Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

147

Vragen van het lid **Erkens** (VVD) aan de Minister van Klimaat en Groene Groei over *het artikel «TenneT wil regels zien voor apps voor zonnepanelen en waarschuwt voor black-outs»* (ingezonden 23 augustus 2024).

Antwoord van Minister **Hermans** (Klimaat en Groene Groei), mede namens de Ministers van Justitie en Veiligheid en van Economische Zaken (ontvangen 2 oktober 2024). Zie ook Aanhangsel Handelingen, vergaderjaar 2023–2024, nr. 2498.

Vraag 1
Bent u bekend met het artikel «TenneT wil regels zien voor apps voor zonnepanelen en waarschuwt voor black-outs»?[1] Hoe apprecieert u dit?

Antwoord 1
Ja. Digitalisering is noodzakelijk om de doelen van de energietransitie te halen. Deze digitalisering brengt echter ook risico's met zich mee. Het kabinet herkent een aantal van de genoemde kwetsbaarheden en daarom werkt het kabinet aan de versterking van de weerbaarheid van de (vitale) energiesector, inclusief installaties voor het opwekken van elektriciteit door middel van zon. Binnenkort wordt nieuwe regelgeving van kracht waarmee er oplossingen komen voor de in het artikel benoemde kwetsbaarheden.

Vraag 2
Welke regels op het gebied van IT-veiligheid gelden er voor fabrikanten van apps en sites voor het beheren van zonnepanelen? Klopt het dat zich hier grote kwetsbaarheden voordoen? Zo ja, welke?

Antwoord 2
Er gelden op dit moment strenge veiligheidseisen voor elektrische materialen. Deze eisen zijn onder meer opgenomen in de laagspanningsrichtlijn 2014/35/EU. Deze laagspanningsrichtlijn is in de Nederlandse wetgeving opgenomen in het warenwetbesluit elektrisch materiaal.
Voor IT-veiligheid zijn extra regels nodig. Vanaf 1 augustus 2025 zijn er veiligheidseisen op grond van de herziene radioapparaten-richtlijn (of Radio Equipment Directive, RED) van kracht. Dit betreft cybersecurity eisen voor draadloos verbonden apparatuur, waaronder zonnepaneelomvormers.

[1] BNR, 20 augustus 2024

ah-tk-20242025-147
ISSN 0921 - 7398
's-Gravenhage 2024

Daarnaast wordt naar verwachting vanaf eind 2027 de Europese verordening cyberweerbaarheid (of Cyber Resilience Act, CRA) van kracht. De CRA is breder dan de RED en geldt niet alleen voor draadloze apparaten, maar voor alle producten met digitale elementen.
In aanloop naar de inwerkingtreding van deze regels, is het van belang dat iedereen in de keten van zonne-energie (fabrikanten, installateurs, verkopers, gemachtigden, importeurs en ook consumenten en bedrijven met zon PV installaties) aan de slag gaat met het nemen van (preventieve) maatregelen ten behoeve van het minimaliseren van digitale kwetsbaarheden. De consument, de installateur en de fabrikant hebben een eigen verantwoordelijkheid om de zonnestroominstallaties te allen tijde goed te beveiligen met sterke wachtwoorden en door regelmatig updates uit te voeren.
Er zijn momenteel inderdaad kwetsbaarheden. De oorzaak hiervan ligt vooral bij slechte beveiliging van omvormers door het gebruik van standaard wachtwoorden die niet uniek zijn en het niet op tijd updaten van hardware.[2] Daarnaast zorgen niet alle fabrikanten van omvormers tijdig voor software-updates om de omvormers veilig te kunnen houden. Omvormers zijn de schakel tussen de opgewekte stroom van de zonnepanelen en het lokale stroomnet. Doordat omvormers aan het internet zijn gekoppeld, kunnen meerdere omvormers gelijktijdig worden gehackt of op een ongewenste manier worden aangestuurd. Daardoor kunnen aanvallen gedaan worden die schaalbaar zijn, waarbij het in theorie bij zeer grote aantallen apparaten fout kan gaan.[3] De kans dat dit gebeurt achten wij echter zeer klein. Gelijktijdige toegang tot grote aantallen apparaten is niet waarschijnlijk.
Zodra de CRA van kracht is en de essentiële cybersecurity eisen op grond van de RED 3.3 D,E en F van toepassing zijn, worden fabrikanten verplicht om hun producten digitaal veilig te maken en houden. Zo zal het niet meer toegestaan zijn om standaard wachtwoorden te gebruiken; ieder apparaat krijgt een uniek wachtwoord. Fabrikanten worden daarnaast verplicht om kwetsbaarheden in de software van het product tijdig op te lossen en te melden.

