NIS2-cyberdirektiv: Hvad skal din virksomhed gøre?

NIS2-direktivet udvider kravene og sanktioneringen af cybersikkerhed. Skærpede krav for flere sektorer betyder, at din organisation skal forholde sig til blandt andet risikostyring, kontrol og tilsyn, men hvor skal I starte, og hvad skal I starte med at gøre?

Hvad er NIS2-direktivet?
NIS-direktivet regulerer virksomheder og myndigheder på cyber- og informationssikkerhedsområdet. EU-direktivet bliver udmøntet i nationale bekendtgørelser og fungerer som bindende lov, hvilket betyder, at din organisation skal efterleve kravene i bekendtgørelsen.
NIS2-direktivet udvider kravene og sanktioneringen af cybersikkerhed for at harmonisere og strømline sikkerhedsniveauet på tværs af medlemslandene i EU.

pwc

Revision. Skat. Rådgivning.

William Sharp
Partner
T: +45 8932 0076
E: william.sharp@pwc.com

Mila Bahir
Senior Associate
T: +45 2164 5182
E: mila.bahir@pwc.com

Thomas Kristmar
Director
T: +45 3945 9860
E: thomas.kristmar@pwc.com

Trin for trin, hvad skal I gøre?

Det kan virke som en uoverskuelig opgave at efterleve den 150 sider lange NIS2-lovgivning. Hvordan finder man hoved og hale i det? Hvor starter man? Hvordan får man kravene implementeret, så de rent faktisk efterleves i praksis? I PwC har vi lavet en trin-for-trin-guide, som hjælper din organisation i gang med at implementere NIS2-kravene.

1. Få foretaget en modenhedsvurdering og skab opbakning fra ledelsen

Første skridt er at få foretaget en vurdering af, hvad det vil kræve for jeres organisation at efterleve NIS2-kravene. Dette kaldes også en modenhedsvurdering og kan udføres af eksterne konsulenter.

Vurderingen viser, hvilke konkrete områder I enten skal starte med eller arbejde videre med for at implementere kravene effektivt. Dette kan I bruge til at få prioriteret de rigtige økonomiske- og FTE-ressourcer.

Vurderingen vil ligeledes kunne bruges til få ledelsens opbakning til arbejdet med NIS2-direktivet. Netop ledelsesopbakning er et centralt emne i direktivet, fordi ledelsen i omfattede organisationer stilles direkte til ansvar for, at kravene bliver overholdt.

2. Scope rigtigt – det er kun jeres driftskritiske aktiver

NIS2-direktivet søger at beskytte kritisk infrastruktur, forsyningskæder til kritisk infrastruktur og andre samfundsvigtige funktioner. Dette er en altafgørende faktor i jeres arbejde med NIS2-direktivet, da det i praksis sætter rammen for, hvilke processer, mennesker, teknologier og leverandører, der er omfattet af direktivet.

For at sætte scopet for arbejdet, skal I foretage en business impact analyse (BIA). Dette gør I ved først og fremmest at identificere, hvilke forretningsprocesser, der understøtter den samfundskritiske drift. Når I har identificeret de driftskritiske forretningsprocesser, skal I kortlægge alle de aktiver, der er relevante for disse processer. Det kan fx være mennesker, systemer og leverandører. Afslutningsvis skal I konsekvensvurdere aktiverne, der i så fald udgør jeres NIS2-scope.

3. Brug en international standard som styringsramme

NIS2-direktivet stiller krav til, at de omfattede organisationer implementerer et ledelsessystem for informationssikkerhed (ISMS). Internationale standarder som ISO 27001 eller NIST evt. IEC kan bruges som effektive styringsrammer til at få etableret et operationelt ISMS. ISO 27001 udgør samtidig et "best practice"-rammeværktøj for en holistisk og ledelsesforankret styring af informationssikkerhed.

For at implementere et effektivt ISMS skal jeres organisation opbygge operationelle politikker, procedurer og processer for at styre informationssikkerheden. Eksempelvis skal I beslutte jer for roller- og ansvar, risikoproces, målsætninger mv.

I kan med fordel planlægge awareness-indsatser, som skaber en reel forandring hos ledere og procesejere. På den måde får jeres ISMS lov at leve i organisationen, og I undgår, at det blot bliver en række dokumenter, der samler støv.

4. Risikovurdér jeres aktiver og implementér formildende foranstaltninger

NIS2-direktivet stiller krav til en risikobaseret tilgang til informationssikkerhed. I praksis betyder det, at jeres organisation skal beskrive en risikoproces, som I skal efterleve. I efterlever processen ved at risikovurdere samtlige af de aktiver, som I har identificeret som værende kritiske for jeres samfundskritiske funktion. Det vil altså sige, at I også skal risikovurdere jeres forsyningskæde og leverandører.

Som en del af jeres risikohåndtering skal I implementere skadesforebyggende foranstaltninger, der formindsker jeres risici. Minimumskrav er:

- Awareness
- HR sikkerhed
- Styring af aktiver
- Hændelseshåndtering
- Sårbarhedsstyring
- Sikring af forsyningskæder og IT-beredskabsplanlægning
- Netværkssikkerhed
- Sikkerhed i udviklingsprocesser
- Adgangsstyring
- Kryptering.

5. Rapportér til CSIRT (Center for Cybersikkerhed)

NIS2 stiller krav til, at organisationer skal rapportere hændelser til CSIRT inden for 24 timer. Derudover skal organisationen løbende opdatere CSIRT'en med status på hændelsen og eventuelle kompromitteringer.

Hvis hændelsen vurderes at have en effekt på flere medlemsstater, vil den blive rapporteret videre igennem ENISA. Formålet med kravet til rapportering er bl.a. at øge kapabiliteten på tværs af det europæiske cyberlandskab.

pwc

Revision. Skat. Rådgivning.