SCHRIFTELIJKE VRAAG

nr. 61
van **ROBRECHT BOTHUYNE**
datum: 17 oktober 2023

---

aan **ZUHAL DEMIR**
VLAAMS MINISTER VAN JUSTITIE EN HANDHAVING, OMGEVING, ENERGIE EN TOERISME

Zonnepanelen - Cybersecurity

Bij het installeren van zonnepanelen is een omvormer een noodzaak om zonne-energie om te zetten in elektriciteit. Deze omvormers zijn in de meeste gevallen verbonden met het internet om zo de eigenaar/gebruiker van die zonnepanelen de mogelijkheid te geven deze te monitoren.

Nu waarschuwt de Rijksinspectie Digitale Infrastructuur, de Nederlandse communicatieregulator, dat die manier van werken hacking kan bevorderen. De omvormers voldoen namelijk niet aan de normen van cyberbeveiliging waardoor hackers vanop afstand de zonnepanelen kunnen uitschakelen of meer nog, persoonsgegevens kunnen opnemen. Tevens zouden de omvormers storingen kunnen veroorzaken. Dat kan leiden tot het van op afstand openen van deuren enzovoort. Fabrikanten van omvormers in Nederland zijn vanaf augustus volgend jaar verplicht om te voldoen aan de eisen van cyberveiligheid.

In antwoord op mijn vraag om uitleg hierover in juni van dit jaar gaf de minister aan dat het Flexibiliteitsplan 2025 voorziet in een actie om cybersecurity en privacy in de energiesector hoog op de agenda te plaatsen.

Het Vlaams Energie- en Klimaatagentschap (VEKA) zou in overleg gaan met Beltug (Belgian association of CIOs and digital technology leaders), met Cyber Security Coalition en de relevante departementen binnen de Vlaamse overheid om een beeld te krijgen van de lopende initiatieven, waarbij het VEKA zich kan aansluiten of waar het VEKA bewustvorming rond kan creëren. De minister zou hen ook vragen om te bekijken hoe de aanbevelingen breed opengezet kunnen worden voor de zonnepaneleneigenaars.

Last but not least maakte ik de suggestie om bij de aanmelding van de installatie, via communicatie, Fluvius, te wijzen op de risico's en op de good practices van bijvoorbeeld het wijzigen van het wachtwoord. De minister vond dat een meerwaarde.

1. Inzake het VEKA en zijn overlegronde:
   a) Hoever staat het VEKA daarmee?
   b) Werden al resultaten geboekt?
      Zo ja, welke?
      Zo niet, wanneer is deadline?
   c) Welke aanbevelingen zal het VEKA doen?

2. Hoever staat Fluvius om, binnen de aanmeldingsprocedure, de eigenaars van zonnepanelen te infomeren/erop te wijzen de privacy en security goed in te stellen? Welke aanbevelingen geven zij aan die eigenaars?
3. Zijn er al ervaringen met hacking via omvormers gemeld in Vlaanderen? Zo ja,
    a) Wat was de top 3 van vormen van hacking?
    b) Op welke manier werden deze aangepakt?
    c) Welke lessen kan men daaruit trekken?
    d) In welke provincie werden die meldingen gedaan?
4. Op welke manier kan en zal men deze vorm van hacking counteren?
5. Welke algemene informatiecampagne zal men opzetten om Vlaamse zonnepaneleneigenaars attent te maken op deze vorm van hacking en van de mogelijkheden om die te counteren?
6. Zal men hier, zoals in Nederland, de fabrikanten normen tot cyberveiligheid opleggen? Welke normen en binnen welke timing?
7. Zal er, net zoals voor groepsaankopen, een kwaliteitscharter ontwikkeld worden zodat gegarandeerd kan worden dat de kwaliteit van de installaties en de omvormers tip top is? Waarom niet? indien wel, wanneer en onder welke vorm mogen we dit verwachten?

ZUHAL DEMIR
VLAAMS MINISTER VAN JUSTITIE EN HANDHAVING, OMGEVING, ENERGIE EN TOERISME

ANTWOORD
op vraag nr. 61 van 17 oktober 2023
van **ROBRECHT BOTHUYNE**

---

1. Het Flexibiliteitsplan 2025 voorziet inderdaad in een actie om cybersecurity en privacy in de energiesector hoger op de agenda te plaatsen. De verschillende acties van het Flexibiliteitsplan, dat nog loopt tot 2025, worden door de trekkers van elke actie op een gefaseerde wijze uitgevoerd. Momenteel focust het Vlaams Energie- en Klimaatagentschap (VEKA) zich hoofdzakelijk op andere acties van dit plan. Van zodra deze acties verder zijn gevorderd, zal het agentschap concrete stappen kunnen ondernomen met betrekking tot deze specifieke actie van het Flexibiliteitsplan 2025.

2. In juni heeft Fluvius aan mijn kabinet hun bezorgdheid overgemaakt over het toevoegen van extra informatie tijdens de aanmeldingsprocedure. Op dat moment dreigt de info over cybersecurity namelijk verloren te gaan tussen de veelheid aan info die de klant op dat moment ontvangt. De aanmeldingsbevestiging bevat immers al info over de verplichte plaatsing van een digitale meter, over de mogelijkheid om een premie aan te vragen en het feit dat leveranciers op hun afrekening pas rekening kunnen houden met een PV-installatie na de verwerking van de aanmelding van de installatie.
   In overleg met Fluvius geef ik er dan ook de voorkeur aan om een link op hun website te plaatsen naar de webpagina van de Vlaamse Overheid over zonnepanelen met informatie over het risico op hacking. Fluvius doet hiervoor momenteel het nodige. Eens deze werkzaamheden zijn afgerond, zal hierover ook een nieuwsitem worden opgenomen in de nieuwsbrief van Fluvius richting installateurs.

