Klima-, Energi- og Forsyningsministeriet

One-pager om kritisk infrastruktur og cybersikkerhed for havvind

Opstillere og operatører af havvindmøller skal overholde de til enhver tid gældende regler, herunder ift. beredskab og cybersikkerhed. Den 7. marts 2025 trådte Lov om styrket beredskab i energisektoren i kraft, der bl.a. implementerer EU's NIS2- og CER-direktiv i energisektoren. Loven har til formål at øge modstandsdygtigheden og beredskabet over for naturskabte, menneskeskabte og teknologiske trusler mod den danske energiforsyning på tværs af energiformer.

Loven indebærer bl.a. at opstillerne og operatørerne vil skulle efterleve en række krav til cybersikkerhed og fysiske foranstaltninger, herunder beskyttelse mod usikker eller uautoriseret fjernadgang.

Krav til leverandørstyring og risiko- og sårbarhedsstyrring i lov om styrket beredskab i energisektoren

Det følger af bekendtgørelse om modstandsdygtighed og beredskab i energisektoren efter lov om styrket beredskab i energisektoren, at omfattede virksomheder i energisektoren bl.a.:

- Skal kunne identificere, vurdere og håndtere risici, der er specifikke for hver direkte leverandør og tjenesteudbyder i virksomhedens forsyningskæde, og at de har metoder til at vurdere modstandsdygtigheden af de leverede produkter.
- Skal forholde sig til risici forbundet med afhængigheder af underleverandøren og internationale forhold i en aftale med en direkte leverandør og tjenesteudbyder.
- Skal have procedurer for styring af fjernadgange for direkte leverandører og tjenesteudbydere, som kan tilgå virksomhedens forsyningskritiske net- og informationssystem.
- Skal sikre at krav om organisatorisk beredskab, fysisk sikring og cybersikkerhed rettet mod direkte leverandører eller tjenesteudbyder fremgår af virksomhedens leverandøraftale.
- Skal gennemføre risikovurdering ved følgende projekter: 1) erhvervelse og udvikling af forsyningskritiske net- og informationssystemer, 2) etablering af nye anlæg eller opkøb af anlæg i klasse 3-5, 3) ændring af eksisterende anlæg i klasse 3-5, som forventes at medføre en ændring i et anlægs klassificering og 4) outsourcing af udviklings-, drifts- og vedligeholdelsesopgaver, der kan påvirke leveringen af virksomhedens tjenester.
- Skal sikre overholdelse af krav om organisatorisk beredskab, fysisk sikring og cybersikkerhed.
- I deres risikovurdering af projekter, hvor der indgår et leverandørforhold, skal der inkluderes en vurdering af risici, som følger af leverandørforholdet. Risikovurderingen skal udarbejdes ved projektets opstart og foreligge skriftligt, inden projektet påbegyndes. Risikovurdering skal opdateres, når projektets omfang, tidsplan og delleverancer ændres i en sådan grad, at det ændrer forudsætningerne for risikovurderingen.
- Fremsende deres risikovurdering til Energistyrelsen til godkendelse ifm. følgende projekter: 1) anlægsprojekter, hvor et anlæg ved fuldførelse forventes at opfylde tærskelværdierne for anlæg i klasse 4 og 5 og 2) erhvervelse eller udvikling af forsyningskritiske net- og informationssystemer.
- Skal sende risikovurderinger til Energistyrelsen senest én måned efter ledelsesorganets godkendelse af en risikovurdering.
- For virksomheder i niveau 4 og 5 skal servere og datacentre, der understøtter virksomhedens forsyningskritiske net- og informationssystemer, placeres inden for EU/EØS-lande.

Kilde: Klima-, Energi- og Forsyningsministeriet.