
Woonhuizen met zonnepanelen in Heerhugowaard. © ANP

Ict-lek zonnepanelen mogelijk bedreigend voor Europese stroomvoorziening

'Omvormer bevat heel scala aan kwetsbaarheden'

Het ministerie van Economische Zaken houdt in de gaten of het nodig is de ict-beveiliging van zonnepanelen te verbeteren. Aanleiding is een onderzoek van ict-beveiliger Willem Westerhof van het Haarlemse beveiligingsbedrijf ITsec. Hij stelt dat de stroomvoorziening in Europa gevaar loopt door een beveiligingslek in zonnepanelen. Stroombedrijven zien het probleem niet, maar onafhankelijke experts erkennen het gevaar.

Door: Laurens Verhagen Bard van de Weijer 4 augustus 2017, 02:00

Het lek zit volgens Westerhof in de vele duizenden omvormers, apparaten die de elektriciteit afkomstig van zonnepanelen geschikt maken voor het stroomnet. Hij stelt dat de apparaten zo slecht zijn beveiligd dat kwaadwillenden ze op afstand kunnen uitschakelen. In het ergste geval kan hierdoor op een zonnige dag in enkele seconden het equivalent van het stroomverbruik van miljoenen huishoudens wegvallen.

Dat kan ertoe leiden dat het elektriciteitsnet in onbalans raakt, waardoor in grote delen van Europa de stroom kan uitvallen. Dat gebeurt als de vraag naar stroom groter wordt dan het aanbod. Als daarbij een kritische grens wordt overschreden, worden automatisch delen in het stroomnet losgekoppeld, zeggen experts. Dan komen complete wijken zonder stroom te zitten.

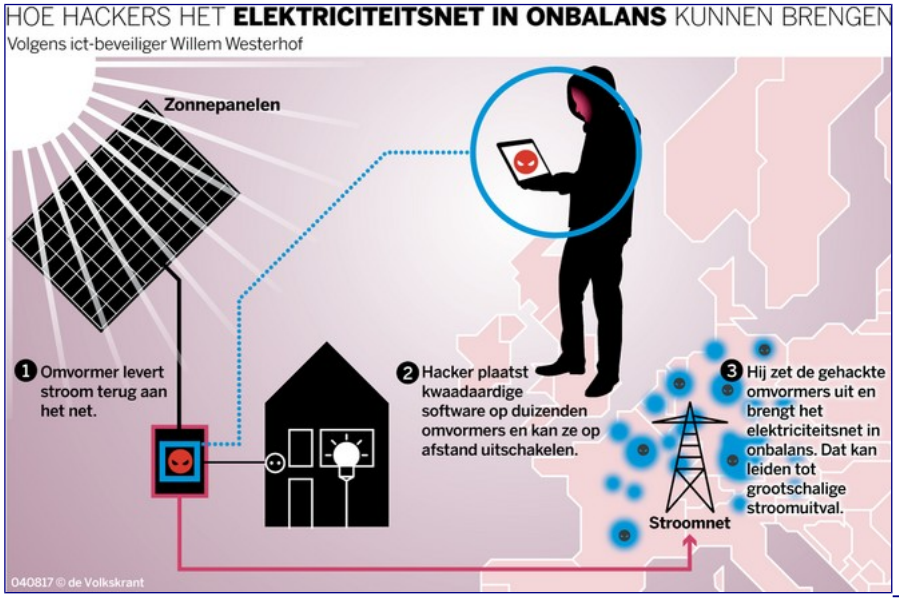
Tennet stelt in een reactie overal op voorbereid te zijn, ook op extreme situaties

Volgens een woordvoerder Economische Zaken staat het ministerie over het rapport van Westerhof in contact met netbeheerder Tennet, dat in Nederland het hoogspanningsnet beheert, en het Nationaal Cyber Security Centrum (NCSC) en zullen 'maatregelen worden genomen als blijkt dat dit noodzakelijk is'.

Tennet stelt in een reactie overal op voorbereid te zijn, 'ook op extreme situaties', aldus een woordvoerder. Het bedrijf zegt fabrikanten van omvormers verantwoordelijk te houden voor de beveiliging daarvan.

Westerhof heeft omvormers van marktleider SMA onderzocht. Daarin is sprake van 'een heel scala aan kwetsbaarheden'. Zo wordt kopers van een omvormer niet gevraagd bij de installatie ervan het standaardwachtwoord te wijzigen, waardoor vaak het makkelijk te raden '0000' wordt gebruikt.

