Managementsamenvatting

De offshore windsector (Wind op Zee) vervult een sleutelrol voor de Nederlandse energietransitie in het behalen van de gestelde klimaatdoelstellingen. Echter, deze snelle groei en de digitalisering van de energiesector heeft geleid tot een toename aan kwetsbaarheden op het gebied van cyberveiligheid van de kritische infrastructuur. Onder leiding van Hans Timmers (Managing Director) heeft adviesbureau ECHT in opdracht van Topsector Energie, de Rijksdienst voor Ondernemend Nederland en TKI Offshore Energy (voorheen 'TKI Wind op Zee') een kwartiermaker verkenning uitgevoerd naar de kansen voor meer kennisdeling en samenwerking op het gebied van cybersecurity binnen de wind op zee sector.

Gedurende een periode van vijf maanden is er door de kwartiermaker en zijn team gesproken met veel verscheidene stakeholders binnen het complexe en dynamische speelveld waar de windenergiesector en cybersecurity elkaar raken. Dit zijn in eerste instantie partijen uit de windenergiesector geweest, zoals de ontwikkelaars van offshore windparken en de toeleverende keten (supply chain), ook wel Original Equipment Manufacturers (OEM's) genoemd. Daarnaast is er gesproken met een breed scala aan partijen die een relevante rol spelen binnen het speelveld van de energieketen en cybersecurity. Denk hierbij aan afgevaardigden van overheidsinstanties, deskundigen vanuit de cybersecurity sector en coördinatoren en deelnemers van overlegstructuren zoals Information Sharing and Analysis Centers (ISAC's. Vanuit gesprekken, kennissessies en overige input zijn patronen kenbaar geworden die hebben geleid tot verschillende aanbevelingen.

Er is een duidelijke behoefte en bereidheid geconstateerd voor meer kennisdeling en samenwerking op het gebied van cybersecurity binnen de wind op zee sector. Dit houdt verband met een aantal achterliggende oorzaken. Ten eerste is er binnen de wind op zee sector sprake van een groeiend besef over het belang van de veiligheidswaarborging van zowel eigen assets als de algehele kritieke infrastructuur. Dit heeft onder andere te maken met de toegenomen geopolitieke onrust en concrete dreiging. De koppeling van de digitale infrastructuur aan de fysieke infrastructuur door de digitalisering van de energieketen vormt hierbij een belangrijke factor. Daarmee heeft cybersecurity een hogere urgentie verkregen op de veiligheidsagenda's van bedrijven binnen de wind op zee sector.

De nieuwe Europese NIS2 richtlijn (Network- and Information Systems), die de initiele NIS vervangt, speelt mee in de bereidheid tot samenwerking en kennisuitwisseling. Na de vertaling van de NIS2 naar de Wet beveiliging netwerk-en informatiesystem (Wnbi) zullen meer bedrijven en organisaties die gekenmerkt worden

als ‘aanbieders van essentiële diensten (AED’s) moeten voldoen aan een zorg- en meldplicht. Windenergieproducenten die meer dan 100 megawatt opwekken vallen hieronder en moeten passende maatregelen treffen. Dit vergroot de behoefte tot kennisdeling binnen de wind op zee sector en brede energieketen, om spreekwoordelijk het ‘wiel’ niet opnieuw uit te hoeven vinden.

Vanuit de gestelde verkenningsvraag aan de kwartiermaker Wind op Zee zijn verschillende voorkeuren en voorwaarden waargenomen omtrent de wenselijke vormgeving van samenwerking rondom cybersecurity. Deze voorkeuren zijn deels gericht op een openbare vorm van kennisdeling binnen de sector, maar voornamelijk gecentreerd rond een besloten overlegstructuur. Bedrijven erkennen het belang van kennisuitwisseling over cybersecurity thematiek binnen de wind op zee sector en geven daarbij voorkeur aan een (ISAC) overleggroep. Daarbij wordt de opbouw van een vertrouwensband tussen de deelnemers als een essentiële factor voor succes beschouwd. Echter komt hierbij ook de roep naar voren voor meer ‘gelaagdheid’ en verbinding tussen niveaus, thema’s en relevante schakels van verschillende overlegstructuren en initiatieven. Een centrale rol hierbij is weggelegd voor de Nederlandse Energie ISAC (E-ISAC). Een groot aantal ontwikkelaars van offshore windparken is al deelnemer van de Energie ISAC. Er is een heldere voorkeur om geen nieuwe losse ISAC te starten maar aansluiting te vinden bij deze overlegstructuur en andere relevante initiatieven.

