Inbreng E-NL & Holland Solar CD Online Veiligheid en Cybersecurity

Op 5 februari staat het Commissiedebat Online Veiligheid en Cybersecurity op de agenda van de Commissie Digitale Zaken. De energiesector is als vitale sector dagelijks bezig met het versterken van de digitale weerbaarheid. Energie-Nederland en Holland Solar geven u daarom graag een aantal overwegingen en vragen mee voor het commissiedebat:

1. Zorg voor samenhang tussen de Cbw en de Netcode on Cybersecurity
2. Ga op tijd van start met het uitwerken van sectorale regelingen onder de Cyberbeveiligingswet
3. Zorg dat de conformiteit van gedistribueerde energieopwek met cyberbeveiligingsnormen onafhankelijk wordt aangetoond

Deze punten worden hieronder verder toegelicht:

1. Zorg voor samenhang tussen de Cbw en de Netcode on Cybersecurity
Het Nederlandse energiesysteem is een vitale sector. Uitval van het systeem kan enorme gevolgen hebben voor Nederland en indirect heel Europa. Het energiesysteem verandert bovendien snel met elektrificatie, digitalisering en snelle toename van lokale opwek d.m.v. zonne-energie en kleinschalige opslag. Als sector werken we hard aan de weerbaarheid van het energiesysteem. De Cyberbeveiligingswet (Cbw) is een goede stap om digitale dreigingen het hoofd te bieden. Het is voor bedrijven in de energiesector cruciaal om duidelijkheid te krijgen over de uitwerking van de Cbw, waaronder de omvangscriteria, zodat bedrijven gepaste investeringsbeslissingen kunnen nemen.

Naast de Cbw komt er voor de energiesector nog een belangrijke verandering die impact gaat hebben: de Netcode on Cybersecurity of Cross-Border Electricity Flows (NCCS). Deze NCCS is een van de codes die de lagere regelgeving vormen onder de Elektriciteitsverordening. De NCCS heeft als doel het verbeteren van cybersecurity van de grensoverschrijdende elektriciteitsvoorziening binnen de EU en het harmoniseren van regels tussen lidstaten. Essentieel is dat deze NCCS zo goed mogelijk aansluit op de Nederlandse Cyberbeveiligingswet en dat de administratieve lasten voor bedrijven die onder beide vallen zo beperkt mogelijk blijven. Essentieel is snelle en duidelijke communicatie van de deadlines uit deze NCCS, deze zijn momenteel zeer onduidelijk.

- *Vraag aan de minister: Kan de minister zo spoedig mogelijk duidelijkheid geven over de deadlines van de Netcode en borging van de samenhang met de Cyberbeveiligingswet?*

2. Ga op tijd van start met het uitwerken van sectorale regelingen onder de Cyberbeveiligingswet

Een groot aantal sectoren gaat onder de Cyberbeveiligingswet vallen. De zonne-energiesector, waar de meeste partijen eerder nog niet onder NIS1/ Wbni vielen, verwelkomt deze verbreding van de reikwijdte van cyberwetgeving omdat het aansluit bij de belangrijke rol die zonne-energie speelt in het energiesysteem. Elk van deze sectoren heeft eigen uitdagingen op het gebied van (cyber)beveiliging, zo heeft de energiesector te maken met de het sterk gedistribueerde karakter van zonne-energie en een grote focus op operationele technologie (OT) bij productielocaties. Niet al deze sectorspecifieke kenmerken zijn met een algemene wet af te dekken. Er zijn dus sectorspecifieke regelingen nodig voor enkele sectoren. Voor de energiesector is het belangrijk dat snel duidelijk is of zij onder een sectorspecifieke regeling gaan vallen en zo ja, wat deze regeling dan behelst.

- *Vraag aan de minister: Kan de minister aangeven op welke termijn er duidelijkheid wordt verwacht over eventuele sectorspecifieke regelingen onder de Cyberbeveiligingswet? En is er een specifieke regeling voor de energiesector gepland?*

3. Zorg dat de conformiteit van gedistribueerde energieopwek met cyberbeveiligingsnormen onafhankelijk wordt aangetoond

Duidelijke regels voor apparatuur die essentieel is voor lokale opwek van energie, onder andere zonne-energie, zijn cruciaal om een gelijk speelveld te creëren en zorg te dragen dat zowel lokale als meer grootschalige installaties veilig zijn. Bestaande wettelijke kaders zijn hier nog niet volledig op ingericht. Zo zijn onder de aankomende Europese Cyber Resilience Act omvormers ingedeeld in de categorie producten waarvoor een zelfevaluatie toereikend is om de markt op te kunnen, in plaats van een onafhankelijk onderzoek zoals dit voor ‘zwaardere’ categorieën geldt.

- *Vraag aan de minister: Is de minister bereid om zich op Europees niveau in te zetten voor beleid waarbij de conformiteit met cyberbeveiligingsnormen voor apparatuur voor decentrale energieopwekking, verplicht onafhankelijk moet worden aangetoond?*