INTERNETCONSULTATIE CYBERBEVEILIGINGSWET

INBRENG ELAADNL

Door de verwachte sterke groei van het aantal laadpunten in Nederland wordt de potentiële impact van een cyberaanval op laadinfrastructuur voor elektrische voertuigen steeds groter. Als een aanval op laadinfrastructuur slaagt kan de mobiliteit in Nederland verstoord worden en bestaat zelfs een kans dat het landelijke elektriciteitsnet uitvalt met grote economische en maatschappelijke schade tot gevolg.

ElaadNL onderschrijft dan ook het belang van de tijdige implementatie van de NIS2 middels de Cyberbeveiligingswet 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 om per AMvB invulling te geven aan de eisen voor laadinfrastructuur, gebaseerd op de al bestaande en breed geaccepteerde ENCS-Requirements.

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 al breed ingezet in aanbestedingen voor publieke laadinfrastructuur. Hoewel er momenteel nog geen formele internationale industriestandaarden zijn, zijn marktpartijen dus al langer bekend met de ENCS-Requirements en sorteren veel partijen al voor middels deze eisen. Door van de laadpuntexploitant/ beheerder te verlangen deze eisen toe te passen, wordt zorggedragen dat laadpunten gedurende de gehele levensduur veilig kunnen functioneren.

In Engeland is al wetgeving van toepassing voor (thuis)laadpunten, waarbij eveneens naar deze 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 in de laadinfrastructuur.

Daarnaast blijkt uit pen- en hacktesten dat laadpalen die aan deze eisen voldoen veel veiliger zijn dan laadpalen die hier niet aan voldoen. Het is dus dé standaard voor het beveiligen van laadpunten en tevens een deel van de keten. De huidige versie EV-301-2019 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 AMvB.