Vraag 3
Hoe verhoudt de wet- en regelgeving voor fabrikanten van apps en sites voor het beheren van zonnepanelen op het gebied van IT-veiligheid zich tot de wet- en regelgeving op dit gebied die geldt voor andere energiebedrijven? Waarom gelden er voor deze bedrijven verschillende regels op het gebied van IT-veiligheid?

Antwoord 3
Er is wet- en regelgeving voor de fabrikanten gericht op de veiligheid van hun producten met digitale elementen en er is wet- en regelgeving voor energiebedrijven gericht op het verhogen van hun digitale weerbaarheid. De gebruikers van de zonne-omvormers kiezen zelf welke producten zij aanschaffen. De energiebedrijven hebben daar maar beperkt invloed op. Daarmee vullen deze regels voor productveiligheid en weerbaarheid van de bedrijven elkaar aan. Hiermee wordt de cyberbeveiliging op verschillende niveaus in de keten versterkt om de cyberweerbaarheid van de gehele keten te verhogen.
Bij vraag 2 is een toelichting gegeven op de regelgeving voor fabrikanten van digitale producten. Voor energiebedrijven, die zijn aangewezen als aanbieder van een essentiële dienst (AED), geldt de Wet beveiliging netwerk- en informatiesystemen (Wbni), waarin de Europese netwerk- en informatiebeveiligingsrichtlijn (NIS1-richtlijn) is geïmplementeerd. Deze wet beoogt de digitale weerbaarheid van Nederland te versterken en heeft als doel de gevolgen van cyberincidenten te beperken om maatschappelijke ontwrichting te voorkomen. Daartoe bevat de Wbni onder meer voor AED's de plicht om passende en evenredige beveiligingsmaatregelen met betrekking tot hun netwerk- en informatiesystemen te nemen én de plicht om ernstige cyberincidenten te melden. Er wordt momenteel gewerkt aan de implementatie van de nieuwe Europese netwerk- en informatiebeveiligingsrichtlijn (NIS2-richtlijn) in de Cyberbeveiligingswet (Cbw). Die wet, met daarin onder meer een

[2] Kamerstuk 26 643, nr. 1038
[3] https://topsectorenergie.nl/documents/1241/2024-Secura-Publicatieversie-Scenarios_en_Maatregelen_Cyberweerbare_Zonnestroo_vqXh809.pdf.

uitgebreidere regeling van de zorg- en meldplicht voor bedrijven, zal naar verwachting in het najaar van 2025 in werking treden. Op 13 juni 2024 is ook de wetgeving over grensoverschrijdende cybersecurity in de elektriciteitssector (Netcode) in werking getreden. Deze regelgeving richt zich op bedrijven die impact kunnen hebben op grensoverschrijdende elektriciteitsstromen en heeft als doel het verhogen van de digitale weerbaarheid van het Europese elektriciteitssysteem. Deze wet- en regelgeving richt zich op de bedrijfscontinuïteit en de continuïteit van dienstverlening van genoemde bedrijven. Bedrijven moeten op basis hiervan maatregelen treffen voor de beveiliging van hun netwerk- en informatiesystemen, ze moeten significante cyberincidenten melden, en ze ontvangen bijstand bij digitale dreigingen of incidenten door het NCSC.

Vraag 4
Klopt het dat indien een beheerder van zonnepanelen wordt gehackt dit een risico op een black-out voor een substantieel deel van Europa met zich meebrengt? Hoe vergaand zouden de gevolgen hiervan zijn?

