der imødekommer NIS2

Ansvar ved manglende efterlevelse af reglerne

Manglende overholdelse af NIS2 kan føre til midlertidig **suspension af enhver person med ledelsesansvar på direktionsniveau** eller **suspension af juridiske repræsentanter i at udøve ledelsesfunktioner**.

Der kan også straffes med **bøder** op til **€ 10 mio**. eller **2% af den årlige globale omsætning**.

2 Hvem omfattes af NIS2?

NIS2 vil både direkte og indirekte komme til at omfatte en meget bred mængde af organisationer. I en kortlægning af NIS2 foretaget af Industriens Fond blev det fremhævet, at **over 1.500 danske organisationer vil berøres af NIS2.** NIS2 vil ***direkte*** berøre de organisationer, der anses for "vigtige" eller "væsentlige" enheder.

Læs mere herom i bilaget ***"Er min organisation omfattet af NIS2?".***

Herudover vil NIS2 ***indirekte*** berøre organisationer, der indgår i **forsyningskæden** med de direkte omfattende organisationer, da disse har pligt til at sikre **forsyningskædesikkerheden**. Hvis du som leverandør leverer ydelser til en NIS2-omfattet organisation, vil du derfor kunne blive mødt med **aftalemæssige krav** om at have tilsvarende og passende sikkerhedsforanstaltninger i dine net- og informationssystemer.

3 IT-trusler som en voksende risikofaktor

Organisationer, der enten direkte eller indirekte bliver omfattet af NIS2**, skal indtænke cybersikkerhed i sine strategier**. Det indebærer også, at organisationerne – navnlig ledelsen – skal tildele de nødvendige ressourcer for at kunne udleve strategierne.

Organisationer, der får implementeret cybersikkerhedsforanstaltninger, skal **løbende tilpasse sig til risici**, der påvirker deres forsyningsområde. De valgte tiltag skal vurderes og tilpasses til de gældende behov og risici, der opstår i de enkelte sektorer.

6 HURTIGE OM NIS2

FOCUS ADVOKATER

4

Hvordan skal du forholde dig til NIS2?

Organisationer kan indtænke NIS2 på samme måde som GDPR. Det vil sige, at der skal laves en kortlægning af de krav, der stilles, og hvor langt organisationen er med at overholde dem. Da der samtidig er en del overlap mellem GDPR, NIS2, og andre cybersikkerhedsregler (f.eks. Cyber Security Act), bør de valgte tiltag være i overensstemmelse med reglerne og principperne i de øvrige regelsæt for at sikre en holistisk tilgang.

5

Hvilke grundlæggende krav stiller NIS2?

Ledelsesforankring

Organisationernes ledelsesorganer skal gennemføres tiltag, der fremmer cybersikkerheden. Det indebærer bl.a.:

- at **godkende** foranstaltninger (f.eks. politikker) til styring af cyberrisici
- at **føre tilsyn** med cybersikkerhedsrisici og
- en pligt til at **følge kurser og undervisning**, der giver ledelsesorganerne kompetencer til at vurdere risici og metoder til styring af cybersikkerhedsrisici.

Risikostyring og cyberrisici

NIS2 stiller krav til **tekniske, operationelle og organisatoriske foranstaltninger**. Organisationer skal navnlig gennemføre disse tiltag inden for følgende områder:

Politikker for risikoanalyse og informations-sikkerhed	Håndtering af hændelser	Backup, reetablering og krisestyring	Forsyningskæde-sikkerhed	Udvikling og vedligeholdelse af informationssystemer
Politikker og procedurer til vurdering af effektiviteten	Praksis for cyberhygiejne og uddannelse af ansatte	Politikker vedrørende brug af kryptering	Personalesikkerhed, adgangspolitikker og forvaltning af aktiver	Multifaktor-autentificering

Rapportering

NIS2 stiller krav til, at organisationerne **underretter tilsynsmyndighederne** efter at der er sket en væsentlige sikkerhedshændelse. Tidsfristerne for underretning er:

- Inden for **24 timer** sendes en "*tidlig varsling*" om, at en væsentlig hændelse er i gang
- Inden for **72 timer** sendes en konkretiseret "*underretning*" om karakteren af hændelsen
- Inden for **en måned** sendes en "*endelig rapport*" om hændelsen med alle relevante detaljer

6

Fristerne nærmer sig

De nationale regler for NIS2 skal offentliggøres senest den 17. oktober 2024, og håndhævelsen af reglerne begynder fra **den 18. oktober 2024**.

Start derfor allerede i dag med at gøre jeres organisation klar til NIS2.

FOCUS ADVOKATER P/S Cortex Park Vest 3 DK 5230 Odense M Tel: 63 14 20 20 www.focus-advokater.dk Version: December 2023
ODENSE SVENDBORG KOLDING KØBENHAVN HAMBORG