Nieuwe cybersecurity eisen (RED 3.3): springplank voor veiligere Smart Energy oplossingen?

Juni 2024

Hoe slimmer de energie-apparaten in huis worden, hoe meer we ook moeten kijken naar cyberveiligheid. Toch bestaan er tot op heden nauwelijks cyberbeveiligingsregels voor dit soort consumentenelektronica. Augustus 2025 komt daar verandering in, met wettelijke eisen waar fabrikanten aan moeten voldoen. Dit is een opstap naar de Cyber Resilience Act, die vanaf 2027 nog veel strengere eisen gaat stellen. In dit stuk gaan we in op de cyberveiligheidsrisico's rond slimme energie-apparatuur en of deze met de nieuwe eisen goed worden afgedekt. Het is bedoeld als gespreksstarter in de energiesector, omdat het probleem complex is en verschillende expertise nodig is, zowel uit de energie- als IT-wereld. We nodigen fabrikanten en leveranciers, evenals brancheorganisaties, beleidsmakers, standaardisatieorganisaties, de toezichthouder en kennispartijen uit om hun visie te delen en met ons en elkaar in gesprek te gaan. Met deze input adviseert de Topsector Energie de overheid bij haar beleidsontwikkeling, bedrijven bij hun innovatie-aanpak en kennisinstellingen bij hun onderzoeksvragen.

topsector energie

Slim energiemanagement dankzij het Internet of Things

De energietransitie zorgt voor elektrificatie van de energievoorziening in en rondom de woning. Steeds meer mensen leggen zonnepanelen op het dak, stappen over op elektrisch rijden en ruilen de cv-ketel in voor een (hybride) warmtepomp. Tegelijkertijd vindt digitalisering plaats. Het aantal apparaten dat op een slimme manier aangestuurd wordt neemt hierdoor toe, denk aan thuislaadpunten, warmtepompen, omvormers voor zonnepanelen en vermoedelijk straks ook thuisbatterijen. Al deze ‘slimme’ apparaten maken onderdeel uit van het Internet of Things* en worden ook wel IoT-apparaten genoemd.

Door fluctuerende energieprijzen en de opkomst van dynamische contracten groeit de behoefte om slimmer om te gaan met energie in huis*. Het Internet of Things biedt mogelijkheden om de opwek en het verbruik van energie te optimaliseren. IoT-apparaten kunnen hun omgeving monitoren en veranderingen detecteren, instructies ontvangen en zelf actie ondernemen op basis van de gegevens die ze verzamelen. Software en algoritmes werken daarbij als ‘energiemanagers’ en sturen de apparaten op afstand aan. Met een Home Energie Management Systeem (HEMS) kun je -via een app op je telefoon of tablet- instellen dat de wasmachine draait als het waait of je geparkeerde elektrische auto oplaadt als de zon schijnt. En in de toekomst kan een hybride warmtepomp mogelijk schakelen tussen gas en elektriciteit op basis van de prijs of de auto stroom terug leveren aan huis als de zon onder is.

Het Internet of Things zorgt echter ook voor veiligheidsrisico’s. IoT-apparaten zijn doorgaans via een thuisnetwerk met het internet verbonden. Door gebrekkige beveiliging, onjuiste configuratie en kwetsbaarheden in de hard- of software ontstaat volgens het Nationaal Cyber Security Centrum het risico dat slimme apparaten vanaf het internet te benaderen zijn voor niet geautoriseerde personen. Iemand met kwade bedoelingen zou informatie kunnen stelen, instellingen veranderen, het apparaat op afstand bedienen of toegang verkrijgen tot het thuisnetwerk en zo tot andere daarop aangesloten apparaten*. Ook kan een apparaat onderdeel worden van een botnet, een netwerk van een groot aantal geïnfecteerde apparaten dat (door criminelen) gebruikt wordt voor het versturen van spam of uitvoeren van DDoS-aanvallen*, waarmee websites of systemen worden overbelast en

platgelegd. Welke impact dit kan hebben werd duidelijk in 2016, toen hackers de bewoners van twee appartementsgebouwen in Lappeenranta, Finland, in de kou zette nadat ze erin slaagden via de slimme thermostaten de klimaatcontrolesystemen te hacken*.

