INTERNETCONSULTATIE CYBERBEVEILIGINGSBESLUIT

INBRENG ELAADNL

Door de verwachte, sterke groei van het aantal laadpunten voor elektrische voertuigen in Nederland wordt de potentiële impact van een cyberaanval op de laadinfrastructuur steeds groter. Een mogelijke aanval op de Nederlandse laadinfrastructuur zal niet alleen de mobiliteit in Nederland verstoren, maar kan ook leiden tot uitval van (delen van) het landelijke en Europese elektriciteitsnet, met grote economische en maatschappelijke schade tot gevolg. ElaadNL onderschrijft daarom het belang van de tijdige implementatie van de NIS2 middels het Cyberbeveiligingsbesluit en kijkt uit naar de verdere, veilige uitrol van laadinfrastructuur in Nederland.

Als kennisinstelling op het gebied van slim, duurzaam en veilig laden, adviseert ElaadNL aan de minister van Klimaat en Groene Groei om per ministeriële regeling invulling te geven aan de zorgplicht voor exploitanten van laadinfrastructuur (Charge Point Operators, CPO's). Hiervoor doet ElaadNL de volgende aanbevelingen:

1. CPO's moeten worden gehouden aan de ENCS-*requirements* door verplichte certificering van laadinfrastructuur op basis van IEC 62443.
2. Om veilig assetbeheer te borgen moet vereist worden dat concessiehouders ISO-27001-gecertificeerd zijn en dat zij dit aantonen met een verklaring van toepasselijkheid.
3. De drempelwaarde voor een significant incident in het kader van de meldplicht moet worden vastgesteld op 100 MW.
4. CPO's moeten worden geacht kennis te nemen van laatste ontwikkelingen op cybergebied, bijvoorbeeld binnen samenwerkingsverbanden als Electric Vehicle Charging -ISAC.
5. In de definitie van mkb-bedrijven moet rekening worden gehouden met dochter- en zusterorganisaties. Deze organisaties delen vaak *backend*-systemen dus moeten even goed beveiligd zijn als grotere CPO's.

Deze punten licht ElaadNL verder toe, waarbij deze punten tevens als uitgangspunten voor de Nederlandse inzet voor Europese harmonisatie kunnen gelden.

ENCS-REQUIREMENTS ALS STANDAARD VOOR PUBLIEKE ÉN PRIVATE LAADINFRASTRUCTUUR

In 2016 heeft European Network for Cyber Security (ENCS) de **'Security requirements for procuring EV charging stations'** ontwikkeld. Deze standaard voor het beveiligen van laadinfrastructuur wordt momenteel breed ingezet in aanbestedingen voor publieke laadinfrastructuur. De nieuwste versie van deze security requirements is gebaseerd op de internationale norm IEC 62443, waardoor laadpunten gecertificeerd kunnen worden. Om ook de veiligheid van assetbeheer te borgen middels deze voorwaarden moeten huidige en toekomstige CPO's ook worden gecertificeerd op basis van ISO-27001. Door van de laadpuntexploitant/-beheerder te verlangen zich te laten certificeren, wordt zorggedragen dat laadpunten beveiligd blijven.

In Engeland is al wetgeving van toepassing voor (thuis)laadpunten, waarbij naar de ENCS-Requirements wordt verwezen als een manier om compliant te zijn. *"Compliance with the European Network for Cyber Security EV Charging Systems Security Requirements is considered an appropriate level of cybersecurity."* Het is dus een internationaal geaccepteerde, bekende norm.

Uit pen- en hacktesten blijkt dat laadpunten die aan deze eisen voldoen veel veiliger zijn dan laadpunten die hier niet aan voldoen. De huidige versie EV-211-2025 richt zich op:

- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communication security
- System acquisition, development and maintenance
- Supplier relationships
- Information security aspects of business continuity management

Om het voor fabrikanten overzichtelijk en betaalbaar te houden, maar ook om een betrouwbare partner te zijn wat betreft de normen die gehanteerd worden, pleiten wij ervoor **de veilige uitrol van laadinfrastructuur te borgen door de ENCS-Requirements tijdig op te nemen in een ministeriële regeling** ter invulling van de zorgplicht voor CPO's.

Mochten zich, ondanks de aanvullende veiligheidsmaatregelen, toch cyberincidenten voordoen, dan moet een drempelwaarde worden vastgesteld voor significante incidenten ten behoeve van de meldplicht. Wij adviseren hiervoor een **drempelwaarde van 100 Megawatt,** net zoals voor elektriciteitscentrales en windparken.

CYBERRISICO'S VOORKOMEN IN DE HELE KETEN

Om cyberrisico's te voorkomen moeten CPO's op de hoogte blijven van de laatste ontwikkelingen op het gebied van cyberveiligheid. Digitale ontwikkelingen gaan snel, waardoor constant nieuwe cyberrisico's opduiken. Samenwerking tussen marktpartijen en cyberbedrijven moet daarom worden aangemoedigd, bijvoorbeeld in Electric Vehicle Charging ISAC-verband, zodat beiden vanuit hun expertise kennis kunnen delen. Daarom moet in de regeling worden vastgelegd dat **CPO's worden geacht kennis te nemen van de laatste ontwikkelingen op het gebied van cybersecurity**.

Ook moet **verhinderd worden dat kleinere CPO's die onderdeel zijn van een grotere, internationale holding worden getoetst als mkb-bedrijven** via een risicogebaseerde benadering. Kleinere CPO's zijn vaak onderdeel van een grotere holding met meerdere dochter- en zusterorganisaties in andere (Europese) landen. Veelal delen zij *backend*-systemen, waardoor cyberrisico's bij het ene bedrijf automatisch leiden tot risico's bij andere bedrijven. Tevens wordt door verdere integratie het elektriciteitsnet een Europees net. Risico's in andere lidstaten zijn dan dus net zo goed risico's voor Nederland. Daarom moet bij het aanwijzen van mkb-bedrijven personeelsaantallen en omzet van zusterorganisaties mee worden gerekend. Tevens vraagt de

Europese integratie van de netten om **uniformering van cybersecurityeisen op Europees niveau**.