In het voorjaar van 2022 lagen drie Nederlandse windparken maandenlang stil door een cyberaanval bij hun buitenlandse toeleverancier. Hoe kunnen we onze stroomvoorziening beter beveiligen?

Tekst **Olaf Geurts**, **Cathérine Minczeles** en **Ron Broeders**

Fotografie **Marcel Berendsen**

3 tot 5 minuten leestijd

In het voorjaar van 2022 stonden de wieken van windpark Oude Maas in de gemeente Hoeksche Waard maandenlang stil. De molens waren zo goed als afgebouwd en hadden duurzame energie moeten leveren aan zo'n vierentwintigduizend huishoudens. Een cyberaanval bij de Duitse leverancier Nordex was de boosdoener. Twee andere windparken, Spuisluis in Velsen en Bommelerwaard in Zaltbommel, konden ook niet starten vanwege het incident in Duitsland.

De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) waarschuwt al langer voor de cyberrisico's van de energietransitie. In een rapport uit juni 2023 noemt de NCTV een verstoring van de energievoorziening een van de vier grote cyberrisico's voor de nationale veiligheid. Zowel landen als criminelen kunnen met hacks windturbines saboteren. Alle zorgen ten spijt: het blijkt dat het toezicht op de cyberveiligheid van onze windmolens vaak in buitenlandse handen is. Momenteel is zo'n 82 procent van alle windturbines op land afkomstig van een fabrikant die sinds 2021 te maken kreeg met cyberincidenten, namelijk Vestas, Enercon of Nordex. Dat blijkt uit onderzoek dat Small Stream Media en The Investigative Desk uitvoerden.

EEN PATROON

Terug naar het incident op 31 maart 2022: hackers vergrendelden het computernetwerk van de Duitse windturbinebouwer Nordex. Ze eisten losgeld voor de toegang. Uit voorzorg schakelde het bedrijf verschillende IT-systemen uit om schade aan de windparken onder hun beheer te voorkomen. Hierdoor werden de Nederlandse windparken in aanbouw Oude Maas, Spuisluis en Bommelerwaard slachtoffer van de hack bij hun toeleverancier. Nordex kon de laatste software-updates niet versturen om de molens te laten draaien. 'Dit heeft de BV Nederland groene energie gekost,' vertelt Ronald Kloet, directeur van Renewable Factory en mede-eigenaar van windpark Oude Maas. 'En ons een centje.' De schade voor het bedrijf bedroeg enkele tonnen.

Nu waren de windturbines geen doelwit, maar in het ergste scenario ontstaat in heel Europa een stroomstoring wanneer hackers deze aantallen turbines in één keer platleggen.

t van een cyberaanval. Het Duitse Enercon liep nevenschade op na een Russische cyberaanval op een communicatiesatelliet als onderdeel van de invasie in Oekraïne. Hierdoor verloor het bedrijf de verbinding met 5.800 windturbines. Nu waren de windturbines geen doelwit, maar in het ergste scenario ontstaat in heel Europa een stroomstoring wanneer hackers deze aantallen turbines in één keer platleggen.

AFHANKELIJKHEID

Nederland is voor zo'n 4,2 procent afhankelijk van windenergie. Dit percentage zal alleen maar toenemen om zo de Nederlandse klimaatdoelen in 2030 te behalen. En de cyberincidenten bij windturbinefabrikanten in Denemarken en Duitsland laten zien: het organiseren van de cyberveiligheid van windmolens overschrijdt al gauw de landsgrenzen. Zo kunnen Nederlandse energiebedrijven die eigenaar van windparken zijn, hun cyberveiligheid wel goed op orde hebben, zoals Eneco of Pure Energie. Maar zij zijn ook afhankelijk van toeleveranciers uit het buitenland die op afstand toegang blijven houden tot de turbines.

Op basis van Europese spelregels stelt de Nederlandse cyberwetgeving dat Nederlandse partijen binnen het elektriciteitsnetwerk hun netwerk- en informatiesystemen veilig moeten houden. In Nederland controleert de Rijksdienst Digitale Infrastructuur sinds 2021 of energieproducenten zich hieraan houden. Grote cyberincidenten moeten hier gemeld worden, maar omdat de windparken Oude Maas, Spuisluis en Bommelerwaard ten tijde van de bovenbeschreven hack nog in aanbouw waren en de gevolgen beperkt bleven, hoefden de exploitanten niet aan de bel te trekken. Verder staat het hoofdkantoor van Nordex in Duitsland, waardoor het onder Duits toezicht valt, niet onder het Nederlandse. De meldplicht voor het incident ligt eveneens in Duitsland.

