Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

**26 643** **Informatie- en communicatietechnologie (ICT)**

**29 023** **Voorzienings- en leveringszekerheid energie**

**Nr. 1038**

## BRIEF VAN DE MINISTER VAN ECONOMISCHE ZAKEN EN KLIMAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 16 juni 2023

Op verzoek van de vaste commissie voor Digitale Zaken van 7 juni 2023 stuur ik u hierbij, mede namens de Minister voor Klimaat en Energie, het rapport «Onderzoek storingsproblematiek en cyberveiligheid omvormers voor zonnepanelen» van de Rijksinspectie Digitale Infrastructuur (RDI) toe, inclusief een kabinetsreactie in deze brief.[1]

De RDI heeft op 30 mei 2023 met dit rapport de uitkomst gepubliceerd van het onderzoek naar omvormers van zonnepaneelinstallaties. Omvormers zetten de energie afgegeven door de zonnepanelen om in elektriciteit die bruikbaar is voor het elektriciteitsnet. Elektrische apparaten als deze kunnen stoorsignalen uitzenden en dienen daarom te voldoen aan eisen ter voorkoming van storingen bij andere draadloze apparaten en communicatienetwerken, zoals vastgelegd in de EMC-richtlijn (2014/30/EU)[2] en de radioapparatuurrichtlijn (2014/53/EU). Ook wordt hierin geregeld dat de functionaliteit van deze apparaten niet negatief beïnvloed mag worden door elektromagnetische velden, zoals rond zendinstallaties. Daar komen medio 2024 eisen bij onder de radioapparatuurrichtlijn voor de cybersecurity van draadloos verbonden apparaten.[3]

De RDI is dit onderzoek in 2021 gestart vanwege een toename van het aantal meldingen van storingen bij zonnepanelen, die voort bleken te komen uit storende apparatuur of onjuiste installaties. De RDI heeft in het onderzoek vastgesteld dat zonnepaneelinstallaties veelal niet voldoen aan de huidige eisen voor het voorkomen van storingen. Daarnaast heeft de RDI de apparaten getoetst aan de toekomstige cybersecurity-eisen, om

[1] Onderzoek storingsproblematiek en cyberveiligheid omvormers voor zonnepanelen | Rapport | Rijksinspectie Digitale Infrastructuur (RDI).
[2] EMC is een afkorting voor elektromagnetische compatibiliteit.
[3] Doordat het benodigde standaardisatieproces langer duurt dan voorzien, stelt de Europese Commissie voor deze datum op te schuiven naar 1 augustus 2025. Hiertoe bestaat draagvlak onder EU lidstaten.

kst-26643-1038
ISSN 0921 - 7371
's-Gravenhage 2023

zowel fabrikanten als de eigen organisatie in de rol van toezichthouder hierop voor te bereiden.

*Storingseisen*

In het onderzoek van de RDI bleek een aanzienlijk deel (5 van de 9) van de onderzochte omvormers niet aan de eisen te voldoen: door deze apparaten werd te veel storing veroorzaakt. Met het op de markt brengen van non-conforme omvormers en accessoires overtreden fabrikanten de Telecommunicatiewet. De betreffende fabrikanten zijn door de RDI in individuele gesprekken gewezen op de geconstateerde overtreding(en) en hun wettelijke verplichtingen. Naar aanleiding van dit onderzoek hebben deze fabrikanten een waarschuwing ontvangen voor deze overtredingen. Er zijn op dit moment geen boetes opgelegd of andere maatregelen genomen, omdat de fabrikanten voldoende bereid waren om passende maatregelen te nemen. De RDI zal op een later moment hercontroles uitoefenen om hier op toe te zien en treedt dan handhavend op bij overtredingen.

*Cybersecurity*

Het rapport maakt daarnaast duidelijk dat het met de cybersecurity van veel zonne-energieomvormers slecht gesteld is. Op het gebied van de toekomstige cybersecurity en de administratieve wettelijke eisen voldeed geen van de onderzochte omvormers. De RDI wijst daarbij op het gevaar van een slechte beveiliging van omvormers, waardoor een groot deel van de zonnepaneelinstallaties gehackt zou kunnen worden. Daarmee zouden ze op afstand uitgeschakeld kunnen worden door onbevoegden. De RDI wijst terecht op de mogelijke risico's voor het elektriciteitsnetwerk als dat massaal gebeurt, en de noodzaak om hier – in afwachting van de verplichte eisen – nu al naar te handelen. Ook hierover is de RDI in gesprek met fabrikanten.

