NIS2: Det du trenger å vite om direktivet og hvordan forberede din virksomhet

Hugo-A. B. Munthe-Kaas
Partner, Head of Compliance

Lars Albert Jøstensen
Senioradvokat

Johan André Eikrem
Senioradvokat

Fra 24. oktober 2024 skal medlemsstatene i EU ha gjennomført NIS2-direktivet i nasjonal rett. Ettersom direktivet er ansett som EØS-relevant, er det ventet at direktivet etter hvert også vil innlemmes i norsk rett. Formålet med NIS2 er å styrke Europas motstandskraft mot cybertrusler ved å etablere felles standarder for cybersikkerhet og et effektivt varslingsregime. Dette vil innebære klare krav til hvordan bedrifter og deres styre, og ledelse skal håndtere cybersikkerhet og varsling av alvorlige sikkerhetsbrudd. Implementeringen vil dermed markere en viktig milepæl for virksomheter som leverer samfunnsviktige tjenester. Brudd på direktivet kan eksponere virksomheter for bøter på opp mot EUR 10 000 000 eller 2 % av årlig omsetning.

Omfattes din virksomhet av direktivet?

Direktivet gjelder for virksomheter som driver virksomhet innen sektorer som defineres som vesentlig («essential») eller viktig («important») for samfunnet og som (i) enten har 50 eller flere ansatte, eller (ii) har en omsetning og/eller balanse på minst EUR 10 000 0000.

Sektorer definert som «essential»

- Energi
- Helse
- Digital infrastruktur
- Transport
- Drikkevann
- IKT-tjenester
- Bank
- Avløpsvann
- Romvirksomhet
- Finansmarkeds-infrastrukturer
- Offentlig forvaltning (sentral og regional)

Sektorer definert som «important»

- Post - og kurertjenester
- Matproduksjon
- Tilbydere av digitale tjenester
- Avfallshåndtering
- Produksjon av visse varer *(medisinsk utstyr, IKT-utstyr, kjøretøy, elektronikk, maskiner, transportutstyr)*
- Forskning
- Produksjon og distribusjon av kjemikalier

Hvilke sektorer som anses som «vesentlig» eller «viktig» er angitt i direktivet, hvorav 11 defineres som vesentlige og 7 som viktige. Konsekvensen av at tilbydere klassifiseres og deles i to ulike kategorier, er at de underlegges forskjellige tilsynsregimer

Direktivet kan også gjelde uavhengig av størrelse hvis tilbyderen har en nøkkelrolle for samfunnet, økonomien eller spesifikke sektorer. Som eksempler på dette, nevner direktivet særlig utsatte virksomheter hvor en cyberhendelse vil gi betydelige effekter på offentlig trygghet, sikkerhet eller helse, eller virksomheter som er eneleverandør av en spesifikk tjeneste i et EU-land. Tilbyderne som innehar en nøkkelrolle i direktivets forstand, skal identifiseres og innmeldes av Norge til EFTAs overvåkningsorgan, ESA.

Hvilke krav stiller direktivet til din virksomhet?

Direktivet stiller blant annet skjerpede sikkerhetskrav og krav til varsling av hendelser.

Direktivet pålegger de berørte virksomhetene å utarbeide en risikostyringsmetode med visse minimumskrav. Blant annet settes det krav til risikoanalyser, hendelseshåndtering, krisehåndtering, overvåkning, testing etc. I tillegg stilles det krav om å håndtere cybersikkerhetsrisiko i forsyningskjeder og hos leverandører.

Direktivet innfører også krav til varsling av hendelser. Dersom hendelsen anses som en såkalt «significant incident» må virksomheten varsle relevante myndigheter innen 24 timer etter at virksomheten fikk kunnskap om hendelsen. Varselet skal kort beskrive hvorvidt hendelsen skyldes ulovlig eller ondsinnet aktivitet eller har potensielle grenseoverskridende følger. Innen 72 timer skal virksomheten sende et oppdatert varsel som inneholder en innledende vurdering av hendelsen, herunder alvorlighetsgrad, virkning og angrepsvektor.

Hvordan bør din virksomhet gå frem for å oppfylle NIS2?

Selv om direktivet ennå ikke er implementert i norsk rett, er det ventet at reglene vil innlemmes i norsk rett på sikt. For å sikre rettidig etterlevelse, kan det derfor være hensiktsmessig allerede nå å kartlegge i hvilken grad man vil være underlagt de nye reglene, samt igangsette arbeidet med å vurdere om eksisterende risikovurderinger og sikkerhetstiltak er i overenstemmelse med de kommende kravene under NIS2.

DLA Piper kan bistå din virksomhet med implementeringen av NIS2

DLA Piper bistår bedrifter, styre og ledelse med beredskap, håndtering av hendelser og etterlevelse av regelverk vedrørende cybersikkerhet. Vi bistår forsikringsselskaper med utarbeidelse av vilkår, hendelseshåndtering og dekningsoppgjør, og samarbeider jevnlig med tverrfaglig ekspertise på håndtering av cyberhendelser.

Kontakt gjerne vårt cyber-team dersom du har spørsmål om NIS2 eller ønsker å diskutere cybersikkerhet for din bedrift.