ZORGPLICHT

Uit het onderzoek van Small Stream Media en The Investigative Desk blijkt dat gemeenten en provincies geen rol hebben in het waarborgen van de cyberveiligheid van windmolens. Gek, want ze buigen zich bij het toekennen van vergunningen wel over slagschaduw, geluidsoverlast, veiligheid voor vogels en de mogelijkheid van het afbreken van wieken. Volgens Willem Bantema, lector bestuur en digitalisering aan de NHL Stenden Hogeschool, moet dat anders. 'Gemeenten hebben een zorgplicht.'

Uit onderzoek naar de vergunningen van acht windparken blijkt dat digitale veiligheid niet één keer wordt genoemd. Na meerdere cyberincidenten bij windturbineleveranciers, zijn in de onderzochte gemeenteraden en provinciale staten geen vragen gesteld.

> 'Een cyberincident kan fysieke gevolgen hebben. Nu vallen bedreigingen buiten het zicht van veiligheidsregio's en provincies, terwijl zij de politie en brandweer aansturen.'

Bantema vindt dat alle overheden een verantwoordelijkheid hebben bij het versterken van de cyberveiligheid van windparken. Maar, zo legt hij uit, dan moeten provincies en gemeenten wel de juiste bevoegdheden krijgen. 'Zo kan veel ellende mogelijk vooraf voorkomen worden.'

de politie en brandweer aansturen.’

SERIEUS NEMEN

Niet alle deskundigen zijn het met Bantema en Van der Ham eens. Volgens Michel van Eeten, hoogleraar bestuurskunde en cybersecurity aan de TU Delft, is het logischer dat de verantwoordelijkheid bij de koper van de windmolens blijft liggen. ‘Als windmolens worden gehackt en stilstaan, dan kost het de eigenaren geld. Zij hebben er dus belang bij om na te gaan of de fabrikant de beveiliging goed op orde heeft.’

Roland van Rijswijk-Deij, hoogleraar netwerkbeveiliging aan de Universiteit Twente, denkt er ook zo over. Het is niet de verantwoordelijkheid van gemeenten en provincies: ‘Ze hebben hier geen cybersecurityspecialisten voor in huis en bovendien hebben ze al zoveel taken.’

Over één ding zijn alle experts het eens: de dreiging moet serieus worden genomen. Energie is tenslotte een primaire levensbehoefte. Van Rijswijk-Deij vindt het naïef om te denken dat landen windturbines niet aanvallen. ‘Cybersecurity is nu extra belangrijk.’

Dit artikel is een samenwerking tussen The Investigative Desk, Small Stream Media en de onderzoeksredactie AD Regionaal als onderdeel van het GGG-project over het handelen van gemeenteraden. Een project dat het stemgedrag van politieke partijen in de Nederlandse gemeenten inzichtelijk maakt, om het voor journalisten makkelijker te maken het politieke handelen bij regio-overschrijdende beslissingen te vergelijken

WANNEER GAAT HET LICHT UIT?

Wat er precies nodig is om het Nederlandse elektriciteitsnetwerk via duurzame stroom te destabiliseren is onbekend. Gebeurtenissen in Europa in januari 2021 geven enig inzicht. Toen ging het licht bijna uit doordat het Europese elektriciteitsnetwerk op een haar na crashte. Dit kwam door een samenloop van omstandigheden. Het was warm op de Balkan, waar massaal het Orthodoxe Kerstfeest werd gevierd. Hierdoor was de vraag naar elektriciteit lager dan gebruikelijk omdat veel bedrijven dicht waren. In Centraal- en Noordwest-Europa was het op dat moment juist kouder dan normaal, waardoor er extra vraag naar elektriciteit was. Het verschil in vraag en aanbod leidde volgens de Europese netbeheerder ENTSO-E tot een domino-effect, met een disbalans op het Europese netwerk tot gevolg. Splitsing van het Europese netwerk was de enige oplossing om een crash te voorkomen. Dat lukte. Hoewel het hier niet om een hack ging, laat het incident zien dat slechts een verschil van 5,8 gigawatt in vraag en aanbod van energie nodig is om een disbalans op het net te veroorzaken met als gevolg een bijna stroomuitval in Europa. Dat is ongeveer evenveel vermogen als alle

ruim een veelvoud van dit vermogen. Cyberincidenten bij een van deze leveranciers kunnen dus gevolgen hebben die veel verder gaan dan de lokale energievoorziening. De waarschijnlijkheid van zo'n scenario is gering, maar niet ondenkbaar.