Cybersecurityrisico's voor het elektriciteitsnet

Bij de Topsector Energie zien we niet alleen een veiligheidsrisico voor de gebruikers van dit soort apparatuur maar ook voor de stroomvoorziening. De energietransitie en digitalisering zorgen voor ingrijpende veranderingen in het elektriciteitssysteem. Welke kwetsbaarheden ontstaan en welke gevolgen er zijn voor de betrouwbaarheid van de stroomvoorziening is nog moeilijk te overzien.
Door elektrificatie neemt het stroomverbruik toe en wordt het netwerk zwaarder belast. De inzet van meer decentrale hernieuwbare bronnen zoals wind- en zonne-energie maakt het afstemmen van opwek en verbruik bovendien een complexe opgave. Dat komt omdat energieproductie meer afhankelijk raakt van het weer en verspreid is over een groter aantal opweklocaties. Het bewaken van de balans op het netwerk, wat cruciaal is voor een veilige en betrouwbare stroomvoorziening, wordt daarmee lastiger voor de landelijke netbeheerder*.

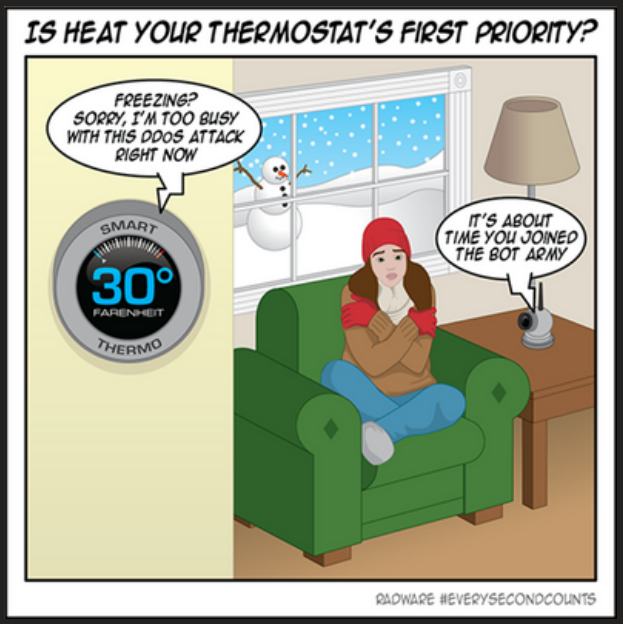
Als een groot aantal huishoudelijke apparaten met relatief hogere vermogens, zoals de warmtepomp of thuislaadpunt, simultaan onvoorspelbaar gedrag vertonen -bijvoorbeeld door op een bepaald moment tegelijkertijd aan te springen- ontstaat er een groot verschil tussen het vooraf ingeschatte verbruik en het actuele verbruik van stroom. De enorme onverwachte piekvraag kan grote gevolgen hebben voor de stabiliteit van het net, met verstoring of uitval in de stroomvoorziening tot gevolg.

De oorzaak kan een niet opzettelijke fout zijn, zoals een misconfiguratie of software-updatefout die een bug introduceert. Maar het kan ook komen door een cyberaanval. Op dit laatste moeten we ons beter voorbereiden. Het Cybersecurity Beeld Nederland 2023* laat zien dat de digitale dreiging vanuit verschillende actoren (statelijke actoren, georganiseerde criminaliteit en hacktivisten) onverminderd groot is. We moeten daarom rekening houden met verschillende scenario's, ook een waarbij een grootschalige gecoördineerde cyberaanval plaatsvindt op een groot aantal energie-apparaten en deze onverwacht aan- of uitgezet worden om de stroomvoorziening te verstoren. Gezien de oplopende geopolitieke spanningen door de oorlog in Oekraïne omschrijft de RDI dit als reëel scenario*.

