8 tips voor digitale veiligheid van oplaadpunten bij VvE's

Oplaadpunten zijn vaak verbonden met internet om de uitwisseling van informatie mogelijk te maken. Hierdoor kan slim laden (smart charging) worden toegepast en kunnen laadtransacties financieel worden afgerekend.

Dit maakt oplaadpunten echter ook kwetsbaar voor cyberaanvallen. Bij de aanschaf, de installatie en het gebruik van de oplaadpunten verdient de digitale veiligheid (cybersecurity) daarom aandacht.

Wij geven je 8 tips voor digitale veiligheid van oplaadpunten bij een VvE:

1. Als je gebruik maakt van een Charge Point Operator, vraag dan of deze ISO 27001 gecertificeerd is.
2. Gebruik voor de communicatie tussen oplaadpunt en back-end het Open Charge Point Protocol (OCPP), bij voorkeur versie 2.0.1 (of nieuwer).
3. Zorg dat alle communicatie beveiligd is door encryptie om inbreuk op de data door ongeautoriseerde derden te voorkomen.
4. Zorg voor beveiliging van digitale toegang tot het oplaadpunt, zodat bijvoorbeeld monteurs niet zonder wachtwoord kunnen inloggen.
5. Vraag aan de Charge Point Operator of deze een melding krijgt als iemand ongeautoriseerd fysieke toegang tot het oplaadpunt probeert te krijgen.
6. Vraag aan de laadpuntfabrikant of de Charge Point Operator of het oplaadpunt voldoende geheugen- en processorcapaciteit heeft om toekomstige software-updates te kunnen installeren.
7. Informeer hoe wordt gecontroleerd dat alleen geverifieerde software (voorzien van de juiste certificaten en digitale handtekeningen) op het oplaadpunt geïnstalleerd wordt.
8. Kijk voor meer informatie bij de Security Requirements die door ElaadNL en ENCS zijn opgesteld.