Tekst gaat verder onder de afbeelding.



© de Volkskrant

Geheime superwachtwoorden

De apparaten zijn niet beveiligd tegen zogenoemde brute force-aanvallen

Ook zijn de apparaten niet beveiligd tegen zogenoemde brute force-aanvallen, waarmee een oneindige reeks wachtwoorden op een apparaat wordt afgevuurd tot het juiste gevonden is.

Een van de grootste gevaren schuilt in het gebruik van geheime superwachtwoorden door de fabrikant. Als een hacker er één weet te achterhalen, heeft hij in een klap de controle over elk apparaat van SMA, zegt Westerhof.

Een mogelijk scenario is volgens hem dat kwaadwilligen malware installeren in bedrijfs- en thuisnetwerken waar de omvormers aan hangen. Daar houdt de malware zich slapend tot het moment dat de hacker de opdracht geeft alle omvormers in een keer uit te schakelen.

Zo'n malwareaanval is vergelijkbaar met het recente Petyavirus dat zich verborgen hield in een Oekraïens boekhoudpakket en dat eind juni wereldwijd computersystemen van bedrijven platlegde, onder meer in de haven van Rotterdam.

> Een hacker die een superwachtwoord bemachtigt heeft in één klap de controle over elk apparaat van SMA
>
> Willem Westerhof, ict-beveiliger bij ITsec

Westerhof zegt dat er voldoende apparaten van SMA benaderbaar zijn om op een zonnige dag 15 gigawatt vermogen te kunnen wegnemen. Maar ook een kleinere dip zal 'al aardig merkbaar' zijn, denkt Richard van Leeuwen, hoogleraar sustainable energy systems van Saxion University of Applied Sciences. Peter Palensky, hoogleraar intelligente energienetwerken aan de TU Delft, zegt eveneens dat een aanval van voldoende schaal de stabiliteit in gevaar kan brengen. Geen van de geraadpleegde experts wil een grenswaarde noemen waarbij het net omvalt. Het afschakelen van complete wijken ziet Palensky als 'een laatste redmiddel'.

Dit afschakelen gebeurt inderdaad zelden, maar komt voor: in 2006 kwamen grote delen van Europa zonder stroom te zitten toen na het afkoppelen van een hoogspanningskabel in Duitsland een tekort van 5 gigawatt ontstond. Onder meer Parijs en Madrid kwamen toen uren zonder stroom te zitten. In Nederland viel de elektriciteit uit in een deel van Noord-Brabant.

Het jaarverslag over 2016 meldt dat SMA alleen al voor de particuliere markt omvormers voor 17 gigawatt aan zonvermogen levert. Westerhof heeft niet naar andere merken gekeken, maar vermoedt dat daar ook veel mis zal zijn met de beveiliging. De resultaten van zijn onderzoek presenteert hij maandag tijdens hackersfestival SHA2017 in Zeewolde.

Nauwelijks iets gedaan

> Fabrikant SMA wijst naar de gebruiker, die moet zorgen dat zijn netwerk honderd procent veilig is

Fabrikant SMA wijst naar de gebruiker. In een document met richtlijnen staat dat deze moet zorgen dat zijn netwerk honderd procent veilig is. De recente Petya-aanval heeft laten zien dat onrealistisch is, zegt de beveiliger van ITsec.

Westerhof heeft zijn bevindingen vorig jaar vóór Kerstmis al gedeeld met SMA, Tennet en het NCSC. Kort daarna heeft SMA Westerhof uitgenodigd om de kwetsbaarheden te bespreken. Nu, ruim een half jaar later, heeft het bedrijf volgens de beveiligingsexpert nauwelijks iets gedaan om de concrete dreiging weg te nemen. Westerhof heeft daarom besloten zijn bevindingen naar buiten te brengen.

SMA ontkent tegen de Volkskrant dat zijn omvormers niet goed beveiligd zijn. Het stelt dat het om 'enkele zeer geïsoleerde producten' gaat en dat er 'technische correcties worden uitgevoerd'. De beveiliger heeft zijn bevindingen voorgelegd aan de zogenoemde Common Vulnerabilities and Exposures Authority (CVE Authority), een internationale organisatie waar beveiligers nieuw

ontdekte kwetsbaarheden melden. Tegenover CVE Authority heeft SMA de gevonden kwetsbaarheden erkend. Ze worden vandaag op de website van de organisatie als zero days (nieuw ontdekte beveiligingslekken) gepubliceerd.