Hoewel er geen praktijkvoorbeelden bekend zijn, blijkt uit simulaties met batterijen in elektrische voertuigen dat gerichte manipulatie een bedreiging vormt voor de stabiliteit van het lokale elektriciteitsnet*. Grootschalig onverwacht piekverbruik kan de servicekwaliteit verminderen,

gevoelige apparatuur beschadigen, stroomstoringen en lokale stroomuitval veroorzaken. Onderzoek naar cascade effecten laat bovendien zien dat cyberaanvallen op het elektriciteitsnet opeenvolgende storingen kunnen veroorzaken, wat kan leiden tot een wijdverspreide black-out*. In het geval van langdurige uitval kan onrust in de samenleving ontstaan met als gevolg daarvan onveiligheid*.

Gezien de grote ontwrichtende gevolgen van dat scenario moeten we niet afwachten tot het een keer misgaat maar nu maatregelen nemen om IoT-apparatuur, evenals het elektriciteitssysteem, beter te beveiligen en meer weerbaar te maken. In het veiliger maken van producten speelt normering door de overheid een grote rol. Zonder normering van de overheid moeten fabrikanten zelf bepalen aan welke veiligheidseisen en marges hun apparaten voldoen.



Bron: Radware

Belangrijke rol voor wetgeving en normen

In 2021 activeerde de Europese Commissie drie nieuwe eisen op het gebied van cybersecurity die vanaf 2025 zullen gaan gelden. Dat gebeurde via een aanpassing in artikel 3.3 van de Richtlijn Radioapparatuur ('RED 3.3'). De eisen moeten ervoor zorgen dat netwerken beter worden beveiligd en dat slimme apparaten geen onderdeel meer kunnen worden van een botnet. Ook moet privacygevoelige data worden beschermd en dient de productgebruiker te worden beschermd tegen online fraude*. Het gaat gelden voor alle consumentenelektronica met draadloze communicatieopties zoals WiFi, bluetooth, LTE of Zigbee.

Deze nieuwe RED 3.3 treedt op 1 augustus 2025 officieel in werking. Om een product na die datum op de EU-markt te brengen moeten fabrikanten en leveranciers aantonen dat ze aan de eisen voldoen. Dat kan op twee manieren. Met een conformiteitsverklaring op basis van een geharmoniseerde norm of via een test met certificering door een Notified Body (NoBo). De Europese Commissie heeft de standaardiseringsorganisaties CEN-CENELEC gevraagd om een geharmoniseerde norm te ontwikkelen, die naar verwachting begin september 2024 beschikbaar zal zijn*.

Het is belangrijk dat deze geharmoniseerd norm op tijd komt. Het gaat om ontzettend veel producten en zonder geharmoniseerde norm is de enige route certificering via een NoBo.

De enige NoBo in Nederland dat een EU-typekeuringscertificaat kan afgeven voor de RED is Kiwa. Hoewel fabrikanten kunnen kiezen voor een andere Europese NoBo, bijvoorbeeld het Spaanse DEKRA of Duitse TÜV, is het zeer de vraag of de Europese NoBo's de capaciteit hebben voor het totaal aan producten die op de markt komen.

Een van de grote uitdagingen bij normering betreft het testen. In tegenstelling tot fysieke testcriteria zoals de weersbestendigheid van een kabel of de hitte die een apparaat mag uitstralen is cybersecurity niet meetbaar*. Als het gaat om productveiligheid zijn IoT apparaten een relatief nieuw domein. Voor de normeringscommissies is het dan ook een uitdaging om, samen met de Europese Commissie, toezichthouders en testhuizen tot een geharmoniseerde norm te komen*.