*Kabinetsreactie*

De veiligheid van digitale producten en diensten vormt een van de vier pijlers in de Nederlandse Cybersecurity Strategie[4]. Het is dan ook een speerpunt van het kabinet om in Europa wetgeving hierover vast te stellen die fabrikanten verplicht de cybersecurity van hun product goed te regelen. Het RDI-rapport toont aan waarom het zo belangrijk is dat deze cybersecurityeisen er komen. De cybersecurityeisen voor draadloos verbonden apparaten onder de radioapparatuurrichtlijn worden in de nabije toekomst van kracht. Nederland heeft zich hiervoor hard gemaakt in de EU als eerste belangrijke stap. De Cyber Resilience Act gaat straks een stap verder en zal cybersecurityeisen stellen aan alle hard- en software die in de Europese Unie op de interne markt wordt gebracht. De cybersecurityeisen onder de radioapparatuurrichtlijn en die onder Cyber Resilience Act zullen dan in principe samengaan in een gemeenschappelijk kader om overlap van regels te voorkomen. Een van de eisen waar draadloos verbonden apparaten zoals de onderzochte omvormers aan zullen moeten voldoen, heeft betrekking op de authenticatie: de controle of degene die inlogt op een apparaat wel degene is die daartoe bevoegd is. Dat een groot aantal apparaten op afstand gelijktijdig zou kunnen worden gehackt, het scenario waar de RDI voor waarschuwt, komt onder andere door het gebruik van standaardwachtwoorden die niet uniek zijn. Het aanbieden van draadloos verbonden apparaten die niet voorzien zijn van unieke standaardwachtwoorden zal onder de nieuwe cybersecurity-eisen niet langer zijn toegestaan.

[4] Kamerstuk 26 643, nr. 925.

Als gevolg van de herziening van de netwerk- en informatiebeveiligingsrichtlijn (NIB-2) zullen meer zonnepaneelbedrijven dan nu in de toekomst moeten voldoen aan wettelijke verplichtingen voor cybersecurity. Deze verplichtingen bestaan uit een meldplicht voor incidenten en een zorgplicht om risico's voor de continuïteit van de dienstverlening te beperken. Hierbij dient ook rekening gehouden te worden met risico's die afkomstig zijn van leveranciers. Daarnaast zal de Europese verordening over grensoverschrijdende cybersecurity in de elektriciteitssector (Netcode) zorgen voor hogere cybersecurity-eisen aan grootschalig aan te sturen omvormers. De Netcode bevat bindende voorschriften voor cybersecurity die worden opgelegd aan entiteiten die, wanneer zij mikpunt zouden worden van een cyberaanval, een risico vormen voor de stabiliteit van het Europese elektriciteitsnet. De Netcode bouwt voort op de cybersecurity-eisen van de radioapparatuurrichtlijn en de implementatie van de betreffende standaarden, en zal naar verwachting eind 2023 in werking treden.

Voor een robuuste en duurzame energietransitie is niet-storende en cyberveilige apparatuur essentieel. Voorkomen moet worden dat met de verdere energietransitie storingsvrij frequentiegebruik ernstig wordt belemmerd en dat de leveringszekerheid van energie in de toekomst op het spel komt te staan. Bij het toepassen van de betreffende eisen zijn ook gelijke concurrentievoorwaarden van belang. Het toezicht van de RDI draagt bij aan het realiseren van deze voorwaarden voor een succesvolle energietransitie. Gezien de huidige situatie in deze sector is het nu al van belang dat fabrikanten, importeurs en installateurs hun verantwoordelijkheid nemen en hun producten en ondersteuning aanpassen om digitale kwetsbaarheden te verminderen. In afwachting van de genoemde verplichtingen voert de RDI daarom gesprekken met deze partijen om vrijwillig invulling te geven aan de betreffende eisen. Zo kunnen installateurs bijdragen door bij installaties gebruikers voor te lichten en hulp te bieden bij beveiligingshandelingen die gebruikers zelf kunnen uitvoeren. Tot slot blijft het kabinet inzetten op bewustwordingscampagnes gericht op gebruikers van met het internet verbonden apparaten. De publiekscampagne «Doe je updates» is hier een voorbeeld van. Daarmee wordt de kans op grootschalige hacks van zonnepanelen in de nabije toekomst naar verwachting kleiner.

De Minister van Economische Zaken en Klimaat,
M.A.M. Adriaansens