3. Er zijn mij en de sector (ODE, Techlink en Fluvius) geen rapporteringen bekend over dergelijke gegevens in de sector. Uit een contact met een expert van één van de grootste leveranciers van omvormers blijkt het volgende:
   a) Er zijn geen incidenten gekend die zich voorgedaan hebben bij particulieren. Wel worden meldingen gemaakt van zogeheten ethische hackers; dit zijn experten in security die op zoek zijn naar zogeheten 'zero day exploits'[1].
   b) Producenten van omvormers beschikken over een securityteam dat waakt over de cybersecurity. Dit van zowel de interne IT-systemen van de producent, als van de meldingen van ethische hackers.
      Deze meldingen worden publiek gemaakt en een bijhorend risicoprofiel wordt opgemaakt. Nadien wordt een gevalideerde oplossing toegepast. In de praktijk moeten namelijk meerdere dergelijke 'zero day exploits' gecombineerd worden om een kwaadwillige persoon toegang met beheersrechten te verlenen op afstand. De meeste exploits hangen af van de beschikbaarheid van wachtwoorden van eindgebruikers, die bijvoorbeeld door social engineering[2] verkregen worden.
   c) Er bestaat al een kader voor cybersecurity in de markt. Dit heeft geresulteerd in de nodige cybersecurity-vereisten. Voorbeeld is de IEEE 1547 standaard met criteria voor interconnectie van gedistribueerde energiebronnen binnen elektriciteitssystemen die de nodige cybersecurity vereisten bevat. Daarnaast zijn

---

[1] Een zero-day exploit is een computeraanval waarbij wordt gepoogd misbruik te maken van een zwakke plek in software die nog onbekend is bij de software-ontwikkelaar.
[2] Social engineering is een techniek waarbij een computerkraker een aanval op computersystemen tracht te ondernemen door de zwakste schakel in de computerbeveiliging, namelijk de mens, te kraken.

er ook andere initiatieven zoals de SunSpec Alliance, Cybersecurity Certification en de Rule 21 interconnection mandate, …
Sensibiliseren van de eindgebruiker blijft evenwel een aandachtspunt. We moeten de aandacht houden op een correcte implementatie: dit omvat het vermijden van het herhalen van wachtwoorden en het kiezen van voldoende complexe wachtwoorden.

d) De sector en ik hebben geen kennis van dergelijke meldingen.

4. Het rapport van de Nederlandse Rijksinspectie Digitale Infrastructuur dat eind mei de pers haalde, doet een aantal aanbevelingen hierover.
Fabrikanten zijn verantwoordelijk voor de conformiteit van hun producten. Maar de gebruiker kan zelf ook problemen signaleren of (gedeeltelijk) oplossen. Zo kan je bijvoorbeeld:
   - de aanwezigheid en juistheid van de verplichte CE-markering van het apparaat controleren;
   - de installateur van de zonnepaneelinstallatie herinneren aan zijn verantwoordelijkheid om installaties veilig en storingsvrij op te leveren;
   - alert zijn op verstoringen van bijvoorbeeld de radio of Wi-Fi, of die van buren;
   - sterke en unieke wachtwoorden gebruiken voor accounts en apparaten;
   - standaardwachtwoorden direct wijzigen;
   - regelmatig apparaten controleren op updates;
   - apparaten via een gastnetwerk verbinden met Wi-Fi;
   - tweefactor-authenticatie inschakelen, als dit kan;
   - ervoor kiezen om apparaten niet met het internet te verbinden, als dit niet nodig is;
   - kritisch bedenken of het nodig is om bepaalde gegevens te verstrekken.

5. Naar aanleiding van de vraag hierover in juni van dit jaar werd er op de webpagina van de Vlaamse Overheid over zonnepanelen informatie toegevoegd over het risico op hacking. Hierin wordt er gewezen op de belangrijkste maatregel om het risico op hacking te beperken, namelijk het vervangen van het standaardpaswoord van de omvormer door een persoonlijk en sterk wachtwoord. Dezelfde aanbeveling wordt gedaan voor een laadpaal. Naast de bewustwording binnen de aanmeldingsprocedure bij Fluvius ben ik op dit moment niet van plan om hiervoor een algemene communicatiecampagne op te zetten. Ik wacht de resultaten van de actie uit het Flexibiliteitsplan af.

6. Op dit moment ben ik dit niet van plan. Enerzijds is productnormering een federale bevoegdheid, anderzijds kunnen normen best opgelegd worden op Europese schaal. Via de NIS2-wetgeving en de Cyber Resilience wetgeving zal in de toekomst de cyberbeveiliging worden afgedwongen. Bijkomend werkt Europa momenteel ook aan een netwerkcode inzake sectorspecifieke voorschriften voor cyberbeveiligingsaspecten van grensoverschrijdende elektriciteitsstromen.

7. Op dit moment heb ik geen plannen om dat te doen. Enerzijds is het voor eigenaars van zonnepanelen, zoals reeds eerder aangehaald, vooral belangrijk om in te zetten op een goed wachtwoordbeheer en anderzijds is het belangrijk om te letten op de aanwezigheid van de verplichte CE-markering. Het implementeren van aspecten inzake cybersecurity in de CE-keuring van omvormers kan best op Europees niveau geregeld te worden, zoals via de Cyber Resilience wetgeving.