De RED 3.3 is een belangrijke stap maar dekt niet alles af

De Topsector Energie ziet de RED 3.3 als zeer belangrijke stap. Fabrikanten, importeurs en leveranciers kunnen straks niet meer om cybersecurity heen als een inherente productkwaliteit. De RED 3.3 gaat hen verplichten om het bewustzijn over cyberveiligheid van de hele keten naar een hoger niveau te tillen en werk te maken van zaken als sterke wachtwoorden, kwetsbaarheidsrapportages en langdurig updatebeleid. Gezien de doorlooptijd van IoT-productontwikkeling is onze oproep aan fabrikanten, importeurs en leveranciers om nu al actie te ondernemen om straks aan de eisen te kunnen voldoen. Lees je in en laat je indien nodig adviseren door een NoBo of cybersecuritytesthuis als eerste stap.

Tegelijkertijd signaleert de Topsector Energie dat we er met de RED 3.3 nog niet zijn. Zelfs als slimme energie-

Hoe staan slimme apparaten er nu voor?

In 2021 startte de Rijksinspectie Digitale Infrastructuur (RDI) een onderzoek naar de cyberveiligheid van omvormers van zonnepaneelinstallaties. Ter voorbereiding op de RED 3.3 werd onderzocht of de omvormers voldoen aan de nieuwe wettelijke eisen. Omdat er nog geen norm voor de RED 3.3 beschikbaar was is getest op basis van de ETSI EN 303 645, een bestaande cyberbeveiligingsnorm. Deze norm bevat richtlijnen voor de beveiliging van IoT-consumentenproducten, bijvoorbeeld voor wachtwoorden, het rapporteren van kwetsbaarheden en software updates. Uit de testen van de RDI bleek dat geen van de negen onderzochte omvormers [op alle punten] voldeed aan de gebruikte norm. Zonnepaneelinstallaties zouden hierdoor eenvoudig te hacken zijn, waarna ze kunnen worden uitgeschakeld of ingezet voor DDoS-aanvallen. Ook kunnen persoons- en gebruiksgegevens worden onderschept.
Lees het onderzoek van de Rijksinspectie Digitale Infrastructuur hier.

apparaten aan de nieuwe eisen en normen voldoen blijft er een risico bestaan voor het elektriciteitssysteem. Cybercriminelen en statelijke actoren zullen zich blijven ontwikkelen, en ook aanvallen plegen via de achterkant van het energiesysteem: de backoffice omgeving en bijhorende infrastructuur.

Omdat IoT-apparaten niet over de benodigde rekenkracht of geheugen beschikken maken ze gebruik van een backoffice-omgeving*. Dat gebeurt via een gateway, een verbindingspunt die communicatie tussen het apparaat en een centrale server mogelijk maakt. Op deze server -een publieke Cloud-omgeving van bijvoorbeeld Microsoft of Amazon, private Cloud of in sommige gevallen een eigen server van de leverancier- worden data verzameld, verwerkt en opgeslagen. De backoffice-omgeving maakt toegang tot het apparaat op afstand mogelijk. Handig voor de gebruiker, maar ook voor de fabrikant die op deze manier software updates draait*. De backoffice omgeving van IoT-apparaten, net als de bijhorende mobiele of webapplicaties, vallen echter niet in scope van de RED 3.3. Dat is zorgwekkend want juist via de backend zijn schaalbare cyberaanvallen mogelijk.

Uit testen door ethische hackers kwam naar voren dat servers waar IoT-apparaten mee communiceren grotendeels niet of slecht beveiligd zijn*. Niet alleen privacygevoelige data bleken uit te lezen, ook was het mogelijk om apparaten te bedienen en software aan te passen. Een ander voorbeeld is de hack op Solarman, een Chinees bedrijf dat de software van verschillende merken omvormers van zonnepanelen beheert. In 2021 lukte het een ethische hacker om toegang te krijgen tot het platform, en kon hij de gps-coördinaten en opbrengsten van zonnepanelen real-time volgen. Ook kon hij de firmware van omvormers downloaden, aanpassen en weer uploaden. In Nederland ging het om 42.000 omvormers, maar wereldwijd waren er 1 miljoen omvormers aangesloten op het platform. De voorbeelden tonen aan dat het mogelijk is om via de backoffice omgeving een schaalbare cyberaanval uitvoeren en op afstand een groot aantal apparaten aan- of uit te zetten*.