De speelveldanalyse laat tevens zien dat er grote variatie bestaat in de mate van cybersecurity volwassenheidsniveaus tussen de verschillende stakeholders. Deze verschillen onderstrepen de behoefte tot meer (thematische) organisatie van overleg. Ook komt het onderwerp ‘ketenverantwoordelijkheid’ op het gebied van cybersecurity duidelijk naar voren in de samenwerkingsbehoefte. Dit komt ook terug in de tendercriteria rondom Internationaal Maatschappelijk Verantwoordelijk Ondernemen (IMVO, of in het Engels International Responsible Business Conduct, IRBC). Organisaties willen en moeten inzichtelijk hebben met welke (keten)partijen zij werken en of zij betrouwbaar zijn. Ook hierbij speelt de NIS2 richtlijn voor bedrijven een belangrijke rol. Denk hierbij aan aansprakelijkheid en aandacht delegeren rondom cybersecurity issues naar toeleverende partijen.

Kortom, er is sprake van een momentum voor meer samenwerking en kennisdeling binnen de wind op zee sector en verbinding met de bredere energieketen.

Aanbevelingen

De speelveldanalyse heeft een waardevolle bevindingen voortgebracht, welke hebben geleid tot een drietal aanbevelingen:

1. Organiseer een cybersecurity overlegstructuur voor Wind op Zee. Oriënteer op de eerste mogelijke stappen om een dergelijke structuur te organiseren.
2. Creëer gelaagdheid en verbinding door aansluiting te vinden bij bestaande samenwerkingsverbanden (met een centrale rol voor de Energie ISAC).
3. Oriënteer op de mogelijkheden tot integratie van cybersecurity normeringen door standaardisatie of beleidsbepaling voor offshore windparken.

De eerste aanbeveling is het organiseren van een mogelijke (ISAC) overlegstructuur/stuurgroep voor de wind op zee sector. De Nederlandse wind op zee sector is een complexe sector waarin veel verschillende partijen betrokken zijn. Deze partijen hebben allemaal hun eigen cybersecuritystrategieën. Door meer overleg en kennisdeling tussen deze partijen kunnen cybersecurity beter worden aangepakt en kan de sector beter worden beschermd tegen cyberaanvallen- en incidenten. Vanwege de grote variatie op verschillende niveaus binnen de sector wordt een structuur aanbevolen met een overkoepelende stuurgroep en thematische werkgroepen. Denk hierbij aan thematische werkgroep over Europese wet- en regelgeving voor ontwikkelaars van windparken. Bedrijven in de sector geven tevens aan behoefte te hebben aan meer concrete kennis (over onder andere wetgevingseisen). Een digitaal en interactief forum voor kennisdeling kan hieraan bijdragen.

De tweede aanbeveling is gericht op de essentiële constatering dat er meer coördinatie nodig is tussen verschillende overlegstructuren, zoals de Energie ISAC. Vanuit het speelveld aan stakeholders komt naar voren dat de waarborging van 'vertrouwensband' binnen cybersecurity overlegstructuren essentieel is, maar er tevens behoefte is aan minder versnippering en verzuiling. Concreet is veelal aangegeven dat er geen behoefte is aan een geïsoleerde losse ISAC voor de wind op zee sector. Er is vraag naar meer onderlinge verbinding en '*gelaagdheid*' tussen de bestaande en toekomstige overlegstructuren en dergelijke initiatieven. Hierbij moet ook aandacht zijn voor volwassenheidsverschillen op het gebied van cybersecurity. Onze aanbeveling luidt om dit te organiseren in samenhang met de Energie ISAC. Hierbij kan de Energie ISAC een centrale verbindende rol bieden.

Tot slot wordt de Nederlandse overheid geadviseerd om samen met de sector na te denken over concrete normen en eisen rondom cybersecurity, waarbij gefocust wordt op het creëren van een *level playing field*. Een logische optie hiervoor zouden kwalitatieve tendercriteria zijn voor nieuwe windparken op zee. Hierdoor kunnen potentiële aanbieders worden gestimuleerd om te investeren in passende hoogwaardige cybersecurity-oplossingen. Er zijn ook andere mogelijkheden zoals de opname van cybersecurity normen in de kavelbesluiten voor windparken of binnen (bestaande) wetgeving zoals de 'Wet windenergie op zee'.