Antwoord 4
De kans dat een dergelijk risico zich voordoet is zeer klein. Er moet een zeer groot aantal zonnepanelen gelijktijdig uitvallen voordat dit risico zich voordoet. Het Europese elektriciteitssysteem is zo ingericht dat de uitval van een bepaalde omvang kan worden opgevangen. In het uiterste geval dat zich een black-out voordoet, dan betekent dit dat er in een deel van het elektriciteitssysteem geen elektriciteit beschikbaar is. Hoe verregaand de gevolgen hiervan zijn ligt aan meerdere omstandigheden. Denk aan het totaal beschikbare vermogen van de getroffen partij(en), de kenmerken, de timing en daarbij ook de (internationale) belastbaarheid op het elektriciteitsnet. De landelijke netbeheerder TenneT heeft, in directe samenwerking met buurlanden, herstelprocedures voor het geval een dergelijke situatie zich voordoet. Deze procedures worden regelmatig in een internationaal samenwerkingsverband geoefend.

Vraag 5
Hoe apprecieert u in dit kader het feit dat Nederlandse hackers de afgelopen twee jaar drie keer zijn binnengedrongen tot de software van dergelijke beheerbedrijven?

Antwoord 5
Het kabinet vindt dit zorgelijk. Dit onderstreept de noodzaak voor de bovenbedoelde wet- en regelgeving die binnenkort van kracht wordt. Het is belangrijk dat er meer aandacht komt voor de cyberveiligheid van deze internationaal opererende beheerbedrijven.

Vraag 6
Deelt u de mening dat er snel betere wet- en regelgeving op het gebied van IT-veiligheid nodig is voor fabrikanten van online controlepanelen? Welke acties kunt u ondernemen?

Antwoord 6
Ja. Er is regelgeving maar er zijn aanvullingen nodig, de ontwikkelingen op dit terrein volgen elkaar in snel tempo op. Het is zaak om regelgeving te maken die inspeelt op de actuele ontwikkelingen. Het is van belang dat de (implementatie van de) nieuwe Europese wet- en regelgeving op het gebied van digitale weerbaarheid snel van kracht wordt.
De Rijksinspectie Digitale Infrastructuur (RDI) bereidt zich als toezichthouder grondig voor op de komende regelgeving. De RDI voert gesprekken met fabrikanten, installateurs, verkopers en importeurs en onderzoekt ook nu al op kleine schaal de cyberveiligheid van deze apparaten, zoals het eerder genoemde rapport uit 2023. De RDI heeft dit onderzoek uitgevoerd vooruitlopend op de komst van bovengenoemde cybersecurityeisen, om fabrikanten en leveranciers erop te wijzen dat zij zich moeten voorbereiden op de nieuwe eisen. Naar aanleiding van dit rapport hebben sectorpartijen, waaronder omvormerfabrikanten, al stappen ondernomen om hogere veiligheidseisen en standaarden te hanteren.

In de Gedragscode Zon op Woningen heeft de sector afspraken gemaakt over het veilig installeren van residentiele systemen. Volgens deze gedragscode zal de installateur de omvormer instellen met een sterk en per installatie uniek wachtwoord voor de onderhoudsinstellingen van de omvormer.
Het kabinet zet ook in op het vergroten van bewustzijn, zoals in de overheids-campagne «Doe je updates», waarin een oproep wordt gedaan om slimme apparaten in huis direct te updaten. Verder werkt het kabinet aan proactieve informatieverstrekking over de komende wet -en regelgeving, zodat de partijen en fabrikanten zich alvast kunnen voorbereiden.

Vraag 7
Loopt Nederland risico doordat andere Europese landen onvoldoende wet- en regelgeving op het gebied van IT-veiligheid hebben voor fabrikanten van apps en sites voor het beheren van zonnepanelen? Zo ja, wat gaat u doen om dit te verbeteren?

Antwoord 7
Vanwege het Europese karakter van het elektriciteitssysteem is er een Europese aanpak om cyberveiligheid te versterken. Deze Europese aanpak is juist gericht op harmonisatie van wet- en regelgeving voor cybersecurity, onder andere ten behoeve van de energiesector. Het kabinet verwacht daarom niet dat Nederland risico loopt doordat andere Europese landen onvoldoende wet- en regelgeving hebben op het gebied van cyber veiligheid.