Kortom, een apparaat kan voldoen aan de RED 3.3 maar nog steeds een cyberrisico vormen voor de stabiliteit van ons elektriciteitssysteem. Het is daarom belangrijk dat er meer inzicht komt in de kwetsbaarheden rondom Smart Energy IoT-apparaten, inclusief de backend omgevingen en applicaties, en de impact die cyberaanvallen op deze apparaten kunnen hebben op het elektriciteitssysteem.

Cyber Resilience Act

Om de weerbaarheid verder te verhogen kondigde de Europese Commissie in 2022 de Cyber Resilience Act (CRA) aan. Dit is een meer omvattende verordening die (naar verwachting) in 2027 inwerking treedt en de RED 3.3 vervangt. De CRA heeft een bredere reikwijdte, namelijk *‘elk software- of hardware product en de oplossingen voor gegevensverwerking op afstand, met inbegrip van software- of*

hardwarecomponenten die afzonderlijk in de handel worden gebracht'. De ondersteunende diensten bij een apparaat, de backoffice-omgeving, vallen daarmee ook binnen deze wetgeving. De CRA bevat verplichtingen voor fabrikanten en softwareontwikkelaars, bijvoorbeeld rond het ontwerpproces en beveiligingsupdates gedurende de hele levenscyclus van een product. Ook aan importeurs en leveranciers worden eisen gesteld*.

Daarnaast zal ook de nieuwe cyberbeveiligingswet (vertaling van de NIS2-richtlijn) van invloed zijn, die zich richt op cyberrisico's voor netwerk- en informatiesystemen en waar zowel de energiesector als clouddienstenleveranciers aan moeten voldoen. Hoe de NIS2 en de RED3.3/CRA zich precies tot elkaar verhouden op het gebied van Smart Energy IoT apparaten zal de komende periode duidelijk moeten worden.

Oproep aan fabrikanten, ontwikkelaars en leveranciers

Kortom: de RED 3.3 is een belangrijke opstap naar betere beveiliging. De nieuwe wettelijke eisen fungeren als noodzakelijke springplank voor fabrikanten, importeurs en leveranciers naar een toekomst met meer inherent cyberveilige apparaten. Bovendien komt er nog meer aan; wat betekent dat als je niet nu aan de slag gaat met de RED 3.3 je nooit op tijd klaar zal zijn voor de CRA. Ook de NoBo's en testhuizen hebben deze springplank nodig. Het zal een flinke uitdaging zijn om de komende jaren meer technische experts aan te trekken en de capaciteit op te bouwen voor het uitvoeren van gedegen IoT-testen en certificering.

De Topsector Energie wil de dialoog over digitaal veilige Smart Energy apparaten stimuleren. Dit stuk is daar een eerste aanzet toe en dient als gespreksstarter met de sector. Herken je de geschetste cyberrisico's en hoe kijk jij naar jouw rol en verantwoordelijkheid? Wat is de verwachtte impact van de RED 3.3 en CRA op de energiesector, voor de beveiliging van apparaten maar ook bijvoorbeeld voor de innovatiekracht op het gebied van slimme energietoepassingen? Welke kennis denk je dat nodig is voor digitaal veiligere apparaten en wie moeten daarvoor bij elkaar gebracht? We nodigen fabrikanten, ontwikkelaars en leveranciers, evenals brancheorganisaties, securitybedrijven en testhuizen, standaardisatieorganisaties, overheid en kennispartijen uit om te reageren en met ons en elkaar in gesprek te gaan.

