AH 3699
2022Z13483

Antwoord van minister Jetten (Klimaat en Energie) (ontvangen 16 augustus 2022)

Zie ook Aanhangsel Handelingen, vergaderjaar 2021-2022, nr. 3440

1

Bent u bekend met de toename aan cyberaanvallen op windturbines op Europees grondgebied?[1]

Antwoord

Ja ik ben bekend met dit bericht.

2

Bent u ermee bekend dat als gevolg hiervan bijvoorbeeld vijf windturbines langs de Oude Maas al maandenlang stilstaan?[2]

Antwoord

Windpark Oude Maas is nog in aanbouw. In februari 2022 is er sprake geweest van stormschade, waardoor onderdelen op de locatie zijn beschadigd. In juli zijn twee windmolens gerepareerd. Deze stormschade staat los van de digitale aanval op de windmolenleverancier Nordex van april dit jaar. De andere drie windmolens konden niet proefdraaiden omdat Nordex problemen ervoer door een cyberaanval.

De digitale aanval op Nordex had betrekking op een IT-applicatie van de organisatie (kantoorautomatisering) en heeft geen impact gehad op de hardware die toegang heeft tot de besturing van de windmolens (continuïteit van de dienstverlening). Er is dus geen sprake van een directe succesvolle cyberaanval op windpark Oude Maas, Nordex is slechts een toeleverancier van het windpark.

---

[1] Techzine, 27 april 2022, «Europese windenergiesector getroffen door golf cyberaanvallen». (https://www.techzine.nl/nieuws/security/486216/europese-windenergiesector-getroffen-door-golf-cyberaanvallen/)

[2] Rijnmond, «What the hack! Hoe de oorlog in Oekraïne windmolens langs Oude Maas al maanden stil laat staan» (https://www.rijnmond.nl/nieuws/1512040/what-the-hack-hoe-de-oorlog-in-oekraine-windmolens-langs-oude-maas-al-maanden-stil-laat-staan)

3

Hoeveel (pogingen tot) cyberaanvallen op systemen en netwerken van Nederlandse windturbines zijn u bekend over het afgelopen jaar? Wie waren hiervoor verantwoordelijk?

4

In hoeveel gevallen waren deze cyberaanvallen succesvol en was er daadwerkelijk sprake van hacks door ransomware zoals bij het windpark Oude Maas?

5

Om welke beheerders en windparken ging dit?

6

Hoe is met deze hacks omgegaan? Zijn ze verholpen en zo ja, hoe?

7

Heeft de (Rijks)overheid hierin een rol gespeeld? Zo ja, welke?

8

Hoeveel voorziene energie is hierdoor in totaal niet opgewekt?

Antwoord 3 t/m 8

Er bestaat geen algeheel overzicht van (pogingen tot) cyberaanvallen op specifieke sectoren zoals windenergie.

Het Cybersecuritybeeld Nederland 2022 (CSBN 2022)[3] beschrijft in algemene zin dat de energietransitie verdere digitalisering stimuleert. Dit gaat gepaard met nieuwe risico's. Zowel statelijke actoren als criminelen maken misbruik van onze afhankelijkheid van digitale technologie. Deze risico's hebben de aandacht van het kabinet. Op dit moment wordt er onder coördinatie van de minister van Justitie en Veiligheid gewerkt aan een nieuwe Nederlandse Cybersecurity Strategie (NLCS) met

[3] Kamerstuk 26643, nr. 891

daarin een brede cybersecurityaanpak. Deze zal na de zomer aan de Kamer worden aangeboden.

Het ministerie van Economische Zaken en Klimaat is verantwoordelijk voor de vitale processen binnen de energiesector. Onderdeel hiervan is elektriciteitsproductie-, distributie en transport. De minister van Klimaat en Energie heeft zogenaamde Aanbieders van Essentiele Diensten (AED's) aangewezen onder de Wet beveiliging netwerk- en informatiesystemen (Wbni). AED's moeten voldoen aan de zorgplicht om hun netwerk- en informatiesystemen te beveiligen. Agentschap Telecom (AT) houdt toezicht op deze aanbieders.

Incidenten met aanzienlijke gevolgen voor de dienstverlening, moeten gemeld worden bij het AT en het Nationaal Cyber Security Centrum (NCSC). Ook kunnen deze AED's andere vrijwillige meldingen doen bij het AT en het NCSC. Het NCSC heeft als primaire taak om vitale aanbieders en Rijksoverheidsorganisaties in geval van dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen te informeren, te adviseren en indien nodig bijstand te verlenen.

Daarnaast wordt er nu gewerkt aan de *Netcode on Cybersecurity*. Dit is specifiek Europese regelgeving waarbij (in aanvulling op de Wbni) extra cybersecuritymaatregelen worden opgelegd aan entiteiten, die een risico kunnen vormen voor het Europese elektriciteitsnet.

Het staat bedrijven echter altijd vrij om voor vragen op het gebied van cybersecurity contact op de nemen met de Rijksoverheid. Ook kunnen vitale bedrijven of Rijksoverheid partijen contact opnemen met het NCSC en niet-vitale bedrijven met het Digital Trust Centrum (DTC). Daarnaast kunnen bedrijven aangifte doen bij de politie als zij te maken krijgen met cybercrime. Het kabinet roept slachtoffers van ransomware of andere vormen van cybercrime ook op om dit te doen.

9

In hoeverre kunt u volhouden dat uw inzet op windenergie ons minder afhankelijk maakt van het buitenland, terwijl u tegelijkertijd via Tennet grote offshore windprojecten gunt aan Chinese staatsbedrijven en uw windturbines vanuit het buitenland gewoon lamgelegd kunnen worden?

Antwoord

Het net op zee en de daarop aangesloten windparken op zee zijn aangewezen als vitale energie-infrastructuur. Toeleverende partijen voor zowel het net op zee als voor de windparken, dienen daarom te voldoen aan de voorwaarden die zijn

gesteld in de Nationale Veiligheidsstrategie 2019 en de actualisering daarvan, zoals de midterm review 2021. Deze bepaling is opgenomen in het ontwikkelkader windenergie op zee, waarmee ik TenneT formeel opdracht geef voor de aanleg van het net op zee, en wordt ook opgenomen in de toekomstige tenderregelingen voor de windparken.

Zoals aangegeven in de set Kamervragen betreffende het gunnen van een groot offshore windproject aan Chinese staatsbedrijven van d.d. 23 februari jl. (kenmerk 2022Z03467), heeft TenneT daarnaast op grond van de Elektriciteitswet 1998 de verplichting de veiligheid en betrouwbaarheid van de netten en van het transport van elektriciteit over de netten op de meest doelmatige wijze te waarborgen. Dit is een wettelijke taak van TenneT. In 2020 is er door het kabinet een nationale veiligheidsanalyse uitgevoerd. Dit heeft geresulteerd in een aantal aanbevelingen tot wijziging van de Elektriciteitswet 1998. Deze wijzigingen maken het mogelijk om nog beter rekening te houden met eisen ten aanzien van de nationale veiligheid. Zo zal het voor bepaalde gevoelige opdrachten mogelijk worden dat netbeheerders gebruik kunnen maken van de Aanbestedingswet Defensie en Veiligheid. Deze wijzigingen zijn meegenomen in de Energiewet die nu ter advisering ligt bij de Raad van State.