VATTENFALL

Vattenfall reactie op consultatie NIS 2.0

Vattenfall waardeert het de ontwerptekst van de het voorstel voor de implementatie van de NIS 2.0. Dit is een belangrijke stap om de beveiliging van het energiesysteem doelmatig en van de beste standaarden te houden. In deze reactie stellen wij onze aanbevelingen voor om de ontwerpwet te versterken.

Veiligheid is de grootste prioriteit voor Vattenfall. Het is zaak dat de wet bijdraagt aan een betere veiligheid en geen onnodige rapportageverplichting oplegt. Het zou daarom goed zijn een onderscheid te maken tussen locaties die financieel of administratief karakter hebben en locaties waar disruptie of calamiteit daadwerkelijke fysieke impact kan hebben zoals bij productielocaties, gasopslag, en warmte distributie.

De belasting van de risico-inventarisatie, zorgplicht, meldplicht, communicatieplicht vragen een gedetailleerde aanpassing in organisatie van bedrijven. Het zou daarom ook goed zijn als daar duidelijke richtlijnen voor worden gedeeld, bij voorkeur op groepsniveau met een enkel aanspreekpunt en in overleg met de sector over de scope en toewijzing aan partijen.

Daarenboven dragen wij graag de volgende aandachtspunten aan:

- In artikel 2d is onvoldoende duidelijk welke criteria worden toegepast op bijna-incidenten, cyberdreigingen en kwetsbaarheden en hoe deze gemeld moeten gaan worden. Het zou goed zijn deze te verduidelijken.
- In artikel 15 en 16 is onduidelijk of stadsverwarming onder de wet valt.
- Artikel 26 (6) beschrijft dat het bestuur van een essentiële entiteit of belangrijke entiteit zal toezien op de maatregelen en de uitvoering van de maatregelen en omvat kennisvereisten voor ieder lid van het bestuur. Wij verzoeken om een toevoeging voor een holdingstructuur. Daarnaast is het belangrijk de criteria voor training zo snel mogelijk duidelijk te maken, waarbij ook duidelijk gemaakt moet worden of de training intern of extern behoort te zijn.
- In artikel 27(2a) wordt uitgelegd wat er onder significant wordt verstaan. In tegenstelling tot NIS1 is een incident nu ook significant als het financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken. Dit is altijd het geval, dus in theorie moet dan alles worden gemeld. Hier verzoeken wij om verduidelijking en merken wij op dat cyber incidenten altijd moeilijk uit te drukken zijn in geld.
- In artikel 45 zou het helpen de moeder-dochter constructie te verduidelijken (zie punt hierboven.

Wij zijn uiteraard graag bereid deze reactie verder toe te lichten en samen te werken bij de implementatie.