Meer weten of meepraten? Neem contact op

Auteur: Soe van Dijk
programmacoördinator Topsector Energie Digitalisering
Soe.vandijk@topsectorenergie.nl
Lees meer over cybersecurity
Vormgeving: Rosa Boon

Bronnenlijst

Flexible Power Alliance (2022) De Kansen Voor Energiemanagement In De Woning, via https://nl.flexible-energy.eu/nieuws-events/energiemanagement-in-en-om-de-woning-biedt-grote-kansen/.

Nationaal Cyber Security Centrum (2023) Basis-beveiligingsmaatregelen Slimme Apparaten, via https://www.ncsc.nl/wat-kun-je-zelf-doen/documenten/factsheets/2019/juni/01/factsheet-beveilig-apparaten-gekoppeld-aan-internet.

Mathews, L. (2016) 'Hackers Use DDoS Attack To Cut Heat To Apartments' Forbes via https://www.forbes.com/sites/leemathews/2016/11/07/ddos-attack-leaves-finnish-apartments-without-heat/#5234234e1a09.

Raad van de Leefomgeving (2018) Stroomvoorziening onder digitale spanning via https://rli.nl/sites/default/files/stroomvoorziening_onder_digitale_spanning_rli_advies.pdf.

Cybersecurity Beeld Nederland 2023 https://www.rijksoverheid.nl/documenten/rapporten/2023/07/03/tk-bijlage-cybersecuritybeeld-nederland-2023.

NOS Nieuws, 30 mei 2023 'Zonnepanelen gevoelig voor hacks en storingen: 'Hack stroomnet is realistisch' via https://nos.nl/artikel/2477039-zonnepanelen-gevoelig-voor-hacks-en-storingen-hack-stroomnet-is-realistisch.

Zhdanova, M. et al (2022) Local Power Grids at Risk – An Experimental and Simulation-based Analysis of Attacks on Vehicle-To-Grid Communication, ACSAC: Annual Computer Security Applications Conference https://www.researchgate.net/publication/366017368_Local_Power_Grids_at_Risk_-_An_Experimental_and_Simulation-based_Analysis_of_Attacks_on_Vehicle-To-Grid_Communication.

Subramaniam Rajkumar, V., Stefanov, A., Presekal, A., Palensky, P., & Rueda, J. L. (2023). Cyber Attacks on Power Grids: Causes and Propagation of Cascading Failures. IEEE Access, 11, 103154-103176 https://research.tudelft.nl/en/publications/cyber-attacks-on-power-grids-causes-and-propagation-of-cascading-.

Gedelegeerde Verordening (EU) 2023/2444 van de Commissie van 20 juli 2023 tot wijziging van Gedelegeerde Verordening (EU) 2022/30 wat de datum van toepassing van de essentiële eisen voor radioapparatuur betreft, en tot rectificatie van die verordening, C(2023)4823 https://ec.europa.eu/transparency/documents-register/detail?ref=C(2023)4823&lang=nl.

NEN Artikel 'Ook fabrikanten zullen aan security eisen moeten voldoen, https://www.nen.nl/en/nieuws/cybersecurity/ook-fabrikanten-zullen-aan-security-eisen-moeten-v
Saidi, S. J., Matic, S., Gasser, O., Smaragdakis, G., & Feldmann, A. (2022). Deep Dive into the IoT Backend Ecosystem. In Proceedings of the 22nd ACM Internet Measurement Conference (pp. 488–503). https://pure.tudelft.nl/ws/portalfiles/portal/137770971/3517745.3561431.pdf.

Kaspersky, What is IoT? Via https://www.kaspersky.nl/resource-center/definitions/what-is-iot.

Whittaker, Z. (2017) 'Exposed IoT servers let hackers unlock prison cells, modify pacemakers' ZDNET via https://www.zdnet.com/article/exposed-servers-hack-prison-cells-alter-pacemakers/.

Schults, S. (2022) Hacker kon software van zonnepanelen met omvormers Chinese Solarman aanpassen, Tweakers via https://tweakers.net/nieuws/199310/hacker-kon-software-van-zonnepanelen-met-omvormers-chinese-solarman-aanpassen.html.

topsector energie